VALTIOVARAINMINISTERIÖ

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä; VAHTIn toimintakertomus vuodelta 2017

Valtiovarainministeriön julkaisu – 16/2018

Julkisen hallinnon ICT

Valtiovarainministeriön julkaisuja 16/2018

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä; VAHTIn toimintakertomus vuodelta 2017

Valtiovarainministeriö, Helsinki 2018

Valtiovarainministeriö

ISBN: 978-952-251-948-1

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2018

Kuvailulehti

Julkaisija	Valtiovarainministeriö		23.5.2018
Tekijät	Kimmo Rousku (toimittaja)		
Julkaisun nimi	Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä; VAHTIn toimintakertomus vuodelta 2017		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisu 16/2018		
Teema	Julkisen hallinnon ICT		
ISBN PDF	978-952-251-948-1	**ISSN PDF**	1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-251-948-1		
Sivumäärä	59	**Kieli**	xxx
Asiasanat	VAHTI, digitaalinen turvallisuus, riskienhallinta, tietoturvallisuus, kyberturvallisuus, tietosuoja, toiminnan jatkuvuus		

Tiivistelmä

Valtiovarainministeriön tehtävänä on julkisen hallinnon tietoturvallisuuden yleinen kehittäminen ja valtionhallinnon tietoturvallisuuden ohjaus. Valtiovarainministeriön toimivalta tietoturvallisuuden ja tietohallinnon ohjauksessa ja kehittämisessä perustuu useisiin lakeihin, säädöksiin ja asetuksiin. Valtiovarainministeriö on asettanut julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) toimimaan julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä.

Vuoden 2017 alusta kolmen vuoden toimikaudelle asetettu VAHTI jatkaa yli kaksikymmentä vuotta jatkunutta tieto- ja kyberturvallisuuden, laajemmin ymmärrettynä digitaalisen turvallisuuden kehittämistä. Tässä julkaisussa kuvataan VAHTIn toimintaa, yhteistyötä ja vaikutusta vuonna 2017.

Vuoden 2017 aikana toteutettiin uusina kehittämistoimenpiteinä julkisen hallinnon digitaalisen turvallisuuden teemaviikko osana EU-alueen laajuista European Cyber Security Month-kokonaisuutta (ECSM). Toinen menestys on ollut vuoden aikana käynnistynyt yhteistyö Julkisen hallinnon tietohallinnon neuvottelukunnan (Juhta) kanssa liittyen tietosuojan ja tietoturvan yhteishankkeisiin. Vuoden aikana julkaistiin viisi julkaisua sekä osallistuttiin Pilkahduksia tulevaisuuteen - digitalisaation ja robotisaation mahdollisuudet –raportin tuottamiseen.

Valtiovarainministeriö mittaa digitaalista turvallisuutta julkisessa hallinnossa. Tavoitteena on tunnistaa kehittämisalueita ja kohdistaa niihin toimenpiteitä. Vuoden aikana toteutettiin ensimmäisen kerran sekä VAHTI-organisaatiokysely että henkilöstön ja johdon tietoturvabarometri valtionhallinnon ohella myös kunnille ja sairaanhoitopiireille. Näiden kyselyiden perusteella sekä organisaatiot että valtiovarainministeriö ovat pystyneet muodostamaan digiturvallisuuden kokonaiskuvaa sekä keskittämään resursseja niihin toimenpiteisiin, joilla saavutetaan parhaiten vaikuttavuutta digitaalisen turvallisuuden kehittämisessä.

Kustantaja	Valtiovarainministeriö
Julkaisun jakaja/myynti	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi

Presentationsblad

Utgivare	Finansministeriet		23.5.2018
Författare	Kimmo Rousku (redaktör)		
Publikationens titel	Ledningsgruppen för informations- och cybersäkerheten inom statsförvaltningen; VAHTI:s verksamhetsberättelse för 2017		
Publikationsseriens namn och nummer	Finansministeriets publikationer 16/2018		
Tema	Offentliga förvaltningens ICT		
ISBN PDF	978-952-251-948-1	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-251-948-1		
Sidantal	59	**Språk**	xxx
Nyckelord	VAHTI, digital säkerhet, riskhantering, informationssäkerhet, cybersäkerhet, datasekretess, verksamhetskontinuitet		

Referat

Finansministeriet ansvarar för den allmänna utvecklingen av informationssäkerheten inom den offentliga förvaltningen och inom statsförvaltningen för styrningen av informationssäkerheten. Finansministeriets behörighet inom styrning och utveckling av informationssäkerheten och informationsförvaltningen bygger på flera lagar, författningar och förordningar. Finansministeriet tillsatte ledningsgruppen för informations- och cybersäkerheten inom statsförvaltningen (VAHTI) som samarbets-, berednings- och koordineringsorgan för organisationer med ansvaret för utvecklandet och styrningen av den digitala säkerheten inom den offentliga förvaltningen.

VAHTI tillsattes för ett treårigt mandat från början av 2017 och fortsätter således den över tjugo år långa, omfattande utvecklingen av informations- och cybersäkerheten, som i framtiden går under det mer omfattande begreppet digital säkerhet. I den här publikationen beskrivs VAHTI:s verksamhet, samarbete och inverkan under 2017.

Nya åtgärder som utfördes 2017 var en temavecka för digital säkerhet inom den offentliga förvaltningen. Temaveckan ingick i den EU-omfattande temahelheten European Cyber Security Month (ECSM). Ett annat framsteg var det samarbete som inleddes tillsammans med delegationen för informationsförvaltningen inom den offentliga förvaltningen (JUHTA). Samarbetet anknyter till gemensamma projekt kring dataskydd och informationssäkerhet. Under året publicerades fem publikationer och projektet deltog i produktionen av rapporten Framtidsblickar – digitaliseringens och robotiseringens möjligheter.

Finansministeriet granskar den digitala säkerheten inom den offentliga förvaltningen. Målet är att identifiera utvecklingsområden och sätta in åtgärder kring dem. Under året genomfördes både VAHTI-organisationsenkäten och barometern för dataskydd bland personal och ledningsgrupp för första gången såväl i statsförvaltningen som i kommunerna och sjukvårdsdistrikten. Utifrån dessa enkäter har både organisationerna och finansministeriet kunnat bilda sig en helhetsbild över den digitala säkerheten. Resurserna har då kunnat koncentreras till de åtgärder som effektivast bidrar till att utveckla den digitala säkerheten.

Förläggare	Finansministeriet
Distribution/ beställningar	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: julkaisutilaukset.valtioneuvosto.fi

Description sheet

Published by	Ministry of Finance		23.5.2018
Authors	Kimmo Rousku (editor)		
Title of publication	The steering body for digital security in public administration; Annual report of the Government Information Security Management Board VAHTI in 2017		
Series and publication number	Ministry of Finance publications 16/2018		
Subject	Public Sector ICT		
ISBN PDF	978-952-251-948-1	**ISSN (PDF)**	1797-9714
Website address (URN)	http://urn.fi/URN:ISBN:978-952-251-948-1		
Pages	59	**Language**	xxx
Keywords	VAHTI; digital security; risk management; information security; cyber security; data protection; continuity of activities		

Abstract

The Ministry of Finance is responsible for developing information security in public administration in general and for steering information security in central government. The Ministry's mandate in these activities is based on a number of statutes and regulations. Public sector digital security management board (VAHTI) was appointed by the Ministry to serve as the cooperation, drafting and coordination body for the organisations responsible for developing and steering digital security in public administration.

During its new three-year term starting in 2017, VAHTI will continue its two-decade-long work to develop information and cyber security. In a broader sense, its future tasks will focus on the development of digital security. This publication describes the operation, cooperation and effects of VAHTI in 2017.

In 2017, a digital security week was organised as part of the European Cyber Security Month (ECSM). Another successful matter was cooperation launched with the Advisory Committee on Information Management in Public Administration (JUHTA) on matters relating to data protection and information security. Also in 2017, VAHTI released five publications and participated in the production of a report entitled 'Glimpses of the future – possibilities of digitalisation and robotisation'.

The Ministry of Finance measures digital security in public administration. The aim is to recognise areas of development and to carry out targeted actions. A VAHTI organisation survey and an information security barometer were conducted for the first time in the course of the year not only for personnel and management but also for municipalities and hospital districts. Based on these surveys, both organisations and the Ministry of Finance have managed to form an overall picture of digital security and to concentrate resources on measures that best enhance the effectiveness of digital security.

Publisher	Ministry of Finance
Distributed by/ Publication sales	Online version: julkaisut.valtioneuvosto.fi Publication sales: julkaisutilaukset.valtioneuvosto.fi

Sisältö

JOHDANTO

Valtiovarainministeriö asetti joulukuussa 2016 julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI) uudelle toimikaudelle 1.1.2017–31.12.2019.

Yleisesti vuotta 2017 voidaan kuvata termillä käyntiinlähtö ja sitä seurannut toiminnan vakiintuminen. Kokonaan uusiutunut toimintamalli, jossa digitaalista turvallisuutta kehitetään viiden asiantuntijaryhmän avulla, on vaatinut oman aikansa, jotta se on saatu toimimaan. Etukäteen eräs keskeisin vuoden 2017 tavoite liittyi tulevan tiedonhallintalainsäädännön yhteydessä uusittavaan tietoturvasäädöksiä koskeviin muutoksiin, ns. VAHTI 100-vaatimuksiin, mutta lainsäädännön aikataulun siirtyminen vuodella eteenpäin muutti ja siirsi tätä tavoitetta vastaavalla tavalla.

Vuoden 2017 menestyksiä ovat olleet VAHTIn yhdessä julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) asettaman tietoturva, tietosuoja ja varautumisen asiantuntijaryhmän kanssa tekemä yhteistyö koskien tietosuojan yhteishankkeita. Toinen menestys oli lokakuussa järjestetty ensimmäinen julkisen hallinnon digitaalisen turvallisuuden teemaviikko (JHDTTV), johon osallistui paikan päällä tai verkon kautta yli 4 000 henkeä.

Vuosi 2017 oli VAHTIn ja samoin JUHTA-toiminnan osalta juhlavuosi. Yhteistä 50 + toimintavuotta juhlistettiin 31.10.2017 järjestetyssä kutsuvierastilaisuudessa. Vaikka vuosittaisia VAHTI-päiviä on järjestetty 20 vuoden ajan, valtiovarainministeriön julkaisussa 6/1992 valtiohallinnon tietoturvallisuuspäätös todetaan, että ”Valtiovarainministeriötä avustaa näissä tehtävissä ministeriön asettama valtionhallinnon tietoturvallisuuden johtoryhmä”. Täten tietoturvallisuuden kehittämiseen aluksi valtion- ja nyt koko julkisessa hallinnossa on pitkät perinteet.

Eräs uuden VAHTIn keskeinen tavoite on ollut tiedon välittäminen toiminnassa olevien asiantuntijoiden ja organisaatioiden kesken. Tässä on onnistuttu hyvin, niin asiantuntijaryhmien kokousten kuin kuukausittaisten VAHTI-pääsihteerin toteuttamien katsausten avulla. Toiminnasta on myös tiedotettu laajasti uutiskirjeiden ja erillisten valtiovarainministeriön julkaisemien tiedotteiden avulla.

Tämän toimintakertomuksen 2. luvussa kuvataan toimikauden ensimmäistä toimintavuotta siten, kuinka valtiovarainministeriön toiminnalle asetetut tavoitteet on saavutettu. Kolmannessa luvussa arvioidaan VAHTIn oman toimintasuunnitelman näkökulmasta tavoitteiden toteutumista. Neljännessä luvussa kuvataan julkisen hallinnon digitaalisen turvallisuuden organisaatiokyselyn sekä VAHTIn henkilöstön ja johdon tietoturvabarometrin keskeiset tulokset ja niitä koskevat havainnot. Toimintakertomuksen viimeinen eli viides luku esittelee VAHTIn toimintaa vuoden 2017 osalta niin johtoryhmän, sihteeristön, asiantuntijajaoston, tilaisuuksien sekä muiden aktiviteettien osalta.

VAHTIn keräämien mittareiden tarkoituksena on mitata toiminnan vaikuttavuutta sekä julkisen hallinnon organisaatioiden digitaalisen turvallisuuden tilannetta. Vuoden 2017 tulokset osoittavat, että tieto- ja kyberturvallisuuden osalta ei ole tapahtunut mitään merkittävää kehittymistä, vaan tilanne on osin varsin vakiintunut. Valtionhallinnon osalta tilanne on varsin vakiintunut, kuntien osalta on tapahtunut pientä parannusta vuoteen 2016 verrattuna. Valtionhallinnon vuosien 2011-2015 nousu johtui vuonna 2010 voimaan astuneesta tietoturvallisuusasetuksesta. Vastaavanlaista kehittymistä voidaan odottaa joko lainsäädäntöön liittyvillä muutoksilla tai muilla erityisillä kehittämisohjelmilla. 25.5.2018 sovellettavaksi tulevan EU:n yleisen tietosuoja-asetukseen liittyvän kehittämistoiminnan vaikutuksia on havaittavissa osassa tuloksia. Valtiovarainministeriössä valmistelussa olevan tiedonhallintalain yhteydessä uudistettavalta, myös tietoturvallisuuteen vaikuttavalta lainsäädännöltä voidaan aikanaan odottaa samaa vaikutusta.

Kaikkea toimintaa tulee parantaa. Olemme keränneet palautetta järjestämistämme tilaisuuksista sekä toimintaan osallistuneilta johtajilta ja asiantuntijoilta. Toimintaa kehitetään vuoden 2018 osalta saadun palautteen perusteella.

Vuoteen 2018 tulee myös positiivisesti vaikuttamaan hallinnollinen toimintamuutos, jossa VAHTI-toiminnan operatiivinen toiminta siirtyi 1.1.2018 alkaen Väestörekisterikeskukseen. Samassa yhteydessä VAHTI saa kevään 2018 aikana lisäresursseja toiminnan kehittämiseen. Vuoden 2018 toiminnasta löydät lisätietoja VAHTIn toimintasuunnitelmasta v. 2018–2019 (VM 12/2018). Linkki: http://urn.fi/URN:ISBN:978-952-251-941-2

Tämä toimintakertomus on hyväksytty VAHTI-johtoryhmän kokouksessa 14.2.2018.

INLEDNING

I december 2016 tillsatte finansministeriet ledningsgruppen för digital säkerhet inom den offentliga förvaltningen (VAHTI) för en ny mandatperiod 1.1.2017–31.12.2019.

Generellt kan år 2017 beskrivas med att verksamheten körde i gång och därefter stabiliserade sig. En helt förnyad verksamhetsmodell, där den digitala säkerheten utvecklas med hjälp av fem sakkunniggrupper, har krävt sin tid för att börja fungera. På förhand sett var ett av de centralaste målen för år 2017 förknippat med de ändringar som gällde revideringen av informationssäkerhetsbestämmelserna i samband med den kommande lagstiftningen om informationshantering, de s.k. VAHTI 100 -kraven. Men då tidtabellen för lagstiftningen sköts fram med ett år, ändrades också detta mål och sköts fram i motsvarande grad.

Framgångar under år 2017 har varit det samarbete som VAHTI har bedrivit med sakkunniggruppen för informationssäkerhet, dataskydd och beredskap som tillsattes av Delegationen för informationsförvaltningen inom den offentliga förvaltningen (JUHTA). Samarbetet gällde gemensamma dataskyddsprojekt. En andra framgång var en första temavecka om digital säkerhet inom den offentliga förvaltningen, som ordnades i oktober. I den deltog över 4 000 personer antingen på plats eller via nätet.

År 2017 var ett jubileumsår både för VAHTI och för JUHTA-verksamheten. Ett gemensamt 50+ verksamhetsår firades med ett evenemang med inbjudna gäster den 31 oktober 2017. Även om årliga VAHTI-dagar har ordnats under 20 års tid, konstaterades det i finansministeriets publikation 6/1992 om statsförvaltningens beslut om informationssäkerheten att finansministeriet bistås i dessa uppgifter av ledningsgruppen för statsförvaltningens informationssäkerhet, vilken har tillsatts av ministeriet. Följaktligen har statsförvaltningen och numera hela den offentliga förvaltningen långvariga traditioner vad gäller att utveckla informationssäkerheten.

Ett centralt mål för nya VAHTI har varit att förmedla information mellan verksamma sakkunniga och organisationer. I detta har man lyckats väl, såväl i fråga om sakkunniggrup-

pernas möten som de månatliga översikterna från VAHTI-generalsekreteraren. Om verksamheten har också informerats vidsträckt med hjälp av nyhetsbrev och separata pressmeddelanden som finansministeriet har gett ut.

I 2 kapitlet i denna verksamhetsberättelse beskrivs mandatperiodens första verksamhetsår på så sätt att det refereras hur de mål som finansministeriet har ställt för verksamheten har uppnåtts. I 3 kapitlet bedöms hur väl målen har uppnåtts med tanke på VAHTIs egen verksamhetsplan. I 4 kapitlet beskrivs de centrala resultaten av en organisationsenkät om den digitala säkerheten i den offentliga förvaltningen samt av en datasäkerhetsbarometer som har besvarats av VAHTIs personal och ledning och iakttagelser gällande dessa resultat. Verksamhetsberättelsens 5:e och samtidigt sista kapitel presenterar VAHTIs verksamhet under år 2017 i fråga om såväl ledningsgruppen, sekretariatet, sakkunnigsektionen och evenemangen som också andra aktiviteter.

Syftet med de mätare som VAHTI har samlat in är att mäta verksamhetens verkningsfullhet samt situationen i fråga om den digitala säkerheten hos den offentliga förvaltningens organisationer. Resultaten för år 2017 visar att ingen betydande utveckling har skett i fråga om informations- och cybersäkerheten, utan situationen är delvis synnerligen stabil. Inom statsförvaltningen är situationen synnerligen stabil, i fråga om kommunerna har det skett en liten förbättring jämfört med år 2016. Nivåhöjningen inom statsförvaltningen åren 2011–2015 berodde på informationssäkerhetsförordningen som trädde i kraft år 2010. Motsvarande utveckling kan förväntas antingen genom ändringar i anknytning till lagstiftningen eller genom andra särskilda utvecklingsprogram. Konsekvenserna av den utvecklingsverksamhet som anknyter till EU:s allmänna dataskyddsförordning, som börjar tillämpas från den 25 maj 2018, kan ses i en del av resultaten. Samma verkan kan i sinom tid förväntas av den lagstiftning som ska revideras i samband med en informationshanteringslag som bereds just nu vid finansministeriet och som även påverkar informationssäkerheten.

All verksamhet bör förbättras. Vi har samlat in respons om våra evenemang både av chefer och av sakkunniga som deltagit i verksamheten. Verksamheten utvecklas för 2018 års del utifrån den respons som erhållits.

År 2018 kommer också att påverkas positivt av en administrativ ändring av verksamheten, där VAHTI-verksamhetens operativa verksamhet den 1 januari 2018 fördes över på Befolkningsregistercentralen. I samband med detta får VAHTI under våren 2018 tilläggsresurser för att utveckla verksamheten. Mera information om verksamheten år 2018 hittar du i VAHTIs verksamhetsplan 2018–2019 (VM x/2018).

Denna verksamhetsberättelse har godkänts vid VAHTI-ledningsgruppens möte den 14 februari 2018.

INTRODUCTION

In December 2016, the Ministry of Finance set up the Government Information Security Management Board; (VAHTI) for the new term 1 January 2017 – 31 December 2019.

The year 2017 can generally be described as the launch period, followed by the establishment of operations. It has taken some time before the completely revamped operating model, in which digital security is developed with the help of five expert working groups, could be set in motion. One of the most important preliminary goals for 2017 was connected with changes to data security legislation (VAHTI 100 requirements), that will be revised in connection with the upcoming information management legislation. However, the legislation schedule was postponed by one year, so the goal was changed and put off by a corresponding amount of time.

The successes in 2017 were the cooperation pursued by VAHTI with the expert working group on data security, privacy protection and contingency planning set up by the Advisory Committee on Information Management in Public Administration (JUHTA) concerning joint privacy protection projects. Another success was the first public administration digital security week (JHDTTV) arranged in October, in which more than 4,000 people participated either at the event or online.

The year 2017 marked the 50+ anniversary of VAHTI and JUHTA, which celebrated the occasion with invited guests on 31 October 2017. Although annual VAHTI days have been arranged for 20 years already, it is stated in the Ministry of Finance publication 6/1992 on the Central Government Data Security Decision that "The Ministry of Finance is assisted in these tasks by the Finnish Government Information Security Management Board set up by the ministry". There are thus long traditions in central government and the whole of public administration in developing data security.

One of the key goals of the new VAHTI was to disseminate information between experts and organisations engaged in operations. This turned out to be highly successful and took the form of expert working group meetings as well as monthly reviews prepared by the

Secretary-General of VAHTI. Information on operations has also been broadly disseminated through newsletters and separate releases published by the Ministry of Finance.

Chapter 2 of this review describes the first year of the term, discussing the way in which the operative goals set by the Ministry of Finance have been achieved. Chapter 3 assesses the achievement of the goals from the point of view of VAHTI's own agenda. Chapter 4 describes the key results of the organisational survey on digital security in public administration and of the data security barometer for VAHTI's personnel and management and discusses the related findings. Finally, Chapter 5 introduces the operations of VAHTI in 2017, with information on the management board, secretariat, expert unit, events and other activities.

The purpose of the indicators gathered by VAHTI is to measure the effectiveness of operations and the status of digital security in different organisations in public administration. The results from 2017 indicate that no appreciable improvements have taken place in data and cyber security, but the situation is quite well established. The situation in public administration is fairly established, and minor improvements have taken place for municipalities from 2016. The improvements in public administration in 2011–2015 were due to the Government Decree on information security in central government that entered into force in 2010. Corresponding developments can be expected from legislative changes or other special development programmes. The effects of the development activities related to the EU's General Data Protection Regulation, which will enter into force on 25 May 2018, can be seen in some of the results. The same impact can also be expected in the future from the legislation that will be revised in connection with the information management legislation currently being prepared by the Ministry of Finance and that will also affect data security.

There is room for improvement in all operations. We have collected feedback on the events we have arranged from the directors and experts who participated in them. The feedback will be used for developing operations during 2018.

The year 2018 will also be affected positively by the administrative change in which VAHTI's operational activities were transferred to the Population Register Centre on 1 January 2018. At the same time, VAHTI will receive additional resources in the spring 2018 for developing its operations. For additional information on operations in 2018, see VAHTI's agenda 2018–2019 (Ministry of Finance x/2018).

This review was approved at the meeting of the VAHTI management board on 14 February 2018.

1 VAHTI-toiminnan tavoitteet ja näiden toteutuminen vuonna 2017

Tässä luvussa kuvataan VAHTIn sen asettamisessa annettujen tavoitteiden edistyminen sekä vuoden 2017 toimintasuunnitelman toteutumista.

1.1 Valtiovarainministeriön toiminnalle asettamat tavoitteet

Valtiovarainministeriö on asettanut VAHTIn toiminnalle seuraavia tavoitteita:

VAHTI on julkisen hallinnon digitaalisen turvallisuuden ohjauksen, kehittämisen ja yhteistyön elin.

Vuoden 2017 osalta voidaan todeta, että VAHTIn toiminnassa on mukana yli 60 organisaatiota sekä sen toimintaan on osallistunut noin 150 johtajaa, esimiestä ja asiantuntijaa.

VAHTIn toiminnalle on asetettu seuraavia tavoitteita, joiden yhteyteen on kuvattu näiden tavoitteiden edistyminen vuoden 2017 osalta.

1. *Valmistelee ja sovittaa yhteen valtiovarainministeriön linjauksia julkisen hallinnon digitaalisesta turvallisuudesta sekä seuraa ja edistää niiden toimeenpanoa.*

Vuonna 2017 johtoryhmä on käsitellyt tietoturvallisuussäädösten uudistamista osana tiedonhallintalakia sekä VAHTI 100-tietoturvavaatimusten kehittämistä.

Koska keväällä 2017 tehtiin päätös lain aikataulun siirtämisestä vuodella eteenpäin, tämän työn painopiste on vastaavasti siirtynyt vuodelle 2018.

2. *Käsittelee julkisen hallinnon digitaalista turvallisuutta koskevat säädökset, ohjeet, suositukset sekä muut tieto- ja kyberturvallisuuden linjaukset.*

Vuoden 2017 aikana julkaistiin seuraavat julkaisut:

- 25/2017 Sähköisen asioinnin tietoturvaohje
- 24/2017 VAHTIn toimintakertomus vuodelta 2016
- 22/2017 Ohje riskienhallintaan
  - Riskienhallintatyökalu - Excel - perusversio
  - Riskienhallintatyökalu - Excel - laajempi versio
  - Ohje riskienhallintatyökaluun

- 21/2017 VAHTIn toimintasuunnitelma vuosille 2017-2019
- 10/2017 Pilkahduksia tulevaisuuteen - digitalisaation ja robotisaation mahdollisuudet
  - Raportin luku 8 käsittelee digitaalista turvallisuutta ”Digitaalinen turvallisuus kehityksen ja toiminnan mahdollistajana”
  - 8/2017 Tietoturvapoikkeamatilanteiden hallinta

3. *Edistää julkisen hallinnon tietoturvakulttuuria ja henkilöstön tietoturvatietoisuutta*

Vuoden 2017 aikana toteutettiin kaksi VAHTI-seminaaria (kesäkuu ja marraskuu) sekä erillinen ensimmäinen julkisen hallinnon digitaalisen turvallisuuden teemaviikko osana EU-alueen laajuista kyberturvallisuuskuukautta (European Cyber Security month). Teemaviikon yhteydessä järjestettiin yksi asiantuntijaseminaari sähköisten palveluiden tietoturvallisuudesta, julkisen hallinnon ylimmän johdon teemaseminaari sekä kahtena päivänä suoria nettilähetyksiä koskien digitaalisen turvallisuuden eri osa-alueita sekä tietosuojaa. Viikon tilaisuuksiin osallistui paikan päällä tai verkkolähetyksiä katsomalla yli 4 000 henkilöä.

Vuoden 2017 aikana kehitettiin MMKT-toimintamalli turvalliseen toimintaan, josta on myös tiedotettu useassa eri yhteydessä ja toimintamallin tueksi on julkaistu kaksi videota. Toimintamallin avulla pyritään vähentämään henkilöstön oman toiminnan mahdollista ns. inhimillisen erehdyksen todennäköisyyttä kiinnit tämällä huomiota enemmän turvalliseen toimintaan sähköisissä toimintaympäristöissä.

MMKT-toimintamallilla halutaan varmistaa, että kiireessä ei tapahtuisi virheitä esimerkiksi salassa pidettävien tietojen luokittelussa, käsittelyssä, niiden luovuttamisessa tai julkaisemisessa.

Toinen MMKT-toimintamallin näkökulma liittyy toimimiseen erilaisilla päätelaitteilla; toivomme henkilöstön kiinnittävän huomiota siihen, miten he reagoivat päätelaitteeseen tai siinä käytössä olevien sovellusten tuottamiin ilmoituksiin. Erityisen tärkeää olisi kyky tunnistaa sellaiset viestit ja ilmoitukset, joiden avulla käyttäjää yritetään ohjata sellaisille sivustoille tai palveluihin, joilla päätelaitteen tietoturvallisuutta yritetään heikentää.

Johdon rooli digitaalisen turvallisuuden johtamisessa keskiöön.

Linkki valtiovarainministeriön tiedotteeseen

- Digitaalisen turvallisuuden teemaviikko (http://vm.fi/digitaalisen-turvallisuuden-teemaviikko)
- Digitaalisen turvallisuuden teemaviikon materiaalit (http://vm.fi/vahti-materiaalit-ja-tilaisuudet)
- Teemaviikon esitysten katseltavissa olevat verkkotallenteet (http://www.mediaserver.fi/live/vahti-teemaviikko)
- Julkisen hallinnon tietoturvaosaamista vahvistetaan digitaalisen turvallisuuden teemaviikolla (uutinen 28.9.2017) (http://vm.fi/artikkeli/-/asset_publisher/julkisen-hallinnon-tietoturvaosaamista-vahvistetaan-digitaalisen-turvallisuuden-teemaviikolla)

4. Edesauttaa tietosuojan toteutumista osana digitaalisen turvallisuuden kehittämistä

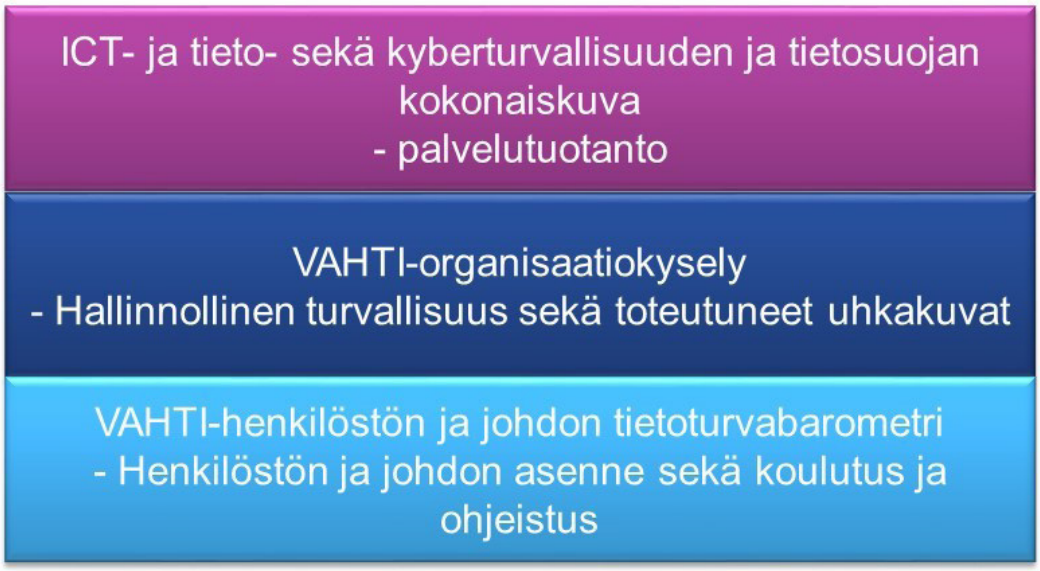
VAHTI on yhteistyössä JUHTAn kanssa toteuttanut yhteishanketta, joka koostuu tietoturvakoulutusvideoiden ja nettitestien tuottamisesta sekä tietosuojan osoitusvelvollisuutta edistävistä työpajatilaisuuksista. Vuoden aikana julkaistiin kaksi tietosuojakoulutusvideota, joilla oli vuodenvaihteessa

- Arjen tietosuojaa – tietosuojaa meille kaikille – noin 50 000 katselukertaa ja arviolta yli 100 000 katselijaa
- Johdon ja esimiesten tietoturvavideo – noin 4500 katselukertaa ja noin 10 000 katselijaa
- Lisäksi vuoden aikana viimeisteltiin kolmas video, tietosuojaa henkilötietoja käsitteleville, joka julkaistiin tammikuussa 2018

Tietosuojan osoitusvelvollisuutta edistäviä työpajatilaisuuksia järjestettiin 7 kappaletta, joissa

- paikan päällä on ollut yli 500 henkilöä sekä nettilähetyksiä seurannut noin 3000 henkilöä tilaisuuksien aikana, lisäksi tallenteita katsotaan aktiivisesti tilaisuuksien jälkeen
- mukana toiminnassa on yli 300 julkisen hallinnon organisaatiota ja yli 700 asiantuntijaa, myös elinkeinoelämä hyödyntää materiaaleja ja tilaisuuksia

5. *Toteuttaa digitaalista turvallisuutta koskevia kyselyitä ja barometrejä sekä julkaisee näistä raportteja sekä havainnoista koostettuja kehittämissuunnitelmia*



VAHTI tuottaa julkisen hallinnon digitaalisen turvallisuuden kokonaiskuvaa, jota tuotetaan kolmen eri kyselyn avulla.

Vuoden 2017 osalta toteutettiin organisaatiokohtainen, erityisesti hallinnolliseen turvallisuuteen liittyvä VAHTI-kysely, johon saimme 147 vastausta jakautuen 63 valtionhallinnon organisaatioon sekä 84 kuntaan tai kaupunkiin. Tämän kyselyn keskeisiä tuloksia ja havaintoja on käsitelty tarkemmin seuraavassa luvussa 3.

VAHTI toteutti vuonna toisen vuosittaisen henkilöstön ja johdon tietoturvabarometrin, johon osallistui 105 organisaatioita ja josta saatiin noin 8100 henkilön vastaus. Tuloksia on käsitelty keskeisimpien havaintojen osalta verraten vuoden 2016 tuloksiin tämän toimintakertomuksen luvussa 4.

6. *Mittaa, kokoaa ja ylläpitää kokonaiskuvaa julkisenhallinnon digitaalisen turvallisuuden tilanteesta sekä raportoi tästä valtiovarainministeriön johdolle*

Vuonna 2017 käynnistettiin julkisen hallinnon, viime vuoden osalta käytännössä valtionhallinnon kriittisten palveluiden ICT-palvelutuotantoa ja tieto- sekä kyberturvallisuuden

ja tietosuojan tilaa käsittävä kokonaiskuvamalli. Vuoden jälkimmäisessä kokonaiskuvassa julkaistiin 13 organisaation 73 palvelun tilanne.

Tämä kokonaiskuva osoittaa sen, että palvelutuotannossa keskeisin ongelma liittyy palveluiden ICT-toiminnan luotettavuuden ja häiriöttömyyden takaamiseen. Vastaavasti näiden palveluiden osalta on raportoitu tieto- ja kyberturvallisuuteen sekä tietosuojaan liittyviä poikkeamia, mutta usea näistä havainnoista ei liity palvelun omaan toimintaan vaan esimerkiksi ulkopuolisten tahojen toteuttamiin palvelunestohyökkäyksiin.

Näitä havaintoja tukevat myös VAHTI-organisaatiokyselyn tulokset, joissa etenkin valtionhallinnon osalta organisaatioiden toimintaa häirinneet palveluiden saatavuuteen liittyvät häiriöt. Lisätietoa näistä löytyy toimintakertomuksen 4. luvussa.

7. *Ohjaa, valmistelee ja sovittaa yhteen julkisen hallinnon digitaaliseen turvallisuuteen liittyviä kehittämisohjelmia ja hankkeita sekä niiden toimeenpanoa.*

Vuonna 2017 käynnistettiin julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman ja sen toimeenpanon valmistelu, jonka on tarkoitus valmistua syksyllä 2018, jonka jälkeen käynnistetään sen toimeenpano.

8. *Kehittää digitaalisen turvallisuuden operatiivista häiriötilanteiden hallintaa osana VIRT-toimintamallia.*

Vuonna 2018 VIRT-ryhmä kokoontui kolme kertaa. VIRT-toiminnan kehittämiseen panostetaan enemmän vuonna 2018 kun sen kehittämiseen liittyvät vastuut ja resurssit siirrettiin 1.1.2018 Väestörekisterikeskukselle.

9. *Käsittelee ja sovittaa yhteen julkisen hallinnon kansainvälisen tietoturvayhteistyön linjauksia ja vaikuttamista kansainvälisessä tietoturvatyössä.*

VAHTIn osalta on osallistuttu OECD EU4Digital: Trust & Security -työpajatilaisuuteen Georgiassa, jossa käsiteltiin hankkeeseen osallistuvien maiden kyberturvallisuutta sekä kansalaisten tunnistamiseen liittyviä kehityshankkeita sekä Viron puheenjohtajuuskaudella syksyllä 2017 järjestettyihin ylimmän johdon tilaisuuksiin.

2 VAHTIn toimintasuunnitelman vuoden 2017 toteutuminen

VAHTIn tehtävänä on toteuttaa valtiovarainministeriön sille asettamia tehtäviä sekä johtoryhmän hyväksymää toimintasuunnitelmaa vuodelle 2017.

VAHTI-toiminnan tavoitteena on varmistaa julkisen hallinnon toiminnan ja palveluiden turvallisuus kehittämällä digitaalisen turvallisuuden osa-alueita.

VAHTIn tavoitteita ovat

- VAHTI tukee valtiovarainministeriön päätöksentekoa ja sen valmistelua julkisen hallinnon digitaalista turvallisuutta koskevissa asioissa.
- VAHTI kehittää digitaalista turvallisuutta, mikä mahdollistaa julkisen hallinnon toiminnan digitalisaation ja robotisaation, toimintojen luotettavuuden, salassa pidettävien tietojen luottamuksellisuuden, tietojen ja toiminnan saatavuuden ja eheyden, toiminnan jatkuvuuden ja varautumisen häiriötilanteisiin sekä parantaa toiminnan laatua ja riskienhallintaa.

Näiden toteuttaminen tapahtuu siten, että VAHTI

- valmistelee ja sovittaa yhteen valtiovarainministeriön linjauksia julkisen hallinnon digitaalisesta turvallisuudesta sekä seuraa ja edistää niiden toimeenpanoa
- käsittelee julkisen hallinnon digitaalista turvallisuutta koskevat säädökset, ohjeet, suositukset sekä muut tieto- ja kyberturvallisuuden linjaukset
- edistää julkisen hallinnon tietoturvakulttuuria ja henkilöstön tietoturvatietoisuutta
- edesauttaa tietosuojan toteutumista osana digitaalisen turvallisuuden kehittämistä
- toteuttaa digitaalista turvallisuutta koskevia kyselyitä ja barometrejä sekä julkaisee näistä raportteja sekä havainnoista koostettuja kehittämissuunnitelmia
- mittaa, kokoaa ja ylläpitää kokonaiskuvaa julkisenhallinnon digitaalisen turvallisuuden tilanteesta sekä raportoi tästä valtiovarainministeriön johdolle
- ohjaa, valmistelee ja sovittaa yhteen julkisen hallinnon digitaaliseen turvallisuuteen liittyviä kehittämisohjelmia ja hankkeita sekä niiden toimeenpanoa
- kehittää digitaalisen turvallisuuden operatiivista häiriötilanteiden hallintaa osana VIRT-toimintamallia
- käsittelee ja sovittaa yhteen julkisen hallinnon kansainvälisen tietoturvayhteistyön linjauksia ja vaikuttamista kansainvälisessä tietoturvatyössä.

Tehtävien toteuttamiseksi ja tavoitteiden saavuttamiseksi VAHTI on laatinut toimintasuunnitelman vuosille 2017–2019, jossa on määritetty niitä keinoja, joilla asetettuihin tavoitteisiin päästään.

Johtoryhmä hyväksyi vuoden 2017 ensimmäisessä kokouksessa toimintasuunnitelman vuosille 2017–2019.

VAHTIn keskeiset osa-alueet digitaalisen turvallisuuden kehittämiseksi vuosille 2017–2019. Vuoden 2017 osalta osa-alueiden etenemistä on kuvattu liikennevaloilla (vihreä, keltainen, punainen). Vuoden 2018 toimintasuunnitelma on esitelty valtiovarainministeriön julkaisussa 12/2018 Toimintasuunnitelma vuosille 2018–2019.

Toimintasuunnitelma vuosille 2017-2019 löytyy omana julkaisuna osoitteessa http://julkaisut.valtioneuvosto.fi/handle/10024/79978, jossa edellisessä kuvassa esitetyt kehittämistoimenpiteet on kuvattu yksityiskohtaisemmin. Tässä luvussa kuvataan tiivistetysti toimenpiteiden tilanne.

Seuraavilla sivuilla olevat viittaukset koskevat toimintasuunnitelman kuvassa käytettyä numerointia alkaen kohdasta 2.1.

2.1 Tietoturvasäädösten uusiminen ja toimeenpano

Aikataulu: 1.1.2017–31.12.2019

Tavoitteen saavuttaminen

– Tavoitetta ei ole saavutettu, koska sitä ei ole myöskään käynnistetty. Kokonaisuuden aikataulua on muutettu keväällä 2017 vuodella eteenpäin osana tiedonhallintalain aikataulun siirtämistä vuodelle 2019. Tämä koskee seuraavia tehtäviä:

2.1.1 Toimeenpanon suunnittelu

Vuoden aikana tehtiin alustava suunnitelma toimeenpanon toteuttamisen ja käytettävien menetelmien osalta. Suunnitelmaa kehitetään esimerkiksi JUHTA/VAHTI-yhteishankkeista saatavien kokemusten perusteella.

2.1.2 Toimeenpanon tukeminen

2.1.3 Tietoturvavaatimusten uudistaminen – VAHTI 100 sekä VAHTI-portaalin kehittäminen

2.2 Digitaalisen turvallisuuden kehittäminen tapahtuu VAHTI-asiantuntijajaoston avulla

VAHTI-asiantuntijajaoston toiminta ja digitaalisen turvallisuuden kehittäminen

Aikataulu: 1.3.2017–31.12.2019

Tavoitteen saavuttaminen asiantuntijajaoston toiminnan osalta

Asiantuntijajaoston keskeisin tehtävä koskien VAHTI 100-vaatimuksia on siirtynyt vuodelle 2018.

2.2. Riskienhallinta on saatu vakiinnutettua osaksi organisaation toimintaa sekä tietoturvallisuuden hallintajärjestelmän uusi malli on toteutuksessa

1 Johtaminen ja riskienhallinta -asiantuntijaryhmä (JORI)

Puheenjohtaja Juha Pietarinen, Valtiokonttori ja varapuheenjohtaja Harri Ihalainen, Rovaniemen kaupunki

– Vuoden 2017 tehtävät:

VAHTI-ohje riskienhallinnasta prosessin jalkauttaminen ja toimeenpano

– Käynnistää osana uuden lainsäädännön toimeenpanon suunnittelua tietoturvallisuuden hallintajärjestelmämallin toteuttaminen, jonka avulla organisaatiot saavat käyttöönsä toimintamallin vaatimustenmukaisen toiminnan mahdollistamiseksi
– JUHTAn Tietoturva, tietosuoja ja varautuminen -asiantuntijaryhmän yhteistyössä VAHTIn kanssa toteuttavien yhteishankkeiden tukeminen
  • Tietosuojakoulutuksen sekä tietosuojan osoitusvelvollisuuden osoittamisen yhteishanke
  • Riskienhallinnan, toiminnan jatkuvuuden sekä tietoturvapoikkeamatilanteiden ja tietosuojaloukkausten hallinta -yhteishanke
– Digitaalisen turvallisuuden tietoisuuden kasvattaminen osana vuosittain lokakuussa toteutettavaa European Cyber Security Month -kuukautta
– Muiden digitaalisen turvallisuuden johtamista ja riskienhallintaa edistävien toimenpiteiden toteuttaminen.

Tavoitteen saavuttaminen

  • vuoden 2017 tehtävät on saatu pääosin saavutettua. Koska tiedonhallintalain valmistelu siirtyy vuodelle 2018, hallintajärjestelmän kehittäminen siirtyy vastavalla tavalla

2.2.2 Organisaatioilla on toimivat menetelmät sen toiminnan jatkuvuuden mahdollistamiseksi sekä häiriötilanteiden hallintaan

2 Toiminnan jatkuvuuden hallinta -asiantuntijaryhmä (TOJA)

Puheenjohtaja 30.9 saakka Esa Keränen Opetushallitus, 1.10.2017 alkaen Jenni Siermala, Pohjois-Pohjanmaan sairaanhoitopiiri ja varapuheenjohtaja Maarit Puhto, sosiaali- ja terveysministeriö

Toiminnan jatkuvuuden hallinnan asiantuntijaryhmä käsittelee niitä keinoja, joilla varmistetaan organisaation kyky selvitä erilaisista häiriötilanteista sekä ennakoivasti varaudutaan ja huolehditaan tarvittavasta jatkuvuus-, valmius- ja toipumissuunnittelusta organisaation eri tasoilla.

Vuoden 2017 tehtävät:

– VAHTI 2/2016 Toiminnan jatkuvuuden ohje ja sen yhteydessä laaditun BIA-vaikutusarviotyökalun tunnettavuuden ja hyödyntämisen lisääminen
  - JUHTAn Tietoturva, tietosuoja ja varautuminen -asiantuntijaryhmän yhteistyössä VAHTIn kanssa toteuttaman Riskienhallinnan, toiminnan jatkuvuuden sekä tietoturvapoikkeamatilanteiden ja tietosuojaloukkausten hallinta -yhteishanke
– Muiden jatkuvuuden hallintaa edistävien toimenpiteiden toteuttaminen.

Tavoitteen saavuttaminen
- vuoden 2017 tehtävät on saatu pääosin saavutettua. Ryhmän puheenjohtajan vaihdos on vaikuttanut hieman ryhmän toimintaan.

2.2.3 Digitaalinen turvallisuus on sisäänrakennettu kaikkeen uuteen toimintaan

3 Turvallisuus kehittämisessä -asiantuntijaryhmä (TUKE)

Puheenjohtaja Kimmo Janhunen, Oikeusrekisterikeskus ja varapuheenjohtaja Pyry Heikkinen, Tulli

Turvallisuus kehittämisessä -asiantuntijaryhmä

Turvallisuus kehittämisessä -asiantuntijaryhmä käsittelee niitä keinoja, joilla huolehditaan tietoturvallisuuden sisältymisestä kehittämisprosessiin ja lopputuloksiin, esimerkiksi uusissa projekteissa, hankkeissa ja palveluissa sekä muussa organisaation kehittämisessä ja hankinnoissa. Tämän tarkoituksena on varmistaa, että digitaalinen turvallisuus nähdään ja toteutetaan vaadittavilta osin sisäänrakennettuna toiminnallisuutena eikä erillisenä, jälkikäteen liimattavana komponenttina.

Vuoden 2017 tehtävät:
– VAHTI 3/2017 Sähköisen asioinnin tietoturvallisuus -ohjeen toimeenpano
– Muiden digitaalisen turvallisuuden kehittämistä edistävien toimenpiteiden toteuttaminen.

Tavoitteen saavuttaminen
- vuoden 2017 tehtävät on saatu pääosin saavutettua.

2.2.4 Tietoturvallisuutta ylläpidetään ja sen toteutumista arvioidaan hyödyntäen turvallisuuden digitalisaation mukanaan tuomat uudet mahdollisuudet

4 Turvallisuuden ylläpito-asiantuntijaryhmä (TUKE)

Puheenjohtaja Juha Ilkka, valtioneuvoston kanslia 30.4.2017 saakka sekä Petri Puhakainen, valtioneuvoston kanslia 1.5.2017 alkaen sekä varapuheenjohtaja Mats Kommonen, Turun yliopisto

Turvallisuuden ylläpito -asiantuntijaryhmän työ käsittää päivittäiset ja jatkuvat toimet, joilla varmistetaan turvallisuusjärjestelyjen asianmukainen toiminta ja ylläpito. Työssä selvitetään keinoja hyödyntää turvallisuuden digitalisointia osana digitaalisen turvallisuuden kehittämistä.

Vuoden 2017 tehtävät:

- VM 8/2017 Tietoturvapoikkeamatilanteiden hallinta -ohjeen jalkauttaminen
- Tietoturvallisuuden arviointitoiminnan kehittäminen, tässä yhteydessä selvitetään myös julkisen hallinnon ICT-palveluiden tietoturvahaavoittuvuuksien etsimiseen tähtäävän palkinto-ohjelman kehittämistä ja sekä sen hyödyntämistä perinteisten tietoturvapalveluiden ja -auditointien tukena.
- Muiden turvallisuuden ylläpitoa edistävien toimenpiteiden toteuttaminen.

Tavoitteen saavuttaminen

- vuoden 2017 tehtävät on saatu pääosin saavutettua. Ryhmän puheenjohtajan vaihdos on vaikuttanut hieman ryhmän toimintaan.

2.2.5 Julkisen hallinnon digitaalisen turvallisuuden mittaaminen sekä kokonaiskuvan raportointi tapahtuu tarkoituksenmukaisesti

5 Seuranta ja arviointi -asiantuntijaryhmä (SETI)

Puheenjohtaja Erja Kinnunen, Verohallinto ja varapuheenjohtaja Timo Nuutinen puolustusministeriö

Seuranta ja arviointi -asiantuntijaryhmän toiminta keskittyy tietoturvallisuuden toteutumisen seurantaan ja arviointiin. Keskeisenä tehtävänä on VAHTI-kyselyiden toteuttaminen ja kehittäminen sekä tieto- ja kyberturvallisuuden mittariston sekä digitaalisen turvallisuuden kokonaiskurvan raportoinnin kehittäminen.

Vuoden 2017 tehtävät:

– Seuranta ja arviointi -asiantuntijaryhmän toiminta keskittyy tietoturvallisuuden toteutumisen seurantaan ja arviointiin. Keskeisenä tehtävänä on VAHTI-kyselyiden toteuttaminen ja kehittäminen sekä tieto- ja kyberturvallisuuden mittariston sekä digitaalisen turvallisuuden kokonaiskurvan raportoinnin kehittäminen.

Vuoden 2017 tehtävät:

– VAHTIn digitaalisen turvallisuuden kokonaiskuvaraportoinnin kehittäminen
– VAHTI organisaatiokyselyn sekä VAHTI henkilöstön ja johdon tietoturvabarometrin kehittäminen sekä niistä saatujen tulosten hyödyntäminen ja näihin liittyvien toimenpideohjelmien toteuttaminen
– Tieto- ja kyberturvallisuuden mittariston kehittäminen julkisen hallinnon tarpeisiin
– Muiden turvallisuuden seurantaa ja arviointia edistävien toimenpiteiden toteuttaminen.

Tavoitteen saavuttaminen

- vuoden 2017 tehtävät on saatu pääosin saavutettua.

2.3 Kyberturvallisuusstrategian toimeenpano-ohjelman toteuttaminen vuosina 2017–2020

Aikataulu: Toimeenpano-ohjelman hyväksymispäivämäärä 20.4.2017–31.12.2019 / jatkuu

VAHTI osallistuu aktiivisesti Suomen Kyberturvallisuusstrategian vuosien 2017–2020 toimeenpano-ohjelman toteuttamiseen. Käytännössä kaikki VAHTIn julkisen hallinnon digitaalista turvallisuutta edistävän toiminnan voidaan katsoa myös kyberturvallisuutta edistäväksi kehittämiseksi. Tämän lisäksi päivitettyyn kyberturvallisuusstrategian toimeenpano-ohjelmaan on nostettu seuraavat kaksi VAHTIn vastuulla olevaa toimenpidettä:

2.3.1 Julkisen hallinnon strategiset tieto- ja kyberturvallisuuden linjaukset on vahvistettu (TPO kohta numero 4)

Valtiovarainministeriö asettaa toimikaudelle 2017–2019 julkisen hallinnon digitaalisen turvallisuuden johtoryhmän (VAHTI). Se käsittelee ja yhteen sovittaa julkisen hallinnon keskeiset strategiset tieto- ja kyberturvallisuuden linjaukset. Lisäksi valtiovarainministeriö arvioi nykyisen tietoturvallisuuslainsäädännön kehittämistarpeet ja – mahdollisuudet. VAHTIn toiminnasta raportoidaan vuosittain.

Tavoitteen saavuttaminen

- vuoden 2017 tehtävät on saatu pääosin saavutettua.

2.3.2 Julkisen hallinnon tieto- ja kyberturvallisuushenkilöstön osaamista parannetaan (TPO kohta numero 22 a)

Valtiovarainministeriö osana VAHTI-toimintaa suunnittelee ja toteuttaa julkisen hallinnon henkilöstön osaamisen kehittämisen hankkeita ja palveluita tieto- ja kyberturvallisuuden alueella. Valtiovarainministeriö määrittelee yhteistoiminnassa muiden viranomaisten kanssa kryptologian alueella tarvittavan omavaraisuuden.

Tavoitteen saavuttaminen

- vuoden 2017 tehtävät on saatu pääosin saavutettua. Kryptologian osalta toimintaa kehitetään vuoden 2018 puolella.

2.4 Laajojen tieto- ja kyberturvahäiriötilanteiden hallinnan kehittäminen

Aikataulu: 1.5.2017–31.12.2019

Valtiovarainministeriö loi osana SecICT-hanketta VIRT-toimintamallin (*Virtual Incident Response Team*) julkisen hallinnon ICT-palveluita koskevien vakavien ja laajojen tieto- ja kyberturvallisuushäiriöiden hallintaan. VAHTI vastaa tämän toimintamallin hallinnollisesta kehittämisestä. Tämä tapahtuu VIRT-toiminnassa mukana olevista toimijoista muodostettavan ryhmän avulla, johon osallistuvat organisaatiot ja henkilöt nimetään erikseen.

Ryhmän tehtävänä on varmistaa toimintamallin jatkuva kehittäminen sekä mahdollistaa sen asteittainen laajentaminen, esimerkiksi maakunta- ja kuntasektorilla. Häiriötilanteiden hallinnan kehittymisestä raportoidaan johtoryhmälle vuosittain.

Tavoitteen saavuttaminen

- toimintaa ei ole päästy kehittämään, mutta tarvittavat VIRT-kokoukset on saatu järjestettyä. Vuoden 2018 ensimmäinen tilaisuus, jossa mukana ovat VIRT-toimijat järjestetään helmikuussa 2018 ja tarkoitus on kokoontua 3-4 kertaa vuodessa, jonka lisäksi mahdolliset häiriötilanteiden aiheuttamat kokoontumiset.

2.5 JUHTA-yhteistyö

Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) alaisuuteen perustettiin tietoturvan, tietosuojan ja varautumisen asiantuntijaryhmä syksyllä 2016. Asiantuntijaryhmän tehtävänä on toteuttaa hankkeita, joilla edistetään ryhmän toimintaan kuuluvien osa-alueiden kehittämistä julkisessa hallinnossa. Ryhmä toteuttaa toimikaudella 1.1.2017–31.12.2018 kaksi hanketta yhteistyössä VAHTIn kanssa.

2.5.1 Tietosuojakoulutuksen toteuttaminen

Aikataulu: 1.2.2017–31.12.2018

Vuonna 2018 kartoitetaan, mitkä koulutusvideot on tarkoituksenmukaista toteuttaa jo julkaistujen kolmen videon ohella (Arjen tietosuojaa – tietosuojaa meille kaikille, johdon ja esimiesten koulutusvideo sekä video henkilötietoja käsitteleville). Alustavasti selvitetään tarvetta opetustoimen ja SOTEn sekä työelämän tietosuojakoulutusvideoille.

Tavoitteen saavuttaminen

- vuoden 2017 tehtävät on saatu saavutettua. Kryptologian osalta toimintaa kehitetään vuoden 2018 puolella.

2.5.1 Tietosuojan osoitusvelvollisuuden toteuttamisen yhteishanke

Aikataulu: 1.4.2017–31.12.2018

JUHTA-yhteistyön toinen merkittävä tietosuojaan liittyvä kokonaisuus on työpajamallinen yhteishanke, joka käsittelee EU-tietosuoja-asetuksen keskeisiä hallinnollisia ja teknisiä vaatimuksia. Samalla on tarkoitus määrittää yhteisesti kansallinen tietosuojavaatimusten ja niiden toteuttamiselta edellytettävien prosessien ja toimintamallien taso, jonka voidaan todeta olevan riittävän osoitusvelvollisuuden toteuttamiseksi.

Tavoitteen saavuttaminen

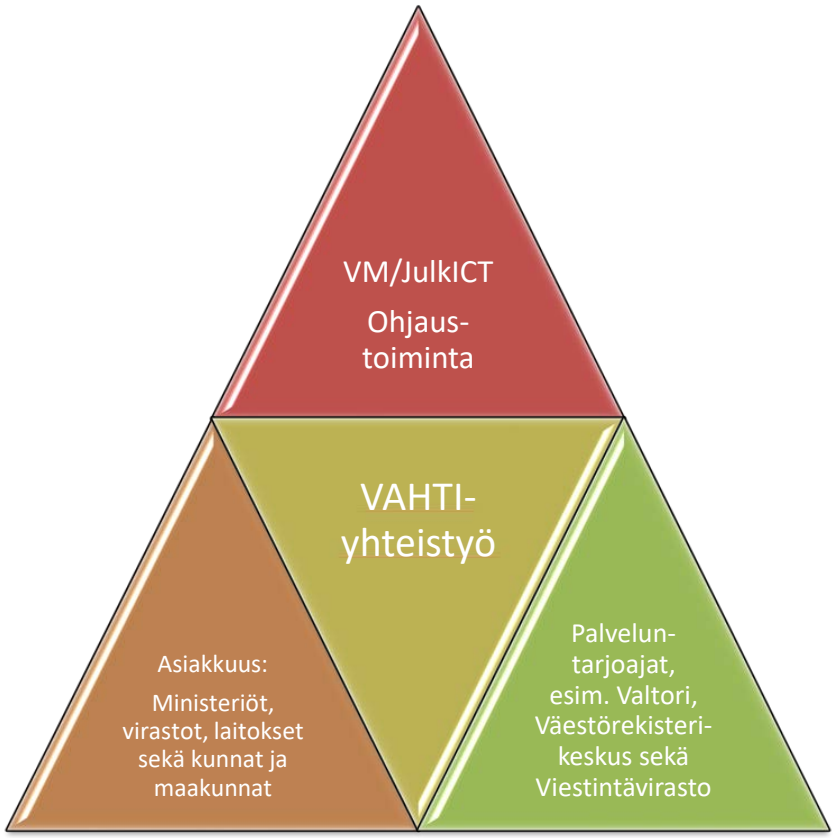
- vuoden 2017 tehtävät on saatu pääosin saavutettua. Kryptologian osalta toimintaa kehitetään vuoden 2018 puolella.

Työpajoissa käydään läpi hyviä käytäntöjä, käsitellään edellytyksiä tietosuoja-asetuksen vaatimuksista asiantuntijoiden johdolla sekä esitellään konkreettisia keinoja näiden täyttämiseksi. Työpajoihin voi osallistua mikä tahansa julkisen hallinnon organisaatio. Tilaisuuksia voi seurata verkkolähetyksen avulla tai ne voi katsoa myöhemmin verkkotallenteilta. Työpajoihin tuotettava materiaali tulee julkiseen jakoon, kuten kaikki tietosuojakoulutuksiin tuotettava materiaalikin.

3 VAHTI-organisaatiokysely 2017

Valtiovarainministeriön tehtävänä on julkisen hallinnon tietoturvallisuuden yleinen kehittäminen ja valtionhallinnon tietoturvallisuuden ohjaus. Tätä toteutetaan usealla eri tasolla, niin valtionhallinnon keskeisten ICT-palveluiden turvallisuuden ohjauksella kuin laajemmalla hallinnollisella kehittämisellä.

Oheisessa kaaviossa on esitetty julkisen hallinnon digitaalisen turvallisuuden johtamisen ja yhteistyön malli.

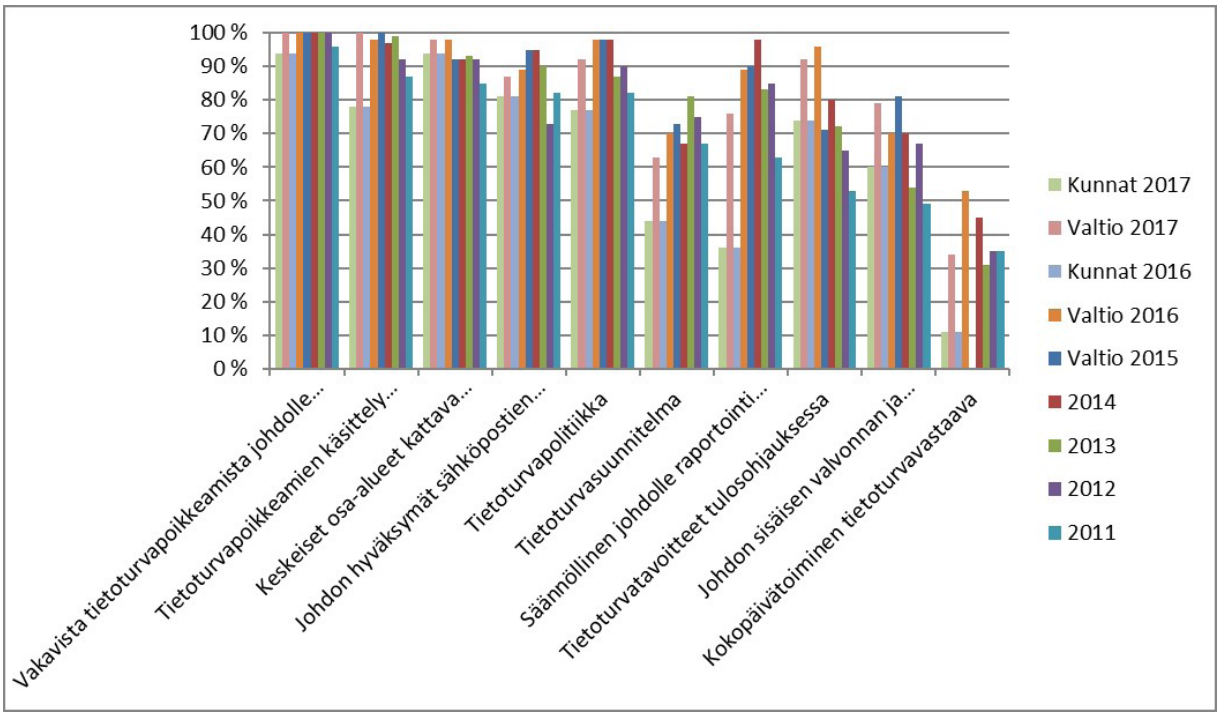


Digitaalisen turvallisuuden ohjausmalli.

3.1 Tietoturvallisuuden johtaminen

Vuoden 2017 VAHTI organisaatiokyselyyn saatiin vastaus 84 kunnasta ja 63 valtionhallinnon organisaatiosta.

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



Tietoturvallisuuden johtamisen mittareita – valtionhallinto vuosina 2011–2017 sekä kunnat vuosina 2016–2017.

Kuvassa esitetään tietoturvallisuuden johtamiseen liittyvien mittarien kehitys vuosina 2011–2017 organisaatioiden oman arvion mukaan. Koska johtaminen on hyvin keskeinen osa-alue, sen seurannassa käytetään kymmentä VAHTIn mittaria. Kuvan tarkoitus on esittää etenkin valtionhallinnon osalta vuodesta 20111 alkanutta pääosin nousujohteista trendiä.

Johtajuus	Kunnat 2017	Valtio 2017	Kunnat 2016	Valtio 2016	Valtio 2015
Vakavista tietoturvapoikkeamista johdolle raportointi	94 %	100 %	96 %	100 %	100 %
Tietoturvapoikkeamien käsittely organisoitu/vastuutettu	78 %	100 %	35 %	98 %	100 %
Keskeiset osa-alueet kattava tietoturvaohjeisto	94 %	98 %	85 %	98 %	92 %
Johdon hyväksymät sähköpostien pelisäännöt	81 %	87 %	83 %	89 %	95 %
Tietoturvapolitiikka	77 %	92 %	78 %	98 %	98 %
Tietoturvasuunnitelma	44 %	63 %	50 %	70 %	73 %
Säännöllinen johdolle raportointi tietoturvallisuudesta	36 %	76 %	35 %	89 %	90 %
Tietoturvatavoitteet tulosohjauksessa	74 %	92 %	63 %	96 %	71 %
Johdon sisäisen valvonnan ja riskien hallinnan arviointi ja vahvistus	60 %	79 %	68 %	70 %	81 %
Kokopäivätoiminen tietoturvavastaava	11 %	34 %	22 %	53 %	42 %
Keskiarvo	**65 %**	**82 %**	**61 %**	**86 %**	**84 %**

Johtajuuden mittareiden kehittyminen valtionhallinnossa vuosina 2015–2017 sekä kunnissa 2016–2017.

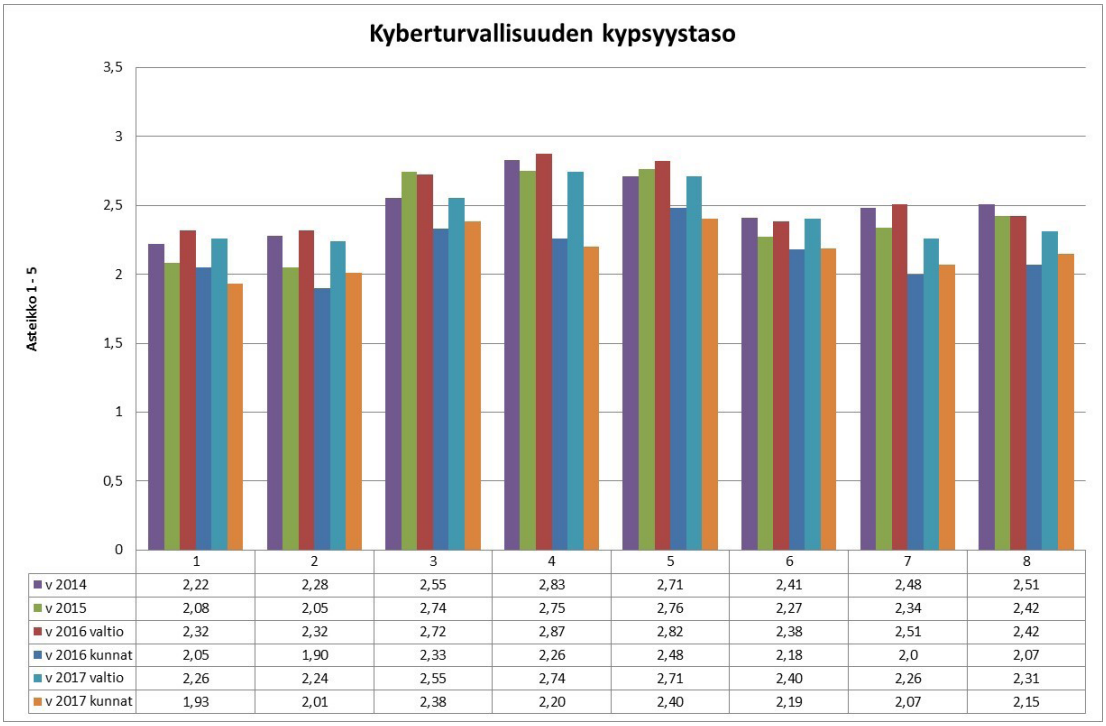
Kehitys on ollut merkittävää vuoteen 2014 asti, jonka jälkeen mittareissa on nähtävissä pienempiä muutoksia. Johtajuuden keskiarvo on pysynyt samalla tasolla vuosina 2014–2015 sekä noussut kaksi prosenttiyksikkö vuonna 2016. Vastaavasti se on laskenut neljä prosenttiyksikköä vuonna 2017 tuloksissa. Kuntien puolella on tapahtunut vastaavasti neljän prosenttiyksikön nousu vuodesta 2016.

Valtionhallinnossa eniten laskenut kohta on säännöllinen raportointi johdolle tietoturvallisuudesta, joka on laskenut 13 prosenttiyksikköä. ”Kokopäivätoimisten tietoturvavastaavien” osuus on laskenut 19 prosenttiyksikköä, joka on varsin merkittävä pudotus. Vastaavasti eniten kehittynyt on kohta ”Johdon sisäisen valvonnan ja riskienhallinnan arviointi ja vahvistuslausumassa käsitellään tietoturvariskejä”, joka on noussut 9 prosenttiyksikköä. Kohta ”Tietoturvapoikkeamien käsittely on organisoitu ja vastuutettu” on noussut 2 prosenttiyksikköä ja siten noussut 100% eli kaikissa valtionhallinnon kyselyyn osallistuneissa organisaatioissa on tämä organisoitu.

Kuntien puolella parhaiten on kehittynyt kohta ”Tietoturvapoikkeamien käsittely on organisoitu/vastuutettu”, jonka mittaustapa on samalla hieman muuttunut, mutta osoittaa selkeää parannusta. ”Keskeiset osa-alueet kattava tietoturvaohjeisto” on noussut 9 prosenttiyksikköä. Kuten valtionhallinnossa, myös kuntapuolella ”Kokopäivätoimisten tietoturvavastaavien osuus” on laskenut 11%, joka on myös suuri pudotus. Osin tähän vaikuttaa myös se, että vastaajaorganisaatioiden koko voi vaihdella kuntasektorilla merkittävästi vuosittain. Pienemmissä kunnissa ei ole tarvetta kokopäivätoimiselle tietoturvavastaavalle.

3.2 Strategiat ja toiminnan tukeminen sekä lainsäädäntö

Suomen kyberturvallisuusstrategia (2013) sekä sen uusin toimeenpano-ohjelma (v. 2017–2020) korostaa VAHTIn roolia ja vastuuta julkisen hallinnon tieto- ja kyberturvallisuuden toimielimenä. VAHTIssa toimivat organisaatiot ovat keskeisessä roolissa strategian toimeenpanossa ja yhteistyössä. VAHTI on aktiivisesti seurannut kyberturvallisuusstrategian toimeenpanoa eri hallinnonaloilla ja tätä koskeva osuus on lisätty VAHTI-organisaatiokyselyyn vuonna 2014.



	1	2	3	4	5	6	7	8
v 2014	2,22	2,28	2,55	2,83	2,71	2,41	2,48	2,51
v 2015	2,08	2,05	2,74	2,75	2,76	2,27	2,34	2,42
v 2016 valtio	2,32	2,32	2,72	2,87	2,82	2,38	2,51	2,42
v 2016 kunnat	2,05	1,90	2,33	2,26	2,48	2,18	2,0	2,07
v 2017 valtio	2,26	2,24	2,55	2,74	2,71	2,40	2,26	2,31
v 2017 kunnat	1,93	2,01	2,38	2,20	2,40	2,19	2,07	2,15

Kyberturvallisuuden kypsyystaso – valtionhallinto vuosina 2014–2017 sekä kunnat vuosina 2016–2017. Kuvassa VAHTI-kyselyn kahdeksan kyberturvallisuuden kypsyystasoon liittyvää kysymystä vuodesta 2014 alkaen.

Kypsyysmalli on viisiportainen, jossa korkein eli viides taso kuvaa sitä, että kyseisen osa-alueen osalta on saavutettu korkein mahdollinen toiminnan tason niin sen toteuttamisen, mittaamisen kuin jatkuvan kehittämisen osalta. Vastaavasti ensimmäinen taso kuvaa aloittelevaa toimintaa, jossa osa-alue on mahdollisesti tunnistettu, mutta sen toteutumiseen liittyen ei ole olemassa selkeää toimintatapaa tai prosessia, jolloin sen toteuttaminen tapahtuu osin sattumanvaraisesti.

Keskiarvo laski valtionhallinnossa kuuden osa-alueen keskiarvon osalta erittäin hieman valtionhallinnossa mitatun neljän vuoden aikana:

Valtionhallinto vuonna 2014 2,50

Valtionhallinto vuonna 2015 2,43

Valtionhallinto vuonna 2016 2,55

Valtionhallinto vuonna 2017 2,43

Valtionhallinnon keskiarvo 2,43 tarkoittaa sitä, että osa-alueen toiminnassa tarvittavat toimintamalli ja prosessit, tarvittavat yhteistyö on tunnistettu ja on osin toiminnassa. Yksittäisiä eroja organisaatioiden välillä esiintyy paljon, koska eri organisaatioilla on merkittäviä eroja ja vastuita huolehtia kyberturvallisuudesta. Keskeistä on tunnistaa se, että mitatun neljän vuoden aikana keskiarvo on pysynyt käytännössä lähes samana, vuosittaiset vaihtelut ovat olleet erittäin pieniä.

Valtionhallinnossa nousi vain yksi osa-alue

Yhteistoiminta

- 2,38 => 2,40

Vastaavasti eniten laskivat

Tiedottaminen tietoturvaloukkauksista: sidosryhmät (muut kuin viranomaiset)

- 2,51 => 2,26

ICT-varautuminen

- 2,72 => 2,55

Valtionhallinnon vastaajaorganisaatioissa kolme parasta osa-aluetta olivat

- Kyber- ja tietoturvariskien hallintaprosessi (tunnistus, arviointi, toimenpiteet) 2,74
- Yhteistoiminta kyber- ja tietoturvariskien hallinnassa 2,71
- ICT-varautuminen 2,55

Vastaavasti matalimmat pistemäärät olivat

- Tietoresurssien kriittisyys ja korvattavuus 2,24
- Toimintayksiköiden ja organisaation tietohallinnon välinen yhteistyö häiriötilanteessa

– Ilmoittaminen tietoturvaloukkauksista: muut viranomaiset 2,29

Kuntien osalta tätä osiota mitattiin toisen kerran ja keskiarvoksi muodostui:

Kunnat vuonna 2016 2,16
vvuonna 2017 2,17

Nousua on siis 0,06 yksikköä eli ei merkittävästi.

Kuntien osalta korkeimmalla tasolla ovat:

– Yhteistoiminta kyber- ja tietoturvariskien hallinnassa 2,40
– ICT-varautuminen 2,38

ICT-varautumisen osalta on tapahtunut nousua 0,05 yksikköä. Eräs tätä selittävä tekijä on Kuntaliiton yhteistyössä Huoltovarmuuskeskuksen kanssa toteuttamat KIJA-yhteishankkeet.

Vastaavasti matalimmat pistemäärät olivat

– Toimintayksiköiden ja organisaation tietohallinnon välinen yhteistyö häiriötilanteessa 1,93
– Tietoresurssien kriittisyys ja korvattavuus 2,01

Jokainen organisaatio voi itse suhteuttaa oman kyvykkyyden sen toiminnalta edellytettävään tasoon. Tämän takia ei voida todeta, että olisi olemassa jokin selkeä yksittäinen arvo tai taso, jota jokaiselta organisaatiolta edellytetään. Koska käytännössä ensimmäinen taso ei sisällä vielä organisaation osalta juuri mitään kyseisen osa-alueeseen liittyviä toimintamalleja tai -prosesseja, voidaan kakkostason saavuttamista pitää kuitenkin suositeltavana vähimmäistasona.

3.3 Henkilöstön kouluttaminen

Eräs VAHTIn koko sen historian tärkeimpiä osa-alueita, johon on myös merkittävästi panostettu, on ollut henkilöstön tietoturva-, kyberturvallisuus- ja ICT-varautumisen tietoisuuden ja osaamisen kehittäminen ja vahvistaminen.

Valtorin tuottama työkalupakki ja verkkokoulutukset

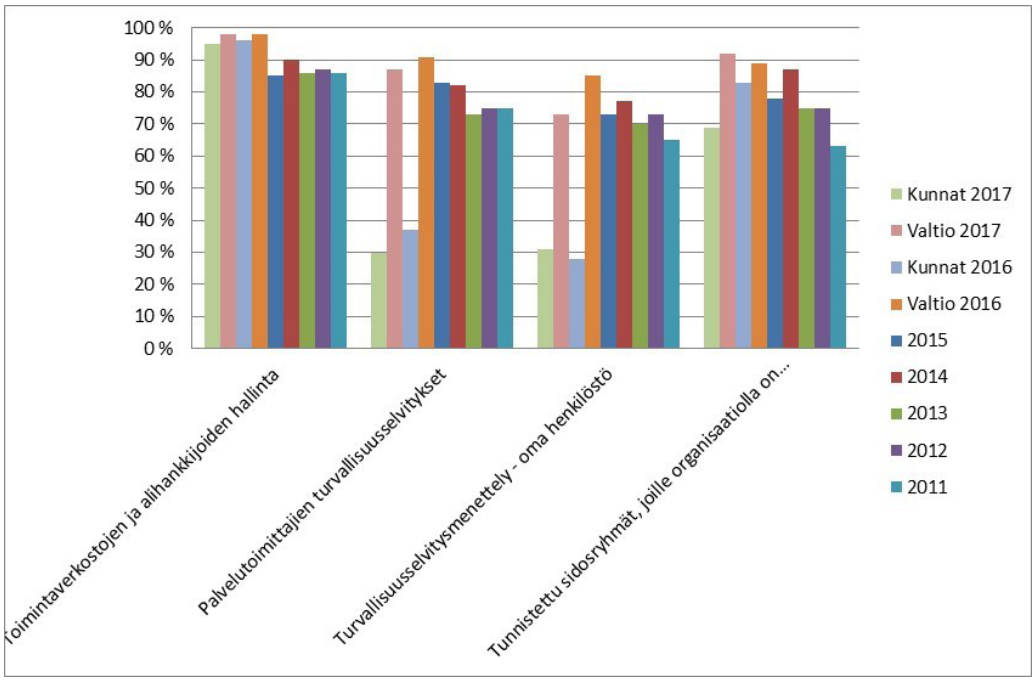
Valtori tukee tietoturvavastaavien työtä ylläpitämällä sähköistä työkalupakkia, joka sisältää materiaaleja ja mallipohjia valtionhallinnon tietoturvallisuudesta vastaaville henkilöille. Työkalujen sisältö perustuu VAHTIn ohjeisiin. Materiaalia hyödynnetään kaikissa virastoissa. Työkalupakki sisältää myös Moodle-pohjaisen verkkokoulutusympäristön. Tarjolla ovat seuraavat koulutusaineistot:

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

Työkalupakin käyttö on maksutonta. Verkkokoulutusten rakennetta tullaan uudistamaan osana uuden VAHTI-portaalin ja Valtorin verkkokoulutusympäristön käyttöönottoa.

3.4 Kumppanuudet ja resurssit

VAHTI toimii jatkuvassa ja tiiviissä yhteistyössä puolustusministeriön johtaman Turvallisuuskomitean ja muiden turvallisuusviranomaisten, kuten kansainvälisistä tietoturvavelvoitteista vastaavan ulkoasiainministeriön NSA-toiminnon ja Viestintäviraston Kyberturvallisuuskeskuksen kanssa. Niiden toimintaa on käsitelty säännöllisesti VAHTIn kokouksissa.



Kumppanuuksien hallinnan mittarit. Kuvassa esitetään seurattavien kohteiden toimeenpano valtionhallinnon organisaatioissa vuosina 2011–2017 sekä kuntapuolellavuosina 2016–2017.

Kumppanuus	Kunnat 2017	Valtio 2017	Kunnat 2016	Valtio 2016	2015
Toimintaverkostojen ja alihankkijoiden hallinta	95 %	98 %	96 %	98 %	85 %
Palvelutoimittajien turvallisuusselvitykset	30 %	87 %	37 %	91 %	83 %
Turvallisuusselvitysmenettely – oma henkilöstö	31 %	73 %	28 %	85 %	73 %
Tunnistettu sidosryhmät, joille organisaatiolla on tietoturvavastuita	69 %	92 %	83 %	89 %	78 %
Keskiarvo	**56 %**	**88 %**	**61 %**	**91 %**	**80 %**

Kumppanuuden mittareiden kehittyminen valtionhallinnossa 2015–2017 sekä kunnissa 2016–2017.

Valtionhallinnon puolella yksi osa-alue on noussut, yksi pysynyt samana ja kaksi osa-aluetta on laskenut.

Kokonaisuuden keskiarvo on laskenut 3 prosenttiyksikköä.

Kuntapuolella on noussut yksi osa-alue ja kolme osa-aluetta on laskenut, keskiarvo on laskenut 5 prosenttiyksikköä.

Valtionhallinto

Tunnistettu sidosryhmät, joille organisaatiolla on tietoturvavastuita 89% => 92%

Kunnat

Turvallisuusselvitysmenettely - oma henkilöstö 28% => 31%

Sekä valtionhallinnon että kuntien puolella palvelutoimittajien turvallisuusselvitykset ovat laskeneet, valtionhallinnossa 4 prosenttiyksikköä ja kunnissa 7 prosenttiyksikköä. Silloin kun kuntapuolen toimijat käyttävät palveluiden tuottamisessa sellaisia alihankkijoita, jotka toimivat myös valtionhallinnon organisaatioiden alihankkijoina, osalle alihankkijoiden henkilöistä on todennäköisesti tehty turvallisuusselvitys.

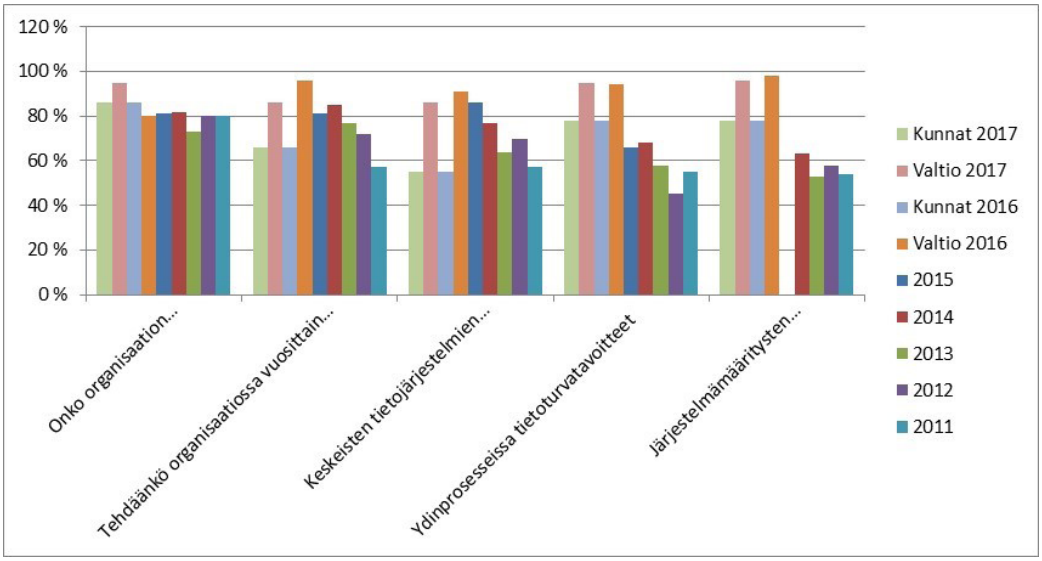
3.4.1 Valtorin tuottama tietoturvallisuuden asiantuntijapalvelu

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, sen kautta on tilattu toimeksiantoja seuraavasti:

vuosi	toimeksiantojen lkm	htp
2017	176	4 600
2016	157	5 402
2015	144	4 194
2014	101	2 812
2013	135	2 576
2012	103	2 491
2011	72	1 130
2010	63	1 091

Palvelun käytössä tapahtui vuonna 2017 pieni lasku, mutta on edelleen palvelun historian toiseksi suurin henkilötyöpäivämäärältään ja suurin toimeksiantojen lukumäärällisesti.

Palvelun tuottamisesta vastaa 1.1.2018 alkaen Väestörekisterikeskus, joka kilpailuttaa ja tuotteistaa palvelua seuraavaa neljän vuoden sopimuskautta varten.



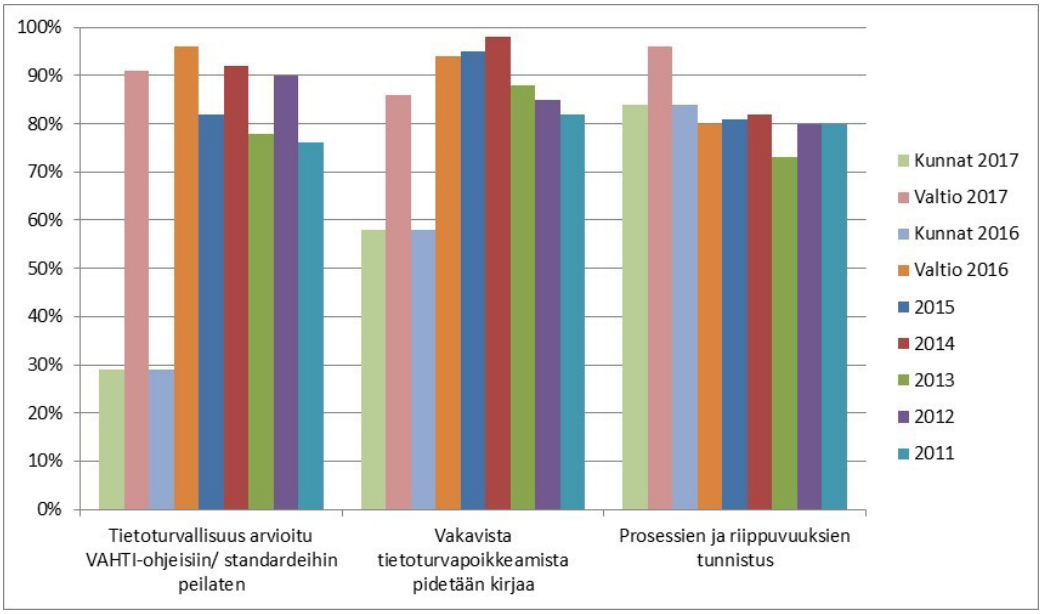
Toiminnan prosessien mittarit. Kuvassa esitetään tietoturvallisuuden prosessien toimeenpano vuosina 2011–2017 valtionhallinnossa sekä vuosina 2016–2017 kunnissa.

Valtionhallinnossa viidestä osa-alueesta kahdessa tapahtui nousua, kolmessa osa-alueessa lievää laskua. Kokonaisuuden keskiarvo pysyi valtionhallinnossa kuitenkin samana.

Kuntien vastausten osalta kaksi osa-aluetta nousi sekä ja kolme osa-aluetta laski. Kokonaisuuden keskiarvo nousi hieman (2%). Tässä tulee huomioida, että ensimmäistä kysymystä ”Onko organisaation ydintoimintojen/prosessien riskit arvioitu ja dokumentoitu?” on hieman muutettu, joten sitä ei suoraan voida suoraan verrata aikaisempiin vuosiin.

Toiminnan prosessit	Kunnat 2017	Valtio 2017	Kunnat 2016	Valtio 2016	2015
Onko organisaation ydintoimintojen/prosessien riskit arvioitu ja dokumentoitu?	86 %	95 %	57 %	80 %	81 %
Tehdäänkö organisaatiossa vuosittain kyber- ja tietoturvallisuuden riskien arviointia?	66 %	86 %	78 %	96 %	81 %
Keskeisten tietojärjestelmien tietoturva-arviointi	55 %	86 %	67 %	91 %	86 %
Ydinprosesseissa tietoturvatavoitteet	78 %	95 %	72 %	94 %	66 %
Järjestelmämääritysten tietoturvavaatimusten auditointi	78 %	96 %	80 %	98%	
Keskiarvo	**73 %**	**92 %**	**71 %**	**92 %**	**79 %**

Toiminnan prosessien mittareiden kehittyminen valtionhallinnossa 2015–2017 sekä kunnissa 2016–2017.



Mittaaminen – valtionhallinto ja kunnat. Kuvassa esitetään tietoturvallisuuden mittaamisen tilannetta vuosina 2011–2017.

Mittaaminen	Kunnat 2017	Valtio 2017	Kunnat 2016	Valtio 2016	2015
Tietoturvallisuus arvioitu VAHTI-ohjeisiin/standardeihin peilaten	29 %	91 %	37 %	96 %	82 %
Vakavista tietoturvapoikkeamista pidetään kirjaa	58 %	86 %	65 %	94 %	95 %
Prosessien ja riippuvuuksien tunnistus	84 %	96 %	57 %	80 %	81 %
Keskiarvo	**57 %**	**91 %**	**53 %**	**90 %**	**86 %**

Mittaamisen mittareiden kehittyminen valtionhallinnossa 2015–2017 sekä kunnissa 2016–2017.

Valtionhallinnossa kohta ”Prosessien ja riippuvuuksien tunnistus” on noussut selvästi (16 %), vastaavasti kaksi muuta osa-aluetta ovat laskeneet jonkin verran. Keskiarvo on kuitenkin noussut yhdellä prosentilla.

Kuntien vastausten osalta positiivista on havaita, että 29% vastaajista on arvioinut omaa turvallisuuttaan VAHT-ohjeisiin tai standardeihin peilaten. Prosessien ja riippuvuuksientunnistus on kehittynyt merkittävästi, mutta parannus johtuu osin uudesta osuuden laskentatavasta. Kokonaisuutena kuntien osalta keskiarvo on noussut neljä prosenttia.

4 VAHTIn henkilöstön ja johdon tietoturvabarometri 2017

4.1 Taustatietoja

VAHTI toteutti syksyllä 2016 ensimmäisen kerran julkisen hallinnon henkilöstölle ja johdolle suunnatun VAHTI-tietoturvabarometrin. VAHTIn historian ensimmäinen tietoturvabarometri onnistui erittäin hyvin. Tähän vapaaehtoiseen kyselyyn osallistui 97 organisaatiota: 66 valtionhallinnon ministeriötä, virastoa tai laitosta, 30 kuntaa sekä yksi sairaanhoitopiiri. Mahdollisia vastaajia kyselyyn oli yli 168 000 ja vastauksia saatiin 13 915, jolloin vastausprosentiksi muodostui 8,3 %.

Kyselyä kehitettiin saadun palautteen perusteella ja se toteutettiin uudelleen syksyllä 2017. Kyselyun osallistui 105 organisaatiota, joista 60 oli valtionhallinnosta, 38 kuntaa, 3 sairaanhoitopiiriä, 3 yliopistoa sekä yksi seurakuntayhtymä. Mahdollisia vastaajia oli 127 144, joista valtiolta 44 815, kuntasektorilta 65 765 ja sairaan-hoitopiireistä 8 556. Kyselyyn vastasi yhteensä 8123 henkilöä. Vastaajista valtiolla työskenteli 3581 eli 44,1 % vastaajista. Kuntasekarotilla 3434 eli 42,3 % vastaajista ja sairaanhoitopiireissä 791 eli 9,7 % vastaajista. Koko kyselyn vastausprosentiksi tuli 6,4 %. Täten vastausprosentti laski 1,9% edellisestä vuodesta.

Erityisen ilahduttavaa oli havaita, että noin 80 organisaatiota osallistui kyselyyn vuonna 2017 ensimmäistä kertaa. Täten tietoturvabarometrin kahtena ensimmäisenä vuotena siihen on osallistunut jo noin 180 eri organisaatiota, jota voidaan pitää hyvänä tuloksena.

Kyselyssä selvitettiin laaja-alaisesti vastaajien kokemuksia ja näkemyksiä tietoturvallisuuden toteutumisesta heidän omassa organisaatiossaan. Näin saatiin valtiovarainministeriön sekä osallistujaorganisaatioiden käyttöön tietoa tietoturvallisuuden tilasta ja kehittämistarpeista. Lisäksi saatiin hyvä yleiskuva tietoturvallisuuden toteutumisesta julkishallinnossa henkilöstön ja johdon näkökulmasta.

Organisaatioiden johdolle (johtoryhmän jäsenet) esitettiin erikseen 15 lisäkysymystä koskien tietoturvallisuuden tärkeyttä, sen toteuttamisen vaikeutta sekä toteuttamisen onnistumista organisaatiossa. Näihin kysymyksiin saatiin vuonna 2016 yhteensä 742 ja vuonna 2017 yhteensä 487 vastausta.

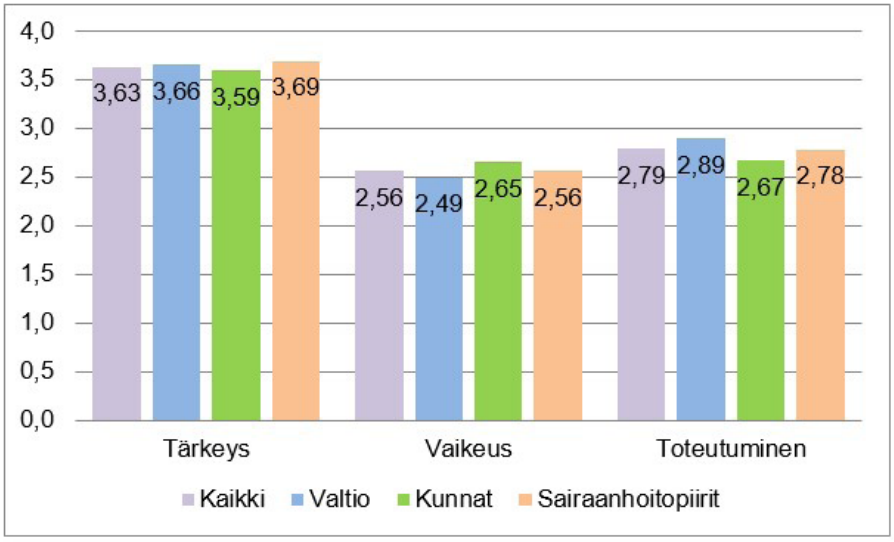
Tietoturvabarometrin tuloksien perusteella tietoturvallisuuden edistäminen ei ole kiinni ainakaan asenteista. Suurin osa vastaajista oli sitä mieltä, että tietoturvallisuus mahdollistaa laadukkaan toiminnan ja antaa heidän organisaatioistaan luotettavan kuvan. Tätä havaintoa tukee se, että organisaation johtoryhmään kuuluvat kokivat eri tietoturvallisuuden osa-alueet pääsääntöisesti erittäin tärkeiksi.

Kyselyssä tuli esiin useita myönteisiä havaintoja, mutta myös kehitettävää. Kyselyn positiivisimpia havaintoja oli se, että vastaajat pitävät tietoturvallisuutta keskeisenä työnteon mahdollistajana (vuonna 2016: 93,1 % ja vuonna 2017: 93,8 %), joka oli jopa kasvanut 0,7% edelliseen vuoteen verrattuna.

Sen sijaan useampi mittari oli laskenut vuoden takaisesta, ei paljoa, mutta kuitenkin havaittavasti. Lähes kaikki vastaajat (vuonna 2016: 96,4 % ja vuonna 2017: 91,9%) kokivat olonsa kuitenkin joko hyvin turvalliseksi tai melko turvalliseksi päätelaitteilla työskennellessään.

Valtaosa vastaajista (96,2 % ja vuonna 2017: 90,8 %) piti myös tietoturvallisuuden toteuttamista organisaatioissa vähintään hyvänä. Erityisesti erittäin turvalliseksi tai erittäin hyvin tietoturvallisuuden toteutumisen arvioineiden osuus laski kuitenkin merkittävästi, osain jopa puolittui edelliseen vuoteen verrattuna. Tämän taustalla on todennäköisesti vuoden 2017 aikana tapahtunut merkittävä uutisoinnin ja tietoisuuden kasvaminen tieto- ja kyberturvallisuuden osalta, joka on tällä tavalla näkynyt tuloksissa. Näitä mittareita on mielenkiintoista seurata tulevien vuosien aikana.

Organisaation ylin johto näki tietoturvallisuuden hyvin tärkeäksi (vuonna 2016: 3,60 ja vuonna 2017: 3,63 asteikolla 1–4), sen toteuttamisen keskivaikeaksi (vuonna 2016: 2,52 ja vuonna 2017: 2,56) sekä toteutumisen kohtalaisen hyväksi omassa organisaatiossa (vuonna 2016: 2,74 ja vuonna 2017:2,79). Keskeisinä kehittämistä edellyttävinä kohteina johdon näkökulmasta nousivat tietoturva-arviointeihin ja johdolle tietoturvallisuuden raportointiin liittyvät osa-alueet. Johdon tulokset parantuivat siis aavistuksen edelliseen vuoteen verrattuna.



Johdon vastauksissa oli hyvin vähän eroja valtionhallinnon, kuntien ja sairaanhoitopiirien johtajien välillä.

Tiivistetysti voidaan todeta, että vuosien 2016 ja 2017 välillä on tapahtunut pieni muutos siinä, että vuonna 2017 vastaajat arvioivat tietoturvallisuuden toteutumisen 5,4 % heikompana kuin vuonna 2016. Samoin turvallisuuden tunne päätelaitteilla työskenneltäessä on laskenut vuodessa 4,5 %. Tähän saattaa vaikuttaa se, että 80 % vastaajaorganisaatioista oli uusia ja toisaalta viimeisen vuoden aikana on mediassa ollut merkittävästi enemmän uutisointia koskien erilaisia, tosin lähinnä Suomen ulkopuolella tapahtuneita tietoturvapoikkeamia.

Vastaajien turvallisuudentunne päätelaitteilla työskennellessä oli korkea ja huolestuneisuus eri uhista yleensä olematonta tai vähäistä. Turvallisuudentunne ja huolestuneisuudenpuute eivät ole kuitenkaan linjassa vastaajien saaman koulutuksen ja ohjeistuksen määrän kanssa: vuonna 2016 ainoastaan 29,7 % koki saaneensa eri tietoturvallisuuden osa-alueisiin riittävästi koulutusta. Esimiehiä ja johtoa oli koulutettu enemmän, mutta ei kuitenkaan riittävästi, joka ilmenee esimerkiksi avovastauksissa.

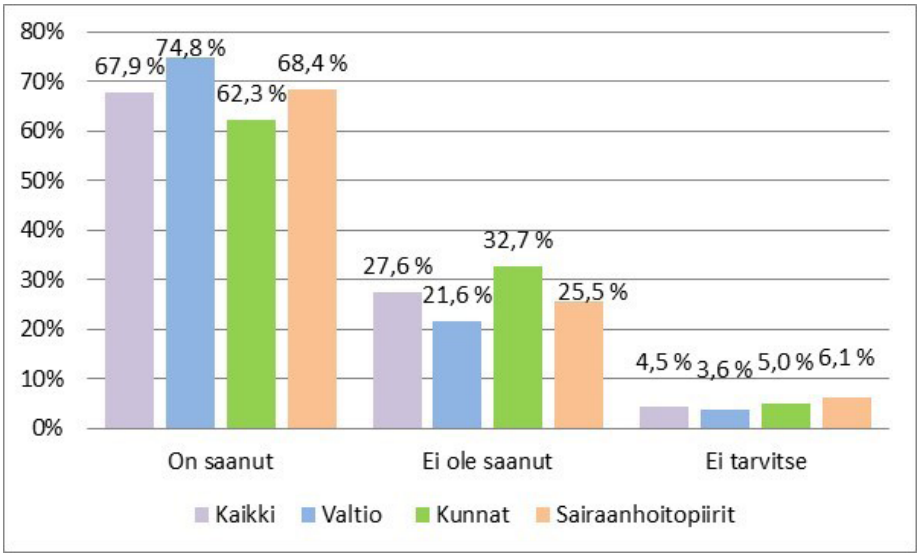
Merkittäviä tietoturvapoikkeamia on raportoitu Suomessa viime vuosina verrattain vähän, ja tämä voi olla yksi syy edelleen varsin hyvään turvallisuudentunteeseen. Jatkossa on mielenkiintoista verrata, miten näissä vuosien 2016-2017 kyselyissä luotujen mittarien tulokset vertautuvat mahdollisiin tuleviin kyselyihin.

Tietoturvallisuudessa ja sen mahdollistamassa toiminnan digitalisaatiossa ei onnistuta ilman koulutusta ja ohjeistusta. Saadun tietoturvaohjeistuksen ja ennen kaikkea puutuvan koulutuksen oletettua pienempi määrä onkin mielenkiintoinen, mutta myös hälyttävä ilmiö. Koulutukseen ja ohjeistukseen panostaminen sekä yleisellä että organisaatiotasolla on välttämätöntä. Havaitut puutteet ja riskit voidaan kääntää osaamiseksi ja mahdolli-

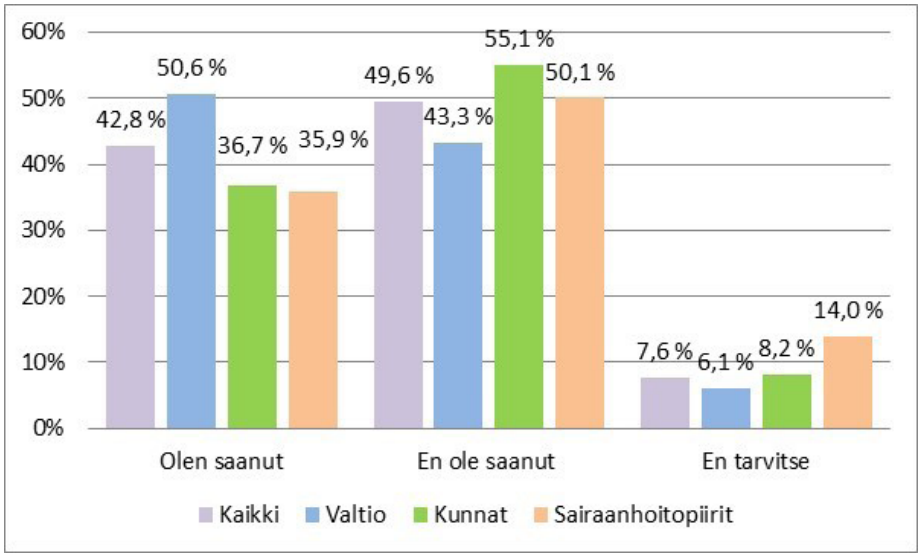
suuksiksi. Riittävällä koulutuksella ja ohjeistuksella voidaan parantaa sekä käytännön tason toiminnan operatiivista tietoturvallisuutta, että turvallisuudentunnetta entisestään.

Koska tätä ohjeistus ja koulutushaastetta haluttiin tutkia tarkemmin, kyselyä kehitettiin vuoden 2017 osalta siten, että se pilkottiin erikseen ohjeistuksen ja koulutuksen osalta, vuonna 2016 nämä olivat niputettu yhteen. Nyt tämän perusteella voidaan hyvin todeta, että henkilöstölle kyllä tuotetaan ohjeistusta, mutta henkilöstöä ei kouluteta läheskään riittävästi.

Täten kehittämiskohteeksi nousevat henkilöstön säännöllinen tietoturvallisuuden eri osa-alueet kattava koulutus ja myös tiedottaminen ajankohtaisista tietoturvallisuuden uhkakuvista.



Vastaajien eri tietoturvallisuuden osa-alueisiin keskimäärin saama ohjeistus. Siinä, kuinka paljon henkilöstö on saanut ohjeistusta, on kolmen eri vastaajaryhmän välillä selkeät erot.



Vastaajien eri tietoturvallisuuden osa-alueisiin keskimäärin saama koulutus. Keskimäärin puolet (49,6 %) vastaajista toteaa, etteivät he ole saaneet koulututa. Tätä ei voi selittää edes sillä, että henkilöstö ei tarvitsisi koulutusta, koska sitä on kysytty erikseen. Erityisesti sairaanhoitopiirien vastaajat kokevat, ettei heillä ole tarvetta koulutukseen.

Vuoden 2017 kyselyssä kysyttiin ensimmäistä kertaa useampia kysymyksiä koskien henkilötietojen käsittelyä sekä tietosuojaa. Tällä tavalla kyselystä luodaan hyvä perustason mittari, jonka avulla voimme arvioida EU:n yleisen tietosuoja-asetuksen ja Suomen tietosuojalain vaikutuksia tulevina vuosina.

Käsittely	Kaikki	%	Valtio	%	Kunnat	%	Sairaanhoitopiirit	%
Päivittäin	4093	50,4 %	1505	42,0 %	1876	54,6 %	634	80,2 %
Useamman kerran viikossa	1196	14,7 %	448	12,5 %	625	18,2 %	55	7,0 %
Kerran viikossa	383	4,7 %	179	5,0 %	164	4,8 %	14	1,8 %
Kuukausittain	579	7,1 %	319	8,9 %	196	5,7 %	11	1,4 %
Harvemmin	992	12,2 %	575	16,1 %	334	9,7 %	29	3,7 %
En käsittele	880	10,8 %	555	15,5 %	239	7,0 %	48	6,1 %
Yhteensä	**8123**	**100,0 %**	**3581**	**100,0 %**	**3434**	**100,0 %**	**791**	**100,0 %**

Kaikkien vastanneiden osalta noin 70% vastaajista käsittelee henkilötietoja vähintään kerran viikossa ja puolet päivittäin. Sairaanhoitopiireissä yli 80% käsittelee päivittäin, mikä ei ole lainkaan yllättävää.

Erityistä huolta aiheuttaa vastaukset kysymykseen tietosuoja-asetukseen valmistautumisessa. Vastaajilta kysyttiin, onko organisaation johdolta tullut ohjeistusta tai koulutusta tulevia muutoksia koskien. Vastausvaihtoehdot olivat:

- Organisaatiossa on jo ryhdytty toimenpiteisiin, joita tietosuoja-asetuksen on arvioitu edellyttävän.
- Organisaatiossa on käynnistetty tai ollaan aikeissa käynnistää hanke tai hankkeita, jotka tähtäävät siihen, että tietosuoja-asetukseen oltaisiin valmiita.
- Organisaatiossa ollaan tietoisia tietosuoja-asetuksesta ja sen aikatauluista. Tois-taiseksi on huolehdittu siitä, että toiminta vastaa nykylainsäädäntöä (henkilötietolaki ja erityislainsäädäntö).
- En ole havainnut

Valmistautuminen	Kaikki	%	Valtio	%	Kunnat	%	Sairaanhoitopiirit	%
Toimenpiteet	1406	17,3 %	676	18,9 %	561	16,3 %	88	11,1 %
Hanke	857	10,6 %	414	11,6 %	331	9,6 %	60	7,6 %
Tietoisia	1239	15,3 %	564	15,7 %	574	16,7 %	68	8,6 %
En ole havainnut	2126	26,2 %	906	25,3 %	954	27,8 %	195	24,7 %
Mikä se on?	2495	30,7 %	1021	28,5 %	1014	29,5 %	380	48,0 %
Yhteensä	**8123**	**100,0 %**	**3581**	**100,0 %**	**3434**	**100,0 %**	**791**	**100,0 %**

Keskimäärin vajaalla kolmasosalla ei tunnu olevan lainkaan tietoa tietosuoja-asetuksesta , reilu neljäsosa ei ole havainnut että organisaatiossa olisi sen osalta ryhdytty toimenpiteisiin. Erityisen huolestuttavana voidaan pitää sairaanhoitopiirien vastauksia tähän kysymykseen.

Kaikista vastaajista 30,7 % ei tiennyt, mikä tietoturva-asetus on. Vastanneista 26,2 % ei ollut havainnoi minkäänlaisia toimenpiteitä, kun 17,3 % oli huomannut toimenpiteitä. Tieto-turva-asetuksesta oli tietoisia 15,3 % vastanneista ja 10,6 % vastanneiden organisaatioissa oli aloitettu hanke

4.2 VAHTI-tietoturvabarometrin yhteenveto

VAHTI tietoturvabarometri on laajuudeltaan kansainvälisestikin arvioituna merkittävä tietoturvallisuuden tilan selvitys. Jotta tietoturvallisuuden tarjoamat mahdollisuudet saataisiin hyödynnettyä, on kyselyssä esiin tulleisiin tarpeisiin vastattava. Tietoturvallisuuteen liittyvät asenteet paranevat entisestään, kun perusasioihin, kuten koulutukseen ja erityisesti ohjeistukseen, häiriöttömiin palveluihin, salasanojen hallintaan sekä turvallisiin toimitiloihin, kiinnitetään huomiota.

Kuntasektorin ja osin sairaanhoitopiirien valtionhallintoa hieman vaatimattomammat tulokset voivat johtua esimerkiksi siitä, että tietoturvallisuuden kehittäminen ei ole samalla tavalla vakiintunutta ja verkostomaista kuin valtionhallinnossa, jossa VAHTI on vastannut kehittämisestä yli kahdenkymmenen vuoden ajan. Lisäksi valtionhallintoa koskee

vuonna 2010 voimaan astunut tietoturvallisuuden kouluttamista edellyttävä tietoturvallisuusasetus. Näitä havaintoja tukee myös vuoden 2017 VAHTI-organisaatiokysely, johon nyt myös kunnat ovat osallistuneet kahtena viime vuotena. Sairaanhoitopiirien osalta on useassa barometrin kysymyksessä sellainen tulos, joka tulee heidän huomioida tietoturva- ja myös tietosuojakoulutusta ja osin ohjeistusta seuraavina vuosina kehitettäessä. Todennäköisesti vuoden 2017 aikana vahvasti mediassa esille nostetut uutiset pääasiassa kansainvälisiin tieto- ja kyberturvapoikkeuksiin ovat osin heijastuneet siinä, että henkilöstö ei koe omaa turvallisuutta tai organisaation turvallisuutta niin hyvällä tasolla kuin 2016. Erityisesti tämän mittarin avulla pystytään hyvin havainnoimaan tulevina vuosina kokonaisuuden kehittymistä julkisessa hallinnossa.

4.3 Kehittämistoimenpiteet

VAHTI-henkilöstön ja johdon tietoturvabarometrin keskeisin havainto on, että koulutusta tulee selvästi kehittää. Valtiovarainministeriön on mahdollista toteuttaa VAHTIn ja yhdessä sidosryhmien kanssa kustannustehokkaasti kattava julkishallinnon koulutuskokonaisuus, joka käsittelee tässä raportissa tunnistettuja kehittämistä edellyttäviä osa-alueita. Henkilöstön osaamista on tarkoitus edelleenkehittää säännöllisemmällä tiedottamisella yhteistyössä esimerkiksi Turvallisuuskomitean, tietosuojavaltuutetun toimiston sekä Viestintäviraston Kyberturvallisuuskeskuksen kanssa. Samoin lokakuun julkisen hallinnon digitaalisen turvallisuuden teemaviikko, jatkossa laajemmin koko teemakuukausi toimii yhtenä keskeisenä aktiviteettina.

Kehittämistoimenpiteet on osin jo otettu ja tullaan ottamaan huomioon suunniteltaessa VAHTIn toimintaa vuosille 2018-2019 sekä julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelmaa luotaessa. Samoin tulevan tiedonhallintalain toimeenpanossa tarvitaan merkittävää henkilöstön tietoturvallisuuden osaamisen kehittämistä.

Toinen keskeinen kehittämistä edellyttävä osa-alue on johtaminen. Tämä käy ilmi myös kyselyn avovastauksissa niin henkilöstön kuin johdon edustajien osalta. Johtaminen tulee siten nostaa osaamisen ja koulutuksen kehittämisen ohella toiseksi keskeiseksi julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman pääteemaksi.

VAHTI-asiantuntijaryhmät käyvät läpi organisaatio- ja henkilöstön ja johdon kyselyn vuoden 2017 tulokset ja havainnot sekä esittävät keinoja osa-alueiden kehittämiseksi. Samaa toivotaan kyselyyn osallistuneilta organisaatioilta, jotka ovat saaneet organisaatiokohtaisen raportin joulukuussa 2017.

5 VAHTIn toiminta vuonna 2017

Valtiovarainministeriö on asettanut Valtionhallinnon tieto- ja kyberturvallisuuden johto-ryhmän (VAHTI) hallinnon tieto- ja kyberturvallisuuden yhteistyön, ohjauksen ja kehittämi-sen elimeksi. Tässä luvussa kuvataan sen organisointi ja kokoonpano sekä keskeiset aktiviteetit.

5.1 VAHTI -toiminnan organisointi ja kokoonpano

VAHTI-johtoryhmä kokoontui viisi kertaa vuoden 2017 aikana. VAHTI -johtoryhmään ovat vuoden 2017 aikana kuuluneet:

Puheenjohtaja:

Anna-Maija Karjalainen	valtiovarainministeriö

Varapuheenjohtaja:

Aku Hilve	valtiovarainministeriö

Sihteeristö:

Pääsihteeri Kimmo Rousku	valtiovarainministeriö
Sihteeri Maarit Koivuniemi	valtiovarainministeriö 15.8.2017 alkaen
Sihteeri Saana Seppänen	valtiovarainministeriö 14.8.2017 saakka

Jäsenet ja varajäsenet

Jäsenet:		**Varajäsenet:**	
Laura Vilkkonen	LVM	Antti Vertanen	MMM
Kalervo Koskimies	OKM	Juha Haataja	OKM
Tarmo Maunu	OM	Matti Aitta	OM
Teemu Anttila	PLM	Juha Pekkola	PLM
Tapio Aaltonen	SM	Kari Santalahti	SM
Tiina Pesonen	STM	Maarit Puhto	STM
Heikki Haukirauma	TEM	Kai Karsma	TEM

Ari Uusikartano	UM	Antti Savolainen	UM
Irja Peltonen	VM	Samuli Bergström	Vero
Aino Jalonen	VNK	Max Hamberg	VNK
Jari Ylitalo	VNK	Roni Kiviharju	YM
Jukka Litmanen	YM		
Simo Tanner	Kuntaliitto 30.9.2017 saakka	Jari Ylikoski	Kuntaliitto 1.10.2017 alkaen
Tuula Seppo	Kuntaliitto		
Anu Laamanen	NSA		
Reijo Aarnio	TSV	Lauri Karppinen	TSV
Vesa Valtonen	Turvallisuuskomitea		
Pasi Lehmus	Valtori	Ilkka Haataja	Valtori
Kirsi Karlamaa	Viestintävirasto	Jarkko Saarimäki	Viestintävirasto
Janne Viskari	VRK		

5.2 VAHTI -sihteeristö:

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmän sihteeristön tehtäviä ovat:

- valmistella ja toteuttaa johtoryhmän kokoukset sekä muut tilaisuudet
- valmistella toimintasuunnitelma sekä tehdä esitykset toimintakertomuksiksi
- toteuttaa digitaalista turvallisuutta koskevia kyselyitä ja barometrejä sekä julkaista niihin perustuvia raportteja sekä havainnoista koostettuja kehittämissuunnitelmia
- julkisen hallinnon digitaalisen turvallisuuden kokonaiskuvan kokoaminen, mittaaminen ja ylläpitäminen sekä siitä raportointi johtoryhmälle
- valmistella ja toteuttaa tarvittavia seminaareja sekä muita VAHTI-tilaisuuksia
- vastata VAHTI-toiminnan viestinnästä sekä esitys- ja tiedotusmateriaalien tuottamisesta.

Sihteeristön ovat muodostaneet:

Kimmo Rousku	valtiovarainministeriö, pääsihteeri
Maarit Koivuniemi	valtiovarainministeriö, ryhmän sihteeri
Saana Seppänen	valtiovarainministeriö 14.8.2017 saakka

Jäsenet:

Tietoturva-asiantuntija	Hanna Heikkinen	Valtion tieto- ja viestintätekniikkakeskus Valtori
ICT-tietoturvapäällikkö	Pyry Heikkinen	Tulli
Tietoturvapäällikkö	Juha Ilkka	Valtioneuvoston kanslia

Turvallisuuspäällikkö	Tuija Kuusisto	Valtiovarainministeriö – 1.9.2017
Erityisasiantuntija	Teemu Luukko	Sisäministeriö – varajäsen
Tilintarkastuspäällikkö	Pentti Mykkänen	Valtiontalouden tarkastusvirasto
Tietoturvapäällikkö	Harri Mäntylä	Puolustusministeriö
Erityisasiantuntija	Ismo Parviainen	Sisäministeriö
Tietoturvapäällikkö	Matti Parviainen	Espoon kaupunki
Tietoturvapäällikkö	Teijo Roine	Jyväskylän yliopisto
Erityisasiantuntija	Tuula Seppo	Kuntaliitto
Asiantuntija	Saana Seppänen	valtiovarainministeriö – 14.8.2017
Erityisasiantuntija	Simo Tanner	Kuntaliitto – varajäsen
Tietoturvapäällikkö	Juha Ilkka	Valtioneuvoston kanslia – 30.4.2017
Päällikkö	Mikko Viitaila	Viestintävirasto, kyberturvalvallisuus-keskus – 31.12.2017

Sihteeristö kokoontui vuonna 2017 kymmenen kertaa.

5.3 VAHTI-asiantuntijajaosto ja sen toiminta vuonna 2017

VAHTI asiantuntijajaoston tehtäviä ovat:

- valmistella valtiovarainministeriön linjauksia julkisen hallinnon digitaalisesta turvallisuudesta sekä seurata ja edistää niiden toimeenpanoa
- valmistella hallinnon digitaalista turvallisuutta koskevat säädökset, ohjeet, suositukset sekä muut tieto- ja kyberturvallisuuden linjaukset
- vastata VAHTI-sivuston sisällön ylläpidosta
- valmistella ja toteuttaa toimenpiteitä, joilla edistetään julkisen hallinnon tietoturvakulttuuria ja henkilöstön tietoturvatietoisuutta ja -osaamista
- valmistella ja toteuttaa toimenpiteitä, joilla edistetään tietosuojan toteutumista osana digitaalisen turvallisuuden kehittämistä
- julkisen hallinnon digitaaliseen turvallisuuteen liittyvien kehittämisohjelmien ja hankkeiden valmistelu sekä niiden toimeenpano
- digitaalisen turvallisuuden operatiivisen häiriötilanteiden hallinnan kehittäminen osana VIRT-toimintamallia
- valmistella julkisen hallinnon kansainvälisen tietoturvayhteistyön linjausten yhteen sovittamista kansainvälisessä tietoturvatyössä

VAHTIlle asetettujen tavoitteiden edistämiseksi sekä toimintasuunnitelmassa sovittujen tavoitteisen saavuttamisen mahdollistamiseksi on toiminnan tueksi asetettu viisi asiantuntijaryhmää.

VAHTIn asiantuntiajaoston toiminta

1 Riskienhallinta ja johtaminen (JORI)

Asiantuntijaryhmän toimintaan osallistuivat:

Puheenjohtajisto

Riskienhallintajohtaja	Juha Pietarinen	Valtiokonttori puheenjohtaja
Tietohallintojohtaja	Harri Ihalainen	Rovaniemen kaupunki varapuheenjohtaja

Jäsenet

Tietoturvapäällikkö	Antti Laulajainen	Eduskunta
Riskienhallintapäällikkö	Juha Kalander	Elintarviketurvallisuusvirasto
Tietohallintojohtaja	Johanna Knekt	Elintarviketurvallisuusvirasto
Tietoturvapäällikkö	Pekka Jäppinen	Hämeenlinnan kaupunki
Tietoturvapäällikkö	Teijo Roine	Jyväskylän yliopisto
Yksikön päällikkö	Esko Hätälä	Liikennevirasto
Johtava asiantuntija	Tuija Lehtinen	Maanmittauslaitos
Erityisasiantuntia	Ari Mannonen	Maa- ja metsätalousministriö
Erityisasiantuntija	Matti Aitta	Oikeusministeriö
Riskinhallintapäällikkö	Kimmo Janhunen	Oikeusrekisterikeskus
Tietoturvapäällikkö	Kaarlo Määttä	Oulun kaupunki
Tietohallintojohtaja	Kari Keinänen	Oulun yliopisto
Tietoturvapäällikkö	Juhana Yrjölä	Poliisihallitus – 31.8.2017
Tietoturvapäällikkö	Tuomas Kokkomäki	Poliisihallitus
Apulaisturvallisuusjohtaja	Kai Knape	Puolustusministeriö
Tietoturvallisuusjohtaja	Juha Tallinen	Puolustusvoimat
Ylitarkastaja	Katri Järvinen	Puolustusvoimat
Tietoturvapäällikkö	Antti-Olli Taipale	Päijät-Hämeen Hyvinvointi-yhtymä
Yksikön päällikkö	Ari Laaksonen	Rajavartiolaitoksen esikunta
Yksikön johtaja	Marja Kylämä	Suomen Akatemia
Tietoturvapäällikkö	Juha Koivisto	Tampereen kaupunki
Tietoturva-asiantuntija	Jari Seppälä	Tampereen teknillinen yliopisto
Tietoturvapäällikkö	Christian Jämsen	Terveyden ja hyvinvoinnin laitos
ICT-tietoturvapäällikkö	Pyry Heikkinen	Tulli
Prosessipäällikkö	Sami Nikula	Valtion talous- ja henkilöstö-hallinnon palvelukeskus

		Palkeet
Valmiuspäällikkö	Janne Kotilahti	Valtion tieto- ja viestintätekniikkakeskus Valtori
Riskienhallintapäällikkö	Tommi Simula	Valtion tieto- ja viestintätekniikkakeskus Valtori
Johtava tilintarkastaja	Mika Halme	Valtiotalouden tarkastusvirasto
Tietoturvapäällikkö	Erja Kinnunen	Verohallinto
Tietoturvapäällikkö	Pekka Ristimäki	Väestörekisterikeskus

Asiantuntijaryhmä kokoontui vuonna 2017 6 kertaa.

2 Toiminnan jatkuvuus (TOJA)

Asiantuntijaryhmän toimintaan osallistuivat:

Puheenjohtajisto

Tietoturvasuunnittelija	Jenni Siermala	Pohjois-Pohjanmaan sairaanhoitopiiri 1.9.2017 – puheenjohtaja
Erityisasiantuntija	Esa Keränen	Opetushallitus puheenjohtaja – 31.8.2017
Tietohallintopäällikkö	Maarit Puhto	Sosiaali- ja terveysministeriö varapuheenjohtaja

Jäsenet

Riskienhallintapäällikkö	Juha Kalander	Elintarviketurvallisuusvirasto
Tietoturvapäällikkö	Matti Parviainen	Espoon kaupunki läsnä
Tietohallintopäällikkö	Sasa Haavisto	Helsingin poliisilaitos
Tietoturvapäällikkö	Simo Poskiparta	Ilmatieteen laitos
Tietoturvapäällikkö	Olavi Manninen	Itä-Suomen yliopisto
Asianhallintapäällikkö	Arja Marjanen	Kilpailu- ja kuluttajavirasto
Tietohallintopäällikkö	Jyrki Tuohela	Opetushallitus
Yhteiskuntatieteiden rehtori	Matti Saren	Oulun yliopisto –31.8.2017
Tietohallintojohtaja	Kari Keinänen	Oulun yliopisto
Tietoturvasuunnittelija	Jenni Siermala	Pohjois-Pohjanmaan sairaanhoitopiiri
Tietoturvapäällikkö	Harri Mäntylä	puolustusministeriö
Suunnittelija	Matti Urvas	Puolustusvoimat
Osastoesiupseeri	Timo Kaartosalmi	Puolustusvoimat
Tietohallintopäällikkö	Pasi Koljonen	Puolustusvoimat
Tietoturvallisuuspäällikkö	Pia Satopää	Puolustusvoimat
Tietoturvavastaava	Kristiina Grönroos	Suomen Ympäristökeskus

Tietoturva-asiantuntija	Jari Seppälä	Tampereen teknillinen yliopisto
Hallintopalvelupäällikkö	Tuija Vihinen	Valtion talous- ja henkilöstöhallinnon palvelukeskus Palkeet
Valmiuspäällikkö	Janne Kotilahti	Valtion tieto- ja viestintätekniikkakeskus Valtori
Turvallisuuspäällikkö	Kai Perikangas	Verohallinto
Erityisasiantuntija	Heidi Kivekäs	Viestintävirasto
Suunnittelija	Tero Kaitosaari	Väestörekisterikeskus

Asiantuntijaryhmä kokoontui vuonna 2017 7 kertaa.

3 Turvallisuuden ylläpito (TUTO)

Asiantuntijaryhmän toimintaan osallistuivat:

Puheenjohtajisto

Tietoturvallisuuspäällikkö	Petri Puhakainen	Valtioneuvoston kanslia puheenjohtaja 1.6.2017-
Tietoturvapäällikkö	Juha Ilkka	Valtioneuvoston kanslia puheenjohtaja –30.4.2017
Mats Kommonen,	Tietoturvapäälikkö	Turun Yliopisto varapuheenjohtaja

Jäsenet

IT-erityisasiantuntija	Pauli Paatsola	ELY-keskusten sekä TE-toimistojen kehittämis- ja hallintokeskus
Ylikonstaapeli	Jyri Hurme	Helsingin poliisilaitos
Tietoturvapäällikkö	Anne Hintzell	Helsingin yliopisto –31.8.2018
Tietoturvapäällikkö	Kenneth Kahri	Helsingin yliopisto
Asianhallintapäällikkö	Arja Marjanen	Kilpailu- ja kuluttajavirasto
Yksikön päällikkö	Jukka Friman	Oikeusrekisterikeskus –31.8.2018
Tietoturva-arkkitehti	Riina Aaltonen	Oikeusrekisterikeskus
Tietoturva-asiantuntija	Petri Bergholm	Patentti- ja rekisterihallitus
Osastoesiupseeri	Timo Kaartosalmi	Puolustusvoimat
Asiahallintajohtaja	Janne Mykrä	Puolustusvoimat
Osastoinsinööri	Juha Savolainen	Puolustusvoimat
Osastoinsinööri	Juha Saarisilta	Puolustusvoimat
Asiahallintapäällikkö	Kristiina Hakala	Puolustusvoimat

ICT-järjestelmäpäällikkö	Samuli Niemi	Puolustusvoimat
Tietoturvapäällikkö	Jani Tossavainen	Rajavartiolaitoksen esikunta
Kehityspäällikkö	Riku Pammo	Rikosseuraamuslaitos
Tietohallintojohtaja	Harri Ihalainen	Rovaniemen kaupunki
Tietoturvapäällikkö	Juha Koivisto	Tampereen kaupunki
Tietoturvapäällikkö	Mats Kommonen	Turun yliopisto
Tietoturva-asiantuntija	Timo Miettinen	Verohallinto
Päällikkö	Arttu Lehmuskallio	Viestintävirasto
Suunnittelija	Tero Kaitosaari	Väestörekisterikeskus
Tietoturvapäällikkö	Jan Wennström	Åbo Akademi

Asiantuntijaryhmä kokoontui vuonna 2017 4 kertaa.

4 Turvallisuuden kehittäminen (TUKE)

Asiantuntijaryhmän toimintaan osallistuivat:

Puheenjohtajisto

Riskienhallintapäällikkö	Kimmo Janhunen	Oikeusrekisterikeskus puheenjohtaja
ICT-tietoturvapäällikkö	Pyry Heikkinen	Tulli varapuheenjohtaja

Jäsenet

Tietoturvapäällikkö	Antti Laulajainen	Eduskunta
IT-erityisasiantuntija	Pauli Paatsola	ELY-keskusten sekä TE- toimistojen kehittämis- ja hallintokeskus
Tietoturvapäällikkö	Anne Hintzell	Helsingin yliopisto – 31.8.2017
Tietoturvapäällikkö	Kenneth Kahri	Helsingin yliopisto
Tietoturvapäällikkö	Pekka Jäppinen	Hämeenlinnan kaupunki – 30.4.2017
Tietoturvapäällikkö	Tuovi Piirainen	Hämeenlinnan kaupunki
Tietoturvapäällikkö	Simo Poskiparta	Ilmatieteen laitos
IT-arkkitehti	Marko Karjalainen	Innovaatiorahoituskeskus Tekes
Suunnittelija	Satu Sorvali	Kansallisarkisto
Ylitarkastaja	Jorma Wall	Keskusrikospoliisi – 31.8.2017
Johtava sovellusasiantuntija	Olli Mensio	Maanmittauslaitos
Tietoturvasuunnittelija	Jenni Siermala	Pohjois-Pohjanmaan sairaanhoitopiiri
Tietoturva-asiantuntija	Petri Bergholm	Patentti- ja rekisterihallitus
Ylitarkastaja	Katri Järvinen	Puolustusvoimat

Osastoinsinööri	Juha Savolainen	Puolustusvoimat
Osastoinsinööri	Juha Saarisilta	Puolustusvoimat
ICT-järjestelmäpäällikkö	Samuli Niemi	Puolustusvoimat
Tietohallintopäällikkö	Pasi Koljonen	Puolustusvoimat
Asianhallintapäällikkö	Anni Rinne	Puolustusvoimat
Tietoturvapäällikkö	Antti-Olli Taipale	Päijät-Hämeen Hyvinvointi-yhtymä Hyvinvointiyhtymä
Tietoturvavastaava	Kristiina Grönroos	Suomen Ympäristökeskus
Tietoturvapäällikkö	Mats Kommonen	Turun yliopisto
Turvallisuuspäällikkö	Juhani Lahti	Työttömyysvakuutusrahasto
Johtava tilintarkastaja	Timo Kerttula	Valtiotalouden tarkastus-virasto
Tietoturvapäällikkö	Olli Joronen	Valtion tieto- ja viestintä-tekniikka Valtori
Erityisasiantuntija	Mika Kuivamäki	Sosiaali- ja terveysalan lupa- ja valvontavirasto Valtori –31.8.2017
Tietoturva-asiantuntija	Ville Härmä	Verohallinto
Erityisasiantuntija	Tomi Kelo	Viestintävirasto
Erityisasiantuntija	Kristian Sélen	Viestintävirasto

Asiantuntijaryhmä kokoontui vuonna 2017 8 kertaa.

5 Seuranta ja arviointi (SETI)

Asiantuntijaryhmän toimintaan osallistuivat:

Puheenjohtajisto

Tietoturvapäällikkö	Erja Kinnunen	Verohallinto puheenjohtaja
Neuvotteleva virkamies	Timo Nuutinen	Puolustusministeriö varapuheenjohtaja

Jäsenet

IT-arkkitehti	Marko Karjalainen	Innovaatiorahoituskeskus Tekes
Tietoturvapäällikkö	Olavi Manninen	Itä-Suomen yliopisto
Tietoturvapäällikkö	Teijo Roine	Jyväskylän yliopisto
Erityisasiantuntia	Ari Mannonen	Maa- ja metsätalousministeriö
Erityisasiantuntija	Matti Aitta	Oikeusministeriö
Tietohallintopäällikkö	Jyrki Tuohela	Opetushallitus
Erityisasiantuntija	Esa Keränen	Opetushallitus – 31.8.2017
Tietoturva-asiantuntija	Juho Isohanni	Poliisihallitus

Neuvotteleva virkamies	Timo Nuutinen	Puolustusministeriö
Tietoturvallisuusjohtaja	Juha Tallinen	Puolustusvoimat
Sektorijohtaja	Mikko Hakuli	Puolustusvoimat – 31.12.2017
Tietoturvallisuuspäällikkö	Pia Satopää	Puolustusvoimat
Turvallisuusupseeri	Vesa Harjula	Puolustusvoimat
Tietoturvallisuuspäällikkö	Laura Kujala	Puolustusvoimat
Erityisasiantuntija	Jari Soininen	Sisäministeriö
Tietohallintopäällikkö	Maarit Puhto	Sosiaali- ja terveysministeriö
Yksikön johtaja	Marja Kylämä	Suomen Akatemia
Tietoturvapäällikkö	Antti Savolainen	Ulkoasiainministeriö
Tietohallintojohtaja	Markku Salakka	Valkeakosken kaupunki
Johtava tilintarkastaja	Mika Halme	Valtiotalouden tarkastusvirasto
Tietoturvapäällikkö	Pekka Ristimäki	Väestörekisterikeskus
Tietoturvapäällikkö	Jan Wennström	Åbo Akademi

Asiantuntijaryhmä kokoontui vuonna 2017 6 kertaa.

5.4 Yhteenvetoa VAHTIn toiminnasta 2017

Kaikkien tällä sivulla esiteltyjen tilaisuuksien materiaalit ovat saatavilla: http://vm.fi/vahti-materiaalit-ja-tilaisuudet

Valtiovarainministeriö toteutti ensimmäisen VAHTI-kesäseminaarin 8.6.2017, paikalla oli vajaa 100 asiantuntijaa. Tilaisuudessa kerrottiin vuoden alusta käynnistyneen uudistetun VAHTI-toiminnan alkutaipaleesta. Lisäksi osallistujille kerrottiin muun muassa tiedonhallintalain ajankohtaiskatsaus sekä ajankohtaista tietosuojasta.

Valtionhallinnon vuosittainen tietoturvallisuuden ajankohtaisseminaari – 20. VAHTI-päivä julkisen hallinnon toimijoille järjestettiin 29.11.2017 valtiovarainministeriössä. VAHTI-päivässä oli paikalla noin 130 julkisen hallinnon edustajaa. Tilaisuudessa myönnettiin VAHTI-organisaatiotunnustus Verohallinnolle merkittävästä, korkeatasoisesta digitaalisen turvallisuuden kehittämisestä vuosina 2016–2017.

Vuoden aikana palkittiin pitkäaikaisesta, laadukkaasta työskentelystä VAHTI-johtoryhmän toiminnassa VAHTI-viirillä erityisasiantuntija Aarne Hummelholm valtiovarainministeriöstä, tietosuojavaltuutettu Reijo Aarnio tietosuojavaltuutetun toimistosta, VAHTIn ensimmäinen puheenjohtaja Kaarlo Korvola sekä erityisasiantuntija Simo Tanner Kuntaliitosta.

VAHTI on ollut aktiivisesti kehittämässä ja tukemassa HAUS Oy:n tietosuojavastaavien koulutusohjelmaa, jossa toteutettiin vuoden 2017 aikana kaksi koulutusohjelmaa, joihin osallistui yli 40 osallistujaa.

VAHTIn toiminnasta on tiedotettu JulkICT-osaston uutiskirjeissä ja tiedotteissa. VAHTIn toimintaa on mahdollista seurata Twitterissä @ VM_vahti sekä #VAHTI-tunnisteella. Toimintaa seuraa Twitterissä 285 seuraajaa.

Kirjoittaja:
Kimmo Rousku

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

ISSN 1797-9714 (pdf)
ISBN 978-952-251-948-1 (pdf)

Toukokuu 2018