VALTIOVARAINMINISTERIÖ

VAHTI

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä

Toimintasuunnitelma vuosille 2017–2019

Valtiovarainministeriön julkaisuja 21/2017

Julkisen hallinnon ICT

Valtiovarainministeriön julkaisuja 21/2017

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä

Toimintasuunnitelma vuosille 2017–2019

Valtiovarainministeriö, Julkisen hallinnon ICT, Helsinki 2017

Valtiovarainministeriö

ISBN: 978-952-251-860-6 (PDF)

ISBN: 978-952-251-859-0 (painettu)

Taitto: Valtioneuvoston hallintoyksikkö, Tietotuki- ja julkaisuyksikkö, Erja Kankala

Helsinki 2017

Kuvailulehti

Julkaisija	Valtiovarainministeriö		Toukokuu 2017
Tekijät	Kimmo Rousku (toimittaja)		
Julkaisun nimi	Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä; Toimintasuunnitelma vuosille 2017–2019		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisuja 21/2017		
Diaari/hankenumero		**Teema**	Julkisen hallinnon ICT
ISBN painettu	978-952-251-859-0	**ISSN painettu**	1459-3394
ISBN PDF	978-952-251-860-6	**ISSN PDF**	1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-251-860-6		
Sivumäärä	28	**Kieli**	suomi
Asiasanat	VAHTI, digitaalinen turvallisuus, tietoturvallisuus, kyberturvallisuus, tietosuoja		

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 uudistettu VAHTI jatkaa siten jo kaksikymmentä vuotta jatkunutta laaja-alaista tieto- ja kyberturvallisuuden, jatkossa laajemmin ymmärrettynä digitaalisen turvallisuuden kehittämistä. Tässä toimintasuunnitelmassa kuvataan niitä hankkeita, yhteistyön ja kehittämisen muotoja, joiden avulla VAHTI vastaa sille asetettujen tavoitteiden saavuttamisesta.

Vuosien 2017–2019 keskeisin kehittämiskohde on vuonna 2010 voimaan astuneen tietoturvallisuusasetuksen uudistaminen osana tietoturvasäädösten uusimista ja toimeenpanoa, joka vastaavasti toteutetaan osana uutta tiedonhallintalakia. Tähän liittyy keskeisesti myös uusien lainsäädäntöön perustuvien vaatimusten toteuttaminen (”VAHTI 100-vaatimukset”) sekä niiden julkaiseminen uudistetussa VAHTI-portaalissa.

Toinen keskeinen muutos VAHTI-toiminnassa on uudistettu digitaalisen turvallisuuden hallintamalli, jota toimeenpannaan jatkossa viidessä asiantuntijajaoston alaisuudessa toimivassa asiantuntijaryhmässä. Ryhmät vastaavat muun muassa edellä mainittujen uusien vaatimusten kehittämisestä, ylläpidosta sekä niiden edellyttämien tukimateriaalien toteuttamisesta. Kolmas keskeinen toimenpide koskee tietosuojan kehittämistä julkisessa hallinnossa. Tämä tapahtuu yhteistyössä julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) kanssa toteutettavien tietosuojakoulutusten sekä tietosuoja-asetuksen osoittamisvelvollisuuden yhteishankkeen avulla. Lisäksi VAHTI kehittää toimikauden aikana digitaalisen turvallisuuden kokonaiskuvan raportointia ja mittaamista organisaatio- ja henkilöstötasolla.

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

Presentationsblad

Utgivare	Finansministeriet		Maj 2017
Författare	Kimmo Rousku (redaktör)		
Publikationens titel	Ledningsgruppen för informations- och cybersäkerheten inom statsförvaltningen; Verksamhetsplan för åren 2017–2019		
Publikationsseriens namn och nummer	Finansministeriets publikationer 21/2017		
Diarie-/ projektnummer		**Tema**	Offentliga förvaltningens ICT
ISBN tryckt	978-952-251-859-0	**ISSN tryckt**	1459-3394
ISBN PDF	978-952-251-860-6	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-251-860-6		
Sidantal	28	**Språk**	finska
Nyckelord	VAHTI, digital säkerhet, informationssäkerhet, cybersäkerhet, datasekretess		

Referat

Finansministeriet ansvarar för den allmänna utvecklingen av informationssäkerheten inom den offentliga förvaltningen och styrningen av informationssäkerheten inom statsförvaltningen. Finansministeriets behörighet inom styrning och utveckling av informationssäkerheten och informationsförvaltningen bygger på nya lagar, författningar och förordningar. Finansministeriet har tillsatt en ledningsgrupp för informations- och cybersäkerheten inom statsförvaltningen (VAHTI) att fungera som ett samarbets-, berednings- och samordningsorgan som svarar för utvecklingen och styrningen av den digitala säkerheten inom den offentliga förvaltningen.

Den förnyade VAHTI som tillsattes för ett treårigt mandat från början av 2017 fortsätter således den redan i 20 år pågående, omfattande utvecklingen av informations- och cybersäkerheten, som i framtiden går under det mer omfattande begreppet digital säkerhet. I denna verksamhetsbeskrivning beskrivs de projekt samt samarbets- och utvecklingsformer, med hjälp av vilka VAHTI uppnår de mål som fastställts för gruppen.

Det viktigaste utvecklingsobjektet för åren 2017–2019 är reformen av informationssäkerhetsförordningen som trädde i kraft 2010 som en del av förnyelsen och genomförandet av informationssäkerhetsförfattningarna, vilket på motsvarande sätt genomförs som en del av den nya informationsförvaltningslagen. Detta är även centralt förknippat med genomförande av kraven som bygger på den nya lagstiftningen (”VAHTI 100-kraven”) samt publicering av dessa i den förnyade VAHTI-portalen. En annan central ändring av VAHTI:s verksamhet är den förnyade förvaltningsmodellen för digital säkerhet, som i framtiden kommer att genomföras i fem expertgrupper som verkar under sakkunnigsektionen. Grupperna ansvarar för bland annat utveckling och underhåll av de nya kraven ovan samt produktion av stödmaterial för kraven. Den tredje centrala åtgärden gäller utvecklingen av dataskyddet inom den offentliga förvaltningen. Detta sker med hjälp av dataskyddsutbildningar som genomförs i samarbete med delegationen för informationsförvaltningen inom den offentliga förvaltningen (JUHTA) samt ett samprojekt som gäller spårbarhetsskyldigheten i samband med dataskyddsförordningen. Därtill utvecklar VAHTI under sitt mandat rapporteringen och mätningen om en helhetsbild av den digitala säkerheten på organisations- och personalnivå.

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

Description sheet

Published by	Ministry of Finance		May 2017
Authors	Kimmo Rousku (editor)		
Title of publication	The Government Information Security Management Board; Agenda 2017–2019		
Series and publication number	Ministry of Finance publications 21/2017		
Register number		**Subject**	Public Sector ICT
ISBN (printed)	978-952-251-859-0	**ISSN (printed)**	1459-3394
ISBN PDF	978-952-251-860-6	**ISSN (PDF)**	1797-9714
Website address (URN)	http://urn.fi/URN:ISBN:978-952-251-860-6		
Pages	28	**Language**	Finnish
Keywords	VAHTI, digital security, data security, cyber security, privacy protection		

Abstract

The Ministry of Finance is responsible for the general development of data security in public administration and governing the data security of state administration. The authority of the Ministry of Finance for governing and developing data security and data administration is based on various statutes and regulations. The Ministry of Finance has appointed the Government Information Security Management Board (VAHTI) to act as the co-operation, drafting and co-ordination agency for the organisations responsible for developing and governing digital security in public administration.

Starting their three-year term in 2017, VAHTI will continue over twenty years of development of comprehensive data and cyber security, seen as parts of the larger concept of digital security going forward. This agenda describes the projects and forms of co-operation and development that VAHTI will employ to reach the objectives set for it.

Between 2017 and 2019, the main development area is the updating of the 2010 Government Decree on Information Security in Central Government as part of the modernisation and implementation of data security legislation, which in turn is part of the implementation of the new data management legislation. The implementation and publication in the updated VAHTI portal of new statutory requirements ("VAHTI100") is closely related to this effort. Another key change in VAHTI activities is the updated digital security management model that will be implemented by five expert workgroups under the supervision of the expert unit. The groups will be responsible for developing and maintaining the aforementioned new requirements, as well as creating the necessary support materials. The third key measure concerns the development of privacy protection in public administration. This will be achieved through privacy protection training executed in co-operation with the Advisory Committee on Information Management in Public Administration (JUHTA), as well as the joint General Data Protection Regulation responsibilities assignment project. During its term, VAHTI will also develop the reporting and measuring of the digital security overview on the organisational and personnel levels.

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

Sisältö

1 VAHTIn toiminnan lähtökohdat

Tarkoituksenmukaisesti toteutettu tieto- ja kyberturvallisuus, laajemmin toteutettuna digitaalinen turvallisuus, on yksi yhteiskunnan toiminnan perusedellytyksistä. Tässä julkisen hallinnon tuottamilla palveluilla on merkittävä rooli. Toiminnan kehittäminen painottuu julkisessa hallinnossa yhä enemmän sen digitalisoimiseen, automatisoimiseen sekä robotiikan ja keinoälyn hyödyntämiseen. Lisäksi erilaisten IoT-laitteiden sensoreilla kerättävää tietoa voidaan rikastaa ja jalostaa uudenlaisilla tavoilla Big Datan avulla. Kansalaiset tuottavat ja hallinnoivat yhä enemmän heihin itseensä liittyvää tietoa osana Omatieto-mallia (MyData). Tämän toimintaympäristön muutoksen takia perinteinen tietoturvallisuus, joka keskittyy ensisijaisesti tiedon luottamuksellisuuden, eheyden ja saatavuuden varmistamiseen, on tarkastelukulmana liian kapea. Uudelleen organisoitu VAHTI-toiminta tähtää aiempaa laaja-alaisempaan digitaalisen toimintaympäristön toiminnan turvaamiseen, jossa keskeisessä roolissa ovat riskienhallinta, tieto- ja kyberturvallisuus sekä toiminnan jatkuvuuden takaaminen.

Valtiovarainministeriön tehtävänä on julkisen hallinnon tietoturvallisuuden yleinen kehittäminen ja valtionhallinnon tietoturvallisuuden ohjaus. Valtiovarainministeriön toimivalta tietoturvallisuuden ja tietohallinnon ohjauksessa sekä kehittämisessä perustuu useisiin lakeihin, säädöksiin ja asetuksiin. Tällaisia ovat laki julkisen hallinnon tietohallinnon ohjaamisesta (634/2011), laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011), valmiuslaki (1552/2011), valtioneuvoston ohjesääntö (262/2003) ja valtioneuvoston asetus valtiovarainministeriöstä (610/2003).

Valtiovarainministeriö vastaa turvallisuusverkkotoiminnan yleishallinnollisesta, strategisesta, taloudellisesta ja tieto- ja viestintäteknisen varautumisen, valmiuden sekä turvallisuuden ohjauksesta ja valvonnasta. Valtiovarainministeriön vastuulla on laissa valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä tarkoitettujen yhteisten palvelujen palvelutuotannon yleishallinnollinen, strateginen sekä tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjaus. Lisäksi valtiovarainministeriön vastuulla on laki hallinnon yhteisistä sähköisen asioinnin tukipalveluista.

Valtiovarainministeriö on asettanut VAHTIn toimimaan julkisen hallinnon digitaalisen turvallisuuden kehittämisestä ja ohjauksesta vastaavien organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä. VAHTIn asema on kirjattu voimassa oleviin valtioneuvoston periaatepäätöksiin Suomen kyberturvallisuusstrategiasta 2013 ja valtionhallinnon tietoturvallisuuden kehittämisestä 2009. Lisäksi VAHTIlla on keskeinen rooli kyberturvallisuusstrategian toimeenpano-ohjelman toteuttamisessa.

Uudelle toimikaudelle annettu nimi, VAHTI Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä, kuvaa tapahtunutta toiminnan ja toimintaympäristön muutosta. Myös henkilötietojen käsittely on digitalisoitunut voimakkaasti, mikä osaltaan vaikuttaa tietosuojan toteutumiseen.

Valtiovarainministeriö vahvistaa ja kehittää VAHTIn toimintaa sekä sen tuloksellisuutta, jotta tuleviin uusiin digitaalisen toimintaympäristön haasteisiin pystytään paremmin vastaamaan. VAHTI edistää myös julkishallinnon toiminnan digitalisaatiota huolehtimalla tarkoitustenmukaisen turvallisuuden vaatimuskehikon laatimisesta ja ylläpitämisestä. Tähän kuuluvat myös turvallisuuteen sekä ICT-toiminnan jatkuvuuteen liittyvät tarkastukset, hyväksynnät ja arvioinnit sekä tieto- ja kyberturvallisuusharjoitustoiminnan edistäminen.

1.1 VAHTIn tavoitteet

VAHTI tukee valtiovarainministeriön päätöksentekoa ja sen valmistelua julkisen hallinnon digitaalista turvallisuutta koskevissa asioissa.

VAHTI kehittää digitaalista turvallisuutta, joka 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
- toiminnan laadun ja riskienhallinnan parantamisen.

VAHTI edistää myös näiden asioiden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta. Lisäksi VAHTI edistää tietojärjestelmien, tietoverkkojen ja tieto- ja viestintäteknisten palvelujen kehittämistä, ylläpitoa, käyttöä ja palvelutuotantoa.

Kehittämällä julkisen hallinnon ja valtionhallinnon digitaalista turvallisuutta sekä niihin liittyvää yhteistyötä VAHTI edistää hallitusohjelman, Yhteiskunnan turvallisuusstrategian, Suomen kyberturvallisuusstrategian, valtionhallinnon tietoturvallisuuden kehittämistä

koskevan valtioneuvoston periaatepäätöksen ja hallituksen sekä valtiovarainministeriön muiden keskeisten linjausten toimeenpanoa.

1.2 VAHTIn tehtävät

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

1. Valmistelee ja sovittaa yhteen valtiovarainministeriön linjauksia julkisen hallinnon digitaalisesta turvallisuudesta sekä seuraa ja edistää niiden toimeenpanoa
2. Käsittelee julkisen hallinnon digitaalista turvallisuutta koskevat säädökset, ohjeet, suositukset
3. Edistää julkisen hallinnon tietoturvakulttuuria ja henkilöstön tietoturvatietoisuutta
4. Edistää tietosuojan toteutumista osana digitaalisen turvallisuuden kehittämistä
5. Toteuttaa digitaalista turvallisuutta koskevia kyselyitä ja barometrejä sekä julkaisee havainnoista koostettuja raportteja ja kehittämissuunnitelmia
6. Mittaa, kokoaa ja ylläpitää kokonaiskuvaa julkisen hallinnon digitaalisen turvallisuuden tilanteesta sekä raportoi siitä valtiovarainministeriön johdolle
7. Ohjaa, valmistelee ja sovittaa yhteen julkisen hallinnon digitaaliseen turvallisuuteen liittyviä kehittämisohjelmia ja hankkeita sekä niiden toimeenpanoa
8. Kehittää digitaalisen turvallisuuden operatiivista häiriötilanteiden hallintaa osana VIRT-toimintamallia
9. Käsittelee ja sovittaa yhteen julkisen hallinnon kansainvälisen tietoturvayhteistyön linjauksia ja vaikuttamista kansainvälisessä tietoturvatyössä.

Utgångspunkterna för VAHTIs verksamhet

Ändamålsenlig informations- och cybersäkerhet, digital säkerhet i en vidare bemärkelse, är en grundläggande förutsättning för att samhället ska fungera. Här spelar de offentliga tjänsterna en viktig roll. Digitalisering, automatisering samt utnyttjande av robotik och artificiell intelligens spelar en allt mera framträdande roll inom den offentliga förvaltningens verksamhet. Material som insamlas av olika slags IoT-sensorer kan dessutom anrikas och förädlas på nya slags sätt med hjälp av Big Data. Medborgarna producerar och administrerar i allt större omfattning information som gäller de själva tack vare MyData-modellen. Denna förändring i verksamhetsomgivningen innebär att traditionell informationssäkerhet, som i första hand fokuserar på säkerställandet av informationens konfidentialitet, enhetlighet och tillgänglighet, utgör ett alldeles för snävt perspektiv. Den omorganiserade VAHTI-verksamhetens övergripande mål är att trygga verksamheten i en digital verksamhetsomgivning så att riskhanteringen, informations- och cybersäkerheten samt säkerställandet av verksamhetens kontinuitet står i fokus.

Finansministeriet svarar för det allmänna utvecklandet av informationssäkerheten inom den offentliga förvaltningen och för styrandet av informationssäkerheten inom statsförvaltningen. Finansministeriets behörighet i fråga om informationssäkerhet och styrningen av informationsförvaltningen baserar sig på flera lagar, föreskrifter och förordningar. Som exempel kan nämnas lagen om styrning av informationsförvaltningen inom den offentliga förvaltningen (634/2011), lagen om bedömning av informationssäkerheten i myndigheternas informationssystem och datakommunikation (1406/2011), beredskapslagen (1552/2011), reglementet för statsrådet (262/2003) samt statsrådets förordning om finansministeriet (619/2003).

Finansministeriet svarar för den allmänna administrativa, strategiska och ekonomiska styrningen och tillsynen samt av styrningen av och tillsynen över den informations- och kommunikationstekniska beredskapen och säkerheten. Finansministeriet ansvarar för den allmänna administrativa och strategiska styrningen av serviceproduktionen som gäller de gemensamma tjänster som avses i lagen om anordnande av statens gemensamma informations- och kommunikationstekniska tjänster samt för styrningen av den informations-

och kommunikationstekniska beredskapen och säkerheten. Finansministeriet ansvarar dessutom för lagen om förvaltningens gemensamma stödtjänster för e-tjänster.

Finansministeriet har tillsatt VAHTI till samarbets-, berednings- och koordineringsorgan för organisationerna som svarar för utvecklandet och styrningen av den digitala säkerheten inom den offentliga förvaltningen. VAHTIs ställning har bekräftats i statsrådets principbeslut om Finlands cybersäkerhetsstrategi från 2013 och om utvecklandet av informationssäkerheten inom statsförvaltningen från 2009. VAHTI spelar dessutom en central roll i genomföringen av verkställighetsprogrammet för cybersäkerhetsstrategin.

Det nya namn som getts för den nya mandatperioden, VAHTI - ledningsgruppen för den digitala säkerheten inom den offentliga förvaltningen, beskriver förändringen i verksamheten och verksamhetsomgivningen. Behandlingen av personuppgifter har digitaliserats i stor omfattning, vilket också har konsekvenser för integritetsskyddet.

Finansministeriet förstärker och utvecklar VAHTIs verksamhet och dess effektivitet så att man ska kunna svara mot nya utmaningar inom den digitala verksamhetsomgivningen. VAHTI främjar även digitaliseringen av verksamheten inom den offentliga förvaltningen genom att svara för utarbetandet och underhållet av ett ändamålsenligt regelverk för säkerheten. Detta inkluderar granskningar, godkännanden och utvärderingar som har ett samband med säkerheten och IKT-verksamhetens kontinuitet samt främjandet av informations- och cybersäkerhetsövningar.

VAHTIs målsättningar

VAHTI stödjer finansministeriet vid beredningen och fattandet av beslut som gäller den digitala säkerheten inom den offentliga förvaltningen.

VAHTI utvecklar digital säkerhet som möjliggör

- digitalisering och robotisering av verksamheten inom den offentliga förvaltningen,
- pålitliga funktioner,
- konfidentialiteten hos sekretessbelagda uppgifter,
- tillgång till och oavbrutenhet hos informationen,
- kontinuerlig verksamhet och beredskap inför störningssituationer samt
- förbättring av verksamhetens kvalitet och riskhanteringen.

VAHTI främjar även integreringen av dessa frågor till en elementär del av verksamheten samt ledningen och resultatstyrningen av förvaltningen. VAHTI främjar dessutom utvecklandet, underhållet, användningen och serviceproduktionen av informationssystem, datanät samt informations- och kommunikationstekniska tjänster.

VAHTI främjar verkställandet av regeringsprogrammet, Säkerhetsstrategin för samhället, Finlands cybersäkerhetsstrategi, Statsrådets principbeslut om utvecklandet av informationssäkerheten inom statsförvaltningen och andra väsentliga riktlinjer som utsakats av regeringen och finansministeriet genom att utveckla den digitala säkerheten och det tillhörande samarbetet inom den offentliga förvaltningen och statsförvaltningen.

VAHTIs uppgifter

VAHTI är ett samarbetsorgan för styrningen och utvecklandet av den digitala säkerheten inom den offentliga förvaltningen.

VAHTI

1. bereder och samordnar finansministeriets riktlinjer för den offentliga förvaltningens digitala säkerhet, samt följer och främjar verkställandet av dem
2. behandlar författningar, anvisningar och rekommendationer som gäller den digitala säkerheten inom den offentliga förvaltningen
3. främjar informationssäkerhetskulturen inom den offentliga förvaltningen och personalens informationssäkerhetsmedvetenhet
4. främjar förverkligandet av integritetsskyddet som ett led i utvecklandet av den digitala säkerheten
5. genomför enkäter och barometrar om den digitala säkerheten och publicerar rapporter och utvecklingsplaner som sammanställts på basis av observationerna
6. mäter, sammanställer och upprätthåller en övergripande bild av läget med den digitala säkerheten inom den offentliga förvaltningen och rapporterar om det till finansministeriet
7. styr, bereder och samordnar utvecklingsprogram och projekt som har ett samband med den digitala säkerheten inom den offentliga förvaltningen samt verkställandet av dem
8. utvecklar den operativa kontrollen av digitala störningssituationer inom VIRT-verksamhetsmodellen
9. behandlar och samordnar riktlinjerna för det internationella informationssäkerhetssamarbetet inom den offentliga förvaltningen och påverkandet inom det internationella informationssäkerhetssamarbetet.

The principles of VAHTI's activities

Appropriately implemented data and cyber security – digital security in the broader context – are basic requirements for a functional society. The services provided by the public administration play a significant role in this. The development of operations in public administration is increasingly focused on their digitalisation and automation, as well as the utilisation of robotics and artificial intelligence. Furthermore, the data collected with the various sensors of IoT devices can be refined in new ways using Big Data. Citizens are increasingly producing and managing their personal information as part of the MyData (Omatieto) model. This change in the operating environment results in the traditional data security point of view being inadequate, as it only involves ensuring the confidentiality, integrity and availability of data. The reorganised VAHTI activities will be aimed at more comprehensive operational security in the digital operating environment, where risk management, data security, cyber security and ensuring the continuity of operations are key.

The Ministry of Finance is responsible for the general development of data security in public administration and governing the data security of state administration. The authority of the Ministry of Finance in governing and developing data security and data administration is based on various statutes and regulations. These include the Act on the governance of data administration in public administration (634/2011), the Act on data security assessments of official information systems and data communication arrangements (1406/2011), the Act on readiness (1552/2011), the Government Rules of Procedure (262/2003) and the Government Decree on the Ministry of Finance (610/2003).

The Ministry of Finance is responsible for the general and strategic governance and monitoring of security network activities, as well as the related financial preparedness, preparedness of information and communications technology, readiness and security. The Ministry of Finance is responsible for the general and strategic governance of the service production of the services described in the Act on the provision of the shared central government information and communication services, as well as the related preparedness of data and communications technology, readiness and security. In addition, the

Ministry of Finance is responsible for the Act on the shared electronic services of central government.

The Ministry of Finance has appointed VAHTI to act as the co-operation, drafting and co-ordination agency for the organisations responsible for developing and governing digital security in public administration. The mandate of VAHTI is set down in the current government resolutions on Finland's cyber security strategy (2013) and the development of data security in state administration (2009). VAHTI is also central to the implementation of the cyber security strategy enforcement plan.

The name used in the new term, Government Information Security Management Board (VAHTI), reflects the change in activities and the operating environment. Digitalisation has also become prevalent in the handling of personal information, which in part affects the realisation of privacy protection.

The Ministry of Finance will strengthen and develop the operations and effectiveness of VAHTI, so that new challenges of the digital operating environment can be met. VAHTI will enhance the digitalisation of public administration operations by preparing and maintaining the appropriate security requirements framework. This will include audits, certification and evaluations related to security and the continuity of ICT operations, as well as the promotion of data and cyber security exercises.

VAHTI's objectives

VAHTI supports the decision-making of the Ministry of Finance and the related preparation work in matters concerning digital security in public administration.

VAHTI develops digital security, enabling

- the digitalisation and robotisation of public administration,
- operational reliability,
- the confidentiality of sensitive information,
- the availability and integrity of information and operations,
- the continuity of operations and preparedness for disruptions,
- the improvement of operational quality and risk management.

VAHTI will also promote the integration of these into the operations, management and steering of administration. Furthermore, VAHTI will advance the development, maintenance, use and service production of information systems, information networks and data and communication services.

By developing the digital security of public administration and state administration, as well as the related co-operation, VAHTI supports the implementation of the other key policies of the government platform, the national security strategy, Finland's cyber security strategy and the government resolution on the development of data security in state administration.

VAHTI's tasks

VAHTI is a body for the governance and development of digital security in public administration, as well as the related co-operation.

VAHTI

1. Prepares and co-ordinates the policies of the Ministry of Finance regarding digital security in public administration, and monitors and supports their implementation
2. Processes the statutes, guidelines and recommendations regarding digital security in public administration
3. Advances the data security culture in public administration and the data security awareness of personnel
4. Furthers the implementation of privacy protection as part of the development of digital security
5. Carries out surveys and the like to assess digital security and publishes reports and development plans based on the observations
6. Measures, assembles and maintains the overall picture of the state of digital security in public administration, and reports it to the Ministry of Finance
7. Steers, prepares and co-ordinates development programmes and projects related to digital security in public administration, as well as their implementation
8. Develops the operative management of disruptions in digital security as part of the VIRT operating model
9. Processes and combines international data security co-operation policies of public administration and the influencing efforts in international data security affairs.

2 Julkisen hallinnon digitaalisen turvallisuuden kehittämistoimet 2017–2019

VAHTI kehittää julkisen hallinnon digitaalista turvallisuutta tässä luvussa kuvatuilla toimenpiteillä. Niillä huolehditaan myös edellä kuvattujen yhdeksän tehtävän toteuttamisesta.

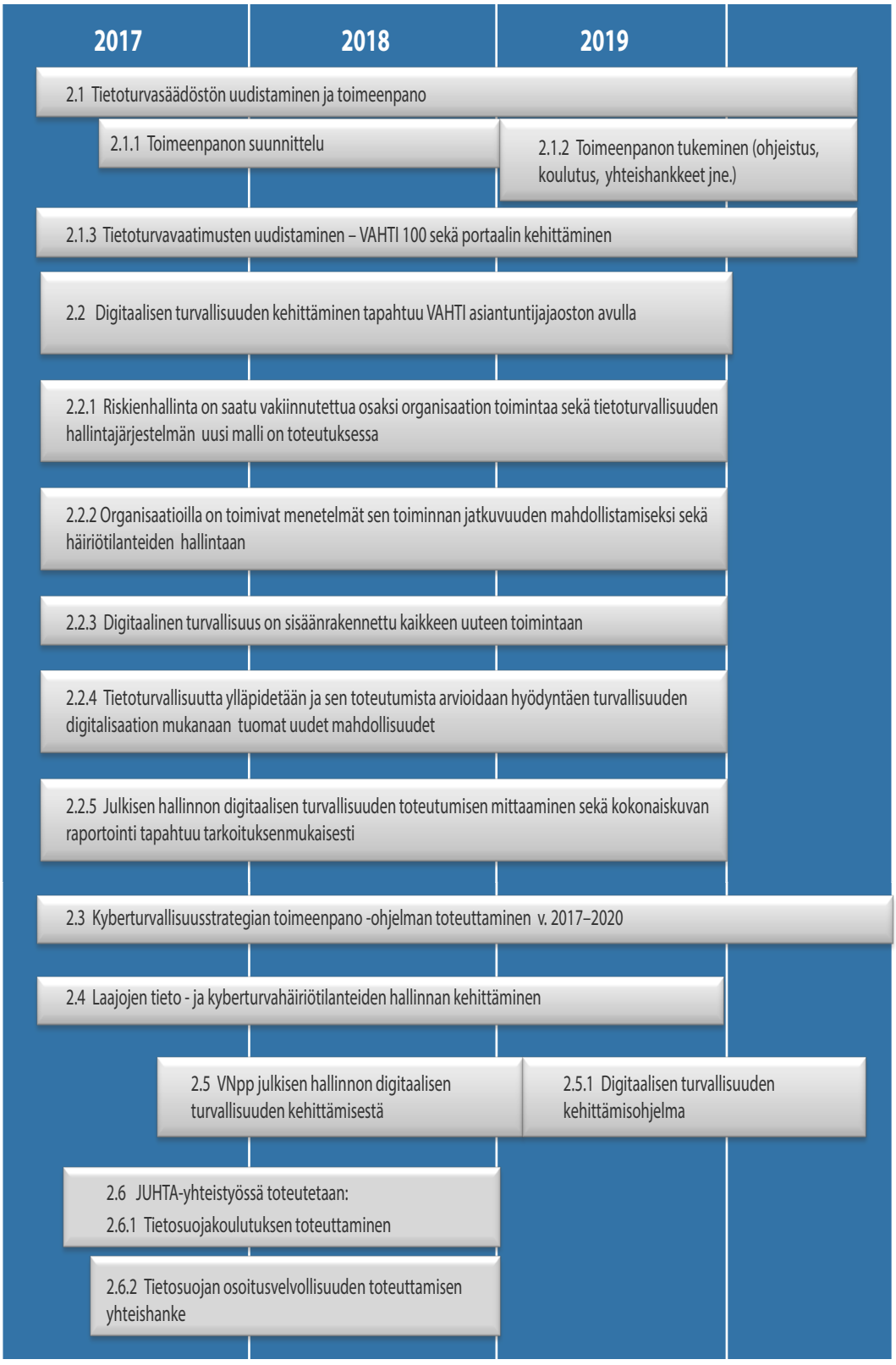
VAHTIn sihteeristö ja asiantuntijaryhmien puheenjohtajat päivittävät toimintasuunnitelman vuosittain siten, että VAHTI-johtoryhmä voi käsitellä ja päättää toimintasuunnitelman päivityksestä.

2.1 Tietoturvasäädösten uusiminen ja toimeenpano

Aikataulu: 1.1.2017–31.12.2019

Valtiovarainministeriön asettama Tietoturvallisuuden säädöstön valmistelun ohjausryhmä, jonka toimikausi oli 11.4.2016–28.2.2017, on toteuttanut sille asettamisessa määritetyt tehtävät. Ne koostuivat

- tietoturva-asetuksen soveltamisen nykytilan kuvauksesta valtionhallinnossa,
- tietoturva-asetuksen soveltamisen nykytilan haasteiden kuvauksesta ja kehittämistarpeista julkisessa hallinnossa,
- tietoturvasäädösten vertailusta keskeisissä EU-maissa,
- tietoturvatutkimustiedon hankkimisesta tavoitetilan pohjaksi Suomesta,
- tietoturvasäännöstön kehittämisen tavoitetilan kuvauksesta Suomessa mukaan lukien suhde kybertoimintaympäristön turvallisuuteen sekä
- tavoitetilan taloudellisen vaikuttavuuden kuvauksesta.



Kuva 1. VAHTIn keskeiset toimenpiteet digitaalisen turvallisuuden kehittämiseksi vuosille 2017–2019.

Edellä mainitun ohjausryhmän työ liittyy valtiovarainministeriön julkisen hallinnon tiedonhallinnon sääntelyä selvittävän työryhmän (Tilke) toimintaan. Tilken tavoitteena on saada voimaan tiedonhallintalaki, jolla ohjataan hyvää tiedonhallintatapaa ja tietojen käsittelyä julkisessa hallinnossa. Osana tätä lainsäädäntöä uudistetaan tietoturvallisuuteen liittyvät säädökset. Tämä edellyttää toimeenpanon suunnittelua ja lainsäädännön toimeenpanoa, erityisesti sovellusalueen koskiessa nykyistä tietoturvallisuusasetusta (681/2010) laajempaa kohdejoukkoa, kuten maakuntia ja kuntia.

2.1.1 Toimeenpanon suunnittelu

Aikataulu: 1.5.2017–31.12.2018

Suunnitteluvaiheessa laaditaan toimenpidesuunnitelma lainsäädännön toimeenpanon toteuttamiseksi siirtymäkauden ajalle alkaen lain voimaantulosta vuonna 2018. Toimeenpanon suunnittelussa hyödynnetään VAHTIn kokemuksia lukuisista vuoden 2010 tietoturvallisuusasetuksen toimeenpanon yhteishankkeista, koulutuksista sekä tietoturvasäädösten nykytilaselvityksen haastatteluissa kerättyä palautetta.

Keskeistä on suunnitella ja laatia tarvittavat ohjeet ja materiaalit sekä koulutukset eri kohderyhmille sekä toteuttaa eri kohderyhmille tarkoitettuja yhteishankkeita. Toimeenpanossa voidaan hyödyntää VAHTI-portaalia kokonaisuuden sähköisenä alustana.

2.1.2 Toimeenpanon tukeminen

Aikataulu: x.x.2019–31.12.2019 / koko lainsäädännön siirtymäkausi

Toimeenpanon tukeminen on yllä kuvatussa suunnitteluvaiheessa määritettyjen toimenpiteiden toteuttamista.

2.1.3 Tietoturvavaatimusten uudistaminen – VAHTI 100 sekä VAHTI-portaalin kehittäminen

Aikataulu: 1.1.2017–31.12.2019 / koko siirtymäkausi

Tietoturvallisuutta koskevan lainsäädäntötyön yksi keskeisistä lopputuloksista on uusitut tietoturvallisuuden vähimmäistason vaatimukset. Käytännössä tämä edellyttää muun muassa:

- tietoturvallisuuden vähimmäistason vaatimuksia, jotka julkisen tiedon osalta jakautuvat tiedon eheyden ja saatavuuden vaatimuksiin sekä tiedon luottamuksellisuuden osalta lisäksi salassapidon toteuttamiseen liittyviin vaatimuksiin
- turvallisuusluokiteltujen tietojen ST IV-, ST III- ja ST II-I -tasoille luokiteltujen tietoaineistojen käytön edellyttämiä vaatimuksia

- riskienarviointiprosessia, jonka avulla organisaatio arvioi vähimmäis- ja ne ylittävien vaatimusten edellyttämät suojauskeinot sekä huolehtii jäännösriskien käsittelystä.

Organisaation tietoturvallisuuden hallintajärjestelmää ja hallinnollista tietoturvallisuutta koskevien vaatimusten lisäksi tarvitaan vaatimuksia koskien kontrolleja, joiden avulla organisaatio toteuttaa teknistä tietoturvallisuutta toiminnassaan.

Edellä kuvatuista vaatimuksista tulee lisäksi toteuttaa yhteistyössä Hansel Oy:n kanssa oma erillinen vaatimuskokonaisuutensa, jota voidaan käyttää hankintavaatimuksina julkisissa hankinnoissa.

Vaatimusten ja samalla tietoturvallisuuden toteutumiseen liittyy niiden arviointi, tarkastus ja muu hyväksymistoiminta. Vaatimuskokonaisuudesta tulee luoda KATAKRI-arviointityökalua varten päivitetty versio, jonka avulla niin organisaatio, toimivaltainen viranomainen kuin kuka tahansa ulkopuolinen taho voi toteuttaa tarvitsemansa arvioinnin.

Vaatimuskokonaisuus julkaistaan VAHTI-portaalissa sinne luodun ns. vaatimuskorttimallin avulla. Vaatimuksia tulee hallita, katselmoida säännönmukaisesti ja reagoida toimintaympäristössä tapahtuviin muutoksiin. Tämä tullaan tekemään osana VAHTI-asiantuntijaryhmien toimintaa.

2.2 Digitaalisen turvallisuuden kehittäminen VAHTI-asiantuntijajaoston avulla

VAHTI-asiantuntijajaoston toiminta ja digitaalisen turvallisuuden kehittäminen Aikataulu: 1.3.2017–31.12.2019

VAHTI on asettanut alaisuuteensa sihteeristön ja asiantuntijajaoston, joka koostuu viidestä asiantuntijaryhmästä. Tämän toimintasuunnitelman toteuttamisessa keskeisessä roolissa on sihteeristön toteuttama asiantuntijaryhmien ohjaus, koordinointi ja toiminnan yhteensovittaminen.

Vuonna 2017 kaikkien asiantuntijaryhmien keskeisin tehtävä on VAHTI 100 vaatimuskokonaisuuden kehittäminen sekä siihen liittyvän VAHTI-portaalin materiaalin tuottaminen. Asiantuntijaryhmillä on asetettu myös muita tehtäviä.

Vuonna 2018 toteutetaan ja jatketaan edelleen voimaan astuvan lainsäädännön toimeenpanoa edistäviä toimenpiteitä ja VAHTI-portaalin sisällöllistä kehittämistä.

2.2.1 Riskienhallinta on saatu vakiinnutettua osaksi organisaation toimintaa ja tietoturvallisuuden hallintajärjestelmän uusi malli on toteutuksessa

Johtaminen ja riskienhallinta -asiantuntijaryhmä

Asiantuntijaryhmän tehtävänä on edistää keinoja, joilla luodaan organisaation perusvalmiudet, kuten menettelyt suojattavien kohteiden tunnistamiseen. Tehtäviin kuuluu myös huolehtia tietoturvallisuuden hallintajärjestelmän toteuttamisen, henkilöstön tietoturvatietoisuuden ja osaamisen sekä kokonaisuuden johtamisen ohjeistamisesta. Lisäksi ryhmä vastaa riskienhallinnan ohjeistuksen kehittämisestä, VAHTI-riskienhallintaohjeen ja prosessin jalkauttamisesta sekä näiden jatkokehittämisestä.

Vuoden 2017 tehtävät:

- VAHTIn riskienhallinnan ohjeen 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, johon sisältyy riskienhallinnan, toiminnan jatkuvuuden sekä tietoturvapoikkeamatilanteiden ja tietosuojaloukkausten hallinnan näkökulma
- Digitaalisen turvallisuuden tietoisuuden kasvattaminen osana vuosittain lokakuussa toteutettavaa European Cyber Security Month -kuukautta
- Muiden digitaalisen turvallisuuden johtamista ja riskienhallintaa edistävien toimenpiteiden toteuttaminen.

2.2.2 Organisaatioilla on toimivat menetelmät toiminnan jatkuvuuden mahdollistamiseksi ja häiriötilanteiden hallintaan

Toiminnan jatkuvuuden hallinta -asiantuntijaryhmä

Toiminnan jatkuvuuden hallinta -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 hallintaohjeen ja sen yhteydessä laaditun Business Impact Analysis (BIA) vaikutusarviotyökalun tunnettavuuden ja hyödyntämisen lisääminen
  - JUHTAn Tietoturva, tietosuoja ja varautuminen -asiantuntijaryhmän yhteistyössä VAHTIn kanssa toteuttamien yhteishankkeiden tukeminen
- Muiden digitaalisen turvallisuuden ja jatkuvuuden hallintaa edistävien toimenpiteiden toteuttaminen.

2.2.3 Digitaalinen turvallisuus on sisäänrakennettu kaikkeen uuteen toimintaan

Turvallisuus kehittämisessä -asiantuntijaryhmä

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

Vuoden 2017 tehtävät:

- VAHTI 3/2017 Sähköisen asioinnin tietoturvallisuus -ohjeen toimeenpano (julkaisu 5-6/2017)
- Muiden digitaalisen turvallisuuden kehittämistä edistävien toimenpiteiden toteuttaminen.

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

Turvallisuuden ylläpito -asiantuntijaryhmä

Turvallisuuden ylläpito -asiantuntijaryhmän työ käsittää päivittäiset ja jatkuvat toimet, joilla varmistetaan turvallisuusjärjestelyjen asianmukainen toiminta ja ylläpito. Työssä selvitetään lisäksi keinoja hyödyntää tieto- ja kyberturvallisuutta, tietosuojaa edistävien, esimerkiksi keinoälyä hyödyntävien uusien palveluiden hyödyntämistä 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 sekä sen hyödyntämistä perinteisten tietoturvapalveluiden ja -auditointien tukena
- Muiden digitaalisen turvallisuuden ylläpitoa edistävien toimenpiteiden toteuttaminen.

2.2.5 Julkisen hallinnon digitaalisen turvallisuuden mittaaminen sekä kokonaiskuvan raportointi tapahtuu tarkoituksenmukaisesti

Seuranta ja arviointi -asiantuntijaryhmä

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
- Digitaalisen turvallisuuden mittariston kehittäminen julkisen hallinnon tarpeisiin
- Muiden digitaalisen turvallisuuden seurantaa ja arviointia edistävien toimenpiteiden toteuttaminen.

2.3 Kyberturvallisuusstrategian toimeenpano-ohjelman toteuttaminen v. 2017–2020

Aikataulu: Toimeenpano-ohjelman hyväksymispäivämäärä 10.4.2017 vuosille 2017-2020

VAHTI osallistuu aktiivisesti Suomen Kyberturvallisuusstrategian vuosien 2017–2020 toimeenpano-ohjelman toteuttamiseen. Käytännössä kaikki VAHTIn julkisen hallinnon digitaalista turvallisuutta edistävä toiminta voidaan katsoa myös kyberturvallisuutta edistä-

väksi 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.

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

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

Tämä tapahtuu esimerkiksi seuraavilla toimenpiteillä:

- Tässä toimintasuunnitelmassa ja toimeenpano-ohjelmassa kuvattujen toimenpiteiden laadukkaalla toteuttamisella parannetaan sekä julkisen hallinnon organisaatioiden tieto- ja kyberturvallisuuden tasoa että niissä työskentelevien asiantuntijoiden osaamista
- VAHTI toteuttaa vuosittain kesäseminaarin ja VAHTI-päivän, jotka toimivat samalla myös henkilöstön koulutus- ja kehittämistilaisuuksina
- Lainsäädännön toimeenpanon yhteydessä rakennetaan tieto- ja kyberturvallisuushenkilöstölle oma koulutusohjelma, jossa huomioidaan heidän keskeinen roolinsa toimeenpanon sujuvassa toteuttamisessa
- VAHTI viestii toiminnastaan usealla eri tasolla, yksi kohderyhmistä on organisaatioiden tieto- ja kyberturvallisuusasiantuntijat.

2.4 Laajojen tieto- ja kyberturvahäiriötilanteiden hallinnan kehittäminen

Aikataulu: 1.6.2017–31.12.2019

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.

2.5 Valtioneuvoston periaatepäätös digitaalisen turvallisuuden kehittämisestä julkisessa hallinnossa

Aikataulu: 1.9.2017–31.12.2018

Julkaisu 7/2009 Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä määrittää tietoturvallisuuden

- lähtökohdat,
- tavoitteet,
- kehittämisen periaatteet,
- kohteet,
- painopisteet,
- toimeenpanon,
- resurssit sekä
- tietoturvallisuuden raportoinnin ja valvonnan toteuttamisen.

VAHTI on toteuttanut periaatepäätöstä edellisten toimikausien aikana menestyksekkäästi.

Uuden valtioneuvoston periaatepäätöksen laatimista edellyttävät

- toimintaympäristön ja käynnissä oleva toiminnan muutos erilaisiin uusiin teknologioihin perustuviin uudenlaisiin prosesseihin ja palveluihin
- perustavanlaatuinen muutos julkisen hallinnon toimintaa uhkaavissa tekijöissä sekä

- toimikaudelle 2017-2019 asetettu uusi VAHTI julkisen hallinnon digitaalisen turvallisuuden johtoryhmä.

Periaatepäätöksen päivittämisestä vastaa tätä varten perustettava erillinen ryhmä.

2.5.1 Digitaalisen turvallisuuden kehittämisohjelma

Aikataulu: x.x.2019–31.12.2022

Kun uusi Valtioneuvoston periaatepäätös digitaalisen turvallisuuden kehittämisestä on saatu voimaan, sen toteuttaminen ja toimeenpano edellyttävät omaa kehittämisohjelmaa. Se voidaan käynnistää osana käynnissä olevaa VAHTI-toimikautta ja sovittaa vuoden 2019 toimintasuunnitelmaan. Periaatepäätöksen toimeenpanoa tulee jatkaa seuraavan VAHTI-toimikauden 2020–2022 aikana.

Tuleva Valtioneuvoston periaatepäätös tukee myös tietoturvasäädösten uudistamista työn aikataulun ja siirtymäkauden rajoissa. Kehittämisohjelman laatiminen voidaan käynnistää loppuvuodesta 2018 osana periaatepäätöksen valmistelua ja sen hyväksynnän viimeistelyä.

2.6 JUHTA-yhteistyö

Julkisen hallinnon tietohallinnon neuvottelukunnan (JUHTA) alaisuuteen on perustettu tietoturvan, tietosuojan ja varautumisen asiantuntijaryhmä. 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.

2.6.1 Tietosuojakoulutuksen toteuttaminen

Aikataulu: 1.2.2017–31.12.2018

Tietosuojan verkkokoulutus jakaantuu kahteen osioon. Nämä ovat ”Arjen tietosuoja - tietosuojan perusteet kaikille” ja ”Työpaikan tietosuoja - tietosuojaa henkilötietoja käsitteleville”. Molempien osuuksien jälkeen on mahdollista suorittaa erillinen nettitesti.

2.6.2 Tietosuojan osoitusvelvollisuuden toteuttamisen yhteishanke

Aikataulu: 1.4.2017–31.12.2018

JUHTA-yhteistyön toinen merkittävä tietosuojaan liittyvä kokonaisuus on 18 työpajaa käsittävä 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.

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.

VAHTI on julkaissut seuraavat ohjeet:

VAHTI 2/2016 Toiminnan jatkuvuuden hallinta -ohje sekä siihen liittyvän toiminnan jatkuvuuden vaikutusarviotyökalun (BIA, *business impact analysis* -työkalu)

VM 8/2017 Tietoturvapoikkeamatilanteiden hallinta

VM x/2017 Ohje riskienhallintaan

- ohjeessa luodaan prosessi riskienhallinnan toteuttamiseksi julkiseen hallintoon

Osana tietosuojan yhteishanketta jalkautetaan näissä ohjeissa olevat parhaat käytännöt ja toimintamallit siten, että organisaatioissa riskienhallinta saadaan toiminnan edellyttämälle tasolle sekä varmistettua organisaation toiminnan jatkuvuuteen liittyvän suunnittelun, suunnitelmien ja prosessien toimivuus. Samassa yhteydessä varmistetaan tietoturvapoikkeamatilanteiden hallinta ja tietosuojaloukkausten hallintaan tarvittavien prosessien toiminta sekä mahdollistetaan organisaation osallistuminen julkisen hallinnon häiriötilanteiden hallintaan osana VIRT-toimintaa. Edellä mainitut ohjeet auttavat organisaatioita myös tietosuojan osoitusvelvollisuuden tietoturvavaatimusten toteuttamisessa.

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

ISSN 1797-9714 (PDF)
ISBN 978-952-251-860-6 (PDF)
ISSN 1459-3394 (nid.)
ISBN 978-952-251-859-0 (nid.)

Toukokuu 2017