VALTIOVARAINMINISTERIÖ

VAHTIn toimintasuunnitelma vuosille 2018–2019

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä

Valtiovarainministeriön julkaisu – 12/2018

Julkisen hallinnon ICT

Valtiovarainministeriön julkaisu 12/2018

VAHTI

Toimintasuunnitelma vuosille 2018–2019

Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä

Valtiovarainministeriö, Helsinki 2018

Valtiovarainministeriö

ISBN: 978-952-251-941-2 (PDF)

Taitto: Valtioneuvoston hallintoyksikkö, Julkaisutuotanto

Helsinki 2018

Kuvailulehti

Julkaisija	Valtiovarainministeriö		4.4.2018
Tekijät	Kimmo Rousku (toimittaja)		
Julkaisun nimi	Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä; Toimintasuunnitelma vuosille 2018–2019		
Julkaisusarjan nimi ja numero	Valtiovarainministeriön julkaisu 12/2018		
Teema	Julkisen hallinnon ICT		
ISBN PDF	978-952-251-941-2	**ISSN PDF**	1797-9714
URN-osoite	http://urn.fi/URN:ISBN:978-952-251-941-2		
Sivumäärä	36	**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 VAHTI jatkaa yli kaksikymmentä vuotta jatkunutta 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 vastaavati toteutetaan osana uutta tiedonhallintalakia. Tähän liittyy keskeisesti myös uusien lainsäädäntöön perustuvien vaatimusten toteuttaminen (”VAHTI 100-vaatimukset”) sekä niiden julkaiseminen uudistetussa VAHTI-portaalissa.

Vuoden 2018 osalta tärkein toimenpide koskee julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman laatimista sekä siihen liittyvän toimenpideohjelman käynnistämistä. Tämän kehittämisohjelman avulla kehitetään kolmea osa-aluetta, jotka koskevat johtamista ja riskienhallintaa, osaavaa henkilöstöä sekä digitaalisen turvallisuuden kehittämistä hyödyntämällä digitalisaatiota apuna myös turvallisuuden kehittämisessä.

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, joita jatketaan vuoden 2018 loppuun saakka.

Lisäksi VAHTI kehittää toimikauden aikana digitaalisen turvallisuuden kokonaiskuvan raportointia ja mittaamista organisaatio- ja henkilöstötasolla.

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

Presentationsblad

Utgivare	Finansministeriet		4.4.2018
Författare	Kimmo Rousku (redaktör)		
Publikationens titel	Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä; Toimintasuunnitelma vuosille 2018–2019 (Ledningsgruppen för informations- och cybersäkerheten inom statsförvaltningen; Verksamhetsplan för åren 2018–2019)		
Publikationsseriens namn och nummer	Finansministeriets publikationer 12/2018		
Tema	Offentliga förvaltningens ICT		
ISBN PDF	978-952-251-941-2	**ISSN PDF**	1797-9714
URN-adress	http://urn.fi/URN:ISBN:978-952-251-941-2		
Sidantal	36	**Språk**	Finska
Nyckelord	VAHTI, digital säkerhet, informationssäkerhet, cybersäkerhet, datasekretess		

Referat

Finansministeriet ansvarar för den allmänna utvecklingen av informationssäkerheten inom den offentliga förvaltningen och för styrningen av informationssäkerheten inom statsförvaltningen. Finansministeriets behörighet inom styrning och utveckling av informationssäkerheten och informationsförvaltningen bygger på flera lagar, författningar och förordningar. Finansministeriet har tillsatt ledningsgruppen för informations- och cybersäkerheten inom statsförvaltningen (VAHTI) som samarbets-, beredning- och koordineringsorgan för de organisationer som ansvarar 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 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 ska uppnå de mål som fastställts för gruppen.

Det viktigaste utvecklingsobjektet för åren 2017–2019 är reformen av informationssäkerhetsförordningen som trädde i kraft 2010 som ett led i förnyelsen och genomförandet av informationssäkerhetsförfattningarna, vilket på motsvarande sätt genomförs som ett led i den nya lagen om styrning av informationsförvaltningen. Detta är även centralt förknippat med genomförande av de krav som bygger på den nya lagstiftningen (”VAHTI 100-kraven”) samt publicering av dessa i den förnyade VAHTI-portalen.

Den viktigaste åtgärden 2018 är ett utvecklingsprogram som ska utarbetas för den digitala säkerheten inom den offentliga förvaltningen samt det relaterade åtgärdsprogrammet som ska initieras. I utvecklingsprogrammet ingår tre delområden som rör ledning och riskhantering, kompetent personal samt utveckling av den digitala säkerheten genom att man utnyttjar digitalisering även för säkerhetsutvecklandet.

Den tredje centrala åtgärden gäller utvecklingen av dataskyddet inom den offentliga förvaltningen. Detta sker i form av dataskyddsutbildningar som genomförs i samarbete med delegationen för informationsförvaltningen inom den offentliga förvaltningen (JUHTA) samt ett samprojekt kring skyldigheten till påvisande i dataskyddsförordningen. Projekten fortgår till slutet av 2018.

Därtill utvecklar VAHTI under sitt mandat rapporteringen och mätningen av en helhetsbild över den digitala säkerheten på organisations- och personalnivå.

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

Description sheet

Published by	Ministry of Finance		4.4.2018
Authors	Kimmo Rousku (toimittaja)		
Title of publication	Julkisen hallinnon digitaalisen turvallisuuden johtoryhmä; Toimintasuunnitelma vuosille 2018–2019		
Series and publication number	Ministry of Finance publications 12/2018		
Subject	Public Sector ICT		
ISBN PDF	978-952-251-941-2	**ISSN (PDF)**	1797-9714
Website address (URN)	http://urn.fi/URN:ISBN: 978-952-251-941-2		
Pages	36	**Language**	Finnish
Keywords	Digital security, information security, cyber security, data protection		

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. The Government Information 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 action plan describes the projects and the ways in which VAHTI will develop and further these activities to meet the set objectives.

The main development work between 2017 and 2019 is to make amendments to the Information Security Decree, which entered into force in 2010. This work is part of the reform and implementation of information security statutes, which is being carried out in connection with the drafting of the new information management legislation. Implementing the statutory requirements ("VAHTI 100 requirements") and their publication in the updated VAHTI portal are an essential part of this work.

Secondly, in 2018, the main focus is on preparing a development programme for digital security in public administration and on launching a related programme of measures. The development programme will be used to improve the following three sectors: leadership and risk management; competent personnel; and development of digital security, including enhancing security using digitalisation.

Thirdly, VAHTI will develop data protection in public administration. This will be done by organising data protection courses together with the Advisory Committee for Information Management in Public Administration (JUHTA) and taking advantage of a joint project related to accountability, set in the data protection decree, which will continue until the end of 2018.

In addition, VAHTI will improve reporting and measurement related to overall digital security at the level of organisations and personnel.

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

Sisältö

1 VAHTIn toiminnan lähtökohdat

Tarkoituksenmukaisesti toteutettu tieto- ja kyberturvallisuus, laajemmin käsitettynä digitaalinen turvallisuus, on yksi yhteiskunnan toiminnan perusedellytyksistä. Tässä julkisen hallinnon tuottamilla palveluilla on merkittävä rooli. Toiminnan kehittäminen painottuu julkisessa hallinnossa yhä enemmän toiminnan digitalisoimiseen, automatisoimiseen, 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).

Edellä mainitun johdosta perinteinen tietoturvallisuus keskittyy ensisijaisesti tiedon saatavuuden, eheyden ja salassa pidettävän tiedon osalta sen luottamuksellisuuden varmistamiseen. Pelkkä tietoturvallisuuden perinteinen näkökulma on liian kapea-alainen näkökulma toimintaympäristössä tapahtuneeseen muutokseen. Tämän vuoksi uudelleen organisoitu VAHTI-toiminta tähtää aiempaa laaja-alaisempaan digitaalisen toimintaympäristön toiminnan turvaamiseen, jossa keskeisessä roolissa ovat riskienhallinta, tieto- ja kyberturvallisuus sekä toiminnan jatkuvuuden takaaminen.

Edellisten rinnalle on vahvasti noussut henkilötietojen käsittelyn, käytännössä tietosuojan tärkeys ja merkitys. Toukokuussa 2018 sovellettavaksi tuleva EU:n yleinen tietosuoja-asetus sekä muu kansallinen, siihen liittyvä tietosuojalainsäädäntö luovat uusia mahdollisuuksia hyödyntää ja käsitellä henkilötietoja niin rekisterinpitäjille, henkilötietojen käsittelijöille kuin rekisteröidyille. Tietosuoja tulee siten nähdä samanlaisena mahdollisuutena, mitä digitaalinen turvallisuus on. Vastaavasti sen toteuttaminen edellyttää uusien toimintamallien ja prosessien kehittämistä myös tietoturvallisuus-näkökulmasta, esimerkiksi henkilötietojen tietoturvaloukkausten osalta. Tietoturvallisuus on siten keskeisessä roolissa tietosuojan toteuttajana.

Valtiovarainministeriön tehtävänä on julkisen hallinnon tietoturvallisuuden yleinen kehittäminen ja valtionhallinnon tietoturvallisuuden ohjaus. Valtiovarainministeriön toimivalta tietoturvallisuuden ja tietohallinnon ohjauksessa sekä kehittämisessä perustuu useisiin

säädöksiin. 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 ohjauksesta sekä tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjauksesta ja valvonnasta. Valtiovarainministeriön vastuulla on laissa määritelty valtion yhteisten tieto- ja viestintäteknisten palvelujen järjestämisestä tarkoitettujen yhteisten palvelujen palvelutuotannon yleishallinnollinen, strateginen sekä tieto- ja viestintäteknisen varautumisen, valmiuden ja turvallisuuden ohjaus. Edellisten 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 vuosien 2017 – 2020 toteuttamisessa.

VAHTI edistää myös julkishallinnon toiminnan digitalisaatiota huolehtimalla digitaalisen turvallisuuden vaatimuskehikon laatimisesta ja ylläpitämisestä. Tähän kuuluvat myös turvallisuuteen sekä ICT-toiminnan jatkuvuuteen liittyvät tarkastukset, hyväksynnät ja arvioinnit sekä tieto- ja kyberturvallisuusharjoitustoiminnan edistäminen.

Valtiovarainministeriö vahvistaa ja kehittää VAHTIn toimintaa ja sen tuloksellisuutta, jotta tuleviin uusiin digitaalisen toimintaympäristön haasteisiin pystytään paremmin vastaamaan. Vuoden 2018 osalta tämä on tapahtunut siirtämällä valtiovarainministeriöstä VAHTIn operatiivinen toiminta, Viestintäviraston Kyberturvallisuuskeskuksen kanssa tehtävä yhteistyö koskien GovCERT-palveluiden kehittämistä sekä harjoitustoiminnan kehittäminen 1.1.2018 alkaen Väestörekisterikeskukseen (VRK). Samalla VAHTI-toimintaa on vahvistettu lisähenkilöresursseilla. Lisäksi 1.1.2018 on siirretty aikaisemmin Valtion tieto- ja viestintätekniikkakeskus (Valtori) vastuulla olleet ulkopuolisten toimittajien tuottamat tietoturvallisuuden asiantuntijapalvelut myös VRK:lle.

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
- parantaa toiminnan laatua ja riskienhallintaa.

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

Kehittämällä julkisen hallinnon ja valtionhallinnon digitaalista turvallisuutta sekä näihin 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 sekä muut tieto- ja kyberturvallisuuden linjaukset
3. Edistää julkisen hallinnon tietoturvakulttuuria ja henkilöstön tietoturvatietoisuutta
4. Edesauttaa tietosuojan toteutumista osana digitaalisen turvallisuuden kehittämistä

5. Toteuttaa digitaalista turvallisuutta koskevia kyselyitä ja barometrejä sekä julkaisee näistä raportteja sekä havainnoista koostettuja kehittämissuunnitelmia
6. Mittaa, kokoaa ja ylläpitää kokonaiskuvaa julkisenhallinnon digitaalisen turvallisuuden tilanteesta sekä raportoi tästä 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.

1b Principerna för VAHTI:s verksamhet

Ändamålsenlig informations- och cybersäkerhet, i en vidare bemärkelse digital säkerhet, är en grundläggande förutsättning för att samhället ska fungera. Här spelar de offentliga tjänsterna en viktig roll. Digitalisering, automatisering samt utnyttjande av robotteknik och artificiell intelligens intar 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 sätt med hjälp av Big data. Medborgarna producerar och administrerar i allt större omfattning information som gäller dem själva tack vare MyData-modellen.

Med anledning av detta fokuserar den traditionella datasäkerheten i fråga om informationens tillgänglighet, integritet och sekretess främst på att trygga dess sekretess. Den traditionella uppfattningen med fokus på enbart datasäkerheten utgör ett alltför snävt perspektiv på förändringarna i verksamhetsmiljön. 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.

Utöver de ovan nämnda aspekterna har behandlingen av personuppgifterna framhållits eftertryckligt, vilket i praktiken avser vikten och innebörden av dataskydd. EU:s allmänna dataskyddsförordning, som träder i kraft i maj 2018, liksom även övrig nationell relaterad dataskyddslagstiftning, ger upphov till nya möjligheter för såväl registeransvariga som registerförare och de registrerade att utnyttja och behandla personuppgifter. Dataskyddet ska således betraktas som en möjlighet lik den digitala säkerheten. Dess genomförande kräver på motsvarande sätt nya verksamhetsmodeller och processutveckling som även beaktar datasäkerheten, exempelvis i fråga om säkerhetsöverträdelser för personuppgifter. Datasäkerheten intar därmed en central roll för genomförandet av dataskyddet.

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 informationssäker-

heten och informationsförvaltningen bygger på flera författningar. Till dessa hör 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) och statsrådets förordning om finansministeriet (610/2003).

Finansministeriet ansvarar för den allmänna administrativa, strategiska och ekonomiska styrningen och tillsynen liksom även för styrningen av och tillsynen över den informations- och kommunikationstekniska beredskapen och säkerheten. Finansministeriet ansvarar även 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 den elektroniska ärendehanteringen.

Finansministeriet har tillsatt VAHTI som samarbets-, berednings- och koordineringsorgan för de organisationer som ansvarar för utvecklandet och styrningen av den digitala säkerheten inom den offentliga förvaltningen. VAHTI:s ställning har fastställts i statsrådets principbeslut om Finlands cybersäkerhetsstrategi från 2013 och om utvecklandet av informationssäkerheten inom statsförvaltningen från 2009. VAHTI spelar dessutom en central roll i genomförandet av verkställighetsprogrammet för cybersäkerhetsstrategin för åren 2017–2020.

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.

Finansministeriet förstärker och utvecklar VAHTI:s verksamhet och dess effektivitet så att man ska kunna svara mot nya utmaningar inom den digitala verksamhetsomgivningen. År 2018 sker detta genom att VAHTI:s operativa verksamhet överförs från finansministeriet, samarbetet med Cybersäkerhetscentret vid Kommunikationsverket kring GovCERT-tjänsterna utvecklas samt att övningsverksamheten från och med den 1 januari 2018 utvecklas i Befolkningsregistercentralen (BRC). Samtidigt har VAHTI-verksamheten stärkts med ytterligare personal. Dessutom har också experttjänsterna inom datasäkerhet, vilka tidigare ankommit på Statens center för informations- och kommunikationsteknik (Valtori), den 1 januari 2018 överförts på BRC.

1.1b VAHTI:s mål

VAHTI stöder finansministeriet vid beredningen av beslut och beslutsfattandet i fråga om 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 av sekretessbelagda uppgifter,
- tillgången till och integriteten i informationen och verksamheten,
- kontinuiteten i verksamheten och beredskap inför störningssituationer och
- förbättring av verksamhetens kvalitet och riskhanteringen.

VAHTI främjar även att dessa frågor görs till en elementär del av verksamheten, ledarskapet och resultatstyrningen samt att informationssystemen, datanäten och informations- och kommunikationstekniska tjänster produceras, utvecklas, underhålls och utnyttjas.

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

1.2b VAHTI:s uppgifter

VAHTI är ett samarbetsorgan för styrning och utvecklande 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 lägesbild över den digitala säkerheten inom den offentliga förvaltningen och rapporterar om det till finansministeriet
7. styr, bereder, samordnar och verkställer utvecklingsprogram och projekt som relaterar till den digitala säkerheten inom den offentliga förvaltningen
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.

1c Current state of VAHTI's tasks

Expediently implemented information and cyber security – digital security in the broader context – is one of the fundamental preconditions for a well-functioning society. In this work, the services provided by the public administration play a significant role. Today, developing operations in public administration focuses on digitalisation and automation, and robotics and artificial intelligence. Furthermore, data collected from various sensors in IoT devices can be enhanced and elaborated in new ways using Big Data. Citizens are increasingly processing and managing their personal data using the MyData (Omatieto) approach.

For this reason, conventional information security concentrates primarily on ensuring the integrity and availability of data and, as concerns secret information, on ensuring its confidentiality. Because of the changes in the operating environment, the traditional perspective of information security is too narrow. The reorganised VAHTI activities aim at safeguarding a more comprehensive operational security in the digital operating environment, where the key elements are risk management, information and cyber security, and ensuring the continuity of operations.

By the side of these, the importance and significance of processing personal data, which in practice means data protection, have gained a strong position. The General Data Protection Regulation of the EU (2016/679), which becomes applicable in May 2018, and other related national data protection legislation will create new opportunities for controllers, personal data processing officials and clients using and handling personal data. Data protection should therefore be considered a similar opportunity to that created by digital security. New models of operation and improved processes are necessary also from the point of view of information security, for example concerning violations of information security related to personal data. Therefore, information security plays a central role in the implementation of data protection.

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.

These include the Act on Information Management Governance in Public Administration (634/2011), the Act on the Assessment of the Information Security of Public Authorities' Information Systems and Telecommunications Arrangements (1406/2011), the Emergency Powers Act (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 administrative, strategic and financial steering of security network activities, as well as for the steering and monitoring of preparedness, readiness and security of information and communications technology. In accordance with the Act on the Provision of Shared Government Information and Communications Technology Services, the Ministry of Finance is responsible for the steering of general administration and strategic governance of shared service production, as well as for related preparedness, readiness and security concerning information and communications technology. In addition, the Ministry of Finance is responsible for the Act on Common Administrative e-Service Support Services.

The Government Information 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. VAHTI's mandate is recorded in the current government resolutions on Finland's cyber security strategy (2013) and on the development of data security in state administration (2009). Additionally, VAHTI plays a central role in implementing the Cyber Security Strategy 2017–2020.

VAHTI promotes the digitalisation of activities in the public administration by taking care of the preparation and maintenance of the framework of requirements of digital security. This includes audits, certifications and evaluations related to security and the continuity of ICT operations, as well as the promotion of data and cyber security exercises.

The Ministry of Finance strengthens and develops the operations and effectiveness of VAHTI, so that new challenges in the digital operating environment can be met. The operative functions of VAHTI, the cooperation related to the development of GovCERT services conducted with the National Cyber Security Centre at the Finnish Communications Regulatory Authority (FICORA), and the development exercises were transferred under the authority of the Population Register Centre on 1 January 2018. More personnel have also been recruited to VAHTI. On 1 January 2018, outsourced specialist data security services, previously provided by the Government ICT Centre Valtori, were also transferred to the Population Register Centre.

1.1c VAHTI 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, which enables

- the digitalisation and robotisation of public administration
- operational reliability
- the confidentiality of secret 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 also promotes the integration of these into the operations, management and performance steering of administration. Furthermore, VAHTI advances the development, maintenance, use and service production of information systems, information networks and data and communications services.

By developing the digital security of public administration and state administration, and related cooperation, VAHTI supports the implementation of the Government Programme, the Security Strategy for Society, Finland's Cyber Security Strategy, the government resolution on the development of data security in state administration, and other central policies of the Government and the Ministry of Finance.

1.2c VAHTI tasks

VAHTI is a body that steers, develops and cooperates in matters related to digital security in public administration. VAHTI

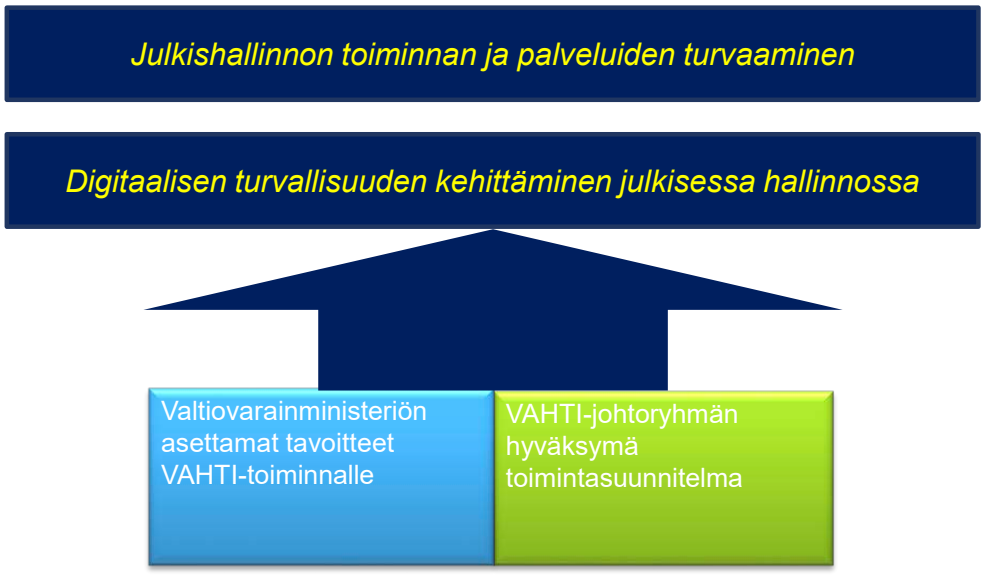
1. prepares and coordinates the policies of the Ministry of Finance concerning digital security in public administration, and monitors and supports their implementation
2. processes the statutes, guidelines, recommendations and other information and cyber security policies related to digital security 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. conducts surveys and barometers to assess digital security and publishes reports and development plans based on the observations
6. makes reviews and assembles material and maintains an overall picture of the state of digital security in public administration, and submits its reports to the Ministry of Finance
7. steers, prepares and coordinates 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 coordinates international data security cooperation policies and advocacy work of the public administration in international data security forums.

2 Julkisen hallinnon digitaalisen turvallisuuden kehittämisen osa-alueet 2018–2019

Valtiovarainministeriö on asettanut edellisessä luvussa kuvatut tavoitteet ja tehtävät VAHTIlle. Näitä toteutetaan tämän toimintasuunnitelman avulla, jonka tehtävänä on digitaalisen turvallisuuden kehittäminen julkisessa hallinnossa.

Tämä vaikuttaa siten, että voimme paremmin turvata näillä toimenpiteillä julkisen hallinnon toimintaa ja palveluita sekä siten ylläpitää ja vahvistaa kansalaisten, asiakkaiden ja muiden sidosryhmien luottamusta julkisen hallinnon toimintaan.



Kuva 1. VAHTI-toiminnan tavoitteena on varmistaa julkisen hallinnon toiminnan ja palveluiden turvallisuus digitaalisen turvallisuuden eri osa-alueiden avulla sekä myös niitä kehittämällä.

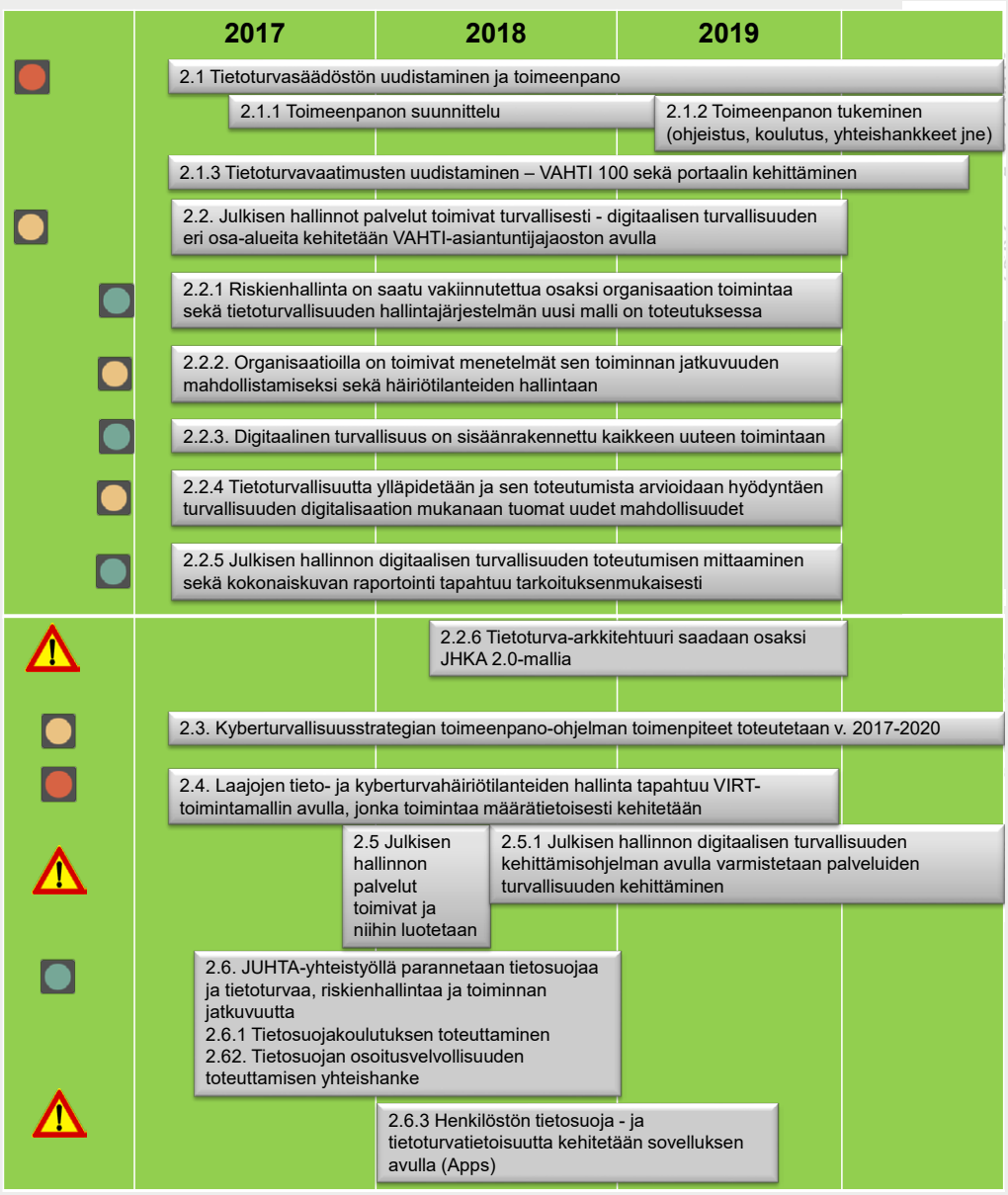
Kehittäminen tapahtuu seuraavien digitaalisen turvallisuuden osa-alueiden avulla

- riskienhallinta
- tietoturvallisuus
- kyberturvallisuus
- toiminnan jatkuvuus
- tietosuoja
- johtaminen

Osa-alueita varten ei ole luotu yksittäisiä kehittämistoimenpiteitä vaan ne ovat osana usein useammassa kehittämisen osa-alueessa. Esimerkiksi JUHTA/VAHTI yhteishankkeissa kehitetään kaikkia edellä mainittuja osa-alueita.

VAHTI kehittää julkisen hallinnon digitaalista turvallisuutta tässä luvussa kuvattujen toimenpiteiden avulla. Toimenpiteillä huolehditaan myös edellä kuvattujen yhdeksän tehtävän toteuttamisesta.

Kuva 2. VAHTIn operatiivista toimintaan voidaan kuvata viiden keskeisen osa-alueen kautta. Jokaiselle osa-alueella on valittu muutama toimenpide, joiden avulla kehittämistä toteutetaan.



Kuva 3. VAHTIn keskeiset toimenpiteet digitaalisen turvallisuuden kehittämiseksi vuosille 2017–2019. Vuoden 2017 osalta tavoitteiden saavuttamista on kuvattu liikennevaloilla (vihreä, keltainen, punainen) sekä vuoden 2018 uusien toimenpiteiden osalta huutomerkillä. Yksityiskohtaisemmin tavoitteiden toteutumista on esitelty valtiovarainministeriön julkaisussa 16/2018 VAHTIn toimintakertomus vuodelta 2017.

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

2.1 Tietoturvasäädösten uusiminen ja toimeenpano

Aikataulu: 1.1.2017–31.12.2019

Valtiovarainministeriön asettama Tietoturvallisuuden säädöstön valmistelun ohjausryhmän toimikausi 11.4.2016–28.2.2017 toteutti sille asettamisessa määritetyt tehtävät. Ne koostuivat tietoturva-asetuksen soveltamisen nykytilan kuvauksesta valtionhallinnossa, tietoturva-asetuksen soveltamisen nykytilan haasteiden kuvauksesta ja kehittämistarpeista julkisessa hallinnossa. Lisäksi toteutettiin tietoturvasäädösten vertailu keskeisissä EU-maissa, tietoturvatutkimustiedon hankkimista tavoitetilan pohjaksi Suomesta, tietoturvasäännöstön kehittämisen tavoitetilan kuvaus Suomessa mukaan lukien suhde kybertoimintaympäristön turvallisuuteen sekä tavoitetilan taloudellisen vaikuttavuuden kuvaus.

Valtiovarainministeriö asetti 17.11.2016 julkisen hallinnon tiedonhallinnan sääntelyn kehittämistä selvittävän työryhmän toimikaudeksi 17.11.2016–15.9.2017. Työryhmä selvitti julkisen hallinnon tiedonhallinnan lainsäädännön kehittämistarpeita ja julkaisi kehittämislinjauksia koskevan raporttinsa (Valtiovarainministeriön julkaisuja 37/2017.pdf). Työryhmä näki kehittämislinjauksia käsittelevässä raportissaan tarpeellisena, että tiedonhallinnan sääntelyn kehittämiseksi ryhdyttäisiin valmistelemaan yleislakia julkisen hallinnon tiedonhallinnasta. Valtiovarainministeriö on asettanut julkisen hallinnon tiedonhallintalain valmistelemiseksi sekä valmistelun tueksi ohjausryhmän ajalle 10.1.2018 – 31.9.2018. Valmistelutyö sisältää myös julkisen hallinnon tietoturvallisuusvaatimukset.

Tämä edellyttää tulevan lainsäädännön toimeenpanon suunnittelua ja lainsäädännön toimeenpanoa, erityisesti sen soveltamisen koskiessa nykyistä tietoturvallisuusasetusta (681/2010) laajempaa kohdejoukkoa, koko julkista hallintoa.

2.1.1 Toimeenpanon suunnittelu

Aikataulu:1.5.2017–1.4.2019

Suunnitteluvaiheessa laaditaan toimenpidesuunnitelma lainsäädännön toimeenpanon toteuttamiseksi alkaen vuodesta 2018 lain siirtymäkauden ajalle. Toimeenpanon suunnittelussa hyödynnetään VAHTIn kokemuksia lukuisista vuoden 2010 tietoturvallisuusasetuksen toimeenpanon yhteishankkeista, koulutuksista sekä tietoturvasäädösten nykytilaselvi-

tyksen haastatteluissa kerätyistä palautteista. Tämän ohella hyödynnetään vuosien 2017-2018 oppeja koskien tietosuoja-asetuksen JUHTA/VAHTI-yhteishankkeita.

Keskeistä on suunnitella, laatia tarvittavat ohjeet, materiaalit ja koulutukset eri kohderyhmille sekä toteuttaa 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
- vähimmäistason ylittävältä osalta ehdotuksia riskienarvion perusteella valittavista lisäkontrolleista tarvittavan vähimmäistason ylittävän turvallisuuden takaamiseksi

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 muu ulkopuolinen taho voi toteuttaa tarvitsemansa arvioinnin.

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

2.2 Julkisen hallinnot palvelut toimivat turvallisesti - digitaalisen turvallisuuden eri osa-alueita kehitetään 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 2018 kaikkien asiantuntijaryhmien keskeisin tehtävä liittyy VAHTI 100 vaatimuskokonaisuuden kehittämiseen sekä siihen liittyvän VAHTI-portaalin kehittämiseen. 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 sekä tietoturvallisuuden hallintajärjestelmän uusi malli on toteutuksessa

1 Johtaminen ja riskienhallinta -asiantuntijaryhmä (JORI)

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

Asiantuntijaryhmän tehtävänä on edistää keinoja, joilla luodaan organisaation perusvalmiudet, kuten menettely tunnistaa suojattavat kohteet. Tehtäviin kuuluu myös huolehtia tietoturvallisuuden hallintajärjestelmän toteuttamisen, henkilöstön tietoturvatietoisuuden ja osaamisen sekä kokonaisuuden johtamisen ohjeistamisesta. Lisäksi ryhmä vastaa riskienhallinnan ohjeistusten kehittämisestä ja riskienhallinnan VAHTI-ohjeen ja prosessin jalkauttamisesta sekä jatkokehittämisestä.

Vuoden 2018 tehtävät:

- VAHTI-ohje riskienhallinnasta prosessin jalkauttaminen ja toimeenpano, riskienhallintaseminaarin ja ohjeen toteuttaminen
- Käynnistää osana uuden lainsäädännön toimeenpanon suunnittelua tietoturvallisuuden hallintajärjestelmä-mallin 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 vuoden 2018 työpajojen osalta
- Digitaalisen turvallisuuden tietoisuuden kasvattaminen osana vuosittain lokakuussa toteutettavaa European Cyber Security Month -kuukautta, käytännössä vuosittaisen julkisen hallinnon digitaalisen turvallisuuden teemaviikon avulla 8-12.10.2018
- Muiden digitaalisen turvallisuuden johtamista ja riskienhallintaa edistävien toimenpiteiden toteuttaminen.

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

2 Toiminnan jatkuvuuden hallinta -asiantuntijaryhmä (TOJA)

Puheenjohtaja 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 2018 tehtävät:

- VAHTI 2/2016 Toiminnan jatkuvuuden ohje ja sen yhteydessä laaditun BIA-vaikutusarviotyökalun tunnettavuuden ja hyödyntämisen lisääminen
  - edellisen perusteella laaditun palveluiden / prosessien arviointityökalun kommentointi ja kriitisyysarviointityökalun kehittäminen
- JUHTAn Tietoturva, tietosuoja ja varautuminen -asiantuntijaryhmän yhteistyössä VAHTIn kanssa toteuttaman Riskienhallinnan, toiminnan jatkuvuuden sekä tietoturvapoikkeamatilanteiden ja tietosuojaloukkausten hallinta -yhteishanke osana JUHTA/VAHTI-yhteishankkeita
  - yhteishankkeisiin liittyvän TAISTO-harjoituksen sisällöllinen kehittäminen yhteistyössä Viestintäviraston Kyberturvallisuuskeskuksen kanssa
- Muiden jatkuvuuden hallintaa edistävien toimenpiteiden toteuttaminen.

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 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 2018 tehtävät:

- tietoturvallisuuden liittäminen osaksi JHKA-kokonaisuutta, asetettavaan hankkeeseen osallistuminen
- hankintojen tietoturvaohjeen tukimateriaalien tuottaminen
- VAHTI 3/2017 Sähköisen asioinnin tietoturvallisuus -ohjeen toimeenpano
- (julkaisu 4-5/2017)
  - asian käsittely VAHTI-kesäseminaarissa
- Muiden digitaalisen turvallisuuden kehittämistä edistävien toimenpiteiden toteuttaminen ja tähän liittyvien linjausten kehittäminen

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

4 Turvallisuuden ylläpito-asiantuntijaryhmä (TUTO)

Puheenjohtaja Petri Puhakainen, valtioneuvoston kanslia ja 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 2018 tehtävät:

- 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.
  - yhteistyö Väestörekisterikeskuksen tuottamien tietoturvallisuuden asiantuntijapalveluiden kehittämisessä
- Muiden turvallisuuden ylläpitoa edistävien toimenpiteiden toteuttaminen.

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 2018 tehtävät:

- VAHTIn digitaalisen turvallisuuden kokonaiskuvaraportoinnin edelleen 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.

2.2.6 Tietoturva-arkkitehtuuri saadaan osaksi JHKA 2.0-mallia

Vuonna 2018 käynnistetään erillinen hanke, jonka tehtävänä on kehittää tarvittavia digitaaliseen turvallisuuteen liittyviä kuvauksia sekä muita malleja osaksi vuonna 2017 uudistettua JHKA-mallia. Hanke ja sen tavoitteet asetetaan erillisellä valtiovarainministeriön päätöksellä.

2.3 Kyberturvallisuusstrategian toimeenpano-ohjelman toimenpiteet toteutetaan v. 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.

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.

Tämä tapahtuu esimerkiksi seuraavilla toimenpiteillä:

- Tässä toimintasuunnitelmassa ja toimeenpano-ohjelmassa kuvattujen toimenpiteiden laadukkaalla ja laaja-alaisella 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
- VAHTI toteuttaa lokakuussa julkisen hallinnon digitaalisen turvallisuuden teemaviikon, joka on myös osa eurooppalaista kyberturvallisuuskuukautta (ECSM)
- 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 hallinta tapahtuu VIRT-toimintamallin avulla, jonka toimintaa määrätietoisesti kehitetään

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.

VIRT sekä muu Viestintäviraston Kyberturvallisuuskeskuksen GovCERT-palveluiden tuottamiseen liittyvä yhteistyö on siirretty Väestörekisterikeskukselle 1.1.2018 alkaen. VRK käynnistää yhteistyössä Kyberturvallisuuskeskuksen kanssa säännölliset VIRT-yhteistyöverkoston kokoukset ja toiminnan muun kehittämisen. Vuoden 2018 aikana toteutetaan 3-4 kpl yhteistilaisuuksia VIRT-toimijoille.

2.5 Julkisen hallinnon palvelut toimivat ja niihin luotetaan

Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman (JUDO) laatiminen

Aikataulu: 1.1.2018–30.6.2018

Kehittämisohjelman tavoitteena on varmistaa julkisen hallinnon palveluiden toimivuus ja luotettavuus sekä kehittää digitaalisen turvallisuuden osa-alueita toimintaympäristön muutoksia vastaavasti.

Toimintaympäristön muuttuminen, käynnissä oleva toiminnan muutos uusia teknologioita hyödyntäviin prosesseihin ja palveluihin, perustavanlaatuinen muutos julkisen hallinnon toimintaa uhkaavissa tekijöissä, uudet julkisen hallinnon ICT- ja digitaalisten palveluiden tuotantomallit sekä tähän liittyvä lainsäädäntö ja toimikaudelle 2017–2019 asetettu uusi julkisen hallinnon digitaalisen turvallisuuden johtoryhmä edellyttävät uuden kehittämisohjelman laatimista.

Kehittämisohjelma laaditaan kattamaan koko julkinen hallinto ja siihen päivitetään aikaisemmassa valtioneuvoston periaatepäätöksessä tietoturvallisuuden kehittämisessä olleet kehittämisen lähtökohdat, tavoitteet sekä periaatteet ja painopisteet vastaamaan toimintaympäristössä tapahtuneita muutoksia.

2.5.1 Julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelman avulla varmistetaan palveluiden turvallisuuden kehittäminen

Aikataulu: 1.7.2018–31.12.2021

Kun uusi julkisen hallinnon digitaalisen turvallisuuden kehittämisohjelma ja sitä tukeva toimeenpano-ohjelma on saatu voimaan, sen toteuttaminen edellyttää erillistä sovittujen toimenpiteiden toimeenpanoa. Kehittämisohjelman toimeenpanoa tulee jatkaa mahdollisen seuraavan VAHTI-toimikauden vuosien 2020–2022 aikana.

Valtiovarainministeriön toteuttamissa kyselyissä keskeisiksi kehittämistä vaativiksi osa-alueiksi on tunnistettu johtaminen ja riskienhallinta, henkilöstön tietoisuuden kasvattaminen erityisesti koulutusta kehittämällä sekä havainnointi- ja reagointikyvyn ja häiriönhallintatilanteiden kehittäminen.

2.6 JUHTA-yhteistyöllä parannetaan tietosuojaa ja tietoturvaa, riskienhallintaa ja toiminnan jatkuvuutta

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.

2.6.1 Tietosuojakoulutuksen toteuttaminen

Aikataulu: 1.2.2017–31.12.2018

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

2.6.2 Tietosuojan osoitusvelvollisuuden toteuttamisen yhteishanke

Aikataulu: 1.4.2017–31.12.2018

JUHTA-yhteistyön toinen merkittävä tietosuojaan liittyvä kokonaisuus on työpaja-mallinen 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 22/2017 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. Edellä mainitut ohjeet auttavat organisaatioita myös tietosuojan osoitusvelvollisuuden tietoturvavaatimusten toteuttamisessa.

Osana yhteishankkeiden toteutusta järjestetään marraskuussa 2018 siihen osallistuville organisaatioille mahdollisuus osallistua organisaatiokohtaiseen TAISTO-harjoitukseen, jonka avulla organisaatiot voivat harjoitella henkilötietojen tietoturvaloukkausten hallitsemiseen liittyviä toimintaprosesseja. Harjoituksen avulla voidaan varmistaa myös tieto- ja kyberturvallisuuden, toiminnan jatkuvuuden sekä tietosuojan näkökulmasta tarvittava kyvykkyys selviytyä erilaisista poikkeama- ja häiriötilanteista.

2.6.3 Henkilöstön tietosuoja - ja tietoturvatietoisuutta kehitetään sovelluksen avulla (Apps)

Aikataulu: 1.5.2018–31.12.2019

Valtiovarainministeriön toteuttamissa kyselyissä ja niiden perusteella laadituissa raporteissa on käynyt ilmi, että eräs keskeinen puute digitaalisen turvallisuuden osalta on aiheeseen liittyvän ohjeistamisen, sekä ennen kaikkea koulutuksen ja säännöllisen tiedottamisen osittainen puuttuminen. Tässä on havaittu myös selkeitä eroja eri organisaatioiden välillä.

Useat tutkimukset (mm. EU, kyberturvallisuustiedoksianto) ovat nostaneet esille henkilöstön merkittävän roolin tieto- ja kyberturvallisuuspoikkeamien aiheuttajana. Valtaosa tällaisesta toiminnasta tapahtuu henkilöstön tiedostamattomana toimintana, useimmiten inhimillisinä virheinä. Osa toiminnasta on tietoista, suoraan ohjeiden vastaista toimintaa.

Sovelluksen avulla olisi mahdollista kehittää julkisen hallinnon henkilöstön tietosuojan ja tietoturvallisuuden osaamista tarjoamalla sovellus, jonka avulla saataisiin niin ajankohtaista tietoa sekä myös hyviä käytäntöjä tietosuojan ja tietoturvallisuuden osalta. Sovelluksen avulla voitaisiin toteuttaa esimerkiksi tiedonhallintalain yhteydessä tarvittavaa toimeenpanoa uusien tietoaineistojen luokitteluohjeiden ja muun tarvittavan koulutuksen osalta. Lisäksi sovellus mahdollistaisi lähes reaaliaikaisen kanavan viestiä ajankohtaisista asioista sen käyttäjille. Vaikka sovellus on ensisijaisesti tarkoitettu julkisen hallinnon henkilöstölle, siitä olisi merkittävää hyötyä myös yksityisellä puolella toimiville organisaatioille.

Kirjoittaja:
Kimmo Rousku

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

ISSN 1797-9714 (pdf)
ISBN 978-952-251-941-2 (pdf)

Huhtikuu 2018