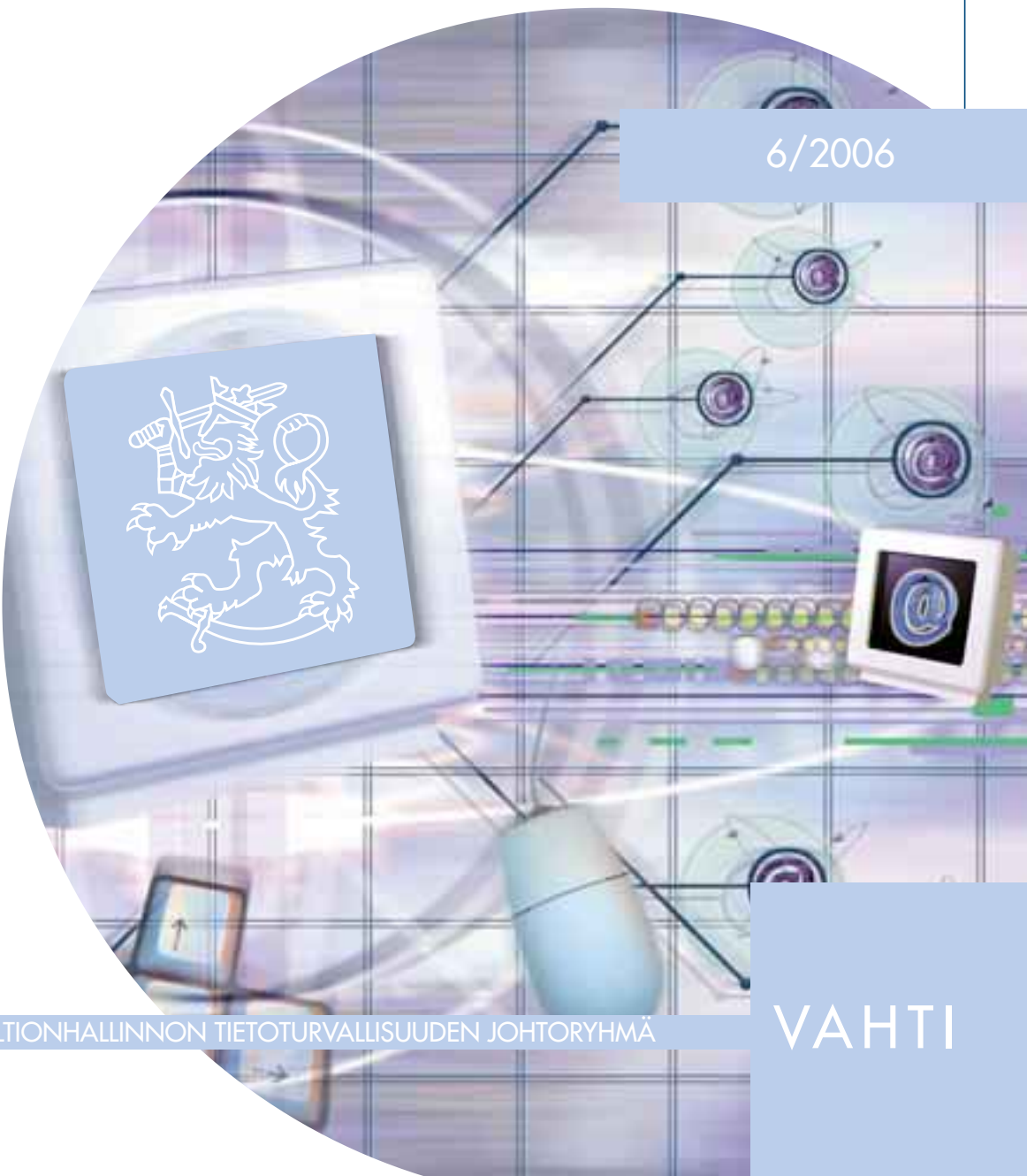
VALTIOVARAINMINISTERIÖ

TIETOTURVATAVOITTEIDEN ASETTAMINEN JA MITTAAMINEN



6/2006

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

TIETOTURVATAVOITTEIDEN ASETTAMINEN JA MITTAAMINEN

6/2006

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28
00023 VALTIONEUVOSTO

Puhelin
(09) 160 01

Telefaksi
(09) 160 33123

Internet
www.vm.fi

Julkaisun tilaukset
Puh. (09) 160 33287
fax (09) 160 33235

ISSN 1455-2566
ISBN 951-804-622-0(nid.)
ISBN 951-804-623-9(pdf)

Edita Prima Oy
HELSINKI 2006

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM 18/01/2006

OHJE
21.6.2006

Ministeriöille, virastoille ja laitoksille

TIETOTURVATAVOITTEIDEN ASETTAMINEN JA MITTAAMINEN

Valtiovarainministeriön ohessa antaman tietoturvaohjeen (jäljempänä ohje) tavoitteena on tehostaa ja yhteensovittaa tietoturvallisuuden sisällyttämistä hallinnon tulosohjaukseen sekä kehittää tietoturvallisuuden mittausta hallinnossa. Ohje on tarkoitettu ministeriöiden ja virastojen johdolle, riskienhallinnan koordinaattoreille, tietohallinto- ja tietoturvajohdolle sekä kaikille tietoturvallisuuden kehittämisestä vastaaville.

Ohje laadittu valtiovarainministeriön asettaman Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI ohjauksessa ja alaisuudessa osana valtionhallinnon tietoturvallisuuden kehitysohjelmaa (VAHTI-julkaisu 1/2004) ja se täydentää laajaa olemassa olevaa valtion VAHTI-tietoturvaohjeistoa.

Tietoturvatyötä tulee johtaa tulosohjauksen keinoin asettamalla sen kehittämiselle ja laadulle useampivuotisia ja vuositavoitteita sekä mittaamalla ja arvioimalla aikaansaatuja vaikutuksia.

Ohjeessa on esitetty vaiheistukseen ja käytännön esimerkkeihin perustuva, organisaation riskienhallintaa palveleva malli tietoturvallisuuden johtamis- ja hallintajärjestelmän rakentamiseksi ja kehittämiseksi.

Tietoturvallisuuden tavoitetaso ja mittarit asetetaan organisaation toiminnan yhteiskunnallisen merkityksen, tietointensiivisyyden ja tietoturvatyön kehitystilanteen perusteella. Ohjeessa esitetyt mittarit perustuvat valtiohallinnon kokemuksiin käytännössä toimivista seurantamittareista.

Asiakirja tulee VAHTIn Internet-sivuille (www.vm.fi/vahti). Ohjetta kehitetään tarvittaessa mm. saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi).

Lisätietoja antavat tietoturvallisuusasiantuntija Juhani Sillanpää ja neuvotteleva virkamies Mikael Kiviniemi (etunimi.sukunimi@vm.fi)

Toinen valtiovarainministeri — Ulla-Maj Wideroos

Neuvotteleva virkamies — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite Tietoturvatavoitteiden asettaminen ja mittaaminen (VAHTI 6/2006)

ESIPUHE

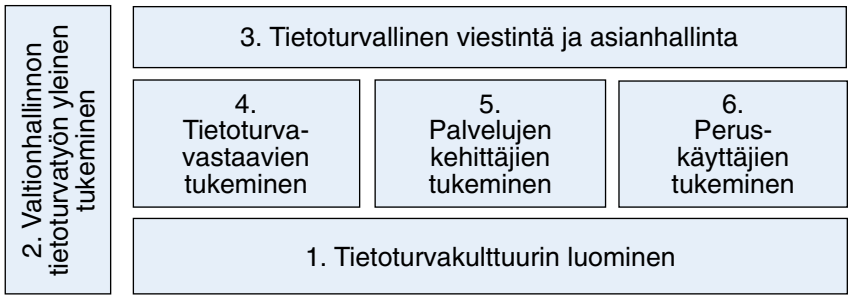
Valtiovarainministeriö (VM) vastaa valtion tietoturvallisuuden ohjauksesta ja kehittämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTIssa ovat edustettuina eri hallinnonalat ja -tasot.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta ja jatkuvuutta sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi valtionhallinnon kaikkea toimintaa. VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat määräykset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset ja toimenpiteet. Valtionhallinnon lisäksi VAHTIn toiminnan tuloksia hyödynnetään laajasti myös kunnallishallinnossa, yksityisellä sektorilla, kansalaistoiminnassa ja kansainvälisessä yhteistyössä. VAHTI on tunnettu muun muassa tietoturvajulkaisuista ja –ohjeista sekä tietoturvahankkeistaan (www.vm.fi/vahti).

Valtion tietoturvallisuuden kehitysohjelma on julkaistu VAHTI-julkaisusarjassa nimellä Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004–2006, VAHTI 1/2004. Kehitysohjelmalla kehitetään tietoturvallisuutta laajasti osana kaikkea toimintaa. Kehitysohjelmaan sisältyy kaikkiaan 29 laajaa kehittämiskohdetta, joista osaa toimeenpannaan työryhmien tai jaostojen valmistelussa ja osaa muilla toimenpiteillä.

Kehitysohjelmaan osallistuvat laajasti kaikki hallinnonalat ja lisäksi osassa hankkeita on mukana kuntien ja elinkeinoelämän edustajia sekä ulkopuolisia asiantuntijoita. Hankkeissa on vuonna 2005 ollut mukana valtionhallintotasolla nimettyinä noin 300 osallistujaa. Osa kehitysohjelman kehitystyöstä toteutetaan hanketyöllä ja osa muulla ohjaus-, kehitys- ja yhteistyöllä. Virallisesti asetetut hankkeet löytyvät valtioneuvoston hankerekisteristä (http://www.hare.vn.fi/) VAHTIn (VM166:00/2003) alahankkeina. Seuraavassa kuvassa on esitettyinä kehitysohjelman osa-alueet.

Kaavio kehitysohjelmasta ja sen hankealueista



Tämä asiakirjan on laatinut VAHTIn alainen tietoturvallisuuden tulosohjaus ja mittaustyöryhmä. Työryhmän työ on osa kehitysohjelman tietoturvakulttuurin luominen- hankealuetta.

VAHTIn toiminnan kokonaisuutta vuodelta 2005 sekä hankkeiden tavoitteita on kuvattuna VAHTIn toimintakertomuksessa (VAHTI 1/2006).

Sisällysluettelo

JOHDON TIIVISTELMÄ

Tietoyhteiskuntaohjelmassa hallitus on asettanut tavoitteeksi kehittää kansalaisten tietoyhteiskuntavalmiuksia ja turvallista tietoyhteiskuntaa. Hallitus haluaa varmistaa, että Suomi pysyy tietoturvallisena, tietoturvallisuuden kilpailukyky on kunnossa ja että tietoturvallisuuteen liittyvät osaaminen ja tietoisuus ovat korkeaa tasoa.

Valtiovarainministeriö ohjaa ja yhteen sovittaa valtionhallinnon tietoturvallisuutta ja sen kehittämistä. Valtionhallinnon tietoturvallisuuden kehitysohjelmassa 2004–2006 (Vahti 1/2004) tärkeimmät kehityskohteet on jaettu kuuteen hankealueeseen. Näistä ensimmäinen on tietoturvakulttuurin luominen, jota tämä julkaisu käsittelee tietoturvallisuuden tulosjohtamisen näkökulmasta. Ohje on tarkoitettu virastojen ylimmälle johdolle, riskienhallinnan koordinaattoreille, tietohallintojohdolle, tietoturvapäälliköille ja tietoturvallisuuden kehittämisestä vastaaville.

Tietoturvallisuuden merkitys organisaatioille lisääntyy toimintojen digitalisoitumisen seurauksena. Verkkopalveluiksi kehitetyt asiakaspalvelut, organisaatioiden välinen viestintä, tiedonsiirto ja toimintaprosessien yhteen liittäminen ovat nykytilassa osa normaalia palvelujen tuotantotapaa.

Hyvän hallintotavan (corporate governance) vaatimusta ja riskienhallinnan merkitystä korostetaan sekä kotimaisessa että kansainvälisessä keskustelussa. Valtion talousarviosta annetun asetuksen mukaan toimintakertomuksen tulee sisältää arviointi sisäisen valvonnan ja siihen sisältyvän riskienhallinnan asianmukaisuudesta ja riittävyydestä - tämä koskee myös tietoturvariskejä.

Tietoturvatyön päämääränä on vähentää toimintaan kohdistuvia häiriöitä. Tietoturvallisuuden strategisena kehittämistavoitteena on organisaation riskienhallintaa palvelevan tietoturvallisuuden johtamis- ja hallintajärjestelmän luominen. Tässä dokumentissa on esitetty vaiheistukseen perustuva malli tämän järjestelmän rakentamiseksi. Tietoturvatyötä voidaan johtaa tulosohjauksen keinoin asettamalla sen kehittämiselle ja laadulle useampivuotisia ja vuositavoitteita sekä mittaamalla ja arvioimalla aikaansaatuja vaikutuksia.

Tietoturvallisuuden tavoitetaso ja mittarit suhteutuvat organisaation tietointensiivisyyttä ja tietoturvatyön kehitystilannetta vasten; tietointensiivisillä organisaatioilla tavoitetaso on muita korkeampi. Tässä raportissa esitetyt mittarit perustuvat pääosin Väestörekisterikeskuksen ja Poliisin tietohallintokeskuksen käytännön kokemuksiin toimivista seurantamittareista. Tyypillisiä seurantakohteita ovat tietoturvapoikkeamat, niiden hallinta ja tietoturvatoiminnan laajuus.

Käytännön tason arviointi- ja mittaustilanteita varten VAHTI -työryhmät ovat tuottaneet useita eri tilanteisiin sopivia ohjeita ja suosituksia, joista pian julkaistava ohje tietoturvallisuuden arvioinnista valtionhallinnossa (VAHTI -ohje, 8/2006) soveltuu hyvin tietoturvatoiminnan laadun ja sisällön arviointitilanteisiin.

Merkittävän osan tiedonhallintapalveluista tuottavat sopimustoimittajat. Tietoturvapalvelujen ja tietoturvatyön tavoitteiden sisällyttämistä sopimuksiin on käsitelty VAHTI -ohjeessa Muutos ja tietoturvallisuus (VAHTI -ohje, 7/2006)

1 JOHDANTO

Valtionhallinnon tietoturvallisuuden kehitysohjelmassa 2004–2006 (Vahti 1/2004) tietoturvallisuuden tärkeimmät kehityskohteet on jaettu kuuteen koriin. Näistä ensimmäinen on tietoturvakulttuurin luominen. Tietoturvakulttuurin luomisen keinoja organisaatioissa ovat henkilöstön kouluttaminen, johdon tietojen ja valmiuksien parantaminen, avainhenkilöiden kouluttaminen ja koulutuksen suosiminen sekä tietoturvallisuuden ottaminen mukaan tulosohjaukseen. Tämä julkaisu käsittelee viimeksi mainittua aihetta ja sen keskeisin päämäärä on edistää tietoturvakulttuurin kehittymistä organisaatioissa.

Valtiovarainministeriö (VM) ohjaa ja yhteen sovittaa valtionhallinnon tietoturvallisuutta ja sen kehittämistä. Valtionhallinnossa tietoturvallisuuden yhteisinä lähtökohtina ovat jokaisen organisaation vastuu oman toimintansa tietoturvallisuudesta sekä säädöksissä määritellyt tietoturvavelvoitteet ja valtiovarainministeriön antamat tietoturvaohjeet. Kunkin ministeriön tulee koordinoida tietoturvallisuuden kehittämistä omalla hallinnonalallaan.

Tietoturvallisuutta on välttämätöntä tarkastella organisaatiotasolla, koska:

– digitalisoituva toimintaympäristö tuo tullessaan uudenlaisia turvauhkia toiminnan jatkuvuudelle ja
– tietoverkkojen varaan kehittyvä verkostotalous luo uudenlaisia laatuvaatimuksia organisaatioiden toiminnan kehittämiselle ja toimintojen toisiinsa liittämiselle.

Valtiovarainministeriön julkaiseman Tulosohjauksen käsikirjan (VM Julkaisuja 2/2005; http://www.vm.fi) mukaan organisaation kokonaistuloksellisuus muodostuu neljästä peruskriteeristä:

– yhteiskunnallinen vaikuttavuus
– toiminnallinen tehokkuus
– tuotokset ja laadunhallinta
– henkisten voimavarojen hallinta.

Näistä tietoturvallisuuden hallinnalla voidaan vaikuttaa varsinkin tuotokseen ja laadunhallintaan, mutta merkittävästi myös toiminnan tehokkuuteen.

Raportin tarkastelunäkökulmassa korostuu tietoturvallisuuden johtamis- ja hallintajärjestelmän kehittäminen tulosohjauksen työvälineeksi. Joissakin organisaatioissa on jo pitkälle kehittynyt tietoturvallisuuden hallintajärjestelmä, joka luo puitteet ja menettelyt tietoturvallisuuden hallinnalle. Valtaosa valtionhallinnon organisaatioista on kuitenkin vasta käynnistämässä toimenpiteitä tietoturvakulttuurin luomiseksi.

Tässä julkaisussa on tulosohjausajattelun viitekehyksenä käytetty edellä mainittua Tulosohjauksen käsikirjaa. Siinä esitettyä ajattelutapaa on pyritty soveltamaan tarkasteltaessa tietoturvallisuuden tulosohjausta ja ottamaan tarkastelussa huomioon tietoturvallisuuden tulosohjauksen erityispiirteet.

Tietoturvallisuuden hallinta on osa organisaation kokonaisvaltaista riskienhallintaa, josta vastuu on organisaation johdolla. Vaikka riskien hallintaa ei olisikaan tarkasteltu organisaatiotasolla, se ei ole este tietoturvallisuuden hallintajärjestelmän kehittämiselle. Tätä tavallisesti useampivuotista kehitystyötä voidaan ohjata tulostavoitteilla ja siirtää samalla aseittain huomio hallintajärjestelmän tuottamien mittaustulosten perusteella tehtävään päätöksentekoon.

Työryhmä keskittyi työssään seuraaviin kysymyksiin:

– keinojen tunnistamiseen, joilla tietoturva-asiat saadaan kytkettyä tulosohjaukseen siinä laajuudessa kuin se on tarpeellista
– organisaation tietoturvallisuuden hallintajärjestelmän kehittämisen haasteisiin ja kehittämisen kytkeytymiseen tulosohjaukseen
– tietoturvallisuuden mittaamiseen tulosohjauksen näkökulmasta.

Työryhmä on käyttänyt hyväkseen valtiovarainministeriön aiemmin tekemää kehitystyötä ja pyrkinyt muodostamaan siihen näkökulman tietoturvallisuuden tulosohjauksesta käsin.

Työryhmän tavoitteet, kokoonpano ja toiminta

Valtiovarainministeriö asetti työn tavoitteiksi tehostaa ja yhteensovittaa tietoturvallisuuden sisällyttämistä hallinnon tulosohjaukseen sekä kehittää tietoturvallisuuden mittausta hallinnossa. Keskeisinä päämäärinä on ollut kehittää menettelyt tietoturvallisuuden sitomiseksi viraston toiminnallisiin tulostavoitteisiin sekä valtion tietoturvamittariston ja mittaamisperiaatteiden valmistelu.

Hanke toteutettiin virkatyönä Valtionhallinnon tietoturvallisuuden johtoryhmän alaisuudessa ja ohjauksessa. Hanke on osa valtionhallinnon tietoturvallisuuden kehitysohjelmaa 2004–2006 (VAHTI 1/2004). Työryhmä työskenteli 1.12.2004 – 22.11.2005 välisen ajan.

Puheenjohtaja	
tietojohtaja	**Seppo Oinonen**, Tiehallinto
Jäsenet	
erityisasiantuntija	**Timo Erjansola**, oikeusministeriö
budjettisihteeri	**Tomi Hytönen**, valtiovarainministeriö
tietoturvallisuuspäällikkö	**Kalevi Hyytiä**, Pääesikunta
lehtori	**Jorma Kajava**, Oulun yliopisto
tietoturvapäällikkö	**Erja Kinnunen**, Ajoneuvohallintokeskus
johtaja	**Kaarina Koskinen**, Ulkomaalaisvirasto
opetusneuvos	**Marja Kylämä**, opetusministeriö
tietohallintopäällikkö	**Tarmo Maunu**, maa- ja metsätalousministeriö
tietohallintopäällikkö	**Marit Olander**, valtioneuvoston kanslia
neuvotteleva virkamies	**Matti Salminen**, valtiovarainministeriö
erikoistutkija	**Reijo Savola**, VTT
tietohallintopäällikkö	**Kristel Sarlin**, TKK
turvallisuuspäällikkö	**Seppo Sundberg**, Valtiokonttori
tietohallintojohtaja	**Ari Uusikartano**, ulkoasiainministeriö

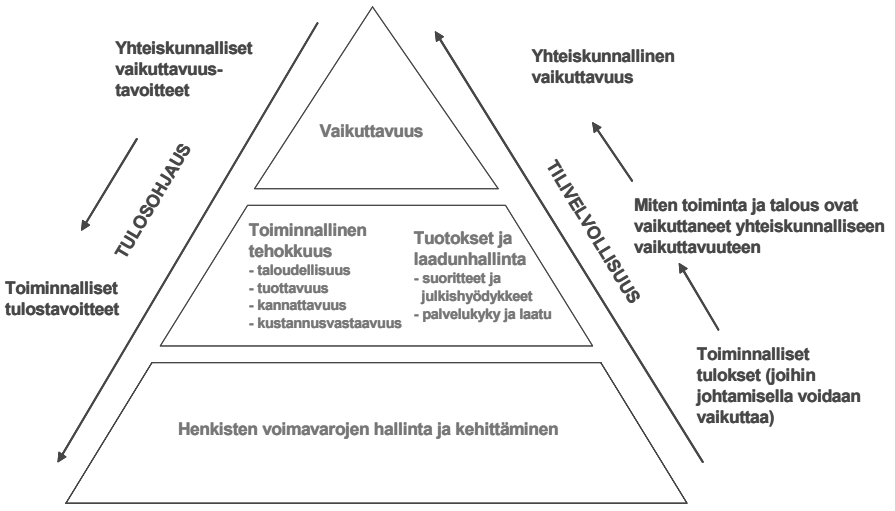
Tehtävän etenemistä raportoitiin ja käsiteltiin VAHTI - johtoryhmän neljässä kokouksessa ja VAHTI -hankevetäjille järjestettyjen seminaarien yhteydessä kahdesti. Keskeiset tulokset esiteltiin valtiovarainministeriön järjestämässä virastojen johdolle suunnatussa johtaminen ja tietoturvallisuus seminaarissa 8.11.2005. Työryhmän esitys loppuraportiksi toimitettiin VAHTI -ryhmälle 03.03.2006 verkkosivuilla kommentointia varten. Raporttiin annettiin 25 lausuntoa, jotka ovat vaikuttaneet raportin lopulliseen muotoiluun. Loppuraportin viimeistelystä ja julkaisemisesta päätettiin VAHTI –johtoryhmässä 27.04.2006.

2 TIETOTURVALLISUUDEN SISÄLLYTTÄMINEN HALLINNON TULOSOHJAUKSEEN

2.1 Tulosohjauksen viitekehys

Tulosohjaus on tässä raportissa esitettynä käsitettävä laajana kokonaisuutena. Se kattaa kaiken kaikkiaan pyrkimykset tuloksellisen toimintaan ottamatta kantaa esimerkiksi siihen, millä aikavälillä toiminta tapahtuu.

Tulosohjauksen käsikirjassa määritellään tulosohjaus seuraavasti:
Tulosohjaus on vuorovaikutteinen sopimusajatteluun perustuva ohjausmalli, jonka toiminnallinen ydin on sopijapuolten kyvyssä löytää oikea tasapaino käytettävissä olevien voimavarojen ja niillä saavutettujen tulosten välillä.



Kuva 2.1. Tuloksellisuuden peruskriteerit.

Yhteiskunnallinen vaikuttavuus kuvaa toimintapolitiikan tavoitteita ja niiden saavuttamisen astetta ja sen kustannuksia.

Toiminnallinen tuloksellisuus puolestaan koostuu tavoitteista, joihin viraston tai laitoksen omalla toiminnalla ja sen johtamisella voidaan välittömästi vaikuttaa.

– *Toiminnalliseen tehokkuuteen* sisältyvät toiminnan taloudellisuus, tuottavuus ja kannattavuus maksullisen palvelutoiminnan osalta.
– *Tuotokset ja laadunhallinta*an sisältyvät mm. suoritteiden ja julkishyödykkeiden määrä sekä toiminnan palvelukyky ja laatu.

Henkisten voimavarojen hallintaan ja kehittämiseen sisältyvät mm. tiedot henkilöstömäärästä ja -rakenteesta, henkilöstökuluista, työhyvinvoinnista ja osaamisesta sekä muusta aineettomasta pääomasta ja toiminnan uusiutumisesta.

2.2 Tietoturvallisuuden kytkeytyminen organisaation johtamiseen

Tietoturvallisuuden tulosjohtamisen perustavoitteena on kehittää tietoturvakulttuuria osana organisaation riskienhallintaa. Tietoturvatoiminnan päämääränä on vähentää toimintaan kohdistuvia häiriöitä ja tietoturvariskejä sekä aikaansaada toiminnallista laatua.

Tietoturvallisuuden johtaminen on osa organisaation kokonaisvaltaista riskien- ja laadunhallintaa. Tavoitetaso määräytyy sen mukaan, mikä on tiedonhallinnan ja tietotekniikan merkitys organisaation palvelutuotannolle ja muulle toiminnalle. Palvelujen verkkoperusteinen tuottaminen, toimintojen verkottuminen sekä prosessien ja järjestelmien yhteen liittäminen sidosryhmien kanssa asettavat uudenlaisia vaatimuksia tietoturvallisuudelle.

Tietoturvatoiminnan perustehtäviin kuuluvat tarjottavien palvelujen perustana olevien tietoaineistojen ja tietoteknisten ratkaisujen turvallisuuden varmistaminen kaikissa oloissa. Nämä perustehtävät on kuvattavissa tietoturvallisuuden hallintajärjestelmänä ja se sisältää ohjeet normaalitoiminnan tietoturvatehtäviin, häiriötilanteiden hallintaan ja poikkeusoloihin varautumiseen.

Tietoturvatoimintaa ohjataan säädöksillä (lait ja asetukset) ja suosituksilla (VAHTI -ohjeistot), jotka määrittävät tietoturvallisuuden minimi- ja tavoitetasoa sekä suositeltavia tapoja toteuttaa tietoturvaratkaisuja.

Tietoturvatoimintaa voidaan johtaa asettamalla sille kehittämistavoitteita ja toteutettavaan turvallisuustasoon liittyviä tavoitteita sekä seuraamalla tuloksia määritellyillä mittareilla tulosohjauksen puitteissa.

Tietoturvatoiminnan tavoitteistoa on perusteltua tarkastella organisaation toiminnan jatkuvuuden ja laadun, asiakaspalvelujen, sidosryhmien, muutoksen hallinnan ja säädösnäkökulmista.

Toiminnan jatkuvuus ja laatu

Organisaation on suojauduttava vakavilta häiriöiltä varmistaakseen sille elintärkeiden toimintojen jatkuvuuden ja välttääkseen häiriöistä aiheutuvat menetykset. Tiedonhallinnan ja sen myötä myös tietoturvallisuuden merkitys organisaation toimintakyvyn ylläpidossa sekä häiriöttömässä ja tuloksellisessa toiminnassa on jatkuvasti lisääntynyt.

Yleisen määritelmän mukaan laatu on niistä organisaation ominaisuuksista koostuva kokonaisuus, johon perustuu toiminnan kyky täyttää siihen kohdistuvat odotukset. Oleellista on toiminnan vastaavuus asiakkaan tarpeisiin ja odotuksiin sekä se, että toimintakokonaisuus vastaa sille asetettuja vaatimuksia.

Julkisen palvelun laatutekijöitä ovat esimerkiksi asiakastyytyväisyys ja palvelun saatavuus, luotettavuus ja turvallisuus, kustannustehokkuus ja asioiden hoidon läpimenoajat.

Asiakasnäkökulma

Kansalaisten ja palvelujen käyttäjien näkökulmasta hallinnon tehtävänä on tuottaa sellaisia sähköisiä palveluja, joiden turvallisuuteen asiakas voi luottaa, ja jotka ottavat huomioon kansalaisten perusoikeudet. Esimerkiksi laissa sähköisestä asioinnista viran-omaistoiminnassa (13/2003) on säädetty viranomaisten ja asiakkaiden oikeuksista, velvollisuuksista ja vastuista sähköisessä asioinnissa. Lain tarkoituksena on lisätä asioinnin sujuvuutta ja joutuisuutta samoin kuin tietoturvallisuutta hallinnossa ja tuomioistuimissa sekä edistää sähköisten tiedonsiirtomenetelmien käyttöä.

Palvelujen tuottaminen

Tietoturvaongelmat ovat esiintyessään vakava este palvelujen tuottamiselle ja tarjoamiselle. Organisaation tuottamien ja siellä kehitettävien palvelujen näkökulmasta tietoturvallisuuden perustekijöiden on oltava kunnossa. Käyttöönotettavien palvelujen tuottamisen kannalta kriittisten tuotantoketjujen laatu on syytä varmentaa myös tietoturvallisuusnäkökohdista. Palvelun laatuun mahdollisesti syntyvää uskottavuusongelmaa on vaikea korjata jälkeenpäin.

Arvoverkosto

Tietoturvallisuudelle asettavat odotuksia ja vaatimuksia myös organisaation sidosryhmät. Näiden merkitys korostuu verkottumisen ja eri organisaatioiden prosessien ja tietojärjestelmien yhteenliittämisen myötä. Usean organisaation läpi kulkevan prosessin kokonaislaadun määrittää ”heikoin lenkki”. Tietoturvatavoitteet ja niiden toteutuminen tulee varmistaa prosessiin osallistuvien toimijoiden yhteistyönä ja kirjata sopimuksin.

Muutoksen hallinta

Tietoturvariskit korostuvat toiminnan muutostilanteissa, joita voivat olla esimerkiksi siirtyminen ostopalvelujen hankintaan, toimintojen ulkoistaminen tai erilaiset organisaatio- ja toimitilajärjestelyt. Viraston toimintaympäristössä tai palvelutuotannossa tapahtuvien muutosten vaikutukset on siten tarpeen arvioida myös tietoturvanäkökulmasta.

Säädösperusta

Tietoturvallisuutta koskeva säädösperusteisuus on laajaa. Kansalaisilla on perustuslaillinen oikeus yksityisyyden suojaan. Lisäksi monet muut lait määrittävät eri tilanteissa sovellettavaa tietoturvallisuuteen liittyvää normistoa.

Esimerkiksi laki viranomaisen toiminnan julkisuudesta 18 § velvoittaa viranomaisen hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtimaan asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muista tietojen laatuun vaikuttavista tekijöistä. Henkilötietolaki asettaa velvoitteita henkilötietojen käsittelyyn.

Valtion talousarviosta annettuun asetukseen (1243/1992) on tehty muutoksia asetuksella 254/2004. Asetuksen 65 §:ssä on vaatimus, että viraston toimintakertomuksen tulee sisältää arviointi sisäisen valvonnan ja siihen sisältyvän riskienhallinnan asianmukaisuudesta ja riittävyydestä ja sen perusteella on laadittava lausuma sisäisen valvonnan tilasta ja olennaisimmista kehitystarpeista. Saman asetuksen 69 b§ edellyttää riskienhallinnan vastuiden ja menettelyjen luomista virastoissa. Taustalla on näkemys, että riskien tunnistaminen ja hallinta on tärkeää myös valtionhallinnon toiminnassa ja johtamisessa (Sisäisen valvonnan ja riskienhallinnan arviointikehikko. Ehdotus suositukseksi valtionhallinnon hyväksi käytännöksi. Valtiovarainministeriö, 2005).

Arviointi- ja vahvistuslausumassa viraston ylin johto ottaa kantaa sisäisen valvonnan tilaan ja olennaisimpiin kehittämistarpeisiin.

Säädösperusteisen tietoturvatason toteuttamista voidaankin pitää minimivaatimuksena organisaation tietoturvatoiminnalle.

2.3 Tietoturvallisuuden johtamis- ja hallintajärjestelmä ja sen kehittäminen

Tietoturvallisuuden hallintajärjestelmää on käsitelty aiemmin mm. VAHTI-ohjeissa Valtion viranomaisen tietoturvallisuustyön yleisohje (VAHTI 1/2001) ja Tietoturvallisuuden hallintajärjestelmän arviointisuositus (VAHTI 3/2003). Ohjeessa 3/2003 on kuvattu, mitä hallintajärjestelmään kuuluu ja miten se muodostetaan. Myös ISO/IEC 17799:2005 kuvaa hallintajärjestelmää ja määrittelee sen vaatimukset. Standardin mukainen toiminta mahdollistaa tietoturvallisuuden hallintajärjestelmän sertifioinnin, mutta standardia voi toki

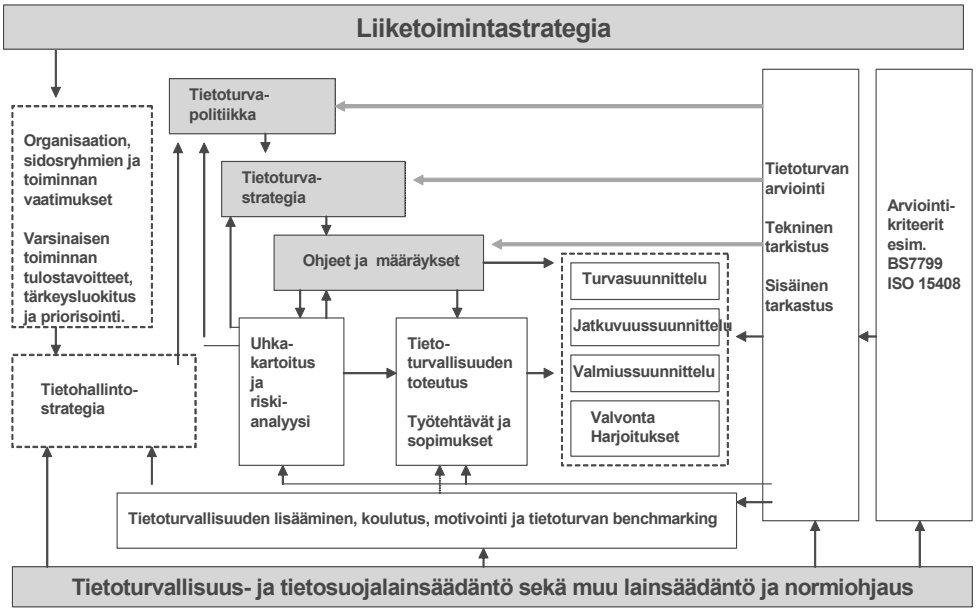
noudattaa, vaikka sertifiointi ei olisikaan organisaation ensisijaisena tavoitteena. Standardin mukainen toiminta osoittaa organisaation johdon sitoutuneisuutta tietoturvallisuuden pitkäjännitteiseen kehittämiseen.

Tietoturvallisuuteen liittyvän riskienhallinnan tarkoituksena on hallita organisaation toimintaan ja tavoitteisiin liittyviä epävarmuustekijöitä. Tavoitteiden saavuttamista edistetään ja epävarmuuksia hallitaan suunnitelmilla, päätöksillä ja toimenpiteillä, jotka ovat osa toiminnan yleistä systemaattista johtamista.

Tietoturvallisuuden johtamis- ja hallintajärjestelmä on luonteeltaan viitekehys, joka on aina sovitettava organisaatiokohtaisesti riippuen tietoturvariskien merkityksestä ja tietoturva-asioiden kehitysvaiheesta organisaatiossa.

Tietoturvallisuuden hallintajärjestelmä perustuu organisaation toimintastrategiaan sekä kokonaisvaltaiseen riskienhallinnan suunnitteluun (sisältää toiminnan uhkakartoituksen ja riskianalyysin sekä riskienhallintasuunnitelman). Se koostuu tietoturvariskien hallintasuunnitelmaan perustuvista toimintamalleista ja dokumenteista (lyhyt sisältökuvaus sanastoliitteessä), joita ovat:

- tietoturvapolitiikka ja -strategia
- tietoturvallisuuden kehittämissuunnitelma
- tietoturvasuunnitelma, joka kuvaa voimassaolevat tietoturvakäytännöt
- tietoturvallisuuden perusohjeistus ja lisäohjeistus
- tietoturva-arkkitehtuurit (topologia- ja ratkaisujen periaatekuvaukset)
- tietoturvaraportointi johdolle
- jatkuvuussuunnitelmat
- poikkeusolojen tietojenkäsittelyn valmiussuunnitelmat
- toimintaan liittyvät tietoturvaprosessit
- auditointisuunnitelma.



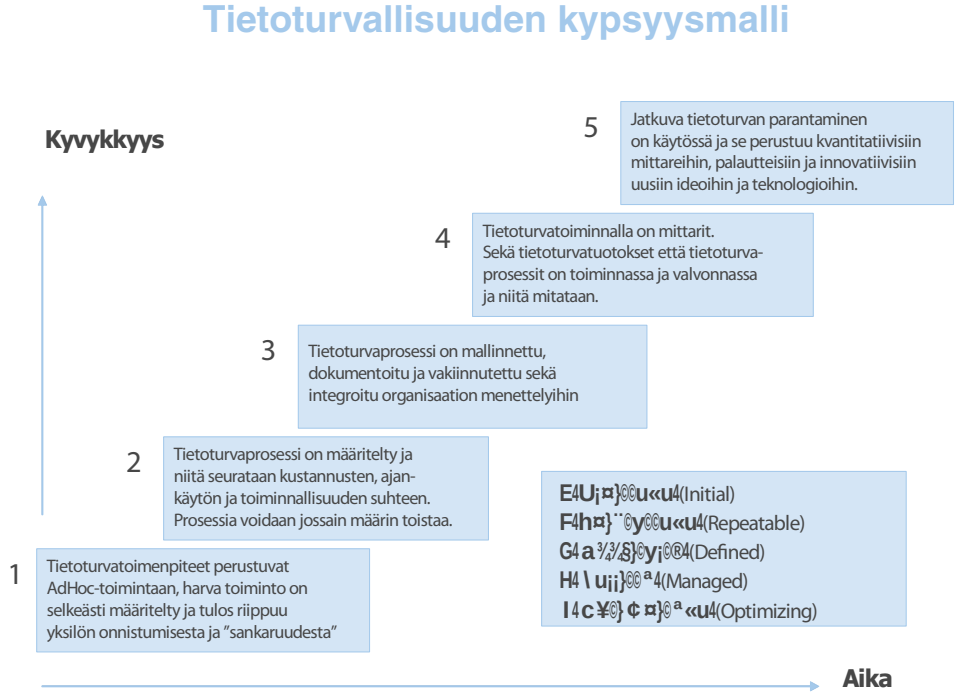
Kuva 2.2. Tietoturvallisuuden hallintajärjestelmä. Lähde: Tietoturvallisuuden johtamis- ja hallintajärjestelmä (VAHTI 3/2003).

Hallintajärjestelmän kehittäminen on evoluutioprosessi, jossa organisaatiolle kehittyy valmiudet hallita systemaattisesti tietoturva-asioitaan.

Hallintajärjestelmän kypsyysaste voidaan arvioida ja tämän toimintatavan tuloksena saadaan organisaation käyttöön tietoturvallisuuden tilan kuvaus ja voidaan tunnistaa siihen liittyvät kehittämistarpeet.

Tietoturvallisuuden ja riskienhallinnan kehittäminen on luonteeltaan jatkuva prosessi, jossa painopiste on laillisuuteen, tuloksellisuuteen, tieto-omaisuuden turvaamiseen ja tietoturvapoikkeamien luotettavaan raportointiin liittyvien tavoitteiden edistämisessä.

Seuraavassa kuvassa on esitetty prosessien kypsyysarviointimalliin (CMM) perustuva näkemys tietoturvallisuuden hallintajärjestelmän kehittymisestä organisaatiossa.



Kuva 2.3. Kypsyysmalli (CMM – Capability Maturity Model) arvioi tuotteiden ja operatiivisten järjestelmien sijaan organisaation kykyä (kypsyyttä) toteuttaa prosesseja.

Tietoturvallisuuden hallintajärjestelmän kehittäminen on monivuotinen tehtävä. Pääosin julkishallinnon organisaatiot ovat vasta tämän kehitystyön ensiaskelmilla. Arviolta enintään kolmasosalla organisaatioista on asetettu tietoturvallisuuteen liittyviä vuosittaisia tavoitteita.

Tietoturvallisuuden johtamis- ja hallintajärjestelmän kehittäminen käynnistyy tavallisesti seuraavista lähtökohdista tai herätteistä:

– havaitut tietoturvaongelmat,
– ennakoidut tietoturvariskit,
– ulkoa tulevat odotukset,
– viranomaismääräykset ja suositukset tai
– laatuvaatimukset.

Seuraavassa on esitetty lyhyet kokemusperäiset kuvaukset kustakin kehitysvaiheesta. Kuvaukset perustuvat työryhmän luomaan näkemykseen kehitystyön etenemisestä..

Aloitusvaiheessa tietoturvatyö on pitkälti organisoitumatonta ja reaktiivista. Ohjeisto-

ja tuotetaan, mutta sekä ohjeistot että vastuut ovat hajanaisia. Organisaatio luo itselleen tietoturvapolitiikan (l. tietoturvalinjaukset) sekä määrittää tietoturvavastuut.

Toisessa kehitysvaiheessa oleellinen piirre on tehtävien toistettavuus. Organisaatiossa on kehitetty tietoturvallisuuden hallintaan säännönmukaisia menettelyjä. Siitä kertovat paitsi laadittu tietoturvapolitiikka, myös voimassa oleva tietoturvallisuuden kehittämissuunnitelma. Tietoturvallisuuden systemaattinen kehittäminen on käynnistynyt.

Kolmannessa vaiheessa syntyy organisaation tietoturvallisuuden hallintajärjestelmä, jolloin tietoturvaprosessit ja tavoitteet on määritelty. Tietoturvaohjeisto on kattavaa, henkilöstön tietoturvakoulutus on oleellinen osa toimintamallia ja organisaatio toimeenpanee laadittua kehittämissuunnitelmaa.

Neljännessä vaiheessa toimitaan laaditun tietoturvallisuuden hallintajärjestelmän mukaisesti ja toiminnalle on asetettu sen tuloksellisuuden ja kehittämistarpeiden arviointia kuvaavat mittarit. Tässä vaiheessa voidaan puhua tietoturvallisuuden johtamis- ja hallintajärjestelmän olemassaolosta.

Viidennessä vaiheessa tietoturvallisuuden johtamis- ja hallintajärjestelmä optimoituu auditointien, muissa organisaatioissa saatujen kokemusten ja muun oppimisen kautta. Tullakseen luontevaksi osaksi organisaation toimintaa turvallisuusasioiden on oltava kiinteä osa organisaation toimintakulttuuria.

Luvussa 5 on esitetty esimerkkejä virastoissa tapahtuneesta tietoturvallisuuden kehittämistyöstä ja voimassa olevista käytännöistä.

3 TIETOTURVALLISUUDEN TULOSOHJAUS

3.1 Tietoturvallisuuden merkityksen arviointi

Tulosohjauksessa organisaation toimintaa tarkastellaan kokonaisuutena ja tulostavoitteiden asettamisessa käytetään useita eri näkökulmia (esim. taloudellisuus, tehokkuus, tuottavuus, innovatiivisuus). Tietoturvallisuuden tulosohjauksessa voidaan hyödyntää sekä laadullisia että määrällisiä tarkasteluja esimerkiksi seuraavien kysymysten avulla:

- Kehitetäänkö tietoturvallisuutta osana viraston toimintaa ja palvelustrategiaa?
- Kuinka tietoturvariskit on tunnistettu asiakkaiden ja toimintaprosessien näkökulmasta?
- Miten lainsäädännön edellyttämät vaatimukset tietoturvallisuuden osalta on toteutettu?
- Kuinka viraston tietojenkäsittelyn tärkeysluokka on huomioitu tietoturvallisuutta kehitettäessä? Onko viraston tietojärjestelmät luokiteltu?
- Raportoidaanko tietoturvallisuuteen liittyvät häiriötilanteet? Kenelle ne raportoidaan? Onko virastossa tehty toiminnan riskikartoitus?
- Miten tietoturvallisuuden kehittämistoimenpiteiden vaikutuksia valvotaan ja arvioidaan? Onko virastolla käytössä mittaristo?
- Miten huolehditaan henkilöstön tietoturvaosaamisen ylläpidosta?

Viraston tulee luonnollisesti mieltää omat keskeiset tehtävänsä ja ryhtyä ensisijaisesti toimenpiteisiin, jotka turvaavat juuri näiden toimintojen jatkuvuuden.

Tietoturvallisuuden merkitys ilmenee laadituista riskikartoituksista ja tietoturvapolitiikasta, jotka antavat vastauksen edellisiin kysymyksiin ja antavat yhdessä kehittämistilanteen kanssa perustan tulostavoitteiden asettamiselle.

Virastolla voi olla myös erityistä merkitystä valmiustoiminnan kannalta, tämä ilmenee mm. viraston tärkeysluokituksessa. Viraston jatkuvan toiminnan kannalta tärkeysluokitetut toiminnot ja niitä tukevat tietojärjestelmät ilmenevät asianomaisista päätöksistä.

3.2 Tietoturvatavoitteiden asettaminen ja seuranta

Tietoturvatavoitteiden asettamista tapahtuu useammalla tasolla
– politiikkatasolla (esim. tietoyhteiskuntaohjelmassa)
– ministeriötasolla
– virasto- tai laitostasolla ja
– tietoturvatoiminnan sisällä.

Tietoyhteiskuntaohjelmaan liittyen hallituksen tavoitteena on kehittää kansalaisten tietoyhteiskuntavalmiuksia ja turvallista tietoyhteiskuntaa. Hallitus haluaa varmistaa, että Suomi pysyy tietoturvallisena yhteiskuntana, tietoturvallisuuden kilpailukyky on kunnossa sekä tietoturvallisuuteen liittyvä osaaminen ja tietoisuus on korkeaa tasoa. Myös julkishallinnon tietohallinnon kehittämiseen pyrkivien erilaisten hankekokonaisuuksien tai työryhmien (esim. ValtIT, VAHTI) päämäärät asettavat suoria ja välillisiä tavoitteita tietoturvallisuuden kehittämiselle. Kattavat strategiset linjaukset (esim. Valtion tietohallintostrategia) tulevat osaltaan ohjaamaan tietoturvallisuuden kehittämistä julkishallinnossa.

Valtiovarainministeriö (VM) ohjaa ja yhteen sovittaa valtionhallinnon tietoturvallisuutta ja sen kehittämistä. Valtionhallinnossa tietoturvallisuuden yhteisinä lähtökohtina ovat mm. jokaisen organisaation vastuu oman toimintansa tietoturvallisuudesta sekä säädöksissä määritellyt tietoturvavelvoitteet ja valtiovarainministeriön antamat tietoturvaohjeet. Kunkin ministeriön tulisi koordinoida tietoturvallisuuden kehittämistä omalla hallinnonalallaan.

Virasto- ja laitostasolla tietoturvallisuus liittyy organisaation kokonaisriskien hallintaan, laadunhallintaan ja usein myös organisaation tietohallintostrategiaan liittyvien tavoitteiden toimeenpanoon.

Organisaation sisällä tietoturvatoimintaa ohjataan tulostavoitteilla.

3.2.1 Tietoturvatavoitteet

Organisaation tietoturvatavoitteet voivat olla suoraan tietoturvatoimintoon liittyviä tavoitteita, mutta myös johdettuja organisaation muista tavoitteista, joissa tietoturvallisuus on keskeisessä asemassa – kuten esimerkiksi sähköisen asioinnin ja sähköisten palvelujen kehittäminen.

Jokaisen organisaation toiminnallisen vastuun näkökulmasta on keskeistä varmistaa tietoturvallisuuden järjestelmällinen hallinta virastoissa. Tällöin strategisena tavoittee-

na on muodostaa virastolle tietoturvallisuuden johtamis- ja hallintajärjestelmä, jonka tavoitetaso määritellään lähtien viraston toiminnan luonteesta ja tietoturvariskien merkityksestä.

Tavoitetason mukaisen hallintajärjestelmän kehittäminen kestää tavallisesti useita vuosia. Tällöin tietoturvallisuuden kehittämiselle tulee tavoitteet asettaa useampivuotisina toiminta- ja taloussuunnitelmassa.

Hallintajärjestelmän kehittäminen on ositettava sopiviin kokonaisuuksiin ja vuositavoitteisiin. Perustan muodostavat riskien arviointi, tietoturvapolitiikka, kehittämissuunnitelma sekä tarvittava ohjeistus ja koulutus. Tuloksena on kattava tietoturvatoiminnan ja sen osaprosessien kuvaus (toimintamallit), niihin liittyvät menettelyt ja ohjeistus sekä seuranta- ja raportointimenettelyt.

Vuositavoitteet voidaan jakaa kahteen osaan:

– tietoturvallisuuden kehittäminen sekä
– tavoiteltava ja mitattavissa oleva tietoturvataso.

Tietoturvallisuuden kehittämistavoitteilla varmistetaan tietoturvallisuuden johtamis- ja hallintajärjestelmän kehittyminen haluttuun tavoitetasoon. Tavoitteet koostuvat kehittämissuunnitelman mukaisista kehittämistoimenpiteistä ja ns. jäännöstavoitteista eli asioista, joissa aiemmin asetettu tavoitetaso ei ole toteutunut. Kehittämistehtävät vaativat

Organisaation omista lähtökohdista johdetut tavoitteet eri aikaväleille	
Aikaväli	**Tavoitealueet**
Strateginen suunnitteluaikaväli	Toiminnan tuottavuus, laatu, palvelutuotannon häiriöttömyys.
Toiminta- ja taloussuunnittelukausi	Tavoiteltavan tietoturvallisuustason (kypsyystaso) määrittäminen ja sen mukaisen kehittämisohjelman läpivienti. Hallintajärjestelmän mukaisen kypsyystason saavuttaminen.
Vuositavoitteet	Mitattavissa olevat tavoitteet tietoturvallisuustason toteutumiselle. Kehittämistavoitteet (vrt. kehittämisohjelman läpivienti).
Reunaehdot Säädösperusteisen tietoturvatason toteutuminen. Johdon lausuma riskien hallinnasta.	

Kuva 3.2. Tietoturvallisuuden tulostavoitteet ja toimenpiteet

normaalisti investointeja ja siten myös investointien optimointia sopivilla arviointimenetelmillä.

Erotuksena kehittämistehtävistä, voidaan operatiiviselle tietoturvatoiminnalle asettaa määrällisillä (kvantitatiivisilla) mittareilla mitattavissa olevia tuloksellisuus- ja laatutavoitteita. Tyypillisiä tavoitteita ovat esimerkiksi häiriöiden vähentyminen, koulutuksen toteutuminen, tietoturvatoiminnan kustannuksiin liittyvät tavoitteet tai pisteyttää toimintaa laadullisen arvioinnin näkökulmasta - arvioida esimerkiksi kypsyystasoa.

Operatiivisen tietoturvatoiminnan johdon tulee varmistaa ja ylimmän johdon valvoa, että säädöspohjainen minimitaso täyttyy ja että tietoturvatason toteutumisesta, poikkeamista ja havaituista riskeistä raportoidaan säännöllisesti johdolle.

Tietoturvatoiminnan organisoinnille ja toimintamalleille on asetettavissa tavoitteita. Tehokkuutta ja kustannussäästöjä toimintamalleissa voidaan tavoitella esimerkiksi tukeutumalla julkishallinnon yhteisiin tietoturvaratkaisuihin, osallistumalla yhteisiin kehittämishankkeisiin sekä käyttämällä yhteisiä resursseja. Jo nyt on olemassa esimerkkejä, että usea virasto on palkannut yhteisen tietoturvapäällikön. Tietoturvatoiminnan koordinointi vaatii syvää erityisosaamista, mutta harvoin täyspäiväisesti; siten tämä tehtävä sopii hyvin useamman viraston yhteisesti resursoitavaksi (Selvitys valtionhallinnon tietoturvaresurssien jakamisesta. VAHTI -ohje).

3.2.2 Budjetointi

Tietoturvatoiminnan taloudellisena tavoitteena on vähentää riskien toteutumisesta toiminnalle aiheutuvia menetyksiä.

Tietoturvamenot voidaan jakaa karkeasti muuttuviin ja kiinteisiin menoihin sekä riskivarauksiin:

- muuttuvia menoja ovat kehittämispanostukset (konsulttityö, investoinnit tieturvaratkaisuihin)
- kiinteitä menoja ovat pysyväisluonteisen tietoturvallisuustoiminnan kulut (oman henkilöstön palkat ja toimintamenot, palvelusopimusten menot)
- erillisiä riskivarauksia tarvitaan mahdollisesti toteutuvista tietoturvariskeistä aiheutuvien vahinkojen korjaamiseen.

Tehtäville investoinneille tulee arvioida takaisinmaksuaika ja niiden on oltava suhteessa arvioituun riskiin.

3.2.3 Seuranta ja raportointi

Tulosohjauksen näkökulmasta tärkeimmät seurantakohteet ovat

- asetettujen tavoitteiden toteutuminen,
- toiminnan laatu ja
- kustannukset.

Seurannassa voidaan käyttää sekä arviointeja että kvantitatiivisia mittareita. Arviointi on usein ainoa keino tarkastella esimerkiksi kehittämistavoitteiden toteutumista ja toiminnan laatua. Sen sijaan kustannuksia ja toteutunutta tietoturvatasoa voidaan seurata kvantitatiivisin perustein.

Seurannalla ja mittaamisella haetaan tukea ohjauspäätöksille. Tällöin arviointien ja mittausten tulee olla tarkoituksenmukaisia juuri tätä taustaa vasten. Seurannan ja arvioinnin kohteena ovat siis asetetut tavoitteet ja operatiiviseen tietoturvatoimintaan liittyvät tapahtumat. Jatkuva toiminnan kehittäminen edellyttää lisäksi trendien seurantaa, itsearviointeja ja/tai ulkoisia auditointeja. Myös nämä ovat johdon näkökulmasta tärkeitä välineitä tietoturvatoiminnon johtamisessa.

Seurantaan kuuluu oleellisena osana toiminnan tuloksellisuuden ja tavoitteiden toteutumisen raportointi johdolle (ks. luku 5, kohta 5.6. Esimerkki raportointimenettelystä).

Nämä raportit voidaan jakaa kahteen osaan:

– Tietoturvatoimintaa kuvaaviin raportteihin, joiden tarkempi sisältö määräytyy kunkin organisaation tarpeiden mukaan. Tyypillisiä raportteja ovat kausiraportit (kuukausi-, osavuosi- ja vuosiraportit) sekä tilannekohtaiset poikkeamaraportit vakavista tietoturvahäiriöistä.
– Normatiiviseen käytäntöön (vrt. asetus valtion talousarviosta, 65 §) kuuluu raportointi riskienhallinnan asianmukaisuudesta ja riittävyydestä johdolle toimintakertomusta varten.

Jatkuvaa raportointia täydentävät muut tietoturvallisuuden tilaa kuvaavat erilliset selvitykset ja raportit (esim. tarkastukset, auditoinnit, arvioinnit).

3.3 Tietoturvatoiminnan johtaminen

Organisaation tietoturvatoiminnan johtaminen ankkuroituu vahvasti sen strategisiin tavoitteisiin, toiminnan luonteeseen ja johdon valitsemiin toimintalinjoihin riskien ja laadun hallinnassa, tietohallinnossa ja tietoturvallisuudessa.

Tietoturvatoiminnan johtaminen kuuluu organisaation johdolle (Valtion viranomaisen tietoturvallisuustyön yleisohje, 1/2001), joka linjaa organisaation riskienhallintapolitiikan ja tietoturvapolitiikan, päättää kehittämissuunnitelmasta, vuositavoitteista, budjetista ja toimivallan delegoinneista. Tavallinen menettely on, että tietoturvallisuuteen liittyvät tehtävät ja toiminnan koordinointi delegoidaan nimetylle vastuuhenkilölle (tietoturvapäällikkö).

Tietoturvallisuuden kehittämiseen liittyy julkishallinnossa valtion poliittisen johdon asettamia tavoitteita. Nämä ilmenevät poliittisina ohjelmina, säädöksinä ja suosituksina, julkishallinnon sisällä myös tulosohjauksena. Ministeriöt asettavat tavoitteita alaisilleen virastoille ja laitoksille tulosohjausjärjestelmän puitteissa.

Tietoturvallisuuden johtamis- ja hallintajärjestelmä määrittää keskeiset tietoturvallisuuden johtamismenettelyt ja hallinta-asiakirjat. Tietoturvapolitiikka on näistä keskeisin ja siinä määritellään tietoturvatoiminnan tavoitteet, toimintalinjat ja vastuut. Tietoturvallisuuden kehittämissuunnitelman laatiminen on tarpeen jo tietoturvatyön alkuvaiheissa.

Tietoturvallisuutta tarkastellaan toiminnan riskien hallinnan, laadun ja jatkuvuuden näkökulmasta, ja tällöin vastuu kuuluu toiminnon tai prosessin omistajalle. Tämä edellyttää koulutusta ja jatkuvaa vuoropuhelua toiminnasta ja tietoturvallisuudesta vastaavien välillä.

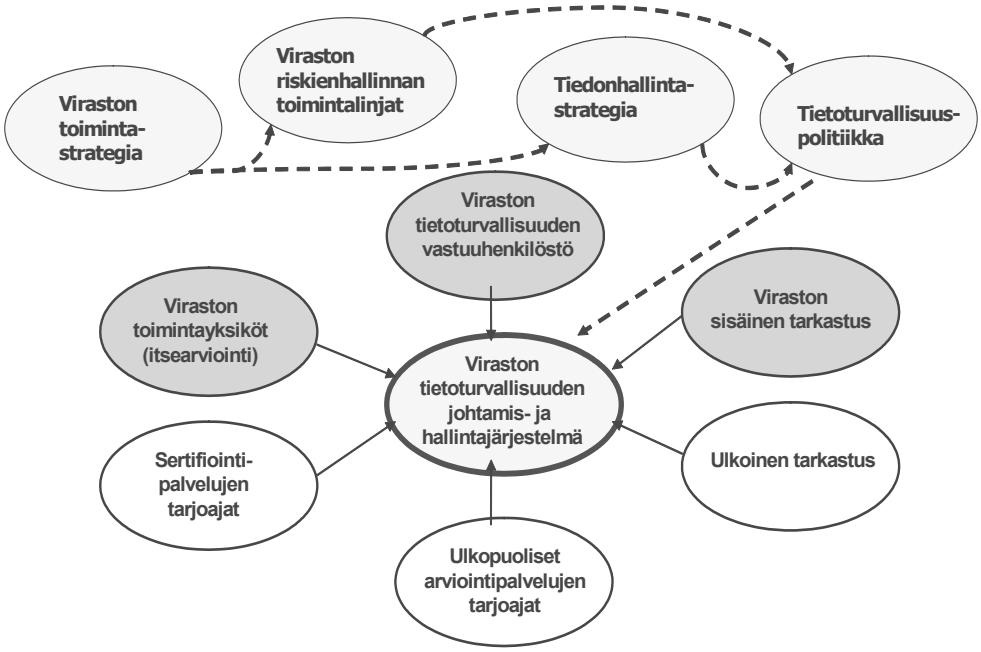
Tietoturvallisuuden kannalta erittäin merkittäviä henkilöstöryhmiä ovat tietopalveluista, -järjestelmistä ja -varastoista sekä teknisistä ratkaisuista vastaavat ja näiden kehittämistä konsultoivat henkilöt sekä atk-tukihenkilöt. Näiden henkilöstöryhmien osaaminen, toiminnan laatu ja sitoutuminen tietoturvatyöhön ovat erittäin merkityksellisiä asetettujen tavoitteiden toteutumiseksi. Tätä työtä voidaan tukea tietoturvallisuuden hallintajärjestelmällä.

On tavallista, että organisaation tietohallinnolle delegoidaan merkittävästi vastuuta tietoturvallisuudesta ja se onkin luonnollista operatiivisen tietoturvatoiminnan osalta. Myös vastuu palvelutoimittajien tietoturvatoiminnan hallinnasta on organisaatiossa sovittava. Myös tätä toimintaa on ohjattavissa tulostavoitteilla sekä sopimuksilla.

Nykyisin tiedonhallinta- ja tietotekniikkapalveluja hankitaan laajasti markkinoilta. Tästä syystä tietoturvallisuuteen ja laatuun liittyvät tekijät sekä niiden seuranta on liitettävä osaksi sopimuksia.

Organisaatiolla saattaa olla erityistä vastuuta valmiussuunnittelusta. Myös tämä näkö-kulma tulee tarkastella osana tietoturvatehtävien organisointia ja tavoitteiden asettamista.

Koska tietoturvallisuuden hallinta on koko organisaation läpi menevä toiminto, on luontevaa perustaa vastuullisen johtajan alaisuuteen tietoturvallisuuden ohjaamista, kehittämistä ja hallintaa ohjaava ryhmä, jossa kaikki edellä mainitut näkökulmat ja avainhenkilöt ovat edustettuina.



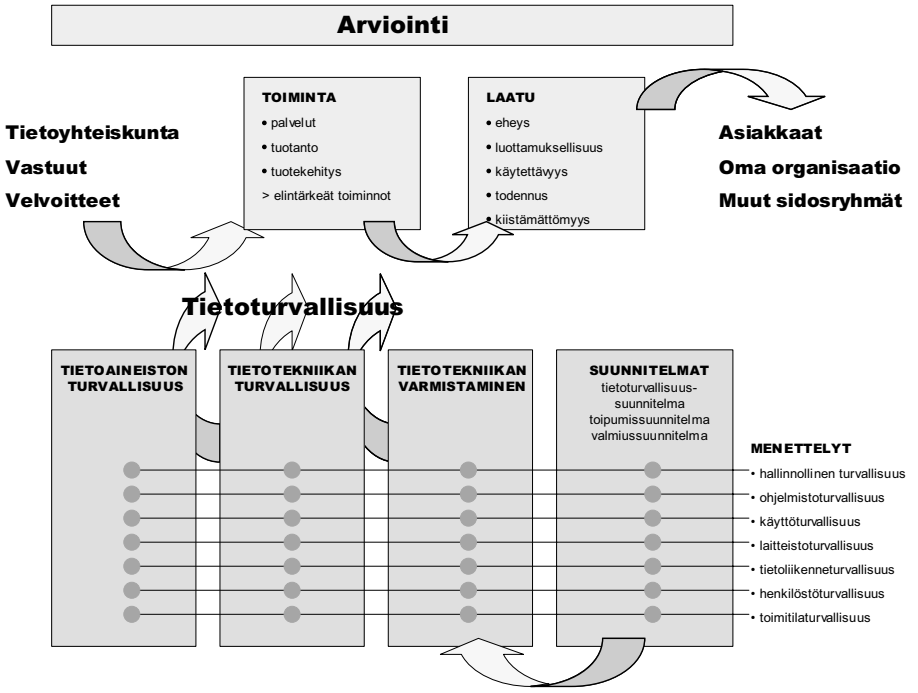
Kuva 3.3. Tietoturvatoimijat ja toiminnan ohjaus. Keskeisessä asemassa tulosjohtamisen näkökulmasta on organisaation tietoturvallisuuden johtamis- ja hallintajärjestelmä.

4 TIETOTURVARISKIEN HALLINTA SEKÄ TIETOTURVALLISUUDEN ARVIOINTI JA MITTAAMINEN

4.1 Toiminnan parantaminen arvioinnin ja mittaamisen tavoitteena

Tietoturvallisuuden tulosohjaukseen kuuluu keskeisesti arviointi ja mittaaminen. Tarkoituksena on saada informaatiota kehittämis- ja muita ohjauspäätöksiä varten.

Seuraavassa kuvassa on tarkastelu tietoturvatekijöiden arviointia toiminnalle asetettujen tavoitteiden ja asiakkaille tuotetun laadun näkökulmasta.



Kuva 4.1. Tietoturvallisuuden ja laadun arviointikokonaisuus. (Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003)

Tietoturvallisuuden hallintajärjestelmän arviointisuosituksessa (VAHTI 3/2003) ja Ohjeessa riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa (VAHTI 7/2003) on kuvattu arvioinnin keskeiset käsitteet ja menettelyt ja niissä tarjotaan apuvälineitä arviointien tekemiseen. Toiminnan laadun arvioinnin ja tietoturvallisuuden välistä yhteyttä on suosituksessa (VAHTI 3/2003) havainnollistettu kuvalla 4.1.

Arvioinnit sopivat tilannekuvan luomiseen suunnitelmien ja tavoitteiden laatimisen tueksi sekä usein myös riippumattoman näkemyksen saamiseksi tietoturvallisuuden tilasta. Systemaattinen, jatkuva mittaaminen sopii hyvin jatkuvan tietoturvatoiminnan seuraamiseen.

4.2 Arviointi- ja mittausmenetelmät

Arvioinnit ovat oleellinen osa tietoturvallisuuden hallintajärjestelmän toimintamallia ja ne muodostavat osaltaan toiminnalle mittareita. Laadullisia ovat tehdyt arviot ja raportoidut tapahtumat, kun taas määrälliset perustuvat systemaattiseen mittaamiseen.

Arviointi on luonteeltaan jatkuva toiminto, jota käytetään ensisijaisesti tietoturvallisuuden kehittämiseen ja laadun parantamiseen. Arviointeja tehdään myös ulkopuolisten tahojen odotuksien tai vaatimusten perusteella.

Itsearviointi on laadunhallinnan ja laatutyön yhteydessä käytetty systemaattinen toiminnan kehittämismenetelmä, joka käynnistyy vahvuuksien ja kehittämiskohteiden määrittelyllä. Itsearviointi sopii erittäin hyvin tietoturvallisuuden kehittämismenetelmäksi osana hallintajärjestelmää. Itsearvioinnissa voidaan käyttää esimerkiksi EFQM[1] tai vastaavia arviointimenettelyjä. Arviointi voi perustua esim. VAHTI-ohjeisiin tai ISO17799 tietoturvastandardin vaatimuksiin.

Ulkoinen arviointi - esimerkiksi kolmen vuoden välein - antaa puolueettoman kuvan organisaation tietoturvallisuuden tasosta ja tuottaa sille parannusesityksiä.

Arviointiin voidaan saada objektiivisuutta myös perustamalla arviointiryhmiä eri tulosyksiköiden kesken siten, että eri yksiköt arvioivat toisiaan.

Benchmarking[2] eli ulkoisten esikuvien löytäminen ja oman toiminnan vertaaminen näihin edelläkävijöihin antaa mahdollisuuden omaksua parhaita käytäntöjä toiminnan laadun kehittämiseen.

Laadullisessa mittaamisessa arvioidaan toiminnan onnistumista ja se sopii hyvin toiminnan tilan ja siinä tapahtuneen kehityksen arviointiin.

Määrällisessä mittaamisessa voidaan seurata esimerkiksi tulosten aikaansaamiseen käytettyä työaikaa, kustannuksia, työajan menetyksiä, tietoturvapoikkeamien lukumää-

1 Euroopan laatupalkintomallissa (EFQM, European Foundation for Quality Management) organisaation toiminnan ja tulosten arvioinnissa käytetään ns. TUTKA-arviointilogiikkaa, joka koostuu tuloksista, toimintatavoista, käytännön soveltamisesta sekä arvioinnista ja parantamisesta.

2 Arviointia, jossa organisaatiot (tai sen osat) vertaavat toimintaansa ja prosessejaan toisen organisaation kanssa.

rää tai tietoturvakoulutuksen määrää. Määrällinen mittaaminen soveltuu hyvin operatiivisen tietoturvatoiminnan mittaamiseen.

Ajoittain tarvitaan tilannekohtaista mittaamista. Se on suunniteltava uusien tilanteiden ja toiminnallisien vaatimusten mukaisesti. Esimerkiksi teknisen tietoturvallisuuden mittaus antaa kokonaiskuvan atk-teknisestä ympäristöstä ja auttaa arvioimaan siihen liittyviä uhkia.

4.3 Tietoturvatoiminnan tuloksellisuuden arviointi ja mittaus

Tuloksellisuuden arviointi ja mittaus perustuu asetettujen tavoitteiden ja toiminnan tilan seurantaa palveleviin mittareihin.

Tulosohjauksen ja tulostavoitteiden kannalta on oleellista, että mikäli tavoitteena on kehittää tietoturvallisuuden hallintajärjestelmää, niin silloin tulee arvioida tietoturvallisuuden hallintajärjestelmän kehitysvaihetta. Lisäksi voidaan mitata kehitysvaiheen mukaisesti tietoturvatoiminnalle asetettuja tuloksellisuus- ja laatutavoitteita sekä kustannuksia.

Näiden avulla voidaan asettaa uusia kehittymistavoitteita ja tuottaa tilannekuvaa valtionhallinnolle organisaatioiden tietoturvallisuuden tilasta sekä kehittämisinvestointien ja tietoturvatyön hyödyistä.

Tietoturvallisuuden kehitystyön kypsyysvaihe ja niihin soveltuvat arviointimenetelmät				
1. Aloittava	2. Toistettava	3. Määritelty	4. Hallittu	5. Optimoituva
Riskienhallinta COSO-ERM malli[3] (ks liite, lähde 11) Ohje riskien arvioinnista tietoturvallisuuden kehittämiseksi valtionhallinnossa. VAHTI 7/2003.	Arvioinnit tietoturvallisuuden osa-alueittain, esim. Valtion keskeisten tietojärjestelmien turvaaminen. VAHTI 5/2004.	Hallintajärjestelmä dokumentoitu. Tietoturvallisuuden hallintajärjestelmän-arviointisuositus. VAHTI 3/2003.	Toiminalle on asetettu tulosmittarit ja tietoturvastandardeja sovelletaan vakiintuneesti.	Toiminnanjatkuva sisäinen ja ulkoinen arviointi ja mittaaminen. Benchmarking.
Ohje tietoturvallisuuden arvioinnista valtionhallinnossa. VAHTI ohje, 2006.				
Muutos ja tietoturvallisuus. VAHTI -ohje, 2006.				

Kuva 4.2. Tietoturvallisuuden arviointi eri kypsyysvaiheissa.

3 Valtionhallinnossa käytettäväksi suositeltu sisäisen valvonnan ja riskienhallinnan arviointikehikko perustuu rakenteeltaan ns. COSO ERM (The Committee of Sponsoring Organizations of the Treadway Commission - Enterprise Risk Management) -viitekehykseen.

Tietoturvallisuuden mittaus on prosessimuotoista ja se on osa johtamisen ja tietoturvallisuuden hallintaprosessia. Prosessimuotoisella ja jatkuvasti kehittyvällä mittaamisella pystytään saavuttamaan oleellista hyötyä tietoturvallisuuden parantamisessa.

Toiminnan ohjausta ja onnistumisen arviointia tapahtuu monella tasolla. Tällöin tarvitaan mittareita eri ohjaustasojen ja tavoitteenasettelujen tarpeisiin. Ylemmällä tasolla käytetään vähemmän ja strategisempia, operatiivisella tasolla enemmän ja tarkempia mittareita.

Ohjaustasot voidaan karkeasti jakaa omistajaohjaukseen, organisaation johtoon ja tietoturvallisuuden toiminnan ohjaukseen. Operatiivisen tason mittareiden tulee osaltaan tukea strategisten tavoitteiden toteutumisen seurantaa.

Jotta mittaamisesta muodostuisi jatkuvaa toimintaa ja aikaansaataisiin aikasarjoja, on käytettävän mittariston oltava riittävän selkeä. Mittareita tulee olla mieluummin vähän ja kuvaavia sekä ohjaavia, kuin paljon ja kaiken kattavia.

Tulosohjauksen kannalta merkittävät tietoturvallisuuden arviointikohteet ovat:

- Toteutuvatko toiminnan riskien hallintaan liittyvät tietoturvatavoitteet?
- Mikä on tietoturvallisuuden nykytaso suhteessa asetettuun tavoitetasoon, ja mitkä ovat edellytykset tietoturvatavoitteiden toteuttamiseen (osaaminen, resurssit)?
- Mikä on tietoturvallisuuden hallintajärjestelmän kehittyneisyys ja laatu?
- Mitä tietoturvariskejä on tunnistettu ja miten tunnistettuja riskejä hallitaan?
- Onko verkko- ja järjestelmätason tietoturvaratkaisujen (tietoturva-arkkitehtuuri) tavoitetila määritelty ja toteutettu?
- Miten eri aikaväleille asetetut tavoitteet ovat toteutuneet?
- Seurataanko tietoturvatoiminnan kustannuksia ja tehdäänkö ohjauspäätöksiä niiden perusteella?
- Onko säädösperusteinen tietoturvataso toteutunut?

Monissa tulosyksiköissä on tarpeellista ottaa arvioinnin ja mittaamisen kohteeksi myös kriittiset tietojärjestelmäkokonaisuudet.

4.4 Tietoturvatoiminnan mittarit

Tietoturvatason toteutumista voidaan seurata pysyväisluontoisilla mittareilla. Seuraavat esimerkit on työstetty Väestörekisterikeskuksen ja Poliisin tietohallintokeskuksen käyttämistä mittareista.

Tyypillisiä seurantakohteita ovat tietoturvapoikkeamat ja tietoturvatoiminta sekä niissä tapahtuneet muutokset. Näille voidaan mitata absoluuttisia arvoja ja siten seurata tietoturvatason kehittymistä.

Luotua mittaristoa voidaan täydentää toiminnan ja tietoturvallisuuteen vaikuttavien tekijöiden mitaamisen kehittymisen myötä. Esimerkiksi auditointitoiminnan kehittyes-

sä voidaan seurantaan lisätä tehdyt auditoinnit kohteittain (tietojärjestelmät, verkot, operaattorin palvelut, jne).

Tapahtuneet tietoturvapoikkeamat. Tavoitteena on seurata ja mitata toiminnalle aiheutuvaa haittaa ja hankkia tietoa tietoturvatoimenpiteiden suunnittelua varten.
- ilmoitetut/tietoon tulleet toimenpiteitä vaatineiden tietoturvatapahtumien lukumäärä
- vahinkojen määrä (esim. sähköposti- ja tietoliikennepalvelujen ja muiden toiminalle kriittisten järjestelmien keskeytysten pituudet ja lukumäärä)
- virus- ja muut haittaohjelmavahingot ja torjuntaprosentti
- tietoverkon poikkeukselliset kuormitustilanteet
- raportoitujen tietoturvarikkomusten luonne ja määrä
- varkauksien lukumäärä.

Tietoturvapoikkeamien hallinta. Tavoitteena on seurata toteutettujen tietoturvatoimenpiteiden tehokkuutta.
- havaitut virus- ja muut haittaohjelmat
- havaitut (esim. palomuuriin pysähtyvät) tunkeutumisyritykset
- havaitut palveluksen estohyökkäykset
- roskapostitilanne
- toteutetut torjuntaohjelmien päivitykset
- toteutetut tietoturvapäivitykset
- tietoliikenneyhteyksien kapasiteetti ja käytettävyys
- epäonnistuneiden tunkeutumisyritysten lukumäärä järjestelmiin.

Tietoturvatoimintaa kuvaavia mittareita. Tavoitteena on arvioida tietoturvatoiminnan tehokkuutta seuraamalla suoritteita ja käytettyjä panoksia.
- tietoturvatoiminnan kustannukset (kehittäminen, operatiivinen toiminta, investoinnit)
- tietoturvallisuustyön työtunnit tai henkilötyöpäivät
- tietoturvaryhmän kokousten lukumäärä
- tietoturvakoulutuksen koulutuspäivien ja/tai opetustuntien määrä, osallistujalukumäärä
- henkilöstölle suunnattujen tiedotteiden lukumäärä
- tietoturvasopimusten lukumäärä ja luonne
- tietoturvakatselmointien lukumäärä kohteittain
  - tietojärjestelmien tietoturvasuunnitelmat (toipumissuunnitelmat)
  - henkilöstöturvallisuus
  - käyttöoikeudet
  - tietoaineistot (suojaus, varmistukset, laatu)
  - operaattorin palvelut

- toimitilat
- tietoliikenne ja verkot
- laitteet
- määriteltyjen prosessien mukainen toiminta
- suunnitelmat ja ohjeet ml. jatkuvuus- ja valmiussuunnitelmat
- vastuut, delegoinnit
- tietoturvasopimukset
- riskikartoituksen ajantasaisuus

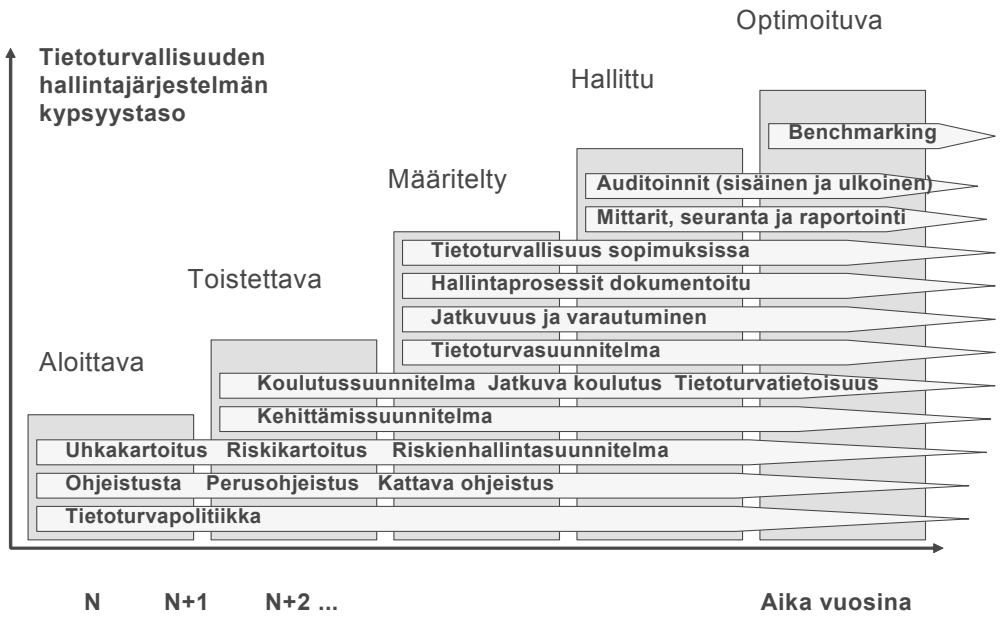
Käytännössä katselmointien suorittaminen edellyttää katselmointien hajauttamista useammalle vuodelle ja niiden kytkemistä ja ajoittamista vuosisuunnitelmiin (vuosikello).

Tietoturvallisuuden mittaamista voidaan tehdä tulostavoitteita vasten, jolloin erikseen mitataan kehittämistavoitteiden toteutumista, tietoturvapoikkeamia ja toiminnan tehokkuutta. Lisäksi organisaation tulee vuosittain arvioida tietoturvallisuuden hallintajärjestelmänsä kypsyysaste ja kehityssuunnitelma, kunnes haluttu tavoitetaso on saavutettu.

Kokemukset organisaatioista, joissa tieturvallisuuden hallintajärjestelmä on pitkälle kehittynyt, antavat kuvaa, että hallintajärjestelmän muodostamisvaiheessa mittareita ja arviointeja on suhteellisen runsaasti, mutta tietoturvatoiminnan kehittyessä ja vakiintuessa mittarien määrää voidaan vähentää. Mittarit vaativat osaltaan jatkuvaa arviointia ja kehittämistä, jotta voidaan varmistua niiden hyödyllisyydestä ja tarkoituksenmukaisuudesta. Muutokset tietoturvallisuuden toimintaympäristössä osaltaan edellyttävät mittarien ja arviointimenetelmien jatkuvaa ajantasaistamista.

5 CASE -ESIMERKKEJÄ VALTION-HALLINNON ORGANISAATIOISTA

Seuraavissa esimerkeissä on kuvattu kypsyysmallin soveltamista käytännössä. Niissä on esimerkin omaisesti kuvattu ne elementit, joita kussakin kehitysvaiheessa tulisi sisällyttää tietoturvallisuuden hallintajärjestelmään. Lopullinen päätös mukaan otettavista komponenteista tai niiden järjestyksestä tulee tehdä organisaatiokohtaisesti.



Kuva 5.1. Kokemusperäinen kypsyysmalli

5.1 Esimerkki 1: Virasto, joka on tunnistanut tietoturvallisuuden kehittämistarpeen

Lähtötilanne

Tietoturvatyön alkaessa virastossa ei ollut nimettyä tietoturvallisuuden vastuuhenkilöä eikä tietoturvatyötä muutenkaan organisoitu. Teknisiä tietoturvaparannuksia oli tehty, mutta ne olivat irrallisia jonkin yksityiskohdan parantamiseen tarkoitettuja toimia. Tietoturvallisuus ei ollut mitenkään erityisesti ollut esillä projekteissa, eikä tietoturvakonsultteja oltu käytetty hankkeissa.

Virasto oli laatinut tietoturvapolitiikan vuosia sitten, mutta sitä ei oltu virallisesti hyväksytty eikä se ollut henkilökunnan tiedossa. Juuri muutakaan tietoturvaohjeistusta ei ollut olemassa, joitakin ohjeita oli laadittu otettaessa käyttöön esim. etäkäyttöratkaisuja, mutta kattavaa ohjepakettia ei ollut olemassa.

Kehittämistyön käynnistyminen

Virasto aloitti tietoturvallisuuden kehittämisen solmimalla yhteistyösopimuksen hallinnonalan muiden virastojen kanssa. Toiseen hallinnonalan virastoon palkattiin tietoturvapäällikkö, jonka ajankäytöstä tehtiin sopimus. Sopimuksen mukaan tietoturvapäällikkö voisi käyttää 10% työajastaan viraston tietoturvatehtäviin.

Viraston tietoturvatilannetta selvitettiin VMn yhteishankkeen puitteissa, johon virasto pääsi mukaan jälki-ilmoittautuneena hankkeen jo alettua. Hankkeen puitteissa suoritettiin tietoriskien kartoitus, josta ilmeni että tekninen tietoturvallisuus oli joiltain osin varsin hyvässä kunnossa ja siihen oli panostettu, mutta hallinnollisen turvallisuuden osa-alueilla ei oltu tehty juuri mitään parannustoimia. Suurimmat puutteet näyttivät olevan henkilökunnan tietoturvatietoisuudessa ja osaamisessa.

Tietoturvapäällikkö aloitti laatimalla tietoturvapolitiikan sekä tietoturvasuunnitelman riskikartoituksen tulosten ja avainhenkilöiden haastatteluiden perusteella. Tietoturvasuunnitelmassa kuvattiin tietoturvallisuuden nyky- ja tavoitetilat sekä laadittiin kehitysohjelma kuluvalle ja seuraavalle vuodelle. Dokumenttien valmisteluun kului puolisen vuotta, koska erityisesti tietoturvasuunnitelmaa kommentoitiin laajasti. Ko. ajan jälkeen dokumentit hyväksyttiin viraston johtoryhmässä ja johto sitoutui tietoturvallisuuden kehittämiseen ja sen tavoitteisiin.

Samoihin aikoihin virastossa laadittiin tietohallintostrategiaa, jossa tietoturvallisuuden merkitys tiedostettiin toiminnan kannalta tärkeänä. Virastossa käynnistyi myös riskienhallintaprojekti, jossa kartoitettiin lähinnä viraston varsinaiseen operatiiviseen toimintaan liittyviä riskejä. Kartoituksessa tuli esille joitakin tietoon liittyviä avainriskejä, jotka toteutuessaan voisivat vaikuttaa koko viraston toimintaan lamauttavasti.

Tietoturvallisuutta oli tähän asti pidetty lähinnä teknisenä asiana, joka oli tietohallinnon hoidossa, mutta politiikkatason dokumenttien laatimisen suurimpana vaikutuksena

voidaan pitää sitä, että tietoturvallisuus saatiin miellettyä koko organisaation tavoitteeksi, ei pelkästään tekniseksi asiaksi.

Em. ohjeiden lisäksi laadittiin mm. sähköposti- ja tietoverkkopolitiikka, jossa huomioitiin vuonna 2004 muuttunut lainsäädäntö, sekä käyttäjän ohjeistusta, mm. tietoturvan huoneentaulu. Uusista ohjeista myös tiedotettiin aktiivisesti intranetissä.

Ohjeistus ja kouluttaminen olivat olleet mukana yhteishankkeen tavoitteissa, mutta niitä ei saatu toteutettua hankkeen aikataulussa. Edistymistä kuitenkin tapahtui, perusohjeistus oli valmiina noin vuosi työn käynnistämisen jälkeen, jonka jälkeen käynnistettiin tietoturvakoulutus. Koulutuspaketti suunniteltiin niin, että koko henkilökunnalle tarjottiin 2 tunnin mittainen tietoturvakoulutus, joka sisälsi yleisen tietoturvakoulutusosuuden ja sen lisäksi opastuksen organisaation omiin ohjeisiin ja käytäntöihin. Noin puolitoista vuotta työn aloittamisen jälkeen koulutuskokonaisuus oli tehty ja koulutuksen oli käynyt läpi 50% koko talon useasta sadasta henkilöstä, joiden toimipisteet sijaitsevat maantieteellisesti hajallaan.

Organisaatioon perustettiin tietohallinnon johtoryhmä, joka toimii myös tietoturvaryhmänä, tältä osin tietoturvatyö oli tosin vasta lähdössä käyntiin.

Yhteenveto

Suurimpana parannuksena voidaan pitää tietoturvatietoisuuden lisääntymistä ja turvatason parantumista tätä kautta. Kehittämisohjelmaan sisällytetyistä toimista osa on toteutunut, osaa ei ole edes aloitettu. Jatkossa tulisi panostaa erityisesti toiminnan jatkuvuuteen liittyviin kehittämistoimiin. Valmiusasioita on suunniteltu, mutta niidenkin käsittelyssä on tietojärjestelmät jääneet vähäiselle huomiolle. Toiminnan jatkuvuuteen liittyviä toimia normaaliajan häiriötilanteissa ei ole tehty, ei myöskään laadittu toipumissuunnitelmia tietojärjestelmiin kohdistuvia häiriöitä varten.

Myös henkilöstö- ja toimitilaturvallisuudessa tapahtui muutoksia kehittämistyön aikana - joko riskikartoituksen tai tietoturvasuunnitelman käynnistämänä tai niistä riippumatta. Henkilökunnalle hankittiin kuvalliset henkilökortit, lukituksia tarkistettiin ja ulkopuolisten liikkumista toimitiloissa rajoitettiin. Organisaation hajanaisuudesta johtuen toimet eivät ole toteutuneet kaikissa yksiköissä ja esim. henkilökorttien käyttö on aiheuttanut paljon vastustusta erityisesti pienemmissä yksiköissä. Ehkä näihin liittyvät riskit on nyt kuitenkin paremmin tiedostettu. Myös salassapitositoumuksia on laadittu sekä oman ylläpitohenkilökunnan että ulkoisten yhteistyökumppaneiden ja konsulttien kanssa.

Tehtyjen parannus- ja kehittämistoimien perusteella organisaation kypsyystason voidaan arvioida olevan tasolla yksi, kun se lähtötilanteessa oli nollatasolla.

Tulosohjaukseen tietoturvallisuutta ei ole vielä kytketty mitenkään mukaan, mutta hallintajärjestelmän muotoutuminen antaa kuitenkin valmiudet kytkentään myöhemmin kun viraston johto näkee sen tarpeelliseksi.

Seuraavassa kehitysvaiheessa pitää uusia tietoriskien kartoitus ja sen pohjalta päivittää tietoturvasuunnitelma vastaamaan olemassa olevaa tilannetta. Kehitystyön edetessä suun-

nitelma ei kaikilta osin ole enää pysynyt ajan tasalla, koska parannustoimia on jo suoritettu. Myös ohjeistusta pitää edelleen lisätä ja parantaa sekä kehittää tietoturvallisuuden raportointia ja seurantaa. Myös tietojärjestelmäkehityksen tietoturvallisuus sekä sopimuskumppanien valinta ja sopimuksiin liittyvät tietoturva-asiat kaipaavat lisäpanostusta.

5.2 Esimerkki 2: Hallintajärjestelmän kehittäminen on käynnistynyt

Esimerkki 2 on ministeriöstä, joka on lähtenyt kehittämään tietoturvapolitiikkaa ja tietoturvastrategiaa. Se kuvaa tietoturvapolitiikan mukaisen tietoturvamenettelyjen käyttöönottoa hallinnonalalla. Työ on edennyt kypsyysmallin toiselle tasolle.

Lähtötilanne

Organisaation tietoturvallisuuden hallintajärjestelmän kehittämisen aloitustilanteessa vuonna 2004 tehtävään käytettiin tietohallinnon virkamiehiä sekä konsulttia.

Lähtötilanteen ongelmiksi todettiin vastuuttamisen puutteet, toiminnan epäjatkuvuus, tietojen vanhentuminen, ohjeiden hajanaisuus sekä kehityssuunnitelmien puuttuminen koskien varsinkin hallinnollista ja organisatorista turvallisuutta. Teknisen turvallisuuden osalta ongelmiksi todettiin tietojen luvaton käyttö, sähköpostinhallinta ja virustorjunta, projektitoiminnan virhearviot sekä ratkaisujen hallintatapojen erilaisuus, lisenssihallinnan ongelmat, toimittajiin ja alihankkijoihin liittyvät riskit, oman henkilökunnan toiminta (vaihtuvuus, varomattomuus, fyysiset uhat), huolimaton ja asiaton tehtävien hoito.

Kehittämistoimenpiteet

Ensimmäisinä tehtävinä oli määritellä organisaation tietoturvapolitiikka, luoda käyttäjien tietoturvaohjeistus, synnyttää tietoturvallisuuden hallintamalli ja hallintamallia hyväksikäyttäen tietoturvastrategia. Strategiassa määriteltiin hallinnonalan yleiset tietoturvauhat sekä riskit. Hallinnollisen ja organisatorisen turvallisuuden kehittämiseksi tunnistettiin tietoturvallisuuden toteutumista ja kehittämistä tukevat prosessit:

- johtaminen
- kokonaisturvallisuuden johtaminen ja hallinta
- tietoturvastrategian ja virastojen tietoturvasuunnitelmien laadinta
- riskien kartoitus
- ohjeiden tuottaminen ja laadinta
- tietoturvatapahtuma hallinta
- tietoturvatoimenpiteet.

Teknisen tietoturvallisuuden kehittämiseksi määriteltiin vastaavat prosessit huomioiden tietohallinnon asema ja tehtävät hallinnonalalla.

Hallintamallin ja prosessimäärityksien pohjalta määriteltiin tarvittavat tietoturvatoi-

menpiteet. Tietoturvallisuuden suhteen keskeisinä toimenpiteinä nähtiin:
- vastuuttaminen ja organisointi hallinnonalalla
- ohjeistuksen kehittäminen
- virastokohtaisten uhka- ja riskikartoitusten teko
- virastokohtaiset tietoturvasuunnitelmat
- toiminnan vaatimusten mukaisuus
- valvonnan kehittäminen
- tietoturvatapahtumiin liittyvän toiminnan kehittäminen
- kehittämisen vaiheistus
- koulutus
- hankintaan, ulkoistuksiin ja sopimuksiin liittyvät asiat
- projektityön ja järjestelmänkehityksen tietoturvallisuus.

Yhteenveto
Hallinnonalan virastot ovat nimenneet tietoturvavastaavansa syksyllä 2005. Tietoturvallisuuden koulutus on aloitettu kouluttamalla nämä henkilöt tavoitteena saada aikaan ensin virastojen uhka- ja riskikartoitukset sekä vuonna 2006 virastojen uudet tietoturvasuunnitelmat. Tukiorganisaationa käytetään tietohallinnon omaa organisaatiota ja varsinkin alueellisia tukihenkilöitä. Erityisenä ongelmana tässä on organisaation laajuus: esim. virastojen tietoturvavastaavien koulutukseen osallistuu noin 250 henkilöä.

Virastojen tietoturvasuunnitelmien valmistumisen jälkeen kehitetään tietoturvan raportoinnin järjestelmä, jonka kautta pystytään seuraamaan toiminnan jatkuvuutta, suunnitelmissa asetettujen tavoitteiden toteutumista vuosi- ja TTS-tasolla, organisatorista toimivuutta sekä tietoturvan resursoinnin kehittymistä.

Teknisen turvallisuuden osalta on edetty tietoliikenneverkon turvallisuuden kehittämisessä sekä etäkäytön edellyttämien turvaratkaisujen kehittämisessä.

5.3 Esimerkki 3: Virasto, jossa hallintajärjestelmä on käytössä

Esimerkki 3 on virastosta, joka on lähtenyt kehittämään systemaattisesti tietoturvallisuuden hallintajärjestelmää ja edennyt kehitystyössä kypsyysvaiheeseen toiselle ja osin kolmannelle tasolle.

Lähtötilanne
Organisaation tietoturvallisuuden hallintajärjestelmän kehittämisen aloitustilanteessa ei ollut henkilöä, joka olisi vastannut tietoturvallisuudesta ja sen toimeenpanosta systemaattisesti. Tehtävään käytettiin osittain konsulttia.

Organisaatio aloitti tietoturvan haltuunoton ja kehittämistyön rekrytoimalla henkilön tietoturvapäällikön tehtävään. Rekrytoinnin jälkeen selvitettiin organisaation tilanne ja

todettiin, että tietoturvallisuus oli hajanaista, muutama ohje sähköpostin ja Internetin käytöstä sekä salasanoista ja tietojärjestelmän pääkäyttäjän tehtävistä. Laadittu riskikartoitus ei tukenut tietoturvallisuutta vaan oli katsauksenomainen muistio organisaation tilanteesta ilman kehittämisohjelmaa. Organisaatio oli aloittanut tietoturvapolitiikan, kehittämissuunnitelman ja ohjeiston (tietoturvasuunnitelma) laatimisen. Nämä työt olivat kesken.

Tietoturvallisuuden hallinta oli reaktiivista. Henkilöstön kouluttaminen ei ollut käynnistynyt. Tietoturvallisuutta ei nähty menestystekijänä eikä ymmärretty sen tukiroolia organisaation perustehtävän suorittamiselle. Organisaation turvallisuusjohtoryhmän toimintaa leimasi tavoitteiden puuttuminen.

Tietoturvallisuuden johtamis- ja hallintajärjestelmän kehittämistyön käynnistyminen

Organisaation tietoturvapäällikkö aloitti laatimalla tietoturvapolitiikan sekä käynnistämällä riskikartoituksen. Tietoturvapolitiikan valmisteluun meni yhdeksän kuukautta.

Tietoturvapolitiikan valmistelun rinnalla valmisteltiin ohjeistusta ja organisaation toiminnan jatkuvuuteen liittyviä suunnitelmia. Tietoturvapäällikön ensimmäinen vuosi meni myyntitehtävässä. Organisaatioon perustettiin tietoturvaryhmä.

Kahden vuoden aikana keskeiset perusohjeistukset saatettiin tyydyttävälle tasolle. Sitoutuminen tietoturvallisuuden kehittämisohjelmaan oli vaisua, josta johtuen ohjelman aikataulu ei pitänyt.

Johto linjasi tavoitteeksi sitoutumisen standardien mukaisiin hallintajärjestelmiin.

Muutoksen hallinta osoittautui haasteeksi. Esimerkiksi turvaluokitellun tiedon käsittelyohje koettiin toiminnan kannalta hankalaksi ja vaikeasti käyttöönotettavaksi, syynä olivat tarvittavat hankinnat ja henkilöstön sitoutuminen tietoturvallisiin toimintatapoihin. Vastaavia haasteita oli henkilöstöturvallisuusasioissa.

Kolmen vuoden aikana saavutettiin merkittäviä tuloksia turvallisuussopimuksissa palveluiden toimittajien kanssa, järjestelmien turvakuvausten käyttöönotossa ja järjestelmien kehittämistyöhön liittyvän järjestelmäkehityksen tietoturvaohjeissa. Tarjouspyynnöissä alettiin vertailla toimittajien tietoturvaratkaisuja sekä antaa niille entistä suurempi painoarvo valintoja tehtäessä. Organisaation edellyttäessä turvallisuutta myös palveluiden ja järjestelmien toimittajat rupesivat tarjoamaan ratkaisuja.

Henkilöstön tietoisuutta lisättiin kampanjoimalla ja ottamalla käyttöön sisäverkossa oleva sähköinen tietoturvaopas. Tietoisuuskasvatuksen runko-ohjelma on laadittu kolmelle vuodelle jonka jälkeen mitataan henkilöstön osaamista eri testeillä.

Tietoturvallisuuden arviointiin liittyvien mittarien laatiminen on ollut osa organisaation governance -mallinnusta ja se on saanut merkittävästi vauhtia ulkopuolisen konsultin esitettyä asian. ICT -strategiassa on päätetty pitää turvallisuusasiat omassa hallussa.

Laadittaessa riskienhallintapolitiikkaa on organisaation johto alkanut hiljalleen näkemään turvallisuusasiat ja sisäisen valvonnan laatuna. Samalla on aidommin alettu sitoutua turvallisuuden kehittämisjärjestelmään ja osoitettu varoja puutteiden korjaamiseen.

Yhteenveto
Tulosohjauksen kannalta organisaation kypsyyttä voidaan ajatella aikajänteellä 2002 - 2005 siten, että muutosta on tapahtunut ja prosesseja on kuvattu sekä haettu toimintamalleja, joihin sitoudutaan. Kypsyysmallissa ollaan tasolla kaksi ja lähestymässä tasoa kolme.

Tietoturvaryhmä on koulutettu tekemään sisäisiä auditointeja BS7799 pohjalta ja pari pidettyä harjoitusta ovat osoittaneet ryhmän toimivan tyydyttävästi.

Tietoturvallisuuden raportointi on saatu toimimaan ja johto saa kerran kuukaudessa kattavan tilannekuvan tapahtumista sekä kolmannesvuosittain ajankohtaiskatsauksen organisaation turvallisuustilanteesta. Tapahtumat ovat tuoneet selvästi esiin toimintaprosessien puutteita.

Suurin panostus on tehty käytössä olevien ja uusien käyttöön otettavien tietojärjestelmien auditointiin niiden tietoturvallisuuden tason todentamiseksi sekä parannuskohteiden paikallistamiseksi. Toimittajat ovat saaneet auditoinneista selvää palautetta oman laatujärjestelmänsä kehittämiseksi.

Kun organisaatio on ratkaissut kaikki edellä kuvatut huonosti olevat asiat ja tehnyt uuden uhka-analyysin ja riskienhallintasuunnitelman voidaan kypsyystasoa nostaa lähemmäs seuraavaa tasoa. Voidaan arvioida, että tähän tarvitaan kaksi vuotta.

5.4 Esimerkki 4: Virasto, jossa tietoturvallisuuden hallintajärjestelmä on ollut käytössä useita vuosia

Esimerkki 5 on virastosta, joka on kehittänyt systemaattisesti tietoturvallisuuden hallintajärjestelmää jo usean vuoden ajan.

Lähtötilanne
Virastossa on jo ennen tietoturvallisuuden hallintajärjestelmän kehittämisvaihettakin panostettu tietoturvallisuuteen ja tietosuojaan. Virastossa on ollut sekä tietoturvapäällikkö että tietosuojan vastuuhenkilö jo ennen tietoturvallisuuden hallintajärjestelmän systemaattista kehittämisvaihetta.

Tietoturvallisuuden hallintajärjestelmän luomiseen käytettiin ulkopuolista konsulttia , jonka ohjauksessa viraston tietoturvapäällikkö valmisteli tietoturvapolitiikan, suunnitteli hallintajärjestelmän prosessit ja tuotti tietoturvallisuuden ohjeistusta. Tietoturvallisuuden hallintajärjestelmä oli valmis vuonna 2002, josta lähtien virastossa on kehitetty hallintajärjestelmää, ohjeistusta sekä prosesseja edelleen. Virastossa tietoturvallisuus ymmärrettiin jo lähtötilanteessa viraston kannalta merkittäväksi asiaksi ja johdon tuki on ollut olemassa koko ajan.

Tietoturvallisuuden johtamis- ja hallintajärjestelmän käyttäminen

Organisaatiossa luotiin aluksi tietoturvapolitiikka, tietohallinto- ja tietoturvastrategiat. Tietoturvapolitiikkaa on tarkasteltu määräajoin ja on sovittu, että tietoturvapolitiikka tarkistetaan samassa yhteydessä kun viraston tietohallinto- ja tietoturvastrategiaakin päivitetään.

Virastossa hallintajärjestelmän käyttöönottovaiheessa tietoturvapäälliköllä oli paljon sellaisia vastuita, jotka olisivat kuuluneet toiminnasta vastaaville yksiköille. Organisaatiossa on päivitetty hallintajärjestelmän prosesseja siten, että yhä enemmän tietoturvapäällikön vastuulla olleita tehtäviä (esimerkiksi riskikartoituksen toimeenpanoa) on vastuutettu kullekin toiminnasta vastaavalle yksikön johtajalle. Käytännössä tietoturvallisuuden johtaminen on saatu osaksi viraston ja yksiköiden johtamisprosesseja. Tietoturvapäällikön rooli on muuttunut siten, että tietoturvapäällikkö tuo tietoturvallisuuden hallintaan menetelmiä ja toimii asiantuntijana.

Hallintajärjestelmän alkuvaiheessa virastolle luotiin paljon ohjeistusta. Ohjeistusta oli liikaa ja se oli osittain päällekkäistä. Virastossa on parin vuoden aikana käyty läpi koko hallintajärjestelmän aikana luotu ohjeistus. Läpikäynnin yhteydessä poistettiin tarpeettomat ja päällekkäiset ohjeet sekä ohjeille haettiin omistajat, jotka vastaavat siitä, että heidän vastuullaan olevat ohjeet ovat ajan tasalla. Suuri osa ohjeista siirtyi tietoturvallisuuden vastuualueelta muille yksiköille. Tietoturvallisuuden vastuualueelle jäi mm. seuraavat ohjeet: tietoturvapolitiikka, tietoturvastrategia, tietoturvatapahtumien reagointiohje, tietoturvallisuuden mittaamisohje sekä muutama hallintajärjestelmän prosesseihin liittyvä ohje. Tietoturvallisuuden vastuualueen yhtenä tehtävänä on tarkastaa sisäisen tarkastuksen yhteydessä, että ohjeet ovat ajantasaisia ja kattavia.

Tietoturvatapahtumien ilmoittaminen on myös uudelleen organisoitu. Yleisenä periaatteena on, että jokaisen työntekijän tulee tehdä ilmoitus viraston intranetissä olevalla ilmoituslomakkeella havaitsemistaan tietoturvatapahtumista. Yleisen ilmoittamisvelvoitteen lisäksi olemme sopineet eri toiminta-alueille omat vastuuhenkilöt, jotka ilmoittavat ko. alueen tapahtumat em. ilmoituslomaketta käyttäen. Virastossa seurataan aktiivisesti tietoturvatapahtumia sekä reagoidaan niihin.

Virastossa toimii tietoturvaryhmä, jossa on edustaja jokaisesta toimintayksiköstä sekä jäseniä erityisalueilta. Tietoturvaryhmän tarkoituksena on kehittää viraston tietoturvallisuutta sekä jakaa tietoturvallisuustietoutta laajasti virastossa. Ryhmä kokoontuu joka toinen kuukausi käsittelemään mm. tietoturvatapahtumia sekä sopimaan yhteisistä tietoturvallisuuden toimintatavoista ja kehittämiskohteista.

Virastossa tehdään nykyisin yksikkökohtaisten riskikartoitusten lisäksi tietojärjestelmien kehittämisprojektien yhteydessä projektin riskienhallinnan lisäksi tietojärjestelmien riskienarviointia.

Toimintoja ulkoistettaessa tietoturva- sekä jatkuvuusvaatimukset ovat osa tarjouspyyntöä. Hankintavaiheessa arvioidaan toimittajien tietoturvaratkaisut. Palvelun käytön aikana puolestaan seurataan, onko toimittaja tuottanut sovitun tasoista palvelua. Virastol-

la on käytössä myös sanktiomenettely, ellei palvelu täytä sovittuja vaatimuksia.

Sisäisten tarkastuksien ja henkilöstön tietoisuusmittausten yhteydessä on todettu, että viraston henkilöstö on hyvin tietoturvatietoista. Henkilöstön tietoisuus on korkealla tasolla viraston luonteestakin johtuen. Pienessä virastossa on helppo myös saada asioita esille. Virastossa on joka vuosi kaksi tietoturvakoulutusta ajankohtaisista tietoturva-asioista.

Yhteenveto

Tulosohjauksen kannalta organisaation kypsyyttä tarkasteltaessa aikajänteellä 2002 - 2005, on kehitystä tapahtunut paljon. Tietoturvallisuuden prosesseja on parannettu ja tietoturvallisuuden johtaminen on tullut osaksi viraston johtamista. Tästä on ollut seurauksena, että johto on sitoutunut tietoturvallisuuden hallintaan yhä paremmin. Kypsyysmallilla arvioituna virasto on tasolla 4.

Tietoturvaryhmä toimii aktiivisesti tietoturvallisuuden kehittämiseksi ja tietoisuuden lisäämiseksi. Tietoturvaryhmä osaa tehdä sisäisiä tarkastuksia ja osa ryhmästä myös riskikartoituksia.

Tietoturvallisuuden raportointi toimii ja virasto raportoi myös ministeriön johdolle merkittävimmät tietoturvallisuuden tapahtumat. Tietoturvatapahtumiin reagoidaan nopeasti. Tietoturvallisuuden mittaaminen nousee esille ISO/IEC FDIS 27001 ja ISO/IEC 17799 tietoturvastandardeissa. Tietoturvallisuuden on kyettävä osoittamaan johdolle, että suojamekanismit toimivat. Tästä syystä virastossa on tarkasteltu tietoturvallisuuden mittareita uudelleen ja vuosi 2006 näyttänee uusien mittareiden toimivuuden.

5.5 Esimerkki 5: Tietoturvallisuus ylimmällä kypsyystasolla

Tarkastelun piirissä olleista virastoista pisimmälle tietoturvallisuuden kehittämisessä edenneet, ovat kypsyysmallilla arvioiden tasolla 4. Käytännön esimerkkiä ei ole siten esittää tasolla 5 toimivasta virastosta. Käytännössä tason 4 saavuttaminen on pääosalle virastoista riittävää.

Mitä sitten taso 5 toisi tullessaan, siitä saa käsityksen kypsyysmallia käsittelevistä julkaisuista. Seuraava kuvaus perustuu julkaisuun Miten tuotan IT:llä arvoa liiketoiminnalle? Hyvän tiedonhallintatavan - it governancen - arviointi ja kehittäminen (Helsingin kauppakorkeakoulu, Sarja B 172).

Organisaatiossa on pitkälle viety ja kehittyvä yhteisymmärrys tietoturvamenettelyistä. Menettelyt ovat kiinteässä yhteydessä organisaation noudattamiin hallintamenettelyihin (Corporate Governance). Tehtävien hoitamiseksi käytetään edelläkäyviä menetelmiä ja teknologioita sekä tehtäviä automatisoivia työkaluja käytetään optimoidulla tavalla tehokkuuden ja laadun parantamiseksi. Tietoturvaprosesseihin liittyvät ongelmat ja poikkeamat tunnistetaan ja analysoidaan tehokkaasti ja nopeasti liiketoimintariskien pitämiseksi hyväksytyllä tasolla. Menettelyt ovat joko parhaiden käytäntöjen tasolla tai niitä vastaa-

via. Lisäksi ne ovat organisaation ylimmän johdon hyväksymiä, määritellyn strategian mukaisia ja toimialan parhaisin käytäntöihin verrattuja. Menettelyä on toistettu jatkuvan paranatamisen periaatteella vähintään viisi vuotta.

5.6 Esimerkki raportointimenettelyistä ja raportoinnin sisällöstä

Esimerkki on virastosta, jossa on käytössä vakiintuneet tietoturvallisuuden raportointimenettelyt ja raportit.

Tausta

Ensimmäinen tietoturvallisuuspolitiikka hyväksyttiin virastossa vuonna 1994. Samaan aikaan laadittiin myös atk-valmiussuunnitelma ja atk-toipumissuunnitelma. Niille tuli käyttöä vuoden 1996 kesällä, kun viraston kaikki toimitilat määrättiin välittömään käyttökieltoon homevaurioiden vuoksi. Riskikartoitus oli tehty ja varautumissuunnitelmat olemassa, mutta niissä ei oltu osattu ottaa huomioon totaalista toiminnan pysähtymistä silloisessa toimintaympäristössä. Suunnitelmat päivitettiin 1997 käyttöjärjestelmän vaihdon yhteydessä.

Ministeriössä aloitettiin jatkuva koko hallinnonalaa koskeva tietoturvallisuustyö 2000-luvun alussa. Vuoden 2003 loppuun mennessä määrättiin kaikki hallinnonalan organisaatiot laatimaan itselleen yhdenmukaiset tietoturvallisuuspolitiikat, tietoturvallisuussuunnitelmat ja tietojenkäsittelyn valmiussuunnitelmat. Vuoden 2005 aikana siirryttiin säännölliseen raportointiin seuraavan mallin mukaisesti.

Hallinnonala tietoturvallisuusraportointi

Hallinnonalalla on otettu käyttöön vuonna 2005 hallinnonalan tietoturvallisuuden ohjausryhmän luoma yhtenäistetty Tietoturvallisuus-raportointi. Raportointi on osa hallinnonalan turvallisuustoimintaa.

Organisaatiokohtainen tietoturvallisuuden raportointi muodostaa ministeriön ja virastojen johdolle koottavan tietoturvallisuusraportin perusaineiston.

Määräaikaisraportointi toteutetaan neljä kertaa vuodessa oheisen aikataulutuksen mukaisesti. Erillisraportointi toteutetaan tilanteen ja tarpeen mukaisesti ja se kattaa havaitut vakavat tietoturvallisuusrikkeet ja - rikkomukset sekä muut mahdolliset tietoturvaan liittyvät vakaviksi luokitellut vaaratilanteet tai havaitut puutteet.

Tarpeen mukaan voidaan lisäksi julkaista tietoturvallisuuteen liittyvää tilastoaineistoa neljännesvuosi-, puolivuosi- tai vuosijaksoittain.

Hallinnonalan ylimmälle johdolle suunnattu tietoturvallisuusraportti ja hallinnonalan organisaatioiden (ministeriön osastot, virastot ja laitokset) raportit laaditaan seuraavaa tietoturvallisuusraportin runkoa pohjana käyttäen.

Virasto/laitos/osasto XX:n tietoturvallisuusraportti III/2005 (1.8. - 31.10.2005)

1. Tiivistelmä

Tähän kohtaan raporttia raportoiva organisaatio kirjoittaa lyhyen ministeriön johdolle osoitetun tiivistyksen kuluneen raportointikauden keskeisimmistä organisaation tietoaineiston, tietojärjestelmien ja tietoliikenneyhteyksien **käytettävyyteen, eheyteen tai luottamuksellisuuteen** vaikuttaneista uhkista, tapahtumista sekä niihin liittyvistä toimenpiteistä.

Esimerkki: *Raportointikaudella virastoon xx on perustettu tietoturvatoimiala ja tietoturvapäällikön tehtävä. Tietoturvastrategian uusiminen on käynnistetty ja tietoturvallisuuskartoitus toteutettu. Raportointikaudella havaittiin yksi epäilty tietomurtoyritys operatiiviseen tietojärjestelmään. Asia on saatettu poliisitutkintaan. Normaalia useammat tietoliikennekatkokset on huomioitu laatupalavereissa sekä varmentavien yhteyksien suunnittelussa. Virastossa on otettu käyttöön virkamiehen asiointikortti sekä kertakirjautuminen kahden järjestelmän osalta.*

2. Raportoitavat tietoturvallisuuden osa-alueet

Raportissa noudatetaan valtioneuvoston (VN) tietoturvallisuuspäätöksen mukaista tietoturvallisuuden jaottelua: hallinnollinen, henkilöstö-, fyysinen, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus.

Jokainen edellä mainituista tietoturvallisuuden eri osa-alueista on huomioitava raportissa (väliotsikot kirjoitettava raporttiin) aina, vaikka kyseisen väliotsikon alle ei asianomaisen kauden aikana olisi tullut mitään raportoitavaa.

2.1 Hallinnollinen tietoturvallisuus

Esimerkki: *Raportointikaudella virastoon xx on muodostettu uusi tietoturvallisuustoimiala ja sen johtoon on nimetty tietoturvallisuuspäällikön tehtävänimikkeellä xx yy. Virastossa on käynnistetty toimenpiteet olemassa olevan tietoturvallisuusstrategian uusimiseksi. Työ pitää esitellä viraston johdolle syksyllä 2005.*

2.2 Henkilöstöturvallisuus

Esimerkki: *Raportointikaudella virastossa xx havaittiin avainhenkilöriski viraston ulkoisiin yhteyksiin liittyvien palomuurien hallinnassa. Vuosilomista ja äkillisistä yhtäaikaisista sairastumisista johtuen palomuurien hallintaan koulutettuja ja kykeneviä henkilöitä ei ollut saatavilla. Toimenpiteet lisähenkilöstön kouluttamiseksi ja perehdyttämiseksi on aloitettu. Raportointikaudella havaittiin yksi epäilty tietomurtoyritys operatiiviseen tietojärjestelmään. Tapahtuma on saatettu poliisitutkintaan.*

2.3 Fyysinen turvallisuus

Esimerkki: *Raportointikauden aikana virastossa xx toteutettiin kaikkiin toimipisteisiin ulottuva fyysiseen turvallisuuteen liittyvä riskikartoitus. Keskeisimpänä havaintona todettiin osin puutteelliset kulunvalvontajärjestelyt. Kartoituksen tulokset käsitellään tarkemmin tietoturvallisuuden kokonaisriskianalyysissä seuraavalla raportointikaudella.*

2.4 Tietoliikenneturvallisuus

Esimerkki: *Raportointikaudella viraston sisäisillä tietoliikenneyhteyksillä oli huomattavasti normaalia enemmän pidempiaikaisia katkoksia. Katkokset aiheutuivat suurimmalta osin joko operaattorin tai kolmansien osapuolten toiminnan/toimimattomuuden seurauksena. Katkokset on otettu esille operaattorien kanssa pidettyjen laatupalaverien yhteydessä. Asiaan on luvattu parannusta. Asia tullaan myös huomioimaan kriittisimpien yhteysvälien osalta varmentavien yhteyksien suunnitteluna ja hankintana. Raportointikauden aikana saatiin lisäksi käyttöön eri toimipisteiden välisten yhteyksien salaus.*

2.5 Laitteistoturvallisuus

Esimerkki: *Raportointikaudella virastossa xx otettiin käyttöön uusittu laitteistoturvallisuuden tietoturvaohjeistus. Keskeisimpinä uusina asiakokonaisuuksina ohjeistettiin uusien oheislaitteiden liittäminen organisaation tietoliikenneverkkoihin liitettyihin työasemiin rajoituksineen. Samalla ohjeistettiin myös monitoimikopiokoneiden (kopiokone, tulostin, skanneri, telefax) sähköpostiominaisuuksien käyttö ja valvonta sekä niihin liittyvissä huoltosopimuksissa huomioitavat tietoturvallisuusasiat.*

2.6 Ohjelmistoturvallisuus

Esimerkki: *Raportointikaudella virastossa xx otettiin käyttöön kahden uuden tietojärjestelmän osalta kertakirjautumismenettely virkamiehen asiointikortin käyttöönottoon liittyen. Raportointikauden aikana saatettiin loppuun organisaatiomuutos, minkä tuloksena koko organisaation tietoturvapäivitykset eri tuotteisiin tehdään yhdestä toimipisteestä keskitetysti.*

Hallinnonalalla yhteisesti käytössä oleva xx-järjestelmä ominaisuuksineen on vaikuttanut eri järjestelmien käytettävyyteen. Järjestelmää hankittaessa ja käyttöönotettaessa ei ole riittävästi kiinnitetty huomiota xx-järjestelmän vaatimaan tietoliikennekapasiteettiin eri käyttäjämäärillä eikä käyttöönoton kiireellisyydestä johtuen sitä päästy testaamaankaan. Useamman yhtäaikaisen käyttäjän tapauksissa osa tietoliikenneyhteyksistä ruuhkautuu. Ongelmaan on pyritty saamaan alustava ratkaisu laajentamalla yhteyksien kapasiteetteja sekä priorisoimalla eri verkkojen liikennettä. Asia olisi tullut huomioida jo ko. järjestelmää kehitettäessä.

2.7 Tietoaineistoturvallisuus

Esimerkki: *Raportointikaudella virastossa xx tarkistettiin ja saatettiin ajan tasalle salassa pidettävään aineiston käsittelyyn, postittamiseen ja arkistointiin liittyvä ohjeistus. Ajantasaistamiseen liittyvä koulutus järjestetään kuluvan raportointikauden aikana. Kiireellisimmät arkistointiin ja säilytykseen liittyvät hankinnat toteutetaan vielä kuluvan vuoden aikana.*

2.8 Käyttöturvallisuus

Esimerkki: *Raportointikaudella virastossa xx otettiin sellaisenaan käyttöön VAHTI:n sähköpostiohjetta täydentävä SM:n hallinnonalan oma ohje. Ohje on laitettu organisaation intranetiin ja sen keskeisimmät asiakokonaisuudet huomioidaan sisäisessä koulutuksessa kuluvalla raportointikaudella.*

3. Tietoturvallisuushankkeet/kehittäminen

4. Varautumiseen ja valmiussuunnitteluun liittyvät asiat

5. Mahdollinen erillisraportointi

Tässä raportoidaan:
– Organisaation/organisaatioiden antamat pikaraportit
– Havaitut vakavat tietoturvarikkomukset
– Merkittävät auditoinnit jne.

6. Toimenpide-ehdotukset johdolle

7. Liitteet

Tähän voidaan lisätä taulukkoja/kuvaajatietoja esimerkiksi:
– Toteutetut haittaohjelmien torjuntaohjelmien päivitykset
– Havaitut haittaohjelmat (virukset, troijalaiset, madot ym.)
– Toteutetut tietoturvapäivitykset
– Havaitut tunkeutumisyritykset
– Havaitut palveluksenestohyökkäykset
– Tietoliikenneyhteyksien kapasiteetti ja käytettävyys
– Roskapostitilanne
– Sekä tarvittaessa vielä tietoturvallisuuden kvartaali-, puolivuosi- ja vuositilastot

Tilastojen perusteella tulisi pyrkiä laatimaan raportin saajalle myös lyhyt johtopäätös sekä mahdolliset toimenpiteet, joihin asiassa on ryhdytty.

Yllä mainittuja tietoja ei ole tarpeellista raportoida joka kerralla, vaan esimerkiksi puolivuosittain tai muun ilmenneen tarpeen perusteella.

LIITE 1 LÄHDELUETTELO

Tulosohjaus
1. Tulosohjauksen käsikirja, VM Julkaisuja 2/2005; http://www.vm.fi/vm/liston/page.lsp?r=96499&l=fi&menu=3865
2. Tulosohjauksen terävöittäminen. Työryhmämuistioita 9/2003. Valtiovarainministeriö, hallinnon kehittämisosasto.

Muiden VAHTI -työryhmien työ
3. Tietoturva-arvioinnit -työryhmä
4. Tietoturvaprosessit -työryhmä

Työssä huomioitavat VAHTI-julkaisut,
http://www.vm.fi/vm/liston/page.lsp?r=3246&l=fi
5. Valtion viranomaisen tietoturvallisuustyön yleisohje, VAHTI 1/2001
6. Tietoturvallisuus ja tulosohjaus, VAHTI 2/2004
7. Information Security and management by Results, VAHTI 1/2005
8. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa, VAHTI 7/2003
9. Tietoturvallisuuden hallintajärjestelmän arviointisuositus, VAHTI 3/2003
10. Valtion keskeisten tietojärjestelmien turvaaminen, VAHTI 5/2004

Muu lähdeaineisto
11. COSO-ERM viitekehys. Sisäisen valvonnan ja riskien hallinnan arviointikehikko. Ehdotus suositukseksi valtionhallinnon hyväksi käytännöksi. Valtiovarainministeriö. Julkaisuja. 2005.
12. Talousarviosäännöstö
13. Tietotekniikan turvallisuus ja toiminnan varmistaminen, PTS 1/2002
14. Tiehallinnon tietoturvallisuuden kehittämissuunnitelma, Tiehallinto 2004

15. Kari Pohjolan esitys ryhmälle, kalvosarja
16. Harri Niemen esitys ryhmälle, kalvosarja
17. Aaro Hallikaisen mittarit (SM poliisiosasto), kalvosarjat
18. Cobit-mallit 2, kalvoaineisto
19. Kypsyysmalli, SSE-CMM 2002, iso/hec 21827; Information Security Maturity Model
20. ISO/IEC 27001:2005 (BS 7799-2:2005) Information technology. Security techniques. Information security management systems. Requirements
21. ISO/IEC 17799:2005 Information technology. Security techniques. Code of practice for information security management
22. Sisäisen valvonnan ja riskien hallinnan arviointikehikko. Ehdotus suositukseksi valtionhallinnon hyväksi käytännöksi. Valtiovarainministeriö, 2005 http://www.vm.fi/vm/liston/page.lsp?r=95514&l=fi&menu=3865
23. Quality Progress, March 2001 Prosessien kypsyysastetta käsittelevät esitykset: http://cgi.qualitas-fennica.fi/artikkelit/prosessittoiminnanlahtokohtana.html http://cgi.qualitas-fennica.fi/artikkelit/kaytakypsyysasteikkoja.html
24. Savola Reijo, Sademies Anni ja Holappa Jarkko (2005): Miksi tietoturvaa tulisi mitata? Ylivuoto, 1/2005, ss. 8-11. ISBN 951-42-7636-1.
25. ISO/IEC 21827. Information Technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM), 2002.
26. Julkisten verkkopalvelujen laatukriteerit 8/2004, VMn julkaisuja, http://www.vm.fi/tiedostot/pdf/fi/85542.pdf
27. Tomi Dahlberg, Anna-Maija Karjanlahti, Hannu Kivijärvi, Pirkko Lahdelma, Seppo Sippa, Tapani Talikainen (2006): Miten tuotan IT;llä arvoa liiketoiminnalle? Hyvän tietohallintotavan - IT Governancen - arviointi ja kehittäminen. LTT-Tutkimus Oy, Helsingin kauppakorkeakoulu. Sarja B 172.

LIITE 2 LAKIVIITTEET

Laki valtion talousarviosta annetun lain muuttamisesta (217/2000)
Talousarvioasetus (1243/1992, muutos 263/2000 ja muutos 254/2004)
Laki viranomaisen toiminnan julkisuudesta (621/1999)
Asetus viranomaisen toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)
Hallintolaki (434/2003)
Valmiuslaki (1080/1991)
Henkilötietolaki (523/1999)
Sähköisen viestinnän tietosuojadirektiivi (2002/58/EY)
Laki yksityisyyden suojasta televiestinnässä ja teletoiminnan tietoturvasta (565/1999)
Sähköisen viestinnän tietosuojalaki (516/2004)
Laki sähköisestä asioinnista viranomaistoiminnassa (13/2003)
Laki yhteistoiminnasta valtion virastoissa ja laitoksissa (651/1988)

LIITE 3 VOIMASSA OLEVA VAHTI-OHJEISTUS JA -JULKAISUT

VAHTI 7/2006	Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi
VAHTI 6/2006	Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 5/2006:	Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 4/2006:	Selvitys valtionhallinnon ympärivuorokautisen tietoturvatoiminnan järjestämisestä
VAHTI 3/2006:	Selvitys valtionhallinnon tietoturvaresurssien jakamisesta
VAHTI 2/2006:	Electronic-mail Handling Instruction for State Government
VAHTI 1/2006:	VAHTIn toimintakertomus vuodelta 2005
VAHTI 3/2005:	Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005:	Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005:	Information Security and Management by Results
VAHTI 5/2004:	Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004:	Datasäkerhet och resultatstyrning
VAHTI 3/2004:	Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004:	Tietoturvallisuus ja tulosohjaus
VAHTI 1/2004:	Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006
VAHTI 7/2003:	Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 6/2003:	Opas julkishallinnon tietoturvakoulutuksen järjestämisestä
VAHTI 5/2003:	Käyttäjän tietoturvaohje Datasäkerhetsanvisning för användaren User´s Information Security Instruction
VAHTI 4/2003:	Valtionhallinnon tietoturvakäsitteistö
VAHTI 3/2003:	Tietoturvallisuuden hallintajärjestelmän arviointi
VAHTI 2/2003:	Turvallisen etäkäytön arkkitehtuuri

VAHTI 1/2003: Valtion tietohallinnon Internet-tietoturvallisuusohje
VAHTI 4/2002: Arkaluonteisten kansainvälisten aineistojen käsittelyohje
VAHTI 3/2002: Etätyön tietoturvaohje
VAHTI 1/2002: Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 6/2001: Tietotekniikkahankintojen tietoturvallisuustarkistuslista
VAHTI 4/2001: Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje
VAHTI 3/2001: Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus
VAHTI 2/2001: Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
VAHTI 1/2001: Valtion viranomaisen tietoturvallisuustyön yleisohje
VAHTI 3/2000: Tietojärjestelmäkehityksen tietoturvallisuussuositus
VAHTI 2/2000: Valtion tietoaineistojen käsittelyn tietoturvaohje (uudistettavana)
VAHTI 2/1999: Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus (uudistettavana)

Ohjeisto löytyy VAHTIn Internet-sivuilta www.vm.fi/vahti ja ohjeita saa myös tilattua hyvin edullisesti painotalo Editasta.

VAHTI

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

6/2006

TIETOTURVATAVOITTEIDEN ASETTAMINEN JA MITTAAMINEN

ISBN 951-804-622-0 (nid.)
ISBN 951-804-623-9 (PDF)
ISSN 1455-2566