KEMI-TORNION AMMATTIKORKEAKOULU

Tietoturvallisuusasetuksen (681/2010) soveltaminen palvelutoimittajan infrastruktuuri-palveluihin

Case Logica

Satu Konu

Liiketalouden koulutusohjelman opinnäytetyö
Julkishallinnon suuntautumisvaihtoehto
Tradenomi

TORNIO 2011

SISÄLTÖ

TIIVISTELMÄ

ABSTRACT

TIIVISTELMÄ

Konu, Satu. 2011. Valtioneuvoston asetuksen tietoturvallisuudesta valtionhallinnossa 681/2010 soveltaminen palvelutoimittajan infrastruktuuri-palveluihin, Case Logica. Opinnäytetyö. Kemi-Tornion ammattikorkeakoulu. Kaupan ja kulttuurin toimiala. Sivuja 57.

Opinnäytetyön keskeisempiä tavoitteita on tutkia julkishallinnon tietoturvallisuusasetusta ja sitä mitä uusia vaateita se tuo Logicalle, joka on julkishallinnon ulkoistuspalvelutarjoaja. Organisaation tulee ottaa myös huomioon Ohjeessa tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010) olevat vaatimukset koskien tietoaineistojen käsittelyä ulottaen sen myös palveluiden tarjoamiseen.

Tietoturvallisuusasetus astui voimaan 1.10.2010. Se velvoittaa viranomaiset saattamaan toimintansa ja tietojenkäsittelynsä vastaamaan asetuksessa säädettyjä perustason tietoturvavaatimuksia. Viranomaisten tulee saattaa toimintansa vastaamaan perustason vaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta eli 30.9.2013 mennessä.

Teoriatiedon hankinnassa on hyödynnetty Internettiä, Finlex:iä, VAHDIN ohjeita ja painettua kirjallisuutta. Tutkimuksen empiirinen osuus perustuu Logican tietoturvapäällikön haastatteluihin, joita on tehty kolme kevään 2011 aikana.

Tutkimus osoittaa, että Logican palveluiden tietoturvallisuustaso on hyvää perustasoa. Organisaation arvioinnin ja sen IT hallinnan läpikäynneissä kummassakin Logican nykytaso on lähes kolme eli yritys täyttää perustason vaatimukset hyvin. Perustason vaatimukset ovat tietoturvallisuusasetuksessa asetettu tavoitetaso.

Hyväksi havaittuja keinoja varmistaa palvelun laatu ja tietoturvavaatimukset ovat esimerkiksi tietoturvallisuuden johtaminen ja kehittäminen ISO/IEC 27001 -standardin mukaisesti, palveluiden tuotteistaminen ja prosessinmukaiset toimintatavat. Oleellista on huolehtia henkilökunnan riittävästä ja säännöllisestä koulutuksesta. Myös johdon sitoutuminen valittuihin toimintatapoihin on tärkeää. Opinnäytetyö on osittain salattu ja tarkoitettu vain Logican sisäiseen käyttöön.

Avainsanat: tietoturvallisuus, laatu, ITIL, ISO/IEC

ABSTRACT

Konu, Satu. 2011. Applying service providers' infrastructure services to The Government Decree on Information Security in Central Government (681/2010), Case Logica. Bachelor's thesis. Kemi-Tornio University of Applied Sciences. The field of Business and Culture. 57 pages.

The objective of this thesis is to study The Government Decree on Information Security in Central Government and the new requirements it inflicts to Logica as the service provider of the public sector. It is also noted that the organisation should take into account the requirements relating to information management outlined in the Instructions on the implementation of the decree on information security in central government (VAHTI 2/2010) and should apply these to the provision of its services.

The Government Decree on Information Security in Central Government has been effective since 1st of October 2010. It obliges authorities to achieve the reference level of the decree in their operations and data/information management. The reference level must be achieved within three years the decree came into effect, which is by 30th of September 2013. Internet, Finlex, VAHTI guidelines and a range of secondary sources were used for the formulation of this report. The empirical part of the report is based on three interviews with the Security Management Executive of Logica, conducted during spring 2011.

The research suggests that the information security level at Logica is at the reference level. After evaluating the organisation and its IT management the findings suggest that both are almost at level three, fulfilling the reference level requirements well. The reference level requirements are set in the decree as the target level.

Information management and development ISO/IEC 27001-standard, service production and process procedures are identified as best practices for guaranteeing service quality. It is vital to ensure sufficient and regular staff training. Also, top management commitment to the chosen procedures is essential. The thesis is partly undisclosed and is meant for Logica internal use only.
Key words: information security, quality, ITIL, ISO/IEC

1 JOHDANTO

Laaksosen, Nevasalon ja Tomulan (2006,17) mukaan tietoturva ei ole itseisarvo. Tietoturvallisuus on jotain, jolla on tarkoitus. He kirjoittavat, että useat yritykset ovat vasta viime vuosina havahtuneet huomioimaan heikon tietoturvan vaikutuksen yrityksen liiketoimintaan, sen imagoon ja taloudellisiin tappioihin.

Nykypäivänä tietoturvallisuus on siis muutakin kuin virusten ja haittaohjelmien torjuntaa. Tietoturvallisuus on kiinteä ja keskeinen osa yhteiskuntaamme ja yritysten liiketoimintaa. Heikko tietoturvallisuus vaikuttaa yrityksen liiketoimintaan, sen imagoon ja pahimmillaan aiheuttaa taloudellisia tappioita. Organisaation tehokkuus, toimivuus ja kehityskyky ovat entistä riippuvaisimpia tietojärjestelmistä ja niiden tietoturvallisuudesta. Julkishallinnon säästötavoitteet ja samanaikainen tarve parantaa tietojärjestelmien tietoturvallisuutta asettaa julkishallinnon niin valtio- kuin kuntapuolella uusien haasteiden eteen. Kansainvälinen yhteistyö velvoittaa viranomaiset huolehtimaan tietoturvallisuudesta aina vain huolellisemmin.

Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien ja palvelujen suojaamista niin normaali- kuin poikkeusoloissa. Tietoturvallisuuden peruskäsitteet ovat luottamuksellisuus, eheys ja käytettävyys. Luottamuksellisuudella tarkoitetaan sitä, että tiedot, palvelut ja järjestelmät ovat vain niiden käyttöön oikeutettujen saatavissa eikä niiden tietoja paljasteta sivullisille. Eheys tarkoittaa tässä, etteivät tiedot, palvelut tai järjestelmät ole vioittuneet tai tuhoutuneet esimerkiksi laitteisto-, ohjelmisto- tai tiedonsiirtovirheiden johdosta. Syynä tuhoutumiseen voi olla myös inhimillinen virhe tai luonnonkatastrofi. Käytätettävyydellä tarkoitetaan sitä, että tiedot, palvelut ja järjestelmät ovat tarvittaessa niihin oikeutettujen käytettävissä. (Hakala & Vainio & Vuorinen 2006, 4-5.)

Tietoyhteiskunta on tätä päivää. Vuonna 2010 paljastui suuri tietotovuoto, jolloin Wikileaks ilmoitti, että sillä on hallussaan 250 000 dokumenttia. Suurin osa kyseessä olevista dokumenteista oli julkista tietoa, mutta mukana oli erittäin salaisiksi ja luottamuksellisiksi luokiteltuja asiakirjoja. Nämä dokumentit Wikileaks julkaisi eri medioiden välityksellä kaikkien luettavaksi. Huhtikuussa 2011 julkaistiin, että Sonyn järjestelmiin oli tehty tietomurto. Tekijä oli saanut käsiinsä kaikkien PlayStation Network- ja Qriocity-palvelujen käyttäjien tiedot. Pelkästään Suomessa PlayStation 3-konsoleita on myyty

noin 240 000 ja PlayStation Networkin käyttäjiä arvioidaan olevaan useita kymmeniä tuhansia. (Cert.fi 2011.)

1.1 Lähtökohdat ja taustatekijät

Opinnäytetyöni on hankkeistettu ja toimeksiantaja on työnantajani Logica. Ajatus tutkimuksen kohteesta syntyi vuoden 2010 lopulla, kun tutustuimme yhdessä asiakkaan kanssa tietoturvallisuusasetukseen Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) ja pohdimme sen vaikutuksia liiketoimintasuhteeseemme. Tietoturvallisuusasetus, joka astui voimaan 1.10.2010, velvoittaa viranomaiset saattamaan toimintansa ja tietojenkäsittelynsä vastaamaan asetuksessa säädettyjä perustason tietoturvavaatimuksia kolmen vuoden kuluessa asetuksen voimaantulosta eli 30.9.2013 mennessä. On kuitenkin huomattava, että tietoturvallisuusasetus ei itsessään tuo mitään uutta valtionhallinnon velvoitteisiin noudattaa hyvää tiedonhallintatapaa.

Valtionhallinnon viranomaisten yleinen velvollisuus huolehtia tietoturvallisuudesta perustuu viranomaisten toiminnan julkisuudesta annettuun lakiin (julkisuuslaki 621/1999). Valtioneuvoston 1.7.2010 julkisuuslain nojalla antamaa tietoturvallisuusasetusta sovelletaan valtionhallinnon viranomaisiin. Näillä tarkoitetaan valtion hallintoviranomaisia, muita valtion virastoja ja laitoksia sekä tuomioistuimia ja muita lainkäyttöviranomaisia. Asetus ja sen turvavaatimukset velvoittavat myös julkishallinnon palvelutoimittajia, joten palvelutoimittajat, kuten Logica, joutuvat arvioimaan palvelunsa suhteessa asetuksen vaatimuksiin.

1.2 Muutos ja muutoksen hallinta

Muutos ja muutoksen hallinta ovat opinnäytetyöni teoreettinen viitekehys. Julkishallinnon toimintaan kohdistuvat muutostekijät vaikuttavat myös tietotekniikkapalveluita tarjoavien yritysten toimintamalleihin ja palveluihin. Market Visionin tutkimuksen (2009) mukaan julkishallinnon muutospaineita aiheuttavat niin organisaation sisäiset kuin ulkoiset tekijät. Sisäisiä muutostekijöitä ovat tuottavuusohjelma ja alueellistami-

nen. Ulkoisia muutostekijöitä ovat ITC-palvelujen tuottaminen matalamman kustannustason maissa ja tieto- ja viestintätekniikan kehittyminen.

Laaksosen ym. (2006, 21) mukaan Suomessa ei ole olemassa erityistä tietoturvaa koskevaa erillislakia, jossa olisi tyhjentävästi säädelty yhteisöjen tai yksittäisten tietotokoneenkäyttäjien tietoturvavelvoitteista tai -oikeuksista. Julkishallinnon puolella eri hallinnonaloilla voi olla suuria eroja tietohallinnossa. Eri virastoilla ei ole ollut esimerkiksi yhteisiä tietoturvan tasomäärityksiä. Valtioneuvoston asetus tietoturvallisuudesta selkeyttää toimintamalleja ja niihin liittyviä vaatimuksia. Globaali moderni toimintaympäristö, jossa kriittisiin tietojärjestelmiin kohdistuu yhä enemmän turvallisuusuhkia, pakottavat julkishallinnon organisaatiot ja heidän ulkoistuspalvelutarjoajansa kehittämään tietoturvallisuutta.

Valtionhallinnossa on pyritty normiperusteiseen tietoturvallisuuden ohjaukseen. Lainsäädännön määräämät velvoitteet sekä tietoturvatoiminnan perusteet ja standardit, että suositukset ovat hallinnan toteuttamisen viitekehyksiä. Teoreettinen viitekehys pohjautuu lakeihin ja asetuksiin, joiden lähteenä hyödynsin Finlexiä, valtion säädöstietopankkia. Käytän lähteinäni myös valtionhallinnon tietoturvallisuuden johtoryhmän VAHDIn ohjeita. Tietoturvasta ja tietoturvastandardeista on julkaistu paljon kirjallisuutta niin suomeksi kuin englanniksi.

1.3 Tutkimuksen tavoitteet ja rajaus

Opinnäytetyössäni selvitän, mitä uusia vaatimuksia julkishallinnon tietoturvallisuusasetus tuo Logicalle, joka on julkishallinnon ulkoistuspalvelutarjoaja. Tutkimuksessa haen vastauksia siihen:

- *Miten Logican palvelut ja prosessit täyttävät tietoturvallisuusasetuksen vaatimukset?*
- *Miten asetusten toteuttamisen mahdolliset poikkeamat ratkaistaan?*
- *Miten varmistetaan, että on toimittu niiden mukaan?*

Vastausten perusteella haen myös tapoja, siihen miten tietoturvallisuusasetuksen toteuttamisen vaikeudet ratkaistaan. Tarvitaanko lisää resursseja? Edellyttääkö asetus jatkos-

sa säännöllisiä auditointeja? Kirjataanko turvallisuusasetuksen velvoitteet sopimuksiin? Miten poikkeamia raportoidaan ja sanktioidaanko ne?

Tietoturvallisuusasetuksen Valtionhallinnon tietoturvallisuuden johtoryhmän eli VAH-DIn ohjeistuksessa on erikseen arviointilomakkeet, joilla ministeriöt ja virastot sekä julkishallinnon palvelutoimittajat arvioivat oman turvallisuustasonsa. Arviointilomakkeita on kaksi. Ensimmäisessä arvioidaan organisaatiota ja toisessa sen IT-hallintaa.

Arvioitavia asioita ovat IT-hallinnan puolella muun muussa raportointi tietoturvavastaavalle, omaisuuden hallinta, tietojenkäsittely-ympäristöjen käyttöönotto ja niiden poisto. Organisaation arvioinnissa käydään läpi johtajuutta, strategiaa, henkilöstöä, kumppaneita ja prosesseja. Arviointilomakkeella on monivalintakysymyksiä, joihin vastataan ”kyllä”, ”ei” ja ”ei sovellu”. Nämä kysymykset käyn läpi Logican tietoturvapäällikön kanssa. Tutkimuksen tuloksena muodostuu käsitys Logican IT-hallinnan ja organisaation turvallisuustasoista.

Rajaan työni koskemaan Logican infrapalveluita, joita ovat konesalipalvelut, palvelinpalvelut, varmistuspalvelut, tietoverkkopalvelut, lokien hallintapalvelut, käyttövaltuushallintapalvelut, työasemapalvelut, sähköposti- ja mobiilipalvelut

Opinnäytetyöni on osittain salattu, koska se sisältää Logican liiketoiminnan kannalta luottamuksellista tietoa.

1.4 Tutkimusmenetelmä

Opinnäytetyöni on kvalitatiivinen tutkimus, jonka tutkimusasetelma on laadullinen vertaileva tapaustutkimus. Kanasen (2008, 24 - 25) mukaan laadullinen tutkimus tarkoittaa mitä tahansa tutkimusta, jonka avulla pyritään ”löydöksiin” ilman tilastollisia menetelmiä tai muita määrällisiä keinoja. Laadullinen tutkimus käyttää sanoja ja lauseita. Omassa työssäni tutkimusaineistoa ovat lait, asetukset ja suositukset eli normiohjaus. Normiohjautuvuudella tarkoitetaan siis ohjaavien lakien, asetusten ja arvojen huomioimista päätöksenteossa.

Toteutan työni tapaustutkimuksena. Tapaustutkimuksessa tutkitaan yksittäistä tapahtumaa ja työ etenee tutkimalla sekä kuvailemalla tapahtumaa esimerkiksi kysymysten

avulla. Kanasen (2008, 84) mukaan tapaustutkimusta ei tehdä yhden tietolähteen varassa, sillä aineisto voi perustua dokumentteihin, haastatteluihin ja havainnointiin. Kananen (2008) jatkaa, että oleellista tapaustutkimuksessa on aineiston monilähteisyys. Toisaalta myös tulkinnan pohjana olevan aineisto tulee esittää tutkimuksessa niin, että päättelyketju on muitten tarkistettavissa. Tämä parantaa tutkimuksen luotettavuutta ja laatua.

Tutkimusta varten kerään tietoja avoimella keskustelunomaisella haastattelulla Logican tietoturvapäälliköltä. Hirsjärven, Remeksen ja Sajavaaran (2010, 207) mukaan haastattelu on yhdenlaista keskustelua. Tutkimushaastatteluni on kuitenkin systemaattista tiedonkeruuta, jossa hyödynnän valmiita arviointilomakkeita.

1.5 Lyhenteet

Tietotekniikka- ja kommunikaatioalan käsitteistö ja päivittäinen kielenkäyttö
on täynnä lyhenteitä ja alan ammattilaiset käyttävät niitä paljon. Ohessa avaan joitakin tärkeimpiä lyhenteitä, joita esiintyy opinnäytetyöni raportissa.

AM	Application management
BPO	Business process outsourcing
COBIT	Control Objectives for Information and related Technology
ICT	Information and communications technology
IM	Infrastructure management
ISO	International Organization of Standardization
IT	Information technology
ITIL	Information Technology Infrastructure Library
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä

1.6 Toimeksiantajan esittely

Logica on kansainvälinen tietotekniikka-alan palveluyritys, joka toimii 36 maassa. Yrityksen palveluksessa on noin 39 000 henkilöä, joista Suomessa 3 100. Logican pääkonttori on Lontoossa, ja yritys on listattu Lontoon ja Amsterdamin pörsseissä. Logican pal-

veluita ovat esimerkiksi konsultointipalvelut, henkilöstöpalvelut, SAP, Oracle, mobiiliratkaisut, tietoturva, asiakkuudenhallinta, sisällönhallinta, pilvipalvelut ja ulkoistaminen. Suomessa Logica aloitti toimintansa vuonna 2006, jolloin se osti pohjoismaisen WM-datan ja sen liiketoiminnot. (Logica 2011.)

Yritys tarjoaa palveluja monelle toimialalle, kuten kaupalle, palveluille, teollisuudelle, liikenteelle, kunnille, terveydenhuollolle ja valtiolle. Logican toimintamalli on yhdistää globaali osaaminen paikalliseen asiantuntemukseen. Yritys keskittyy asiakkaisiin ja palveluihin. Ulkoistamispalvelut jaetaan kolmeen alueeseen: IM eli infrastruckture management, AM eli application management ja BPO eli business process outsourcing. Opinnäytetyössäni keskityn infrastruckture management -palveluihin ja siihen, miten julkishallinnon tietoturvallisuusasetus 681/2010 vaikuttaa Logican infrapalveluihin ja prosesseihin. (Logica 2011.)

2 TIETOTURVALLISUUS ULKOISTUKSISSA

Laaksosen ym. (2006, 239) perusajatus ulkoistusten tietoturvallisuuden hallinnassa on se, että vaikka jokin toiminta on ulkoistettu, tulee tämän toiminnan tietoturvallisuuden asianmukaisesta hoidosta varmistua aivan samalla tavalla kuin toiminto olisi oman yrityksen hoidettavana. Toisin sanoen, jos joku menee pieleen, toimintakatkoista, maineen menetyksestä ja muista seurauksista kärsii ulkoistuksen tehnyt yritys, ei yleensä suoraan ulkoistuspalveluntarjoaja.

Laaksosen ym.(2006, 239) mukaan vastuunjakoa voidaan kuitenkin tietyissä rajoin muuttaa sopimuksin. Tosin hyvätkään sopimukset eivät aina ole riittävä tapa hoitaa ulkoistuksien tietoturvallisuutta. Sopimuksissa voidaan määritellä sanktioita, mutta niiden määritteleminen häiriötilanteissa riittävän kattavaksi on osoittautunut vaikeaksi, ja toisaalta maineen kärsimisen aiheuttamia kustannuksia on vaikea mitata ja perätä sopimuksen perusteella ulkoistuspalveluntarjoajalta.

Iivarisen ja Laaksosen (2009, 220) mukaan yleensä palvelun ostajalla ja tuottajalla on omasta mielestään hyvinkin selkeä käsitys palveluun liittyvistä rooleista ja vastuista. Käytännössä tai sopimuksissa nämä käsitykset eivät kuitenkaan välttämättä kohtaa, ja asiat, joista ei selkeästi ole sovittu, jäävät todennäköisesti hoitamatta. Laaksosen ym. (2006, 239) mukaan hyvätkään sopimukset eivät siten ole riittävä tapa hoitaa ulkoistuksen tietoturvallisuutta. Parasta on varautua tilanteeseen sopimuksin, mutta myös muuten varmistaa tietoturvallisuuden riittävä huomioon ottaminen ulkoistuksen yhteydessä. Olennaisempia komponentteja on osapuolten roolien määrittäminen sekä oikeuksien ja vastuiden riittävän selvä jakamien ja dokumentointi.

2.1 Ulkoistuksen lyhyt historia

VAHTI 7/2006 -ohjeessa on lyhyesti kuvattu kuinka, ulkoistus on noussut liikeelämässä esille viimeisen parinkymmenen vuoden aikana. Tosiasiallista ulkoistamista on tehty tätä ennenkin, mutta ratkaisevaan muutokseen vaikutti kaksi seikkaa. Ensiksi yrityksissä alettiin entistä useammin arvioida, kannattaako jokin tuote tai palvelu val-

mistaa itse. Muutosajurina oli kustannustehokkuus, mutta myöhemmin kuvaan astuivat strategiset asiat. Vaikka oma valmistus saattoi olla kannattavaa lyhyellä aikavälillä, se ei ollut sitä pitkällä tähtäimellä. Pääomien vapauttaminen ja yleinen halu keskittyä ydinliiketoimintaan ajoivat organisaatioita yhä suurempiin ulkoistuksiin. Toiseksi palvelua tai tuotetta ei ollut välttämätöntä tuottaa itse. Syntyi yrityksiä, joiden ydinliiketoiminta koostui juuri niistä toiminnoista, mitä asiakasyrityksissä ulkoistettiin.

2.2 Sopimusten hallinta

Valtionhallinnolta löytyy monia apuvälineitä ja malleja sopimusten hallintaan. Ohjeita sopimusten hallintaan ovat muun muassa VAHTI 2/2008 -ohje, Tärkein tekijä on ihminen, henkilöstöturvallisuus osana tietoturvallisuutta, jossa käsitellään erityisesti henkilöstöturvallisuutta osana tietoturvallisuutta. VAHTI 7/2006 -ohje, Muutos ja tietoturvallisuus – alueellistamisesta ulkoistamiseen – hallittu prosessi, on sisällöltään hyvin kattava. Julkisen hallinnon IT-hankintojen sopimusehtoa JIT 2007 (JHS 166) sovelletaan kaikissa julkishallinnon IT-tuotteiden ja palvelujen hankinnoissa.

2.3 Ulkoistuksen roolit ja vastuunjaot

Laaksosen ym. (2006, 240) mukaan yksi yleisimmistä tietoturvallisuuteen liittyvistä ongelmista ulkoistuksen yhteydessä on roolien ja vastuiden riittämätön määrittely. Erityisen hankalaa vastuiden ja muidenkin tietoturvallisuuden kannalta oleellisten asioiden määritteleminen on julkishallinnon suorittamissa ulkoistuksissa, jotka usein perustuvat tarjouskilpailuun. Laaksonen ym. (2006, 242) toteavatkin, että ulkoistuksen huolellinen suunnitteleminen ja suunniteltujen seikkojen vieminen sopimukseen halutussa muodossa ja laajuudessa ovat tärkeimpiä tekijöitä ulkoistushankkeessa. Toinen merkittävä tekijä on ulkoistussopimuksen mukainen toiminta, jota ulkoistajan tulee aktiivisesti seurata. Yksi keino kontrolloida sopimuksen täyttämistä on sopia vuosittaisesta ulkoisesta auditoinnista.

2.4 Ulkoistuksen auditointi

Laaksosen ym. (2006, 242) mukaan ulkoistuksen tietoturvallisuuteen pätee sama kuin muuhunkin tietoturvallisuuteen: luottamus hyvä, kontrolli parempi. Hänen mukaansa kaikkiin ulkoistussopimuksiin kannattaa pyrkiä sisällyttämään auditointioikeus joko asiakkaan itsensä tai kolmannen osapuolen toimesta. Tietoturvallisuuden toteutumista pitää kuitenkin seurata jatkuvasti. Palvelutuotannon seurantapalavereissa, joita on yleensä kerran kuussa, seurataan yhdessä asiakkaan kanssa sovitulla tavalla tietoturvallisuuden toteutumista. Seurannan apuvälineenä voi olla tietoturvaraportti, josta ilmenee takautuvasti edellisen kuukauden määritellyt tietoturvapoikkeamat.

2.5 Tietoturvavelvoitteet ulkoistussopimuksissa

Laaksosen ym. (2006, 243) mukaan ulkoistaminen on hyvin vaativa prosessi, ja se edellyttää useiden liiketoiminnallisten näkökohtien arviointia ja punnintaa. Tietoturvan kannalta ulkoistussopimuksessa on olennaista, että siinä on riittävässä määrin selvitetty, mitä tietoturvalta halutaan, missä laajuudessa ja minkä laatuisena. Tähän tuo selkeyttä valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010). Tietoturvallisuusasetus velvoittaa viranomaiset saattamaan toimintansa ja tietojenkäsittelynsä vastaamaan vähintään asetuksessa säädettyjä perustason tietoturvavaatimuksia.

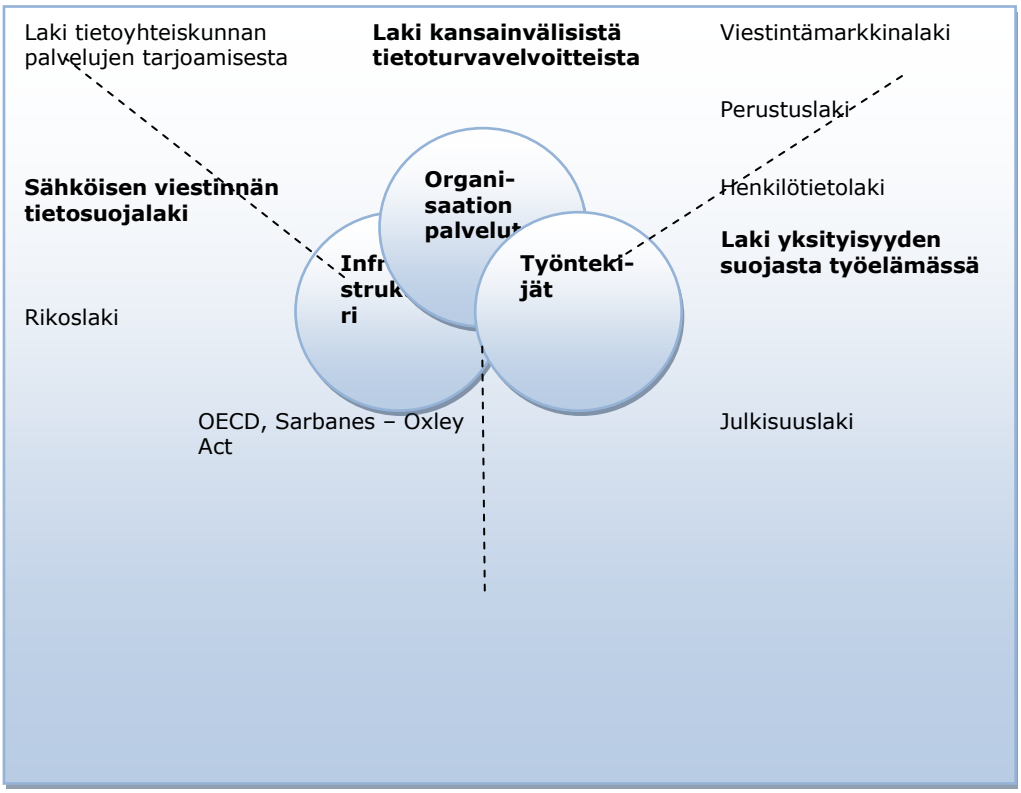
2.6 Valtionhallinnon ICT-toiminnan muutostekijät

Market Visionin tutkimuksen (2009) mukaan valtionhallinnon ICT-palveluostot ovat kasvaneet viime vuosina IT-palvelujen kokonaismarkkinoita nopeammin. Julkishallinto on nyt ja jatkossa merkittävä asiakas ICT-palvelutoimittajille. Valtioneuvoston periaatepäätöksessä valtionhallinnon IT-toiminnan kehittämisestä keskeisiä tekijöitä ovat esimerkiksi tuottavuuden parantaminen, ICT-varautuminen, IT-palvelujen tuottaminen matalamman kustannustason maissa, kansalaisten ikärakenteen muutos ja konsepti, jota kutsutaan Green IT:ksi.

3 LAINSÄÄDÄNTÖ, STANDARDIT JA TOIMINTAMALLIT

Laaksosen ym. (2006, 21) mukaan Suomessa ei ole erityistä tietoturvaa koskevaa erillislakia ja tästä ollaan yleisesti sitä mieltä, että lisää lainsäädäntöä ei tarvita. Yritykset haluavat kuitenkin viranomaisilta enemmän ohjeistusta ja kannanottoja siitä, mitä tulisi tai saisi tehdä, jotta tietoturvan ylläpitäminen ja parantaminen olisi lainmukaista. Suurimmat haasteet yrityksissä liittyvät tekniikan huimaan kehitykseen, joka mahdollistaa väärissä käsissä vakavia rikkomuksia. Toisaalta on myös laadittu uusia yksilön yksityisyyden suojaa koskevia lakeja kuten Laki yksityisyyden suojasta työelämässä (13.8.2004/759).

Tässä kappaleessa kerään yhteen suomalaisen lainsäädännön, kansainvälisen ohjeiston sekä tietoturvallisuus standardit, jotka liittyvät tietoturvallisuuden sääntelyyn. Ohessa Laaksosen ym. (2006, 23) esittämä kuva, josta ilmenee, mitkä eri lait pitää huomioida sekä tietoturvallisuutta että sen hallintaa suunniteltaessa ja millaisia vuorovaikutussuhteita niillä on.



Kuvio 1. Tietoturvallisuutta käsittelevää suomalaista lainsäädäntöä ja kansainvälistä ohjeistoa (Laaksonen ym. 2006, 23.)

3.1 Kansainvälinen normisto ja ohjeistus

OECD

OECD (Organization for Economic Cooperation and Development - Taloudellisen yhteistyön ja kehityksen järjestö) on kansanvaltaisten markkinatalousmaiden yhteistyöjärjestö, joka laati ensimmäisen ohjeistuksen tietojärjestelmien ja tietoverkkojen tietoturvaperiaatteista vuonna 1992. Vuonna 2002 ohjeistus päivitettiin ja samassa esiteltiin käsite turvallisuuskulttuuri. Tietoturvallisuudesta tulee kantaa huolta ja ottaa vastuuta hallinnon ja elinkeinoelämän kaikilla tasoilla ja tahoilla. (Laaksonen ym. 2006, 23 - 24.)

OECD:n ohjeistuksessa esitellään yhdeksän tietoturvaperiaatetta, jotka ovat turvallisuustietoisuus, vastuullisuus, vastatoimet, eettisyys, demokratia, riskien arviointi, turvallisuuden suunnittelu ja täytäntöönpano, turvallisuuden hallinta ja uudelleenarviointi. Tämä ohjeistus on huomioitu laajasti ja myös BS 7799/ISO7799 -standardi huomioivat nämä periaatteet. Valtiovarainministeriön VAHTI-ryhmän laatimissa tietoturvaohjeissa pohjana on OECD:n ohjeistus. (Laaksonen ym. 2006, 24.)

Sarbanes-Oxley Act–SOX

Sarbannes-Oxley -säädös koskee vain Yhdysvalloissa pörssilistattuja yhtiöitä, mutta se koskee myös muunmaalaisia palvelutarjoajia, joilla on asiakkainaan SOX-säädösten alaisia yrityksiä. SOX asettaa yhtiöille tarkat säädökset siitä, miten taloudellista tietoa tulee käsitellä ja säädösten rikkomisesta voi seurata vakavia rangaistuksia. Esimerkiksi jos yritys muuntaa, tuhoaa tai vääristelee tilinpäätöstä koskevaa materiaalia voi yritysjohto saada jopa 20 vuoden vankeustuomion. SOX-säädös saikin alkunsa Yhdysvalloissa muun muassa Enron-tapauksen perusteella. (Laaksonen ym. 2006, 24–25.)

3.2 EU-lainsäädäntö

Euroopan unionin jäsenyyden myötä kansallisen lainsäädännön rinnalla vaikuttaa Euroopan yhteisön direktiivit. Tietoturvaa koskevia direktiivejä on useita ja ne on implementoitu osaksi Suomen kansallista lainsäädäntöä. Direktiivi yksilöiden suojelusta hen-

kilötietojen käsittelystä ja tietojen vapaasta liikkuvuudesta (95/46/EY) annettiin 24.10.1995.

> Kyseistä direktiiviä sovelletaan automatisoituun tietojenkäsittelyyn (esimerkiksi tietokoneella oleviin asiakasrekistereihin) sekä sellaisten tietojen manuaaliseen käsittelyyn, jotka sisältyvät tai joiden on tarkoitus sisältyä paperiasiakirjoihin. Direktiivillä on tarkoitus suojella yksilöiden henkilötietojen käsittelyyn liittyviä oikeuksia ja vapauksia vahvistamalla pääperiaatteet, joita noudatetaan näiden käsittelyjen laillisuuden määrittämisessä.

3.3 Kansallinen lainsäädäntö

Suomessa ei ole olemassa yhtä erillistä tietoturvalakia, vaan tietoturvavelvoitteet on määritelty osana muuta lain säädäntöä. Suomessa tietoturvan lainsäädännöllinen kehys alkaa perustuslain määritelmistä.

Perustuslaki

Perustuslain (731/1999) 10 § määrittelee yksityisyyden suojan seuraavasti:

> Jokaisen yksityiselämä, kunnia ja kotirauha on turvattu. Henkilötietojen suojasta säädetään tarkemmin lailla. Kirjeen, puhelun ja muun luottamuksellisen viestin salaisuus on loukkaamaton. Lailla voidaan säätää perusoikeuksien turvaamiseksi tai rikosten selvittämiseksi välttämättömistä kotirauhan piiriin ulottuvista toimenpiteistä. Lailla voidaan säätää lisäksi välttämättömistä rajoituksista viestin salaisuuteen yksilön tai yhteiskunnan turvallisuutta taikka kotirauhaa vaarantavien rikosten tutkinnassa, oikeudenkäynnissä ja turvallisuustarkastuksessa sekä vapaudenmenetyksen aikana.

Julkisuuslaki

Suomessa viranomaistieto on lähtökohtaisesti julkista. Tiedon salassapito on poikkeus ja laissa on säädetty peruste tiedon salassapidolle. Julkisuuslain (621/1999) 1 § todetaan, että viranomaisten asiakirjat ovat julkisia, jollei tässä tai muussa laissa erikseen toisin säädetä. Opinnäytetyössäni tutkin julkisuuslain perusteella annettua turvallisuusasetusta *Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa* (681/2010). Turvallisuusasetuksen 1 luvun 1 § määritellään asetuksen soveltamisala seuraavasti:

> Tässä asetuksessa säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista.

Turvallisuusasetuksen tavoitteena on luoda edellytykset valtionhallinnon tietoturvatyön kehittämiseksi sekä yhtenäisten menettelyjen luomiseksi salassa pidettäviä ja käytöltään rajoitettuja tietoaineistoja käsiteltäessä (VAHTI 2/2010).

Henkilötietolaki

Tietoturvan kannalta henkilötietolaki (523/1999) on tärkeä. Henkilötietolaki on yleislaki ja henkilötietojen suojausta säädetään myös muissa laissa. Henkilötietolaki sisältää merkittäviä velvoitteita tietoturvan kannalta (Laaksonen ym. 2006, 31.)

> Tätä lakia sovelletaan henkilötietojen automaattiseen käsittelyyn. Myös muuhun *henkilötietojen* käsittelyyn sovelletaan tätä lakia silloin, kun henkilötiedot muodostavat tai niiden on tarkoitus muodostaa *henkilörekisteri* tai sen osa.

Laissa on termejä joiden sisältöä tarkennan ohessa. Laaksonen ym. (2006, 32) mukaan henkilötiedolla tarkoitetaan kaikenlaista luonnollista henkilöä tai hänen ominaisuuksiaan tai elinolosuhteitaan kuvaavia merkintöjä, joiden voidaan tulkita häntä tai hänen kanssaan yhteisessä taloudessa eläviä koskeviksi. Henkilörekisteri käsitteenä on tärkeä, koska lähes kaikki yritysten ja muiden yhteisöjen tietojärjestelmät sisältävät henkilörekistereitä. Jotta määritelmä henkilörekisteri täyttyy, pitää rekisterin sisältää luonnollisen henkilön esim. työntekijän henkilötietoja, joista hyvä esimerkki on palkkahallinnon rekisteri.

Hyvin monessa yrityksessä on Windows-verkon Active Directory (AD) tai vastaava hakemistopalvelu. AD-palveluiden tarjoaminen EU:n ulkopuolelta kuten Intiassa edellyttää henkilötietolain säännösten huomioimista. Tietosuojavaltuutetun kannanotossa on todettu, että yrityksellä on oikeus siirtää henkilötietoja EU:n tai ETA:n ulkopuolelle henkilötietolain 23 § 2 kohdan perusteella muun muussa siinä tapauksessa, että siirto on tarpeen rekisteröidyn ja rekisterinpitäjän välisen sopimuksen täytäntöön bpanemiseksi.

Laki kansainvälisistä tietoturvallisuusvelvoitteista

Laki kansainvälisistä velvoitteista (588/2004) on säädetty viranomaisten toimenpiteistä kansainvälisten tietoturvallisuusvelvoitteiden toteuttamiseksi.

> Lakia sovelletaan myös elinkeinonharjoittajaan ja tämän palveluksessa olevaan silloin, kun elinkeinonharjoittaja on sopimusosapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana.

Lakia sovelletaan tapauksissa joissa tietoa pidetään lähettävässä valtiossa tai kansainvälisessä järjestössä lähtökohtaisesti valtio- tai turvallisuussalaisuuksina. (Laaksonen ym. (2006, 48.)

Laki yksityisyyden suojasta työelämässä

Lain yksityisyyden suojasta työelämässä (759/2004) tarkoituksena on toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia työelämässä. Laaksosen ym. (2006, 49) mukaan tietoturvan kannalta laki asettaa työnantajalle olennaisia vaatimuksia käytännön tietoturvan suunnittelun ja ylläpitämisen näkökulmasta.

Työsopimuslaissa on tarkemmin määritelty työnantajan direktio-oikeus. Sen perusteella työnantaja voi antaa työntekijälle sitovia ohjeita ja määräyksiä, jotka liittyvät työntekijälle osoitettujen työtehtävien suorittamiseen tai tietoturvatoimenpiteiden noudattamiseen työpisteessä. Laki velvoittaa työnantajat noudattamaan yhteistoimintalain mukaista käsittelyä esimerkiksi tilanteissa joissa työpaikalle otetaan käyttöön teknisiä apuvälineitä työntekijöiden valvonnassa, Internetin, verkon tai kameroiden käytöstä työpaikalla. (Laaksonen ym. 2006, 50.)

Sähköisen viestinnän tietosuojalaki

Sähköisen viestinnän tietosuojalain (516/2004) soveltamisala on:

> Lain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolisten sähköisen viestinnän palvelujen tasapainoista kehittymistä.

Laki koskettaa lähes kaikkia yrityksiä, koska nykyään yrityksien viestintäverkoissa, kuten puhelin- tai tietoverkoissa, käsitellään työntekijöiden luottamuksellisia viestejä. (Laaksonen ym. 2006, 54.)

Kesäkuun 2009 alussa astui voimaan sähköisen viestinnän tietosuojalainmuutokset, jotka helpottivat yritysten toimintaedellytyksiä ja oikeutta käsitellä työntekijöiden sähköpostiviestien tunnistamistietoja oletetuissa väärinkäytöstapauksissa. Lakimuutos herätti paljon keskustelua ja se oli hyvin kiistelty. Lakimuutosta on kutsuttu myös Lex Nokiaksi, koska Nokia ajoi voimakkaasti muutoksen läpivientiä. Nokian perustelu muutokselle liittyi haluun suojata yrityssalaisuuksia.

Laki tietoyhteiskunnan palvelujen tarjoamisesta

Lain tietoyhteiskunnan palvelujen tarjoamisesta (458/2008) soveltamisalaa on:

> Tässä laissa säädetään tietoyhteiskunnan palvelujen tarjoamiseen liittyvistä seikoista, erityisesti palvelujen tarjoamisen vapaudesta, palvelun tarjoajien velvollisuudesta antaa tietoja, sopimusta koskevien muotovaatimusten täyttämisestä sähköisesti sekä välittäjänä toimivien palvelun tarjoajien vastuuvapaudesta.

Lain 2§:ssä todetaan**,** että tietoyhteiskunnan palvelulla tarkoitetaan tässä laissa palvelua, joka toimitetaan:

- etäpalveluna eli ilman, että osapuolet ovat yhtä aikaa läsnä;
- sähköisesti eli lähettämällä ja vastaanottamalla palvelu tietoja sähköisesti käsittelevien laitteiden tai tietojen säilytyksen avulla ja siten, että palvelun lähettämiseen, siirtoon ja vastaanottamiseen käytetään yksinomaan johtimia, radioyhteyttä, optisia laitteita tai muita sähkömagneettisia laitteita;
- palvelun vastaanottajan henkilökohtaisesta pyynnöstä tapahtuvana tiedonsiirtona;
- tavallisesti vastiketta vastaan.

Tietoviikko uutisoi vuoden 2009 lopussa, että Suomen tietoyhteiskunta rämpii erilaisissa tietoyhteiskunnan kehitystä mittaavissa vertailuissa. Esimerkiksi YK:n e-participation indeksissä Suomi oli eräällä it-yhteiskuntamittarilla mitattuna sijalla 45. Indeksi mittaa kolmea asiaa kuinka hyvin julkinen sektori antaa tietoa toiminnastaan web-sivujen kautta, kuinka paljon web-sivuja käytetään kansallismielipiteen selvittämi-

seen ja julkisen päätöksenteon tukena. Uusimmassa The Global Information Technology -raportissa (2009 - 2010) Suomi on noussut sijalle 30, joten tehdyt toimenpiteet ovat olleet selvästi oikeansuuntaisia.

Viestintämarkkinalaki

Viestintämarkkinalain (393/2003) tavoitteet ovat:

> Lain tavoitteena on edistää palvelujen tarjontaa ja käyttöä viestintäverkoissa sekä varmistaa, että viestintäverkkoja ja viestintäpalveluita on kohtuullisin ehdoin kaikkien teleyritysten ja käyttäjien saatavilla koko maassa. Lain tavoitteena on lisäksi huolehtia siitä, että Suomessa saatavilla olevat mahdollisuudet televiestintään ovat käyttäjien kohtuullisten tarpeiden mukaisia, keskenään kilpailevia, teknisesti kehittyneitä, laadultaan hyviä, toimintavarmoja ja turvallisia sekä hinnaltaan edullisia.

Laki koskee ennen kaikkea teleyrityksille asetettavia yleisiä tietoturvevelvoitteita.

3.4 Tietoturvan hallinnointiin liittyvät standardit ja toimintamallit

Tietoturvallisuuden kehittämisen ja hallinnoinnin avuksi on kehitetty erilaisia standardeja, viitekehyksiä ja toimintamalleja. Tietotekniikan roolin korostuessa on tarve toimintavarmoille ja laadukkaille tietotekniikkapalveluille kasvanut. Standardeja ja toimintamalleja on olemassa useita, mutta tässä käsittelemäni mallit ITIL (IT infrastructure library), COBIT (The Control Objectives for Information and related Technology) ja ISO 20 000 (International Organization of Standardization) ovat laajalti käytettyjä. Tiivistettynä voidaan sanoa, että ITIL on ICT-palvelujen tuottamisen ja niiden johtamisen viitekehys ja COBIT on prosessien, kuten ITIL:n määrittelemien prosessien, valvonnan viitekehys. ISO 20 000 on ITIL:in pohjautuva organisaatioiden palvelutuotannon laatustandardi (Wakaru 2011.)

Information Technology Infrastructure Library (ITIL®)

ITIL on useille palvelutoimittajille, kuten Logicalle de facto -standardi. ITIL on yhteinen kieli, jota ymmärtävät sekä tietotekniikkapalveluja tarjoavat yritykset, että heidän asiakkaansa. ITIL on viitekehys, joka perustuu parhaisiin käytäntöihin (best practises). ITIL määrittelee ICT -organisaatioissa tarvittavat ICT-palveluiden johtamisen tavoitteet, tarvittavat aktiviteetit, yksittäisten prosessien syötteet ja tulokset sekä yksittäisten prosessien keskinäiset suhteet. (Wakaru 2011.)

ITIL:n suosion syy on selvä, siitä on yksinkertaisesti hyötyä kaikille osapuolille. ITIL:n hyötyjä on mitattu useissa organisaatiossa ja tutkittu opinnäytetöissä. Esille ovat nousseet mm. seuraavat hyödyt:

- Malli on hyvin kattava ja mahdollistaa mittaamisen.
- Malli luo ja tarjoaa yhtenäisen sanaston, jota alalla tarvitaan.
- Malli luo standardeja laadunvalvonnalle.
- Malli jäsentää niin pienten kuin isojenkin organisaatioiden toimintaa.

(Wakaru 2011.)

ITIL sai alkunsa jo 1980-luvun lopulla Englannin hallituksen aloitteesta ja sen tarpeisiin laadituissa ohjeistuksissa. ITIL:n laajaa hyväksyntää on edesauttanut tietotekniikkaa liiketoiminnassansa hyödyntävien organisaatioiden aktiivinen yhteistyö IT Service Management Forumissa (itSMF), jolla on maajaoksia jo lähes 50 maassa. ITIL tarjoaa selkeän prosessimallin palveluiden, erityisesti ICT-palvelujen tuottamiseen. (Wakaru 2011.)

ITIL:stä on julkaistu jo kolmas versio - ITIL versio 3. Sen ydin koostuu viidestä kirjasta, joissa kuvataan palveluiden koko elinkaari palvelustrategian luomisesta, niiden suunnitteluun, käyttöönottoon, tuottamiseen ja jatkuvaan kehittämiseen.

Kirjat ovat:

Service Strategy –kirjassa kuvataan palvelustrategia ja arvontuottaminen, ICT-palvelujen linkittäminen liiketoiminnan tarpeisiin sekä palvelustrategian suunnittelu ja käyttöönotto.

Service Design –kirjassa kuvataan palvelujen suunnittelun tavoitteet ja elementit, palvelumallin valinta, kustannusmallit, riski/hyöty-analyysit, palvelusuunnitelman käyttöönotto sekä palvelujen mittaus ja valvonta.

Service Transition –kirjassa kuvataan organisaation ja organisaatiokulttuurin muutoksen hallinta, Knowledge Management, Service Knowledge Management System, menetelmät ja käytännöt sekä työkaluohjelmistot että palvelujen mittaus ja kontrolli.

Service Operation –kirjassa kuvataan sovellusten hallinta, muutoksenhallinta, tuotannon hallinta, kontrolliprosessit ja funktiot sekä mittaus ja valvonta.

Continual Service Improvement –kirjassa kuvataan organisaatiomuutoksen ja organisaatiokulttuurimuutoksen hallinta, kehittämisen liiketoiminta- ja teknologia-ajurit, menetelmät ja käytännöt sekä työkalut että mittaus ja valvonta. (Wakaru 2011.)

ITIL on siis prosessimalli, jonka avulla palveluja voidaan johtaa tehokkaasti. Prosessimallista on hyötyjä sekä asiakkaalle että palveluntarjoajalle. Prosessimallin mukaan toimittaessa palvelut ovat tasalaatuisempia, koska palveluiden sisältö on määritelty ja palveluntarjoajalla on selkeät kommunikointitavat.

The Control Objectives for Information and related Technology (COBIT)

Wakarun (2011) mukaan COBIT on ICT-palvelujohtamisen hyvän hallintotavan kontrollimalli. Se on prosessien, kuten ITIL:n määrittelemien prosessien, valvonnan viitekehys. COBIT:in lähestymistapa on liiketoimintakeskeinen, prosessiorientoitunut, kontrollipohjainen ja mittausta suosiva. COBIT:sta on kehittynyt avoin standardi ja se on kansainvälisesti omaksuttu ICT-palvelujohtamisen kontrollimalli.

Wakaru (2011) jatkaa, että COBIT-mallin taustalla ovat ISACA (Information Systems Audit and Control Association) ja nykyisin ITGI (IT Governance Institute). Mallin ensimmäinen versio vuodelta 1996 oli lähinnä tietojärjestelmätarkastajien työkalu. Toiseen versioon lisättiin prosessien hyvät käytännöt ja kontrollitavoitteet. Kolmannessa versiossa mukaan saatiin prosesseihin liittyvät mittarit ja kypsyystasomalli. Uusin versio julkaistiin vuoden 2005 lopussa sisältäen kaikki keskeiset elementit: strateginen yhteen sovittaminen, lisäarvon tuottaminen, resurssien hallinta, riskien hallinta ja suorituskyvyn mittaaminen.

ISO-standardit

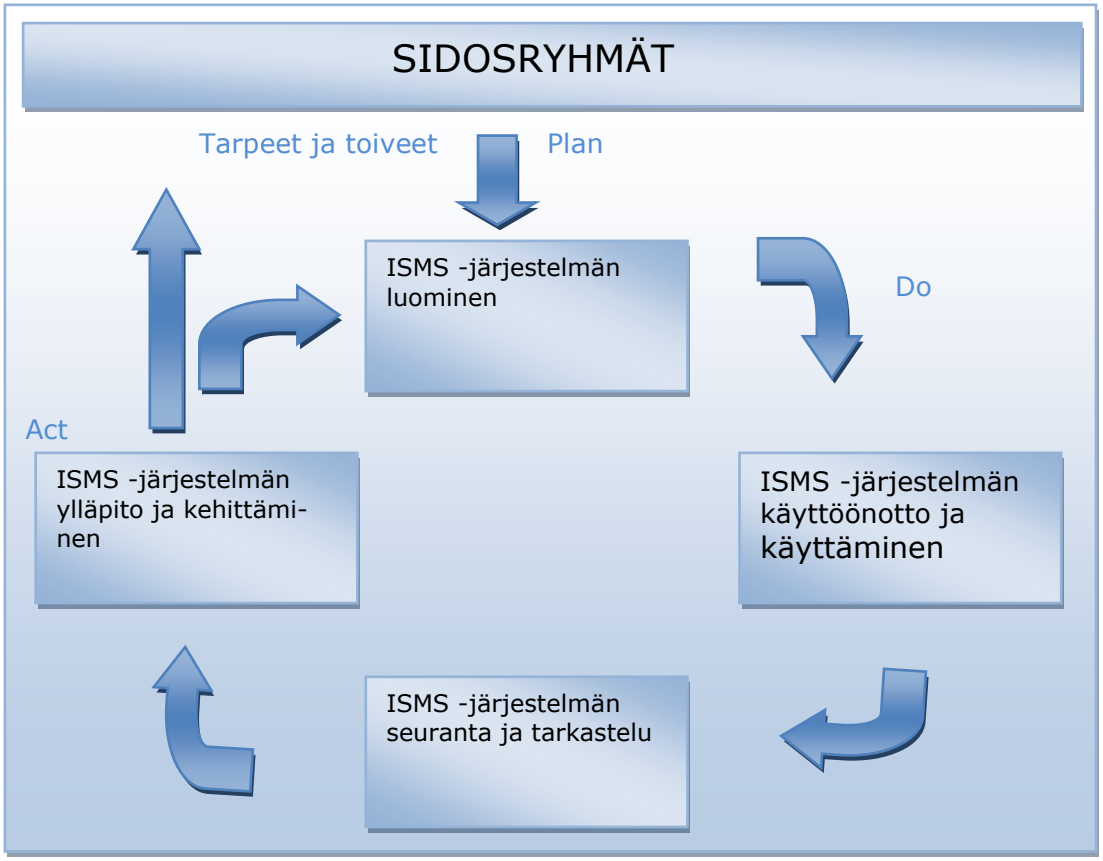
Keskeisimmät tietoturvastandardit ovat ISO-standardit. ISO-standardit ovat laajasti levinneitä ja tunnistettuja ja ISO:n jäsenenä ovat 160 maan kansalliset standardointielimet. ISO-standardeja on paljon mutta tietotekniikkapalveluiden johtamiseen ja hallintaan on kehitetty ISO 20000 -standardi. Standardin tavoitteena on edistää kustannustehokkaiden ja laadukkaiden IT -palveluiden tuottamista yhtenäisten ja tehokkaiden prosessien avulla. (Wakaru 2011.)

Standardit sisältävät suuntaviivat ja yleisperiaatteet tietoturvallisuuden hallintaan, mutta tietoturvallisuuden hallintajärjestelmän sertifioinnin perustan määrittelee ISO 27001 -standardi. ISO 27001 -standardi on yhteydessä yleisten laatujärjestelmästandardien kuten ISO 9001 ja ISO 14001 kanssa. Standardin perusajatuksena on tietoturvallisuuden hallintajärjestelmän kehittäminen prosessinomaisesti PDCA-mallin (Plan, Do, Check, Act) mukaisesti. (Hakala ym. 2006, 46.)

Wakarun (2011) mukaan tarve yhteiselle kansainvälisesti hyväksytylle standardille on noussut ITIL:n ja CobIT:n kaltaisten yleisesti hyväksyttyjen viitekehysten käytön myötä. Toisena merkittävänä ajurina ovat olleet yksittäisten organisaatioiden käytännön tarpeet varmistaa liiketoiminnan jatkuvuus ja tunnistaa siihen liittyvät riskit. Kolmantena merkittävänä syynä on ollut USA:n Sarbanes Oxley -lainsäädäntö ja siitä johdetut vaatimukset, jotka kohdistuvat myös tietotekniikkapalveluja tarjoaviin yrityksiin.

3.5 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmä eli ISMS (Information Security Management System) on hyvin käytännönläheinen ja prosessinomainen lähestymistapa tietoturvallisuuteen.



Kuvio 2. Tietoturvallisuuden hallintajärjestelmä (Hakala ym. 2006, 46.)

Hakalan ym. (2006, 49) mukaan ISO/IEC 27001 -standardi määrittelee tietoturvallisuuden hallinnan, joka sisältää järjestelmän perustamisen. Sillä on myös kiinteä yhteys organisaation yleisiin toimintamalleihin ja myös laatujärjestelmiin. Tietoturvallisuuden hallinnan klausuulit ovat:

1. ISMS-järjestelmän perustaminen, käyttöönotto ja käyttö, valvonta ja katselmukset, ylläpito ja kehittäminen, dokumentointi ja dokumenttien hallinta
2. Johdon sitoutuminen, tarvittavien resurssien varmistaminen, lainsäädännön ja sopimusten vaikutusten arvioiminen, katselmusten järjestäminen ja sen tuloksiin

reagointi, turvallisuustietoisuuden edistäminen sekä koulutuksen järjestäminen ja sen tulosten kirjaaminen

3. Sisäinen tietoturvallisuuden hallintajärjestelmän auditointi
4. Johdon suorittaman hallintajärjestelmän katselmus. Katselmuksen edellyttämät lähtötiedot ja sen tuloksen syntyvät tiedot.
5. Tietoturvallisuuden hallintajärjestelmän kehittäminen. Jatkuva kehittäminen, korjaavat toimenpiteet sekä ehkäisevät toimenpiteet.

Näiden klausuulien lisäksi standardissa on kolme taulukkoliitettä: tavoitteet ja toimenpiteet, OECD:n periaatteiden ja standardin ISMS-prosessin vertailu ja standardin vastaavuus laatujärjestelmästandardeihin ISO 9001 ja ISO 140001.

Logican laatupäällikön Mikko Niitamon (2011) mukaan Logican tietoturvallisuuden hallintajärjestelmä kehitettiin suojaamaan Logica Suomen käyttämää omaa ja asiakkaiden tietoa sen kaikissa käsittelyvaiheissa ja tallennusmuodoissa. Tieto suojataan siis riippumatta siitä, onko se sähköisessä tai paperisessa muodossa tai vaikkapa työntekijöiden muistissa. Suojaamiseen käytetään turvamekanismeja, joita voivat olla lukko ovessa, tiedostojen salaus tai toimintatapaohje, jonkin prosessin suorittamiseksi. Hallintajärjestelmän avulla tiedon suojaaminen on johdonmukaista, dokumentoitua ja ohjattua.

4 TIETOTURVALLISUUSASETUS JA SIIHEN LIITTYVÄT OHJEET

Valtio kehittää omaa tietoturvallisuuttaan jatkuvasti. Valtiovarainministeriö ohjaa ja yhteen sovittaa julkishallinnon ja erityisesti valtionhallinnon tietoturvallisuuden kehittämistä. Ministeriön asettama Valtionhallinnon tietoturvallisuuden johtoryhmä eli VAHTI on hallinnon tietoturvallisuuden ohjaamisen, kehittämisen ja koordinaation elin.

VAHDIn mukaan eri hallinnonaloilla on suuria eroja tietohallinnossa. On katsottu myös, että eri virastot ovat niin erilaisia, ettei niillä voi olla yhteisiä tietoturvan tasomäärityksiä. Linja on muuttunut ja nyt asetettu tietoturvallisuusasetus Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010) on kaikille hallinnonaloille yhteinen. VAHDIn mukaan:

- Tietoturvallisuus on osa johtamista, ei pelkkä tekninen ratkaisu.
- Julkishallinnon tuottavuusohjelma ei tarkoita että tietoturvasta tingittäisiin.
- Toimijoiden pitää huolehtia toiminnan jatkuvuudesta, laadusta ja riskienhallinnasta.

(KPMG, 2011.)

4.1 Tietoturvallisuusasetus

Valtionhallinnon viranomaisten yleinen velvollisuus huolehtia tietoturvallisuudesta perustuu viranomaisten toiminnan julkisuudesta annettuun lakiin (julkisuuslaki 621/1999). Valtioneuvosto antoi 1.7.2010 julkisuuslain nojalla uuden tietoturvallisuusasetuksen Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (681/2010), jota sovelletaan valtionhallinnon viranomaisiin. Näillä tarkoitetaan valtion hallintoviranomaisia ja muita valtion virastoja ja laitoksia sekä tuomioistuimia ja muita lainkäyttöviranomaisia (3 § 1 k). Asetuksella kumottiin viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallinta-tavasta annetun asetuksen 1030/1999 julkisuusasetus 2 ja 3 §.

Tietoturvallisuusasetuksen (681/2010) soveltamisalaa ovat siis:

> Tässä asetuksessa säädetään valtionhallinnon viranomaisten asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyssä noudatettavista tietoturvallisuusvaatimuksista.

Asetuksessa on viisi lukua ja 23 pykälää. Tietoturvallisuusasetus astui voimaan 1.10.2010. Asetuksessa on määritelty, että viranomaisten tulee saada tietojenkäsittelynsä tietoturva asetuksen 5 §:ssä säädetylle perustasolle 30.9.2013 mennessä. Viranomaisten tulee varmistaa, että kaikki tietoturvallisuuden perustason vaatimukset täytetään sovitussa aikataulussa. Annettu tietoturvallisuusasetus ja siihen liittyvät ohjeet ovat tärkeä osa valtionhallinnon tietoturvallisuuden kehittämistä koskevan valtioneuvoston periaatepäätöksen 26.11.2009 toimeenpanoa. Tietoturvallisuusasetus ei sinällään tuo mitään uutta valtionhallinnon velvoitteisiin noudattaa hyvää tiedonhallintatapaa. (VAHTI 2/2010, 7.)

Asetuksen myötä valtionhallintoon saadaan yhtenäinen luokittelu ja tietoturvallisuustoimet. Jatkossa kaikkien valtionhallinnon viranomaisten tulee saavuttaa vähintään perustason tietoturvallisuusvaatimukset. Perustason tietoturvallisuus koostuu erilaisista toimenpiteistä ja järjestelyistä, joita koskevat säädökset ovat olleet voimassa yli kymmenen vuotta. Asetus on valmisteltu samanaikaisesti ja samassa VAHTI-työryhmässä kuin ohjeet asetuksen täytäntöönpanosta. (VAHTI 2/2010, 7.)

4.2 Tietoturvallisuustasot

Tietoturvallisuustasojen avulla määritellään organisaatiolle ja sen tietojenkäsittelyympäristölle tarvittavat niin tekniliset kuin hallinnolliset vaatimukset. Tietoturvatasoja on kolme: tietoturvallisuuden perustason ympäristö (perustaso), korotetun tietoturvallisuustason ympäristö (korotettu taso) ja korkean käytettävyyden tietoturvallisuustason ympäristö (korkea taso). Alin sallittu taso on jatkossa perustaso. Tietoturvallisuustasojen vaatimukset on ryhmitelty kahteen osakokonaisuuteen: hallinnollinen tietoturvallisuus ja teknillinen tietoturvallisuus. Tietoturvallisuustasot määrittelevät ne vaatimukset, jotka liittyvät valtionhallinnon organisaatiossa tietoturvatoimintaan ja -prosesseihin. (VAHTI 2/2010, 14 - 16.)

4.3 Ohje asetuksen täytäntöönpanosta

Valtiovarainministeriö on tehnyt ohjeen, Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta (VAHTI 2/2010), jonka tavoitteena on tehostaa ja yhdenmukaistaa tietoturvallisuusasetuksen täytäntöönpanoa.

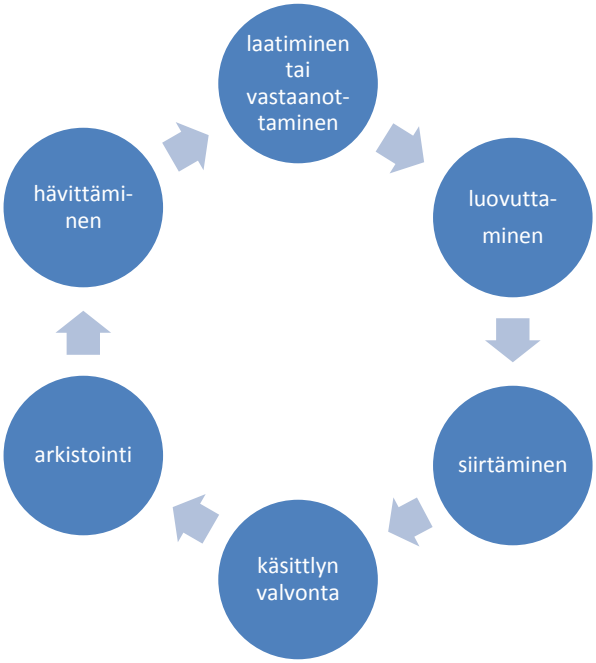
Muita ajankohtaisia ohjeita ovat Sisäverkko-ohje (VAHTI 3/2010) sekä Valtioneuvoston periaatepäätös tietoturvallisuuden kehittämisestä (VAHTI 7/2009). Näiden lisäksi valtionhallinnon organisaatio voi noudattaa Kansallista turvallisuusauditointikriteeristöä (KATAKRI), jota sovelletaan ennen kaikkea kansainvälisessä ja NATO-yhteistyössä. (VAHTI 3/2010, 15.)

Ohjeiden tavoitteena on edistää hyvää tiedonhallintatavan toteutumista valtionhallinnossa. Hyvän tiedonhallinnan onnistumisen edellytyksiä ovat muun muassa tietovarannon suunnittelu, erilaisten vaatimusten täyttäminen liittyen tietoverkot, tietojärjestelmät, toimitilat, asiakirjahallinto ja käyttövaltuushallinta. Toimenpiteiden tarkoituksena on luoda turvallinen ja tehokas työympäristö tiedon käsittelylle ennen kaikkea kaikissa tiedon elinkaaren vaiheissa. Keskeisessä roolissa ovat tunnistetusti tieto ja sen elinkaaren hallinta. (VAHTI 2/2010, 13.)

Tietoturvallisuusasetuksen ja erilaisten VAHTI-ohjeiden tavoitteena on luoda edellytykset valtionhallinnon tietoturvatyön kehittämiseksi. Samalla luodaan yhtenäiset menettelytavat salassa pidettävän tietoaineiston käsittelyyn. Valtionhallinnon tavoitteena on myös vahvistaa hallinnon asiakkaiden ja sidosryhmien luottamusta hallintoon ja sen tietojenkäsittelyyn. Tavoitteena on myös luoda puitteet sähköisen asianhallinnan ja sähköisten palveluiden kehittämiselle. Julkishallinnossa julkaistiinkin sosiaalisen median tietoturvaohje vuoden 2010 lopussa. (VAHTI 2/2010, 13.)

4.4 Tietoaineistojen käsittely ja hallinta

Tiedon merkitys yhteiskunnassa ja viranomaisten toiminnassa korostuu koko ajan. Arkistolaissa (831/1994) ohjataan tiedon elinkaaren hallintaa, koska hyvän tiedonhallintatavan toteuttaminen edellyttää sitä. Tiedon elinkaaren hallinta ei sinällään ole monimutkaista, kyseessähän on yksinkertaistettuna asiakirjan käsittelyvaiheet eli sen laatiminen tai vastaanottaminen, luovittaminen, siirtäminen, käsittelyn valvonta, arkistointi ja hävittäminen.



Kuvio 3. Tiedon elinkaarenhallinta (VAHTI 2/2010, 69 - 72.)

Lähtökohtaisesti julkisuuslain mukaan viranomaisten asiakirjat ovat julkisia, jollei lailla toisin säädetä. Salassa pidettäviä asiakirjoja ovat ne asiakirjat ja tiedot, jotka ovat julkisuuslain 24.1 § mukaan salassa pidettäviä. Tietoturvallisuusasetuksen 8 §; 9 § 2 mom. on nyt tarkemmin luokiteltu salassa pidettävä tietoaineisto. Salassa pidettävä tietoaineisto luokitellaan eri suojaustasojen mukaan, joita ovat suojaustaso I (ST I), suojaustaso II (ST II), suojaustaso III (ST III) ja suojaustaso IV (ST IV). Näiden turvallisuusluokitusmerkinnät ovat vastaavasti erittäin salainen, salainen, luottamuksellinen ja käyttö rajoitettu. (VAHTI 2/2010, 54 - 57.)

On kuitenkin hyvä huomioida ettei asiakirjojen luokittelu ole asetuksen mukaan pakollinen. Viranomaisten on mahdollista kohdistaa luokittelu vain tiettyihin asiakirjoihin tai

sellaisiin käsittelyaiheisiin, jotka halutaan erikseen suojata. Luokittelulla on kuitenkin tarkoitus helpottaa viranomaisten välistä salassa pidettävien tietojen vaihtoa, minkä vuoksi luokittelu on tärkeää niillä viranomaisilla, jotka käsittelevät salassa pidettävää aineistoa. (VAHTI 2/2010, 7 - 8.)

4.5 Tietoturvallisuusasetuksen täytötönpanosta

Asetuksen täytötönpanosta vastaa viranomainen. Viranomaisen tulee huolehtia riittävän hyvän tiedonhallinta- ja tietojenkäsittelytavan toteutumisesta. Viranomaisen tulee ohjata palveluksessaan olevia henkilöitä käsiteltävien asiakirjojen julkisuudesta, tietojen antamisesta, turvallisuusjärjestelyistä ja tietojärjestelmien suojaamisesta. Viranomainen vastaa myös koulutuksen antamisesta tarvittaville tahoille. Samoin viranomaisen tulee valvoa säännöllisesti luokiteltujen tietoaineistojen tietoturvatoimenpiteiden toimivuutta. Tietoaineistojen käsittelyyn liittyvien riskien seurantaa ja niiden aktiivista raportointia johdolle viranomaisten tulee ylläpitää. (VAHTI 2/2010, 23 - 25.)

Viranomainen vastaa tietoturvallisuustasojen toimeenpanosta yhteistyössään ja toiminnoissaan. Kuten olen jo aiemmin kirjoittanut, tietoturvallisuuden perustaso tulee olla toteutettuna koko valtionhallinnossa 30.9.2013 mennessä. Toiminnoissa jotka edellyttävät korotetun tai korkean turvallisuustason toimintaympäristöä, vaatimukset tulee toteuttaa viiden vuoden kuluessa siitä, kun viranomainen on ottanut luokituksen käyttöön. (VAHTI 2/2010, 23 - 25.)

4.6 Hyvä tiedonhallintapa

Julkisuuslain 18 §:ssä otetaan kantaa viranomaisten hyvään tiedonhallintatapaan. Hyvä tiedonhallintatapa edellyttää tiedonhallinnan suunnittelua. Tiivistettynä viranomaisen tulee huolehtia siitä, että julkiset asiakirjat ovat vaivattomasti löydettävissä. Asiakirja- ja tietohallinto sekä tietojärjestelmät toteutetaan siten, että asiakirjojen julkisuus voidaan vaivattomasti toteuttaa. Niihin liittyvät tiedot arkistoidaan tai hävitetään asianmukaisesti. Viranomaisten tulee myös huolehtia, että sen palveluksessa olevilla on tarvittava tieto käsiteltävien tietojen julkisuudesta. (VAHTI 2/2010, 27.)

Hyvän tiedonhallintatavan suunnittelu alkaa selvittämällä viranomaisten toimintaprosessit. Prosessin eri vaiheet kuvataan tarkasti alkaen miten asiat tulevat vireille, mitä toimenpiteitä käsittelyvaiheisiin liittyy, miten asiat päätetään, kuka osallistuu prosessin eri vaiheisiin, mitä asiakirjoja ja tietoja missäkin vaiheessa syntyy. Viranomaisten asiakirjojen käsittely edellyttää arkistonmuodostussuunnitelman olemassaoloa. Kansallisarkistosta saa yksityiskohtaiset ohjeet suunnitelman tekoa varten. Henkilötietolaissa ja sen 6 §:ssä on esitetty miten henkilötietojen käsittely pitää suunnitella. (VAHTI 2/2010, 27.)

4.7 Tietojenkäsittelyn yleiset tietoturvavaatimukset

Viranomaisten toiminnan jatkuvuus ja laatu varmistetaan huolehtimalla tietoturvallisuudesta. VAHTI-ohjeessa todetaan että ”viranomaisten on toteutettava ja ylläpidettävä vähintään tietoturvallisuuden perustason vaatimukset täyttävää tiedonkäsittelyympäristöä”. Viranomaisten tulee myös päättää otetaanko virastossa käyttöön asiakirjojen luokitus. Tämä ei siis ole pakollinen, mutta viranomaisen pitää, vaikka ei luokittelekaan asiakirjoja, noudattaa julkisuuslain 18 §:ssä ja turvallisuusasetuksen luvussa 2 säädettyjä velvoitteita. Ilman henkilökunnan koulutusta ei voida edellyttää hyvän tiedonhallintatavan toteutumista. Viranomaisten pitääkin järjestää tietoturvakoulutusta henkilökunnalleen säännöllisesti. (VAHTI /2010, 35 - 37.)

Henkilökunnan pitää myös ymmärtää tietoturvallisuuteen liittyvät riskit, tuntea viranomaisten tietoturvaohjeistuksen ja sitoutua noudattamaan annettuja ohjeita. Suurin tietoturvariski on henkilökunta. Syynä tähän voi olla huolimattomuus tietoaineiston tai työvälineiden käytössä. Toinen yleinen syy on piittaamattomuus annettuja ohjeita kohtaan. Kolmas syy on se, ettei henkilökunnalle ole annettu riittävää koulutusta ja ohjeistusta. (VAHTI /2010, 35 - 37.)

Tietoteknistä ympäristöä ja tietopalveluja koskevat vaatimukset pohjautuvat tietoturvallisuustasoihin eli perustasoon, korotettuun tai korkeaan tasoon. Vaatimukset koskevat tietoverkkoja ja tietojärjestelmiä sekä näiden valvontaa. Erilaiset työvälineet kuten hait-

taohjelmien torjuntajärjestelmät, tietoaineistojen salausmenettelyt sekä käyttöoikeuksien hallintamenettelyt pitää olla ajan tasalla ja dokumentoituna. (VAHTI 2/2010, 41.)

4.8 Tietoturvallisuustasojen perusteet

Perustason ympäristö mahdollistaa suojaustason IV sisältävien tietojen ja asiakirjojen käsittelyn selväkielisessä muodossa, kun taas korotettu taso mahdollistaa suojaustason III sisältävien tietojen ja asiakirjojen käsittelyn selväkielisessä muodossa. Suojaustason II sisältävien selväkielisten tietojen ja asiakirjojen käsittely on mahdollinen vain korkean tietoturvallisuustason ympäristössä. Suojaustasoa I sisältävien selväkielisten tietojen käsittely voidaan toteuttaa vain erillisessä ja rajatussa verkkoympäristössä, josta ei ole liitäntöjä esimerkiksi Internetiin. (VAHTI 2/2010, 42 - 43.)

Tietoturvallisuustasojen avulla asetetaan myös vaatimukset teknisille ja hallinnolliselle turvallisuudelle. Tietoturvallisuustaso eri toimintaympäristöissä määritellään toimintaprosessien ja niissä käsiteltävien tietojen sisällön ja merkityksen sekä niihin kohdistuvien uhkien ja riskien pohjalta. Tietoturvallisuustasojen avulla selkeytetään eri viranomaisten ja heidän sidosryhmiensä välillä tapahtuvaa salassa pidettävien tietojen vaihtoa. (VAHTI 2/2010, 43.)

Keskeinen tekijä on tietenkin tunnistaa suojattavat kohteet. Esimerkkejä suojattavista kohteista ovat tietoaineistot, työasemat, tietojärjestelmät ja niiden tilat sekä tietoverkot. Riskien arviointi on kehittämisen pohjana. Tiedon käsittelyyn käyttämien ympäristöjen tietoturvallisuus pitää arvioida. Tähän viranomaiset tai heidän palvelutoimittajansa voivat käyttää joko itsearviointimenetelmää tai ulkoista arvioijaa. Apuvälineenä arvioinnissa käytetään VAHTI -ohjeistoa sekä Valtion IT -palvelukeskuksen tarjoamia välineitä. (VAHTI 2/2010, 44.)

Toimeksiantajani näkökulmasta oleellisista on Valtiovarainministeriön tekemien arviointitaulukoiden läpikäynti suhteessa Logican Infrapalveluihin. Arviointitaulukoita on kaksi: tietoturvatasot IT -arviointi ja tietoturvatasot organisaation arviointi. Tutkimus tehdään haastattelemalla Logican tietoturvapäällikköä.

5 POHDINTA JA JOHTOPÄÄTÖKSET

Market Visionin tutkimuksen (2009) mukaan julkishallinnon muutospaineita aiheuttavat niin organisaation sisäiset kuin ulkoiset tekijät. Sisäisiä muutostekijöitä ovat tuottavuusohjelma ja alueellistaminen. Ulkoisia muutostekijöitä ovat esimerkiksi IT-palvelujen tuottaminen matalamman kustannustason maissa ja tieto- ja viestintätekniikan kehittyminen.

Valtionhallinnon rakenteiden muuttaminen ja uudistaminen sekä tuottavuuden lisäystavoitteiden saavuttaminen edellyttävät paljon tietotekniikkaa ja tietotekniikkapalveluja. Toisaalta tuottavuusohjelman mukaisesti IT-henkilöstön määrää tulisi vähentää 500 henkilötyövuotta vuoteen 2015 mennessä. Alueellistamisen tavoitteena taas on 4000 - 8000 työpaikan sijoittaminen pääkaupunkiseudun ulkopuolelle vuoteen 2015 mennessä.

Market Vision arvion (2009) mukaan vuonna 2010 arvioidaan noin 15 prosenttia kaikista Suomessa ostetuista IT-palveluista tuotettavan matalamman kustannustason maissa (offshore). Julkishallinnon puolella on suhtauduttu varauksella offshore-palvelujen käyttöön.

Market Visionin tutkimuksessa (2009) todetaan, että tieto- ja viestintätekniikan kehittyessä avautuu myös uusia tapoja hyödyntää sähköistä viestintää ja uuden tyyppisiä medioita. Esimerkkinä uuden tyyppisistä medioista on sosiaalinen media. Sosiaalinen media muuttaa tapaa, jolla kansalaiset saavat tietoa, jakavat tietoa, muodostavat käsityksiä ja mielipiteitä.

Myös globaali moderni toimintaympäristö, jossa kriittisiin tietojärjestelmiin kohdistuu yhä enemmän turvallisuusuhkia, velvoittavat yritykset ja julkishallinnon organisaatiot kehittämään toimintatapojaan.

Kaikki nämä merkittävät muutokset vaikuttavat jollakin aikataululla julkishallinnon ICT–ulkoistuksiin. Valtionhallinnossa tavoitellaankin suurempia organisaattorisia kokonaisuuksia, joista esimerkkinä on Valtion IT -palvelukeskus (VIP). Sen tehtävä on yhdistää pääosin markkinoilta hankituista ICT-palveluista valionhallinnolle sopivia palvelukokonaisuuksia.

VAHTI toteaa, että eri hallinnonaloilla on ollut suuria eroja, miten tietohallintoa toteutetaan ja johdetaan. Linja on nyt kuitenkin muuttunut ja nyt asetettu tietoturvallisuusasetus *Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa* (681/2010) on kaikille hallinnonaloille yhteinen. VAHDIn mukaan tietoturvallisuus on osa organisaation johtamista. VAHTI ohjeistaa myös, että julkishallinnon tuottavuusohjelma ei tarkoita, että tietoturvasta tingittäisiin. VAHTI painottaa, että toimijoiden pitää jatkossakin huolehtia toiminnan jatkuvuudesta, laadusta ja riskienhallinnasta. (KPMG 2011.)

Miten jatkossa tietoturvallisuusasetus vaikuttaa julkishallinnon ulkoistuksiin? Laaksosen ym. (2006, 240) mukaan erityisen hankalaa vastuiden ja muidenkin tietoturvallisuuden kannalta oleellisten asioiden määritteleminen on julkishallinnon ulkoistuksissa, koska ne perustuvat tarjouskilpailuihin. Näissä tarjouskilpailuissa toimittajien pitää lähtökohtaisesti toimittaa sitä, mitä tarjouspyynnössä pyydetään. Jatkossa julkishallinnon tarjouspyynnöissä ehkä määritellään tarvittava tietoturvallisuuden taso asetuksessa annettujen vaatimusten perusteella. Se, kuinka hyvin asetuksessa on onnistuttu määrittelemään tietoturvallisuuden tasojen vaatimukset, vaikuttaa eri toimittajien tarjoaminen palveluiden sisällön ja hintojen vertaamiseen.

Logica sai tehdyssä organisaation arvioinnissa arvosanaksi 2,94 ja sen IT-hallinnan arvosanaksi 2,85. Yritys täyttää näin ollen turvallisuusasetuksen perustason vaatimukset. Keinoja ratkaista ja varmistaa se, että toimitaan vaatimusten mukaisesti, on useita. Tietoturvallisuutta johdetaan ja kehitetään ISO/IEC 27001 -standardin näkökulmasta. Palvelut tuotteistetaan mahdollisimman pitkälle ja toimintamallit ovat prosessinmukaisia. Henkilökuntaa koulutetaan riittävästi, Logican johto sitoutuu valittuihin keinoihin ja varmistaa, että niiden mukaan toimitaan.

Tutkimuksessa hain vastauksia siihen miten Logican palvelut ja prosessit täyttävät tietoturvallisuusasetuksen vaatimukset, miten asetusten toteuttamisen mahdolliset poikkeamat ratkaistaan ja miten varmistetaan, että on toimittu niiden mukaan. Vastausten perusteella hain myös ratkaisuja, miten tietoturvallisuusasetuksen toteutuksessa esiin tulevat haasteet ratkaistaan.

LÄHTEET

Painetut

Hakala, M. & Vainio, M & Vuorinen, O. 2006. Tietoturvallisuuden käsikirja. Docendo Finland Oy. Jyväskylä.

Hirsjärvi, Sirkka & Remes, Pirkko & Sajavaara, Paula 2010. Tutki ja kirjoita. 15.–16. painos. Tammi. Helsinki.

Iivari, Mika & Laaksonen, Mika 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. Tietosanoma. Tallinna.

Laaksonen, M. & Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Ohjeistus, toteutus ja lainsäädäntö. Edita Publishing Oy. Helsinki.

Kananen, Jorma 2008. Kvalitatiivisen tutkimuksen teoria ja käytänteet. Jyväskylän Yliopistopaino. Jyväskylä.

Painamattomat

Arkistolaki. Luettu 14.4.2011. <http://www.finlex.fi/fi/laki/ajantasa/1994/19940831>

Cert.fi 2011. Sony PlayStation Network -käyttäjien tietoja varastettu. Luettu 8.9.2011. <https://www.cert.fi/varoitukset/2011/varoitus-2011-01.html>

Direktiivi 95/46/EY. Luettu 14.4.2011. <http://europa.eu/legislation_summaries/information_society/4012fi.htm>

Henkilötietolaki. Luettu 22.4.2011. <http://www.finlex.fi/fi/laki/ajantasa/1999/19990523>

KPMG - Tietoturvan ajankohtaisaamupäivä 2011. Esitys 12.2.2011. Tietoturvallisuusasetus sekä VM:n VAHTI-ohjeet ja muut toimet.

Laki kansainvälisistä tietoturvallisuusvelvoitteista. Luettu 24.4.2011. < http://www.finlex.fi/fi/laki/ajantasa/2004/20040588>

Laki tietoyhteiskunnan palvelujen tarjoamisesta. Luettu 6.5.2011. < http://www.finlex.fi/fi/laki/ajantasa/2002/20020458>

Laki turvallisuusselvityksistä. Luettu 10.5.2011. < http://www.finlex.fi/fi/laki/ajantasa/2002/20020177>

Laki viranomaisten toiminnan julkisuudesta. Luettu 10.5.2011. < http://www.finlex.fi/fi/laki/ajantasa/1999/19990621>

Laki yksityisyyden suojasta työelämässä. Luettu 18.3.2011.
< http://www.finlex.fi/fi/laki/ajantasa/2004/20040759>

Lex Nokia. Luettu 14.4.2011
<http://www.llr.fi/index.php?page=96347a71d94311f8ae7ea20544e15b4>

Logica 2011. Luettu 25.2.2011.
<http://www.logica.fi/>

Market Vision 2009. Keskeiset muutostekijät valtionhallinnon IT-toiminnassa. Tutkimus. Julkaistu 27.3.2009.

Miksi Suomen tietoyhteiskunta rämpii tutkimuksissa? Tietoviikko 16.12.2010.
<http://www.tietoviikko.fi/kaikki_uutiset/article351614.ece>

Niitamo, Mikko 2011. Logican tietoturvallisuuden johtaminen. Sähköposti.

Rikoslaki. Luettu 19.2.2011.
< http://www.finlex.fi/fi/laki/ajantasa/1889/18890039001>

Suomen perustuslaki. Luettu 8.5.2011.
<http://www.finlex.fi/fi/laki/ajantasa/1999/19990731>

Sähköisen viestinnän tietosuojalaki. Luettu 1.4.2011..
<http://www.finlex.fi/fi/laki/alkup/2004/20040516>

The Global Information Technology Report 2009–2010. Luettu 27.2.2011
<http://networkedreadiness.com/gitr/main/analysis/showdatatable.cfm>

Tietoturvallisuusasetus. Luettu 11.1.2011.
<http://www.finlex.fi/fi/laki/alkup/2010/20100681>

Tietoturvallisuuden arviointi valtionhallinnossa 2006. Luettu 15.3.2011.
<http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060802Tietot/A_vahti_08_netti.pdf>

Tilastokeskus 2007. Väestöennuste 2007-2040.Luettu 9.5.2011
<http://www.stat.fi/til/vaenn/2007/vaenn_2007_2007-05-31_tie_001.html>

VAHTI 7/2006. Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen – hallittu prosessi. Luettu 8.9.2011.
<http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20060724Muutos/Vahti_7_06.pdf>

VAHTI 7/2009. Valtioneuvoston periaatepäätös valtiohallinnon tietoturvallisuudesta.
<http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20091126Valtio/name.jsp>

VAHTI 2/2010. Ohje tietoturvallisuudesta valtionhallinnossa. Luettu 3.2.2011.

<http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinon_tietoturvallisuus/20101028Ohjeti/02_>

VAHTI 3/2010. Sisäverkko-ohje. Luettu 4.4.2011.
<http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101203Sisaeve/name.jsp>

VAHTI 4/2010. Sosiaalisen median tietoturvaohje. Luettu 5.4.2011.
<http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101222Sosiaa/name.jsp>

Valtionhallinnon tietoturvakäsitteistö 2003. Luettu 4.5.2011.
<http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/50903/50902_fi.pdf>

Viestintämarkkinalaki. Luettu 8.5.2011.
< http://www.finlex.fi/fi/laki/ajantasa/2003/20030393>

Wakaru 2011. Luettu 16.4.2011.
< http://www.wakaru.fi/fi/>