Viranomaisten salassa pidettävien tietojen käsittely valtionhallinnossa

Turvallisuusjohdon koulutusohjelma 12

Tutkielma

Erja Kinnunen

Valtiokonttori, Valtion IT-palvelukeskus

Helsinki 23.3.2013

Aalto University Professional Development – Aalto PRO

Tiivistelmä

Opinnäytetyössä käsitellään viranomaisten salassa pidettävien tietojen luokittelua ja käsittelyä. Työssä kuvataan kansalliset ja kansainväliset salassapitoon liittyvät säädökset ja määräykset. Lisäksi kuvataan kansainvälisiin velvoitteisiin liittyvät toimivaltaiset viranomaiset sekä kansalliset ohjeet ja suositukset jotka on laadittu tukemaan velvoitteiden toteuttamista.

Työssä tarkastellaan myös velvoitteiden toteutumista eri viranomaisten toiminnoissa sekä niitä suosituksia ja toimenpiteitä jotka on käynnistetty edesauttamaan velvoitteiden toteutumista viranomaistoiminnoissa.

Työssä tarkastellaan velvoitteiden toteuttamiseen liittyviä haasteita ja annetaan suosituksia siitä miten tietoturvatyötä ja salassa pidettävien tietojen käsittelyyn liittyvien velvoitteiden toteutumista voitaisiin edistää valtionhallinnossa ja muissa toimijoissa.

Sisältö

1 Johdanto

1.1 Työn esittely

Tässä opinnäytetyössä tarkastellaan viranomaisten salassa pidettävien tietojen suojaamista. Salassa pidettävällä tiedolla tarkoitetaan viranomaisten kansallisia tietoaineistoja sekä ulkomaisilta sopimuskumppaneilta saatuja tietoja, jotka ovat salassa pidettäviä joko kansallisten tai kansainvälisten säädösten nojalla.

1.2 Työn tavoite ja käsittelytapa

Tämän opinnäytetyön tavoitteena on kartoittaa viranomaisten tietojen salassapitoon liittyvät säädökset sekä muu ohjeistus. Tarkoitus on myös kuvata salassa pidettävien tietojen käsittelyn nykytilaa ja siihen liittyviä haasteita. Työn tavoitteena on lisäksi antaa kehitysehdotuksia, joilla viranomaisten toimintaa voitaisiin helpottaa ja edesauttaa tietojen salassapidon ja hyvän tiedonhallintotavan toteutumista.

Työhön sisältyy selvitys nykyisestä säädöspohjasta. Tietojen käsittelyn nykytilaa arvioidaan omien havaintojen ja haastatteluiden pohjalta. Tilanteen kartoituksessa hyödynnetään myös vastauksia Valtiovarainministeriön vuotuiseen tietoturvakyselyyn, joka tehdään vuosittain joulu-tammikuussa. Lähteenä on käytetty vuosien 2011 ja 2012 tietoturvakyselyitä.

Suositusten laadinnassa hyödynnetään Valtion IT-palvelukeskuksen ja sen asiakkaiden kokemuksia siitä, mitä haasteita nykytilanteeseen liittyy ja millaisia parannusehdotuksia niihin saatiin.

Haastatteluosuudessa on haastateltu Valtion IT-palvelukeskuksen virkamiehiä, jotka toimivat tietoturvapäällikön tehtävissä useassa eri ministeriössä.

2 Teoriataustaa

2.1 Tietoturvallisuuden tarkoitus

Tietoturvallisuus on tietojen luottamuksellisuuden, eheyden ja käytettävyyden suojaamista ulkopuolisten uhkien aiheuttamilta riskeiltä. Käytettävyydestä voidaan käyttää myös nimitystä saatavuus. Näitä pyritään turvaamaan erilaisin teknisin ja hallinnollisin toimenpitein. Tietoturvatoimenpiteiden tarkoituksena on turvata organisaation ydin- tai liiketoimintaa, joten ne pyritään mitoittamaan siten, että tarkoituksenmukaisella tavalla pystytään suojautumaan arvioituja riskejä vastaan. Suojattavat kohteet ja tiedot liittyvät yleensä palveluun tai toimintaan, jota organisaatio tuottaa. Tietojen suojaamisen perimmäisenä tarkoituksena on organisaation toiminnan ja sen tuottamien palveluiden jatkuvuuden turvaaminen, sekä ulkopuolisten luottamuksen säilyttäminen organisaation toimintaan. Tietoturvallisuuden toteuttaminen on myös edellytyksenä viranomaisten ja valtion sisäisen turvallisuuden, ulkosuhteiden ja maanpuolustuksen hyvälle hoitamiselle.

Tässä työssä tarkastellaan viranomaisten salassa pidettävien tietojen suojaamista, joten näkökulmana on tietojen luottamuksellisuuden suojaaminen sekä viranomaisten toimintojen turvaaminen ja kansalaisten luottamuksen säilyttäminen viranomaisten toimintaan.

2.2 Erityissuojattavat tietoaineistot

Tässä asiakirjassa tarkastellaan viranomaisten erityissuojattavia tietoaineistoja, jotka on määritelty salassa pidettäviksi. Suomalaisessa yhteiskunnassa lähtökohtana pidetään viranomaisten toiminnan julkisuutta. Viranomaisten toiminta ja asiakirjat ovat lähtökohtaisesti julkisia, ellei niitä ole määrätty

salassa pidettäviksi. Salassapito perustuu aina johonkin lakiin tai muuhun säädökseen.

Viranomaisten tietoturvallisuuden lähtökohtana toimii julkisuuslaki (Laki viranomaisten toiminnan julkisuudesta, 21.5.1999/621), jossa on määritelty perusteet asiakirjojen salassapidolle. Julkisuuslaissa määritelty ”asiakirjan” käsite on hyvin laaja, se kattaa perinteisten paperiasiakirjojen lisäksi myös kaikki sähköiset tallenteet, olivatpa ne sitten dataa, kuvaa tai ääntä. Julkisuuslaki koskee kaikkea viranomaisten käsittelemää ja hallussa pitämää tietoa riippumatta sen olomuodosta.

Kun salassa pidettäviä asiakirjoja käsitellään, niin ohjeiden ja käytänteiden luominen paperisille asiakirjoille on suhteellisen helppoa, mutta sähköisten tallenteiden käsittely on niin monimuotoista, että uusia menettelyitä, ohjeita ja parhaita käytäntöjä joudutaan etsimään ja muokkaamaan kaiken aikaa.

3 Säädöspohja

3.1 Yleistä

Tarkastelun kohteena ovat sekä viranomaisten kansalliset asiakirjat että kansainväliset asiakirjat.

Kansallisten asiakirjojen julkisuudesta on säädetty laissa viranomaisten toiminnan julkisuudesta, jota kutsutaan yleisesti julkisuuslaiksi. Lain pohjalta on annettu kaksi asetusta; Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 12.11.1999/1030 sekä Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681. Asiakirjojen salassapito voi perustua julkisuuslain lisäksi myös muuhun lainsäädäntöön kuten henkilötietolakiin tai viranomaisia ja niiden tietojärjestelmiä koskevaan substanssilainsäädäntöön.

Kansainvälisten asiakirjojen käsittelystä on annettu laki kansainvälisistä tietoturvallisuusvelvoitteista 24.6.2004/588 ja salassapito perustuu yleensä seuraaviin määräyksiin tai sopimuksiin:

- EU Neuvoston päätös turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi (2011/292/EU)
- NATO:n turvallisuussäännöstö ”Security within the North Atlantic Treaty Organisation, Document C-M(2002)49, 17.6.2002” liitteineen ja direktiiveineen, erityisesti ”NATO Security Committee Directive on the Security of Information AC/35-D/2002-REV3”
- muut EU ja NATO-säädökset
- Suomen ja muiden maiden kahdenväliset bilateraalisopimukset

Suomen kansallinen turvallisuusviranomainen NSA (National Security Authority) on antanut ohjeen kansainvälisten turvallisuusluokiteltujen tietoaineistojen käsittelystä. NSA-toiminnasta vastaa Suomessa ulkoasiainministeriö.

3.2 Julkisuuslaki ja siihen liittyvät asetukset

Julkisuuslain 24§ määritellään mitkä viranomaisen asiakirjat ovat salassa pidettäviä. Lisäksi sen 18§ säädetään hyvästä tiedonhallintatavasta, jota viranomaisen tulee noudattaa asiakirjoja käsitellessään. Julkisuuslain perusteella on annettu kaksi asetusta:

- Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta, 12.11.1999/1030 ja
- Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa, 681/2010.

Vuoden 1999 asetuksessa määriteltiin tarkemmin, miten hyvää tiedonhallintatapaa tulee toteuttaa sekä miten salassa pidettävät asiakirjat luokitellaan ja miten luokiteltuja asiakirjoja käsitellään. Asetuksessa säädetty luokitustapa ei kuitenkaan vastannut kansainvälistä luokittelua ja siitä syystä asetuksen pykälät 2 ja 3 korvattiin uudella asetuksella, joka saatiin pitkällisen kirjoitustyön päätteeksi voimaan 1.10.2010.

Vuonna 2010 julkaistun asetuksen mukaan salassa pidettävät tietoaineistot luokitellaan suojaustasoille sen mukaan miten vakavaa haittaa tai vahinkoa salassa pidettävän tiedon paljastumisesta ulkopuolisille aiheutuu. Suojaustasoja on neljä (ST I – ST IV), joista suojaustaso I on kaikkein korkein. Lisäksi salassa pidettäviin asiakirjoihin voidaan tehdä erityinen turvallisuusluokitusmerkintä julkisuuslain 24 §:n 1 momentin 2 ja 7—10 kohtien mukaan jos tiedon paljastuminen voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle.

Tässä asetuksessa on tietoaineistojen luokittelun ja käsittelyn ohella säädetty toinenkin velvoite, joka on erittäin tärkeä viranomaisten tietoturvallisuuden kannalta. Asetuksessa on kuvattu tietoturvallisuuden perustaso sekä velvoitettu, että kaikkien viranomaisten tulee saavuttaa tietoturvallisuuden perustaso sekä korotettu tai korkea tietoturvataso silloin kun käsitellään suojaustason III tai sitä korkeamman suojaustason materiaalia. Perustaso tulee saavuttaa kolmen vuoden siirtymäajan puitteissa eli lokakuun 2013 alkuun mennessä, korotetun ja korkean tason siirtymäaika on viisi vuotta siitä kun

viranomainen on päättänyt luokitella tietonsa tietoturvallisuusasetuksen mukaisesti.

Julkisuuslaki koskee kaikkea julkishallintoa, sen perusteella annetut asetukset sen sijaan vain valtionhallintoa. Asetusten ulkopuolelle jäävät mm. kunnat, yliopistot ja valtion liikelaitokset.

3.3 Kansainväliset säädökset

3.3.1 EU Neuvoston päätös turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi

EU neuvoston antama turvallisuussäännöstö koostuu useista määräyksistä, jotka muodostavat hierarkisen kokonaisuuden. Otsikossa mainittu ja lähdeluettelossa listattu päätös turvallisuussäännöistä muodostaa säännöstön ylimmän tason ja sen alle kuuluu iso joukko erilaisia sääntöjä ja määräyksiä. Ylimmän tason säännöstö on julkinen dokumentti, joka on julkaistu EU:n virallisessa lehdessä. Suurin osa tarkentavista dokumenteista on merkitty salassa pidettäviksi ja näin ollen vain niiden viranomaisten saatavilla, jotka käsittelevät luokiteltua EU-tietoa. Tarkentavissa määräyksissä asetetaan vaatimuksia mm. salaustuotteille, verkkoratkaisuille ja hajasäteilyn suojaukselle.

3.3.2 NATO Security Committee Directive on the Security of Information AC/35-D/2002-REV

Myös NATO:n turvallisuussäännöstö koostuu useista dokumenteista. Otsikon mukainen säännöstö on merkitty leimalla ”NATO unclassified”, joka tarkoittaa että dokumentti ei ole turvallisuusluokiteltu, mutta ei myöskään täysin julkinen. Dokumentti löytyy kuitenkin internetistä.

3.3.3 Suomen ja muiden maiden kahdenväliset bilateraalisopimukset

Suomi on tehnyt useiden kymmenien maiden kanssa kahdenvälisiä sopimuksia turvallisuusluokitellun tiedon vastavuoroisesta suojaamisesta. Näissä sopimuksissa on kuvattu miten eri maiden luokitellut tiedot vastaavat toisiaan ja mitkä ovat ne velvoitteet joita asiakirjojen käsittelyyn liittyy. Lisäksi sopimuksissa on kuvattu kummankin maan toimivaltaiset turvallisuusviranomaiset ja heidän velvoitteensa. Kahdenvälinen turvallisuussopimus mahdollistaa turvallisuusselvitysten teettämisen toisen maan kansalai-

sista tai yrityksistä ja siten mahdollistaa kaupallisen yhteistyön myös silloin kun siihen liittyy salassa pidettäviä tietoja.

3.3.4 Muut EU ja NATO-säädökset

Vaikka EU:lla ja NATO:lla on yleinen turvallisuussäännöstö, niin kaikki niiden alaiset toimielimet eivät noudata säännöstössä kuvattua tietojen luokitusta. Esimerkiksi EU:ssa rahoitusmarkkinoihin liittyvillä toimielimillä on käytössä oma kolmiportainen luokitus, johon liittyvä käsittelysäännöstö poikkeaa merkittävästi EU:n yleisistä turvaluokiteltujen tietojen käsittelysäännöistä.

3.3.5 Kansainvälisten säädösten toteuttaminen Suomessa

Suomessa ylin politiikkataso ja sen toteutumisen valvonta NSA:n vastuulla. Alatason politiikkojen toteuttamisesta ja niihin liittyvistä kansallisista ohjeista ja toimenpiteistä vastaavat määrätyt turvallisuusviranomaiset (DSA, Designated Security Authority), joita ovat Puolustusvoimat, Suojelupoliisi ja Pääesikunta sekä kansallinen tietoturvaviranomainen Viestintäviraston NCSA-yksikkö (National Communications Security Authority).

Ulkoasiainministeriön sivuilta löytyy lista kahdenvälisistä sopimuksista. Listaus tosin on vuodelta 2009, joten se on todennäköisesti vanhentunut. Varsinaiset sopimukset löytyvät lakitietokannasta www.finlex.fi.

3.4 Kansallisen ja kansainvälisten EU- ja NATO-merkintöjen vastaavuus

Alla olevassa taulukossa on esitetty miten tietoturvallisuusasetuksen ja edellä mainittujen EU:n ja NATO:n turvallisuussääntöjen luokitukset vastaavat toisiaan:

Kansallinen luokitus		EU	Nato
ST I	Erittäin salainen	EU TOP SECRET (EU TS)	COSMIC TOP SECRET (CTS)
ST II	Salainen	EU SECRET (EU-S)	NATO SECRET (NS)
ST III	Luottamuksellinen	EU CONFIDENTIAL (EU-C)	NATO CONFIDENTIAL (NC)
ST IV	Käyttö rajoitettu	EU RESTRICTED (EU-R)	NATO RESTRICTED (NR)
Ei vastaavuutta		EU Limite	NATO Unclassified
	Julkisuuslaki 24 §, 1 mom. 2 ja 7-10 k.		

4 Säädösten täytäntöönpano Suomessa

Seuraavissa kappaleissa on kuvattu erilaisia ohjeita, joiden tarkoituksena on konkretisoida kansainvälisiin ja kansallisiin säädöksiin ja määräyksiin sisältyviä velvoitteita.

4.1 Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje

Kansallinen turvallisuusviranomainen NSA, joka toimii ulkoasiainministeriössä, on 30.11.2010 antanut ohjeen kansainvälisen turvallisuusluokitellun tietoaineiston käsittelystä. Ohje kuvaa yleiset kansainväliseen turvallisuusluokiteltuun aineistoon liittyvät velvoitteet, mutta se ei korvaa alkuperäisiä sopimusmääräyksiä tai muita kansainvälisiä tietoturvallisuusvelvoitteita. Viranomaisten, jotka käsittelevät kansainvälisiä aineistoja, tulee itse huolehtia velvoitteiden toteutumisesta.

Kansallisista ja kansainvälisistä turvallisuusselvityksistä Suomessa vastaavat DSA-viranomaiset.

4.2 KATAKRI

KATAKRI eli kansallinen turvallisuusauditointikriteeristö on turvallisuusviranomaisten ja elinkeinoelämän yhteistyönä valmisteltu auditointi- ja tarkastuskriteeristö. Katakrin vaatimukset on laadittu kansallisten ja kansainvälisten velvoitteiden pohjalta ja sitä käytetään suomalaisten organisaatioiden turvallisuustason todentamiseen silloin kun ne käsittelevät valtionhallinnon tai kansainvälisten sopijapuolten turvallisuusluokiteltuja aineistoja tai osallistuvat turvallisuushankkeisiin.

Katakria käytetään myös silloin, kun suomalaisten yritysten turvallisuustaso varmennetaan kansainvälisen viranomaispyynnön perusteella ja tavoitteena on yritysturvallisuustodistuksen myöntäminen.

Turvallisuusauditointikriteeristö jakaantuu neljään osioon, jotka ovat hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus.

Katakrin ensimmäinen versio julkaistiin vuonna 2009 ja päivitetty versio 2.0 vuonna 2011. Vuonna 2012 käynnistyi Katakrin päivitystyö, jonka seurauksena on tarkoitus julkaista versio 3 syksyllä 2013. Päivitystyön yhteydessä auditointikriteeristöä mahdollisesti täydennetään lisäosioilla.

4.3 VAHTI 2/2010

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI julkaisi marraskuussa 2010 ohjeen tietoturvallisuusasetuksen täytäntöönpanon tueksi. Ohjeessa pääosa sisällöstä käsittelee salassa pidettävän tietoaineiston käsittelyä ja sitä, miten viranomaisten tulisi organisoida niihin liittyvät turvatoimenpiteet.

Toinen viranomaisten kannalta merkittävä asia ohjeessa on tietoturvatasojen määrittely ja eri tietoturvatasoille asetetut vaatimukset, jotka viranomaisten tulee toteuttaa. Tietoturvatasomääritykset on alun perin laadittu erillisessä hankkeessa, mutta niiden toteuttamisvelvoite haluttiin sitoa tietoturvallisuusasetukseen, joten myös tasovaatimukset sisällytettiin asetuksen täytäntöönpanoa koskevaan ohjeeseen.

Tietoturvatasojen toteuttaminen vaatii tietoturvallisuuden huomioimista kaikissa viranomaisten prosesseissa. VAHTI 2/2010 ohjeessa kuvatut tietoturvatasojen vaatimukset kohdistuvat sekä organisaatioon että sen omistamiin tietojärjestelmiin. Vaatimukset koskevat menettelytapoja, prosesseja, tehtävien organisointia ja vastuita ja niiden toteuttaminen on edellytyksenä viranomaisen tietoturvallisuuden turvaamiselle.

4.4 Muita VAHTI-ohjeita

Tietoturvatasot jakaantuu kahteen vaatimuskokonaisuuteen, joista ensimmäinen kohdistuu organisaatioon ja toinen ICT-ympäristöön. Nämä vaatimukset kohdistuvat prosesseihin ja ovat luonteeltaan hallinnollisia, joten ne eivät anna riittävän tarkkoja määrityksiä teknisten ympäristöjen toteuttamiselle.

Samanaikaisesti tietoturvatasojen määrittelyn kanssa laadittiin VAHTI-ohjetta valtionhallinnon sisäverkoille. Myös tässä ohjeessa päätettiin ottaa näkökulmaksi salassa pidettävän tietojen suojaus ja määritellä verkon rakenteen, tekniikan ja palveluiden vaatimukset erikseen perus-, korotetulle ja korkealle tasolle. Toteutuksen taso tulee valita tietoaineiston luokituksen mukaan. Sisäverkko-ohje, VAHTI 3/2010 julkaistiin joulukuussa 2010.

Sisäverkko-ohje ei vielä riittänyt kattamaan kaikkia teknisiä ratkaisuja. Tätä puutetta pyrittiin korjaamaan VAHTI-hankkeessa, jossa laadittiin Teknisen ympäristön tietoturvataso-ohje, VAHTI 3/2012. Ohjeessa täsmennetään tietoturvatasojen vaatimuksia ja kerrotaan yksityiskohtaisella tasolla miten ne pitää teknisissä ympäristöissä toteuttaa. Lisäksi ohjeen mukana julkaistiin erilaisia apuvälineitä, jotka tukevat tietoturvatasojen toteuttamista valtionhallinnossa. Näistä eniten käytetty on ollut Tärkeysjärjestys-apuväline, jota käytetään organisaation palveluiden tai tietojärjestelmien kriittisyysluokitukseen.

VAHTI:n antamaa ohjetta Valtion ICT-hankintojen tietoturvaohje, VAHTI 3/2011 käsitellään kappaleessa 4.7.6.

4.5 VAHTI Tilaturvallisuusohje

Salassa pidettävän tietoaineiston käsittely edellyttää turvallisia toimitiloja, mutta niille ei ole aiemmin ollut kattavaa vaatimusmäärittelyä. Katakri sisältää toimitiloja koskevia vaatimuksia, mutta Katakrin vaatimukset eivät ole pakollisia niille viranomaisille ja järjestelmille, jotka käsittelevät kansallista salassa pidettävää ainaistoa.

Tämän puutteen korjaamiseksi perustettiin keväällä 2012 VAHTI-työryhmä, jonka tehtävänä oli laatia ohje tietoturvallisille toimitiloille. Ohje oli lausun-

tokierroksella marraskuussa 2012 ja se julkaistaan keväällä 2013. Ohjeessa on kuvattu toimitiloille asetettavat vaatimukset silloin kun käsitellään salassa pidettävää tietoaineistoa. Ohjeluonnos sisältää myös vaatimukset IT-laitetiloille, joten se korvaa vanhan VAHTI-ohjeen Tietoteknisten laitetilojen turvallisuussuositus, VAHTI 1/2002. Ohjeessa otetaan kantaa myös sähkömagneettiseen hajasäteilyyn, jota käsitellään tarkemmin seuraavassa kappaleessa.

4.6 Sähkömagneettinen hajasäteily

Salassa pidettäviä tietoja suojattaessa myös sähkömagneettisen hajasäteilyn riskit tulee ottaa huomioon. Kaikki elektroniset laitteet, kuten tietokoneet, lähettävät ympäristöönsä säteilyä, jota kaappaamalla seurantakohteen laitteiston säteilemää informaatiosisältöä pystytään seuraamaan.

Tietyn laitteen seuraaminen ja erityisesti erottaminen muista säteilylähteistä vaatii hyökkääjiltä resursseja, joten seurannan todennäköisyys ja siitä aiheutuva riski pitää arvioida tiedon luottamuksellisuuden ja hyökkääjän resurssien mukaan. Kansainvälisissä EU- ja NATO-turvamääräyksissä hajasäteilyn suojaus tulee ottaa huomioon turvallisuusluokasta III lähtien. Suojaustasoille luokitelluissa kansallisissa tietoaineistoissa riski tulee arvioida käsiteltäessä suojaustason III tietoa, mutta kustannussyistä suojaus on pakollinen vasta ST II lähtien. Suojaustasoilla I ja II kansalliset ja kansainväliset vaatimukset ovat yhtenevät.

EU:n ja NATO:n hajasäteilyä koskevat määräykset ovat lähes samoja. Viestintävirasto valmistelee kansallista ohjeistusta, joka julkaistaan vuonna 2013 VAHTI tilaturvallisuusohjeen julkaisun jälkeen.

Hajasäteilyä voidaan estää joko tilojen tai laitteiden suojauksella. Toimitiloja suojattaessa tilojen ulkopuolelle kantautuvaa säteilyä voidaan vähentää käyttämällä sellaisia seinärakenteita, jotka vaimentavat säteilyä mahdollisimman tehokkaasti. Toimitilat jaetaan vyöhykkeisiin ja valitaan kullekin henkilölle sopiva työtila vyöhykejaon perusteella. On päätettävä, kuka saa käsitellä luokiteltuja tietoja ja missä, ja työskentelytilat on sijoitettava vastaavasti.

Laitteita suojattaessa niihin rakennetaan erilaisia säteilyä vaimentavia suojakuoria tai -kerroksia. Hajasäteilyltä suojatut laitteet maksavat moninkertaisesti tavallisen laitteen verran ja niiden ylläpidettävyys on huono, sillä kokoonpanoa ei saa muuttaa ilman uutta hyväksyntää.

Kun halutaan arvioida kuinka todennäköistä laitteiden seuranta organisaation ulkopuolelta on, täytyy arvioida sekä kohteen kiinnostavuutta että myös mahdollisen seuraajan käytössä olevia resursseja. Riskejä arvioitaessa on otettava huomioon organisaation toiminnan luonne. Jos se kiinnostaa ulkopuolisia, niin esim. tuotekehitys tai ylin johto voivat olla kiinnostavia seurantakohteita. Riskin arvioinnissa kannattaa huomioida myös, että tietyn laitteen seuranta on helppoa, mutta sen identifiointi on vaikeaa.

4.7 Säädösten täytäntöönpanon tukeminen ja valvominen

4.7.1 Asiakirjojen luokittelu

Tietoturvallisuusasetuksessa säädetään seuraavaa: ”*Jos valtionhallinnon viranomainen on päättänyt luokitella asiakirjansa tietoturvallisuuden toteuttamiseksi, luokittelussa on noudatettava 3 luvussa säädettyjä perusteita.”* Asetus siis jättää luokituspäätöksen tekemisen viranomaisen omaan harkintaan. Jos päätöstä ei tehdä, niin tietoaineistojen luokittelu ja käsittely voi tapahtua jollain muulla perusteella, yleisimmin 1999 annetun asetuksen mukaisesti.

Tietoturvallisuusasetus määrittelee tietoturvallisuuden perustason siirtymäajaksi kolme vuotta, korotetun ja korkean tason viiden vuoden siirtymäaika sen sijaan käynnistyy luokituspäätöksestä ja voi vaihdella runsaasti eri viranomaisilla.

Ministeriöt voivat omilla hallinnonaloilla edellyttää alaisiaan virastoja tekemään luokituspäätöksen ja näin ottamaan asetuksen mukaisen luokituksen käyttöön.

4.7.2 Yhteishankkeet

Valtiovarainministeriö on käynnistänyt keväällä 2011 yhteishankkeet tietoturvallisuusasetuksen toimeenpanon tukemiseksi. Hankkeiden käytännön toteutuksesta vastaa Valtion IT-palvelukeskus, joka oli jo aiemmin aloitta-

nut vastaavan hankkeen toteutuksen kuuden asiakasministeriön kanssa. Tästä hankkeesta saatuja kokemuksia käytettiin hyväksi VM:n yhteishankkeissa. Hankkeita käynnistettiin alun perin kolme kappaletta 2011 – 2012, mutta vuoden 2012 lopussa päätettiin käynnistää vielä neljäs hanke, jonka työ alkoi tammikuussa 2013. Yhteishankkeissa on mukana kaikkiaan noin 70 ministeriötä ja virastoa. Hankkeissa pääpaino on tietoturvallisuuden perustason saavuttamisessa, mutta osana perustason saavuttamista niissä käsitellään myös tietoaineistojen luokittelua ja käsittelyä. Hankkeet toimivat työpajamuotoisesti ja kuukausittaisissa tapaamisissa käsitellään valittua tietoturvallisuuden osa-aluetta, jonka toteuttamiseen osallistujille tarjotaan neuvoja, ohjeita, malleja ja muiden osallistujien kokemuksia. Osallistujilta edellytetään sitoutumista hankkeen työskentelyyn sekä aktiivista osallistumista, joka ilmenee mm. kotitehtävien suorittamisena.

Yhteishankkeissa pyritään toteuttamaan kussakin organisaatiossa tietoturvallisuuden hallintajärjestelmä. Osana hallintajärjestelmän muodostamista kartoitetaan organisaation suojattavat kohteet. Suojattaviin kohteisiin kuuluu organisaation tieto-omaisuus, joka pitäisi pystyä luokittelemaan oikein ja valita suojaustoimenpiteet luokituksen mukaan.

4.7.3 Muut valtion IT-palvelukeskuksen tietoturvapalvelut

Valtion IT-palvelukeskuksen tietoturvapalvelut-yksikkö tukee yhteishankkeiden toteuttamista ja muuta viranomaisten tietoturvatyötä ja vaatimusten täytäntöönpanoa tarjoamalla viranomaisten käyttöön erilaisia ohjeita ja mallipohjia. Lisäksi tarjotaan asiakkaiden käyttöön omaa asiantuntijatyötä tietoturvapäällikköpalveluna tai tuntityönä. Ulkopuolisten toimittajien tuottamana tarjotaan skannauspalveluita sekä yhteisesti kilpailutettuja auditointi- ja konsultointipalveluita.

4.7.4 Auditoinnit

Kansainvälisten turvallisuusluokiteltujen tietoaineistojen käsittelyn ohjeistamisesta ja valvonnasta vastaa kansallinen turvallisuusviranomainen NSA. Se ohjaa kansallista toimintaa ja vastaa muun muassa kansainvälisten turvallisuussopimusten valmistelusta. Sen apuna velvoitteiden toimeenpanossa toimivat määrätyt turvallisuusviranomaiset (DSA, Designated Security Authority), joita ovat puolustusministeriö, suojelupoliisi ja pääesikunta. Niillä kullakin on omat vastuualueet kansallisen turvallisuusviranomaisen tehtävä-

kentässä. Viestintävirasto toimii kansallisena tietoturvaviranomaisena (NCSA, National Communications Security Authority), joka vastaa turvallisuusluokitellun aineiston sähköiseen tiedonsiirtoon ja -käsittelyyn liittyvistä tehtävistä Suomessa. Turvallisuusviranomaiset huolehtivat mm. henkilöiden ja yritysten turvallisuusselvityksistä sekä kansainvälisiin velvoitteisiin liittyvistä auditoinneista. Ne käyttävät auditointikriteeristönään Katakria. NCSA voi antaa auditoidulle tietojärjestelmälle virallisen hyväksynnän eli akkreditoinnin osoituksena siitä, että se täyttää sille asetetut vaatimukset. Auditoinneista on annettu Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011).

Myös EU- ja NATO-viranomaiset suorittavat auditointeja niihin viranomaistahoihin, jotka käsittelevät EU:n tai NATO:n turvallisuusluokiteltuja tietoaineistoja. Auditoinnit perustuvat em. järjestöjen turvallisuussääntöihin sekä kunkin viranomaisen omiin vaatimuksiin.

Kansallisen salassa pidettävän tietoaineiston käsittely tulee tapahtua tietoturvallisuusasetuksen mukaisesti. Asetus on annettu oikeusministeriön toimesta, ja asetus sekä sen toimeenpanoa tukeva ohjeistus on laadittu yhteistyössä VAHTI:n kanssa. Kansallisella puolella ei salassa pidettävän tietoaineiston käsittelylle ole kuitenkaan määritelty auditointivelvoitetta. Valtion IT-palvelukeskus tarjoaa palveluita kaikille valtionhallinnon viranomaisille ja tukee tietoturvallisuusasetuksen toimeenpanoa edellyttämällä asiakkailtaan hyvää tietoturvallisuutta. VIP:in palveluiden käyttöönoton edellytyksenä on, että sen palveluihin liittyvällä asiakkaalla ei saa olla kriittisiä poikkeamia tietoturvallisuuden perustasoon nähden. Asiakkaan tietoturvatason arvioi ulkopuolinen auditoija, ja asiakkaat useimmiten tilaavat auditoinnin VIP:in tietoturvapalveluiden kautta.

VM:n yhteishankkeiden tavoitteena on tietoturvallisuuden perustason täyttäminen todennetusti, joten VM edellyttää vastaavaa auditointia ja perustason saavuttamista kunkin yhteishankkeen päätyttyä siihen osallistuneilta organisaatioilta.

4.7.5 VM:n tietoturvakysely

Valtiovarainministeriö tekee vuosittain valtionhallinnolle tietoturvakyselyn, jossa kartoitetaan ministeriöiden, virastojen ja laitosten tietoturvallisuuden tilaa. Tietoturvallisuusasetuksen voimaantulon jälkeen kyselyyn lisättiin

salassa pidettävien tietojen luokittelua ja käsittelyä sekä tietoturvatasoja koskevia kysymyksiä. Kyselyn tavoitteena on saada seurantatietoa tietoturvatason kehittymisestä, mutta vähintään yhtä tärkeä seikka on kiinnittää viranomaisten huomiota näiden seikkojen tärkeyteen. Kyselyn vastaukset kerää usein organisaation tietoturvavastaava, mutta monissa organisaatioissa vastaukset käsitellään organisaation johtoryhmässä tai ne menevät sinne ainakin tiedoksi.

4.7.6 Hankinnat

Sekä tietoturvallisuusasetus että kansainväliset vaatimukset edellyttävät, että viranomaisen tulee varmistaa salassa pidettävien tietojen oikea käsittely myös silloin kun joku ulkoinen osapuoli käsittelee tietoja viranomaisen toimeksiannosta. Tämä tarkoittaa, että säädökset on huomioitava silloin kun hankitaan ulkopuolisia tietojenkäsittelypalveluita tai ulkoistetaan viranomaistehtäviä. Vaatimukset tulee huomioida tarjouspyynnöissä ja sopimuksissa.

VAHTI on laatinut ohjeen Valtion ICT-hankintojen tietoturvaohje, VAHTI 3/2011, jossa kuvataan miten vaatimukset voi tarkoituksenmukaisella tavalla sisällyttää hankintoihin. Tietoturvavaatimukset pitää kuvata vaatimusmääritysvaiheessa samalla tavoin kuin muutkin tarjouspyyntöön sisällytettävät vaatimukset. Hankintavaiheessa vaatimukset tulee sisällyttää sopimuksiin ja palvelukuvauksiin, jotta palveluntarjoaja sitoutuu niiden toteuttamiseen. VAHTI hankintaohjeen liitteenä on mallipohjia vaatimuksille sekä turvallisuussopimukselle ja vaitiolositoumukselle.

Valtion IT-palvelukeskus on tuottanut hankintoja varten mallipohjia, joita voi käyttää hankinnoissa apuna. Vaikka malleja vaatimuksista löytyykin, niin hankintatilanteessa jokainen vaatimus pitää käydä erikseen läpi ja harkita sen soveltuvuus kyseessä olevaan hankintaan. Tietoturvatasojen tai Katakrin vaatimuksia ei siis sellaisenaan sisällytetä tarjouspyyntöihin, vaan kuvataan miten hankittavana olevan palvelun tulee toteuttaa viitekehyksissä asetetut vaatimukset.

Myös viranomaistehtävien ulkoistaminen usein edellyttää, että palvelua tuottavan sopimuskumppanin henkilöstö käsittelee salassa pidettäviä tietoja, kuten arkaluonteisia henkilötietoja. Myös näille sidosryhmille pitää asettaa tietoturvavaatimukset esimerkiksi turvallisuus- tai tietoturvasopimuksen

muodossa. Lisäksi salassa pidettäviä tietoja käsittelevät henkilöt tulee ohjeistaa ja kouluttaa hoitamaan tehtäviään oikealla tavalla.

5 Erityissuojattavan tietoaineiston käsittely käytännössä

5.1 Teoria vs. käytäntö

Viranomaisilta edellytetään luokituspäätöstä osoituksena siitä, että ne ovat ottaneet tietoturvallisuusasetuksen mukaisen luokituksen käyttöönsä ja alkavat toteuttaa asetuksen velvoitteita sekä tietoturvatasojen että tietojen luokituksen ja käsittelyn osalta. Vuoden 2013 alussa noin puolet ministeriöistä on tehnyt luokituspäätöksen ja virastoista vain murto-osa, vaikka asetus on ollut voimassa jo yli kaksi vuotta. VM:n tietoturvakyselyyn vastanneista viranomaisista kaksi kolmannesta ei ole tehnyt luokituspäätöstä vuoden 2012 loppuun mennessä.

Luokituspäätöksen teko edellyttää henkilökunnan ohjeistamista ja kouluttamista tietoaineistojen käsittelyn suhteen. Ohjeiden laadinta ei ole aina kovin helppoa; asetuksen antamat perusteet oikean luokan valinnasta ovat niin ylimalkaiset, että oikean luokituksen valinta voi olla haasteellista. Se on kuitenkin tärkeää, koska aliluokittelu voi johtaa tiedon paljastumiseen asiattomille ja yliluokittelu aiheuttaa kovemmat tietoturvavaatimukset. Korkeamman luokituksen edellyttämän korotetun tai korkean tietoturvatason toteuttaminen voi aiheuttaa merkittävä lisäkustannuksia.

Alussa ohjeistuksen puute oli luultavasti pääasiallinen syy luokituspäätöksen lykkäämiseen. Myöhemmin tärkeämpi syy on ollut luokituspäätöksestä käynnistyvä viiden vuoden siirtymäaika korotetulle tietoturvatasolle. Useimmilla viranomaisilla on suojaustasolle III kuuluvia tietoaineistoja, monilla merkittäviä määriä. Kaikkien näitä tietoja sisältävien tietojärjestelmien tulee täyttää korotetun tietoturvatason vaatimukset siirtymäajan puitteissa. Viranomaiset pelkäävät muutostoimenpiteistä aiheutuvia kustannuksia ja osittain siitä syystä lykkäävät luokituspäätöstä.

Hyvin monet viranomaiset ovat ulkoistaneet tietojärjestelmiensä käyttöpalvelut. Ulkoistetuissa palveluissa järjestelmille asetettavat tietoturvavaatimukset tulee huomioida tarjouspyynnöissä ja sopimuksissa. Ennen tietoturvallisuusasetuksen voimaantuloa hankituissa palveluissa niitä ei luonnollisestikaan ole pystytty huomioimaan, ja näin ollen vaatimukset täyttyvät vasta uusissa sopimuksissa. Uusien vaatimusten sisällyttäminen vanhoihin sopimuksiin kesken sopimuskauden on joko mahdotonta tai tulee yleensä suhteettoman kalliiksi.

Luokituspäätös ja asetuksen mukaisten ohjeiden noudattaminen ovat kuitenkin ainoa tae siitä, että viranomaiset pystyvät käsittelemään salassa pidettäviä tietoja samalla tavalla. Viranomaiset luovuttavat paljon tietoja toisille viranomaisille. Tietojen omistajan tai luovuttajan tulisi varmistaa vastaanottajan kyvykkyys käsitellä tietoa oikealla tavalla, mutta se on lähes mahdotonta, jos luokitus ei ole käytössä tiedon vastaanottajalla. Salassa pidettäviä tietoja käsitteleville voidaan toki laatia erillinen ohjeistus, mutta kaikkein helpoiten yhtenäiset käsittelymenettelyt voitaisiin toteuttaa edellyttämällä luokituspäätöstä ja sitä tukevaa ohjeistusta.

5.2 Suurimmat puutteet ja ongelmat käsittelyssä

5.2.1 Tietoaineiston oikea luokitus

Valtiovarainministeriön tietoturvakyselyssä kysyttiin vastaajilta mikä on korkein organisaatiossa käsiteltävän kansallisen ja kansainvälisen tietoaineiston luokitus. Kansallisissa aineistoissa 20 % vastaajista ilmoitti käsittelevänsä ST I aineistoa, kansainvälisissäkin aineistoissa oli useita vastaajia jotka ilmoittivat käsittelevänsä Top secret -tason aineistoa. Kansallisissa tietoaineistoissa yli puolet vastaajista ilmoitti käsittelevänsä joko ST I tai ST II aineistoa. Sen sijaan kansainvälisissä aineistoissa yli puolet vastaajista ilmoitti, ettei käsittele lainkaan turvallisuusluokiteltua aineistoa tai vastaajalla ei ole siitä tietoa.

ST I / TL I aineiston osuuden suuresta määrästä voi vetää sen johtopäätöksen, että viranomaiset joko yliluokittelevat tietoja tai vastaajat eivät tiedä minkä tasoista aineistoa eri organisaation osissa käsitellään.

5.2.2 Velvoitteiden tunteminen

Viranomaisten tulisi huolehtia salassa pidettävien tietojen suojauksesta velvoitteiden edellyttämällä tavalla. Erityisesti EU- ja NATO-tietojen käsittelyä koskevat velvoitteet ovat ehdottomia ja tulee huomioida sekä asiakirjojen sähköisessä että manuaalisessa käsittelyssä. Viranomaisilla ei kuitenkaan ole paljon auditoituja ja akkreditoituja tietojärjestelmiä. Tästä voisi päätellä, että viranomaiset joko eivät tunne heitä koskevia velvoitteita taikka eivät kykene täyttämään niiden vaatimuksia. Myös käytännön kokemus osoittaa, etteivät kaikki organisaatiot tai edes niiden nimetyt tietoturvavastaavat tunne salassa pidettävien tietojen käsittelyä koskevia velvoitteita.

5.2.3 Velvoittavuus

Vaikka viranomaisten tuleekin toiminnassaan noudattaa lakeja, niin lakisääteinen velvoittavuus ei aina riitä takaamaan oikeita toimintatapoja – tarvitaan myös muuta ohjausta. Esimerkiksi tietoturvallisuusasetus velvoittaa täyttämään tietoturvallisuuden perustason vaatimukset syyskuuhun 2013 mennessä. Lainsäädännössä ei ole kuitenkaan määritelty minkäänlaisia sanktioita eikä muita seuraamuksia velvoitteen täyttämättä jättämisestä. Tällä hetkellä on epäselvää, mitä säädöksen noudattamatta jättämisestä seuraa.

Toteuttamista voisi edesauttaa, jos asetuksen rikkominen olisi jotenkin sanktioitu. Velvoite voitaisiin esimerkiksi kytkeä tulosohjaukseen jolloin valtiovarainministeriö edellyttäisi sen täyttämistä muiden ministeriöiden kanssa tekemissään tulossopimuksissa ja ministeriöt puolestaan edellyttäisivät sitä oman hallinnonalansa virastoilta.

Myös tietohallintolaki (Laki julkisen hallinnon tietohallinnon ohjauksesta 634/2011) voisi mahdollistaa vahvempaa velvoittavuutta.

5.2.4 Ristiriitaiset vaatimukset

Salassa pidettävien tietoaineistojen käsittelyn edellyttämät vaatimuskokonaisuudet – Tietoturvatasot ja Katakri – ovat päällekkäisiä ja ristiriitaisia. Tietoturvatasojen vaatimukset on laadittu Valtionvarainministeriön ValtIT-hankkeessa, samanaikaisesti mutta erillään tietoturvallisuusasetuksen valmistelusta. Kun vaatimusten velvoittavuutta alettiin pohtia, niin vaatimukset päätettiin sisällyttää osaksi tietoturvallisuusasetusta. Tietoturvatasojen vaatimukset perustuvat kypsyystasoajatteluun; eri tietoturvatasojen täyttyminen

kuvaa tietoturvaprosessien toimintaa eri kypsyystasolla. Lisäksi vaatimuksia voi toteuttaa monella eri tavalla, ja toteuttamistavan valinnassa käytetään apuna riskienhallintaa.

Katakrin auditointikriteeristö puolestaan on muokattu pääosin kansainvälisistä velvoitteista. Sen vaatimukset ovat ehdottomia, lisäksi joissakin kohdin perus-, korotetun ja korkean tason vaatimukset ovat identtiset.

Kirjoitushetkellä keväällä 2013 on menossa VAHTI-hanke, jonka tavoitteena on luoda työväline useiden eri vaatimuskokonaisuuksien samanaikaiseen hallintaan sekä tehdä ehdotuksia vaatimusten yhdenmukaistamisesta. Yhteensovittaminen on haasteellista, mutta hankeryhmä tulee kuitenkin esittämään kehitysehdotuksia, jotka voidaan huomioida tietoturvatasojen ja Katakrin päivitystyössä.

5.2.5 Suojaustaso- ja turvallisuusluokitus

Tietoturvallisuusasetuksessa määritelty kahden luokitustavan käyttö aiheuttaa hämmennystä monissa viranomaisissa. Suojaustasojen ja turvallisuusluokittelun ero ei ole selvää eikä aina tiedetä mitä luokitusta tulisi käyttää.

Kahden eri luokittelun käyttö on perusteltua, koska kansainvälisistä tietoturvallisuusvelvoitteista tulevia tiukkoja vaatimuksia ei haluta ulottaa kaikkeen kansalliseen tietoon. Kansallista luokiteltua tietoa on valtavia määriä ja tiukkojen turvakontrollien toteuttaminen tulisi erittäin kalliiksi ja joissain tapauksissa estäisi sähköisten asiointipalveluiden toteuttamisen.

Esimerkiksi verottaja on viime vuosina toteuttanut laajasti sähköisiä palveluita. Verotustiedot on luokiteltu suojaustasolle III. Jos ne luokiteltaisiin turvallisuusluokkiin ja toteutettaisiin niihin liittyvät turvallisuusvaatimukset, niin järjestelmien tietoturvavaatimusten toteuttaminen olisi erittäin haastavaa ja kallista. Pahimmillaan ne voisivat estää verotustietojen käytön sähköisessä asioinnissa.

Tiedon luokituksen aiheuttamat käsittelyvaatimusten erot aiheuttavat epätietoisuutta toimijoissa. Ei ole aina selvää pitäisikö kansallista turvallisuusluokiteltua tietoa käsitellä kuten kansainvälistä vai kuten vastaavaa suojaustasoluokiteltua tietoa.

5.2.6 Poikkeavat luokitukset

Kappaleessa 3.3.4 mainitut tavanomaisesta luokituksesta poikkeavat EU- ja NATO-luokitukset aiheuttavat haasteita näitä asiakirjoja käsitteleville viranomaisille. Poikkeaviin luokituksiin voi liittyä käsittelysääntöjä, jotka poikkeavat muiden asiakirjojen käsittelystä. Nämä viranomaiset joutuvat tekemään omat, erilliset ohjeet näiden asiakirjojen käsittelystä. Usein ohjeet joudutaan laatimaan osasto- tai yksikkökohtaisesti koska samat viranomaiset käsittelevät usean eri sopimuksen piiriin kuuluvaa kansainvälistä tietoa.

5.2.7 Tilojen ja laitteiden suojaaminen

Tilaturvallisuuteen ja hajasäteilyn suojaukseen liittyvien vaatimusten toteuttaminen aiheuttaa isot kustannukset. Niihin kumpaankin liittyvät vaatimuskokonaisuudet ovat vielä työn alla ja esimerkiksi toimitilaturvallisuuden osalta tietoturvallisuusasetuksen siirtymäaika on vain viisi vuotta. Tiloihin tehtävät muutokset eivät aina ole edes mahdollisia ja jos ovat, niin ne yleensä maksavat paljon. Vanhoihin tiloihin ja vuokrasopimuksiin muutoksia on hankalaa tehdä, kustannustehokkainta se on yleensä muuttojen ja remonttien yhteydessä.

Hajasäteilyn suojaukseen liittyvien vaatimusten täyttäminen voi olla teknisesti helpompaa, mutta se aiheuttaa aina merkittäviä kustannuksia. Myös nämä vaatimukset saadaan parhaiten huomioitua toimitilamuutosten yhteydessä.

5.3 Haasteet kansallisessa tietoturvatyössä

Suomessa viranomaisten tietoturvatyön suurin haaste lienee ohjauksen hajanaisuus. Valtiovarainministeriön Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI on yhteistyöelin, jonka asettamispäätöksessä todetaan ”*VAHTI toimii hallinnon tietoturvallisuuden ja tietosuojan kehittämisestä ja ohjauksesta vastaavien hallinnon organisaatioiden yhteistyö-, valmistelu- ja koordinaatioelimenä sekä edistää verkostomaisen toimintatavan kehittämistä julkishallinnon tietoturvatyössä*.” VAHTI julkaisee tietoturvallisuuden eri osa-alueille suosituksia, mutta niiltä puuttuu velvoittavuus. VAHTI on ylin valtionhallinnon tietoturvallisuudesta vastaava elin, mutta sillä ei ole toimivaltaa kansainvälisissä tietoturva-asioissa. Lisäksi myös kansallisella tasolla

on viranomaisia joilla on omaan sektoriin tai toimintakenttään kuuluvia tietoturvatehtäviä.

Kansainvälisissä tietoturvatehtävissä toimivia viranomaisia on useita, mutta niiden vastuualueet on selkeästi määritelty. Sen sijaan kansainvälisten ja kansallisten tehtävien vastuuraja on epäselvä. Viestintävirasto esimerkiksi tekee turvallisuustuotteiden evaluointeja, antaa määräyksiä ja julkaisee listaa hyväksytyistä salaustuotteista silloin kun käsitellään kansainvälistä turvallisuusluokiteltua tietoa. Tätä listaa ei kuitenkaan tarvitse noudattaa kansallisen tiedon käsittelyssä eikä kansallisella puolella ole vastaavaa viranomaista. Suomessa kuitenkin tietoturvaresurssit ja osaaminen ovat rajallisia, joten jossain tehtyä hyvää työtä kannattaisi hyödyntää myös muissa viranomaisissa.

VAHTI on julkaissut ohjeistusta jo 1990-luvulta lähtien. Koska ohjeistoa on kehitetty pitkän ajan kuluessa ja eri henkilöiden toimesta, niin ne ovat osittain päällekkäisiä ja ristiriitaisiakin. Lisäksi vanhoissa ohjeissa on vanhentuneita tietoja ja osioita, mutta ohjeet on haluttu pitää voimassa koska uusi ohjeistus ei ole niitä kokonaisuudessaan korvannut. VAHTI-ohjeet ovat suosituksia, mutta useimmat viranomaiset haluavat niitä noudattaa ja käyttää ohjenuorana tietoturvatyössään. Ohjeita käytetään laajasti myös valtionhallinnon ulkopuolella.

6 Johtopäätökset ja suositukset

6.1 Tietoturvallisuuden ohjaus

Tietoturvatyön ohjaus tulisi Suomessa keskittää yhteen paikkaan. Nyt ongelmana on se, että vastuut on hajautettu eri viranomaisille ja hallinnonaloille, ja kukin toimija haluaa pitää kiinni saamastaan vallasta ja vastuusta. Tietoturvatoimien toteuttamista viranomaisissa helpottaisi huomattavasti jos ohjaus tulisi yhdestä paikasta ja vaatimukset olisivat yhteneväiset.

Yhtenäinen ohjaus on nähdäkseni mahdollista vasta sitten kun valtionhallinnon keskushallinnon uudistus toteutuu. Kun ministeriöiden hallinnollisia tehtäviä yhdistetään niin on mahdollista, että myös tietoturvatyön ohjausta voidaan toteuttaa yhdestä paikkaa.

Lisäksi Suomen kansalliset ohjeet olisi hyvä koota yhtenäisen ohjeiston alle, jossa ylimmän tason muodostaa koko valtionhallintoa sitova tietoturvapolitiikka tai -määräys ja sen alle kootaan eri osa-alueita koskevia määräyksiä tai suosituksia.

6.2 Hallinnonalojen tietoturvavastuu

Nykyisessä tietoturvallisuuden ohjausmallissa VAHTI-johtoryhmä toimii valtiovarainministeriön JulkICT-toiminnon alaisena. Valtiovarainministeriöllä on käytössään tietohallintolain (Laki julkisen hallinnon tietohallinnon ohjauksesta, 10.6.2011/634) antama asetuksenantovaltuus. Mahdollista asetusta voitaisiin käyttää edesauttamaan tietojen luokitusta ja oikeaa käsittelyä koko valtionhallinnon laajuudessa.

Valtiovarainministeriö tekee muiden ministeriöiden kanssa vuosittain tulossopimukset, joissa asetetaan hallinnonalojen tulostavoitteet. Jokainen ministeriö tekee tulossopimukset oman hallinnonalansa virastojen kanssa. VM

voisi edistää tietoaineistojen luokittelua ja oikeaa käsittelyä liittämällä luokituspäätöksen teon ministeriöiden tulossopimuksiin. Tällöin ministeriöt myös helpommin ulottaisivat velvoitteen omille hallinnonaloilleen.

Kaikille ministeriöille suositellaan luokituspäätöksen tekemistä ja sen edellyttämistä myös niiden alaisilta virastoilta.

Tietoturvallisuusasetus on laadittu oikeusministeriössä valtiovarainministeriön ohjauksessa. Näiden kahden ministeriön tulisi edelleen tehostaa toimia asetuksen täytäntöönpanon tueksi. VM:n yhteishankkeet ovat auttaneet merkittävästi tietoturvallisuuden perustason toteuttamista valtionhallinnon organisaatioissa. Tällä hetkellä suurin ongelma onkin henkilökunnan tietoisuuden parantaminen tietoaineistojen oikeasta luokituksesta ja käsittelystä. Ministeriöiden tulisi käynnistää yhteiset koulutukset luokitusta toteuttaville henkilöille, joihin kuuluu virastoissa asiakirjahallinnosta ja tietoturvallisuudesta vastaavia henkilöitä, mutta myös lakimiehiä. Vastuuhenkilöille voitaisiin järjestää muutama koulutustilaisuus. Lisäksi tulisi tuotteistaa yhdessä Valtion IT-palvelukeskuksen kanssa henkilökunnan koulutuksia, joita voivat virastoille tilauksesta toteuttaa joko VIP:in virkamiehet tai VIP:ille palveluita tuottavat konsultit.

6.3 Jokaisen viranomaisen tietoturvavastuu

Viranomaisten tulee täyttää tietoturvallisuuden perustaso viimeistään syyskuussa 2013. Tietoturvatasoja ei tule nähdä niinkään yksittäisinä, pistemäisinä vaatimuksina vaan tietoturvallisuuden hallintajärjestelmänä, joka auttaa tietoturvallisuuden integroinnissa organisaation varsinaiseen toimintaan.

Kun tietoturvallisuuden hallintajärjestelmää rakennetaan, niin yksi ensimmäisistä toimenpiteistä on organisaation toimintojen ja niihin liittyvien suojattavien kohteiden kartoittaminen. Tieto-omaisuus on tärkein suojattava kohde, jota ilman mikään viranomainen ei pysty toimimaan. Kun tietoaineistoa kartoitetaan, samassa yhteydessä tulisi tarkistaa tietojen oikea luokitus. Salassa pidettäville tiedoille tulee antaa luokitus- ja käsittelyohjeet. Jokainen viranomainen tuntee itse omaan ydintoimintaansa liittyvät tiedot ja pystyy parhaiten arvioimaan niiden paljastumisesta aiheutuvan haitan. Siitä syystä jokainen organisaatio joutuu laatimaan oman ohjeistuksensa, mitään

yleispätevää ohjeistusta ei ole mahdollista laatia. Kun ohjeet on annettu, niin ne tulee jalkauttaa organisaatioon sekä sen tietoja käsitteleville sidosryhmille tiedotuksen ja koulutuksen avulla.

Kun organisaation tiedot on luokiteltu oikein, niin sen jälkeen tulee tarkistaa, että organisaation tilat ja tietojärjestelmät täyttävät luokitellun tiedon käsittelylle asetetut tekniset ja hallinnolliset tietoturvavaatimukset. On muistettava, että ST IV tietojen käsittelylle riittää tietoturvallisuuden perustaso, mutta ST III tietojen sähköinen käsittely edellyttää korotettua ja ST II tiedot korkeaa tietoturvatasoa. Kansainvälinen luokiteltu tieto edellyttää vastaavasti Katakrin oikean tason toteuttamista.

Jos tietoturvatason toteutumisessa on puutteita, niin niiden korjaus tulee vastuuttaa, aikatauluttaa ja budjetoida. Jos työtä on paljon, niin se kannattaa organisoida yhden tai useamman projektin toteutettavaksi.

On huomattava, että kansainvälistä luokiteltua tietoa käsittelevien viranomaisten joukko on rajallinen, sen sijaan kansallista ST III tietoa on kaikilla viranomaisilla, koska tähän luokkaan luokitellaan lain perusteella salassa pidettävät arkaluonteiset henkilötiedot. ST II luokiteltu tieto liittyy usein valmiusasioihin eikä niitä ole kaikilla viranomaisilla. Näin ollen korkean tietoturvatason vaatimukset koskevat vain osaa viranomaisista, korotetun tason vaatimukset käytännössä kaikkia, mutta niiden toteuttaminen voidaan rajata valittuihin toimintoihin tai tietojärjestelmiin.

Tietoturvatasojen organisaatiotason vaatimusten toteuttaminen vaatii pääosin työtä ja aiheuttaa vain vähän kustannuksia. Sen sijaan ICT-järjestelmiä koskevien vaatimusten toteuttaminen voi vaatia tietojärjestelmämuutoksia ja aiheuttaa näin huomattavia kustannuksia. Tehokkainta toimenpiteiden toteuttaminen on järjestelmämuutosten tai uusien hankintojen yhteydessä.

6.4 Suositukset palveluntarjoajille

Valtionhallinnon viranomaisten tulee täyttää tietoaineistojen käsittelyyn liittyvät vaatimukset omassa toiminnassaan, mutta niiden tulee ulottaa velvoitteet myös niihin sidosryhmiin, jotka hoitavat viranomaistehtäviä tai muuten käsittelevät viranomaisten salassa pidettäviä tietoja.

Yksi merkittävä sidosryhmä on erilaisia tietotekniikkapalveluita tarjoavat palvelutalot. Yhä useampi viranomainen ulkoistaa yrityksille tietoteknisiä tehtäviä tai käyttöpalveluita. Tietoturvatasoja koskevat vaatimukset tulee sisällyttää tarjouspyyntöihin ja palvelusopimuksiin jolloin ne koskevat palvelutoimittajia. Sama koskee Katakrin vaatimuksia silloin kun käsitellään kansainvälistä turvallisuusluokiteltua tietoa.

Tulevissa kilpailutuksissa palveluilta tullaan vaatimaan vähintään tietoturvallisuuden perustasoa, useissa tapauksissa myös korotettua tasoa. Korkean tietoturvatason ympäristöt ovat harvinaisempia, niitä toteuttavat lähinnä turvallisuusviranomaiset.

Jos IT-palvelutalot haluavat ennakoida tulevia kilpailutuksia, niin niiden kannattaa määritellä valmiiksi ne menettelytavat ja teknologiat joiden avulla ne aikovat toteuttaa perus- ja korotetun tietoturvatason ympäristöt. Tärkeintä on erilaisten toimintaprosessien määrittely ja niihin liittyvien palvelukuvausten laadinta. Kun määritystyö on tehty valmiiksi, niin palveluiden toteuttaminen on nopeampaa ja helpompaa. Se voi nopeuttaa ja helpottaa tarjousten laadintaa ja antaa toimittajalle kilpailuetua muihin tarjoajiin nähden.

7 Lähdeviitteet

EU Neuvoston päätös turvallisuussäännöistä EU:n turvallisuusluokiteltujen tietojen suojaamiseksi, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2011:141:0017:0065:FI:PDF

Kahdenväliset turvallisuussopimukset, www.finlex.fi

Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje, http://formin.finland.fi/public/download.aspx?ID=68032&GUID={25313BDA-49BD-43EF-B106-3E9CE01AF6B0}

Kansallinen Turvallisuusauditointikriteeristö, versio II, http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

Kansallinen turvallisuusviranomainen (National Security Authority, NSA), http://formin.finland.fi/public/default.aspx?nodeid=46935&contentlan=1&culture=fi-FI

Laki julkisen hallinnon tietohallinnon ohjauksesta 10.6.2011/634, http://www.finlex.fi/fi/laki/ajantasa/2011/20110634

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621, http://www.finlex.fi/fi/laki/ajantasa/1999/19990621

NATO Security Committee Directive on the Security of Information AC/35-D/2002-REV3, http://www.nbf.hu/anyagok/jogszabaly/AC_35-D_2002-REV2.pdf

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010, http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101028Ohjeti/name.jsp

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

Teknisen ICT-ympäristön tietoturva-ohje, VAHTI 3/2012 http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20121122Teknis/name.jsp

VAHTI asettamispäätös,
www.hare.vn.fi/mHankePerusSelaus.asp?h_iId=12914

VAHTI Toimitilojen tietoturvaohjeluonnos,
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20121102Toimit/name.jsp

Valtion ICT-hankintojen tietoturvaohje, VAHTI 3/2011,
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20111207Valtio/name.jsp

Valtiovarainministeriön tietoturvakyselyn tulokset 2011, VAHTI toiminta-kertomus 2011,
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20120606VAHTIn/name.jsp

Valtiovarainministeriön tietoturvakyselyn tulokset 2012, VAHTI toiminta-kertomus 2012 (ei vielä julkaistu)

Vieraiden valtioiden kanssa tehdyt sopimukset I - kahdenväliset (UM 2009),
http://formin.finland.fi/public/download.aspx?ID=43963&GUID={9B6C81B7-3862-49DA-8D01-38DE8E81EC2B}