

Pääsynvalvonta osana valtionhallinnon tietoturvallisuustasovaatimuksia

Isohanni, Juho

2013 Laurea Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Pääsynvalvonta osana valtionhallinnon tietoturvallisuustasovaatimuksia

Isohanni, Juho
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Marraskuu, 2013

Isohanni, Juho

Pääsynvalvonta osana valtionhallinnon tietoturvaluustasovaatimuksia

Vuosi	2013	Sivumäärä	38
-------	------	-----------	----

Opinnäytetyö perustuu pitkälti syksyllä 2010 voimaantulleeseen asetukseen tietoturvaluudesta valtionhallinnossa (681/2010; jäljempänä tietoturva-asetus). Asetuksen tavoitteena on luoda yhtenäiset menettelyt salassa pidettävien tietoaineistojen käsittelystä sekä edistää hyvän tiedonhallintatavan toteutumista valtionhallinnossa.

Tietoturva-asetus velvoittaa valtionhallinnon organisaatiota täyttämään tietoturvaluuden perustason 30.9.2013 mennessä. Tietoturvaluustasojen avulla määritellään organisaatiolle ja tietojenkäsittely-ympäristöille tekniset ja hallinnolliset vaatimukset. Yksi aihealue tietoturvasojen vaatimuksissa on pääsynvalvonta.

Opinnäytetyö esittelee tietoturva-asetuksen ja siihen liittyvän täytäntöönpano-ohjeen (Ohje tietoturvaluudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010) sekä käy läpi pääsynvalvonnalle asetetut tietoturvaluustasovaatimukset. Poikkeuksetta pääsynvalvonnan tietoturvaluustasovaatimukset kohdistuvat tunnistautumiseen, todentamiseen sekä lokitietoihin. Opinnäytetyössä käsitellään korostetusti edellä mainittuja pääsynvalvontamekanismeja.

Opinnäytetyössä tutkitaan pääsynvalvonnan tietoturvaluustasovaatimuksia laajemmassa mittakaavassa kuin niiden alkuperäisessä julkaisussa eli VAHTI 2/2010-ohjeessa. Opinnäytetyössä selvitetään myös millä toimenpiteillä vaatimuksia voidaan täyttää sekä esitellään joitakin esimerkkiratkaisuja.

Lopuksi opinnäytetyössä pohditaan pääsynvalvonnan tietoturvaluustasovaatimusten täyttymistä ja niiden aiheuttamaa työmäärä valtionhallinnossa. Pohdinta ulottuu myös opinnäytetyöprosessiin sekä sen aikana tapahtuneeseen uuden oppimiseen.

Isohanni, Juho

Access control as a part of information security levels in central government

Year	2013	Pages	38
------	------	-------	----

The implemented decree on information security in central government (681/2010; later referred to as information security decree) has been used as the theoretical framework for this thesis. The purpose of the decree is to create unified procedures for managing confidential information material in addition to improving the implementation of well thought-out data management practices in the central government.

The information security decree obligates the central government organisation to fulfil a base level in information security by 30.9.2013. The technical and administrative requirements for organisations and data processing environments are defined with the help of information security levels. One field of these information security level requirements is access control.

This thesis will present the information security decree and the implementation instructions manual attached to it (Instructions on Implementing the Decree on Information Security in Central Government, VAHTI 2b/2010) in addition to addressing requirements of information security set for access control. The requirements of information security levels for access control are without exception targeted at identification, authentication and log entries. The thesis will also study the aforementioned access control mechanisms with a highlighted emphasis.

This thesis will examine the information security requirements for access control in a wider context than they were examined in the original publication of the VAHTI 2b/2010- instructions. This thesis will also clarify the procedures on how these requirements are possible to fulfil while also presenting some exemplary solutions.

Finally the thesis will contemplate the fulfillment of the requirements for information security levels and the workload it causes for the central government. Considerations will also extend to the process of writing a thesis and the learning of new knowledge that took place while working on the thesis.

Keywords information security, access control, Government Decree on information security in central government, VAHTI, Identification, log

Sisällys

1	Tietoturvallisuus osana ihmisten ja organisaatioiden arkea.....	6
2	Tavoitteet ja rakenne	6
2.1	Rajaukset	7
3	Lainsäädäntö ja ohjaavat tekijät.....	7
3.1	Asetus tietoturvallisuudesta valtionhallinnossa.....	8
3.2	Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI	11
3.3	Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta.....	12
4	Tietoturvallisuus	14
5	Pääsynvalvonta	15
5.1	Pääsynvalvonnan suhde käyttövaltuushallintaan	15
5.2	Pääsynvalvontatyypit	16
6	Tunnistautuminen ja todentaminen	17
6.1	Käyttäjäidentiteetti	17
6.2	Salasana.....	19
6.3	Biometrinen tunnistus.....	20
6.4	Varmenteet.....	21
6.4.1	Varmennekortti	21
6.4.2	Mobiiliasiointivarmenne	22
6.5	TUPAS	22
7	Lokitiedostot	23
7.1	Lokitiedostot pääsynvalvonnassa	23
7.2	Sovellustason pääsynvalvontalokit	24
7.3	Verkkotason pääsynvalvontalokit.....	25
7.4	Tietoturvallisuustasovaatimukset ja lokien kerääminen	25
8	Yhteenveto ja arviointi	27
8.1	Yhteenveto tietoturvallisuustasovaatimusten toteuttamisesta	27
8.2	Opinnäytetyöprosessi	28
8.3	Tavoitteiden saavuttaminen	28
	Lähteet	30
	Kuvat.....	33
	Kuviot.....	34
	Taulukot	35
	Liitteet.....	36

1 Tietoturvallisuus osana ihmisten ja organisaatioiden arkea

Muutaman viime vuoden aikana tietoturvallisuuteen ja tietosuojaan liittyvien uutisten määrä on räjähdysmäisesti kasvanut mediassa. Nykymaailman kehityssuunta on, että yhä suurempi osa ihmisten elämästä siirtyy digitaaliseen maailmaan niin ajankäytön kuin henkilökohtaisten tietojen osalta. Ihmiset kertovat itsestään yhä enemmän julkisissa yhteisöpalveluissa ja jättimäiset monikansalliset yritykset kuten Google keräävät tiedot ja käyttävät niitä kaupallisiin tarkoituksiin. Tämän lisäksi on olemassa yksilöitä ja ryhmittymiä, jotka hakeroivat laittomasti esiin tietoja ihmisten yksityisestä elämästä kuten luottokorttinumeroita ja henkilötietoja. Erityisesti yhdistelemällä julkisia ja yksityisiä tietoja väärin tarkoituksiperin voidaan saada aikaan suurta vahinkoa niin taloudellisesti kuin sosiaalisestikin.

Ongelma ei ole ainoastaan tavallisten kansalaisten vaan myös yritysten sekä valtioiden. Hyvänä esimerkkinä on Suomen ulkoministeriön vakoiluskandaali, jossa ulkopuolinen taho on vuosien ajan vakoillut ministeriön tietoverkkoa (MTV3 2013). Valtionhallinto on viime vuosien aikana hitaasti herännyt tietoturvallisuuden tärkeyteen ja tästä esimerkkinä on vuonna 2010 voimaan tullut Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681 (tietoturva-asetus). Tämän opinnäytetyön juuret ovat edellä mainitussa tietoturva-asetuksessa, joka määrittää tietojenkäsittely-ympäristölle sekä hallinnollisia, että teknisiä vaatimuksia valtionhallinnossa. Tietoturva-asetuksen täytäntöönpanoa varten valtionvarainministeriö on julkaissut VAHTI-ohjeen nimeltä: Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, joka tarkentaa tietoturva-asetuksen vaatimuksia ja täsmentää vaatimusten täytäntöönpanon määräajat. (Valtiovarainministeriö 2010)

Olen työskennellyt joulukuusta 2012 lähtien valtionhallinnon organisaatiossa, joka on valtion virastona velvoitettu noudattamaan tietoturva-asetusta ja sen myötä VAHTI-ohjeiden vaatimuksia. Alun perin tarkoitukseni oli tehdä kehittämissuunnitelma opinnäytetyönä työnantajallani VAHTI-ohjeiden vaatiman korotetun tietoturvatason saavuttamiseksi. Suunnitelmat kariutuivat suureen määrään salassa pidettävää materiaalia, jota ei voi julkisessa opinnäytetyössä käsitellä. Edellä mainitun vuoksi keskityn opinnäytetyössäni perehtymään yhteen tietoturvallisuuden ja VAHTI-ohjeiden vaatimusten alaiseen osa-alueeseen: pääsynvalvontaan. Teen pääsynvalvonnasta tutkielmatyypin opinnäytetyön, jota työnantajani sekä muut tahot voivat käyttää vapaasti hyödykseen täyttäessään VAHTI-ohjeiden vaatimuksia.

2 Tavoitteet ja rakenne

Tämän opinnäytteen tavoitteena on tuoda ilmi mitä pääsynvalvonnalla tarkoitetaan ja minkälaisia menetelmiä sekä tekniikoita liittyy pääsynvalvontaan. Tavoitteena on myös selvittää miten pääsynvalvonta tulisi ottaa huomioon tietoturvallisuuden osana erityisesti valtionhallinnon organisaatiossa. Yhtenä tavoitteena on pohtia, minkälaisilla käytännön ratkaisuilla voidaan toteuttaa tietoturvaluustasojen tuomat vaatimukset.

Opinnäytetyössä käsitellään tietoturvaluuteen liittyvää lainsäädäntöä sekä valtionvarainministeriön VAHTI-ohjeiden vaatimuksia valtionhallinnon organisaatiolle. Myös pääsynvalvontaan liittyviä tietoturvaso-vaatimuksia käsitellään useaan otteeseen sekä pohditaan millaisilla käytännönratkaisuilla niitä voidaan täyttää. Lopuksi kokonaisuudesta tehdään yhteenveto, jossa pohditaan täyttyivätkö työlle asetetut tavoitteet.

2.1 Rajaukset

Tässä opinnäytetyössä käsitellään pääsynvalvontaa tietoturvaluuden teknisestä näkökulmasta, kuitenkin menemättä liian yksityiskohtaiselle tasolle. Pääsynvalvontaan keskitytään VAHTI 2/2010 -ohjeen liitteen 5 kohdan 2.6 vaatimusten mukaisesti, joka löytyy opinnäytetyön lopusta liitteenä numero kaksi. Sekä VAHTI-ohjeista että pääsynvalvontaan liittyvistä vaatimuksista kerrotaan tarkemmin niille osoitetuissa kappaleissa. Kaikki muu pääsynvalvonta jätetään opinnäytetyön ulkopuolelle kuten fyysinen kulunvalvonta.

Käsiteltävien teemojen valinta sekä painottaminen tuodaan suoraan tietoturvaluustasojen pääsynvalvontavaatimuksista. Tietoturvaluustasoissa painotetaan tunnistautumisen ja pääsynvalvontalokien tärkeyttä, joten tässä opinnäytetyössä samat teemat ovat korostettuja. Tietoturvaluustasojen korkea taso jätetään vähäisemmälle tarkastelulle, koska sen vaatimukset vaikuttavat selkeästi pienempään osaan valtionhallinnon organisaatioita kuin perustaso ja korotettu taso.

3 Lainsäädäntö ja ohjaavat tekijät

Syksystä 2010 lähtien valtionhallinnon tietoturvaluuden ohjaavana säädöksenä on ollut asetus tietoturvaluudesta valtionhallinnossa 681/2010 (tietoturva-asetus), joka on annettu lain viranomaisten toiminnan julkisuudesta 621/1999 (julkisuuslaki) nojalla. Ennen tietoturva-asetuksen voimaantuloa julkisuuslaki ohjasi viranomaisia huolehtimaan tietoturvaluudesta. VAHTI 2/2010 tiivistää hyvin julkisuuslain vaatimukset hyvästä tiedonhallintatavasta, jossa otetaan myös tietoturvaluus huomioon: "Lain mukaan viranomaisten on huolehdittava, että asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suoja, eheys ja laatu turvataan asianmukaisin menettelytavooin ja tietoturvajärjestelyin ottaen huomioon tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tieto-

turvatoimenpiteistä aiheutuvat kustannukset” (Valtiovarainministeriö 2010). Tietoturvallisuutta siis ohjaa, kuten muutakin viranomaisten toimintaa, lainsäädäntö. Tietoturvallisuuden ohjaavaksi ministeriöksi on valikoitunut valtiovarainministeriö, mutta myös muilla ministeriöillä voi olla hallinnonalaansa liittyviä ohjeistuksia, kuten kuviossa 1 näkyy. (Oikeusministeriö 2010)



Kuvio 1: Tietoturvallisuus sekä normit ja ohjaus (Valtiovarainministeriö 2013)

3.1 Asetus tietoturvallisuudesta valtionhallinnossa

Opinnäytetyössä keskeisenä säädöksenä on valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa, joka annettiin 1.7.2010 ja tuli voimaan 1.10.2010. Tietoturva-asetuksen tavoitteena on asettaa yhteneväiset vaatimukset tietoturvallisuudesta valtionhallinnon organisaatioille. Asetus velvoittaa viranomaisia erityisesti asiakirjojen luokitteluun sekä luokiteltujen asiakirjojen tietoturvalliseen käsittelyyn. Tietoturvallisuuden perustaso on tietoturva-asetuksen tuoma uudistus tietoturvallisuuden hallintaan valtionhallinnossa. Asetuksen 5 § määrittää, mitä tietoturvallisuuden perustaso tarkoittaa. Pykälä pitää sisällään 10 kohdan vaatimuslistan viranomaisille:

1. Viranomaisen toimintaan liittyvät tietoturvallisuusriskit kartoitetaan.
2. Viranomaisen käytössä on riittävä asiantuntemus tietoturvallisuuden varmistamiseksi ja että tietoturvallisuuden hoitamista koskevat tehtävät ja vastuu määritellään.
3. Asiakirjojen käsittelyä koskevat tehtävät ja vastuut määritellään.
4. Tietojen saanti ja käytettävyys eri tilanteissa turvataan ja luodaan menettelytavat poikkeuksellisten tilanteiden selvittämiseksi.
5. Asiakirjojen ja niihin sisältyvien tietojen salassapito ja muu suoja varmistetaan antamalla pääsy asiakirjoihin vain niille, jotka tarvitsevat salassa pidettäviä tietoja tai henkilörekisteriin talletettuja henkilötietoja työtehtäviensä hoitamiseksi.

6. Tietojen luvaton muuttaminen ja muu luvaton tai asiaton käsittely estetään käyttöoikeushallinnan, käytön valvonnan sekä tietoverkkojen, tietojärjestelmien ja tietopalvelujen asianmukaisilla ja riittävillä turvallisuusjärjestelyillä ja muilla toimenpiteillä.
7. Asiakirjojen tietojenkäsittely- ja säilytystilat ovat riittävästi valvottuja ja suojattuja.
8. Henkilöstön ja muiden asiakirjojen käsittelyyn liittyviä tehtäviä hoitavien luotettavuus varmistetaan tarvittaessa turvallisuusselvitysmenettelyn ja muiden lain perusteella käytettävissä olevien keinojen avulla.
9. Henkilöstölle ja muille asiakirjojen käsittelyyn liittyviä tehtäviä hoitaville annetaan ohjeet ja koulutusta asiakirjojen ja niihin sisältyvien tietojen asianmukaisesta käsittelystä.
10. Annettujen ohjeiden noudattamista valvotaan ja niiden muutostarpeita arvioidaan säännöllisesti. (Asetus tietoturvallisuudesta valtionhallinnossa, 5 §)

Tietoturva-asetuksen vaatimukset tietoturvallisuuden perustasolle ovat hyvin ympäröityä; pykälää lukemalla olisi hyvin vaikea täyttää perustason vaatimukset. Asetuksen täytäntöönpanon helpottamiseksi sekä tulkintavirheiden minimoimiseksi valtiovarainministeriön alainen yhteistyöryhmä VAHTI on tehnyt useita ohjeistuksia valtionhallinnon tietoturvallisuuden yhdenmukaistamiseksi. Erityisesti VAHTI 2/2010 ohjaa viranomaisia tietoturva-asetuksen täytäntöönpanossa.

Tietoturva-asetus tuo uutena uudistuksena valtionhallintoon uuden salassa pidettävien tietojen luokittelujärjestelmän: suojaustasot. Suojaustasot ovat jaoteltu välille I - IV, jossa suojaustaso I vaatii korkeimmat ja suojaustaso IV vähäisimmät suojausmenettelyt. Luokituksen ulkopuolella on julkinen tieto, jolle ei ole kohdennettu suojausmenettelyvaatimuksia. Tietoturva-asetuksen 9 § määrittelee suojaustasot seuraavasti:

”Salassa pidettävien asiakirjojen luokittelussa käytetään seuraavia luokkia:

- 1) suojaustaso I, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa erityisen suurta vahinkoa salassapitosäännöksessä tarkoitettulle yleiselle edulle;
- 2) suojaustaso II, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa merkittävää vahinkoa salassapitosäännöksessä tarkoitettulle yleiselle edulle;
- 3) suojaustaso III, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa salassapitosäännöksessä tarkoitettulle yleiselle tai yksityiselle edulle;

4) suojaustaso IV, jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa haittaa salassapitosäännöksessä tarkoitettulle yleiselle tai yksityiselle edulle.” (Asetus tietoturvallisuudesta valtionhallinnossa, 9 §)

Viranomaiset luokittelevat tarvittaessa salassa pidettävät tietonsa suojaustasojen mukaisesti. Esimerkiksi henkilötunnuksen sisältävä asiakirjaa tulee käsitellä suojaustason IV mukaisesti, ellei asiakirja sisällä muuta tietoa, jonka vuoksi sen käsittelyvaatimukset voisivat olla korkeamman suojaustason mukaiset. (Valtiovarainministeriö 2010)

Suojaustasojen lisäksi tietoturva-asetus toi mukanaan turvallisuusluokitusmerkinnät. Tiettyjen vaatimusten täyttyessä suojaustasomerkintään voidaan liittää turvallisuusluokitusmerkintä. Tietoturva-asetus määrittelee turvallisuusluokitusmerkinnät seuraavasti:

”Jos asiakirjan tai siihen sisältyvän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa vahinkoa kansainvälisille suhteille, valtion turvallisuudelle, maanpuolustukselle tai muulle yleiselle edulle viranomaisten toiminnan julkisuudesta annetun lain 24 §:n 1 momentin 2 ja 7-10 kohdassa tarkoitettulla tavalla, salassa pidettävän asiakirjan suojaustasoa koskevan merkinnän yhteyteen tai sen sijasta voidaan tehdä erityinen turvallisuusluokitusmerkintä.

Turvallisuusluokitusmerkintä tehdään:

- 1) suojaustasoon I kuuluvaan asiakirjaan merkinnällä "ERITTÄIN SALAINEN";
 - 2) suojaustasoon II kuuluvaan asiakirjaan merkinnällä "SALAINEN";
 - 3) suojaustasoon III kuuluvaan asiakirjaan merkinnällä "LUOTTAMUKSELLINEN";
 - 4) suojaustasoon IV kuuluvaan asiakirjaan merkinnällä "KÄYTTÖ RAJOITETTU".
- (Asetus tietoturvallisuudesta valtionhallinnossa 11 §)

Perusteet suojaustaso- tai turvallisuusluokitusmerkinnän käyttöön tulevat useammasta eri laista tai asetuksesta. Viranomaistoiminnassa julkisuuslain 24.1 § on usein käytetty peruste salassapidolle. Edellä mainitun pykälän kohdissa 3-6 ja 11-33 käytetään suojaustasomerkintää ja kohdissa 2, 7-10 käytetään turvallisuusluokitusmerkintää. Muita salassapitopykälä on kerrottu kuviossa 2, jossa kuvataan viranomaisen tietoja ja asiakirjoja kokonaisuutena. Kuviosta 2 voidaan huomata myös, että julkinen tieto on erotettu viranomaisen asiakirjojen turvaluokittelusta. Luvussa 3.4 kuvataan suojaustasojen ja turvallisuusluokitusmerkintöjen suhdetta tietoturvallisuustasoihin.

VIRANOMAISEN TIEDOT JA ASIAKIRJAT	
- Viranomaisen luomat tiedot ja asiakirjat - Viranomaisen vastaanottamat tiedot ja asiakirjat - Viranomaisen valmisteltavana olevat tiedot ja asiakirjat	
Viranomaisen asiakirjojen tietoturvaluokittelu	
Salassa pidettävä, viranomaisharkinta, käyttötarkoituussidonnaisuus	
Suojaustasomerkintä	Turvallisuusluokitusmerkintä
Suojaustaso I	ERITTÄIN SALAINEN
Suojaustaso II	SALAINEN
Suojaustaso III	LUOTTAMUKSELLINEN
Suojaustaso IV	KÄYTTÖ RAJOITETTU
TiTuA 681/2010, 9 § JulkL 621/1999 24.1 § 3-6, 11-33 K HetiL 523/1999 11 § Muu lainsäädäntö	TiTuA 681/2010, 11 § JulkL 621/1999 24.1 § 2, 7-10 k KansVäliTiTuL 588/2004, 8 §
JULKINEN TIETO	

Kuvio 2: Viranomaisen tiedot ja asiakirjat (Valtiovarainministeriö 2010)

3.2 Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI

VAHTI on valtiovarainministeriön alainen Valtionhallinnon tietoturvallisuuden johtoryhmä. VAHTIn tarkoituksena on toimia valtion tietoturvallisuuden kehityksen ja ohjauksen yhteistyöelimenä. VAHTI julkaisee VAHTI-ohjeita, jotka käsittelevät tietoturvallisuuden eri osa-alueita kuten: henkilöstöturvallisuus, sovelluskehityksen tietoturva, toimitilojen tietoturva ja ICT-hankintojen tietoturva. VAHTI-ohjeiden tarkoituksena on ohjata valtionhallinnon organisaatioiden tietoturvaa sekä auttaa sen kehittämisessä. (Valtiovarainministeriö 2013)

VAHTI kuvaa tavoitteitaan seuraavasti: "VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohejausta. VAHTI edistää Hallitusohjelman, Yhteiskunnan elintärkeiden toimintojen strategian (YETT), Valtion IT strategian ja hallituksen muiden keskeisten linjausten toimeenpanoa kehittämällä valtion tietoturvallisuutta ja siihen liittyvää yhteistyötä. VAHTI kehittää, yhteensovittaa ja ohjaa valtionhallinnon tietoturvallisuutta ja siihen liittyvää kansallista ja kansainvälistä yhteistoimintaa hallinnon kehittämisen, sähköisen hallinnon, toimintojen varmistamisen, tietoyhteiskuntakehityksen, tietoturvakehityksen ja -uhkien sekä toimintojen, tietojenkäsittelyn ja tietoliikenteen verkottumisen ja muun kehityksen edellyttämällä tavalla. VAHTI tukee toiminnallaan valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa ja sen valmistelussa." (Valtiovarainministeriö 2007)

VAHTI on jaettu kahteen ryhmään. Ensimmäinen on VAHTI-johtoryhmä, joka tekee valtionhallinnon tietoturvallisuuteen liittyvät linjaukset sekä on vastuullinen VAHTI - ohjeista. Toinen ryhmä on VAHTI-sihteeristö, jonka asiantuntijat valmistelevat VAHTI - ohjeet sekä toimeenpanevat varsinaisen VAHTI-johtoryhmän linjaukset. Sekä VAHTI-johtoryhmän että -sihteeristön asiantuntijat ovat virkamiehiä valtionhallinnon eri organisaatioissa ja he toimivat VAHTI:ssä oman virkansa ohessa. (Valtiovarainministeriö 2013)

3.3 Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta

Tämän opinnäytetyön näkökulmasta tärkein VAHTI - ohje on Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010. Kyseisessä ohjeessa käydään läpi hyvät tiedonhallinta- ja käsittelytavat, suojaustasot, tietoaineistojen luokittelu sekä tietotekniset että hallinnolliset tietoturva-vaatimukset. Erityisesti VAHTI 2/2010 -ohjeen liite 5 (Tietoturvallisuustasojen yksityiskohtaiset vaatimukset) on tämän opinnäytetyön kannalta tärkeä dokumentti. (Valtiovarainministeriö 2010)

Tietoturvallisuustasojen tarkoituksena on määrittää organisaatiolle ja sen tietojenkäsittelyympäristölle tekniset ja hallinnolliset vaatimukset. Tietoturvallisuustasot velvoittavat jokaista valtionhallinnon organisaatiota ja niiden saavuttamiseksi on tietoturva-asetuksessa määritelty aikataulut. Tietoturvallisuustasot ovat kolmeen eri vaatimusluokkaan: tietoturvallisuuden perustaso, korotettu taso ja korkea taso. Tietoturva-asetuksessa mainitaan ainoastaan vaatimukset tietoturvallisuuden perustason täyttämiseksi. Korotetun ja korkea tietoturvallisuustason vaatimukset tulevat ilmi VAHTI-ohjeista, kuten myös perustason tarkemmat vaatimukset. Tietoturva-asetuksen ja tietoturvatasojen vaikutukset pääsvalvontaan näkyvät suoraan tietoturvatasojen teknisten vaatimusten listassa, jossa pääsvalvonnalla on oma kokonaisuutensa (liite 1). (Valtiovarainministeriö 2010)

Tietoturva-asetus on tuonut valtionhallinnon tietoturvallisuuteen mukanaan suojaustasot, turvallisuusluokitusmerkinnät sekä tietoturvallisuustasot. Taulukossa 1 kuvataan mitkä ovat edellä mainittujen tasojen suhde toisiinsa. Esimerkkinä suojaustason IV materiaalia voidaan käsitellä perustason tietojenkäsittely-ympäristössä selväkielisenä. Mikäli materiaali on salattu, sitä voidaan käsitellä yhtä pykälää alemmalla tietoturvallisuustasolla. Esimerkiksi suojaustason III voidaan käsitellä salattuna perustason tietojenkäsittely-ympäristössä. Suojaustason I materiaali pitää olla aina vahvasti salattu ja sen käsittely on sallittua ainoastaan valvotuissa erillisverkoissa. (Valtiovarainministeriö 2010)

Suojaustaso	Turvallisuusluokitusmerkintä	Tietoturvaluokitus
Suojaustaso IV	Käyttö rajoitettu	Perustaso
Suojaustaso III	Luottamuksellinen	Korotettu taso
Suojaustaso II	Salainen	Korkea taso
Suojaustaso I	Erittäin salainen	Korkea taso + lisävaatimukset

Taulukko 1: Suojaustasojen ja turvallisuusluokitusten suhde tietoturvaluokituksiin

Alla olevassa listassa pääsynvalvontaan liittyvät tietoturvasov vaatimukset ovat jaoteltuna perus-, korotettuun ja korkeaan tasoon.

Perustaso:

1. Tietojärjestelmän omistaja hyväksyy kuinka luotettavaa identiteettiä ja vahvaa tunnistamista järjestelmän sisältämien tietojen käyttöön tarvitaan.
2. Sekä onnistuneet että epäonnistuneet sisäänkirjautumiset kirjoitetaan lokiin niin, että yksittäisen käyttäjän kirjautumiset järjestelmään voidaan selvittää ja yhdistää hänen henkilöllisyyteensä luotettavasti.
3. Huonolaatuisten salasanojen käyttöä estetään.
(Valtiovarainministeriö 2010)

Korotetun tason lisävaatimukset:

4. Organisaatiossa on kirjallinen pääsynvalvontapolitiikka, jossa kerrotaan mm. eri turvatasoilla hyväksyttävät tekniset tunnistusmenetelmät, tunnusten lukitus- ja avausperiaatteet sekä salasanan tai muiden tunnisteiden laatuvaatimukset ja vaihtoperiaatteet.
5. Pääsynvalvontalokit säilytetään niin, että niitä ei päästä jälkikäteen muuttamaan.
6. Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin tärkeimpiin järjestelmiin tai palveluihin aiheuttaa tunnuksen lukittumisen.
(Valtiovarainministeriö 2010)

Korkean tason lisävaatimukset:

7. Varmenteiden myöntämisestä, käytöstä ja uusimisesta on kirjallinen ohjeisto ja käytössä olevista varmenteista ajantasainen lista.
8. Korkean tason järjestelmissä pääsynvalvontalokeja ja kirjausketjuja tuotetaan myös järjestelmän sisällä toimimisesta toiminnan vaatimusten mukaisesti.
9. Tunnistuksen epäonnistumista ja muita oikeuksien puutteeseen kariutuvia toimenpiteyrityksiä tilastoidaan.
(Valtiovarainministeriö 2010)

Tietoturvallisuuden perustaso on alin sallittu taso viranomaisen tietojenkäsittely-ympäristölle. Valtionhallinnon viranomaisten on saavutettava tietoturvallisuuden perustaso viimeistään 30.9.2013. Määräaika korotetulle ja korkealle tietoturvaluustasolle on viisi vuotta siitä lähtien kun valtionhallinnon organisaatio on tehnyt tietojen luokittelupäätöksen. Saavutettava tietoturvataso määräytyy viranomaisen käsittelemien tietoa-aineistojen ja -järjestelmien luokittelun mukaan.

4 Tietoturvallisuus

Tietoturva-asetus määrittelee tietoturvallisuuden seuraavasti: "tietoturvallisuudella (tarkoitetaan) tietojen salassapitovelvollisuuden ja käyttörajoitusten noudattamiseksi sekä tietojen saatavuuden, eheyden ja käytettävyyden varmistamiseksi toteutettavia hallinnollisia, teknisiä ja muita toimenpiteitä ja järjestelyjä". (Asetus tietoturvallisuudesta valtionhallinnossa)

Tietoturvallisuuden (Information security / Data security) tarkoituksena on suojata tietoja palveluissa, tietoliikenteessä ja tietojärjestelmissä. Tietoturvallisuuden tavoitteena on tietojen luottamuksellisuuden, eheyden ja saatavuuden turvaaminen laitteisto- ja ohjelmistovikojen, luonnontapahtumien sekä tahallisten, tuottamuksellisten tai tapaturmaisten tekojen aiheuttamilta uhilta ja vahingoilta. Tietojen suojaaminen toteutetaan erilaisilla hallinnollisilla ja teknisillä menettelyillä, joihin perehdytään tässä opinnäytetyössä pääsynvalvonnan näkökulmasta. (Andreasson & Koivisto 2013, 29.)

Tietojen suojattavat ominaisuudet jaetaan tietoturvallisuudessa yleensä kolmeen osaan:

- Luottamuksellisuus (Confidentiality)
- Saatavuus (Availability)
- Eheyys (Integrity)

Luottamuksellisuudella tarkoitetaan, että tietoa pystyvät käsittelemään vain ja ainoastaan sellaiset henkilöt, joilla on siihen oikeus. Saatavuudella tarkoitetaan, että tieto on käytettävissä aina sitä tarvittaessa. Eheyttä suojatessa suojataan tiedon muuttumattomuutta ja paikansapitävyyttä. Tieto saa muuttua vain hallitusti ja sellaisen käyttäjän toimesta, jolla on oikeus muuttaa sitä. Tässä opinnäytetyössä keskistytään erityisesti luottamuksellisuuteen, koska pääsynvalvonta on yksi tapa suojata tiedon luottamuksellisuutta. (Järvinen 2003, 29-31.)

Luottamuksellisuutta, saatavuutta ja eheyttä täydennetään useasti kolmella lisäkäsitteellä:

- Kiistämättömyys (Nonrepudiation)
- Tunnistaminen (Identification)

- Todentaminen (Authentication)

Kiistämättömyydellä tarkoitetaan, ettei tiedon lähettäjä voi kiistää lähettäneensä viestiä tai olleensa jossain tapahtumassa osapuolena. Kiistämättömyyttä todennetaan varmenteilla ja aikaleimoille ja sen periaatteet liittyvät erityisesti tiedon eheyteen. Tunnistaminen tarkoittaa, että henkilö tunnustetaan tietyksi yksilöksi suuremmasta käyttäjämäärästä. Todentaminen liittyy oleellisesti tunnistamiseen. Todentamisen tarkoituksena on varmistaa, että tunnistautunut käyttäjä on se, joka hän väittää olevansa. Sekä tunnistaminen että todentaminen ovat erittäin tärkeitä osa-alueita pääsynvalvonnassa ja sen vuoksi niihin perehdytään syvällisemmin tämän opinnäytetyön luvussa 6. (Järvinen 2003, 32-33.)

Tietoturvallisuudesta puhuttaessa on hyvä määritellä myös tietosuojaa. Tietosuojasta puhuttaessa tarkoitetaan henkilöihin liittyvien tietojen suojaamista. Tietosuojan tarkoituksena on ihmisten yksityisyyden suojaaminen ja ylläpito. Tässä opinnäytetyössä tietosuojaa jää toissijaiseksi tietoturvallisuuteen nähden, mutta tietosuojaa käsitellään osittain pääsynvalvontalokeihin liittyvässä kappaleessa. (Andreasson & Koivisto 2013, 27.)

5 Pääsynvalvonta

Pääsynvalvonnalla (Access Control) toteutetaan luottamuksellisuuden säilymistä tietoturvallisuudessa. Ideaalitilanteessa pääsynvalvonnan toteuttaminen aloitetaan pääsynvalvontapolitiikan määrittelystä. Pääsynvalvontapolitiikan pitäisi sisältää esimerkiksi eri turvatasoilla hyväksytyt tekniset tunnistusmenetelmät, tunnusten lukitus- ja avausperiaatteet sekä salasanan tai muiden tunnisteiden laatuvaatimukset. Kun riittävät määrittelyt on tehty pääsynvalvontapolitiikkaan, voidaan ottaa käyttöön tekniset turvamekanismit, joilla toteutetaan politiikan linjauksia. Mikäli pääsynvalvontapolitiikkaa ei ole määriteltä, voidaan pääsynvalvontaa toteuttaa teknisillä menettelyillä, joiden tarkoituksena on säilyttää suojattavan tiedon luottamuksellisuus estämällä oikeudettomien tahojen pääsy suojattaviin resursseihin. (Karvi 2010, 13; Valtiovarainministeriö 2010)

5.1 Pääsynvalvonnan suhde käyttövaltuushallintaan

Pääsynvalvonnan tietoturvallisuustasovaatimukset (liite 1) ovat osa 2/2010 VAHTI-ohjetta. Kyseisessä ohjeessa on myös käyty laaja-alaisesti läpi myös muita teknisen tietoturvan osa-alueita kuten käyttäjien ja käyttövaltuuksien hallinta (liite 2). Vertailtaessa pääsynvalvonnan ja käyttövaltuuksien hallinnan tietoturvallisuustasovaatimuksia voi huomata, että monet käyttövaltuuksiin liittyvät vaatimukset vaikuttavat suoraan pääsynvalvontaan. Esimerkkinä voidaan pitää käyttövaltuuksien hallinnan perustason vaatimusta 3: "Käyttövaltuudet perustuvat palvelussuhteeseen tai muuhun kirjalliseen sopimukseen ja järjestelmien käyttö estetään

teknisesti ilman tarpeetonta viivytystä perusteen päätyttyä.”, jossa hallinnollisesti toteutetaan pääsynvalvontaa estämällä järjestelmän käyttö viivytyksettä käyttöperusteen päätyttyä. Voidaan siis todeta, että käyttövaltuuksien hallinnalla toteutetaan osaksi myös pääsynvalvontaa ja sen vuoksi niiden välillä ei ole tarkkaa rajaa; ne ovat käsitteinä limittäin. Edellä mainittu asia voidaan myös ajatella toisin päin, että teknisellä pääsynvalvonnalla toteutetaan käyttövaltuuksien hallintaa esimerkiksi niin, että tietyllä käyttövaltuudella voidaan evätä pääsy tietoon ja toisella käyttövaltuudella sallia. Tästä huolimatta tietoturvasuostasoissa on jaoteltu erikseen pääsynvalvonta ja käyttövaltuuksien hallinta, jonka vuoksi tässä opinnäytetyössä käytetään samaa jaottelua. (Valtiovarainministeriö 2010)

5.2 Pääsynvalvontatyypit

Pääsynvalvontatyypit voidaan jakaa seuraaviin tyypeihin:

Yksilöpohjaisessa pääsynvalvonnassa (Discretionary Access Control) objektin omistaja määrittää objektin käyttöoikeudet. On tärkeää huomioida, että yksilöpohjainen pääsynvalvonta perustuu subjektin identiteettiin, jolle objektin omistaja asettaa pääsyrajoitukset. Yksilöpohjaista pääsynvalvontaa käytetään yleisesti tietokoneiden käyttöjärjestelmissä. (Karvi, T. 2010)

Sääntöpohjaisessa pääsynvalvonnassa (Rule Based Access Control) objektit on luokiteltu hierarkkisille tasoille niiden turvavaatimusten mukaisesti. Esimerkkinä voivat olla valtionhallinnon turvallisuusluokitusmerkinnät: Käyttö rajoitettu, Luottamuksellinen, Salainen ja Erittäin salainen. Subjekteille on määritelty turvatasot. Mikäli subjekti - objekti pari täyttää molemmille määritellyt ehdot, subjektille sallitaan pääsy objektiin. (Karvi, T. 2010)

Luontipohjaisessa pääsynvalvonnassa (Originator Controlled Access Control) tärkein rooli on objektin luojalla. Luoja voi päättää kenellä on pääsy ja keneltä evätään pääsy objektiin, joka voi esimerkiksi olla tiedosto tai kansio. Objektin omistaja ei pysty muuttamaan luojaan määrittelemää pääsyä objektiin. (Karvi, T. 2010)

Viimeisenä pääsynvalvontamallina on roolipohjainen pääsynvalvonta (Role Based Access Control), joka perustuu käyttäjän funktionaaliseen rooliin organisaatiossa. Roolipohjaisessa pääsynvalvonnassa ei puututa yksittäiseen subjektiin vaan siihen liitettyyn rooliin, jonka eri subjektit voivat ottaa tai saada organisaation sääntöjen mukaisesti. Roolin kohdalla voidaan noudattaa yksilöpohjaista, sääntöpohjaista tai luontipohjaista pääsynvalvontaa. Tarkoituksena on, että henkilön tehtäväkuva määrää hänen roolinsa pääsynvalvonnassa. Esimerkiksi henkilöstöpäälliköllä täytyy olla pääsy organisaation työntekijöiden tietoihin, mutta viestintäpäälliköllä ei tarvitse. Roolien määrä voi vaihdella muutamasta roolista aina tuhansiin riippuen

muu muassa organisaation henkilöstömäärästä ja työntekijöiden tehtäväkuvista. (Thomas 2004, 87; Karvi, T. 2012).

6 Tunnistautuminen ja todentaminen

Käsitteet tunnistautuminen ja todentaminen ovat pääsynvalvonnan perusydintä. Tiedon luotamuksellisuuden säilyttämiseksi on tärkeää kysyä miten tunnistamme ja todennamme käyttäjän riittävän luotettavasti? Ennen tunnistamista ja todentamista käyttäjälle pitää luoda käyttäjäidentiteetti, johon tunnistaminen kohdistetaan.

6.1 Käyttäjäidentiteetti

Käyttäjäidentiteetti on tärkeä osa käyttäjän tunnistamista verkkopalvelussa tai tietojärjestelmässä. Käyttäjäidentiteetillä kuvataan järjestelmässä olevia käyttäjän henkilöllisyyttä kuvaavia tietoja. Tietojen avulla käyttäjä voidaan yksilöidä muista käyttäjistä. Yleensä käyttäjäidentiteetti luodaan silloin kun käyttäjä rekisteröityy järjestelmän käyttäjäksi. Käyttäjältä kerätään häneen liittyviä tietoja rekisteröintiprosessissa, jonka luotettavuus riippuu tarkistettavien tietojen määrästä. Mikäli käyttäjän antamia tietoja ei tarkasteta ollenkaan, käyttäjäidentiteetin luotettavuus on hyvin alhainen, jopa olematon. Mikäli rekisteröinnin yhteydessä käyttäjän henkilöllisyys selvitetään esimerkiksi kasvotusten, käyttäjäidentiteetin luotettavuus on korkea. Internetissä toimivat palvelut voivat fyysisesti sijaita toisella puolella maapalloa, joten luotettavasti kasvotusten henkilöllisyyden selvittäminen on käytännön syistä erittäin haastavaa, ellei lähes mahdotonta. Tämän vuoksi on olemassa myös verkon välityksellä toteutettuja tunnistautumismenetelmiä, kuten varmenteet tai TUPAS. (Valtiovarainministeriö 2006, 18 - 19)

Läheskään aina palvelussa tai järjestelmässä ei ole tarkoituksenmukaista varmistua käyttäjäidentiteetistä. Sen vuoksi käyttäjäidentiteetin luotettavuudelle on määritelty nelitasoinen luokitus.

1. Anonyymikäyttäjät. Käyttäjiä ei rekisteröidä ollenkaan eivätkä he ole eroteltavissa käyttäjäidentiteetin mukaan toisistaan. Täyttä anonyymiteettia on silti haastava saada koska verkkopalveluissa voidaan tunnistaa anonyymikäyttäjän päätelaite IP-osoitteen perusteella ja laite voidaan mahdollisesti yhdistää käyttäjään.
2. Yksilöitävissä olevat käyttäjät. Jokaisella käyttäjällä on rekisteröity käyttäjäidentiteetti. Käyttäjät ovat yksilöitävissä palvelussa, mutta heidän käyttäjätietoja ei ole varmistettu.
3. Kevyesti todennetut käyttäjät. Käyttäjien käyttäjäidentiteeteistä on rekisteröinnin yhteydessä varmistettu niin, että ainakin osa käyttäjään liittyvistä tiedoista pitävän paikkansa.

4. Vahvasti todennetut käyttäjät. Käyttäjien henkilöllisyys on selvitytetty luotettavasti virallisella henkilöllisyystodistuksella.
(Valtiovarainministeriö 2006, 19)

Tunnistautuminen (Identification) on prosessi, jossa käyttäjä tunnistetaan. Tunnistamisen tarkoituksena on yksilöidä tietty käyttäjä muista käyttäjistä. Perinteisesti käyttäjä tunnistetaan käyttäjätunnuksella, joka on käyttäjän yksilöllinen merkkijono. Käyttäjätunnus ei ole ainoa tapa tunnistaa käyttäjä; tunnistaminen voidaan myös tehdä esimerkiksi henkilötunnuksella tai pankin tilinumerolla. Väärinkäytösten estämiseksi käyttäjä kannattaa tunnistamisen lisäksi myös todentaa. (Ruotsalainen 2002, 19)

Todentaminen (Authentication) on prosessi, jossa varmistetaan, että käyttäjä on se joka hän väittää olevansa. Todentamisen tarkoituksena on saada käyttäjän digitaalinen identiteetti selville. Todentaminen on kriittistä palvelun tai tietojärjestelmän pääsynvalvonnassa, koska on erittäin haitallista, että kirjautuva henkilö ei ole se henkilö, joka hän väittää olevansa. Todentaminen voidaan tehdä esimerkiksi yhteisen salaisuuden tai kolmannen osapuolen avulla. (Thomas 2004, 115 - 116)

Identiteetistä voidaan varmistua neljällä eri tavalla:

1. Jotain mitä tiedät (esim. salasana, PIN-koodi)
2. Jotain mitä omistat tai mitä sinulla on (esim. passi)
3. Jotain mitä olet (esim. verkkokalvo, sormenjälki)
4. Jotain mitä osaat tehdä (esim. allekirjoitus)

(Hämäläinen, T.)

Usein kohta 4 liitetään osaksi kohtaa 3, koska riippuen tulkinnasta allekirjoitus voidaan laskea myös biometriseksi tunnisteeksi yhdessä verkkokalvon ja sormenjäljen kanssa.

Heikkoon todentamiseen tarvitaan vähintään yksi todentamistapa yllä mainituista. Esimerkkejä heikosta tunnistamisesta ovat:

- käyttäjätunnus + salasana
- puhelinsoitto
- biotunnistus

(Valtiovarainministeriö 2006, 20)

Puhuttaessa vahvasta todentamisesta tarvitaan vähintään kaksi edellä mainittua todentamistapaa. Käytännön esimerkkejä vahvasta todentamisesta ovat:

- TUPAS-tunnistus
- pankkikortti + tunnusluku

- käyttäjätunnus + salasana + puhelinsoitto haltijan matkapuhelimeen
 - varmenteellinen sirukortti + PIN-koodi
 - varmenteellinen sirukortti + biotunnistus
 - laatuvarmenteellinen sirukortti + PIN-koodi
 - laatuvarmenteellinen sirukortti + biotunnistus
- (Valtiovarainministeriö 2006, 20)

6.2 Salasana

Käyttäjätunnuksen ja salasanan yhdistelmä on yleisin tunnistamis- ja todentamismenetelmä. Käyttäjätunnuksen ja salasanan -yhdistelmässä identiteetistä varmistutaan salasanan avulla, joka on käyttäjän ja järjestelmän yhteinen salaisuus. Ideaalitulanteessa vain ja ainoastaan kirjautuja sekä järjestelmä tietävät salasanan ja sen lisäksi järjestelmässä oleva salasana on tallennettuna salakirjoitetussa muodossa. Käyttäjätunnusta ja salasanaa käytetään yleisesti esim. käyttöjärjestelmään tai sähköpostitilille kirjautuessa. (Järvinen 2003, 35)

Kaikki salasanat eivät ole suojaamistarkoituksessa yhtä hyviä. Yleisesti ollaan hyvin tietoisia siitä, että esimerkiksi merkkijonoltaan pidempi salasana on parempi kuin lyhyemmän merkkijonon salasana. Salasanaalle on olemassa laatuvaatimuksia, joita noudattamalla salasana murtaminen on haastavampaa tai ainakin enemmän aikaa vievää. Vaikka salasanan tietäisi vain ja ainoastaan sen omistaja, se ei nykyaikana välttämättä takaa yhtään mitään. Salasanan ja muidenkin immateriaalitietojen heikkoutena on, että sitä voi monistaa ja jakaa loputtomasti. Lisäksi salasanassa on aina unohdusvaara, varsinkin kun ihmiset ovat nykyään rekisteröityneet useisiin salasanalla suojattuihin palveluihin, joka tekee muistamisesta vielä haastavampaa. (Järvinen 2003, 35)

VAHTI-ohjeet määrittelevät laatuvaatimuksia myös salasanoille. Laatuvaatimukset ovat teknisiä vaatimuksia esimerkiksi salasanan pituudelle, siinä käytettävien erikoismerkkien määrälle ja kuinka usein salasana pitää vaihtaa. Vaatimukset ovat määritelty erikseen tietoturvallisuuden perustasolle ja korotetulle tasolle. Tietoturvallisuuden perustasolta löytyy vain yksi suora vaatimus salasanoille: "Huonolaatuisten salasanojen käyttö estetään". Vaatimus jättää paljon tulkinnanvaraa lukijalle ja sen vuoksi on vaatimuksena haastava. Tämän tyyppisen vaatimuksen täyttämiseen kannattaa ottaa selvää salasanojen muodostuksen hyvistä käytänteistä (Best Practice), joita löytyy esimerkiksi VAHTI 3/2010 Sisäverkko-ohjeesta. (Valtiovarainministeriö 2010)

Korotetun tason laatuvaatimukset ovat konkreettisempia ja sen vuoksi helpompi toteuttaa ilman lisäselvitystä. Korotetun tason laatuvaatimukset salasanoille ovat:

- Salasanan pituus on vähintään 10 merkkiä.

- Salasana on vaihdettava 90 päivän välein.
- Järjestelmä muistaa 10 viimeisintä salasanaa ja estää niiden käytön uudelleen.
- Salasanan on sisällettävä kolmea seuraavista neljästä merkkiryhmästä: isot kirjaimet, pienet kirjaimet, numerot ja erikoismerkit. (Valtiovarainministeriö 2013)

Yllä mainittujen vaatimusten lisäksi sekä tietoturvallisuuden perustasolle että korotetulle tasolle on olemassa vaatimus, että ”epäonnistuneet kirjautumisyritykset sekä muut valtuuksien puutteeseen kariutuvat toimenpideyritykset kirjataan”. Korotetulla tasolla vaatimusta täsmennetään vielä lisäksi, että ”tunnus lukittuu, mikäli järjestelmään yritetään epäonnistuneesti liian monta kertaa”. Kyseiset vaatimukset eivät ole suoraan salasanojen laatuvaatimuksia, mutta ne ovat läheisessä yhteydessä salasanojen käyttöön. (Valtiovarainministeriö 2013)

6.3 Biometrinen tunnistus

Tietoturva-asetus määrittelee seuraavasti biometrisen tunnistuksen: ”Biometrisillä tunnistetiedoilla (tarkoitetaan) henkilön tunnistamisessa käytettäviä, henkilön yksilöiviä tietoja, jotka perustuvat luonnollisen henkilön fysiologiseen ominaisuuteen taikka käyttäytymiseen.” (Asetus tietoturvallisuudesta valtionhallinnossa)

Biometrinen tunnistus eli biotunnistus on henkilön tunnistamista käyttäen hyväksi ihmisen kehon yksilöllisiä piirteitä. Biometrinen tunnistaminen onnistuu esimerkiksi sormenjäljistä, kasvoista, äänestä, silmän verkkokalvosta sekä kämmenen muodosta. Täysin varma ratkaisu biometrisen tunnistamisen ei ole, koska on olemassa ihmisiä joilla on samanlaiset biometriset tunnistetiedot, mutta se on äärimmäisen harvinaista. Biometrinen tunnistus yhdistettynä johonkin muuhun tunnistamiseen kuten varmennekorttiin luokitellaan vahvaksi tunnistautumiseksi. (Tietosuojavaltuutetun toimisto 2010)

Biometrisen tunnistamisen etuihin kuuluu muun muassa, ettei biometrisiä tunnistetietoja voi unohtaa kotiin ja biometristen tunnistuslaitteiden huijaaminen on vaikeaa. Biometrisen tunnistautuminen on käyttäjäystävällisempää ja vaivattomampaa kuin monet muut tunnistautumismenetelmät, koska tunnistautuminen voidaan esimerkiksi tehdä katsomalla kameraan tai puhumalla mikrofooniin. (Tietosuojavaltuutetun toimisto 2010)

Biometrisellä tunnistamisella on myös huonot puolensa. Biometrisiä tunnistetietoja voi kerätä sekä käyttää ilman, että kohde tietää koko asiasta mitään ja tällä tavoin esiintyä hänen käyttäjäidentiteetillään. Edellä mainitun vuoksi biometristä tunnistamista ei pitäisi käyttää yksinään suurta turvallisuutta vaativissa asioissa. Biometrisistä tunnistetiedoista voidaan saada selville ihmisestä myös sellaisia henkilökohtaisia tietoja, jotka eivät kuulu tunnistautumiseen mitenkään.

kään. Esimerkkinä DNA:sta voidaan tehdä päätelmiä ihmisen terveydestä ja perimästä. Tämän vuoksi DNA ei ole suositeltava biometrinen tunnistus. (Tietosuojavaltuutetun toimisto 2010)

6.4 Varmenteet

Internetin laajuuden ja sen käyttötapojen vuoksi perinteiset kasvokkain tapahtuvat tunnistusmenetelmät eivät ole käytännössä mahdollisia. Tunnistamisongelman yhdeksi vakiintuneeksi ratkaisuksi on kehitetty varmenteet (Certificate). Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617 määrittelee varmenteen seuraavasti: ”varmenteella (tarkoitetaan) sähköistä todistusta, joka todentaa henkilöllisyyden tai todentaa henkilöllisyyden ja liittää allekirjoituksen todentamistiedot allekirjoittajaan ja jota voidaan käyttää vahvassa sähköisessä tunnistamisessa sekä sähköisessä allekirjoituksessa”. Edellä mainitusta voidaan todeta, että varmenteella on myös muitakin käyttötarkoituksia kuin todentaminen.

Varmenteella todentaminen perustuu epäsymmetriseen salaukseen. Esimerkiksi Väestörekisterikeskus käyttää varmenteissaan julkisen avaimen menetelmää (Public Key Infrastructure, PKI). PKI-järjestelmäksi kutsutaan varmenteiden myöntämiseen, jakeluun, hallintaan ja ylläpitoon kuuluvaa kokonaisuutta. PKI:ssa todentaminen tapahtuu kolmannen osapuolen, ns. varmentajan (Certificate Authority, CA) avulla, joka vahvistaa palveluun tai tietojärjestelmään kirjautuvan käyttäjän henkilöllisyyden. (Järvinen 2003, 165)

Varmenteita on useisiin erilaisiin käyttötarkoituksiin esimerkiksi kansalais-, organisaatio-, palvelin-, mobiili-, ja sähköpostivarmenne.

6.4.1 Varmennekortti

Varmennekortti on muovinen luottokortin kokoinen mikropiirillä eli sirulla varustettu kortti. Vaikka siru on hyvin vaatimattoman kokoinen, se sisältää prosessorin, monenlaista muistia sekä väylän tietoliikennettä varten. Siru voi pitää sisällä esimerkiksi kansalaisvarmenteen tai organisaatiovarmenteen sekä varmenteet allekirjoittamiseen ja salaamiseen. Varmennekortti työnnetään tunnistautuessa kortinlukijaan ja sen jälkeen käyttäjä näppäilee henkilökohtaisen PIN-koodin järjestelmään. (Järvinen 2003, 173-174)

Kansalaisvarmenne on suomalaisille tai vakinaisesti Suomessa asuville tarkoitettu sähköisen asioinnin tunnistautumisväline. Kansalaisvarmenne on poliisin myöntämän henkilökortin sirulla ja sen toimittamisesta vastaa Väestörekisterikeskus. Siru pitää sisällään muun muassa omistajan nimitiedot sekä sähköisen asiointitunnuksen. (Väestörekisterikeskus 2013)

Organisaatiovarmenne on yritysten, yhteisöjen tai muiden organisaatioiden käyttöön tarkoitetun organisaatiokortin sirulla oleva varmenne. Organisaatiovarmenteen käyttöön otolla pystytään parantamaan tunnistautumista palveluihin ja järjestelmiin, mikä on etenkin valtionhallinnon organisaatioilla erittäin tärkeätä tietoturvasovaatimusten vuoksi. (Väestörekisterikeskus 2013)

6.4.2 Mobiiliasiointivarmenne

Mobiiliasiointivarmenne (Mobiilivarmenne) on suomalaisten teleoperaattoreiden luoma tunnistautumismenetelmä. Mobiilivarmenne on sim-korttiin liitetty varmenne sim-kortin omistajan identiteetistä. Mobiilivarmenteella tunnistautuessa käyttäjä antaa palveluun käyttäjätunnuksensa tai matkapuhelinnumeron. Palvelusta lähetetään matkapuhelimeen tieto kirjautumisyhteyksestä. Tämän jälkeen käyttäjä näppäilee salaisen 4-8 numeron tunnuslukunsa, jonka jälkeen matkapuhelin lähettää tiedon onnistuneesta tunnistamisesta verkkosivuille ja palvelu aukeaa käyttöön. (Suomalaiset teleoperaattorit)

Mobiilivarmeneminen on määritelty vahvaksi tunnistautumiseksi. Mobiilivarmenne eroaa TUPAS-tunnistautumisesta siinä, ettei käyttäjällä ole vaihtuvaa tunnuslukua vaan pysyvä salainen tunnusluku. Myös mobiilivarmennetta voidaan käyttää sähköisen tunnistamisen lisäksi viestinnän salaamiseen ja sähköiseen allekirjoitukseen. (Suomalaiset teleoperaattorit 2011, 7)

6.5 TUPAS

Pankit olivat jo 1980-luvulla sähköisen asioinnin edelläkävijöitä. Tuolloin pankit alkoivat jakaa DOS-ohjelmaa, jolla pystyi maksamaan laskuja pankkiin. Internetin myötä pankkien verkkopalveluiden käyttö kasvoi räjähdysmäisesti ja yksi syy siihen on ollut hyvin toiminut TUPAS (TunnistusPalvelu ASiointipalveluntuottajille). TUPAS-tunnistuspalvelu on Suomessa toimivien pankkien yhteisesti määrittelemä tapa tunnistaa käyttäjä verkkopalvelussa. TUPAS-määritystä hallinnoi, kehittää ja ylläpitää Finanssialan Keskusliitto. TUPAS-palvelu käyttää hyväkseen vahvaa tunnistautumista. (Finanssialan Keskusliitto, 2011; Järvinen 2003, 191)

TUPAS-tunnistautumisen tarkoitus on tunnistaa käyttäjä pankkien verkkopankkitunnuksilla sekä salasanalistoilla. Kun käyttäjä kirjautuu palveluun verkkopankkitunnuksilla, hänet ohjataan palveluntarjoajan sivuilta pankin sivuille tunnistautumisen ajaksi. Käyttäjä syöttää pankin sivuilla henkilökohtaisen käyttäjätunnuksensa ja salasanan, jonka jälkeen palveluun syötetään vielä joka kerta vaihtuva tunnusluku. Mikäli edellä mainittu prosessi suoritetaan virheittä, pankki lähettää palveluntarjoajalle tiedot kirjautujan identiteetistä ja käyttäjä voi

jatkaa palvelun käyttöä tunnistettuna käyttäjänä. TUPAS on hyväksytty vahvaksi todentamismenetelmäksi. (Finanssialan Keskusliitto, 2011.)

7 Lokitiedostot

Lokitiedostojen (Logfile) tarkoituksena on dokumentoida tapahtumia ja niiden aiheuttajia tietyssä ajankohtana. Lokitiedostoja käytetään seurantaan ja valvontaan niin normaali- kuin poikkeusolosuhteissa. Normaaliolosuhteissa lokien käyttötarkoitus on tietojärjestelmien ja tietoverkkojen toiminnan seuraaminen sekä käytön tilastointi. Poikkeusolosuhteissa lokitiedostojen rooli korostuu ja niitä tarvitaan tilanteen normalisointiin ja tapahtuman syiden sekä niiden laajuuden selvittämiseen. Pelkistetty lokitiedosto on tekstitiedosto, jossa on mainittu ajankohta sekä tapahtumat kyseisenä ajankohtana. Lähes jokainen tietojärjestelmä kerää lokitietoja omaan tietokantaansa. (Lokiohje, VAHTI 3/2009, 13 - 14)

Lokitiedostot voivat pitää sisällään hyvin arkaluonteista tietoa liittyen esimerkiksi tunnistetietoihin tai henkilötietoihin ja sen vuoksi lainsäädäntö asettaa useita erilaisia vaatimuksia lokien käsittelylle. Mikäli lokitiedostoon kerääntyy henkilöitä koskevaa tunnistettavaa tietoa, sitä pitää käsitellä henkilörekisterinä ja lainsäädäntö asettaa sille tietyjä suojausvaatimuksia. On tärkeää, että lokitietoja käsitellään asianmukaisella tavalla koko niiden elinkaaren aikana. Lokien elinkaareen voivat kuulua esimerkiksi seuraavat vaiheet: kerääminen, analysointi, säilyttäminen, luovuttaminen ja tuhoaminen tai arkistointi. Jokaisen vaiheen tulee olla suunnitelmallista, huolellista sekä tarkoitussidonnaista. (Kajantie 2009)

Lokitiedostoja voidaan käyttää myös tekniseen valvontaan organisaatioissa ja tällöin asia pitää käsitellä yhteistoimintamenettelyssä työelämän tietosuojalain mukaisesti. (Lokiohje, VAHTI 3/2009, 20 - 21)

Tärkeimpiä lokien käsittelyyn liittyviä lakeja Suomessa ovat:

- Henkilötietolaki (523/1999)
- Julkisuuslaki (621/1999)
- Laki yksityisyyden suojasta työelämässä (759/2004)
- Sähköisen viestinnän tietosuojalaki (526/2004)

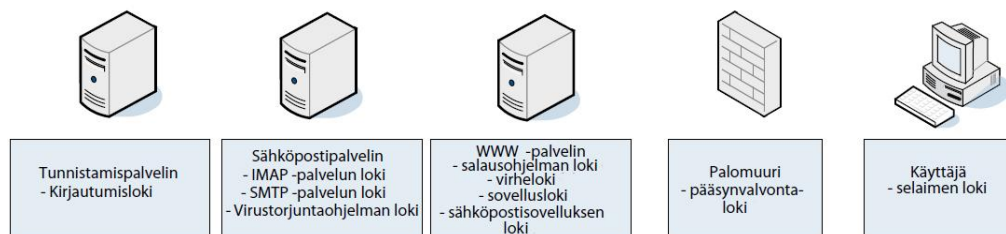
VAHTI jakaa lokitiedostot neljään kategoriaan: ylläpitolokit, käyttölokit, muutokset ja virhe-lokit. Lokien yksiselitteinen luokittelu eri kategorioihin tietosisältöjen mukaan on hankalaa, koska eri lokit voivat kuulua sisällöltään useampaan kategoriaan.

7.1 Lokitiedostot pääsynvalvonnassa

Pääsynvalvontalokit voidaan luokitella käyttölokeiksi, koska ne ilmaisevat onnistuneet ja epäonnistuneet yritykset käyttää järjestelmän suojattuja resursseja. Pääsynvalvontalokit voidaan osittain luokitella myös virhelokeiksi, koska ne paljastavat virheelliset kirjautumisyritykset järjestelmään. Pääsynvalvontalokien tärkein tehtävä on valvoa järjestelmien käyttöä sekä niiden turvallisuutta. (Lokiohje, VAHTI 3/2009, 29)

Lokien tärkeydestä osana pääsynvalvontaa kertoo se, että niistä on vaatimus jokaisella tietoturvasuustasolla: perustasolla, korotetulla tasolla ja korkealla tasolla (liite 1). Pääsynvalvonnan näkökulmasta tietyt lokitiedostot ovat tärkeämpiä kuin toiset. Esimerkiksi palomuurin lokitiedostot ovat pääsynvalvontaa tutkiessa mielenkiintoisempia kuin työasemassa olevan Internet-selaimen loki. Lokitiedostoihin liittyviä vaatimuksia löytyy tietoturvasovatuksista muualtakin kuin pääsynvalvonnan alta, mutta tässä luvussa keskitytään lähinnä pääsynvalvonnan vaatimuksiin. (Valtiovarainministeriö 2010)

Lokitietoja keraantyy erittäin suuria määriä, koska niihin kirjataan pienimmätkin tapahtumat mitä tietojärjestelmissä tapahtuu ja sen vuoksi niiden hallinta voi olla hyvin haastavaa. Hahmottamisen helpottamiseksi kuvassa 2 esitetään lokien muodostuminen yksinkertaisessa toimenpiteessä kuten sähköpostipalvelun käyttämisessä Internet-selaimella. Monesti tilanne on monimutkaisempi ja lisäksi voi syntyä lokitiedostoja DNS -palvelimella sekä muita lokitietoja liittyen sähköpostipalveluun. (Lokiohje, VAHTI 3/2009, 68)



Kuva 1: Lokien synty www-pohjaisessa sähköpostipalvelussa (Lokiohje, VAHTI 3/2009, 68)

7.2 Sovellustason pääsynvalvontalokit

Organisaation sisällä sovellustason pääsynvalvontalokien tarkoituksena on kertoa mistä IP-osoitteesta on muodostettu yhteys suojattavaan järjestelmään ja millä käyttäjäidentiteetillä kirjautuminen on tapahtunut. Tämän lisäksi sovellustasolla voidaan pitää kirjaa epäonnistuneista yhteysyrityksistä ja käyttövaltuuksien ylittämiseen liittyvistä väärinkäyttöyrityksistä. Mikäli tietoturvasovatuksena on tapahtunut, sen selvittämiseksi sovellustason pääsynvalvontalokit tarjoavat tiedon lähteosoitteesta ja käyttöoikeuksista, joita yhdistelemällä on mahdollista saada ehjä kirjausketju tapahtuneesta. Esimerkkejä tarpeellisista sovellustason pääsyn-

valvontalokeista organisaation sisällä ovat taloushallinnon, tilausjärjestelmien ja toiminnanohjausjärjestelmien lokit. (Lokiohje, VAHTI 3/2009, 32 - 33)

Mikäli puhutaan julkisesta palvelusta, eikä organisaation sisäisestä toiminnasta, sovellustason pääsynvalvontalokeilla on hieman erilainen tehtävä. Sisäisillä sovelluksilla on lähtökohtaisesti tiedossa oleva käyttäjäjoukko eli organisaation työntekijät. Edellä mainittua lähtökohtaa ei välttämättä ole julkisessa palvelussa ja siksi lokista ilmenee myös mahdollinen kirjautumiseen liittyvä käyttäjätunnus sekä tunnistautumisen onnistuminen tai epäonnistuminen, jos palvelu vaatii tunnistautumisen. Tämän lisäksi pääsynvalvontalokista ilmenee verkko-osoite, josta on otettu yhteys palveluun. (Lokiohje, VAHTI 3/2009, 33)

7.3 Verkkotason pääsynvalvontalokit

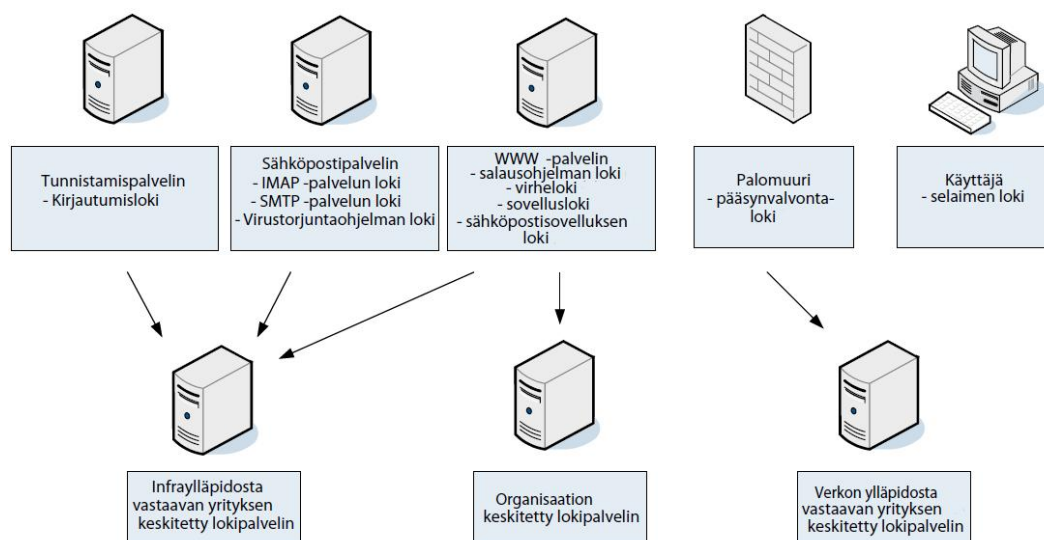
Verkkotason pääsynvalvontalokit kertovat tyypillisesti mistä verkko-osoitteesta on mennyt liikennettä mihin verkko-osoitteeseen. Lokia keräävät verkon aktiivilaitteet kuten palomuurit ja reitittimet. Verkkotason pääsynvalvontalokien tarkoituksena on vikatilanteiden selvittäminen, mutta niistä saa myös tietoa tietoturvasovellusten selvittämiseen. Yleensä verkon aktiivilaitteiden lokitiedot ovat tunkeutujan ulottumattomissa, ellei tunkeutuja murtaudu verkon lisäksi myös itse aktiivilaitteeseen. Palomuri- ja reitinlokeista saa selville hyökkäyksen kulkureitin sisäverkon puolelle, mutta lokit eivät kerro mitä murretulle palvelimelle on tapahtunut tai, että siihen on yleensäkin murtauduttu. Yleensä palomuurien lokiasetukset kirjaavat hyvin epäonnistuneet yhteydenottoyritykset, mutta jättävät pienemmälle huomiolle onnistuneet yhteydet. Mikäli palvelin tai verkko, jota suojataan palomuurilla, sisältää salassa pidettävää materiaali, kannattaa kirjata myös onnistuneet yhteydet palvelimelle. (Lokiohje, VAHTI 3/2009, 36)

7.4 Tietoturvaluustasovaatimukset ja lokien kerääminen

Lokien kerääminen on tietoturvallisuuden kannalta tavanomaisia pääsynvalvontatapoja. Edellisen väittämän puolesta puhuu se, että jo perustason tietoturvaluustasovaatimukset vaativat lokien keräämistä. Perustason täyttämiseksi lokien keräämisessä on hyvä ottaa huomioon, että esimerkiksi palomuurit keräävät epäonnistuneiden yhteydenottoyritysten kirjaamisen lisäksi myös onnistuneet yhdenotot. Tämän saavuttamiseksi kannattaa katselmoida ja tarvittaessa muuttaa verkon aktiivilaitteiden lokiasetukset. Kannattaa myös tarkastaa, että verkon käyttäjät ovat tunnistettuja eikä anonymikäyttäjiä sallita verkossa. Tämän vuoksi aktiivilaitteiden sekä järjestelmien on kirjattava käyttäjän tiedot myös pääsynvalvontalokeihin.

Korotetulla tasolla on erityisvaatimus kerättyjen pääsynvalvontalokien säilyttämisen suhteen. Mikäli lokitietoja keräävään järjestelmään on murtauduttu, myös sen keräämät lokitiedot

ovat vaarassa korruptoitua tai tuhoutua murtautujan toimesta. Tämän vuoksi olisi organisaatiolla hyvä olla olemassa keskitetty lokipalvelin tai kokonaan keskitetty lokienhallinta. Lokipalvelimen tulee olla hyvin suojattu hyökkäyksiä vastaan ja se ei saa näkyä sisäverkon ulkopuolelle. Keskitettyyn lokipalvelimeen lähetetään muilta lokeja keraäviltä palvelimilta talteen. Riskiä lokitietojen eheyden menettämistä vastaan voidaan varautua useammalla keskitetyllä lokipalvelimella kuten kuvassa 2. Mikäli erillisille lokipalvelimille ei ole mahdollista käyttää, olisi hyvä siirtää lokitiedot säännöllisin väliajoin talteen niitä tuottavasta järjestelmästä. (Viestintävirasto 2011)



Kuva 2: Lokien kerääminen www-pohjaisessa sähköpostipalvelussa (Lokiohje, VAHTI 3/2009, 68)

Suoraa vaatimusta korotetulla tasolla ei ole keskitetyille lokienhallinnalle, mutta se voi olla mahdollisesti edullisempi ratkaisu kuin lokien suojaaminen ja tallentaminen paikallisesti. Mikäli lokitiedostot tallennetaan paikallisesti, tulee muistaa, että kyseisen järjestelmän pääkäyttäjällä on mahdollisuus manipuloida niitä. Tällaisessa tapauksessa korotetun tietoturvatason vaatimus ei välttämättä täyty. Keskitetyssä lokienhallintajärjestelmässä lokien säilyttäminen on turvallista ja silloin ei olla tilanteessa, jossa valvottavat valvovat itseään.

Korkealla tietoturvaluustasolla on myös vaatimus lokitiedostoja kohtaan: "Korkean tason järjestelmissä pääsynvalvontalokeja ja kirjausketjuja tuotetaan myös järjestelmän sisällä toimimisesta toiminnan vaatimusten mukaisesti." Myös tietoturvapoikkeamien valvonnan korkean tietoturvaluustason vaatimuksissa on maininta lokien seurannasta: "Lokien seurannan perusteella muodostetaan tilannekuvaa ja havaitaan tietoturvapoikkeamia sekä kehitetään toimintaa." Edellä mainitut vaatimukset asettavat lähes suoraan vaatimuksen SIEM-järjestelmälle (Security Information and Event Management). SIEM-järjestelmäinen kirjo on suuri ja ne kehittyvät alati, joten ominaisuuksien kuvaaminen on haastavaa. Yleisesti voi-

daan sanoa, että SIEM tuottaa tilannekuvaa ja hälytyksiä lokitietojen, IDS-havaintojen ja haavoittuvuuslistauksien perusteella. SIEM-järjestelmällä voidaan erotella eri verkkosegmenttien liikenteet ja se antaa hyvät työkalut vikojen etsimiseen niin palomuurista, kytkimestä tai muusta lokeja tuottavasta järjestelmästä. SIEM-järjestelmät ja muut reaaliaikaista tilannekuvaa antavat järjestelmät ovat tällä hetkellä paras ratkaisu lokien käsittelyyn ja luultavasti hinnatkin sen mukaiset. Mikäli korkein tietoturvataso on saavutettava, SIEM-järjestelmä on hyvä, ellei lähes pakollinen valinta lokien käsittelyyn. (Valtiovarainministeriö 2010; Cygate 2013)

8 Yhteenveto ja arviointi

Opinnäytetyön viimeisessä luvussa käsitellään ja arvioidaan opinnäytetyöprosessin ja tavoitteiden onnistumista. Myös prosessin aikana esille tulleet vastoinkäymiset ja ongelmat otetaan esille tässä luvussa.

8.1 Yhteenveto tietoturvaluustasovaatimusten toteuttamisesta

Opinnäytetyössä on käyty läpi pääsynvalvonnan tietoturvaluustasovaatimuksia ja muutamia esimerkkejä miten ne voidaan toteuttaa käytännössä. Yksityiskohtaisempia käytännön esimerkkien löytäminen esimerkiksi liike-elämästä on hyvin haastavaa, koska organisaatiot eivät ole valmiita paljastamaan tietoturvaluuteen liittyviä käytäntöjään. Edellä mainittu on hyvin ymmärrettävää, koska tiedot voisivat päätyä väärin käsiin ja aiheuttaa suurta vahinkoa tiedot julkistaneelle organisaatiolle. Tämän vuoksi esimerkkien kuvaaminen tarkemmalla tasolla on haastavaa. Vielä suurempi haaste on löytää resurssit esimerkkien toteuttamiseen koko valtionhallinnon mittakaavassa.

Tietoturvaluustasot aiheuttavat erittäin paljon tietoturvan kehittämistä valtionhallinnossa ja se vaatii sekä aikaa että rahaa. Tässä asiassa törmätäänkin yhteen valtionhallinnon ongelmista liittyen tietoturvaluuden kehittämiseen, joka on ristiriita kehittämistarpeiden ja rahoituksen välillä. Valtionhallinto on vähentänyt vuosina 2005 - 2010 yhteensä yli 5600 henkilötyövuotta valtion tuottavuusohjelman vuoksi (Yle, 2011). Tietoturvaluuden kehittämistarpeiden täyttäminen virkatyönä on hyvin haastavaa, mikäli valtio vähentää kehittämistä työskäviä virkamiehiä. Yksityiset palveluntarjoajat tekevät varmasti tietoturvaluustasojen vaatimia kehittämistoimenpiteitä niin hallinnollisesti kuin teknisesti viranomaisien laskuun, mutta se voi käydä hyvin kalliiksi valtiolle. Kehittämisen ulkoistaminen voi aiheuttaa myös muita ongelmia kuten tietojärjestelmien yhteensopivuusongelmia tai herättää kysymyksen: onko valtiovalan tietoturvaluuden ylläpitäminen liukumassa viranomaisilta liiaksi yksityiselle sektorille? Myös media luo painetta valtiohallinnon suuntaan julkaisemalla jatkuvalla syötöllä uutisia vakoiluskandaaleista ja verkkorikollisuudesta. Voidaan siis todeta, että opinnäytetyös-

sä kuvattujen tietoturvaluustasovaatimusten toteuttaminen on loppuen lopuksi vähäpätöinen haaste valtion tietoturvaluuden kehittämisen kannalta.

8.2 Opinnäytetyöprosessi

Opinnäytetyöprosessia voidaan kuvata erittäin kiireiseksi. Kuten johdannossa todettiin, ensimmäinen aihe opinnäytetyöksi kariutui laajaan määrään salassa pidettävää tietoa, jota opinnäytetyössä ei voi julkaista. Tämän vuoksi keksittiin vaihtoehtoinen aihe, josta voidaan tehdä opinnäytetyö yleisemmällä tasolla ja ilman salassa pidettävää tietoa. Aiheeksi valikoitui pääsynvalvonta, joka on erittäin mielenkiintoinen aihe, mutta syksy oli jo pitkällä ja aika vähissä. Suurin syy ajan puutteeseen oli työn ja opinnäytetyön kirjoittaminen yhdistäminen. Aluksi opinnäytetyön tiedonhankinta tehtiin vain viikonloppuisin, mutta loppuvaiheessa kirjoittamista tehtiin töiden ohessa seitsemänä päivänä viikossa. Tämän vuoksi jaksaminen nousi sitä suuremmaksi haasteeksi mitä lähemmäksi palautuspäivä tuli.

Tiedonhankinta tapahtui pääosin syksyn aikana, mutta perehtyneisyys VAHTI-ohjeita kohtaan oli alkanut jo päivätyön ohessa paljon aikaisemmin. Tämän vuoksi opinnäytetyöprosessia ei tarvinnut lähteä rakentamaan tyhjältä pöydältä, koska perehtyneisyyttä oli jo kertynyt aikaisemmin. Tiedonhankintaa hankaloitti suomenkielisten lähteiden vähyys tai niiden väärä näkökulma aihetta kohtaan. Englanninkielellä lähteitä löytyi liikaakin, mutta ne keskittyivät sellaisiin pääsynvalvonnan alakategorioihin, joita VAHTIn tietoturvaluustasovaatimuksissa ei oltu huomioitu pääsynvalvonnan osalta. Opinnäytetyössä jouduttiin olosuhteiden pakosta käyttämään paljon valtionhallinnon dokumentteja lähteinä, koska opinnäytetyön aihe oli sidoksissa valtionhallintoon hyvin vahvasti.

Opinnäytetyön kirjoittaminen sujui kokonaisuutena hyvin, vaikka tyhjän paperin kammo vaivasi alkuvaiheessa hyvinkin paljon. Kirjoittaminen ajoitettiin viikonloppuihin, loppuvaiheessa käytettiin hyödyksi myös arki-illat sekä muutaman kerran yöt. Haasteita kirjoitusprosessiin aiheutti lähes päivittäin näkökulman vaihtaminen työkirjoittamisesta opinnäytetyön kirjoittamiseen. Sekä päivätöissä että opinnäytetyössä pyörivät tutut käsitteet: tietoturva-asetus, tietoturvaluustasot ja VAHTI, mutta näkökulma ja tavoitteet poikkesivat paljon toisistaan. Opinnäytetyön kirjoitusprosessin lähtökohtana oli oppiminen ja sen esille tuominen, kun taas työpaikalla lähtökohtana oli kehittää työnantajan tietoturvaluutta. Onneksi edellä mainituissa oli myös paljon samankaltaisuutta ja osittain ne myös tasapainottivat toisiaan.

8.3 Tavoitteiden saavuttaminen

Opinnäytetyön tavoitteiden täytyminen onnistui kohtalaisen hyvin. Hyvin onnistuivat esimerkiksi lokitietojen tietoturvaluusvaatimusten täyttämiseen liittyvät käytännön esimerkit

sekä salasanoihin liittyvien laatuvaatimuksien esitteleminen. Edellä mainituissa asioissa päästiin käytännön ratkaisuihin asti, mikä oli yksi alussa asetetuista tavoitteista. Pieni osa tavoitteista jäi saavuttamatta eli tässä tapauksessa varmenteiden suhteen käytännön erimerkit eivät yltäneet niin konkreettiselle tasolle kuin lokien ja salasanojen kanssa. Laajemmalla perehtymisellä olisi voitu käydä läpi käytännön ratkaisut myös varmenteiden korkean tason tietoturvallisuusvaatimusten täyttämiseen. Opinnäytetyöprosessin aikana osa tavoitteista priorisoitui ja sen vuoksi tietyt aiheet nousivat tärkeämmiksi kuin toiset. Tämän vuoksi osa alkupe-
räisistä tavoitteista muuttui vähemmän merkityksellisiksi, kuten pääsynvalvonnan yksityiskoh-
tainen tekninen kuvaaminen ja sen vuoksi huomio kiinnittyi enemmän valtionhallinnon näkö-
kulmaan asiasta.

Opinnäytetyössä esitellään pääsynvalvonta tietoturvallisuustasojen näkökulmasta sekä pohdi-
taan tasojen toteuttamisen haasteita valtionhallinnolle. Tältä osin tavoitteet täyttyvät ja vie-
vät opinnäytetyötä teknisistä ratkaisuista kohti kirjoittajan omaa aiheeseen liittyvää pohdin-
taa. Tämä voidaan mieltää positiiviseksi muutokseksi, koska avain uuden oppimiseen ja var-
sinkin oppien sisäistämiseen syntyy omassa päässä saavutetun pohdinnan tuloksena.

Lähteet

Andreasson, A. & Koivisto J. 2013. Tietoturvaa toteuttamassa. Tallinna: Tietosanoma.

Asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681

Cygate, 2013. Tietoturvatapahtumat. Viitattu 22.11.2013.

<http://www.cyategroup.com/templates/Page.aspx?id=3376>

Finanssialan Keskusliitto, 2011. Pankkien Tupas-tunnistepalvelun tunnistusperiaatteet. Viitattu 19.10.2013.

http://www.fkl.fi/teemasivut/sahkoinen_asiointi/Dokumentit/Tupas-tunnistusperiaatteet_v20b.pdf

Hämäläinen, T. Todentaminen ja pääsynhallinta. Viitattu 12.11.2013.

<http://users.jyu.fi/~timoh/TIES326/luento4.pdf>

Kajantie, S. 2009. Lokitietojen käsittelystä. Viitattu 9.11.2013.

http://tietoturva.tkk.fi/fi/linkkeja/lokitietojen_kasittely_sk.pdf

Karvi, T. 2010. Tietoturvan perusteet, luentomateriaali. Viitattu 19.10.2013.

<http://www.cs.helsinki.fi/u/karvi/turva-perusteet-luvut-1-3.pdf>

Karvi, T. 2011. Pääsynvalvonta. Viitattu 20.10.2013.

http://www.cs.helsinki.fi/u/karvi/perusteet-luku2-bea_11.pdf

Karvi, T. 2012. Tietoturvan perusteet. Viitattu 19.10.2013.

http://www.cs.helsinki.fi/u/karvi/perusteet-luku1-bea_12.pdf

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista 7.8.2009/617.

Laki viranomaisten toiminnan julkisuudesta 21.5.1999/621.

MTV3, 2013. Suomen ulkoministeriö laajan verkkovakoilun kohteena vuosia. Viitattu 3.11.2013. <http://www.mtv3.fi/uutiset/kotimaa.shtml/2013/10/1826649/mtv3-suomen-ulkoministerio-laajan-verkkovakoilun-kohteena-vuosia>

Oikeusministeriö, 2010. Yhtenäiset tietoturvallisuustoimen valtionhallintoon. Viitattu 11.11.2013.

<http://oikeusministerio.fi/fi/index/ajankohtaista/tiedotteet/2010/07/yhtenaisettietoturvasuustoi.html>

Oulun yliopisto. Yleisesti tietoturvasta. Viitattu 13.11.2013.

<http://www oulu.fi/tietohallinto/tietoturva/sisalto/kannettavientietoturva/tietoturvasta.html>

Ruotsalainen, P. 2002. Ehdotus Sosiaali- ja terveydenhuollon sähköisen asiain arkkitehtuuriksi - terveydenhuollon PKI-arkkitehtuuri. Viitattu 27.10.2013.

http://www.julkari.fi/bitstream/handle/10024/103059/osve4_02.pdf?sequence=1

Suomalaiset teleoperaattorit, 2011. MOBIILIASIOINTIVARMENNE - VARMENNEPOLITIikka - Operaattoreiden mobiiliasiointivarmennteita varten. Viitattu 12.11.2013.

<http://www.mobiilivarmenne.fi/documents/Mobiiliasiointivarmenne-Varmennepolitiikka.pdf>

Thomas, T. 2004. Verkkojen tietoturva: perusteet. Suomentaja Holttinen, J. Helsinki: Edita Publishing.

Tietosuojavaltuutetun toimisto 2010. Biometrinen tunnistus, mikä se on? Viitattu 10.11.2013

http://www.tietosuoja.fi/uploads/xvgogkse_2.pdf

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 1.7.2010/681

Valtiovarainministeriö 2006. Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006. Helsinki. Edita.

Valtiovarainministeriö 2007. Valtionhallinnon tietoturvallisuuden johtoryhmä. Viitattu 10.11.2013. http://www.hare.vn.fi/mHankePerusSelaus.asp?h_ild=12914

Valtiovarainministeriö 2009. Lokiohje, VAHTI 3/2009. Helsinki: Edita.

Valtiovarainministeriö 2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010. Viitattu 27.10.2013.

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20101028Ohjeti/02_Ohje_tietoturvallisuudesta_valtionhallinnossa.pdf

Valtiovarainministeriö 2013. Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI. Viitattu 5.11.2013. http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp

Valtiovarainministeriö 2013. VAHTIn toimintakertomus 2012. Viitattu 10.11.2013.

https://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvaluus/20130603VAHTIn/Vahti_3_2013.pdf

Valtiovarainministeriö 2013. Sovelluskehityksen tietoturvaohje, VAHTI 1/2013. Viitattu 21.11.2013.

https://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvaluus/20130207Sovell/VAHTI_1_Sovelluskehityksen_tietoturvaohje_NETTI.pdf

Viestintävirasto 2011. Ohje 1/2011 Verkkopalvelun ohjelmistoalustan valinta ja palvelun turvallinen ylläpito. Viitattu 10.11.2013. http://www.cert.fi/ohjeet/2011_23/ohje-1-2011.html

Väestörekisterikeskus 2013. Kansalaisvarmenne henkilökortilla. Viitattu 1.11.2013.

<http://www.vaestorekisterikeskus.fi/default.aspx?id=148>

Väestörekisterikeskus 2013. Organisaatiovarmenne. Viitattu 1.11.2013.

<http://www.vaestorekisterikeskus.fi/default.aspx?id=146>

Yle, 2011. Viiden vuoden aikana valtiolta lähti yli 5000 henkilötyövuotta. Viitattu 17.11.2013.

http://yle.fi/uutiset/viiden_vuoden_aikana_valtiolta_lahti_yli_5_000_henkilotyovuotta/2844782

Kuvat

Kuva 1: Lokien synty www-pohjaisessa sähköpostipalvelussa.....	24
Kuva 2: Lokien kerääminen www-pohjaisessa sähköpostipalvelussa.....	26

Kuviot

Kuvio 1: Tietoturvallisuus sekä normit ja ohjaus (Valtionvarainministeriö 2013, 19)	8
Kuvio 2: Viranomaisen tiedot ja asiakirjat (Valtiovarainministeriö 2010)	11

Taulukot

Taulukko 1: Suojaustasojen ja turvallisuusluokitusten suhde tietoturvaluokituksiin.....	13
---	----

Liitteet

Liite 1 Pääsynvalvonnan tietoturvasovaatimukset.....	37
Liite 2 Käyttäjien ja käyttövaltuuksien hallinnan tietoturvasovaatimukset	38

Liite 1: Pääsynvalvonnan tietoturvasovaatimukset

6. Pääsynvalvonnan tietoturvasovaatimukset	Tietoturvaso
1. Tietojärjestelmän omistaja hyväksyy kuinka luotettavaa identiteettiä ja vahvaa tunnistamista järjestelmän sisältämien tietojen käyttöön tarvitaan.	Perus
2. Sekä onnistuneet että epäonnistuneet sisäänkirjautumiset kirjoitetaan lokiin niin, että yksittäisen käyttäjän kirjautumiset järjestelmään voidaan selvittää ja yhdistää hänen henkilöllisyyteensä luotettavasti.	Perus
3. Huonolaatuisten salasanojen käyttöä estetään.	Perus
4. Organisaatiossa on kirjallinen pääsynvalvontapolitiikka, jossa kerrotaan mm. eri turvasoilla hyväksyttävät tekniset tunnistusmenetelmät, tunnusten lukitus ja avausperiaatteet sekä salasanan tai muiden tunnistusten laatuvaatimukset ja vaihtoperiaatteet.	Korotettu
5. Pääsynvalvontalokit säilytetään niin, että niitä ei päästä jälkikäteen muuttamaan.	Korotettu
6. Tunnistuksen epäonnistuminen liian monta kertaa peräkkäin tärkeimpiin järjestelmiin tai palveluihin aiheuttaa tunnuksen lukittumisen.	Korotettu
7. Varmenteiden myöntämisestä, käytöstä ja uusimisesta on kirjallinen ohjeisto ja käytössä olevista varmenteista ajantasainen lista.	Korkea
8. Korkean tason järjestelmissä pääsynvalvontalokeja ja kirjausketjuja tuotetaan myös järjestelmän sisällä toimimisesta toiminnan vaatimusten mukaisesti.	Korkea
9. Tunnistuksen epäonnistumista ja muita oikeuksien puutteeseen kariutuvia toimenpideyrityksiä tilastoidaan.	Korkea

Liite 2: Käyttäjien ja käyttövaltuuksien hallinnan tietoturvasovaatimukset

7. Käyttäjien ja käyttövaltuuksien hallinta:	Tietoturvaso
1. Organisaatiossa on sovittu käyttövaltuuksien hallintaperiaatteet. Tunnusten ja valtuuksien myöntö, muuttaminen ja poisto on organisoitu ja vastuutettu periaatteiden mukaisesti.	Perus
2. Käyttövaltuudet ovat henkilö- tai roolikohtaisia.	Perus
3. Käyttövaltuudet perustuvat palvelussuhteeseen tai muuhun kirjalliseen sopimukseen ja järjestelmien käyttö estetään teknisesti ilman tarpeetonta viivytystä perusteen päätyttyä.	Perus
4. Yksittäisen käyttäjän käyttövaltuudet voidaan selvittää.	Perus
5. Uuden henkilön tullessa organisaatioon ensimmäinen tunnistus tehdään valokuvallisesta henkilöllisyystodistuksesta tai sähköiseen palveluun rekisteröitymisen osalta käyttäen samantasoista todennusmenetelmää.	Perus
6. Organisaatiossa on kirjallinen käyttövaltuuspolitiikka ja hallintaprosessi.	Korotettu
7. Jokaisella käyttövaltuudella on omistaja.	Korotettu
8. Järjestelmien käyttövaltuudet katselmoidaan vähintään kerran vuodessa ja tarpeettomat tunnukset, roolit ja valtuudet suljetaan tai poistetaan.	Korotettu
9. Myöntöprosessista jää jälki, millä perusteella käyttäjälle on myönnetty käyttövaltuus.	Korotettu
10. Kielletyt työ- ja rooliyhdistelmät on dokumentoitu ja valtuuksia myönnettäessä tai muutettaessa kiellettyjen yhdistelmien syntymistä seurataan ja estetään.	Korotettu
11. Ylläpito- ja pääkäyttäjäoikeuksien määrää seurataan ja tilastoidaan.	Korkea
12. Käyttövaltuuksien poistoon kuluvaa aikaa seurataan ja tilastoidaan.	Korkea
13. Organisaatiossa on dokumentoitu menettely käyttäjätunnuksen tai käyttövaltuuksien välittömään poistoon tai passivointiin.	Korkea