PELASTUSOPISTO

VARANTO & TIETOTURVA

VARANTO-hankkeen tietoturvaselvitys

Selvitys pelastustoimen VARANTO-hankkeeseen liittyvistä tietoturvakysymyksistä ja riskeistä sekä tietoturvasuosituksista, -velvoitteista ja lain edellyttämistä tietoturvavastuista.

Pelastusopiston julkaisu

D-Sarja: Muut

4/2013

ISBN 978-952-5905-37-3

ISSN 1795-9187

PELASTUSOPISTO

VARANTO & TIETOTURVA - VARANTO-hankkeen tietoturvaselvitys

Hassinen Marko, FT, Pelastusopisto

Marttila-Kontio Maija, FT, Itä-Suomen Yliopisto

Päivinen Niina, FT, Itä-Suomen Yliopisto

Tutkimusraportti 45 s., 1 liite (7 sivua)

Toukokuu 2013

TIIVISTELMÄ

Pelastusopiston ProntoX hankkeen lopputuloksena syntyi hahmotelma pelastustoimen yhteisestä tietovarannosta, mikä johti VARANTO hankkeen käynnistymiseen. ProntoX hankkeessa nähtiin tarpeelliseksi selvitellä pelastustoimen järjestelmien tietoturvaan liittyviä lähtökohtia, lakeja, asetuksia ja ohjeistuksia. Tämä raportti käy läpi kirjoittamisaikanaan relevantin lainsäädännön sekä valtionhallinnon VAHTI ohjeistusta kuin myös kansallista turvallisuusauditointikriteeristöä (KATAKRI). Raportin tavoitteena on antaa laajamittainen perustietämys pelastustoimen järjestelmiin liittyvien tietoturvatarpeiden perusteista ja hahmottaa tapoja tuoda tietoturvaa näihin järjestelmiin samalla huomioiden käytettävyys ja pelastustoiminnan ominaispiirteet.

PELASTUSOPISTO

VARANTO & TIETOTURVA - VARANTO-hankkeen tietoturvaselvitys

Data Security principles for the VARANTO data warehouse project

Hassinen Marko, Ph.D., Emergency Services College

Marttila-Kontio Maija, Ph.D., University of Eastern Finland

Päivinen Niina, Ph.D., University of Eastern Finland

Research report 45 s., 1 attachment (7 pages)

May 2013

ABSTRACT

The Emegency Services College had a project for developing the registry for operational statistics of emergency services. In this project a new data warehouse idea was developed. The warehouse aims at uniting the emergency services data systems under a common data store.

Under the course of the design it became clear that a survey on the legislation, and rules and regulations concerning data security was needed. This document describes the findings of a research group that went through a vast amount of legal and regulatory documents. Also, the document summarizes the legislative situation and proposes good practices that could be followed in the data security design of emergency services data systems.

SISÄLLYSLUETTELO

Dokumentissa käytetyt lyhenteet

ERICA	Valtion turvallisuusviranomaisten tietojärjestelmä (*Emergency Response Integrated Common Authorities*)
HeTil	Henkilötietolaki
ICT	Tieto- ja viestintätekniikka (*Information and Communications Technology*)
JHS	Julkisen hallinnon suositukset
JUHTA	Julkisen hallinnon tietohallinnon neuvottelukunta
JulkA	Julkisuusasetus (Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta)
JulkL	Laki viranomaisten toiminnan julkisuudesta
KATAKRI	Kansallinen turvallisuusauditointikriteeristö
KEJO	Kenttäjohtamisjärjestelmä
Pronto	Pelastustoimen toimenpiderekisteri
ProntoX	Pelastusopiston tutkimus- ja kehittämisyksikön hanke, jossa tutkitaan Pronton uudistamistarpeita ja mahdollista korvaavaa tietojärjestelmää
TiTuA	Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa
TUPO	Pelastustoimen operatiivisten tietojärjestelmien tietoturvapolitiikka -hanke
TUVE	Turvaverkkoratkaisu
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä
VARANTO	Pelastustoimen tietovaranto -hanke
YTS	Yhteiskunnan turvallisuusstrategia

1. JOHDANTO

Palosuojelurahaston tukemassa Pelastusopiston tutkimus- ja kehittämisyksikön ProntoX-hankkeessa tutkittiin jo pitkään käytössä olleen pelastustoimen toimenpiderekisterin, Pronton, uudistamistarpeita ja mahdollista korvaavaa tietojärjestelmää. ProntoX-hankkeen tuloksena syntyi ajatus pelastustoimen keskitetystä tietovarannosta, joka sittemmin jalostui VARANTO-hankkeeksi. Keskeinen ajatus VARANTO-hankkeessa on luoda koko Suomen pelastustoimen yhdistävä, yhteinen tietovaranto, jossa toimenpiderekisterin lisäksi on useita muita rekistereitä sekä yhteyksiä ulkoisiin tietovarantoihin. Tavoitteena on hyödyntää täysimittaisesti erilaisten pelastustoimen rekisterien, esimerkiksi palotarkastusten ja pelastustoimen resurssien tiedot ja ennen kaikkea näitä tietoja yhdistelemällä tuottaa lisäarvoa pelastuslaitosten toimintaan. VARANTO-tutkimussuunnitelmassa (Kortelainen 2012) tavoitteet ovat ilmaistu seuraavasti: *Hankkeen kokonaistavoitteena on pelastustoimen yhtenäisen tietovarannon ja siihen liittyvien järjestelmäpalvelujen suunnittelu ja määrittely. Keskeisimpiä palveluja ovat: valvontatoiminta (palotarkastukset ym.), resurssienhallinta (ulkoiset ja sisäiset resurssit), tilastot ja seuranta, palontutkinta ja onnettomuustietojen kirjaaminen sekä jatkossa myös valvontaan liittyvä kansalaiskäyttö.* VARANTO-hankkeen tutkimussuunnitelma syntyi ProntoX -hankkeen tuloksena. Samaten tämä tietoturvaselvitys on osa ProntoX -hanketta.

Tietoturvakysymykset nousevat esille usein tietojärjestelmiä suunniteltaessa ja määriteltäessä. Tietoturvan tarve ja merkitys kasvavat jatkuvasti ja etenkin viranomaistoiminnassa lainsäädännön mukanaan tuomat velvoitteet asettavat ajoittain tiukkojakin vaateita viranomaisten sähköisille järjestelmille. Erityisen haasteellinen tilanne on eri toimialojen viranomaisten yhteistoiminnassa ja tiedon vaihdossa viranomaisten välillä. Tietoturvaan liittyvissä vaatimuksissa kuten myös niiden toteuttamisessa on toimialakohtaisia eroja ja pelastustoimessa tämä näkyy eritoten valtion viranomaisten ja kuntaviranomaisten yhteistoiminnassa. Lähtökohtaisesti lainsäädäntökin eroaa kuntaviranomaiseen ja valtion viranomaiseen kohdistuvissa tietoturvavaatimuksissa. Lainsäädännön ja muun normatiivisen ohjauksen merkitys ja toisaalta heterogeenisyys näkyvät myös tässä selvitystyössä, jossa normatiivisen ohjauksen käsittelyyn on käytetty verraten paljon aikaa ja palstatilaa.

Tietoturvaan liittyvä tieto ja tietämys kehittyvät jatkuvasti. Lisäksi uhkat ja uhkakuvat muuttuvat uusien riskien ilmaantumisen myötä. Näin ollen myös ohjeistus kehittyy vastaamaan olemassa olevaa turvallisuustilannetta. Esimerkkinä kehittyvästä ohjeistuksesta voidaan ottaa tätä selvitystyötä laadittaessa ilmestynyt uusi kyberturvallisuustrategia.

Kappaleessa kaksi käydään kompaktissa muodossa läpi toimeksianto jonka perusteella tämä selvitystyö on tehty. Kappaleessa kolme puolestaan on tiivistetty olennaisin normatiivinen (lait, asetukset, määräykset ja sitoviksi katsottavat ohjeistukset soveltuvin osin) materiaali koskien VARANTOa. Tiiviistä esitystavastaan huolimatta kappale on verraten laaja. Kappaleessa neljä puolestaan käsitellään laajemmin tietoturvaan liittyvää ohjeistusta, kuten VAHTI ohjeita, kansallista turvallisuusauditointikriteeristöä (KATAKRI) ja vastikään valmistunutta kyberturvallisuusstrategiaa. Kappale viisi käsittelee teknisiä ratkaisuja lähinnä KATAKRIin nojautuen.

Yhtenä tämän selvitystyön toimeksiannon osana oli laatia riskianalyysi koskien VARANTOa. VARANTO hankkeen ollessa vasta alkuvaiheessaan, riskianalyysissä on rajauduttu käsittelemään sitä sisältöä joka tätä selvitystä tehtäessä on ollut tiedossa tai jonka on voitu olettaa tulevan osaksi lopullista VARANTOa. Riskianalyysi on syytä tehdä uudestaan siinä vaiheessa, kun VARANTO on saanut selkeämmin muotonsa.

Selvitystyön varsinaiset havainnot ja suositukset esitetään kappaleessa seitsemän. Tässä kappaleessa on käsitelty muun muassa lainsäädännön (normatiivinen ohjaus) ja erilaisten ohjeiden vaikutusta ja miten ne tulisi huomioida järjestelmää suunniteltaessa.

Haasteelliseksi tässä työssä osoittautui olemassa olevien dokumenttien suuri määrä sekä dokumenttien hallinnointitahojen laaja kirjo. Dokumenttien nopea ja jatkuva päivittyminen aiheutti haasteita työn edetessä.

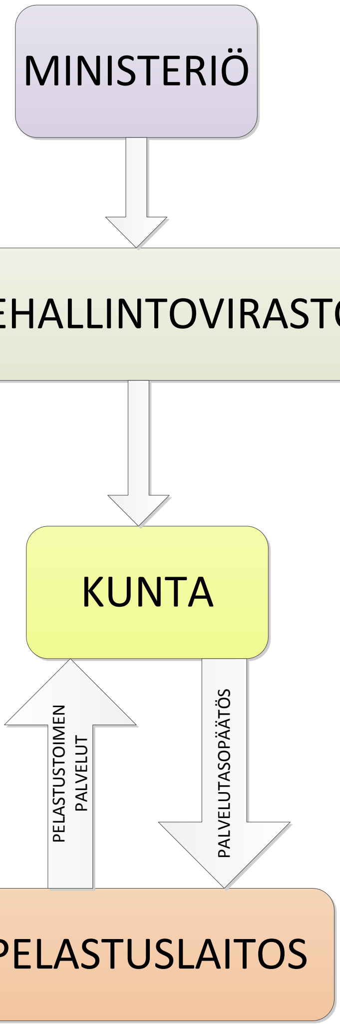
2. TOIMEKSIANTO JA KESKEISET TIETOTURVAKYSYMYKSET

Tämän toimeksiannon sopijaosapuolina ovat dokumentin kirjoittajat (Hassinen, Marttila-Kontio, Päivinen) sekä Pelastusopisto. Toimeksiannon tavoitteena oli kuvata ja luokitella pelastustoimen keskitettyyn tietovarantoon ja järjestelmään (VARANTO) liittyvät keskeiset tietoturvaan liittyvät kysymykset sekä tietoturvaan vaikuttavat tekijät ja muodostaa näiden perusteella tietoturvasuunnitelma VARANTO -järjestelmään. Tietoturvallisuuteen pohjautuen toimeksiannossa tuli arvioida tietoturvan toteutumisesta lainsäädännön ja julkishallinnon suositusten näkökulmasta, arvioida tietovarantoon ja sen sisältämiin rekistereihin liittyvää tietoturvaa, arvioida tietoturva-asetuksen ja turvaverkkoratkaisun (TUVE) vaikutuksia VARANTO -järjestelmään tietoturvan näkökulmasta, sekä selvittää VARANTO -järjestelmän pääsynhallinnan toteutusta.

Yllä olevien lisäksi toimeksiannossa tuli tuottaa tietovarantoon ja järjestelmään kohdistuva riskianalyysi. Riskianalyysissä suoritettiin kunkin riskin yksityiskohtainen kuvaus ja riskin vaikuttavuuden arviointi.

Jo dokumentin alussa on huomioitavaa, että julkisen sektorin *toimijahierarkiaan* ja sitä kautta julkisen sektorin järjestelmiin sekä niiden tietoturvaan liittyvät kysymykset ovat erityisen monitulkintaisia. Paikka paikoin voi olla ristiriitaista tulkita, hallinnoiko kunta, valtio vai pelastuslaitos itse pelastuslaitoksen tietokantaa. Se taho, joka lopulta järjestelmää hallinnoi ja on järjestelmästä vastuuvelvollinen, sanelee pitkälti *tietoturvaan liittyvät yleiset neuvot, suositukset, asetukset, lait, ohjeet* ja *määräykset*. Tästä poikkeuksena on itse pelastustoimen tietokannassa oleva *tieto*, jonka omistaa pelastuslaitos.

Kuvassa 1. selvitetään pelastuslaitoksen (ja sen tietojärjestelmien) hierarkkista suhdetta ylempiin, pelastuslaitoksen toiminnasta osittain tai kokonaan, päättäviin tahoihin.



Kuva 1. Pelastuslaitoksen toimintaan ja tietojärjestelmiin kohdistuva toimijahierarkia.

3. NORMATIIVINEN TIETOTURVALLISUUDEN OHJAUS

Useat turvallisuusalan viranomaiset käyttävät tulevaisuudessa yhteisiä tietojärjestelmiä, kuten hätäkeskustietojärjestelmä ERICA ja viranomaisten yhteinen kenttäjohtamisjärjestelmä KEJO. Käyttötarve on sekä valtion viranomaisilla että kuntaviranomaisilla. Järjestelmien tietoturvamenettelyjen osalta ongelmallista on että valtion viranomaisia koskee jossain määrin erilainen tietoturvalainsäädäntö kuin kuntaviranomaista. VARANTO-järjestelmän osalta tämä ongelma on myös olemassa kun järjestelmään tallennettavia tietoja tullee tarvitsemaan myös valtion viranomaiset. Samoin VARANTOon on nähtävissä tarve tuoda tietoa valtion viranomaisten tietojärjestelmistä, kuten ERICAsta. Tämä luku käsittelee viranomaistoimintaa koskevaa tietosuoja- ja tietoturvalainsäädäntöä ja siihen liittyvää muuta normatiivista ohjeistusta.

3.1. Perusoikeudet

Perustuslaki säätää yksityiselämän suojan (10 §) sisältävän yksityiselämän, kunnian ja kotirauhan suojan. Samassa säädetään puhelun, kirjeen ja muun luottamuksellisen viestin loukkaamattomuus. Vastaavasti perustuslaki säätää sananvapauden oikeudeksi ilmaista, julkistaa ja vastaanottaa tietoja, mielipiteitä ja muita viestejä ilman ennakkosensuuria (12 §). Samassa pykälässä säädetään viranomaisten asiakirjat ja muut tallenteet julkisiksi (ellei tähän ole lailla säädettyä estettä), ja että niistä on jokaisella oikeus saada tieto.

3.2. Julkisuusperiaate

Laki viranomaisten toiminnan julkisuudesta (myöh. julkisuuslaki, JulkL) lähtee liikkeelle olettamasta että viranomaistoiminta on pääsääntöisesti julkista, julkisuusperiaate on lain 1 pykälässä. Julkisuuslain tavoite on edistää viranomaistoiminnan avoimuutta ja se myös velvoittaa hyvään tiedonhallintatapaan (JulkL 3 §). Viranomaisen asiakirjan käsite on julkisuuslaissa määritelty (JulkL 5 §) samoin kuin se milloin asiakirja tulee julkiseksi (JulkL 6 §). On kuitenkin syytä huomata että julkisuuslaissa asiakirjan julkiseksi tuleminen tarkoittaa julkisuuslain soveltamisen voimaan tuloa kyseisen asiakirjan osalta. Viranomaisen asiakirja voi olla julkinen, ei julkinen tai salassa pidettävä. Ei julkinen asiakirja on asiakirja johon ei sovelleta julkisuuslakia, esimerkiksi asiakirja jonka valmistelu on kesken. Samoin viranomaisen sisäiseen toimintaan, esimerkiksi sisäiseen koulutukseen, liittyvät asiakirjat eivät ole julkisia, ellei niillä ole suoranaista vaikutusta jokin viranomaisen asian käsittelyyn (Mäenpää, 2008, s.102). Asiakirjan tultua julkisuuslain soveltamisen piiriin, se on oletusarvoisesti julkinen, ellei jokin lakiin perustuva seikka tee siitä salassa pidettävää (osittain tai kokonaisuudessaan).

3.3. Tiedonsaantioikeus

Tiedonsaantioikeus julkisesta viranomaisen asiakirjasta on subjektiivinen, pyyntöä ei tarvitse perustella eikä tiedon pyytäjän tarvitse identifioida itseään. Tiedonsaanti ei julkisesta asiakirjasta on viranomaisen harkintavallan piirissä (JulkL 9 §). Vastaavasti salassa pidettävästä asiakirjasta ei tietoa saa antaa ilman laissa olevaa säädöstä (JulkL 10 §). Asianosaisella on laajempi tiedonsaantioikeus sellaisiin asiakirjoihin jotka voivat vaikuttaa hänen asiansa käsittelyyn (JulkL 11§) samassa pykälässä luetelluin rajoituksin. Asianomaisella tarkoitetaan henkilöä tai tahoa jonka etuuteen, oikeuteen tai velvollisuuteen tai sellaisesta päättämiseen asiakirja liittyy. Asianosaisen tiedonsaantioikeus ei luonnollisestikaan voi olla subjektiivinen oikeus, vaan asianosainen on aina tunnistettava ennen tiedonsaantipyyntöön suostumista. Asianosaisjulkisuuden ja sen rajoitusten huomioiminen tietojärjestelmien rakentamisessa on syytä ottaa huomioon ja tarkastella erikseen muusta tiedonsaannista.

3.4. Tiedon antaminen

Tiedon antaminen viranomaisen asiakirjasta on olennainen osa viranomaisen tietojärjestelmiä ja siten tiedon antamista on syytä tarkastella tietojärjestelmiä rakennettaessa. Asiakirjan (eli tiedon) pyytämisen lähtökohdat ovat julkisuuslain pykälässä 13 ja antamisesta päättämisen ja päätöksen siirtäminen toiselle viranomaiselle on säädetty pykäliin 14 ja 15. Tietojen saamista ei saa rajoittaa ilman lakiin perustuvaa syytä ja viranomaisen on salassa pidettävästäkin asiakirjasta tapauskohtaisesti harkittava voiko tiedon antaa. Harkinnassa on huomioitava salassapitosäännöksen luonne ja tietopyynnön tapauskohtaiset piirteet. Salassapitosäännöksiä on kolmea tyyppiä:

Vahinkoedellytyslausekkeeton salassapitosäännös tarkoittaa ehdotonta salassapitoa, kuten esimerkiksi JulkL 24§, kohta 1.

" valtioneuvoston ulkopoliittisia asioita käsittelevän valiokunnan asiakirjat, jollei valiokunta toisin päätä, sekä ulkoasioita hoitavan ministeriön ja Suomen edustustojen poliittiset tilannearvioinnit, poliittisista tai taloudellisista suhteista toisen valtion kanssa käytyjä neuvotteluja koskevat asiakirjat ja ulkoasiainhallinnon alaan kuuluvat salakirjoitetut viestit, jollei asianomainen ministeriö toisin päätä;"

Säännöksessä ei toisin sanoen jätetä viranomaiselle minkäänlaista harkintavaltaa salassapidon osalta.

Julkisuusolettamaan perustuva salassapitosäännös tarkoittaa sitä että säännöksessä kuvattu tieto on oletusarvoisesti julkista ja salassapito perustuu tiedon antamisen aiheuttamaan haittaan. Esimerkiksi JulkL 24§, kohta 8.

" asiakirjat, jotka koskevat onnettomuuksiin tai poikkeusoloihin varautumista, väestönsuojelua taikka turvallisuustutkintalain (525/2011) mukaista tutkintaa, jos tiedon antaminen niistä vahingoittaisi tai vaarantaisi turvallisuutta tai sen kehittämistä, väestönsuojelun toteuttamista tai poikkeusoloihin varautumista, vaarantaisi turvallisuustutkinnan tai sen tarkoituksen toteutumisen, vaarantaisi tiedon saantia tutkintaa varten taikka loukkaisi onnettomuuden, vaaratilanteen tai poikkeuksellisen tapahtuman uhrien oikeuksia tai heidän muistoaan tai läheisiään;"

Tällaiset tiedot voidaan määritellä salassa pidettäviksi vain silloin kun on perusteltua olettaa tiedon antamisen aiheuttavan säännöksessä kuvattuja haittavaikutuksia ("jos tiedon antaminen niistä vahingoittaisi …").

Salassapito-olettamaan perustuva salassapitosäännös lähtee liikkeelle siitä että säännöksessä kuvattu tieto on lähtökohtaisesti salassa pidettävää, mutta tieto voidaan antaa, mikäli voidaan olla varmoja, ettei tiedon antaminen aiheuta säännöksessä kuvattuja haitallisia vaikutuksia. Esimerkiksi JulkL 24§, kohta 7.

"henkilöiden, rakennusten, laitosten, rakennelmien sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat ja niiden toteuttamiseen vaikuttavat asiakirjat, jollei ole ilmeistä, että tiedon antaminen niistä ei vaaranna turvajärjestelyjen tarkoituksen toteutumista;"

Julkisuuslain 17 § edellyttää salassa pidettävää tietoa annettaessa, että tiedonsaajalla on julkisuuslain mukainen vaitiolovelvollisuus. Lisäksi vain erityisen painavista syistä tietoa voi antaa viranomaisten ulkopuolelle. Asianosaisilla on muita laajemmat tiedonsaantioikeudet ja heille luovutetuissa asiakirjoissa saattaa olla muitakin kuin asianosaista koskevia salassa pidettäviä tietoja. "*Salassapitomerkinnän tarkoitus on saattaa asianosaisuuden perusteella salassa pidettäviä tietoja saanut tietoiseksi siitä, että niiden käyttöön liittyy salassapidosta johtuvia rajoituksia*" (Voutilainen 2012,s. 114) Luovuttajan velvollisuus on varmistaa että vastaanottaja pystyy huolehtimaan luovutuksessa syntyvistä velvoitteista salassapidon osalta.

3.5. Salassapito

Julkisuuslain 6 luku sisältää säädökset salassa pidettävien tietojen käsittelyyn ja tunnistamiseen. Lain 22§ määrittelee asiakirjasalaisuuden koskevaksi asiakirjaa joka on laissa määrätty salassa pidettäväksi taikka jos se sisältää tietoa josta on laissa määrätty vaitiolovelvollisuus. Lain 23§ määrittelee myös hyväksikäyttökiellon jonka mukaisesti luottamuksellista tietoa ei saa käyttää omaksi hyödyksi tai toisen vahingoksi.

Julkisuuslain 24 § erikseen luettelee salassa pidettävät viranomaisasiakirjat. Lisäksi tietojen salassapitoa määrittelee mm. Henkilötietolaki (HeTil) sekä terveydenhuoltoa koskevat lait potilaan oikeuksista ja potilastiedosta. Henkilötietolaki 523/1999 antaa verraten lavean ohjeistuksen henkilötietojen suojauksesta 32 pykälässä: "Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi ". Lisäksi henkilötietolaissa erikseen säädetään millä edellytyksillä ja kuka saa henkilörekisteriä pitää sekä tietyt arkaluontoiset henkilötiedot joita rekisterissä ei saa olla, kuten seksuaalinen suuntautuminen jne. Julkisuuslaissa salassa pidettäväksi määrättyjen asiakirjojen osalta ainakin seuraavat pykälän 24 kohdat ovat pelastustoimessa huomioon otettavia:

- 7 henkilöiden, rakennusten, laitosten, rakennelmien sekä tieto- ja viestintäjärjestelmien turvajärjestelyjä koskevat … asiakirjat

- 8 asiakirjat, jotka koskevat onnettomuuksiin tai poikkeusoloihin varautumista, väestönsuojelua taikka turvallisuustutkintalain mukaista tutkintaa … taikka loukkaisi onnettomuuden, vaaratilanteen tai poikkeuksellisen tapahtuman uhrien oikeuksia tai heidän muistoaan tai läheisiään
- 17 asiakirjat, jotka sisältävät tietoja valtion, kunnan tai muun julkisyhteisön tai 4 §:n 2 momentissa tarkoitetun yhteisön, laitoksen tai säätiön liike- tai ammattisalaisuudesta…
- 25 …taikka tietoja henkilön terveydentilasta tai vammaisuudesta taikka hänen saamastaan terveydenhuollon ja kuntoutuksen palvelusta …
- 32 asiakirjat, jotka sisältävät … tietoja henkilön elintavoista, osallistumisesta yhdistystoimintaan tai vapaa-ajan harrastuksista, perhe-elämästä tai muista niihin verrattavista henkilökohtaisista oloista;

Näistä kohdat 7 ja 8 ovat sellaisia joissa dokumentit voidaan myös turvaluokitella (Tietoturva-asetus 11 §) sikäli kuin ne ovat valtion viranomaisen dokumentteja (tietoturva-asetus). Tietoturva-asetusta käsitellään tuonnempana. Pelastustoimen osalta kohdan 8 dokumentteja ei ole yleensä tarve käsitellä tietojärjestelmissä. Kohta 7 on ongelmallisempi, näitä tietoja tarvitaan mm. kohdekorteissa ja pelastussuunnitelmissa.

Päätöksen salassapidosta tekee joko asiakirjan laatija tai erikseen työjärjestyksessä mainittu organisaation henkilö.

3.6. Luokittelu

Julkisuuslain 25 § säätää merkintävelvollisuuden salassa pidettäviin asiakirjoihin. Sama velvoite koskee myös suullisesti annettua tietoa. Samassa pykälässä mainitaan asiakirjojen luokittelu, joka kertoo, minkälaisia tietoturvallisuusvaatimuksia salassa pidettävän asiakirjan käsittelyssä vaaditaan. Salassa pidettävä tieto voidaan (mutta ei ole pakko) määritellä jollekin neljästä suojaustasosta, joista Suojaustaso 1 on edellyttää korkeinta tietoturvatasoa. Luokittelua ei siis ole välttämätöntä tehdä, vaan tieto voi olla yksinkertaisesti salassa pidettävää ilman että sitä olisi sijoitettu millekään suojaustasolle. Lienee kuitenkin tavanomainen käytäntö tehdä suojaustasomerkintä aina kun tieto on salassa pidettävää.

3.7. Suojaustasot

Salassa pidettävä dokumentti on tavanomaista sijoittaa jollekin neljästä suojaustasosta. Seuraavassa käydään läpi perusteet, joilla asiakirja voidaan määritellä tietylle tasolle (TiTuA 9§).

Suojaustaso 1: Asiakirja määritellään suojaustasolle 1 (suojaustaso I), *jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **erityisen suurta vahinkoa** salassapitosäännöksessä tarkoitetulle **yleiselle edulle**;*

Suojaustaso 2: Asiakirja määritellään suojaustasolle 2 (suojaustaso II), *jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **merkittävää vahinkoa** salassapitosäännöksessä tarkoitetulle **yleiselle edulle**;*

Suojaustaso 3: Asiakirja määritellään suojaustasolle 3 (suojaustaso III), *jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **vahinkoa** salassapitosäännöksessä tarkoitetulle **yleiselle tai yksityiselle edulle**;*

Suojaustaso 4: Asiakirja määritellään suojaustasolle 4 (suojaustaso IV), *jos asiakirjaan sisältyvän salassa pidettävän tiedon oikeudeton paljastuminen tai oikeudeton käyttö voi aiheuttaa **haittaa** salassapitosäännöksessä tarkoitetulle **yleiselle tai yksityiselle edulle**.*

Suojaustasolle 4 voidaan tietyin reunaehdoin sijoittaa myös sellaista tietoa tai asiakirjoja jotka eivät ole salassa pidettäviä (TiTuA 10§).

3.8. Turvallisuusluokittelu

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (TiTuA 681/2010) määrittelee myös turvallisuusluokituksen pykälässä 11.

*"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 tarkoitetulla 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".

Turvallisuusluokitusmerkintää ei saa käyttää muissa kuin 1 momentissa tarkoitetuissa tapauksissa, ellei merkinnän tekeminen ole tarpeen kansainvälisen tietoturvallisuusvelvoitteen toteuttamiseksi tai asiakirja muutoin liity kansainväliseen yhteistyöhön."

VARANTO -järjestelmän osalta turvallisuusluokittelun tarvetta on vaikea nähdä, mutta viranomaisten yhteistoiminnan edellytysten varmistamiseksi on syytä tiedon tallentamisessa ja käsittelyssä varautua käsittelemään myös turvallisuusluokiteltua tietoa. Tietoturvallisuuteen ja tiedon käsittelyyn liittyvät vaatimukset turvallisuusluokitellun materiaalin osalta ovat vastaavan suojaustason vaatimukset. Tietoturva-asetus koskee vain valtion viranomaisia ja näin ollen pelastustoimi kunnallisena toimijana ei ole velvoitettu käyttämään turvaluokittelua tai muutoinkaan toimimaan tietoturva-asetuksen vaatimalla tavalla. Toisaalta viranomaisten yhteistoiminnan näkökulmasta tilanne on mutkikkaampi.

Olennaista turvaluokittelussa on siis se, että turvaluokitus määrää asiakirjan luokitusta vastaavalle suojaustasolle. Suojaustaso puolestaan säätelee asiakirjan käsittelyyn ja säilyttämiseen liittyvät tekniset ja organisatoriset vaatimukset. Kansallinen turvallisuusauditointikriteeristö (KATAKRI) määrittelee millaisia tietoteknisiä ja organisatorisia vaatimuksia kullekin suojaustasolle sijoitetun asiakirjan säilyttämiseen ja käsittelyyn tarvitaan. Pääsääntöisesti pelastustoimen salassa pidettävä tieto sijoittuu suojaustasolle 4, mikä tarkoittaa että tietojärjestelmiltä edellytetään niin sanottua perustietoturvatasoa.

Tietoturva-asetus määrittelee tietoturvallisuuden perustason (TiTuA 5§). Tietoturvallisuuden perustason tuottamisessa on huolehdittava siitä että:

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.

Vaikkakin edelleen valtion viranomaisia koskeva, tämä perustaso on syytä toteuttaa kaikissa kunnallisen sektorin tietojenkäsittely-ympäristöissä joissa käsitellään viranomaisten yhteistoiminnassa tarvittavaa tietoa. "..., *jonka (TiTuA) säännökset tulee ottaa huomioon myös* *kuntien asiakirja- ja tietohallinnossa, koska kunnatkin joutuvat käsittelemään valtionhallinnon viranomaisten asiakirjoja ja tietojärjestelmiä*" (Voutilainen 2012, s 114). Samassa lähteessä, s. 124 todetaan että perustason vaatimukset ovat johdettavissa joko henkilötietolaista tai julkisuuslaista suoraankin ja siten niiden voidaan katsoa velvoittavan myös kuntia ja muita julkisuuslain piiriin kuuluvia toimijoita.

Tietojenkäsittely-ympäristöt on luokiteltu kolmeen tasoon: perustaso, korotettu taso ja korkea taso. Viranomaisten tietojärjestelmien täytyy minimissään toteuttaa perustaso (VAHTI 2/2010, Ohje tietoturvallisuudesta valtion hallinnossa annetun asetuksen täytäntöönpanosta). Kyseissä VAHTI ohjeessa käsitellään viranomaisia yleensä, erittelemättä kuntasektoria, joten epäselvää on missä määrin perustason vaatimus juridisesti ulottuu kuntaviranomaisiin. Tasolle kolme sijoittuvat asiakirjat vaativat korotetun tietoturvatason, mikä tarkoittaa lisääntyviä kustannuksia kun tietojenkäsittely-ympäristöt täytyy rakentaa vastaamaan annettuja vaatimuksia. Vaade löytyy mm. tietoturva-asetuksesta: "*Valtionhallinnon viranomainen voi sallia, että suojaustasoon III kuuluva asiakirja siirretään viranomaisen tietoverkossa, jonka käyttö on rajoitettu, jos viranomainen on varmistanut, että tietoverkko ja tietojenkäsittely kokonaisuudessaan täyttävät tavanomaisesti sovellettavan korotetun tietoturvallisuuden tason vaatimukset*."(TiTuA 19§).

3.9. Salassapidon elinkaari

Tiedon salassa pidolle on olemassa ajallisia rajoitteita. Asiakirjaa ei saa pitää salassa kun laissa säädetty tai lain nojalla määräytynyt salassapitoaika on kulunut (JulkL 31§). Yleinen salassapitoaika viranomaisen asiakirjassa on 25 vuotta, yksityiselämän suojaamiseksi salassa pidettävissä asiakirjoissa (JulkL 24§, 24-32 kohdat) 50 vuotta kyseessä olevan henkilön kuolemasta tai 100 vuotta ellei henkilön kuolemasta ole tietoa. Turvallisuusluokiteltua tietoa voidaan tarveharkintaisesti pitää salassa kauemminkin (JulkL 31§). Salassapito myös lakkaa edellä mainittua määräaikaa aiemmin, jos salassapitosäännöksen suojaamaa etua ei ole enää tarvetta suojata salassapidolla. Tällainen voi esimerkiksi olla puretun rakennuksen turvallisuusjärjestelyitä suojaava salassapitovelvoite.

3.10. Hyvä tiedonhallintatapa

Yleisesti ottaen viranomaisella on velvollisuus edistää tiedonsaantia ja hyvää tiedonhallintatapaa. Julkisuuslain 18 pykälä säätää hyvän tiedonhallintatavan. Hyvä tiedonhallintatapa sisältää asiakirjojen, tietojärjestelmien sisältämien tietojen ja tietojärjestelmiin liittyvien tietojen saatavuuden, käytettävyyden, eheyden ja suojaamisen. Pykälässä viitataan mm. tietoturvajärjestelyihin ja tietojärjestelmiin liittyviin uhkatekijöihin. Kokonaisuudessaan pykälä on syytä huomioida rakennettaessa tietojärjestelmiä viranomaiskäyttöön. Hyvästä tiedonhallintotavasta säädetään myös asetuksella (Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintotavasta) .

Julkisuuslain pykälä 18 listaa seuraavat velvollisuudet:

1) pitää luetteloa käsiteltäviksi annetuista ja otetuista sekä ratkaistuista ja käsitellyistä asioista tai muutoin huolehtia siitä, että sen julkiset asiakirjat ovat vaivattomasti löydettävissä;

2) laatia ja pitää saatavilla kuvaukset pitämistään tietojärjestelmistä sekä niistä saatavissa olevista julkisista tiedoista, jollei tiedon antaminen ole vastoin 24 §:n tai muun lain säännöksiä;

3) selvittää tietojärjestelmien käyttöönottoa sekä hallinnollisia ja lainsäädännöllisiä uudistuksia valmisteltaessa suunniteltujen toimenpiteiden vaikutus asiakirjojen julkisuuteen, salassapitoon ja suojaan sekä tietojen laatuun samoin kuin ryhtyä tarpeellisiin toimenpiteisiin tietoon liittyvien oikeuksien ja tiedon laadun turvaamiseksi sekä asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suojan järjestämiseksi;

4) suunnitella ja toteuttaa asiakirja- ja tietohallintonsa samoin kuin ylläpitämänsä tietojärjestelmät ja tietojenkäsittelyt niin, että asiakirjojen julkisuus voidaan vaivattomasti toteuttaa ja että asiakirjat ja tietojärjestelmät sekä niihin sisältyvät tiedot arkistoidaan tai hävitetään asianmukaisesti ja että asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen suoja, eheys ja laatu turvataan asianmukaisin menettelytavoin ja tietoturvallisuusjärjestelyin ottaen huomioon tietojen merkitys ja käyttötarkoitus sekä asiakirjoihin ja tietojärjestelmiin kohdistuvat uhkatekijät ja tietoturvallisuustoimenpiteistä aiheutuvat kustannukset;

5) huolehtia siitä, että sen palveluksessa olevilla on tarvittava tieto käsiteltävien asiakirjojen julkisuudesta sekä tietojen antamisessa ja käsittelyssä sekä niiden ja asiakirjojen ja tietojärjestelmien suojaamisessa noudatettavista menettelyistä, tietoturvallisuusjärjestelyistä ja tehtävänjaosta, samoin kuin siitä, että hyvän tiedonhallintavan toteuttamiseksi annettujen säännösten, määräysten ja ohjeiden noudattamista valvotaan.

3.11. Hyvä julkisuus- ja salassapitorakenne

Hyvällä julkisuus- ja salassapitorakenteella tarkoitetaan sitä, että julkiset tiedot ovat helposti saatavilla eikä salassa pidettävien tietojen luottamuksellisuus vaarannu (Voutilainen 2006, s.67). Julkisten tietojen saatavuuteen liittyy myös erityisryhmien, kuten näkövammaisten, mahdollisuudet saada tietoja viranomaisten tietojärjestelmistä. Perustuslaki säätää yhdenvertaisuusperiaatteen, jonka mukaisesti tietojärjestelmissä pitäisi mahdollisuuksien mukaan huomioida myös erityisryhmien tiedon saanti.

Tiedon saanti julkisista asiakirjoista on subjektiivinen oikeus jolloin tietojärjestelmän käyttäjää ei voi velvoittaa tunnistautumaan palveluun. Tiedon saanti julkisista tiedoista täytyy onnistua anonyymisti. Asianosaisjulkisuuteen perustuva tiedon saanti puolestaan on aina harkintaan perustuvaa ja silloin tiedon pyytäjä on aina tunnistettava luotettavasti ennen kuin tietoja voidaan luovuttaa (Voutilainen 2006, s. 250). Tämä tulisi ottaa huomioon tietojärjestelmän julkisuus- ja salassapitorakenteessa.

VAHTI-ohjeistus (mm. VAHTI 2/2010) ottaa kantaa salassapidon ulottuvuuteen asiakirjassa. Salassapitomerkinnästä ohjeistus sanoo, että *"merkinnästä tulee käydä ilmi, miltä osin asiakirja on salassa pidettävä ja mihin salassapito perustuu".* Sähköisissä järjestelmissä tietojen metatietoja kannattaa hyödyntää siten että salassapito voidaan määritellä tietoyksiköittäin ja siten julkisen tiedon eritteleminen asiakirjasta on mahdollista. Arkistonmuodostussuunnitelma on hyvä apuväline tällaisen salassapitorakenteen luomisessa. VAHTI 2/2010 -ohjeessa todetaan "*Asianhallinnan metatietomäärityksen (SÄHKE2) mukaan salassapitoa koskevat metatiedot tulevat oletusarvoisina arkistonmuodostussuunnitelmasta*".

3.12. Kansainväliset tietoturvallisuusvelvoitteet

Kansainvälisellä tietoturvallisuusvelvoitteella tarkoitetaan sellaista Suomea sitovaan kansainväliseen sopimukseen sisältyvää määräystä sekä sellaista muuta Suomea koskevaa velvoitetta, jota Suomen on noudatettava ja joka koskee erityissuojattavan aineiston suojaamiseksi tarvittavia toimenpiteitä. Toimenpiteet tulevat voimaan esimerkiksi silloin, kun ko. tietoaineiston Suomeen tuonut osapuoli tekee turvallisuusluokitusta koskevan merkinnän. Vastaavasti Suomessa toimiva viranomainen voi tehdä käsillä olevaan tietoaineistoon kansainvälisen turvallisuusluokitusmerkinnän.

Erityissuojattavalla tietoaineistolla tarkoitetaan: ”salassa pidettäviä asiakirjoja ja materiaaleja, asiakirjoista ja materiaaleista saatavissa olevia tietoja, sekä näiden perusteella tuotettuja asiakirjoja ja materiaaleja, jotka kansainvälisen tietoturvallisuusvelvoitteen mukaisesti on turvallisuusluokiteltu” (Laki kansainvälisistä tietoturvallisuusvelvoitteista).

Turvallisuusluokitellulla sopimuksella tarkoitetaan kansainvälisessä tietoturvallisuusvelvoitteessa tarkoitetulla tavalla laadittua sopimusta, joka on toisen valtion viranomaisen tai siellä kotipaikkaansa pitävän yrityksen taikka kansainvälisen järjestön tai toimielimen ja Suomessa kotipaikkaansa pitävän elinkeinonharjoittajan välillä. Sopimus laaditaan osapuolten välille esimerkiksi kun tarjouskilpailuun osallistuminen tai sopimuksen toteuttaminen voi edellyttää pääsyä erityissuojattavaan tietoaineistoon.

Tämän lain soveltaminen voi tulla kyseeseen mm. yhteiskunnallisesti elintärkeiden toimintojen turvaamisen yhteydessä raja-alueilla.

3.13. Tietoturvallisuustoimenpiteet

Kansainvälisen tietoturvallisuusvelvoitteen alaisissa tietoaineistoissa ja niiden käsittelyssä tulee ottaa huomioon mm. seuraavat toimenpiteet

1. Tietoaineistoon on pääsy vain niillä, jotka tietoja tarvitsevat tehtävänsä hoitamisessa. Henkilöt on nimettävä etukäteen.
2. Tietoaineisto on pidettävä salassa, ellei kansainvälisessä tietoturvallisuusvelvoitteessa toisin mainita.
3. Vaitiolovelvollisuus ja hyväksikäyttökielto
4. Tietoaineistoon on aina tehtävä luokittelumerkintä siitä, minkälaisia tietoturvallisuusvaatimuksia sen käsittelyssä on noudatettava.

VARANTO-järjestelmässä ei tällä hetkellä suunnitellussa kokoonpanossaan ole nähtävissä kansainvälisen tietoturvavelvoitteen alaista materiaalia. On kuitenkin syytä huomata että esimerkiksi kohta 1 on yleinen tietoturvaperiaate (*need to know*) ja ohjeistettu yleisemminkin materiaalien suhteen mm. VAHTI 2/2010 -ohjeistuksessa. Usein velvoitetaan myös ylläpitämään luetteloa niistä henkilöistä, joilla on oikeus käsitellä salassa pidettävää tietoa. Sisäasiainministeriön määräyksessä on todettu että, "Viranomaisen on pidettävä luetteloa omasta henkilökunnastaan, eli tietoa siitä, kuka saa missäkin työtehtävässä käsitellä salassa pidettäviä asiakirjoja tai henkilörekisteriin kuuluvia asiakirjoja (Sisäasiainministeriön määräys salassa pidettävien tietoaineistojen luokittelusta ja käsittelystä, 2011). Samoin kohta 3 on säädetty useissa yhteyksissä, mm. JulkL 23§, 3 momentti.

3.14. Arkistointiin liittyvä lainsäädäntö

Arkistolaki (831/1994) velvoittaa mm. valtion virastoja, laitoksia, kunnallisia viranomaisia sekä muita yhteisöjä ja toimielimiä niiden suorittaessa julkista tehtävää lain tai asetuksen perusteella siltä osin kuin niille kertyy viranomaisten toiminnan julkisuudesta annetussa laissa (621/1999) tarkoitettuja asiakirjoja. Arkistoon kuuluvat asiakirjat, jotka ovat saapuneet arkistonmuodostajalle sen tehtävien johdosta tai syntyneet arkistonmuodostajan toiminnan yhteydessä. Arkistotoimen tehtävänä on varmistaa asiakirjojen käytettävyys ja säilyminen, huolehtia asiakirjoihin liittyvästä tietopalvelusta, määritellä asiakirjojen säilytysarvo ja hävittää tarpeellinen aineisto. Arkistotointa on hoidettava siten että se tukee sekä arkistonmuodostajan tehtävien suorittamista että yksityisten ja yhteisöjen oikeutta saada tietoja julkisista asiakirjoista. Lisäksi yksityisten ja yhteisöjen oikeusturva, samoin kuin tietosuoja, on otettu asianmukaisesti huomioon. Yksityisten ja yhteisöjen oikeusturvaan liittyvien asiakirjojen saatavuus on varmistettu ja asiakirjat palvelevat tutkimuksen tiedon lähteinä. Pysyvään säilytykseen määrätyt asiakirjat on laadittava ja tiedot tallennettava pitkäaikaista säilytystä kestäviä materiaaleja ja säilyvyyden turvaavia menetelmiä käyttäen. Asiakirjoja on säilytettävä siten, että ne ovat turvassa tuhoutumiselta, vahingoittumiselta ja asiattomalta käytöltä. Asiakirjat, joita ei ole määrätty pysyvästi säilytettäviksi tulee hävittää niille määrätyn säilytysajan jälkeen siten, että tietosuoja on varmistettu.

3.15. Pelastuslaki

Pelastuslain (379/2011) tavoitteena on parantaa ihmisten turvallisuutta ja vähentää onnettomuuksia. Tässä laissa säädetään pelastustoimen viranomaisten organisaatiosta, hallinnosta ja toimivallasta. Pelastustoimen palveluksessa olevia ja pelastustoimintaan osallistuvia koskee vaitiolovelvollisuus, joka ei kuitenkaan estä ilmaisemasta hengen tai terveyden suojaamiseksi tarpeellista tietoa. Pelastusviranomaisella on myös velvollisuus tilastotietojen antamiseen. Pelastuslaitos saa pitää toimenpiderekisteriä (teknisenä ylläpitäjänä Pelastusopisto), varautumistehtävien rekisteriä sekä valvontarekisteriä.

3.16. Tietoturvallisuuden arviointi

Laki tietoturvallisuuden arviointilaitoksista (1405/2011) säätää menettelystä, jonka avulla yritykset voivat osoittaa luotettavasti ulkopuolisille, että niiden toiminnassa on toteutettu määrätty tietoturvallisuuden taso. Tätä lakia sovelletaan elinkeinonharjoittajiin ja palvelutehtäviä julkishallinnolle tarjoaviin yksiköihin, jotka toimeksiannosta arvioivat tietoturvallisuustason ja jotka haluavat toiminnalleen Viestintäviraston hyväksynnän. Tietoturvallisuuden arviointiperusteina voidaan tässä laissa tarkoitetussa arvioinnissa käyttää arvioinnin kohteen valinnan mukaan:

1. lailla tai asetuksella säädettyjä viranomaisten toimintaa koskevia tietoturvallisuusvaatimuksia ja valtiovarainministeriön tietoturvallisuutta koskevia ohjeita;
2. kansainvälisistä tietoturvallisuusvelvoitteista annetussa laissa tarkoitetun kansallisen turvallisuusviranomaisen antamia kansainvälisten tietoturvallisuusvelvoitteiden toteuttamista koskevia ohjeita;
3. Euroopan unionin tai muun kansainvälisen toimielimen antamia tietoturvallisuutta koskevia säännöksiä tai ohjeita;
4. julkaistuja ja yleisesti tai alueellisesti sovellettuja tietoturvallisuutta koskevia säännöksiä, määräyksiä tai ohjeita;
5. vahvistettuun standardiin sisältyviä tietoturvallisuutta koskevia vaatimuksia.

3.17. Tietojärjestelmistä vaadittavat selosteet

Julkisuuslain tarkoittamia viranomaisen tietojärjestelmiä ovat järjestelmät joka sisältävät tietovarantoja tai tietokantoja, jotka muodostuvat pääsääntöisesti julkisuuslain tarkoittamista asiakirjoista tai asiakirjatiedosta. Tällaisia tietojärjestelmiä eivät ole esimerkiksi työkaluohjelmistot (mm. tekstinkäsittely) tai tietoliikenneohjelmistot.

Lainsäädäntö velvoittaa viranomaista tuottamaan ja pitämään saatavilla useita tietojärjestelmiinsä ja niihin tallennettuihin tietoihin liittyviä selosteita järjestelmien rakenteesta ja niihin tallennetuista tiedoista.

Julkisuusasetus (Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta) säätää velvoitteen laatia tietojärjestelmäseloste: *Viranomaisen on laadittava ylläpitämistään tietojärjestelmistä seloste, josta ilmenee tietojärjestelmän käyttötarkoitus ja siihen talletettavat tiedot. Seloste on pidettävä yleisön saatavilla kirjaamossa tai muussa yleisöpalvelupisteessä, jollei salassapitosäännöksistä muuta johdu. Seloste voidaan sisällyttää myös osaksi arkistonmuodostussuunnitelmaan (*JulkA, 8§*).* Tietojärjestelmäselosteen laatimista on ohjeistettu mm. Valtiovarainministeriön toimesta julkaisussa Julkisuuslain (Laki viranomaisten toiminnan julkisuudesta 621/1999) mukaisen tietojärjestelmäselosteen laadintasuositus.

Henkilötietolain (523 /99) 10 § säätää velvollisuuden laatia henkilörekisteristä rekisteriseloste, josta ilmenee:

1) rekisterinpitäjän ja tarvittaessa tämän edustajan nimi ja yhteystiedot;

2) henkilötietojen käsittelyn tarkoitus;

3) kuvaus rekisteröityjen ryhmästä tai ryhmistä ja näihin liittyvistä tiedoista tai tietoryhmistä;

4) mihin tietoja säännönmukaisesti luovutetaan ja siirretäänkö tietoja Euroopan unionin tai Euroopan talousalueen ulkopuolelle; sekä

5) kuvaus rekisterin suojauksen periaatteista.

Selostuksen on oltava saatavilla, usein se löytyy rekisterin pitäjän www-sivuilta. Erityisistä, lähinnä turvallisuuteen liittyvistä syistä, rekisteriselosteen saatavilla olosta voidaan poiketa.

3.18. *Sähköiseen asiointiin liittyvä normiohjaus*

Sähköisen asioinnin mahdollisuuksia viranomaistoiminnassa helpottamaan ja edistämään on säädetty laki sähköisestä asioinnista viranomaistoiminnassa. Lain tarkoituksena on selkeyttää viranomaisten ja palveluita käyttävien asiakkaiden oikeudet, velvollisuudet ja vastuut. Laki velvoittaa viranomaisen tarjoamaan sähköisiä palveluita (5 §):

Viranomaisen, jolla on tarvittavat tekniset, taloudelliset ja muut valmiudet, on niiden rajoissa tarjottava kaikille mahdollisuus lähettää ilmoittamaansa sähköiseen osoitteeseen tai määriteltyyn laitteeseen viesti asian vireille saattamiseksi tai käsittelemiseksi. Tällöin on lisäksi kaikille tarjottava mahdollisuus lähettää sähköisesti viranomaiselle sille toimitettavaksi säädettyjä tai määrättyjä ilmoituksia, sen pyytämiä selvityksiä tai muita vastaavia asiakirjoja taikka muita viestejä.

Lisäksi saatavuudelle on säädetty pykälässä 6 vaatimus, että palvelujen tulee olla saatavilla muulloinkin kuin viraston aukioloaikana. Viranomaisen on kuitenkin viipymättä ilmoitettava lähettäjälle asiakirjan tai viestin vastaanottamisesta (12§). Sähköinen asiakirja on arkistoitava siten että sen eheys ja alkuperäisyys voidaan todentaa.

Sähköisen viestin (*sähköisellä viestillä tarkoitetaan sähköisellä tiedonsiirtomenetelmällä lähetettyä tarvittaessa kirjalliseen muotoon tallennettavissa olevaa informaatiota 1§)* perillemenosta vastaa lähettäjä. Viestissä tai muussa asiakirjassa ei tarvita omakätistä allekirjoitusta, ellei ole jostain syystä epäillä viestin eheyttä tai alkuperää ja siinä on tiedot lähettäjästä (9§). Sähköinen viesti tai asiakirja voidaan sähköisesti allekirjoittaa vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetun lain mukaisella sähköisellä allekirjoituksella.

3.19. Vahva sähköinen tunnistaminen ja sähköiset allekirjoitukset

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista määrittelee vahvan sähköisen tunnistamisen henkilön yksilöimiseksi siten että käytetty tunniste voidaan todentaa aidoksi ja oikeelliseksi. Todentamisen tulee perustua vähintään kahteen näistä kolmesta tekijästä:

a) salasanaan tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltija tietää;

b) sirukorttiin tai johonkin muuhun sellaiseen, mitä tunnistusvälineen haltijalla on hallussaan; tai

c) sormenjälkeen tai johonkin muuhun tunnistusvälineen haltijan yksilöivään ominaisuuteen;

Sinällään kyseessä on vakiintunut vahvan tunnistamisen (strong authentication, esim. Scheier 1996) määritelmä. VAHTI-ohjeissa käytetään myös kevyen tunnistamisen käsitettä (esim. VAHTI 12/2006, Tunnistaminen julkishallinnon verkkopalveluissa), jolla tässä yhteydessä tarkoitetaan yhden tekijän käyttöön perustuvaan tunnistamiseen. Vahvaa tunnistamista tulee käyttää mm. silloin, kun käytetään korotetun tai korkean tietoturvatason palveluita organisaation ulkopuolisista tietoliikenneverkoista tai turvattomiksi katsotuista toimitiloista. (VAHTI 3/2012, Teknisen ICT-ympäristön tietoturvataso-ohje)

Sähköinen allekirjoitus on edellä mainitun lain 54 mukaan oikeustoimikelpoinen "*Jos oikeustoimeen vaaditaan lain mukaan allekirjoitus, vaatimuksen täyttää ainakin sellainen kehittynyt sähköinen allekirjoitus, joka perustuu laatuvarmenteeseen ja on luotu turvallisella allekirjoituksen luomisvälineellä*". Laatuvarmenne on erikseen määritelty lain pykälässä 30.

3.20. Potilastiedot

Potilastietoihin liittyvät velvoitteet salassapidon osalta samoin kuin potilaan, potilaan omaisen ja terveydenhuollon ammattihenkilöiden tiedonsaantioikeudet säädetään laissa potilaan asemasta ja oikeuksista (Laki potilaan asemasta ja oikeuksista). Lain 3§ säätää potilaan yksityisyyden kunnioituksen, mikä tarkoittaa luonnollisesti potilaan yksityisyyteen kuuluvien hoitoon liittyvien dokumenttien salassapitoa. Tiedonsaantioikeus on säädetty pykälässä 5, jossa säädetään tiedon antaminen terveydenhuollon ammattihenkilön tehtäväksi ja muutoin viitataan henkilötietolakiin ja julkisuuslakiin. Alaikäisen tai omasta hoidostaan päätöksentekoon kykenemättömän henkilön huoltajan tai edustajan tiedonsaantioikeus on säädetty pykälässä 9. Pykälä 12 säätää tietojen hävittämisestä niiden tullessa tarpeettomiksi ja 13§ käsittelee varsinaista salassapitoa. Tiedon on pidettävä salassa eikä niitä saa ilman suostumusta luovuttaa sivulliselle. On huomattavaa että *"Sivullisella tarkoitetaan tässä laissa muita kuin asianomaisessa toimintayksikössä tai sen toimeksiannosta potilaan hoitoon tai siihen liittyviin tehtäviin osallistuvia henkilöitä."* (13§, kirjoitusvirhe korjattu lain alkuperäisestä sanasta toimeksiannosta). Tiedon saanti siis edellyttää osallistumista potilaan hoitoon. Tieteelliseen tutkimukseen tiedon saanti on erikseen turvattu samassa pykälässä.

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (9.2.2007/159) on säädetty tarkoituksena "*edistää sosiaali- ja terveydenhuollon asiakastietojen tietoturvallista sähköistä käsittelyä*". Laissa säädetään tietojen saatavuuden ja käytettävyyden vaatimus, samoin kuin eheys ja muuttumattomuus (4§). Tässä on mielenkiintoinen käsitemäärittely, tietoturvamielessä tiedon eheys tarkoittaa samaa kuin muuttumattomuus. Suora vaatimus tietoturvan osalta on pykälässä 9: "*Asiakastietojen eheys, muuttumattomuus ja kiistämättömyys tulee varmistaa sähköisellä allekirjoituksella tietojen sähköisessä käsittelyssä, tiedonsiirrossa ja säilytyksessä. Luonnollisen henkilön sähköisessä allekirjoittamisessa tulee käyttää vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista annetussa laissa tarkoitettua kehittynyttä sähköistä allekirjoitusta*".

Nämä lain kohdat on syytä ottaa huomioon arvioitaessa esimerkiksi toimenpiderekisterin osalta henkilöihin liittyvien kirjausten sisältöjä.

3.21. Pelastustoimen erityispiirteet

Tietojärjestelmien osalta sopimuspalokunnat ovat tietoturva-asioiden osalta omalaatuisessa asemassa, kun ajatellaan esimerkiksi viranomaisten yhteistä kenttäjohtamisjärjestelmää. Pelastustoimi on ainoa sisäministeriön toimiala jolla toimijat eivät aina ole viranomaisia. Sosiaali- ja terveydenhuoltosektorilla tosin myös kunnallisena toimialana on käyttäjiä, joilla ei välttämättä ole virkastatusta mutta joiden tarvitsee käyttää samoja järjestelmiä. Esimerkkinä näistä ovat yksityiset sairaankuljetusyritykset.

Pelastuslaki määrää että pelastusviranomainen on alueen pelastuslaitoksen nimittämä virkamies. Näin ollen sopimuspalokuntalaista ei voi periaatteessa nimittää virkamieheksi, koska hän ei ole virkasuhteessa pelastuslaitokseen. Sopimuspalokuntalainen voi kuitenkin toimia pelastustoiminnan johtajana: *"Pelastustoimintaa voi kuitenkin tilapäisesti johtaa muu pelastuslaitoksen palveluksessa oleva tai sopimuspalokuntaan kuuluva siihen saakka, kun toimivaltainen pelastusviranomainen ottaa pelastustoiminnan johtaakseen. Pelastustoiminnan johtaja toimii virkavastuun alaisena."* (Pelastuslaki, 34§)

Muun muassa kenttäjohtamisjärjestelmää olisi kuitenkin tarpeen pystyä käyttämään yhdessä muiden viranomaisten kanssa, jotta esimerkiksi yhteinen tilannekuva voidaan muodostaa. Samoin VARANTO-järjestelmästä tulisi tilannepaikan johtajan pystyä saamaan tilanteen johtamisessa tarvittava tieto.

3.22. Lainsäädännön vaikutus VARANTO-järjestelmän suunnitteluun

Tietoturvamenettelyjen suunnittelu sovelluksen suunnittelun alkuvaiheessa on tärkeää ja siinä on syytä ottaa huomioon sovelluksen erilaisten käyttäjäryhmien valmiudet toteuttaa vaadittuja tietoturvaan kuuluvia toimenpiteitä. KATAKRI määrittelee erilaisille tietoturvatasoille vaaditut toimenpiteet, mutta on tilanteita joissa eri tasoille toteutetuissa tietoturvaympäristöissä toimivat viranomaiset tarvitsevat yhteistoimintamahdollisuuden. KATAKRI määrittelee perustietoturvatasolle tietoturvamenettelyt joiden käyttö pelastustoimen näkökulmasta on varsin tavanomaista, tai ainakin nähtävissä käyttökelpoisiksi. Tilanne muuttuu jossain määrin silloin kun käsitellään suojaustaso 3:n asiakirjoja (suojaustaso 1 tai 2 tuskin tulee kysymykseenkään). Tällöin sovellusympäristö tulee sijoittaa korotetulle tietoturvatasolle, mikä KATAKRIn mukaisesti (I 501.0) tarkoittaa mm. vahvaa tunnistautumista. Tosin KATAKRI vaatimuksessa sanotaan "*Käyttäjän tunnistamiseen käytetään vahvaa käyttäjäntunnistusta, mikäli samalla tietojärjestelmällä hallinnoidaan useampia kuin yhtä ko. suojaustason hanketta tai projektia.*" Vaatimus on epäselvä ja tulkinnan varainen.

Yleisin tapa toteuttaa vahvan tunnistautumisen vaatimus on sirulla varustettu toimikortti. Sivutoimisen ja vapaaehtoisen sopimuspalokuntalaisen osalta tämä alkaa tuntua hieman turhan vaativalta, jos pelastustoimen tehtävää ei voi hoitaa ilman toimikorttia. Isompi vaiva tämä kuitenkin on pelastuslaitoksille, jotka maksavat kustannukset korttien hallinnoinnista. Vähintään yhtä iso kuluerä pelastuslaitoksille on tietoteknisten ympäristöjen saattaminen korotetulle tasolle.

Olennaista sekä tietoturvan että lainsäädännön ja tiedonsaantioikeuksien toteuttamiseksi on noudattaa hyvää julkisuus- ja salassapitorakennetta. Tämän rakenteen on syytä olla mahdollisimman atomaarinen ja perustua tiedon ja asiakirjojen metatietojen hyödyntämiseen. "*Hyvän julkisuus- ja salassapitorakenteen noudattaminen tarkoittaa myös sitä, että salassapitosäännöksiä tulee tulkita, jos se on lain sanamuodon mukaisesti mahdollista, tietoyksiköittäin eikä asiakirjakohtaisesti*" (Voutilainen 2012, s 113).

VAHTI 2/2010 -ohje käsittelee erikseen laajojen tietovarantojen luokittelua koskevia suosituksia (VAHTI 2/2010, s. 60). Ohjeistuksessa tuodaan esille että vaikka tietovarannon yksittäiset asiakirjat tai tietoyksiköt olisivat julkisia, niiden yhdistäminen saattaa johtaa tilanteeseen, jossa syntyy tarvetta suojata tietoyhdistelmä. Ohjeessa sanotaan "*Onkin suositeltavaa, että viranomainen arvioi koko tietovarannon suojaustarpeen sekä käyttää tarvittaessa yksittäisten asiakirjojen arviointia laajempaa vaikutusarviointia tietovarannon suojaustarpeesta ja soveltaa sen mukaisia tietoturvamenettelyjä*". Tietovarastojen yksittäisten tietoyksiköiden yhdistelemisestä syntyvät luottamuksellisuusongelmat ovat sangen vaikeita hallita. Aihetta on toistaiseksi tutkittu verraten vähän ja on nähtävissä että tutkimusalue tulee jatkossa saamaan aiempaa enemmän huomiota. Jukka Mähönen on Pro gradu -tutkielmassaan *Web-palvelujen tiedon käytön rajoitukset* tehnyt ansiokkaan katsauksen aiheeseen liittyvään tietojenkäsittelytieteelliseen teoriaan ja olemassa oleviin teknologioihin (Mähönen 2013).

Potilastiedoista säädetty tietoturvaan liittyvä ohjaus on huomattavan seikkaperäistä ja velvoittavaa. Lainsäädännön vaatima tietoturvan taso ja siihen liittyvät menetelmät vaativat verraten mittavia panostuksia järjestelmien suunnittelussa, toteutuksessa ja käytössä. Ottaen huomioon VARANTO-järjestelmässä mahdollisesti nähtävissä olevan potilastiedoksi luokiteltavan tiedon marginaalisen luonteen, ei mielestämme ole järkevää lähteä luomaan järjestelmää siten että siinä varaudutaan potilastiedon tallentamiseen.

3.23. Operatiivinen tietoturvapolitiikka

Olennainen dokumentti tietoturvatasojen määrittelyssä on organisaation tietoturvapolitiikka. Pelastustoimen osalta 22 aluelaitosta toimivat pääsääntöisesti isäntäorganisaationsa tietoturvapolitiikan mukaisesti. Tilanne jossa yhdellä toimialalla on mahdollisesti 22 toisistaan eriävää tietoturvapolitiikkaa, on kestämätön ainakin sovellustuotannon näkökulmasta. Pelastustoimi tarvitsee mahdollisimman pian laitosten yhteisen, operatiivisten tietojärjestelmien tietoturvapolitiikan ja mm. VARANTO-hankkeen osalta se pitäisi yhteen sovittaa muiden toimialojen kanssa, mikäli halutaan että muut toimialat voivat hyödyntää esimerkiksi palotarkastustietoja.

Onkin tarpeen selvittää pelastustoimen osalta eri aluelaitosten tietoturvapolitiikat ja vertailla niitä tavoitteena analysoida yhtäläisyydet ja eroavaisuudet. Näistä lähtökohdista voidaan luoda luonnos pelastustoimen operatiivisten tietojärjestelmien tietoturvapolitiikaksi. Samalla kerätään ja analysoidaan muiden toimialojen vastaavat dokumentit ja pyritään löytämään yksi, yhteiset nimittäjät koostava tietoturvapolitiikka joka on sekä pelastuslaitosten että muiden toimialojen hyväksyttävissä. Tietoturvapolitiikassa myös sopimuspalokunnat tulee huomioida ainakin siten että pääsynhallinnassa voidaan luoda tehtäväkohtaisia pääsyoikeuksia jolloin sopimuspalokunnan yksikönjohtaja tai vastaava saa tarvittavat palvelut virka-aseman puuttumisesta huolimatta. Tietoteknisesti ja tietoturvamenettelyin tällainen tehtäväkohtainen pääsynvalvonta on toteutettavissa.

Yhteinen tietoturvapolitiikka luo pohjan toimialojen yhteisten tietojärjestelmien tietoturvamääritysten tekemiselle.

4. SUOSITUKSET, OHJEISTUKSET

Tietoturvallisuuteen liittyvät suositukset ja ohjeistukset eivät velvoita tietokanta- tai järjestelmäylläpitäjää erityisiin tietoturvallisuutta koskeviin toimiin mutta niiden noudattamien on hyvän tavan mukaista. Tärkeimpiä tietoturvallisuuteen liittyviä suosituksia ja ohjeistuksia ovat valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) ohjeistus, Kansallinen turvallisuusauditointikriteeristö (KATAKRI), julkisen hallinnon suositukset (JHS), yhteiskunnan turvallisuusstrategia (YTS) sekä valtiovarainministeriön julkaisema hyvä tiedonhallintatapa. Lisäksi kuntien ICT-varautumista koskeva dokumentti on tulevaisuusnäkökulmasta huomion arvioinen.

4.1. VAHTI

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI tukee valtioneuvostoa ja valtiovarainministeriötä hallinnon tietoturvallisuuteen liittyvässä päätöksenteossa. VAHTI käsittelee kaikki merkittävät valtionhallinnon tieto- ja kyberturvallisuutta koskevat säädökset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset. Lisäksi se ohjaa valtionhallinnon tietoturvatoimenpiteitä. Tässä dokumentissa viitataan lukuisiin eri VAHTI-säädöksiin ja -ohjeisiin eikä tässä yhteydessä esitellä niitä yksityiskohtaisemmin.

Valtionhallinnon alaisuudessa toimivien järjestelmien lisäksi VAHTI-ohjeistuksen voidaan katsoa koskevan myös pelastustoimen tietovarantoja, varsinkin, kun pelastustoimen tietovarannot ovat yhteydessä sellaisiin valtionhallinnon alaisuudessa toimiviin tietojärjestelmiin, joita koskevat valtionhallinnon VAHTI-säädökset ja -ohjeet.

4.2. KATAKRI

KATAKRI on Kansallinen turvallisuusauditointikriteeristö ja se on tarkoitettu työkaluksi turvallisuusviranomaisille yritysten tai yhteisöjen turvallisuustason todentamiseen sekä sen varmistamiseen, että valtionhallinnolle palveluja tarjoava taho kykenee toimimaan riittävän turvallisesti valtionhallinnon turvallisuusluokitelluissa hankkeissa. KATAKRI on pyritty laatimaan tietoturvallisuusasetuksen sekä sitä täydentävien ohjeiden kanssa ristiriidattomaksi. KATAKRI koostuu neljästä pääosasta (*hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus sekä tietoturvallisuus*), joita ei ole tarkoitettu itsenäisiksi kokonaisuuksiksi.

Turvallisuusjohtamisen lähtökohtana on se, että toimintaa koskevat laki- ja sopimusperustaiset vaatimukset on tunnistettu ja täytetty (KATAKRI A105.1). Organisaation turvallisuuspolitiikassa tai -ohjeistossa on kuvattu keskeiset turvallisuustavoitteet (KATAKRI A108.0). Kaikki suojattavaa tietoa käsittelevät tietoverkot ja -järjestelmät ovat tietoturvaperiaatteiden mukaisesti suojattuja (KATAKRI A306.0), sekä toiminnalle tärkeät suojattavat kohteet (toiminnot, tiedot, järjestelmät ja prosessit) on tunnistettu ja niiden suojausmenetelmät on suhteutettu kohteisiin sekä niihin kohdistuviin riskeihin (KATAKRI A401.1). Henkilöstöturvallisuus tarkoittaa salassa pidettävään tietoon pääsevän henkilöstön hallinnointia, ja sen tärkeimmät osa-alueet ovat henkilöstön turvallisuuskoulutus (KATAKRI P103.0) sekä salassapito- ja vaitiolositoumuksien allekirjoittaminen ennen pääsyoikeuden saamista suojattavaan tietoon (KATAKRI P407.0).

4.3. Kuntien ICT-varautuminen

Vuonna 2011 tehdyn *Kuntien ICT-varautuminen* -selvityksen mukaan kuntien varautuminen tietojärjestelmiin kohdistuviin ulkoisiin ja sisäisiin riskeihin on erittäin heikolla tasolla. Dokumentissa todetaan, että kuntien ICT-varautumista tulee kehittää radikaalisti. Kunnilla ei tällä hetkellä ole yhteistä ICT-varautumisen ohjeistokokonaisuutta ja ICT-varautumisen ohjaus ja johtaminen kunnissa on epäyhtenäistä ja osittain puutteellista. Tämä johtaa erinäisiin vaikeuksiin, kun laajan verkottuneen ympäristön varautumista häiriötilanteisiin pitäisi toteuttaa kustannustehokkaasti. Kuntiin kohdistuvat ICT-varautumisen strategiset muutokset vaikuttavat näin ollen kuntien vastuulla olevien tietojärjestelmien tietoturvaratkaisuihin ja tietoturvallisuutta koskeviin käytänteisiin. Perusajatuksena ICT-varautumisen kehittämisessä on se, että kunnat tuottavat yhteiskunnan elintärkeiden toimintojen kannalta välttämättömiä palveluita. Valtionhallinnon ICT-varautumiselle on määritetty vaatimukset, jotka vastaavat normaaliolojen häiriötilanteiden sekä erityistilanteiden ja poikkeusolojen tarpeita. Yhteiskunnan elintärkeiden toimintojen turvaamisen (YETT/YTS) mukaisesti ne tulee huomioida kuntien ICT-varautumisessa (ks. Suomen kyberturvallisuusstrategia).

Jokaisella kunnalla tulee olla ICT-varautumisen velvoitteet täyttävä toimintastrategia ja tietoturvapolitiikkaan (riskienhallintapolitiikkaan) pohjautuva ICT-varautumisen kehittämis- ja toimintasuunnitelma. Vuoden 2016 loppuun mennessä kuntien tulee saavuttaa kriittisissä toiminnoissa ICT-varautumisen perustaso. Edelleen, vuoden 2020 loppuun mennessä kuntien on kokonaisuudessaan pitänyt saavuttaa ICT-varautumisen perustaso sekä erikseen määritellyiltä osiltaan korotettu tai korkea taso.

Strategian yhteydessä tarvitaan siihen liittyvät keskitetyt velvoittavat ohjeet. Strategian kehittämistyössä voidaan hyödyntää valtionhallinnon tuottamaa ICT-varautumisen käyttöön tarkoitettua aineistoa (ks. mm. huoltovarmuuskeskus), sekä VAHTIn ja JHS:n tuottamia ohjeistuksia, jotka eivät kuitenkaan ole sitovia ICT-varautumista tai tietoturvallisuutta ohjaavia asiakirjoja (JHS).

Tärkeänä osana kuntien ICT-varautumisessa on riskienhallinta ja jatkuvuuden hallinta. Riskianalyysissä kartoitetaan uhka-arviot, jonka perustana käytetään YTS:n uhka-arviota. Lisäksi riskianalyysissä luodaan omien suojattavien toimintojen tarpeet sekä haavoittuvuus- ja vaikuttavuustarkastelut. Jatkuvuuden hallinta tarkoittaa sitä, että mahdollisen häiriötilanteen sattuessa tuetaan toiminnan edellyttämän palvelutason ylläpitämistä.

Koska kunnat käyttävät palvelutuotannossaan mm. Väestörekisterikeskuksen, Verottajan, Kansaneläkelaitoksen, valtiovarainministeriön, sosiaali- ja terveysministeriön, sisäministeriön ja opetusministeriön tietojärjestelmien tuottamia palveluita tai perusrekistereitä, kuntien on huolehdittava näitä tietojärjestelmiä hyödyntävien palveluidensa turvallisuudesta ja ICT-varautumisesta asettamalla toimialojensa tietojärjestelmille valtionhallinnon kanssa yhtenevät vaatimukset (Kuntien ICT-varautuminen). Toteutuksen tukena on kuntien suositeltavaa käyttää esimerkiksi julkishallintoa varten tehtyjä turvallisuussopimusmalleja (VAHTI 7/2006, liite 1, Turvallisuussopimusmallit).

Kriittisissä ja keskeisissä valtakunnallisissa tieto- ja viestintäjärjestelmissä yksittäisen kohteen lamautuminen tai vaurio ei saa lamauttaa koko järjestelmää. Tietojärjestelmät ja tietovarannot on hajautettava maantieteellisesti vähintään kahteen paikkaan.

Yhteiskunnan toimivuudelle kriittisiä tietojärjestelmiä suunniteltaessa ja rakennettaessa on varmistettava, että niihin liittyvän ohjauksen, ylläpidon, järjestelmähallinnan ja teknisen tuen osaaminen säilyy Suomessa tai ohjaus- ja hallintakyky on oltava mahdollista palauttaa Suomeen. Sovellusten tietovarantojen tulee olla Suomessa. Tietojärjestelmät ja niiden muodostamat kokonaisuudet tulee dokumentoida.

Sähköisten palvelujen ja tietovarantojen varautumisen vaatimuksista ja niiden toteuttamisesta ovat vastuussa kaikki palvelujen käyttöön, ylläpitoon ja tuottamiseen osallistuvat tahot.

Kunnan yhteisille tietovarannoille ja niitä tukeville palveluille *ei* (vielä) ole asetettu yleisellä tasolla vaatimuksia.

4.4. Suomen kyberturvallisuusstrategia ja yhteiskunnan turvallisuusstrategia (YTS)

Suomen kyberturvallisuusstrategia liittyy kiinteästi aiemmin tunnettuun ”yhteiskunnan elintärkeiden toimintojen turvaamisen strategiaan” (YETTS). YETTS on sittemmin korvattu yhteiskunnan turvaamisen strategialla (YTS 2010), johon kyberturvallisuusstrategiassa viitataan.

Suomen kyberturvallisuusstrategialla tarkoitetaan kykyä hallita koko laajaa kybertoimintaympäristöä sekä normaali- että poikkeusoloissa. Perusperiaatteena on turvata elintärkeiden toimintojen sujuvuus sellaisessa yhteiskunnassa, joka on riippuvainen tietoverkkojen ja tietojärjestelmien toiminnasta.

Yhteiskunnan elintärkeät toiminnot ovat:

- Valtion johtaminen
- Kansainvälinen toiminta
- Valtakunnan sotilaallinen puolustaminen
- Sisäisen turvallisuuden ylläpitäminen
- Talouden ja infrastruktuurin toimivuus
- Väestön toimeentuloturva ja toimintakyky

- Henkinen kriisinkestävyys

Kuntien rooli yhteiskunnan elintärkeiden toimintojen turvaamisessa on keskeinen, koska peruspalveluiden ja muiden yhteiskunnan elintärkeiden toimintojen järjestäminen on normaaliolosuhteissakin erityisesti kuntien vastuulla. Näin ollen YTS osaltaan säätelee kuntien ICT-varautumista ja sitä kautta vaikuttaa pelastustoimen tietojärjestelmiin, jotka toimivat kuntien sekä osin valtion alaisuudessa.

Erityisesti johtamiseen ja elintärkeiden toimintojen ohjaamiseen tarvittavat sähköisen viestinnän ja tietoliikenteen sekä energiahuollon järjestelmät on suojattava ja varmennettava jo normaalioloissa kestämään myös erilaisten häiriötilanteiden ja poikkeusolojen vaatimukset. (Turvallisuustilanteita ovat normaaliolot, häiriötilanteet ja poikkeusolot, joissa saattaa syntyä erityistilanteita.)

Erityisesti tilannekuvan muodostaminen, ylläpitäminen, analysoiminen ja jakaminen tarvitsijoille korostuvat. Häiriötilanteissa on tiedotettava aktiivisesti tilanteesta, viranomaisten toiminnasta ja toimintaohjeista sekä valtionjohdon linjauksista.

Häiriötilanteissa ja poikkeusoloissa sähköisiä tieto-, viestintä- ja energiajärjestelmiä käytetään viranomaisten, organisaatioiden ja elinkeinoelämän yritysten johtamistoimintaan.

Yhteiskunnallisesti elintärkeiden toimintojen uhkamallit YTS:n mukaan ovat:

- voimahuollon vakavat häiriöt
- tietoliikenteen ja tietojärjestelmien vakavat häiriöt
- kuljetuslogistiikan vakavat häiriöt
- yhdyskuntatekniikan vakavat häiriöt
- elintarvikehuollon vakavat häiriöt
- rahoitus- ja maksujärjestelmän vakavat häiriöt
- julkisen talouden rahoituksen saatavuuden häiriintyminen
- väestön terveyden ja hyvinvoinnin vakavat häiriöt
- suuronnettomuudet, luonnon ääri-ilmiöt ja ympäristöuhkat
- terrorismi ja muu yhteiskuntajärjestystä vaarantava rikollisuus
- rajaturvallisuuden vakavat häiriöt
- poliittinen, taloudellinen ja sotilaallinen painostus sekä
- sotilaallisen voiman käyttö.

Yllä olevassa listassa kohta: *tietoliikenteen ja tietojärjestelmien vakavat häiriöt* on tämän dokumentin kannalta oleellisin. Uhkamalliin pohjautuen mm. kuntien ja valtion hallinnon alaisten tietojärjestelmien suunnittelussa, muokkaamisessa, rakentamisessa sekä ylläpidossa tulee ottaa huomioon yllä alla esitetyt skenaariot, riskit sekä toimintamallit.

Sähköiset tietojärjestelmät ja niitä yhdistävät tiedonsiirtoverkot muodostavat järjestelmäkokonaisuuksia, joiden häiriöiden mahdolliset vaikutukset laajenevat yksittäisistä palveluista aina koko järjestelmiä koskeviksi. Verkkojen lisäksi kokonaisuuteen kuuluvat tietokoneet, matkapuhelimet, verkkojen palvelimet ja muu infrastruktuuri. Kyseiset järjestelmät toimivat sähköenergian varassa, mikä tekee niistä haavoittuvia kaikissa turvallisuustilanteissa. Yhteiskunnan kehitykseen liittyvät tekijät, kuten tietoverkkojen lisääntyvä käyttö teknologioiden monimutkaistuminen, reaaliaikaisuus saattavat muodostua riskeiksi.

Tietojärjestelmiä, tiedonsiirtoa sekä sähköistä joukkoviestintää voivat uhata luonnonilmiöiden, inhimillisen toiminnan tai tekniikan pettämisen aiheuttamat onnettomuudet sekä järjestelmiin kohdistuvat tahalliset sähköiset ja fyysiset hyökkäykset, tietojärjestelmän luvaton käyttö tai häirintä. Eräs tunnetuimmista keinoista Internet-palveluiden häiritsemiseen on palvelunestohyökkäys, jonka tarkoituksena on ylikuormittaa verkkopalvelimet tai Internetpalveluntarjoajan toimintakapasiteetti automaattisesti muodostettavilla viesteillä.

Tietojärjestelmien suurimpina uhkina voidaan pitää seuraavia:

- madot, virukset
- salakuuntelu
- väärään sähköiseen identiteettiin perustuvat petokset
- sähköiset hyökkäykset
- kriittisten tietoteknisten järjestelmien häiriöt
- ilkivalta
- siirtokapasiteetin ylikuormitus
- haittaohjelmat
- *phishing*-hyökkäykset

Lisäksi tietojärjestelmän uhkana voidaan mainita varusohjelmistoon sekä niiden hallintaan liittyvät uhkat. Suomalaisten tietojärjestelmien riskitekijänä on nimenomaan sellaiset varusohjelmistot, joiden lähdekoodeja ei ole Suomessa yleensä käytettävissä (pois lukien avoimen lähdekoodin ohjelmistot). Lisäksi varusohjelmistojen syvällisen asiantuntemuksen keskittyminen ulkomaisiin osaamiskeskuksiin on selkeä uhka kotimaisten järjestelmien tietoturvallisuudelle. Varusohjelmistojen lisenssien hallinta on usein kokonaan ulkomailla. Huomattavana riskitekijänä voidaan myös pitää mahdollisuutta pysäyttää tiedonkäsittely maamme rajojen ulkopuolelta jättämällä päivittämättä varusohjelmistojen lisenssejä.

4.4.1. Sähköisten tieto- ja viestintäjärjestelmien vaatimukset

Sähköisten tieto- ja viestintäjärjestelmien tärkeimpiä vaatimuksia ovat luotettavuus ja turvallisuus. Kyberturvallisuusstrategian mukaan kyberturvallisuuden edellytys on jokaisen kybertoimintaympäristössä toimivan toteuttamat tarkoituksenmukaiset ja riittävät tietojärjestelmien ja tietoverkkojen turvallisuusratkaisut.

Yhteiskunnan turvallisuusstrategiassa, johon Suomen kyberturvallisuusstrategia nojaa, järjestelmien toimivuus on varmistettu tarkoituksenmukaisin menetelmin asianomaisten viranomaisten sekä yritysten yhteistyön avulla. Yhteiskunnan turvallisuusstrategiassa painotetaan tarkoituksenmukaista, nopeaa, oikeisiin tietoihin ja arviointeihin perustuvaa tilannetietoisuutta ja tilannekuvaa. Tämän tärkeys korostuu erityisesti poikkeusoloissa ja silloin, kun yhteiskunnan turvallisuus on jollakin tavoin uhattuna. Hyvä tilannetietoisuus ja tilannekuva vaativat sujuvaa yhteistoimintaa. Tämä tarkoittaa yhteistyötä ja osaamista eri toimijoiden (viranomaisten, päätöksentekijöiden, ym.) välillä. Lisäksi vaatimus velvoittaa erilaisten sähköisten tieto- ja viestintäjärjestelmien ongelmatonta yhteentoimivuutta. Tämä tarkoittaa, että ”tietojärjestelmien tulee mahdollistaa systemaattinen tietolähteiden käyttö ja yhteistoiminta sekä siihen liittyvä joustava tilannetietoisuuden jakaminen”. Tilannekuvan tuottaminen on YTS:n mukaan hajautettu koko hierarkkiselle kentälle valtion ylimmästä johdosta aina kuntatasolle saakka. YTS ei erikseen mainitse, kuinka tämä strategia vaikuttaa pelastustoimen tietojärjestelmiin.

Kyberturvallisuusstrategiassa käytettyjä termejä: *toimija* ja *keskeinen toimija* ei ole tarkoin määritelty, jolloin näihin tekijöihin liittyvät vastuut ja velvoitteet jäävät osin kyseenalaisiksi.

5. TEKNISET RATKAISUT TIETOTURVALLISUUDEN NÄKÖKULMASTA

Tietoturva koostuu kolmesta osasta: luottamuksellisuus (*confidentiality*, C), eheys (*integrity*, I) ja saatavuus (*availability*, A). Luottamuksellisuudella tarkoitetaan sitä, että tietoon pääsevät käsiksi vain ne, joilla on siihen oikeus; saatavuuden mukaan tieto on aina saatavilla. Eheys takaa sen, että tietoon kohdistuu vain auktorisoituja muutoksia.

Tietojenkäsittely-ympäristölle asetettavat tietoturvatason vaatimukset riippuvat siitä, minkä suojaustason aineistoa niissä käsitellään. Tämä tarkoittaa esimerkiksi sitä, että perustasoa korkeamman suojaustason dokumentteja ja aineistoja voi käsitellä selväkielisenä (salakirjoittamatta) vain sellaisessa ympäristössä, joka on tämän tason sääntöjen mukainen (VAHTI 3/2012, VAHTI 2/2010). Riittävät suojaustasot määritellään riskiarviointimenettelyn avulla.

Toimitilaturvallisuus (fyysinen turvallisuus) on eräs tietoturvan tärkeistä osa-alueista. Siinä otetaan huomioon tietoverkkojen ja -järjestelmien sisältämien laitteiden sijoittelu turvallisiin tiloihin (VAHTI 1/2002). Erityistä huomiota on kiinnitettävä niiden fyysisten tilojen suojaukseen, joissa käsitellään tai säilytetään turvallisuusluokiteltua materiaalia. Toimitilaturvallisuuden takaamiseksi liikkumista on rajoitettu ja sitä seurataan videovalvonnalla (KATAKRI F103.0, F104.0). Kaikkien käyttäjien pääsy- ja käyttöoikeuksia hallitaan suppeimpien oikeuksien periaatteen mukaisesti, ja laitetiloissa on rikosilmoitin-, kulunvalvonta- sekä kameravalvontajärjestelmät (KATAKRI F301.0, F302.0, F303.0, F304.0). Tarkemmat laitetilojen turvallisuusohjeet löytyvät VAHTI 1/2002 -ohjeesta sekä Kansallisesta turvallisuusauditointikriteeristöstä (KATAKRI).

Organisaation tietoverkko on erotettu palomuurilla julkisesta internetistä. Lisäksi verkko on jaettu vyöhykkeisiin ja segmentteihin, joiden välistä liikennettä valvotaan ja rajoitetaan. Turvallisuusluokiteltu aineisto siirretään aina salattuna (KATAKRI I401.0). Sisäverkon rakenteen ja siinä kulkevan liikenteen tarpeeton näkyminen on estetty, ja sisäverkon osoitteet eivät kuulu julkiseen verkkoon (KATAKRI I407.0). Reitityksen turvallisuudesta on huolehdittu riskienarvioinnin mukaisesti (KATAKRI I410.0). Reitityksessä määritellään tarpeelliset ja riittävät suotimet informaation välittämiseen; erityistä huomiota on kiinnitettävä verkkovyöhykkeet ylittävään liikenteeseen.

Organisaation tiedot on luokiteltu niiden merkittävyyden ja lakisääteisten vaatimusten perusteella. Tietosisällöltään suojattavat dokumentit varustetaan suojaustasoa kuvaavalla merkinnällä (KATAKRI I601.0). Suojattavaa tietoa sisältäviä aineistoja ja tietovälineitä säilytetään turvallisesti (esim. kassakaapissa) (KATAKRI I602.0). Suojattavia tietoja sisältävät, sekä sähköiset että ei-sähköiset, aineistot hävitetään luotettavasti (KATAKRI I603.0). Suojattavan aineiston kopiointi ja tulostaminen on järjestetty riskienarvioinnissa riittävän turvalliseksi katsotulla menettelyllä (KATAKRI I604.0, VAHTI 3/2012). Suojattavat tiedot siirretään aina asianmukaisesti suojaten (KATAKRI I605.0). Suojaus on otettava huomioon myös esimerkiksi tallennettaessa tietoa päätelaitteelle tai siirrettävälle apumuistille, tai lähetettäessä tietoa sähköpostilla (VAHTI 3/2012).

Palomuurin säännöstö on organisaation tietoturvaperiaatteiden mukainen, ja sen toimintaa seurataan jatkuvasti esim. lokitiedostojen avulla (KATAKRI I402.0, I403.0). Esimerkkejä hyvien tietoturvaperiaatteiden mukaisista säännöistä löytyy Kansallisesta turvallisuusauditointikriteeristöstä (KATAKRI).

Verkon aktiivilaitteet on kovennettu (oletussalasanat vaihdettu; vain tarpeelliset palvelut ovat päällä; verkkolaitteiden ohjelmistojen tietoturvapäivitykset ovat ajan tasalla; hallinta mahdollista vain todentamisen kautta; laitteistot konfiguroitu valmistajien ja luotettujen tahojen ohjeiden mukaisesti; työasemat eivät voi suoraan kommunikoida keskenään kytkimien välityksellä; verkkolaitteiden lokitiedostoista pystytään näkemään hallintatoimenpiteet sekä niiden suorittajat; käyttämättömät portit on poistettu käytöstä) (KATAKRI I405.0), ja uudet järjestelmät asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus (KATAKRI I502.0). Langattomien tiedonsiirtoyhteyksien käyttö voi olla rajattua tai ne voidaan kieltää kokonaan. Jos langaton liikenne on sallittu, se salataan luotettavasti päästä-päähän (KATAKRI I406.0).

Organisaation verkossa olevista laitteista ja ohjelmistoista pidetään rekisteriä. Tuntemattomien laitteiden kytkeminen verkkoon estetään (KATAKRI I508.0). Laitteilla tarkoitetaan kaikkia päätelaitteita, kuten pöytä- ja tablettitietokoneita, kannettavia tietokoneita, älypuhelimia ja muita vastaavia laitteita. On huomattava, että BYOD-mallia (*bring your own device*) ei voi soveltaa suojausluokitellun aineiston yhteydessä (VAHTI 3/2012).

Verkkoa, järjestelmiä ja niiden käyttöä valvotaan toimintavaatimusten ja riskienarvioinnin mukaisesti; normaalit liikennemäärät ja käytössä olevat protokollat verkon eri osissa tiedetään. Resurssit on mitoitettu siten, että kriittiset tietoliikennejärjestelmät toimivat turvallisesti myös normaaliliikenteestä poikkeavilla liikennemäärillä riskienarvioinnin mukaisesti (KATAKRI I408.0).

Käyttäjät tunnistetaan ja todennetaan ennen pääsyn sallimista organisaation tietoverkkoon ja -järjestelmiin. Pääsyä valvotaan turvallisen sisäänkirjautumismenettelyn avulla, sekä käytetään tunnettua ja turvallisena pidettyä tekniikkaa. Todennus tehdään vähintään henkilökohtaista salasanaa käyttäen; ylemmillä suojaustasoilla käytetään vahvaa tunnistusta (KATAKRI I501.0). Vahvassa tunnistuksessa voidaan käyttää esimerkiksi toimikorttia, puhelimen mobiilivarmennetta tai luotettavaksi tiedettyä kansallista tunnistuspalvelua (VAHTI 3/2012, VAHTI 12/2006).

Autentikaatiodataa ei säilytetä tietojärjestelmissä selväkielisenä, vaan sen asemasta tallennetaan yksisuuntaisella tiivistefunktiolla tai vastaavalla luotettavana pidetyllä menetelmällä autentikaatiodatasta saatuja tiivisteitä (KATAKRI I521.0).

Suojattavat tiedot on tietojärjestelmissä eritelty käyttöoikeusmäärittelyillä ja järjestelmän käsittelysäännöillä (KATAKRI I506.0). Korkean suojaustason tiedot säilytetään aina luotettavasti salakirjoitettuna, ja ne pidetään erillään julkisista tiedoista. Suojattavaa tietoa sisältävät kiintolevyt ja muut tallennusmediat ovat luotettavasti suojattuja. Suojattavaa tietoa sisältävät älypuhelimet suojataan riskienarvioinnin mukaisesti; korkean suojaustason materiaalin käsittely älypuhelimilla voidaan kieltää (KATAKRI I506.0). Kaikki suojattavaa tietoa sisältävät laitteistojen osat tyhjennetään luotettavasti käytöstä poiston tai huoltoon lähetyksen yhteydessä. Kolmannen osapuolen suorittamia huoltotoimenpiteitä valvotaan (KATAKRI I507.0).

Järjestelmissä käytetään tunnettuja ja yleisesti luotettavina pidettyjä salausratkaisuja (KATAKRI I509.0). Salaiset avaimet ovat vain valtuutettujen käyttäjien ja prosessien käytössä. Salausavainten hallinnan prosessit ja käytännöt ovat dokumentoituja ja asianmukaisesti toteutettuja. Avainten on oltava kryptografisesti vahvoja, ja niitä vaihdetaan säännöllisesti (KATAKRI I510.0). Sopivan salausratkaisun valinnassa voidaan hyödyntää Viestintäviraston NSCA-FI -yksikön hyväksymien salausratkaisujen listaa.

Haittaohjelmientorjuntaohjelmistot on asennettu kaikkiin sellaisiin järjestelmiin, joiden tiedetään olevan alttiita haittaohjelmatartunnoille. Torjuntaohjelmistot ovat aina käynnissä ja niiden päivitykset pidetään ajan tasalla. Ne tuottavat toiminnastaan lokitiedostoja, joita seurataan. Järjestelmien USB-portit ja vastaavat liitynnät voidaan poistaa käytöstä, jos niiden käytölle ei ole todellista perustetta (KATAKRI I503.0).

Istunnonhallinnassa käytetään tunnettua ja luotettavana pidettyä tekniikkaa (KATAKRI I511.0). Pääteistunnot ovat aina salattuja, ja tarvittaessa vahvasti tunnistettuja. Etäkäyttöyhteyksissä ja etätyössä täytyy huomioida tietoturvatasot sekä niiden vaatimat tekniset ratkaisut (VAHTI 3/2012).

Ohjelmistoja hankitaan ja asennetaan vain luotettavista ja luvallisista lähteistä (KATAKRI I513.0). Tietoturva-asiat otetaan huomioon laitehankinnoissa (KATAKRI I514.0).

Organisaation verkot, järjestelmät ja niihin liittyvät asennukset on dokumentoitu siten, että viat ja toimintahäiriöt pystytään korjaamaan toimintavaatimusten mukaisesti. Suojattavaa tietoa käsittelevän ympäristön dokumentaatio on yhdenmukainen toteutuksen kanssa; eroavaisuuksia käsitellään tietoturvapoikkeamina (KATAKRI I702.0). Organisaatiossa on selkeät periaatteet ja toimintatavat siitä, ketkä saavat asentaa ohjelmistoja, tietoliikenneyhteyksiä ja laitteita. Periaatteiden noudattamista valvotaan. Turva-asetusten ja -ohjelmien valtuuttamaton muokkaus on estetty peruskäyttäjiltä. Suojattavan tiedon käsittelyyn käytetään vain viranomaisen hyväksymiä verkkoja ja järjestelmiä (KATAKRI I703.0). Kaikista järjestelmiin kohdistuvista toiminnoista jää automaattisesti merkintä lokitiedostoon (kuka teki mitä, aikaleima). Lokitiedostoja ei muokata niiden muodostumisen jälkeen, eikä niitä poisteta. (VAHTI 3/2012)

Viranomaisten, laite- ja ohjelmistovalmistajien sekä muiden vastaavien tahojen tietoturvatiedotteita seurataan ja tarpeelliset tietoturvapäivitykset asennetaan hallitusti. Verkon palvelut ja palvelimet sekä verkkoon kytketyt laitteet skannataan säännöllisesti haavoittuvuuksien löytämiseksi (KATAKRI I706.0).

Riittävästä varmuuskopioinnista on huolehdittu. Varmuuskopiot säilytetään eri fyysisessä sijainnissa kuin varsinainen järjestelmä. Varmuuskopioihin pääsy on estetty muilta kuin valtuutetuilta käyttäjiltä. Suojattavaa tietoa sisältävät varmuuskopiot säilytetään tiedon suojaustason edellyttämässä tilassa ja tarvittaessa salakirjoitettuna. Varmistusmedioista on olemassa rekisteri (KATAKRI I710.0). Varmuuskopioinnin piiriin sisältyvät kaikki järjestelmän osat, kuten tietoaineistot, tietokannat, autentikointitiedot ja lokitiedostot.

Tarkempia esimerkkejä laitteiden, tietoliikenteen ja palvelinten teknisistä suojausratkaisuista löytyy VAHTI 3/2012 -ohjeesta sekä Kansallisesta turvallisuusauditointikriteeristöstä (KATAKRI).

6. RISKIANALYYSI

Tietoturva on perusluonteeltaan riskien hallintaa. Täydellistä tietoturvaa on yleensä mahdotonta saavuttaa, joten jonkin suuruinen riski, niin sanottu jäännösriski, jää yleensä laajamittaistenkin tietoturvatoimenpiteiden jälkeen tietosysteemiin. Tietoturvatyön olennainen osa onkin päätöksen teko sen suhteen millainen jäännösriski on hyväksyttävissä. Tietoturvamenetelmät maksavat aina jotain joko rahassa tai työajassa, joten usein joudutaan tekemään päätöksiä sijoitettavan panoksen ja sen jälkeen jäljelle jäävän riskin suhteen.

Jotta lähtökohtaisesti saadaan jonkinlainen käsitys tietojärjestelmään liittyvistä tietoturvariskeistä, täytyy suorittaa riskianalyysi. Riskianalyysissä tarkastellaan tietosysteemiin kohdistuvia riskejä ja niiden torjumiseen tarvittavia resursseja, eli kustannuksia. Kustannusanalyysi kattaakin tarvittavien panosten arvioinnin ja yhdessä riskianalyysin kanssa antaa pohjan tehdä hankintapäätöksiä tietoturvatoimenpiteiden tuottamiseksi.

Yleinen arvio tietomurroista ja niitä vastaan suojautumisesta asettaa suojautumisen kustannukseksi noin 4% vastaavan tietomurron aiheuttamista kuluista. Näin ollen usein sijoittaminen tietoturvaan on kannattavaa, vaikka tarkka euromääräinen arvio onkin hyvin haasteellista tehdä. Lisäksi tietoturvatarpeita taloudellisten lähtökohtien ohella ohjaavat lait ja asetukset, sekä yleinen mielipide.

Riskianalyysiä suunniteltaessa lähdettiin VARANTO-järjestelmän osalta liikkeelle tietoturvan peruselementeistä, eli luottamuksellisuus (Confidentality), eheys (Integrity) ja saatavuus (Availaility). Nämä muodostavat niin sanotun CIA-triadin, joka on tietojärjestelmien tietoturvan vähimmäisvaatimus. Lisäksi yleisiä tietoturvavaatimuksia ovat kiistämättömyys (Non-repudiation), autentikointi (Authentication) ja pääsyn valvonta (Access control).

Riskianalyysiä on syytä suorittaa heti tietojärjestelmän suunnittelun alkumetreiltä, koska 50% tietoturvaongelmista tulee suunnitteluvaiheessa, jolloin niiden torjuminen järjestelmän valmistuttua on hyvin vaikeaa ja kallista (McGraw, 2006). Riskianalyysi on siten tiukasti sidottu sovelluksen/tietojärjestelmän suunnitteluun ja vaatii sovellusalueen ymmärtämistä.

Riskianalyysissä voidaan nähdä kaksi (usein toisiaan täydentävää) lajia, eli määrällinen ja laadullinen. Määrällisen analyysin koettaessa löytää euromääräisiä hintalappuja eri riskeille, laadullinen pyrkii enemmän pureutumaan riskin toteutumisen aiheuttamaan vahinkoon ja määrittelemään riskin vaikutuksen laajemmalla asteikolla. Molemmissa tapauksissa, olennaista on määritellä torjuntasuunnitelma (mitigation plan) jotta riskeihin voidaan oikeasti kohdistaa toimenpiteitä. Riskianalyysi ilman torjuntasuunnitelmaa on hyödytön.

6.1. Käsitteitä

Omaisuus (Asset) on jokin tietojärjestelmässä oleva tai järjestelmään kuuluva arvokkaaksi koettu asia. Omaisuus käsitteen alle kuuluvat sekä aineettomat että aineelliset hyödykkeet. Riskianalyysissä omaisuus on asia joka riskin toteutuessa voidaan menettää tai se voi turmeltua.

Uhka tai uhkaaja (Threat) on tapahtuma tai toimija joka voi aiheuttaa omaisuuden menetyksen tai turmeltumisen. Uhka tietojärjestelmässä voi olla esimerkiksi henkilötietojen luottamuksellisuuden menetyksen aiheuttava tietomurron suorittava hakkeri.

Todennäköisyys (Propability) riskianalyysissä (määrällisessä) tarkoittaa perinteistä matemaattista todennäköisyyttä, jolla epävarman tapahtuman tarkka kuvaaminen tapahtuu 1 ja 0 välille sijoittuvalla reaalinumerolla. Vastaavasti laadullisessa riskianalyysissä todennäköisyys (likelihood) saa huomattavasti väljemmän määritelmän, diskreetti arvo matala, keskinkertainen tai korkea. Riskianalyysin englanninkielisessä kirjallisuudessa on siis kahdenlaista todennäköisyyttä.

Vaikutus (Impact) tarkoittaa tietoturvapoikkeaman tai vahingollisen tapahtuman aiheuttamaa vahinkoa. Vaikutusta voidaan joskus mitata rahassa, esimerkiksi lisääntyneet palkkakustannukset aiheutuneiden vahinkojen korjaamisessa. Usein vaikutuksella on myös ulottuvuuksia joita on vaikea tai mahdotonta rahassa mitata, kuten maineen menetys, asiakaskunnan kaikkoaminen, luottamusongelmat jne.

Riski (Risk) on vaikutuksen ja todennäköisyyden yhdistelmänä syntyvä potentiaalinen menetys. Mitä korkeampi todennäköisyys ja vaikutus, sitä korkeampi riski. Riskin arviointi todennäköisyyden ja vaikutuksen funktiona on riskianalyysin perusta.

Haavoittuvuus (vulnerabiilty) on riskille altistava tekijä, kuten koodissa oleva ohjelmointi -tai suunnitteluvirhe, järjestelmän looginen virhe, huonosti toteutettu toiminto jne.

6.2. Määrällinen riskianalyysi

Määrällinen riskianalyysi koettaa vastata kysymykseen miten tietoturvainvestointi perustellaan? Analogia on löydettävissä vaikkapa palovakuutuksesta. Tietyn arvon omaavan rakennuksen vakuuttamisen hinta on suhteessa rakennuksen arvoon ja vakuutuksen hintaan vaikuttavat muut sellaiset tekijät jotka vaikuttavat tulipalon tapahtumisen todennäköisyyteen, kuten käyttötarkoitus, ja tulipalon tapahtuessa aiheutuviin vahinkoihin, kuten sprinklerijärjestelmä. Määrällisessä riskianalyysissä käytetään seuraavia käsitteitä (Ashbaugh, 2008):

Vuositappio-odotus VTO (ALE, Annualized Loss Expectancy) tarkoittaa kyseisen riskin toteutumisen vuositasolla aiheuttamien vahinkojen keskimääräistä rahasummaa.

Kertatappio-odotus KTO (SLE, Single Loss Expectancy) tarkoittaa riskin toteutumisen aiheuttamaan kertaluotoista rahamääräistä vahinkoa.

Vuositapahtuma-aste VTA (ALE, Annualize Rate of Occurrence) tarkoittaa keskimääräistä riskin toteutumisen tapahtumien vuosittaista määrää.

Vuositappio-odotus voidaan laskea jos kertatappio-odotus ja vuositapahtuma-aste on tiedossa seuraavalla kaavalla:

VTO = VTA * KTO

Esimerkki: Tietyn tyyppisiä luottokorttipetoksia tapahtuu vuodessa keskimäärin 40 kappaletta, yhden petoksen yhteydessä yhtiö menettää keskimäärin 137 euroa. Kannattaako yhtiön investoida ylimääräinen tietoturvajärjestelmä jonka hankintahinta on 44 000 euroa ja vuosikulu 5500 euroa? (Huomautus: täysin fiktiivinen esimerkki)

Erään pankin verkkosivuilta:
”Ota käyttöösi maksun lisävahvistus.
Maksun lisävahvistuksen avulla voit varmistaa, ettei maksua ole väärennetty tietokoneella toimivan haittaohjelman avulla. Lisävahvistus on maksuton palvelu, joka pyytää sinua silloin tällöin tarkistamaan matkapuhelimeesi lähettämästämme tekstiviestistä, ovatko maksun tiedot varmasti oikein.

Voit ottaa maksun lisävahvistuksen käyttöösi xxx.fi-palvelussa kohdassa Omat tiedot > Omat yhteystiedot > Pankkiasiat > Ota lisävahvistus käyttöösi.”

Edellisessä esimerkissä maksun lisävahvistusta ei käytetä jokaisen maksun yhteydessä, vain silloin kun maksu poikkeaa maksajan tavanomaisista maksutapahtumista.

6.3. Laadullinen riskianalyysi

Euromääräisten arvioiden tekeminen on usein hyvin vaikeaa tai jopa mahdotonta. Suurin ongelma määrällisessä riskianalyysissä on puuttuva historiatieto vuositapahtuma-asteen määrittelyssä. Samaten kertatappio-odotuksen arviointi on usein hyvin hankalaa jos vaikutus kohdistuu esimerkiksi maineeseen tai vaikkapa asiakassuhteiden menetyksiin. Laadullisessa riskianalyysissä rahallisten arvojen sijaan keskitytään riskien aiheuttamien vaikutusten laatuun

Vaikutus (Impact) laadullisessa riskianalyysissä on tavanomaista ilmaista kolmiportaisella asteikolla: Matala, Keskitaso, Korkea. Tällöin arvioidaan vaikutuksia organisaation toimintakykyyn, yksilöiden toimintakykyyn, organisaation maineeseen tai omaisuuteen (aineellinen tai aineeton). Kolmiportaisessakin asteikossa on vaikeaa joskus sijoittaa vaikutusta ja paras tapa päästä kohtuulliseen lopputulokseen on käyttää riittävän laajaa asiantuntijapohjaa (organisaation sisältä) vaikutusten kategorisoinnissa. Olennaista on löytää eri riskien vaikutusten keskinäiset voimasuhteet.

Todennäköisyys (Likelihood) ei laadullisessa riskianalyysissä tarkoita matemaattista todennäköisyyden käsitettä. Valitettavasti hyvää suomenkielistä vastinetta on vaikea löytää. Laadullisen riskianalyysin todennäköisyys vastaakin parhaiten maallikon, ei matemaatikon, käsitystä todennäköisyydestä. Laadullisessa riskianalyysissä on usein tapana käyttää samanlaista kolmiportaista jaottelua kuin vaikutuksen osaltakin. Usein tapana on tarkastella uhkaajan motiiveja ja keinoja sekä vastatoimien tehokkuutta.

Matala = Uhkaajalta puuttuu motiivi tai keinot, vastatoimet ovat tehokkaita

Keskitasoinen = Uhkaajalta puuttuu joko motiivi tai keinot, vastatoimet ovat osittain tehokkaita

Korkea = Uhkaajalla on sekä motiivi että keinot, vastatoimet ovat tehottomia

Riskiaste (Risk level) muodostuu vaikutuksen ja todennäköisyyden yhdistelmänä (Taulukko 1). Riskiastetta on myöskin tapana kuvata kolmiportaisena ja alla oleva yksinkertainen taulukko kuvaa yhden tavan tuottaa riskiaste vaikutuksen ja todennäköisyyden yhdistelmänä.

VARANNON luonne (ei kovaa liiketoimintaa) varmaan edustaa helpoiten laadullista riskianalyysiä. Näin ollen riskianalyysiä on lähdetty tekemään CIA-triadin pohjalta siten, että järjestelmän eri toimintoja on pohdittu luottamuksellisuuden, eheyden ja saatavuuden näkökulmista. Tulokset löytyvät liitteestä 1.

Todennäk \ Vaikutus	**Matala**	**Keskitaso**	**Korkea**
Matala	Matala riskitaso	Matala riskitaso	Keskinkertainen riskitaso
Keskitaso	Matala riskitaso	Keskinkertainen riskitaso	Keskinkertainen riskitaso
Korkea	Keskinkertainen riskitaso	Keskinkertainen riskitaso	Korkea riskitaso

Taulukko 1:Riskitaso muotoutuu todennäköisyyden ja vaikutuksen yhdistelmänä

6.1. Torjuntasuunnitelma

Kuten alussa todettiin, pelkkä riskianalyysi ei tuota mitään lisäarvoa, ellei sitä oteta huomioon torjuntasuunnitelmaa tehtäessä. Torjuntasuunnitelma yksinkertaisesti tarkastelee kutakin riskiä ja ottaa kantaa siihen, miten kyseinen riski voidaan poistaa tai miten sitä voidaan pienentää. Torjuntasuunnitelma myös selkeästi toteaa mitkä ovat jäännösriskit.

Torjuntasuunnitelman vastatoimien tulee olla toteuttamiskelpoiset ja kunkin vastatoimen kustannusvaikutusta tulee arvioida mahdollisimman tarkasti. Kukin vastatoimi tulee kuvata sillä tarkkuudella että kuvauksen perusteella vastatoimi voidaan toteuttaa.

Torjuntasuunnitelman tekemiseen vaikuttaa ratkaisevasti tietojärjestelmän arkkitehtuuri ja ulkoiset tekijät, kuten verkkoympäristö. VARANTO järjestelmän arkkitehtuurin ja toimintaympäristön ollessa tätä riskikartoitusta tehtäessä varsin pitkälti avoinna ja vasta suunnitteluasteella, ei merkityksellistä torjuntasuunnitelmaa ole järkevää lähteä tekemään. Tässä vaiheessa tehty torjuntasuunnitelma jäisi siinä määrin abstraktille tasolle, että selvityksen tekijät näkevät paremmaksi jättää torjuntasuunnitelman tekeminen siihen vaiheeseen kun järjestelmän arkkitehtuuri on selvillä ja torjuntatoimiin vaikuttavasta ympäristöstä on selkeä käsitys.

7. JOHTOPÄÄTÖKSET

VARANTO-järjestelmä tulee palvelemaan muitakin käyttäjiä kuin pelastustoimen operatiivista käyttäjäkuntaa. Olennaisesti on nähtävissä tarve, ainakin rajallisessa määrin, tarjota palveluita myös valtion turvallisuusviranomaisille ja samalla kansalaisille. Näin ollen käyttäjäkunta on nähtävissä hyvin heterogeeniseksi ja tietoturvamenettelyjen tulisi lähtökohtaisesti tyydyttää kaikkien näiden käyttäjäkuntien tarpeita. Näin ollen suosittelemme, että järjestelmän tietoturva-arkkitehtuurista tehdään mahdollisimman joustava ja erilaiset käyttäjät huomioiva. Tällä tarkoitamme sitä, että järjestelmään voidaan tallentaa sekä julkista että salassa pidettävää tietoa. Arkkitehtuurin tulisi olla siinä määrin avoin, että se ei rajoita eri suojaustasoille sijoitetun tiedon tallentamista ja käyttämistä. Eri asia sitten on mitä nämä suojaustasot tulevat olemaan ja mihin tietoturvavaatimuksiin niihin varautuminen johtaa.

Esittämässämme geneerisessä tietoturva-arkkitehtuurissa on modulaarinen rakenne siten, että järjestelmä voidaan rakentaa sisältämään sekä julkista että salassa pidettävää tietoa. Suojaustasomäärittelyjä ei sinällään ole pakko kuntasektorilla käyttää, mutta niiden pois jättäminen suunnittelun alkuvaiheessa olisi lyhytnäköistä. VARANTO-hankkeen ollessa määrittelynsä alkutaipaleella, on mahdoton ennustaa kuinka valtion hallinnon ja kuntasektorin tietoturvavaatimukset ja -vastuut tulevat muuttumaan siihen mennessä kun järjestelmä on hankintavaiheessa. VARANTO-järjestelmän kehittämisen ideologiaa tukee hyvin YTS:n toteamus "Hätäkeskustoiminta yhdenmukaistetaan ja tietojärjestelmät integroidaan turvallisuusviranomaisten operatiivisiin johtamisjärjestelmiin." Tämän strategisen linjauksen toteutumista ei voida vielä pitää täysin varmana, mutta se viitoittaa suunnan VARANTOa vastaavien hankkeiden tarpeellisuudelle ja hyödyllisyydelle.

Turvallisuusluokittelu koskee vain pientä osaa tiedosta ja pääsääntöisesti valtion viranomaista, mutta VARANTO-järjestelmä kannattaa rakentaa siten, että tietoon voidaan liittää suojaustasomäärittely. Olennaista rakenteen modulaarisuudessa on se, että julkiselle tiedolle, salassa pidettävälle tiedolle ja eri suojaustasoille määritellään omat pääsynhallinnan modulit. Nämä modulit huolehtivat, ettei tietoa anneta tahoille, joille se ei ole luvallista eikä tietoa saa tallentaa järjestelmään muu kuin sellainen käyttäjä jolla tiedon tallentamiseen on lupa. Tavoitteena on, että jostain tietokokonaisuudesta voidaan muodostaa useita toisistaan poikkeavia näkymiä eri pääsyoikeudet omaaville käyttäjille.

Salassa pidettävän tiedon tallentaminen luonnollisesti asettaa vaatimuksia tietojenkäsittely-ympäristölle. Lähtökohtaisesti VARANTO-järjestelmän tulee toteuttaa tietoturvallisuuden perustaso, joka mahdollistaa salassa pidettävän tiedon tallentamisen ja suojaustasoluokitellun tiedon käsittelyn suojaustasolla 4. Vaatimuksia näiden tasojen toteuttamisesta löytyy mm. ohjeista VAHTI 2/2010, Liite 5: "Tietoturvallisuustasojen yksityiskohtaiset vaatimukset" sekä VAHTI 3/2012, "Teknisen ICT-ympäristön tietoturvataso-ohje". Koska sekä ohjeet että normatiiviset dokumentit päivittyvät varsin usein ja nopealla tahdilla, on järjestelmän modulaarisuus hyvin tärkeä ominaisuus näiden vaatimusten täyttämisessä. Tätä selvitystä kirjoitettaessa on tihkunut osittaisia tietoja uudesta kansallisesta turvallisuusauditointikriteeristöstä (KATAKRI versio 3). Tällaisten normatiivisten dokumenttien päivitysten aiheuttamiin muutoksiin parhaiten varaudutaan tietojärjestelmän helpohkon päivittämisen mahdollistavalla modulaarisuudella. Myös tietoturvaan liittyvien toimijoiden vastuut ja velvollisuudet ovat jossain määrin epäselviä, mitä kuvaa osaltaan se, että mm. Kyberturvallisuusstrategiassa käytettyjä termejä: toimija ja keskeinen toimija ei ole tarkoin määritelty, jolloin näihin tekijöihin liittyvät vastuut ja velvoitteet jäävät osin kyseenalaisiksi.

VARANTO-järjestelmän tietoturva-arkkitehtuurin tarkempaa teknistä tarkastelua olemme tehneet kansainvälisen julkaisun muodossa (Hassinen, Marttila-Kontio, Päivinen 2013). Artikkelissa kuvataan tarkemmin ehdotetun arkkitehtuurin modulaarista rakennetta ja toimintatapaa. Samalla artikkeli käsittelee salassa pidettävien tietojen yhdistämisestä mahdollisesti aiheutuvien, yksittäisiä tietoja arkaluonteisempien yhdistelmien käsittelyä. Tämä vaatii oman tarkastelunsa myös tietojen suojaustasojen määrittelyn yhteydessä.

VARANTO-järjestelmää suunniteltaessa on myös syytä tarkastella järjestelmän rajauksia muunkin kuin sen toiminnallisuuden osalta. Tietoturvan osalta tällaisia rajauksia voidaan nähdä tehtävän kustannus-hyöty perusteisesti, koska tietoturvan toteuttamisella on aina hintalappu. Näin ollen näemme järkevänä rajata tietojoukkoja esimerkiksi siten, että VARANTO ei sisällä potilastietoa. Tällä tarkoitetaan henkilökohtaista terveydentilaan tai hoitoon liittyvää tietoa. VARANTO-järjestelmän osalta potilastiedon nähtävissä oleva tallennustarve on hyvin vähäinen. Samalla se kuitenkin asettaa huomattavia vaatimuksia tietoturvan suhteen, alistaa järjestelmän useille muutoin tarpeettomille normatiivisille vaatimuksille ja aiheuttaa suhteettoman suuria kustannuksia.

Pelastustoimen tietoturvaongelmat eivät ratkea tällä selvitystyöllä, vaan tietoturvatyötä on tarve jatkaa koko pelastustoimen näkökulmasta ja maanlaajuisella mandaatilla. Pelastustoimi täytyy saada tietoturvan osalta näyttäytymään yhtenä toimialana ja sille tulee laatia yhteiset ja kaikkien pelastuslaitosten hyväksymät tietoturvamenettelyt. Pelastusopiston TUPO-hanke (Pelastustoimen operatiivisten tietojärjestelmien tietoturvapolitiikka) jatkaa tätä työtä määritellen tietoturvamenettelyjä koko maan pelastustoimen käyttöön ja hyödyksi. Samalla hanke toimii pelastustoimen edunvalvojana tietoturvamäärittelyissä ja pyrkii yhteensovittamaan menettelytapoja valtiosektorin kanssa. TUPO myös tuottaa ohjeistusta pelastustoimen tietojen salassa pidettävyyden määrittelyyn sekä mahdollisten suojaustasojen määrittelyyn.

8. LÄHTEET

Arkistolaki (831/1994)

Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999)

Hassinen, Marttila-Kontio, Päivinen 2013: Proceedings of the Third International Conference on Digital Information and Communication Technology and its Applications (DICTAP 2013).

Henkilötietolaki (523/1999)

Huoltovarmuus, huoltovarmuuskeskus, www.huoltovarmuus.fi

ICT-varautumisen vaatimukset, VAHTI 2/2012

JHS, JHS-suositukset www.jhs-suositukset.fi

Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje, 30.11.2010

KATAKRI: Kansallinen turvallisuusauditointikriteeristö. Versio II, 2011. Puolustusministeriö.

Kortelainen Pekka: VARANTO tutkimussuunnitelma, 2012

Kuntien ICT-varautuminen, Valtiovarainministeriö 5/2011

Laki kansainvälisistä tietoturvallisuusvelvoitteista (588/2004)

Laki potilaan asemasta ja oikeuksista (785/1992, potilaslaki)

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä (159/2007)

Laki sähköisestä asioinnista viranomaistoiminnassa (24.1.2003/13)

Laki tietoturvallisuuden arviointilaitoksista (1405/2011)

Laki vahvasta sähköisestä tunnistamisesta ja sähköisistä allekirjoituksista (7.8.2009/617)

Laki viranomaisten tietojärjestelmien ja tietoliikennejärjestelyjen tietoturvallisuuden arvioinnista (1406/2011)

Laki viranomaisten toiminnan julkisuudesta (621/1999)

Mäenpää, Olli: Julkisuusperiaate. WSOY 2008

Mähönen, Jukka: Web-palvelujen tiedon käytön rajoitukset. Pro Gradu tutkielma, Itä-Suomen yliopisto 2013.

NCSA-FI:n hyväksymät salausratkaisut. Viestintävirasto

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. VAHTI 7/2003

Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, VAHTI 2/2010

Pelastuslaki (379/2011)

Schneier Bruce: Applied Cryptography. 1996

Security Software Development: Assessing and Managing Security Risks, Douglas A. Ashbaugh, 2008

Sisäasiainministeriön määräys salassa pidettävien tietoaineistojen luokittelusta ja käsittelystä, 2011

Software Security: Building Security In, Gary McGraw, 2006

Suomen kyberturvallisuusstrategia, Valtioneuvoston periaatepäätös 24.1.2013

Suomen perustuslaki (731/1999)

Sähköisen viestinnän tietosuojalaki (516/2004)

Teknisen ICT-ympäristön tietoturvataso-ohje. VAHTI 3/2012

Tietoteknisten laitetilojen turvallisuussuositus. VAHTI 1/2002

Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan, VAHTI 3/2007.

Tietoturvallisuusasetus (681/2010)

Tunnistaminen julkishallinnon verkkopalveluissa, VAHTI 12/2006

Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa (TiTuA 681/2010)

Viestintävirasto, Kansallinen tietoturvaviranomainen NCSA-FI

Voutilainen, Tomi: Hyvä sähköinen hallinto, Edita, Helsinki, 2006

Voutilainen, Tomi: Oikeus tietoon, 2012

YETTS, Yhteiskunnan elintärkeiden toimintojen turvaamisen strategia, Valtioneuvoston periaatepäätös, Puolustusministeriö, 23.11.2006

YTS, Yhteiskunnan turvallisuusstrategia, Valtioneuvoston periaatepäätös, Puolustusministeriö, 16.12.2010

LIITE1: VARANTO tietoturvatyöpaja - riskianalyysi

Ei oteta kantaa tietoliikenteeseen, päätelaitteeseen tai käyttöliittymään

Osa-alue	Kuvaus	Luottamuksellisuus	Eheys	Saatavuus
Palotarkastus + muu valvonta Kertomus Tuottaminen	Varantoon tallennetut palotarkastuskertomukset Palotarkastuskertomuksen tuottaminen tuottaa hallintopäätöksen.	Sisältää salassa pidettävää tietoa, henkilötietoja ja yrityssalaisuuksia Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen Oikeustoimivaikutus Julkisuuskuvavaikutus	Palotarkastuskertomuksen oikeellisuus vaikuttaa tarkastajan oikeusturvaan Riskitaso: Matala Vaikutus: Keskinkertainen Oikeustoimivaikutus	Tarkastusrekisteriä käytetään kentältä. Saatavuuden oltava hyvä. Riskitaso: Keskinkertainen Vaikutus: Matala
Palotarkastus + muu valvonta Kertomus Käyttäminen	Kohteen palotarkastustietojen käyttö muuhun kuin tarkastustoimintaan	Sisältää salassa pidettävää tietoa, henkilötietoja ja yrityssalaisuuksia Riskitaso: Keskinkertainen Vaikutus: Korkea	Palotarkastuskertomuksen oikeellisuus vaikuttaa tarkastettavan oikeusturvaan Riskitaso: Matala Vaikutus: Keskinkertainen	Tarkastustietoja käytetään mm. kohdekorteissa (oper. käyttö) Riskitaso: Keskinkertainen Vaikutus: Korkea
Omavalvonta Tietojen käyttö	Omakotitalokohteiden palotarkastusta korvaava toiminto	Sisältää asianomaisjulkisuuden piiriin kuuluvaa salassa pidettävää tietoa Riskitaso: Matala Vaikutus: Keskinkertainen	Omavalvontakertomuksen oikeellisuus vaikuttaa talon omistajan oikeusturvaan Käyttö myös operatiivisesti Riskitaso: Keskinkertainen Vaikutus: Matala	Omavalvontatietoja käytetään mm. kohdekorteissa (oper. käyttö) Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen

Omavalvonta Tuottaminen	Omakotitalokohteiden palotarkastusta korvaava toiminto	Sisältää asianomaisjulkisuuden piiriin kuuluvaa salassa pidettävää tietoa Riskitaso: Matala Vaikutus: Matala, yksittäinen kohde	Omavalvontakertomuksen oikeellisuus vaikuttaa talon omistajan oikeusturvaan Riskitaso: Matala Vaikutus: Matala	Järjestelmältä odotetaan kohtuullista uptime suorituskykyä Riskitaso: Matala Vaikutus: Matala
Pelastussuunnitelman tekolomake	Pelastussuunnitelman tekemistä tukeva järjestelmä	Sisältää asianomaisjulkisuuden piiriin kuuluvaa salassa pidettävää tietoa yksittäisestä kohteesta Riskitaso: Matala Vaikutus: Keskinkertainen	Tietojen oikeellisuuden vaatimus korkea. Riskitaso: Keskinkertainen Vaikutus: Korkea	Järjestelmältä odotetaan kohtuullista uptime suorituskykyä Riskitaso: Matala Vaikutus: Matala
Kiinteistötiedot Rakennustiedot	Pohjatiedot järjestelmään saadaan VRK:sta.	Ei ole kaikilta osin julkista, sisältää salassa pidettävää tietoa Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen	Toimenpiteen kohdistuminen väärään kiinteistöön/ rakennukseen Riskitaso: Matala Vaikutus: Keskinkertainen	Päivitykset eräajona (?) Riskitaso: Matala Vaikutus: Matala
Ajoneuvojen tiedot	Taustatiedot erilaisista ajoneuvoista, tekniset tiedot. Mistä nämä tiedot saadaan?	Julkista tietoa, vaikuttaa mahdollisesti muuhun päätöksen tekoon Riskitaso: Matala Vaikutus: Matala	Tietojen oikeellisuudella voi olla jotain merkitystä mutta ei operatiivisessa käytössä Riskitaso: Matala Vaikutus: Matala	Aiheuttaako saatavuus jonkin toisen sovelluksen käytön vaikeutumisen? Riskitaso: Matala Vaikutus: Keskinkertainen
Kohdekortti Tuottaminen	Olennaiset tiedot onnettomuuden kohteena olevasta rakennuksesta tai kiinteistöstä	Kohdekortissa voi olla luottamuksellista henkilö- tai liikesalaisuustietoa Riskitaso: Keskitaso Vaikutus: Matala, jos yksittäisestä kohteesta kyse	Kohdekortin tietojen oikeellisuus on hyvin tärkeää päätöksen teossa Riskitaso: Matala Vaikutus: Korkea	Kohdekortin saatavuus tärkeää, mutta ei kriittistä Riskitaso: Matala Vaikutus: Keskinkertainen
Kohdekortti Kohteen tuottamat tiedot	Kohteen pelastuslaitokselle pelastustoimintaa varten tuottamat tiedot	Luottamuksellisen tiedon osuus kohtuullisen pieni Riskitaso: Keskinkertainen Vaikutus: Matala	Olemassa olevan tiedon tulee olla oikeaa ja ajantasaista. Riskitaso: Matala oikeellisuuden osalta, Korkea ajantasaisuuden	Järjestelmältä odotetaan kohtuullista uptime suorituskykyä Riskitaso: Matala

			osalta Vaikutus: Korkea	Vaikutus: Keskinkertainen
Kohdekortti Käyttö + muu pelastustehtävän aikainen "rekisterikysely"	Pelastustoiminnan aikana VARANTOsta saatavat tiedot	Kohdekortissa voi olla luottamuksellista henkilö- tai liikesalaisuustietoa Riskitaso: Keskitaso Vaikutus: Matala, yleensä yksittäisestä kohteesta kyse	Eheysongelman saattaa aiheuttaa virheitä pelastustoiminnan päätöksenteossa. Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen	Pelastustehtävän aikainen saatavuus kriittinen Riskitaso: Korkea Vaikutus: Keskinkertainen. Haittaa tehokasta pelastustoimintaa
Vastemäärittely	Vasteen suunnittelu ja tietojen tallentaminen ja muuttaminen	Periaatteessa julkista dataa. Riskitaso: Matala Vaikutus: Matala Terrorismi tms?	Vastetason määrittelyssä syntyvä virhe, esim. hlömäärä Riskitaso: Matala Vaikutus: Keskinkertainen. Hälytetään virheellinen vaste	Järjestelmältä odotetaan kohtuullista uptime suorituskykyä Riskitaso: Matala Vaikutus: Keskinkertainen
Nuohousrekisteri	Nuohottujen kohteiden nuohoustietojen tallentaminen, tarvittaessa palotarkastuspyyntö	Periaatteessa julkista dataa. Riskitaso: Matala Vaikutus: Matala	Voi vaikuttaa asianosaisten vakuutusturvaan (lakisääteinen nuohous) Riskitaso: Matala Vaikutus: Korkea	Järjestelmältä odotetaan kohtuullista uptime suorituskykyä Riskitaso: Matala Vaikutus: Keskinkertainen
Väestönsuojien tarkastusrekisteri	Tarkastettujen väestönsuojien tietojen tallentamien	Periaatteessa julkista dataa. Voidaanko katsoa olevan JulkL 24§, kohta 7 tietoa? Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen	Onko juridisia vaikutteita asianosaisiin? Riskitaso: Matala Vaikutus: Matala	Järjestelmältä odotetaan kohtuullista uptime suorituskykyä Riskitaso: Matala Vaikutus: Keskinkertainen
Onnettomuustietojen sähköinen vastaanotto	KEJOsta ja ERICAsta saatavilla olevat onnettomuuteen liittyvät tiedot	Sisältää salassa pidettävää tietoa, mm. osoitteita, valokuvia Riskitaso: Korkea Vaikutus: Keskinkertainen. Oikeustoimivaikutus, Julkisuuskuva	Tiedon eheys merkityksellistä mm. tutkinnan vuoksi Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen	Voidaanko tuoda eräajona? Tarvittaessa käsin syöttö Riskitaso: Matala Vaikutus: Keskinkertainen
Pelastus- ja avunantotehtävien tietojen kirjaus	Pelastushenkilö kirjaa selosteen tapahtuneesta onnettomuudesta	Salassa pidettävää tietoa, Julkl 24§ Kiinnostaa helposti ulkopuolisia Riskitaso: Korkea Vaikutus: Keskinkertainen	Selosteen sisällön vaikutus mm. asianosaisten vakuutus- ja oikeusturvaan Riskitaso: Matala	Järjestelmältä odotetaan kohtuullista uptime suorituskykyä Riskitaso: Matala

			Vaikutus: Keskinkertainen	Vaikutus: Keskinkertainen
Palontutkinnan (taso 2 ja 3) suorittaminen ja tietojen kirjaus	Erikoiskoulutuksen saanut pelastushenkilö kirjaa tekemänsä tutkimuksen tulokset	Salassa pidettävää tietoa, Julkl 24§ Kiinnostaa helposti ulkopuolisia Riskitaso: Korkea Vaikutus: Keskinkertainen	Selosteen sisällön vaikutus mm. asianosaisten vakuutus- ja oikeusturvaan Riskitaso: Matala Vaikutus: Keskinkertainen	Järjestelmältä odotetaan kohtuullista uptime suorituskykyä Riskitaso: Matala Vaikutus: Keskinkertainen
Pelastus- ja avunantotehtävät Tietojen käyttö	Yksittäisen tapauksen tapahtumien ja toimenpiteiden dokumentoinnin katselemien (esim. oikeuteen)	Voi sisältää salassa pidettävää tietoa Riskitaso: Matala Vaikutus: Keskinkertainen	Vaikuttaa asianosaisten oikeus- ja vakuutusturvaan Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen	Järjestelmältä odotetaan kohtuullista uptime suorituskykyä Riskitaso: Matala Vaikutus: Matala
Turvallisuusviestintä Tietojen kirjaus	Yksittäisen tilaisuuden dokumentointi	Julkista dataa. Riskitaso: Matala Vaikutus: Matala	Periaatteessa julkista dataa, virheet saattavat vääristää tilastointia Riskitaso: Matala Vaikutus: Keskinkertainen	Järjestelmältä odotetaan kohtuullista uptime suorituskykyä Riskitaso: Matala Vaikutus: Keskinkertainen
Turvallisuusviestintä Tietojen käyttö	Yksittäisen tilaisuuden dokumentoinnin katseleminen	Julkista dataa. Riskitaso: Matala Vaikutus: Matala	Periaatteessa julkista dataa, virheet saattavat vääristää tilastointia Riskitaso: Matala Vaikutus: Keskinkertainen	Järjestelmältä odotetaan kohtuullista uptime suorituskykyä Riskitaso: Matala Vaikutus: Matala
Henkilöstötiedot (pel. laitos)	Osaaminen Koulutus Kokemus Suoritetut tehtävät työvuorosuunnittelu? harjoitusrekisteri?	Sisältää henkilötietoja (myös salassa pidettäviä), ei muodosta henkilörekisteriä (palvelussuhteeseen liittyvät tiedot) Riskitaso: Keskinkertainen Vaikutus: Oikeustoimi	Vaikutus mm. kelpoisuuksiin ja siten vaikutta oikeusturvaan ja vakuutusturvaan Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen	Olennainen toiminto, vaikuttaa mm. henkilöstön käytettävyyteen pelastus-toiminnassa Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen

	Vapautukset sodan ajan palveluksesta (VAP)			
Ajoneuvotiedot (pel. laitos)	Pelastuslaitoksen omien ajoneuvojen tiedot	Julkista tietoa Riskitaso: Matala Vaikutus: Matala	Julkista tietoa, oikeellisuus ja ajantasaisuus Riskitaso: Keskinkertainen (ajantaisaisuus) Vaikutus: Matala	Tarvitaan vastemäärittelyssä Riskitaso: Matala Vaikutus: Matala
Kalustotiedot (pel. laitos)	Pelastuslaitoksen kalusto, kuten työkalut, letkut, paineilmalaitteet jne.	Julkista tietoa Riskitaso: Matala Vaikutus: -	Julkista tietoa, oikeellisuus ja ajantasaisuus Riskitaso: Keskinkertainen (ajantaisaisuus) Vaikutus: Matala	Tarvitaan vastemäärittelyssä Riskitaso: Matala Vaikutus: Matala
Henkilövaraukset	Varautumisen henkilövaraukset Muut henkilövaraukset	Muodostaa henkilörekisterin (salassa pidettävää tietoa) Riskitaso: Korkea Vaikutus: Keskinkertainen, Oikeustoimi	Oikeellisuus ja ajantasaisuus. Tietojen oikeellisuus tärkeää toiminnan kannalta Riskitaso: Matala (Korkea, ajantasaisuus) Vaikutus: Keskinkertainen	Tarvitaan vastemäärittelyssä Riskitaso: Matala Vaikutus: Matala (syötettäessä tietoja) Keskinkertainen (haettaessa tietoja)
Tilavaraukset	Varautumisen tilavaraukset (johtopaikat, evakuointipaikat)	Varautumisen tiedot ovat salassa pidettäviä (JulkL 24 §) Riskitaso: Korkea Vaikutus: Varautumisen toiminnan vaarantuminen	Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen, Erheellinen kuva varautumisen tasosta	Poikkeustilassa kriittisen tärkeä Riskitaso: Matala Vaikutus: Matala (syötettäessä tietoja) Keskinkertainen (haettaessa tietoja)
Kalustovaraukset	Varautumisen kalustovaraukset (kuljetuskalusto, kaivinkoneet…)	Mahdollisesti salassa pidettävää (henkilön varallisuus) Riskitaso: Keskinkertainen Vaikutus: Julkisuusvaikutus	Eheyttä suurempi riski tietojen vanhentuminen ? Riskitaso: Matala, Korkea (ajantasaisuus) Vaikutus: Matala	Pelastustoiminnassa tiedot olisi oltava käytössä Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen Pelastustoiminnan vaikeutuminen

Toiminnan suunnittelu (palvelutaso)	Pelastuslaitoksen toiminnan suunnittelu, esim. riskialueet, saavutettavuustiedot.	Julkista tietoa (?) Riskitaso: Matala Vaikutus: Matala	Virheet esimerkiksi numeerisessa datassa saattavat aiheuttaa virheitä vastemäärittelyssä Riskitaso: Matala Vaikutus: Matala	Hallinnollinen käyttö, ei kriittinen saatavuudeltaan Riskitaso: Matala Vaikutus: Matala (syötettäessä tietoja) Keskinkertainen (haettaessa tietoja)
Tilastot	Vakiomuotoiset ja määritellyt tilastotiedot	Julkisia Riskitaso: Matala Vaikutus: Matala	Tilastodatan luotettavuus ja oikeellisuus Riskitaso: Keskinkertainen Vaikutus: Matala, Virheellinen tieto	Julkaistaan tarvittaessa Riskitaso: Matala Vaikutus: Matala
Tutkimus	Tietovarannon tai sen rajatun osan tiedot	Myös salassa pidettävää tietoa. Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen. Oikeustoimi Julkisuuskuva	Riskitaso: Vaikutus:	Järjestelmältä odotetaan kohtuullista uptime suorituskykyä Riskitaso: Matala Vaikutus: Matala
Seuranta	Pelastuslaitosten toiminnan arviointi	Julkista tietoa Riskitaso: Matala Vaikutus: Matala	Tiedon oikeellisuus Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen, Virheellinen tieto	Järjestelmältä odotetaan kohtuullista uptime suorituskykyä Riskitaso: Matala Vaikutus: Matala
Palaute	Pelastuslaitoksen kaikesta toiminnasta kerättävä palaute	Julkista tietoa Riskitaso: Matala Vaikutus: Keskinkertainen	Tiedon oikeellisuus Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen, Virheellinen tieto	Huono saatavuus romahduttaa saadun palautteen määrän Riskitaso: Matala Vaikutus: Keskinkertainen (syötettäessä tietoja) Keskinkertainen (haettaessa

Käyttäjähallinta	VARANTO käyttäjähallinta (roolit, oikeudet)	Käyttäjien roolit ja oikeudet ovat ei julkista tietoa Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen	Käyttäjähallintatiedon oikeellisuus on koko käyttäjähallinnan turvallisuuden kulmakivi Riskitaso: Korkea Vaikutus: Korkea	Käyttäjätietoja tarvitaan jotta järjestelmää voidaan käyttää ylipäänsä Riskitaso: Keskinkertainen Vaikutus: Korkea, käyttämisen estyminen
Arkaluonteiset henkilötiedot	Henkilötietolaissa mainitut arkaluonteiset henkilötiedot	Varantoon ei tallenneta arkaluonteisia henkilötietoja Riskitaso: Matala Vaikutus: Korkea , Oikeustoimivaíkutus	Varantoon ei tallenneta arkaluonteisia henkilötietoja Riskitaso: Matala Vaikutus: Korkea, Oikeustoimivaíkutus	Varantoon ei tallenneta arkaluonteisia henkilötietoja Riskitaso: Matala Vaikutus: Matala
Ajoneuvot	Tiedot onnettomuuden kohteeksi joutuneesta ajoneuvosta	Salassa pidettävää tietoa Riskitaso: Keskinkertainen Vaikutus: Keskinkertainen, asianosaisten luottamuksellisen tiedon paljastuminen	Asianosaisten oikeus- ja vakuutusturvaan vaikuttavaa tietoa Riskitaso: Matala Vaikutus: Keskinkertainen	Hallinnollinen käyttö, ei kriittinen saatavuudeltaan Riskitaso: Matala Vaikutus: Matala (syötettäessä tietoja) Keskinkertainen (haettaessa)