**Milla Kinnunen**

# KINNULAN KUNNAN PERUSTURVATOIMIALAN TIETOTURVASUUNNITELMA

**Opinnäytetyö**
**CENTRIA-AMMATTIKORKEAKOULU**
**Tekniikan ylempi ammattikorkeakoulututkinto**
**Teknologiaosaamisen johtaminen -koulutusohjelma**
**Kesäkuu 2014**

**TIIVISTELMÄ OPINNÄYTETYÖSTÄ**

| **Yksikkö**<br>Centria ammattikorkeakoulu | **Aika**<br>Kesäkuu 2014 | **Tekijä**<br>Milla Kinnunen |
|---|---|---|
| **Koulutusohjelma**<br>Teknologiaosaamisen johtaminen | | |
| **Työn nimi**<br>Kinnulan kunnan perusturvatoimialan tietoturvasuunnitelma | | |
| **Työn ohjaajat**<br>KTT Pekka Nokso-Koivisto, TkL Eero Pikkarainen | | **Sivumäärä**<br>48 |
| **Työelämäohjaaja**<br>YTM Kirsi Alonen-Kinnunen | | |


Tämän opinnäytetyön tarkoituksena oli kartoittaa Kinnulan kunnan perusturvatoimialan tietoturvariskejä sekä laatia toimialalle tietoturvasuunnitelma.

Tutkimuksessa haastateltiin kunnan sosiaalijohtajaa, ylilääkäriä, johtavaa hoitajaa, tietosuojavastaavaa, kunnanrakennusmestaria sekä IT-palveluntuottajaa. Haastatteluiden perusteella tehtiin riskianalyysi, joka toimi lähtökohtana perusturvatoimialan tietoturvasuunnitelmalle.

Riskikartoituksessa havaittiin pääasiassa vähäisiä tai kohtalaisia riskejä. Havaitut riskit kehittämisehdotuksineen eriteltiin ja analysoitiin osa-alueittain tietoturvasuunnitelmaa mukaillen.

Tietoturvasuunnitelmassa määriteltiin perusturvatoimialan hallinnolliseen tietoturvallisuuteen, fyysiseen tietoturvallisuuteen, henkilöstöturvallisuuteen, laitteistoturvallisuuteen ja tietoliikenneturvallisuuteen liittyvät tietoturvakäytännöt. Tietoturvasuunnitelma minimoi tietoturvariskejä ja estää vakavien ongelmien syntymistä. Suunnitelma sisältää ne vastuualueet, joista kukin viranhaltija huolehtii ja antaa menettelyohjeita ongelmatilainteisiin. Tietoturvasuunnitelma toimii apuvälineenä johtavien viranhaltijoiden työssä.



**Asiasanat**
Riskienhallinta, tietoturva, tietoturvasuunnitelma

**ABSTRACT**

| CENTRIA UNIVERSITY OF APPLIED SCIENCES | Date<br>June 2014 | Author<br>Milla Kinnunen |
|---|---|---|
| **Degree programme**<br>Master`s Degree for Technology Competence Management | | |
| **Name of thesis**<br>INFORMATION SECURITY PLAN FOR THE DEPARTMENT OF HEALTH AND SOCIAL SERVICES OF KINNULA MUNICIPALITY | | |
| **Instructors**<br>Pekka Nokso-Koivisto, Eero Pikkarainen | | **Pages**<br>48 |
| **Supervisor**<br>Kirsi Alonen-Kinnunen | | |


The goal of the study was to discover the information security risks and to create an information security plan for the Department of Health and Social Services of Kinnula municipality.

The study was made by interviewing the director of social services, medical director, director of nursing services, data protection officer, director of technical services and the information technology service provider. The information security risks discovered as the result of the interviews were the basis of the information security plan.

The information security risks were estimated mainly low or medium. To improve information security, suggested actions were written for minimizing or removing every information security risk discovered.

The practices of administrative information security, physical security, personnel security, equipment security and data-communications security were defined for the information security plan. The goal of information security plan is to minimize the information security risks and to prevent serious security incidents. The information security plan includes the responsibilities of every officials. It is also a guide which helps the leading officials in their work.



**Key words**
Information security, Information security plan, Risk management

TIIVISTELMÄ
ABSTRACT

SISÄLLYS

1 JOHDANTO 1

2 TIETOTURVASUUNNITELMA 2
2.1 Hallinnollinen tietoturvallisuus 3
2.1.1 Riskienhallinta johtamisen tukena 3
2.1.2 Tietoturvariskien hallinta 5
2.2 Henkilöstöturvallisuus 9
2.3 Fyysinen turvallisuus 10
2.3.1 Kulunhallinta 11
2.3.2 Palo-, vesi-, ja pölyvahinkojen torjunta 12
2.3.3 Muut kiinteistötekniset suojauskeinot 13
2.4 Laitteistoturvallisuus 14
2.5 Ohjelmistoturvallisuus 15
2.6 Tietoliikenneturvallisuus 16
2.6.1 Rakenteellinen tietoturva 17
2.6.2 Valvonta ja dokumentointi 18
2.6.3 Suojaus 19
2.7 Tietoaineistoturvallisuus 20
2.7.1 Käyttöoikeudet 20
2.7.2 Salassapitosopimukset 21
2.7.3 Tietoaineiston käsittely ja säilyttäminen 21
2.7.4 Tietoaineiston hävittäminen 22
2.8 Käyttöturvallisuus 23
2.8.1 Käyttäjätunnukset ja salasanat 23
2.8.2 Viestinnän turvallisuus 24

3 TUTKIMUKSEN TEKEMINEN JA TULOKSET 25
3.1 Hallinnollinen tietoturvallisuus 25
3.1.1 Tehtävät ja vastuut 26
3.1.2 Riskien tunnistaminen ja raportointi 27
3.1.3 Kehittäminen, päivitys ja seuranta 29
3.2 Henkilöstöturvallisuus 30
3.2.1 Rekrytointi 30
3.2.2 Työnkuva 30
3.2.3 Sijaisjärjestelyt 30
3.2.4 Tiedonsaanti- ja käyttöoikeudet 31
3.2.5 Salasanat 31
3.2.6 Tietoturvakoulutus 31
3.2.7 Väärinkäytökset 32
3.3 Fyysinen turvallisuus 32
3.3.1 Kiinteistön turvallisuus 32
3.3.2 Toimistotilat 33
3.3.3 Arkistotilat 33

**3.3.4 Asiakastilat** **33**
**3.3.5 Varavoimajärjestelmät** **33**
**3.4 Tietoliikenneturvallisuus ja laitteistoturvallisuus** **34**
**3.4.1 Verkon valvonta ja hallinta** **34**
**3.4.2 Suojaus** **34**
**3.4.3 Etätyö** **35**
**3.4.5 Dokumentaatio ja ohjeistus** **35**
**3.4.6 Laitteiston käyttö, huolto ja rikkoutuminen** **35**
**3.5 Tietoaineistoturvallisuus** **36**
**3.5.1 Tietojen luokitus** **36**
**3.5.2 Tarpeettoman tietoaineiston hävittäminen** **38**
**3.5.3 Tietovälineiden käsittely ja käytöstä poisto** **38**
**3.5.4 Tietoaineiston säilytys ja arkistointi** **39**
**3.6 Liittyvät dokumentit ja niiden sijainti** **39**
**3.7 Yhteenveto tutkimustuloksista** **39**
**3.7.1 Hallinnolliseen tietoturvallisuuteen liittyvät riskit** **40**
**3.7.2 Henkilöstöturvallisuuteen liittyvät riskit** **41**
**3.7.3 Fyysiseen turvallisuuteen liittyvät riskit** **42**
**3.7.4 Laitteistoturvallisuuteen liittyvät riskit** **43**
**3.7.5 Tietoaineistoturvallisuuteen liittyvät riskit** **45**

**4 JOHTOPÄÄTÖKSET** **47**

**LÄHTEET** **49**

**KUVIOT**

KUVIO 1. Teoreettinen viitekehys **2**

**TAULUKOT**

TAULUKKO 1. Uhkan todennäköisyys **6**
TAULUKKO 2. Uhkan vakavuus **7**
TAULUKKO 3. Riskien arviointi **8, 29**
TAULUKKO 4. Hallinnolliseen tietoturvallisuuteen liittyvät riskit **40**
TAULUKKO 5. Henkilöstöturvallisuuteen liittyvät riskit **41**
TAULUKKO 6. Fyysiseen turvallisuuteen liittyvät riskit **43**
TAULUKKO 7. Laitteistoturvallisuuteen liittyvät riskit **44**
TAULUKKO 8. Tietoaineistoturvallisuuteen liittyvät riskit **46**

# 1 JOHDANTO

Tämän opinnäytetyön lähtökohtana on Kinnulan kunnan perusturvatoimialan tietoturvakäytäntöjen puutteellinen dokumentointi. Tutkimuksen pääongelma on, että tietoturvariskejä ei ole perusturvatoimialalla kartoitettu lainkaan, eikä tietoturvasuunnitelmaa ole riittävässä laajuudessa laadittu. Tämän opinnäytetyön tarkoituksena on kartoittaa Kinnulan kunnan perusturvatoimialan tietoturvariskejä sekä laatia toimialalle tietoturvasuunnitelma.

Tutkimuksessa syvähaastatellaan kunnan sosiaalijohtajaa, ylilääkäriä, johtavaa hoitajaa, tietosuojavastaavaa, kunnanrakennusmestaria sekä IT-palveluntuottajaa. Haastatteluiden perusteella tehdään riskianalyysi, joka toimii lähtökohtana perusturvatoimialan tietoturvasuunnitelmalle.

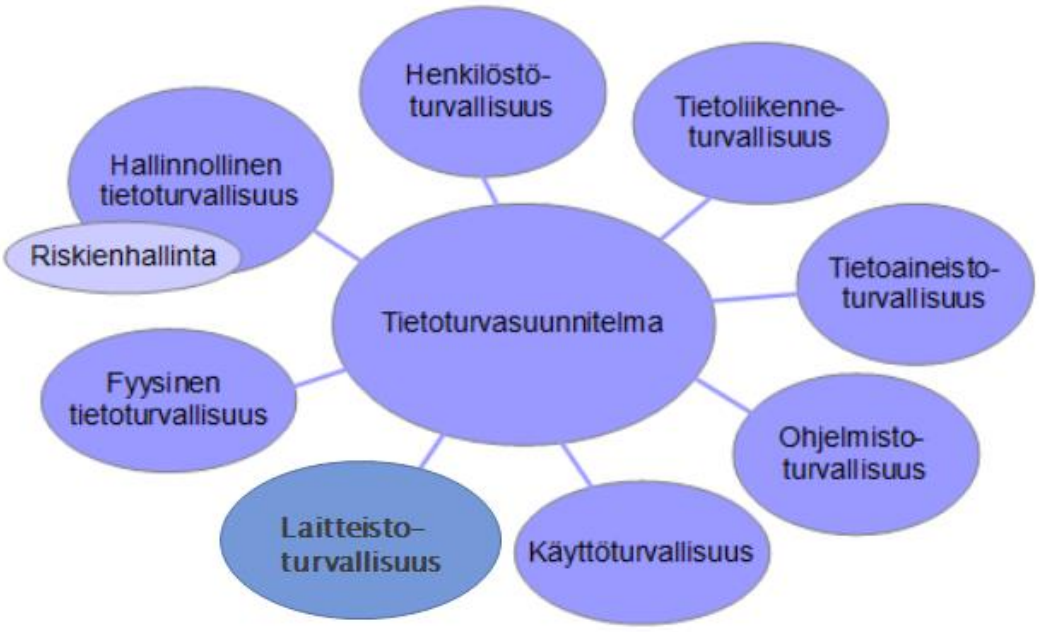
Tämän työn seuraavassa luvussa esitellään yleisesti tietoturvasuunnitelman osa-alueet sekä työn teoreettinen viitekehys. Teoriaosuudessa on esitelty kahdeksan tietoturvallisuuden luokkaa: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, käyttöturvallisuus, ohjelmistoturvallisuus ja tietoaineistoturvallisuus.

Luvussa kolme esitellään työn tuloksena Kinnulan kunnan perusturvatoimialan tietoturvasuunnitelma, jossa määritellään hallinnolliseen tietoturvallisuuteen, fyysiseen tietoturvallisuuteen, henkilöstöturvallisuuteen, laitteistoturvallisuuteen ja tietoliikenneturvallisuuteen liittyvät tietoturvakäytännöt. Tietoturvasuunnitelman tarkoituksena on jatkossa minimoida tietoturvariskejä ja estää vakavien ongelmien syntymistä. Suunnitelma sisältää ne vastuualueet, joista kukin viranhaltija huolehtii ja antaa menettelyohjeita ongelmatilainteisiin. Tietoturvasuunnitelman tarkoituksena on toimia apuvälineenä johtavien viranhaltijoiden työssä. Tuloksissa on esitelty myös ne riskit, joita haastatteluissa tuli ilmi. Riskit on jaoteltu osa-alueittain hallinnolliseen tietoturvallisuuteen, henkilöstöturvallisuuteen, fyysiseen turvallisuuteen, laitteistoturvallisuuteen ja tietoaineistoturvallisuuteen liittyviin riskeihin.

## 2 TIETOTURVASUUNNITELMA

Valtioneuvosto on tehnyt periaatepäätöksen (7/2009, 1. luku 4. mom) tietoturvallisuudesta: ”Jokaisen viranomaisen tulee huolehtia siitä, että riittävän hyvä tietoturvallisuus ja henkilötietojen suoja toteutuvat omassa organisaatiossa ja yhteistyössä sidosryhmiensä kanssa sekä hankittaessa palveluita organisaation ulkopuolelta. Kansalaisille ja yhteisöille tarjottavien hallinnon palveluiden ja muun julkisen vallan käytön tulee tapahtua niin, että voidaan turvata riittävällä tavalla käytössä olevien tietojen, tuotettujen palveluiden ja järjestelmien tietoturvallisuus.” (Valtiovarainministeriö 2009e, 8)

Tietoturvasuunnitelma koostuu kahdeksasta tietoturvallisuuden luokasta: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, käyttöturvallisuus, ohjelmistoturvallisuus ja tietoaineistoturvallisuus. Joissakin kirjallisuudessa käyttöturvallisuuteen liittyvät asiat – kuten esimerkiksi salasanakäytännöt - on sisällytetty muihin osa-alueisiin, eikä käyttöturvallisuutta ole esitetty omana alakohtanaan. Tässä opinnäytetyössä käyttöturvallisuus esitellään kuitenkin lyhyesti omana osa-alueenaan.




KUVIO 1. Teoreettinen viitekehys. (mukaillen Paavilaista 1998, 108)

## 2.1 Hallinnollinen tietoturvallisuus

Hallinnollinen tietoturvallisuus on tietoturvatoiminnan lähtökohta. Se koostuu toimenpiteistä, joissa päätetään tietoturvatoiminnan suuntaviivat ja turvallisuutta parantavat toimenpiteet. Hallinnollisen tietoturvallisuuden tarkoituksena on luoda organisaatioon toimintatapa, jossa pystytään välttämään ja estämään tietoturvaan liittyvät riskit. (Paavilainen 1998, 48-49)

Tietoturvan kohottaminen aloitetaan yleensä kartoittamalla tietoriskit. Tietoriski on tilanne, jolloin tieto tai tietojärjestelmä ei ole käytettävissä, tieto on muuttunut jonkin tapahtuman kautta tai päätynyt ulkopuolisten haltuun. Tietoriskit ovat vahinkoriskejä, joiden toteutumiseen liittyy aina menetyksiä, niin taloudellisia kuin imagoon liittyviä. Kartoituksen avulla olemassa olevat uhat saadaan paikallistettua mahdollisimman hyvin. Riskianalyysin perusteella luodaan tarvittava ohjeistus ja toimintaohjeet. (Paavilainen 1998, 48-49; Valtiovarainministeriö 2003, 5)

### 2.1.1 Riskienhallinta johtamisen tukena

Riskienhallinta on jatkuva prosessi, jolla organisaatio ja sen johto pyrkivät tunnistamaan ja hallitsemaan riskejä ennakoivasti. Riski on epävarmuus tulevasta tapahtumasta, jolla voi olla vaikutusta organisaation tai sen osan tavoitteiden saavuttamiseen. Ennakointi tarkoittaa siis sitä, että tunnistamalla riski etukäteen sen tapahtumisen todennäköisyyttä voidaan pienentää tai sen vaikutuksia voidaan lieventää. Riskienhallinnan tulee nykyaikaisen ajattelutavan mukaan kattaa organisaation kaikki keskeiset prosessit ja tasot, eikä identifioitua yksittäisen henkilön toimintaan ja tehtäviin. On myös olennaista, että koko organisaatiolla on yhtenäinen näkemys tunnistettujen riskien kokonaisuudesta. (Grönfors-Kallio & Suomela 2014)

Hyvä johtaminen vaikuttaa selvästi organisaation riskienhallintakykyyn. Hyvässä johtamisessa asioita käsitellään avoimesti; puutteista tai ongelmista keskustellaan rakentavasti. Vahinkoriskien hallintaan voidaan käyttää monia erilaisia keinoja: asiantuntijaryhmiä, riskikartoituksia ja tarkistuslistoja. Riskienhallintaa ei voi kuitenkaan tehdä kukaan toisen puolesta. Organisaation on hyvä ottaa informaatio vastaan asiantuntijoilta, mutta sen jälkeen on itse alettava johtaa omaa riskienhallintaa ja turvallisuutta. Esimiehet ja henkilöstö ovat avainasemassa, kun riskienhallinnasta pitää saada osa arjen tekemistä. (Nyrhinen 2013)

Riskienhallinta on johtamisen tukiprosessi. Se kannattaa liittää esimerkiksi yrityksen strategia- ja muihin vuosittain tehtäviin suunnitteluprosesseihin, jotta se ei jäisi irralliseksi organisaation muusta toiminnasta. Riskienhallintaa suunnitellessa kannattaa kysyä, mitä riskienhallinnan pitäisi tuottaa organisaatiolle? Riskienhallinnan suunnittelu ei ole paikallaan pysyvä olotila, ja sitä tulee kehittää jatkuvasti. (Pisto 2010)

Riskienhallinnan johtamisen pitää perustua ylimmän johdon riskienhallinnalle asettamiin tavoitteisiin. On tärkeää määritellä keskeiset käsitteet sekä riskienhallintaan liittyvät roolit ja vastuut. Myös riskienhallinnan prosessien kuvaukset olisi hyvä kirjoittaa organisaation riskienhallintapolitiikkaan. (Pisto 2010)

Koska riskienhallinta on osa johtamista, riskienhallinnan kokonaisuutta ei voi ulkoistaa. Riskien hallitsemisella ja sillä, kuka riskit ”omistaa”, on suora yhteys yrityksen johtamisen vastuuseen. Riskienhallinta on jokaisen johtajan työnkuvaan kuuluvaa vastuuta. Se ei kuitenkaan tarkoita sitä, ettei ulkopuolista apua voi käyttää taikka ettei osia riskienhallinnasta voisi ulkoistaa. Organisaation on kuitenkin säilytettävä koko ajan kyky ymmärtää asioidensa tila. (Pisto 2010)

### 2.1.2 Tietoturvariskien hallinta

Tietoturvariskien hallinta on suojautumista tietoriskeiltä. Riskienhallinnan päätehtävänä on suojaustoimenpiteiden käytännön toteutus ja suojaustason päivittäinen seuranta. Riskienhallinta on osa johtamista. (Paavilainen 1998, 51)

Riskienhallinnan toimenpiteet voidaan Paavilaisen (1998, 52) mukaan luokitella kolmeen vaiheeseen:

1) ennakointi, johon kuuluu riskien välttäminen ja niiden syntymisen estäminen
2) tapahtumien seuraaminen eli turvallisuusjärjestelyiden ja niiden antavan suojan riittävyyden tarkkailu ja seuranta
3) vahingon jälkeiset toimenpiteet, joilla pyritään minimoimaan vahingot ja estämään uusien vahinkojen syntyminen.

Riskienhallinnan ensimmäinen vaihe on uhkien tunnistaminen. Kun uhkat on tunnistettu ja niiden toteutumisen todennäköisyys ja seurausten vakavuus arvioitu, voidaan suunnitella ja päättää toimenpiteistä riskien hallitsemiseksi. Riskejä voidaan hallita monin keinoin. Keskeiset toimintavaihtoehdot Paavilaisen (1998, 52) mukaan ovat:

- Riskin välttäminen. Tämä on usein mahdollista vain, jos ko. toiminnasta pidättäydytään kokonaan.
- Riskin poistaminen. Yksittäinen riski voidaan mahdollisesti poistaa kokonaan. Poistaminen saattaa kuitenkin aiheuttaa uusia riskejä.
- Riskin pienentäminen. Ensisijaisesti on pyrittävä estämään vahinkojen syntyminen tai vähentämään niiden seurauksia. Riskin seurausten pienentämiseksi voidaan erilaisilla kontrolleilla pyrkiä vähentämään seurausten vakavuutta tai tapahtuman todennäköisyyttä.
- Riskin siirtäminen esimerkiksi sopimuksin tai vakuuttamalla.
- Riskin pitäminen omalla vastuulla. Osa riskeistä joudutaan tai kannattaa pitää omalla vastuulla. Tällöin otetaan tietoinen riski siitä, että uhka voi toteutua.

Jotta riskien arviointi olisi yhdenmukaista, on syytä käyttää apuvälineenä ennalta määriteltyjä kriteerejä. Riskin suuruuteen vaikuttavat mahdollisten seurausten vakavuus ja todennäköisyys. Kaikkia uhkia on mahdotonta hoitaa yhdellä kertaa, joten on tärkeää tunnistaa ne isoimmat riskit, jotka kiireisimmin vaativat ratkaisua. Tämän vuoksi määritellään ensin riskin suuruus arvioimalla uhkan seurauksena mahdollisesti syntyvien vahinkojen suuruus ja vahingon todennäköisyys. Riskin suuruuden arviointi antaa perusteet toimenpiteiden suunnittelulle ja suuntaamiselle. (Valtiovarainministeriö 2003, 41)

Taulukoissa 1-3 on esitetty Valtiovarainministeriön (2003, 41-43) määrittelyt riskien vakavuuden, todennäköisyyden ja suuruuden arvioimiseksi.

TAULUKKO 1. Uhkan todennäköisyys.

| | | |
|---|---|---|
| **Korkea** | **3** | • Toiminto tai järjestelmä on heikosti valvottua<br>• Toimintoon tai järjestelmään pääsy on helppoa<br>• Toimintoa tai järjestelmää kohtaan on suurta mielenkiintoa<br>• Toiminnon ohjeistusta ei ole<br>• Tapahtuma ilmenee kerran kuukaudessa<br>• Uhkan toteuttaminen on mahdollista suurelle määrälle käyttäjiä (oma henkilöstö, yhteistyökumppanit, ulkopuoliset) |
| **Keskimääräinen** | **2** | • Toiminto on osittain valvottua<br>• Toiminnon ohjeistus on puutteellista<br>• Tapahtuma ilmenee 1–2 kertaa vuodessa<br>• Uhkan toteuttaminen on mahdollista tietyille käyttäjäryhmille (atk-tuki) |
| **Alhainen** | **1** | • Toiminto on hyvin valvottua ja siihen pääsy on hallittua.<br>• Toiminto on hyvin ohjeistettu<br>• Toimintoa kohtaan ei ole mielenkiintoa<br>• Tapahtuma ilmenee kerran vuodessa<br>• Uhkan toteuttaminen on mahdollista vain yksittäisille työntekijöille (asiantuntijat) |
| **Ei merkitystä** | **0** | • Todennäköisyys on tasan nolla. Tämä uhka ei voi toteutua missään olosuhteissa |

Kaikkiin uhkien tunnistamismenetelmiin voidaan liittää riskin määrittely karkealla tasolla. Kun uhkan syyt on tunnistettu ja seuraukset arvioitu, voidaan kyseisen riskin suuruus määritellä. Riskin suuruuteen vaikuttavat tapahtuman todennäköisyys ja seurausten vakavuus. Yksinkertainen karkea luokittelu on usein helppoa laatia ja antaa hyvän kuvan eri riskien keskinäisistä eroista. Uhkien luokitteluun voidaan käyttää taulukon 1 asteikkoa, jossa uhkat on jaoteltu karkeasti korkeisiin, keskimääräisiin, alhaisiin ja merkityksettömiin riskeihin. Kuitenkin asteikon soveltamisessa on käytettävä harkintaa ja sovellettava sitä oman organisaation tilanteen mukaisesti. (Valtiovarainministeriö 2003, 41)

TAULUKKO 2. Uhkan vakavuus.

| | | |
|---|---|---|
| **Erittäin vakavat** | **3** | • Seuraukset koskevat kaikkia tietojen tai palveluiden käyttäjiä<br>• Uhkan toteutuminen aiheuttaa välittömiä toimenpiteitä<br>• Uhkan toteutuminen aiheuttaa raportoinnin ministeriölle ja tiedotusvälineille<br>• Uhkan toteutuminen aiheuttaa toiminnan keskeytymisen tunneista useisiin päiviin<br>• Uhkan toteutuminen aiheuttaa suuria taloudellisia kustannuksia<br>• Uhkan toteutuminen aiheuttaa vakavan häiriön organisaation toiminnassa (useiden avainhenkilöiden menetys)<br>• Uhkan toteutuminen aiheuttaa luottamuksellisuuden menetyksen<br>• Toiminta on lainsäädännön velvoitteiden vastaista. |
| **Vakavat** | **2** | • Seurauksilla on vaikutuksia organisaation sisällä, esimerkiksi yksittäisten työntekijöiden työmäärät kasvavat (avainhenkilön menetys)<br>• Seuraukset koskevat useita tietojen tai palveluiden käyttäjiä<br>• Seurauksilla on vaikutus organisaation toimintaan (saatava kuntoon tunneissa)<br>• Uhkan toteutuminen aiheuttaa tiedotteen tekemisen<br>• Uhkan toteutuminen aiheuttaa merkittäviä taloudellisia kustannuksia |
| **Vähäiset** | **1** | • Seuraukset koskevat muutamia tietojen tai palveluiden käyttäjiä<br>• Uhkan toteutuminen ei aiheuta välittömästi toimenpiteitä<br>• Uhkan toteutuminen aiheuttaa sisäisen raportoinnin<br>• Uhkan toteutuminen aiheuttaa vähäisiä taloudellisia kustannuksia<br>• Toiminnan keskeytyminen on muutaman minuutin pituinen |

Uhkan seurausten vakavuuden arviointiin voidaan käyttää taulukon 2 esimerkkiluokittelua. Myös tämän asteikon soveltamisessa on käytettävä harkintaa oman organisaation tilanteen mukaisesti. Seurausten vakavuutta mietittäessä voidaan pohtia esimerkiksi, mitä vahingosta voi pahimmassa

tapauksessa aiheutua tai mitä vahingosta normaalisti aiheutuu. Lisäksi on hyvä miettiä, mihin kaikkeen vahinko vaikuttaa. Miten monia ihmisiä, töitä, koneita, asiakkaita tai esimerkiksi yhteistyötahoja vahinko ja sen seuraukset koskevat. Myös laajempia vaikutuksia on pohdittava: mitkä ovat vahingon välilliset seuraukset. Joskus välilliset seuraukset voivat olla välittömästi seuraavaa vahinkoa suuremmat. (Valtiovarainministeriö 2003, 42-43)

Kun riskien todennäköisyys ja vakavuus on arvioitu, voidaan arvioida riskin suuruutta. Apuvälineenä voidaan käyttää taulukon 3 mukaista esimerkkiä, jossa seurausten vakavuudelle ja uhkan todennäköisyydelle on kolme eri tasoa. Tehtyjen selvitysten perusteella valitaan ensiksi seurausten vakavuus taulukon ylimmältä riviltä ja sen jälkeen tapahtuman todennäköisyys ensimmäisestä sarakkeesta. Riski on valittujen kohtien leikkauspisteessä olevan arvon suuruinen. Riskin suuruus saa pienimmillään arvon 1 (merkityksetön riski) ja suurimmillaan arvon 5 (sietämätön riski). (Valtiovarainministeriö 2003, 43)

TAULUKKO 3. Riskien arviointi.

| Kriittisyys | | Seurausten vakavuus | | |
|---|---|---|---|---|
| | | Vähäinen (1) | Vakava (2) | Erittäin vakava (3) |
| Uhkan toden-näköi-syys | Korkea (3) | 3. Kohtalainen riski | 4. Merkittävä riski | 5. Sietämätön riski |
| | Keskimääräinen (2) | 2. Vähäinen riski | 3. Kohtalainen riski | 4. Merkittävä riski |
| | Alhainen (1) | 1.Merkityksetön riski | 2. Vähäinen riski | 3. Kohtalainen riski |

Toimenpiteet riippuvat riskin vakavuudesta. Valtionhallinnon tietoturvallisuuden johtoryhmän (Valtiovarainministeriö 2003, 45-46) esimerkkiä noudattaen toimenpiteet voivat olla seuraavia:

Merkityksetön riski: Toimenpiteitä ei tarvita.

Vähäinen riski: Toimenpiteitä ei välttämättä tarvita. Voidaan kuitenkin harkita parempia ratkaisuja, jotka eivät aiheuta lisäkustannuksia tai seurata tilannetta ja varmistaa, että riski pysyy hallinnassa.

Kohtalainen riski: On ryhdyttävä toimiin riskin pienentämiseksi. Toimenpiteiden toteutukselle voidaan suunnitella sopiva aikajänne. Toimenpiteiden kustannuksia on mietittävä tarkasti. Jos riskiin liittyy erittäin haitallisia seurauksia (esimerkiksi vakava henkilövahinko tai tulipalo), on tarpeen selvittää tapahtuman todennäköisyys tarkemmin.

Merkittävä riski: Riskin pienentäminen on välttämätöntä. Toimenpiteet tulee aloittaa nopeasti. Riskialtista toimintaa ei pidä aloittaa ennen kuin riskiä pienennetty. Riskialtista toimintaa voidaan jatkaa, mutta kaikkien on tunnettava riski ja toiminta pitää saada loppumaan nopeasti.

Sietämätön riski: Riskin poistaminen on välttämätöntä. Toimenpiteet tulee aloittaa välittömästi. Riskialtista toimintaa ei pidä aloittaa. Riskialtis toiminta pitää keskeyttää, kunnes riski on poistettu.

### 2.2 Henkilöstöturvallisuus

Henkilöstöturvallisuudella tarkoitetaan henkilöstöstä aiheutuvien riskien hallintaa. Tietoturvallisuuden näkökulmasta henkilöstöturvallisuudella tarkoitetaan henkilöstöön liittyvien salassapito- ja käytettävyysriskien hallintaa tietoja ja tietojärjestelmiä käytettäessä. (Valtiovarainministeriö 2008, 11-12)

Henkilöstöturvallisuus on henkilöstöön liittyvien tietoturvariskien hallintaa muun muassa toimenkuvien, käyttöoikeuksien ja koulutuksen avulla. Henkilöstö on tietoturvan näkökulmasta suurin riskitekijä. Henkilöstöturvallisuuteen kuuluvat sekä oman henkilöstön että vierailijoiden tarkkailu ja valvonta. Henkilöstöturvallisuuden tarkoituksena on estää inhimillisestä toiminasta aiheutuvat tietoturvavahingot. (Paavilainen 1998, 87-89)

Lähtökohtaisesti tietoaineistoturvallisuus ja hallinnollinen turvallisuus, muun muassa tiedon omistajuus, luokitus, käsittelysäännöt, ohjeistus ja koulutus, ovat edellytyksiä henkilöstöturvallisuudelle, mutta niiden lisäksi henkilöstöturvallisuudessa on otettava huomioon muitakin mekanismeja.

Työprosessit ja käsittelyketjujen tietovirrat on alun perin suunniteltava sellaisiksi, että henkilöstön tahallisia ja tahattomia virheitä voidaan ennalta estää. (Valtiovarainministeriö 2008, 20)

Koulutuksen ja ohjeistuksen merkitystä ei pidä vähätellä. Joskus pieni virhekin saattaa kertaantua, jos selkeitä toimintaohjeita ei ole. Ihminen saattaa epätavallisessa tilanteessa toimia paniikinomaisesti aivan toisin kuin hän normaalisti toimisi. Pienen virheen hätäinen korjaus saattaa aiheuttaa monin verroin enemmän vahinkoja kuin alkuperäinen tilanne olisi aiheuttanut. (Paavilainen 1998, 91-92)

Henkilöstön vaihtuvuus muodostaa usein yllättävän suuria riskejä. Tilanteita saattaa ilmetä esimerkiksi sijaisten tai uuden henkilön palkkaamisen tai henkilön palveluksesta eroamisen tai erottamisen yhteydessä. Riskien minimoimiseksi henkilön palkkauksen yhteydessä henkilön luotettavuus tulisi aina tarkistaa ja tehdä tarvittaessa salassapitositoumus. Henkilön työsuhteen päättyessä on aina huolehdittava siitä, että kaikki hänen käytössään olevat kulkuluvat, luottokortit, käyttäjätunnukset ym. takavarikoidaan ja niiden voimassaolo lopetetaan. (Paavilainen 1998, 92-93)

Erityiseksi riskitekijäksi henkilöstövaihtuvuudessa saattaa pienessä organisaatiossa muodostua hiljaisen tiedon häviäminen. Olisi tärkeää, ettei kenestäkään tule organisaatiolle korvaamaton, vaan osaamista jaetaan useamman työntekijän kesken. Tärkeät tiedot tulisi dokumentoida aina huolellisesti, jotta tietoa ei häviä.

### 2.3 Fyysinen turvallisuus

Fyysisellä turvallisuudella tarkoitetaan laitteisto-, käyttö-, varasto- ja arkistotilojen fyysistä suojaamista. Fyysinen turvallisuus kattaa rakenne-, rakennus- ja ympäristön suunnittelun. Siihen kuuluvat myös kulunvalvonta, tekninen valvonta, vartiointi sekä palo-, vesi-, sähkö-, ilmastointi-, murto- yms. vahinkojen torjunta ja estäminen. Fyysinen turvallisuus ja laitteistoturvallisuus

ovat lähellä toisiaan. Erona voidaan pitää, että fyysinen turvallisuus suojaa tiloissa olevia laitteita fyysisesti tapahtuvilta uhkatekijöiltä ja laitteistoturvallisuus muilta uhilta. Fyysisistä uhkatekijöistä keskeisimmät ovat palo- ja vesivahingot, lämpövauriot, valvomaton liikkuminen sekä laitteiden, ohjelmien tai tietojen varkaudet. (Paavilainen 1998, 95-96)

Usein toimitilojen hallinta ja turvallisuusjärjestelyjen toteutus on kiinteistöhallinnon tai rakennuksen omistajan tehtävä. Toimintojen ja sen käyttämän tietotekniikan turvallisuustarpeet tuntee kuitenkin parhaiten käyttäjäorganisaation johto, joka päättää turvallisuusratkaisuista. Toimitilaturvallisuuden kehittämistarpeet otetaan huomioon vuosisuunnitelmia laadittaessa. (Valtiovarainministeriö 2009a)

Toimitilaturvallisuutta käsitteleviä lakeja ja säädöksiä ovat arkistolaki (831/1994, 12§), laki yksityisyyden suojasta työelämässä (759/2004), pelastuslaki (468/2003, 8§) ja työturvallisuuslaki (738/2002, 27§, 29§, 32§). Lisäksi kunnallishallinnossa voidaan soveltaa myös seuraavia valtionhallinnon ohjeita ja suosituksia: tietoteknisten laitetilojen turvallisuussuositus (Valtiovarainministeriö 2002) ja valtionhallinnon keskeisten tietojärjestelmien turvaaminen (Valtiovarainministeriö 2004a, luku 7).

### 2.3.1 Kulunhallinta

Kulunhallinnan tärkein yksittäinen osa-alue on kulunvalvonta. Kulunvalvonnan tärkein tehtävä sallia kohteeseen pääsy niille henkilöille, joilla siihen on oikeus, ja estää pääsy muilta henkilöiltä. Pääsyä kohteeseen rajataan käyttäjän tunnistuksen avulla. Tunnistus perustuu yleensä käyttäjän hallussa, tiedossa tai omistuksessa olevaan asiaan. Näitä voivat olla esimerkiksi muistettavat tunnisteet (salasanat, numerokoodit), tunnistusmateriaali (avaimet, kulkukortit) tai käyttäjän ominaisuudet (puheentunnistus, sormenjäljet). (Paavilainen 1998, 98-99)

Kulunhallinta sisältää myös muita elementtejä, kuten kiinteistössä liikkumisen linjausten, politiikkojen, standardien sekä toimintaohjeiden ylläpidon ja kehittämisen, käytettävien kulunhallinnan toteutuskeinojen määrittelyn ja valinnan sekä näiden asioiden johtamisen (Miettinen 1999, 181).

### 2.3.2 Palo-, vesi-, ja pölyvahinkojen torjunta

Suomessa paloturvallisuudesta on pääsääntöisesti huolehdittu hyvin, koska kiinteistöjen tekniset rakennemääräykset ovat varsin tiukat erityisesti paloturvallisuusvaatimuksissa. Myös vakuutusyhtiöt asettavat omia tiukkoja vaatimuksiaan paloturvallisuudelle. Automaattinen paloilmoitinjärjestelmä on yksi yleisimmin käytetyistä palosuojelun menetelmistä. Siihen kuuluu ilmaisimia, jotka tarkkailevat ympäröivää tilaa, sekä keskusyksikkö, joka tekee tarvittaessa palohälytyksen ilmaisimilta tulevien tietojen (savunmuodostuksen tai lämpötilan) perusteella. Automaattinen sammutusjärjestelmä on toinen yleisesti käytössä oleva palosuojelun menetelmä. Organisaation tiloissa on oltava myös asianmukaiset alkusammutusvälineet, kuten sammutuspeitteet ja käsisammuttimet. (Miettinen 1999, 183-184)

Vesivahingoilta suojautuminen on otettava huomioon IT-laitetilojen rakenteissa. IT-laitetiloihin ei saa rakentaa putkistoja siten, että ne rikkoontuessaan aiheuttaisivat vesivahingon. Laitetilat on aina rakennettava alapohjan päälle siten, että alle voidaan sijoittaa vesivahingosta hälyttävät anturit. Jos laitetiloissa on lattiakaivoja, on ne varustettava takaiskuventtiilillä veden sisääntulon estämiseksi.  Rakennettaessa IT-laitetila pohjaveden keskipinnan alapuolelle, tulee tila varustaa ulkopuolisesta sähkönsaannista riippumattomalla vuotovedenpoistolaitteella. (Valtiovarainministeriö 2002, 12)

Pöly voi aiheuttaa laitteiden rikkoutumisen tai muodostaa tulipaloriskin. Siivouksesta huolehtiminen on siksi tärkeää. IT-laitetilassa lattian tai seinien pintamateriaali ei saa muodostaa pölyä eikä muistakaan rakenteista saa irrota pölyä, joka mahdollisesti vaikeuttaisi laitteistojen jäähdytystä esimerkiksi tukkimalla laitteiden jäähdytysilmanottoaukkoja tai laitteiden prosessorien

tuulettimia.  Mahdolliset tulostimet tulisi sijoittaa eri palotilaan (pöly, palokuorma). Tuloilman suodatuksesta on huolehdittava siten, että ulkoilman epäpuhtaudet, kuten hiekkapöly tai muu ilmassa oleva aines ei kulkeudu sisätiloihin. Ilmanvaihtokanavien siivous on hoidettava säännöllisesti, jotta niihin ei pääse muodostumaan pölyä. (Valtiovarainministeriö 2002, 12)

### 2.3.3 Muut kiinteistötekniset suojauskeinot

Fyysiseen turvallisuuteen voidaan vaikuttaa myös varautumalla poikkeustilanteita varten. Tällaisia keinoja ovat esimerkiksi kiinteistöjen sähkönsyötön varmentaminen ja tilojen suojaaminen sähkömagneettisia sekä mikroaaltopulsseja vastaan. Lisäksi tietoturvallisuuteen voidaan vaikuttaa tilojen äänieristyksellä. (Miettinen 1999, 184)

Tyypillisesti sähkönsyöttö on varmistettu joko katkeamattoman virransyöttömenetelmän eli UPS (Uninterruptible Power Supply) –laitteiston tai polttomoottorikäyttöisten varavoimageneraattorien avulla, jotka käynnistyvät automaattisesti sähkökatkoksen aikana. Näissä kummassakin automatiikka tarkkailee laitteen sähkönsyöttöä ja energiakatkoksen jälkeen laite siirtyy käyttämään automaattisesti joko akuista tai polttomoottorigeneraattorista tulevaa varavoimaa. (Miettinen 1999, 185)

Voimakkaat sähkömagneettiset sekä mikroaaltopulssit pystyvät tuhoamaan laitteiden virtapiirit kehittämällä niihin voimakkaan virran, joka polttaa piirit ja lamauttaa laitteiden toiminnan tai ainakin häiritsee sitä voimakkaasti. Voimakas sähkömagneettinen pulssi eli EMP (Electro Magnetic Pulse) voi syntyä ilmakehässä tapahtuneen ydinräjähdyksen jälkeen ja se voi kulkeutua tuhansia kilometrejä ilmakehää pitkin. EMP-pulssia todennäköisempi uhka on kuitenkin mikroaaltoaseet, joiden avulla voidaan lamauttaa laitteiden toiminta. (Miettinen 1999, 185)

Äänieristyksien avulla organisaation tietoturvallisuutta voidaan parantaa nopeasti ja edullisesti. Eristämisessä seiniin lisätään tarvittava määrä äänieristemateriaalia, joka estää äänien kuulumisen huoneen ulkopuolelle. (Miettinen 1999, 185)

### 2.4 Laitteistoturvallisuus

Laitteistoturvallisuus koostuu laitteiden kokoonpanoon, kunnossapitoon ja laadunvarmistukseen liittyvistä turvallisuusnäkökohdista. Laitteistoturvallisuudella käsitetään myös niihin suoranaisesti liittyvät varusohjelmat. Tyypillisimmät laitteet ovat palvelimet, tietokoneet, tulostimet ja verkkokomponentit (sillat, reitittimet, toistimet, kytkimet). (Paavilainen 1998, 164-165)

Ylipäätään laitteistoturvallisuudella turvataan laitteiston elinkaarta, johon myös kuuluvat asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja -sopimukset sekä laitteiston turvallinen käytöstä poisto. (Valtiovarainministeriö 2009b)

Laitteiston elinkaareen liittyvien palvelusopimuksien palvelun tasoa määrittelevien rajojen ja vasteaikojen sopimisella voi olla merkittäviä vaikutuksia tietoturvatason ylläpidettävyyteen ja tietoturvapoikkeamiin reagointiin. Palvelusopimusten vasteaikoihin tukeutumalla voidaan vähentää varastoitavaa varalaitteistoa, mutta toisaalta riippuvuus toimittajan kyvystä toimia vasteaikojen puitteissa kasvaa. Erityisen tärkeää on määritellä sopimuksilla menettelytavat tilanteissa, joissa joko koko palvelu sijaitsee palvelun tarjoajalla. On myös kiinnitettävä erityistä huomiota laitteiden fyysisen turvallisuuden järjestämiseen, mikäli ne sijaitsevat toisen osapuolen tiloissa. Näissä tapauksissa palvelusopimukset ulotetaan koko järjestelmään ja vaaditaan riittävän tarkat selvitykset verkkoyhteyksistä ja fyysisestä pääsystä järjestelmään työajan ulkopuolella, mikäli palvelun täytyy olla jatkuvasti asiakkaiden käytettävissä. On myös huolehdittava, että laitteiston käyttöjärjestelmistä, ohjelmistoista ja niiden asetuksista on olemassa varmuuskopiot. Järjestelmien tietoturvapäivityksiä

varten tarvitaan selkeät ohjeet ja ne testataan ennen tuotantojärjestelmän asennusta. Päivitysten peruminen tulee olla mahdollista, mikäli päivityksessä havaitaan ongelmia. (Valtiovarainministeriö 2009b)

Laitteistoturvallisuuteen liittyviä lakeja ja asetuksia ovat: henkilötietolaki (523/1999, 5-10 §, 7. luku, 48 §), laki viranomaisen toiminnan julkisuudesta (621/1999 1§, 3 §, 10 §, 5. luku, 6. luku, 7. luku), asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999), laki yksityisyyden suojasta työelämässä (759/2004), sähköisen viestinnän tietosuojalaki (516/2004, 2. luku, 3. luku, 5. luku) sekä viestintämarkkinalaki (393/2003). Lisäksi kunnallishallinnossa voidaan soveltaa seuraavia valtionhallinnon ohjeita ja suosituksia: Älypuhelimien tietoturvallisuus – hyvät käytännöt (Valtiovarainministeriö 2007), Valtionhallinnon lähiverkkojen tietoturvallisuussuositus (Valtiovarainministeriö 2001a, luku 4.5), Haittaohjelmilta suojautumisen yleisohje (Valtiovarainministeriö 2004b), Valtionhallinnon keskeisten tietojärjestelmien turvaaminen (Valtiovarainministeriö 2004a, luku 9), Tietoteknisten laitetilojen tuvallisuussuositus (Valtiovarainministeriö 2002, luku 2) sekä Valtionhallinnon tietotekniikkahankintojen tarkastuslista (Valtiovarainministeriö 2001b, luku 3).

### 2.5 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan kaikkien käytettävien ohjelmistojen ja sovellusten tietoturvallisuusominaisuuksia (Paavilainen 1998, 185).

Ohjelmistoturvallisuuteen kuuluvat ohjelmistoihin liittyvät seikat, kuten ohjelmistoversioiden ja lisenssien hallinta sekä ohjelmistojen testaus, jolla varmistetaan mm. sovellusten sopivuus suunniteltuun käyttötarkoitukseen, ohjelmistojen keskinäinen yhteensopivuus sekä toiminnan luotettavuus ja virheettömyys (Hakala ym. 2006, 11-12).

Ohjelmistoturvallisuutta voidaan tarkastella joko ohjelmiston sisäisten suojausominaisuuksien tai erityisesti suojaamiseen tarkoitetuilla ohjelmistoilla.

Tyypillisiä sisäisiä suojausominaisuuksia ovat esimerkiksi ohjelmiston pääsynvalvonta, lokitietojen keruu sekä salasanojen automaattinen vanheneminen. Erillisiä tietoturvallisuutta parantavia suojausohjelmia ovat virustorjuntaohjelmistot, tietojen ja tietoliikenteen salausohjelmistot sekä tietojen varmuuskopiointiohjelmistot. Lisensointiin liittyvillä ohjelmistoilla voidaan hallita lisenssejä ja huolehtia siitä, että organisaatio käyttää vain luvallisia ja lisensoituja ohjelmistoja. (Miettinen 1999, 21)

Ohjelmistoturvallisuuden tärkeimpiä perussuojausmenetelmiä ovat ohjelmiston pääsynvalvonta, ohjelmiston tapahtumatietojen seuranta, varmuuskopiointi, asianmukainen ohjelmistodokumentaatio, asianmukaisesti laaditut ylläpito- ja huoltosopimukset sekä rekisteröityjen ohjelmistojen käyttö. (Miettinen 1999, 226)

Ohjelmiston pääsynvalvonnan avulla pyritään estämään valtuuttamattomien käyttäjien pääsy tietojärjestelmän sisältä. Se on toteutettu tavallisesti käyttäjätunnuksen ja salasanan avulla. Tapahtumatietoja eli lokitietoja seuraamalla voidaan varmentaa, ettei väärinkäytöksiä ole tapahtunut. Varmuuskopioinnin avulla varmistetaan, että ohjelmien tai niiden tietojen vaurioituessa tai tuhoutuessa tiedot voidaan palauttaa. Automaattinen varmuuskopiointi on paras vaihtoehto, jotta käyttäjän ei tarvitse huolehtia siitä erikseen. Ohjelmistodokumentaatiolla tarkoitetaan esimerkiksi ohjelmiston rakenteen ja toiminnan kuvausta sekä käyttöohjeita. Huolto- ja ylläpitosopimukset on laadittava siten, että viat saadaan korjattua mahdollisimman nopeasti ja viiveittä. (Miettinen 1999, 226-228)

### 2.6 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus koostuu toimenpiteistä, joilla varmistetaan verkoissa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys. Päämääränä on varmistaa viestien alkuperäisyys, koskemattomuus ja luottamuksellisuus, todentaa lähettäjä ja vastaanottaja, varmentaa tietoliikennelaitteiden fyysinen turvallisuus sekä estää väärinreititys. Tietoliikenneturvallisuuteen kuuluvat kaikki

asiat, jotka koskevat verkkojen rakentamista, suunnittelua ja verkkoliikennettä. (Paavilainen 1998, 108)

Tietoliikenneverkkojen uhat voidaan jakaa sisäisiin ja ulkoisiin uhkiin. Sisäisiä uhkia ovat esimerkiksi oma henkilöstö, vierailijat, laiteviat, tuhotyöt ja tulipalot. Ulkoisia uhkia ovat esimerkiksi hakkerointi, vakoilu, salakuuntelu, laitteiden häirintä tai manipulointi tai verkon kuormittaminen. (Paavilainen 1998, 137-139)

### 2.6.1 Rakenteellinen tietoturva

Tietoverkon turvallisuus on otettava huomioon jo suunnittelussa. Myöhemmin tehtävät turvallisuuspaikkaukset eivät useinkaan pysty korjaamaan ennen verkon rakentamista tehtyjä virheitä ja muutokset tulevat usein kalliiksi. Tietoverkon suunnitteluvaiheessa on hyvä tehdä tietovirta-analyysi, analyysi turvallisuustavoitteista ja suunniteltava niiden pohjalta tietoverkon turva-arkkitehtuuriratkaisut, turvakomponenttien sijoitteluratkaisut sekä mitoitettava verkon siirtokapasiteetti ja huomioitava tarvittavien tietoliikenneprotokollien mahdolliset erikoistarpeet. Suunnitteluvaiheeseen kuuluu myös verkon valvonnan suunnittelu sekä testaussuunnitelman laadinta. Suunnittelun pohjana ovat tiedot, joita siirretään ja niiden turvaluokka. (Valtiovarainministeriö 2009c)

Verkon käytettävyysasteen korkeana pitämiselle on tärkeää, että jo suunnitteluvaiheessa otetaan huomioon vaihtoehtoisten tiedonsiirtoreittien ja –resurssien käyttö. Kahdennetut yhteydet ja varayhteydet tulee suunnitella siten, että ne eivät missään kohdassa ole riippuvaisia yksittäisestä toimivasta komponentista. Järjestelyt tulee tarkastaa päästä päähän sekä loogisella että fyysisellä tasolla. Huomiota tulee kiinnittää erityisesti sellaisiin paikkoihin, joihin kaapeleiden vetäminen on vaikeaa. Tällöin saattaa paljastua, että useat kaapelit saattavat kulkea joko jopa samassa kaapelitunnelissa tai erittäin lähellä toisiaan. (Valtiovarainministeriö 2009c)

Varmistukset ja varajärjestelyt tulee suhteuttaa verkon kriittisyyteen; kriittisen verkon tulee olla mahdollisimman vikasietoinen ja turvattu varajärjestelyin vikasietoisuuden pettämisen varalta. Varmistusten ja varajärjestelyjen tila tulee selvittää myös sidosryhmien osalta silloin, kun niistä ollaan riippuvaisia. Varayhteyksien on oltava joko jatkuvassa käytössä osana tuotantojärjestelmää tai ne on testattava säännöllisesti. Varajärjestelyt tulee mitoittaa siten, että ne takaavat riittävän palvelutason. (Valtiovarainministeriö 2009c)

Langattomiin tietoliikenneyhteyksiin liittyy riskejä, joista suurimmat ovat liikenteen luvattomassa kuuntelussa, liikenteen häirinnässä ja luvattomassa liittymisessä langattomaan verkkoon. Keskeisten tietojärjestelmien kriittisissä yhteyksissä tulee suosia langallisia tiedonsiirtokanavia. Mikäli kriittinen yhteys on langaton, sillä tulee olla käytettävyyden turvaamiseksi varayhteys, joka ei ole langaton. Langattomia yhteyksiä käytettäessä todennusmekanismien tulee olla riittäviä, koska langattomaan verkkoon voi lähettää dataa kuka tahansa sopivan lähettimen omistava. Koska langatonta yhteyttä voi kuunnella sopivalla vastaanottimella, tulee luottamuksellinen liikenne salata. (Valtiovarainministeriö 2009c)

### 2.6.2 Valvonta ja dokumentointi

Tietoverkko pitää dokumentoida asianmukaisesti ja dokumentointia tulee myös ylläpitää ja valvoa. Tietoliikenneyhteyksistä tulee dokumentoida myös käyttö; dokumenteista tulee ilmetä tietovirrat, tietojen omistajuus sekä tietojen käyttäjät. Tietoliikenteeseen liittyvät rajapinnat ja tiedonsiirtoprotokollat on dokumentoitava varayhteyksineen ja manuaalisine varajärjestelmineen. (Valtiovarainministeriö 2009c)

Verkon valvonnan tulee kattaa sekä verkon fyysisen valvonnan (topologia, komponentit, jne.) että liikenteen valvonnan (profiili, protokollat, jne.). Fyysistä valvontaa tekevien järjestelmien tulee pystyä havaitsemaan ainakin luvattomat laitteet, luvattomat kiinnitäytymiset verkkoon sekä näiden yritykset. Liikenteen valvontaan tulee kuulua tunkeutumisen havainnointi- ja estojärjestelmä.

Valvonta- ja varajärjestelyt tulee toteuttaa siten, että myös heikentynyt toiminta havaitaan. (Valtiovarainministeriö 2009c)

Keskeisten järjestelmien käyttämissä tietoverkoissa tulee suosia pysyviä, yksikäsitteisiä verkko-osoitteita, kuten kiinteät IP-osoitteet sekä vianmäärityksen helpottamiseksi että turvapolitiikasta poikkeavan toiminnan paikallistamisen helpottamiseksi. Aitojen kiinteiden IP-osoitteiden sijasta voidaan myös käyttää verkkokorttitunnisteeseen sidottuja dynaamisia IP-osoitteita; tällöin laite saa ensimmäisellä kerralla verkkoon liittyessään IP-osoitteen verkon osoiteavaruudesta ja jatkossa aina saman osoitteen. (Valtiovarainministeriö 2009c)

### 2.6.3 Suojaus

Suojaus toteutetaan palomuurin avulla. Palomuurin tehtävänä on erottaa toisistaan kaksi tai useampi verkkosegmentti ja kontrolloida näiden verkkosegmenttien välistä liikennettä asennetun sääntökannan mukaisesti. Palomuuri voi olla joko sovellus, jota ajetaan normaalissa tietokonelaitteistossa tai erillinen laite, joka sisältää laitealustan, käyttöjärjestelmän ja palomuurisovelluksen. (Valtiovarainministeriö 2009c)

Palomuurit voidaan toimintansa puolesta jakaa kolmeen perustyyppiin: pakettisuodattimiin, välityspalvelimiin ja sovellustason yhdyskäytäviin. Pakettisuodattimet ovat laitteita, jotka hylkäävät liikennettä lähde- ja kohdeosoitteiden sekä sovellusten käyttämien porttinumeroiden perusteella. Välityspalvelimet ovat laitteita, jotka avaavat käyttäjän puolesta yhteyden johonkin palveluun. Niihin on etukäteen määritelty, mistä laitteista yhteyden voi muodostaa johonkin tiettyyn palveluun. Ne mahdollistavat usein myös laitteen käyttäjän luotettavan tunnistuksen, autentikoinnin, ennen yhteyden avaamista. Ainoastaan ennalta määrättyjä palveluita voidaan käyttää, muita palveluita käyttävä liikenne hylätään. Yhdyskäytävä välittää liikenteen asiakas- ja palvelinohjelmiston välillä sekä tutkii jokaisen paketin sisällön. Se toimii virustentorjuntaohjelmiston tavoin havaitessaan normaalista poikkeavia

paketteja. Niitä ei välitetä eteenpäin ja ne voidaan tarvittaessa tallentaa tarkempaa analyysiä varten. Epäilyttävät paketit aiheuttavat hälytyksen, joka välitetään palomuurin käyttöhenkilöstölle. Sovellustason yhdyskäytävä tutkii kaiken lävitseen kulkevan sallitun liikenteen paketti paketilta ja analysoi sisällön ennen sen lähettämistä eteenpäin. (Hakala ym. 2006, 187-188)

## 2.7 Tietoaineistoturvallisuus

Tietoaineistoturvallisuus on asiakirjojen, tietueiden, tiedostojen ja muiden tietovälineiden tunnistamista ja turvaluokitusta sekä tietovälineiden hallintaa, säilytystä ja käsittelyä asianmukaisesti kaikissa tiedonkäsittelyprosessien eri vaiheissa. Tietoaineostoturvallisuuteen liittyy olennaisena osana myös tiedon varmistaminen, asianmukainen säilytys ja hävittäminen. (Paavilainen 1998, 26)

### 2.7.1 Käyttöoikeudet

Jotta käyttäjän oikeus tietoon voidaan myöntää, on ensin varmistuttava, että käyttäjä on se kuka hän väittää olevansa. Tyypillisimpiä tapoja tunnistamiseen ovat henkilökohtainen tuttavuus, avaimet, käyttäjätunnukset ja salasanat sekä toimikortit. (Paavilainen 1998, 26)

Käyttöoikeudet tulee mahdollisuuksien mukaan luoda siten, että käyttäjällä on ainoastaan tarvittavat oikeudet tehtäviensä hoitamiseen. Käyttöoikeudet tulee jakaa siten, että vaarallisia yhdistelmiä ei pääse syntymään; käyttäjällä ei esimerkiksi saa olla oikeuksia oman työnsä hyväksyntään tai tarkastamiseen. Käyttöoikeudet tulee sitoa työtehtäviin. Kun henkilön työtehtävät vaihtuvat, käyttöoikeudet tulee päivittää vastaaviksi. Virastolla tulee olla dokumentoidut työtehtävien muutosprosessit (sisältäen työhöntulon ja työsuhteen päättymisen), jotka huomioivat myös muutokset käyttöoikeuksissa. (Valtiovarainministeriö 2009d)

### 2.7.2 Salassapitosopimukset

Erillisillä salassapitosopimuksilla voidaan varmistaa tietoaineiston säilymistä turvallisena. Niillä täydennetään laissa määrättyä salassapitovelvollisuutta. Salassapitovelvollisuus saadaan täten koskemaan kaikkea vaihdettavaa materiaalia. Salassapitosopimuksien avulla voidaan tiedon paljastamiseen lisätä esimerkiksi rahallisia sanktioita. Salassapitosopimus koskee molempia osapuolia. Salassapitositoumus on mahdollista tehdä, jos halutaan yksipuolinen salassapitovelvollisuus. Usein erillistä salassapitosopimusta tai -sitoumusta ei tarvitse tehdä, koska lainsäädäntö kattaa tietojen salassapidon. Varsinaisissa sopimuksissa on kuitenkin hyvä tuoda kirjallisesti esille lain vaatimukset. (Valtiovarainministeriö 2009d)

### 2.7.3 Tietoaineiston käsittely ja säilyttäminen

Turvalliseen tiedonkäsittelyyn pyrittäessä on varmistuttava tiedon koko elinkaaren mittaisen käsittelyn turvallisuudesta, aina ensimmäisestä luonnoksen tekemisestä viimeiseen tiedon tuhoamispisteeseen. Jokaisessa vaiheessa on varmistuttava, ettei tietoja käsittele muu henkilö kuin se, jolla on siihen oikeus. Tallenteen on säilytettävä siihen tallennettu tieto muuttumattomana. (Paavilainen 1998, 39)

Siirrettäviä tallennusvälineitä, joilla on salassa pidettävää tietoa, tulee käsitellä samojen vaatimusten mukaisesti kuin salassa pidettävää paperiasiakirjaa. Tietovälineitä tulee käsitellä huolellisesti, vaikka niille olisi tallennettu pelkästään julkista aineistoa, koska kadotettu tietoväline tekee helposti vahinkoa julkisuuskuvalle. (Valtiovarainministeriö 2009d)

Tietoaineisto voidaan säilyttää ja arkistoida joko sähköisessä tai manuaalisessa muodossa. Tietoaineiston säilytystilojen turvallisuus tulee mitoittaa säilytettävän aineiston kriittisyyden mukaan. Huomioitavia asioita ovat riittävä murtosuojaus,

paloturvallisuus, lämpötila, ilman kosteus, pöly, valo jne. Eri tietovälineillä on säilytyksen osalta erityisvaatimuksia. (Valtiovarainministeriö 2009d)

Tietojärjestelmissä oleva tieto tulee varmuuskopioida säännöllisesti. Pääsääntöisesti ainakin yksi varmuuskopio tulisi sijoittaa fyysisesti eri palotilaan kuin alkuperäinen aineisto. Mikäli varmuuskopioiden luottamuksellisuus halutaan turvata, voidaan kopioitava materiaali salata. Varmuuskopion eheys voidaan varmistaa sähköisellä allekirjoituksella. Tarvittaessa voidaan käyttää sekä salausta että allekirjoituksia. (Valtiovarainministeriö 2009d)

### 2.7.4 Tietoaineiston hävittäminen

Tietoaineisto on hävitettävä asianmukaisesti. Eri tallenteet vaativat erilaiset hävittämistavat. Normaalit paperiasiakirjat voidaan hävittää joko laittamalla ne suoraan paperinkeräykseen tai vasta silppuamisen jälkeen riippuen tiedon arkaluonteisuudesta. Erittäin salainen aineisto on silputtava ns. ristiinsilppuavalla koneella, jolloin syntyvä silppu on erittäin pientä ja aineiston uudelleenkasaaminen silpusta on erittäin vaikeaa. Arkaluonteisen tiedon hävittämisestä olisi hyvä myös pitää kirjanpitoa, jotta voidaan tarvittaessa varmentaa, mitä tietoja on hävitetty ja miten hävittäminen on suoritettu. (Paavilainen 1998, 44-47)

Salassa pidettävä materiaali on erotettava muusta hävitettävästä materiaalista. Hävittämisen saavat tehdä vain siihen oikeutetut ja hävittämistä on valvottava. Mikrofilmit tulee silputa, polttaa ongelmajätelaitoksessa tai niistä tulee poistaa hopea erikoisliikkeessä. Sähköiset ja magneettiset tietovälineet joko tyhjennetään päällekirjoituksella tai tuhotaan fyysisesti. Optiset tietovälineet hävitetään rikkomalla. (Valtiovarainministeriö 2009d)

## 2.8 Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan niitä tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyviä keinoja, joilla parannetaan tietoturvallisuutta. (Valtiovarainministeriö 2009f)

### 2.8.1 Käyttäjätunnukset ja salasanat

Käyttäjätunnuksen ja salasanan yhdistelmä on yleisin käyttäjän tunnistusmenetelmä. Käyttäjätunnukset ovat julkisia, joten tietoturvan näkökulmasta salasana nousee tärkeään asemaan. Salasanan olisi hyvä täyttää Paavilaisen (1998, 169) mukaan seuraavat vaatimukset:

- salasanan yhdistäminen käyttäjään tulisi olla mahdollisimman vaikeaa
- salasana tulisi vaihtaa pakotetusti tietyin väliajoin
- vanhoja salasanoja ei saa käyttää uudelleen
- uuden salasana johtaminen vanhasta ei saa olla mahdollista
- salasanalla on oltava tietty vähimmäispituus
- salasana tulee antaa sisäänkirjauduttaessa tietyssä ajassa
- kolmen virheellisen sisäänkirjautumisen jälkeen käyttöoikeus lukittuu
- salasanan paljastuttua käyttäjän tulee voida vaihtaa se välittömästi
- salasanojen on oltava salakirjoitettuja, mikäli niitä siirretään julkisessa verkossa
- pitää olla olemassa menettely, jolla käyttäjä saa uuden salasanan unohdetun tilalle
- salasanoja ei saa tallentaa työaseman kiintolevylle
- käyttäjätunnuksen ja salasanan luovuttaminen vieraalle henkilölle on sanktioitava yrityksen sisäisesti

Lisäksi henkilöstöä tulisi ohjeistaa, että samoja salasanoja ei tulisi käyttää useissa palveluissa (esimerkiksi sosiaalisessa mediassa tms.).

### 2.8.2 Viestinnän turvallisuus

Matkapuhelimet muodostavat yhä suuremman tietoturvariskin, varsinkin, jos käyttäjä ei ole riittävän perehtynyt laitteen toimintoihin. Älypuhelimet ovat toiminnoiltaan tietokoneiden veroisia, mutta niiden suojaus on usein puutteellinen. Matkapuhelin on huono viestinvälityskanava salaiselle tiedolle. GSM/2G -verkoissa käytetty tekniikka on vanhentumassa, ja käytössä olevat salausratkaisut ovat tietyissä olosuhteissa murrettavissa. 3G-verkkoa kannattaa suosia, sillä se on turvallisempi. Kirjautumistunnukset, suojakoodit ja PIN-koodit tulee vaihtaa laitteen käyttöönoton yhteydessä, samoin sisältö tulisi salata, mikäli se on mahdollista. Langattomien tekniikoiden kanssa on noudatettava erityistä varovaisuutta, esimerkiksi Bluetooth-yhteys kannattaa sulkea, kun se ei ole käytössä. Haittaohjelmia vastaan voi suojautua palomuurin ja virustorjuntaohjelmiston avulla, lisäksi puhelin on pidettävä päivitettynä ja ohjelmistoja tulee ladata vain luotetuista lähteistä. (Viestintävirasto 2013)

# 3 TUTKIMUKSEN TEKEMINEN JA TULOKSET

Tietoturvasuunnitelman tekeminen toteutettiin syvähaastattelemalla Kinnulan kunnan sosiaalijohtajaa, ylilääkäriä, johtavaa hoitajaa, perusturvatoimialan tietosuojavastaavaa, kunnanrakennusmestaria ja IT-palveluntuottajaa. Haastattelut olivat kestoltaan 45 minuuttia - 1,5 tuntia. Haastatteluiden pohjana käytettiin soveltuvin osin Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) tarkistuslistoja. Lisäksi käytettiin täydentäviä kysymyksiä. Haastattelut äänitettiin analysointia varten.

Haastatteluiden perusteella saatua tietoaineistoa arvioitiin Valtiovarainministeriön ohjeita hyödyntäen. Apuna käytettiin ohjetta riskien arvioinnissa tietoturvallisuuden edistämiseksi valtionhallinnossa soveltuvin osin. Riskianalyysiin sisällytettiin kehittämisehdotuksia, joissa pyrittiin huomioimaan se, ettei riskin korjaamisesta tai poistamisesta muodostu mittavia taloudellisia kustannuksia.

Tehdyn riskianalyysin ja haastatteluiden tuloksista laadittiin kunnan perusturvatoimialalle tietoturvasuunnitelma, johon kirjattiin perusturvatoimialan tietoturvakäytännöt, vastuut sekä toimintaohjeita. Tietoturvasuunnitelmaan sisällytettiin hallinnollisen tietoturvallisuuden, henkilöstöturvallisuuden, fyysisen turvallisuuden, tietoliikenneturvallisuuden, laitteistoturvallisuuden ja tietoaineistoturvallisuuden osa-alueet. Lisäksi luetteloitiin tietoturvallisuuteen liittyvät dokumentit ja niiden sijainnit.

## 3.1 Hallinnollinen tietoturvallisuus

Hallinnollisen tietoturvallisuuden osa-alueen alle koottiin tehtävät sekä vastuualueet. Lisäksi laadittiin ohjeistus riskien raportointia ja arviointia varten.

### 3.1.1 Tehtävät ja vastuut

Sisältö on poistettu liikesalaisuussyistä

### 3.1.2 Riskien tunnistaminen ja raportointi

Sisältö on poistettu liikesalaisuussyistä

Sisältö on poistettu liikesalaisuussyistä

### 3.1.3 Kehittäminen, päivitys ja seuranta

Sisältö on poistettu liikesalaisuussyistä

## 3.2 Henkilöstöturvallisuus

Sisältö on poistettu liikesalaisuussyistä

### 3.2.1 Rekrytointi

Sisältö on poistettu liikesalaisuussyistä

### 3.2.2 Työnkuva

Sisältö on poistettu liikesalaisuussyistä

### 3.2.3 Sijaisjärjestelyt

Sisältö on poistettu liikesalaisuussyistä

### 3.2.4 Tiedonsaanti- ja käyttöoikeudet

Sisältö on poistettu liikesalaisuussyistä

### 3.2.5 Salasanat

Sisältö on poistettu liikesalaisuussyistä

### 3.2.6 Tietoturvakoulutus

Sisältö on poistettu liikesalaisuussyistä

### 3.2.7 Väärinkäytökset

Sisältö on poistettu liikesalaisuussyistä

## 3.3 Fyysinen turvallisuus

Sisältö on poistettu liikesalaisuussyistä

### 3.3.1 Kiinteistön turvallisuus

Sisältö on poistettu liikesalaisuussyistä

### 3.3.2 Toimistotilat

Sisältö on poistettu liikesalaisuussyistä

### 3.3.3 Arkistotilat

Sisältö on poistettu liikesalaisuussyistä

### 3.3.4 Asiakastilat

Sisältö on poistettu liikesalaisuussyistä

### 3.3.5 Varavoimajärjestelmät

Sisältö on poistettu liikesalaisuussyistä

### 3.4 Tietoliikenneturvallisuus ja laitteistoturvallisuus

Sisältö on poistettu liikesalaisuussyistä

#### 3.4.1 Verkon valvonta ja hallinta

Sisältö on poistettu liikesalaisuussyistä

#### 3.4.2 Suojaus

Sisältö on poistettu liikesalaisuussyistä

### 3.4.3 Etätyö

Sisältö on poistettu liikesalaisuussyistä

### 3.4.5 Dokumentaatio ja ohjeistus

Sisältö on poistettu liikesalaisuussyistä

### 3.4.6 Laitteiston käyttö, huolto ja rikkoutuminen

Sisältö on poistettu liikesalaisuussyistä

## 3.5 Tietoaineistoturvallisuus

Sisältö on poistettu liikesalaisuussyistä

### 3.5.1 Tietojen luokitus

Sisältö on poistettu liikesalaisuussyistä

Sisältö on poistettu liikesalaisuussyistä

### 3.5.2 Tarpeettoman tietoaineiston hävittäminen

Sisältö on poistettu liikesalaisuussyistä

### 3.5.3 Tietovälineiden käsittely ja käytöstä poisto

Sisältö on poistettu liikesalaisuussyistä

### 3.5.4 Tietoaineiston säilytys ja arkistointi

Sisältö on poistettu liikesalaisuussyistä

## 3.6 Liittyvät dokumentit ja niiden sijainti

Sisältö on poistettu liikesalaisuussyistä

## 3.7 Yhteenveto tutkimustuloksista

Sisältö on poistettu liikesalaisuussyistä

### 3.7.1 Hallinnolliseen tietoturvallisuuteen liittyvät riskit

Sisältö on poistettu liikesalaisuussyistä

TAULUKKO 4. Hallinnolliseen tietoturvallisuuteen liittyvät riskit

| Riski | Arviointi | Toimenpiteet |
|---|---|---|
| Sisältö on poistettu liikesalaisuussyistä | | |
| | | |

Sisältö on poistettu liikesalaisuussyistä

### 3.7.2 Henkilöstöturvallisuuteen liittyvät riskit

Sisältö on poistettu liikesalaisuussyistä

TAULUKKO 5. Henkilöstöturvallisuuteen liittyvät riskit

| Riski | Arviointi | Toimenpiteet |
|---|---|---|
| Sisältö on poistettu liikesalaisuussyistä | | |
| | | |
| | | |
| | | |
| | | |

Sisältö on poistettu liikesalaisuussyistä

### 3.7.3 Fyysiseen turvallisuuteen liittyvät riskit

Sisältö on poistettu liikesalaisuussyistä

TAULUKKO 6. Fyysiseen turvallisuuteen liittyvät riskit

| Riski | Arviointi | Toimenpiteet |
|---|---|---|
| Sisältö on poistettu liikesalaisuussyistä | | |
| | | |

Sisältö on poistettu liikesalaisuussyistä

### 3.7.4 Laitteistoturvallisuuteen liittyvät riskit

Sisältö on poistettu liikesalaisuussyistä

TAULUKKO 7. Laitteistoturvallisuuteen liittyvät riskit.

| Riski | Arviointi | Toimenpiteet |
|---|---|---|
| Sisältö on poistettu liikesalaisuussyistä | | |
| | | |
| | | |
| | | |
| | | |
| | | |

Sisältö on poistettu liikesalaisuussyistä

Sisältö on poistettu liikesalaisuussyistä

### 3.7.5 Tietoaineistoturvallisuuteen liittyvät riskit

Sisältö on poistettu liikesalaisuussyistä

TAULUKKO 8. Tietoaineistoturvallisuuteen liittyvät riskit.

| Riski | Arviointi | Toimenpiteet |
|---|---|---|
| | | |

# 4 JOHTOPÄÄTÖKSET

Tutkimuksen keskeisin tulos oli kunnan perusturvatoimialan tietoturvasuunnitelma, jota ei tässä laajuudessa ollut toteutettu aiemmin. Myöskään riskianalyysia ei ollut toimialalla tehty. Tutkimuksen tuloksena saatiin tehtyä kartoitus tietoturvariskeistä, suositelluista kehittämistoimenpiteistä sekä ohjeistus riskien raportoinnista jatkossa. Tietoturvasuunnitelma on asiakirja, jota tulee päivittää säännöllisesti mahdollisten uusien havaittujen riskien seurauksena.

Tutkimuksessa havaittiin merkittäviä, välitöntä korjaamista vaativia riskejä ainoastaan yksi fyysisen turvallisuuden osa-alueella. Kohtalaisia riskejä havaittiin yhteensä neljä, joista kaksi olivat hallinnollisen tietoturvallisuuden osa-alueella, yksi henkilöstöturvallisuuden osa-alueella ja yksi tietoaineistoturvallisuuden osa-alueella. Vähäisiä riskejä oli eniten, yhteensä yhdeksän. Laitteistoturvallisuuden osa-alueella vähäisiä riskejä havaittiin viisi, fyysisen turvallisuuden osa-alueella yksi ja henkilöstöturvallisuuden osa-alueella kolme. Myös pienet riskit kirjattiin, merkityksettömiä riskejä löydettiin yksi laitteistoturvallisuuden osa-alueelta.

Yhteenvetona riskikartoituksesta voidaan sanoa, että yleisellä tasolla henkilöresurssien vähyys ja henkilöstön kuormittuminen oli yleinen riskitekijä kaikilla osa-alueilla.

Tutkimusmenetelmänä käytettiin syvähaastattelua. Tutkimuksen tekemiseen aiheuttivat haasteita kunnassa viime aikoina tapahtuneet merkittävät henkilöstövaihdokset, jolloin vaarana oli, että kaikkea tutkimustietoa ei saatu käyttöön. Kuitenkin tutkimusaineisto antoi riittävässä laajuudessa kokonaiskuvan merkittävistä seikoista, jotta tutkimus oli riittävän validi.

Vastaustuloksissa saatiin muutamia vastauksia, jotka poikkesivat toisistaan. Näissä tapauksissa käytettiin täydentäviä kysymyksiä, jotta voitiin varmistua vastauksen oikeellisuudesta. Poikkeamat johtuivat lähinnä siitä, ettei vastaajalla ollut riittävää tietoa erityistä asiantuntijuutta (esimerkiksi yksityiskohtaisia

tietoteknisiä seikkoja) vaativissa kysymyksissä. Täydentävien kysymysten perusteella tutkimuksen reliabiliteetin voidaan kuitenkin arvioida olevan riittävä.

Riskienhallinta on merkittävä osa johtamista. Tutkimuksessa ilmeni, että riskienhallintaan pitäisi kiinnittää jatkossa enemmän huomiota. Riskikartoitukset on syytä tehdä säännöllisin väliajoin. Ennaltaehkäisyn merkitystä ei voi koskaan korostaa liikaa tietoturva-asioissa, jotta voidaan säästyä turhilta taloudellisilta kustannuksilta. Jatkotutkimusta olisi aiheellista tehdä kaikilla kunnan toimialoilla riskikartoituksena ja tietoturvasuunnitelman ajantasaisuuden selvittämisenä.

## LÄHTEET

Arkistolaki 831/1994. Helsinki. Opetusministeriö 1.10.1994.

Asetus viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta 1030/1999. Helsinki. Oikeusministeriö. 1.12.1999.

Grönfors-Kallio, A. & Suomela, T. 2014. Talouden ja rahoituksen johtaminen. Kokonaisvaltainen riskienhallinta johtamisen tukena. Kauppalehti. Uutiskirje 2/2014. Internet-sivut. Luettu 9.6.2014. http://johtaminen.kauppalehti.fi/book/talouden-ja-rahoituksen-johtaminen/corporate-governance-sisainen-valvonta-ja-riskienhallinta-2

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

Henkilötietolaki 523/1999. Helsinki. Oikeusministeriö. 1.6.1999.

Laki yksityisyyden suojasta työelämässä 759/2004. Helsinki. Työministeriö. 1.10.2004.

Laki viranomaisen toiminnan julkisuudesta 621/1999. Helsinki. Oikeusministeriö. 1.12.1999.

Miettinen, J. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Kauppakaari OYJ, Helsinki.

Nyrhinen, A. 2013. Riskienhallinta yhtä kuin hyvää johtamista? Blogikirjoitus. Internet-sivut. Luettu 9.6.2014. http://www.kauppalehti.fi/sponsoroidutblogit/op-pohjola/riskienhallinta-yhta-kuin-hyvaa-johtamista

Paavilainen, J. 1998. Tietoturva. Gummerus Kirjapaino Oy, Jyväskylä.

Pelastuslaki 468/2003. Helsinki. Sisäasiainministeriö. 1.1.2004.

Pisto, M. 2010. Riskienhallinnan johtaminen, osa II: Johda riskejä!. Turvallisuuslehti 5/2010. Internet-sivut. Luettu 9.6.2014. http://srhy.fi/uploads/artikkelit/Turvallisuuslehti_5_2010_Johda_riskeja.pdf

Sähköisen viestinnän tietosuojalaki 516/2004. Helsinki. Liikenne- ja viestintäministeriö. 1.9.2004.

Valtiovarainministeriö 2000. Valtionhallinnon tietoaineistojen käsittelyn tietoturvallisuusohje. Vahti 2/2000. Internet-sivut. Luettu 8.5.2014. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3386/3388_fi.pdf

Valtiovarainministeriö 2001a. Valtionhallinnon lähiverkkojen tietoturvallisuussuositus. Vahti 2/2001. Internet-sivut. Luettu 8.5.2014. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/3375/3378_fi.pdf

Valtiovarainministeriö 2001b. Valtionhallinnon tietotekniikkahankintojen tarkastuslista. Vahti 6/2001. Internet-sivut. Luettu 8.5.2014. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/6193/6194_fi.pdf

Työturvallisuuslaki 738/2002. Helsinki. Sosiaali- ja terveysministeriö. 1.1.2003.

Valtiovarainministeriö 2002. Tietoteknisten laitetilojen turvallisuussuositus. Vahti 1/2002. Internet-sivut. Luettu 20.3.2014. http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20020101Tietot/turvallisuussuositus.pdf

Valtiovarainministeriö 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Vahti 7/2003. Edita Prima Oy, Helsinki.

Valtiovarainministeriö 2004a. Valtionhallinnon keskeisten tietojärjestelmien turvaaminen Vahti 5/2004. Edita Prima Oy, Helsinki.

Valtiovarainministeriö 2004b. Haittaohjelmilta suojautumisen yleisohje (VAHTI 3/2004). Edita Prima Oy, Helsinki.

Valtiovarainministeriö 2007. Älypuhelimien tietoturvallisuus – hyvät käytännöt. Vahti 2/2007. Edita Prima Oy, Helsinki.

Valtiovarainministeriö 2008. Tärkein tekijä on ihminen – henkilöstöturvallisuus osana tietoturvallisuutta. Vahti 2/2008. Edita Prima Oy, Helsinki.

Valtiovarainministeriö 2009a. Vahti-ohjeet. Fyysinen turvallisuus. Internet-sivut. Luettu 20.3.2014. https://www.vahtiohje.fi/web/guest/fyysinen-turvallisuus

Valtiovarainministeriö 2009b. Vahti-ohjeet. Laitteistoturvallisuus. Internet-sivut. Luettu 20.3.2014. https://www.vahtiohje.fi/web/guest/laitteistoturvallisuus

Valtiovarainministeriö 2009c. Vahti-ohjeet. Tietoliikenneturvallisuus. Internet-sivut. Luettu 20.3.2014. https://www.vahtiohje.fi/web/guest/tietoliikenneturvallisuus

Valtiovarainministeriö 2009d. Vahti-ohjeet. Tietoaineistoturvallisuus. Internet-sivut. Luettu 20.3.2014. https://www.vahtiohje.fi/web/guest/tietoaineistoturvallisuus

Valtiovarainministeriö 2009e. Valtioneuvoston periaatepäätös valtionhallinnon tietoturvallisuuden kehittämisestä 26.11.2009. Edita Prima Oy, Helsinki.

Valtiovarainministeriö 2009f. Vahti-ohjeet. Käyttöturvallisuus. Internet-sivut. Luettu 20.3.2014. https://www.vahtiohje.fi/web/guest/kayttoturvallisuus1

Viestintämarkkinalaki 393/2003. Helsinki. Liikenne- ja viestintäministeriö. 25.7.2003.

Viestintävirasto 2013. Tietoturva. Laitteen turvallinen käyttö: Matkapuhelin. Internet-sivut. Luettu 20.3.2014. https://www.viestintavirasto.fi/tietoturva/laitteenturvallinenkaytto/matkapuhelin.html

**Haastattelut:**

Alonen-Kinnunen, Kirsi 2014. Sosiaalijohtaja. Kinnulan kunta. Haastattelu: 7.2.2014.

Hämäläinen, Hannu 2014. Ylilääkäri. Kinnulan kunta. Haastattelu: 7.2.2014.

Kinnunen, Ossi 2014. Kunnanrakennusmestari. Kinnulan kunta. Haastattelu: 4.3.2014.

Muhonen, Marko 2014. Kasesoft Oy. Kinnulan kunnan IT-palveluntuottaja. Haastattelu: 5.3.2014.

Piispanen, Minna 2014. Tietosuojavastaava, perusturvatoimiala. Kinnulan kunta. Haastattelu: 14.1.2014.

Viinikainen, Leena 2014. vs. Johtava hoitaja. Kinnulan kunta. Haastattelu: 14.1.2014.