jamk.fi

Tietoturvatyön kehittäminen

Johanna Myllymäki

Opinnäytetyö
Marraskuu 2014

Tietotekniikan koulutusohjelma
Tekniikan ja liikenteen ala

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Myllymäki, Johanna	Opinnäytetyö	18.11.2014
	Sivumäärä 39	Julkaisun kieli Suomi
		Verkkojulkaisulupa myönnetty: x

Työn nimi
Tietoturvatyön kehittäminen

Koulutusohjelma
Tietotekniikan koulutusohjelma

Työn ohjaaja(t)
Kotikoski, Sampo; Häkkinen, Antti

Toimeksiantaja(t)
Muuramen kunta

Tiivistelmä

Opinnäytetyö on tehty Muuramen kunnalle. Opinnäytetyön tavoitteena oli luoda Muuramen kunnalle tietoturvapolitiikka ja tietoturvaohjeita.

Työn teoriaosuudessa selvitetään tietoturvan perusteita, tietoturvastandardeja, tietoturvan johtamista, suunnittelua sekä tietoturvapolitiikan perusteita.

Työn toteutusosassa Muuramen kunnalle tehtiin luonnos tietoturvapolitiikasta. Tietoturvaohjeista toteutettiin henkilöstön tietoturvaohje, mobiilikäyttäjän tietoturvaohje sekä tietoturvaan liittyviä toimintaohjeita eri tilanteisiin.

Tietoturvapolitiikka ja tietoturvaohjeet tehtiin soveltuvin osin VAHTI-ohjeiden ja tietoturvastandardien pohjalta.

Avainsanat (asiasanat)

Standardit, Tietoturvallisuus, Tietoturvapolitiikka

Muut tiedot

JYVÄSKYLÄN AMMATTIKORKEAKOULU
JAMK UNIVERSITY OF APPLIED SCIENCES

Description

Author(s)	Type of publication	Date
Myllymäki, Johanna	Bachelor´s Thesis	18.11.2014
	Number of pages 39	Language of publication Finnish
		Permission for web publication: x

Title of publication

Development of Information Security work

Degree programme

Information Technology

Tutor(s)

Kotikoski, Sampo; Häkkinen, Antti

Assigned by

Municipality of Muurame

Abstract

The purpose of this thesis was to create information security policy and information security instructions for Muurame municipality. The thesis was assigned by Muurame municipality.

The theoretical part of the thesis consists of information security fundamentals, standards, information security management,- planning and information security policy fundamentals.

Information security policy and instruction have been created based on VAHTI guidelines and instructions.

As a result of the thesis information security policy draft, information security instructions for the employees of the organization and information security guidelines for handheld users have been succesfully created for the use of the staff of Muurame municipality.

Keywords/tags (subjects)

Information security, Standards, Information security policy

Miscellaneous

Sisältö

Kuviot

1 Työn lähtökohdat

1.1 Toimeksiantajan esittely

Muuramen kunta sijaitsee Pohjois-Päijänteen länsipuolella, ja sitä ympäröivät kunnista Jyväskylä ja Toivakka. Muuramen kunnan asukasmäärä on noin 9600. Muuramen kunta itsenäistyi vuonna 1921, kun se irtosi Korpilahdesta. Muuramen kunnan arvot ovat luotettava, avoin, luova ja rohkea. Muurame tunnetaan yrittäjäystävällisyydestä. Suurimmat työnantajat ovat Harvia Oy, Nokka-yhtiöt Oy, John Crane Safematic Oy, Kytölä Oy, SKF Oy Ab, Muuratpuu Pohjonen Oy, HK-Instuments Oy, Sten & Co Oy Ab, Muuramen kunta, Kinkomaan sairaala, terveyskeskus ja Muuramen seurakunta. (Muurame Info n.d.)

Muuramen kunta on yksi Muuramen merkittävimmistä työllistäjistä. Henkilöstömäärä oli vuoden 2013 lopussa 438 henkilöä. Eniten henkilöstöä on lapsi- ja perhepalveluiden palvelualueella. Sen henkilöstömäärä on 192. Asukaspalveluiden palvelualueen henkilöstömäärä on 140, teknisissä palveluissa 88 ja hallinto- ja talouspalveluissa 18. Ammattiryhmittäin tarkasteltuna suurimmat ammattiryhmät ovat opetushenkilökunta 39% ja päivähoitohenkilökunta 21%. (Muuramen kunnan henkilöstökertomus 2013, 4-5.)

1.2 Toimipisteet ja palvelut

Muuramen kunnan toimipisteitä sijaitsee ympäri Muuramea. Virastotalo sijaitsee Muuramen keskustassa Virastotiellä, siellä työskentelee lähes 70 henkilöä. Virastotalolla toimivat mm. talous- ja hallintopalvelukeskus, tekniset palvelut, sosiaalipalvelut ja varhaiskasvatuspalvelut. Eniten työntekijöitä on koulunmäellä, jossa sijaitsevat peruskoulu ja lukio: Mäkelänmäen koulu on alakoulu, Nisulanmäen koulu on yläkoulu sekä Muuramen lukio. Kinkomaalla, Niittyahossa ja Isolahdessa sijaitsevat alakoulut.

Kunnallisia päiväkoteja Muuramessa on kaksi: Rajalan päiväkoti Rajalassa ja päiväkoti-korttelikoulu Leikari Tervamäessä. Lisäksi ryhmäperhepäivähoitopaikkoja on kuusi, ja ne sijaitsevat eri puolella Muuramea. Muuramen kunnan pääkirjasto sijaitsee virastotalon yhteydessä Virastotiellä. Niittyahon sivukirjaston toimipaikka on Niittyahon alakoulun yhteydessä. Muuramen keskustassa sijaitsee Koskikoti, joka tarjoaa asumispalveluja ikääntyville. Samoissa tiloissa toimivat kotipalvelun ja vammaispalvelun toimistot. Muuramen työpaja toimii Ratastiellä, sen tavoitteena on edistää nuorten ja erittäin pitkään työttömänä olleiden henkilöiden yksilöllisiä keinoja työllistymiseen ja koulutukseen. Nuorisotilat ja nuorisotyöntekijöiden toimisto sijaitsevat Muuramentiellä Y4-talolla.

Lapsi- ja perhepalveluiden lautakunnan alaisuudessa toimii lapsi- ja perhepalvelualue. Sen ydinprosesseja ovat mm. varhaiskasvatus, perusopetus, toisen asteen koulutus, taiteen perusopetus, lasten ja perheiden hyvinvointipalvelut sekä nuorisotyö. Asukaspalveluiden lautakunnan palvelualueen tehtäväalueet ovat asukaspalveluiden hallinto, vanhus- ja vammaispalvelut, aikuissosiaalityö, vapaa-aikapalvelut sekä terveydenhuollon palvelut. Teknisten palveluiden lautakunnan palvelualueen vastuulla ovat mm. maankäytön ja rakentamisen suunnittelu, mittaustoimi, rakennusvalvonta, ympäristönsuojelu, palo- ja pelastustoimi, kadut, yksityistiet, puistot, ulkoilu- ja urheilualueet, kiinteistöt, ruokahuolto, siivous, vesihuolto ja jätehuolto. (Muuramen kunnan talousarvio vuodelle 2014 ja taloussuunnitelma vuosille 2015-2016, 43, 70, 106.)

Kaikissa toimipaikoissa on nopeat tietoliikenneyhteydet ja suurin osa toimipisteistä on yhdistetty Muuramen kunnan tietoverkkoon, jolloin työntekijät saavat käyttöönsä tarvittavat keskitetyt verkkopalvelut, joita ovat mm. verkkolevylle tallennus ja verkkosovellukset.

1.3 Tehtävät ja tavoitteet

Muuramen kunnalla ei ole virallista tietoturvapolitiikkaa eikä kaikkia tarvittavia virallisia tietoturvaohjeita, osa ohjeista on vanhentuneita ja ne tulee päivittää vastaamaan nykytilannetta. Opinnäytetyön tavoitteena oli laatia koko organisaation kattava tietoturvapolitiikka sekä tarvittavat tietoturvaohjeet, joita olivat

mm. mobiililaitteiden tietoturvaohje ja henkilöstön tietoturvaohje. Ohjeistuksen laatimisen tavoitteena oli täsmentää toimintatapoja tietoturvan suhteen, lisätä työntekijöiden tietoturvatietoisuutta ja painottaa tietoturvan merkityksen ymmärtämistä jokapäiväisessä työskentelyssä. Tietoturvan ollessa todella laaja kokonaisuus tuli työn rajaaminen tehdä tarkasti. Rajallisen käytettävissä olevan ajan puitteissa tietoturvapolitiikan ja ohjeistuksen sekä tietojärjestelmäkuvauksien katsottiin olevan riittävä. Jo näistä valituista aiheista olisi ollut paljon enemmänkin kirjoitettavaa. Työn teoriaosuudessa käydään läpi mm. tietoturvan perusteita, riskienhallintaa ja tietoturvallisuuden johtamista. Varsinaista uhkakartoitusta ja siihen liittyvää riskienhallintaa ei otettu osaksi tätä opinnäytetyötä, vaan se tehdään myöhemmässä vaiheessa.

Tietoturvapolitiikan laatimiseen osallistuivat mm. ATK-käyttöpäällikkö, ATK-tukihenkilöt sekä toimialajohtajat. Tarvittaessa tietoa kerättiin myös toimialojen työntekijöiltä. Henkilöstön tietoturvaohjeen laativat lähinnä ATK-tuen työntekijät, apuna käytetään mm. VAHTI-ohjeita, joita käytettiin soveltuvin osin. Laaditut ohjeet lisättiin Muuramen kunnan Intranet-sivuille, joista ne ovat koko henkilöstön saatavissa. Samalla uudistettiin ja päivitettiin Intranetissä olevat tietoturva-sivut.

Toimeksiantajan vaatimukset tietoturvan suhteen

Julkisuuslainsäädännön mukaan tieto on julkista, ellei sitä ole erikseen määritelty salaiseksi julkisuuslain tai muiden säädösten perusteella. Julkishallinnossa käsitellään julkista ja salassa pidettävää tietoa. Suomen lainsäädännössä on paljon tietoturvavelvoitteita. Tietoturvallisuus perustuu viranomaisten toiminnan julkisuudesta annetun lain (621/1999) ja asetuksen (1030/1999) lisäksi useisiin muihin lakeihin. Valtioneuvoston asetuksessa tietoturvallisuudesta valtionhallinnossa (681/2010) määrätään tietoaineistojen käsittelystä sekä perus-, korotetun ja korkean tietojenkäsittely-ympäristön toteuttamisesta. (VAHTI 4/2013, 19.)

VAHTI-ohjeeseen nimeltä Henkilöstön tietoturvaohje (Vahti 4/2013) on koottu joitakin keskeisiä laeissa asetettuja tietoturvavelvoitteita:

- *Viranomaisen tulee hyvän tiedonhallintatavan luomiseksi ja toteuttamiseksi huolehtia asiakirjojen ja tietojärjestelmien sekä niihin sisältyvien tietojen asianmukaisesta saatavuudesta, käytettävyydestä ja suojaamisesta sekä eheydestä ja muista tietojen laatuun vaikuttavista tekijöistä.* (Laki viranomaisten toiminnan julkisuudesta 18 §, Hyvä tiedonhallintatapa).

- *Rekisterinpitäjän on toteutettava tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä.* (Henkilötietolaki 32 §, Tietojen suojaaminen).

- *Salassa pidettävät asiakirjat tai niihin sisältyvät tiedot voidaan luokitella sen mukaan, minkälaisia tietoturvallisuutta koskevia vaatimuksia niiden käsittelyssä on tarpeen noudattaa. Luokittelu voidaan suorittaa myös siten, että tietoturvallisuutta koskevat vaatimukset kohdistetaan vain sellaisiin asiakirjoihin tai sellaisiin asiakirjan käsittelyvaiheisiin, joissa erityistoimenpiteet ovat suojattavan edun vuoksi tarpeen.* (Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa 8 §, Luokituksen perusteet).

2 Tietoturvallisuuden perusteet

2.1 Tietoturvan määritteleminen

Tietoturva-käsitettä ei voi määritellä yhdellä lauseella. Tietoturva koostuu useista eri tekijöistä, joiden yhteisvaikutuksella tietoturvallisuus saavutetaan. Perinteisesti tietoturvan katsotaan koostuvan kolmesta tiedon (sekä tietojärjestelmien, tietoaineistojen ja palveluiden) perustekijästä: luottamuksellisuudesta, eheydestä ja käytettävyydestä. (Hakala, Vainio & Vuorinen 2006, 4.)

- *Luottamuksellisuudella* tarkoitetaan sitä, että tietoja ja tietojärjestelmiä saavat käyttää ainoastaan siihen oikeutetut henkilöt työtehtävien vaatimalla tavalla. Se varmistetaan käyttäjätunnuksin ja salasanoin. Tiedot ja järjestelmät tulee suojata sivullisten mahdollisuudelta käsitellä, muuttaa tai poistaa tietoja. Arkaluontoisen tiedon suojaamiseen voidaan

käyttää salakirjoitusmenetelmiä. (Hakala ym. 2006, 4; Vahti 4/2013, 17.)

- *Eheydellä* tarkoitetaan tietojen paikkansapitävyyttä, oikeellisuutta ja ajantasaisuutta. Tiedot eivät saa paljastua, muuttua tai tuhoutua hallitsemattomasti asiattoman toiminnan tai häiriöiden vuoksi. Tietoja suojataan mm. ohjelmointiteknisin ratkaisuin, esimerkiksi käyttämällä syöttörajoitteita ja tarkistuksia. (Hakala ym. 2006, 4-5.)

- *Käytettävyydellä* tarkoitetaan sitä, että tiedot, järjestelmät ja palvelut ovat käytettävissä oikeassa muodossa ajasta ja paikasta riippumatta. Sähköisiä palveluja käyttäessä käyttäjätunnistus on tärkeässä asemassa, samoin tapahtumienvalvonta. Käytettävyys taataan myös käyttämällä riittävän tehokkaita ja tarpeeseen sopivia laitteistoja ja järjestelmiä. Järjestelmistä saatavan tiedon tulee olla riittävän pitkälle jalostettua eli käyttäjän tulee saada tieto tarvitsemassaan muodossa. (Hakala ym. 2006,4-5; Vahti 4/2013, 17.)

Hakala ja muut (2006, 5-6) laajentavat kirjassaan edellä kuvattua tietoturvan määritelmää kirjassaan kahdella osatekijällä: kiistämättömyydellä ja pääsynvalvonnalla.

- *Kiistämättömyydellä* tarkoitetaan mm. tietojärjestelmän kykyä tunnistaa ja tallentaa luotettavasti käyttäjän tiedot.

- *Pääsynvalvontaan* kuuluvat mm. ne toimet, joilla rajoitetaan tietojenkäsittelyinfrastruktuurin käyttöä muuhun kuin työkäyttöön. (Hakala ym. 2006, 5-6.)

ISO 17799 -standardin tietoturvallisuuden määritelmässä tieto kuvataan olevan mm. asianmukaisesti suojattava kohde, joka on tärkeä muiden liiketoiminnallisten kohteiden lisäksi. Informaatio voi esiintyä painettuna tai paperille kirjoitettuna, sähköisesti tallennettuna, postin kuljettamana tai sähköisesti välitettynä ynnä muussa muodossa. (SFS-ISO/IEC 17799 2006, 14.)

VAHTI-ohjeessa Henkilöstön tietoturvaohje (Vahti 4/2013) kuvataan tietoturvallisuuden tärkeyttä mm. seuraavasti: tietoturvallisuus on tärkeää, koska sillä turvataan yksilön, yhteisön ja yhteiskunnan etuja, siksi tietoturvallisuus on yhteiskunnan toimintojen, palvelujen, sovellusten ja tietoteknisen infrastruktuurin perusedellytys.

2.2 Tietoturvan osa-alueet

Tietoturvallisuus koostuu useasta eri osa-alueesta, joita ovat hallinnollinen-, henkilöstö-, tietoaineisto-, fyysinen-, laitteisto-, ohjelmisto- ja tietoliikenneturvallisuus sekä käyttöturvallisuus ja haittaohjelmilta suojautuminen. Kaikkien osa-alueiden tulee olla kunnossa hyvän tietoturvatason saavuttamiseksi. Tietoturvallisuuden jakaminen eri osa-alueisiin helpottaa laajan kokonaisuuden käsittelemistä.

2.2.1 Hallinnollinen turvallisuus

Hallinnollisen turvallisuuden tarkoituksena on varmistaa tietoturvan kehittäminen ja johtaminen. Tietoturvallisuuden johtamisen on lähdettävä liikkeelle yrityksen johdosta. Hallinnollisesta tietoturvallisuudesta vastaa yleensä tietohallinto. Hallinnolliseen turvallisuuteen liittyy myös yhteydenpito muihin turvallisuudesta vastaaviin tahoihin, niin organisaation sisä- ja ulkopuolella. (Hakala ym. 2006, 10.)

VAHTI-ohjeessa Valtionhallinnon keskeisten tietojärjestelmien turvaaminen (Vahti 5/2004), on koottuna mm. seuraavia kohtia vaatimuksineen ja kuvauksineen:

- Tietoturvastrategia; johdon linjaamat tietoturvallisuuden tavoitteet.
- Tietoturvapolitiikka; johdon dokumentoimat ja tiedottamat näkemykset tietoturvallisuuden merkityksestä, periaatteista ja toteutuksesta.
- Tietojen omistajuus; tiedoille on nimetty vastuuhenkilö, joka vastaa tietojen eheydestä.

- Käytettävyydestä ja luottamuksellisuudesta.

- Dokumentointi; järjestelmät, prosessit, tietoturvaratkaisut ja niiden perustelut, toimintaperiaatteet, suunnitelmat ja käytännöt on dokumentoitu.

2.2.2 Henkilöstöturvallisuus

Henkilöstöturvallisuus koskee kaikkia organisaatiossa työskenteleviä työntekijöitä. Sen avulla työntekijöille luodaan edellytykset tietojärjestelmien käyttöön sekä rajataan tietojärjestelmien käyttöä mm. antamalla käyttöoikeudet vain työntekijän tarvitsemiin tietoihin. Varamiesjärjestelyillä varmistetaan toimintojen jatkuminen työntekijän poissaolotilanteessa. Tietojärjestelmiin annetaan koulutusta, jotta työntekijät voivat käyttää niitä. Lisäksi henkilöstöturvallisuuteen katsotaan kuuluvaksi tietojärjestelmien vastuiden ja oikeuksien määritteleminen. Vastuullisena toimijana tietohallinnon lisäksi toimii yleensä henkilöstöhallinto. Henkilöstöturvallisuus sisältää toimenpiteet, joilla estetään henkilöstöön kohdistuvia uhkia sekä henkilöstöstä johtuvia uhkia. Esimerkkeinä ovat henkilön taustatietojen selvittäminen (kuten rikosrekisteritiedot), tarkat työnkuvaukset ja vaitiolovelvollisuus. (Hakala ym. 2006, 11.)

Aiemmin mainitussa Vahti-ohjeessa Valtionhallinnon keskeisten tietojärjestelmien turvaaminen (Vahti 5/2004) on mm. seuraavia vaatimuksia kuvauksineen:

- Dokumentoidut tulo- ja lähtöprosessit; mm. työhönotto ja työsuhteen päättäminen tapahtuvat etukäteen dokumentoidun prosessin mukaisesti.

- Kirjallinen toimenkuva; työntekijän työtehtäväkuvaus sisältää tehtävät, vastuut, oikeudet ja velvollisuudet.

2.2.3 Tietoaineistoturvallisuus

Tietoaineistoturvallisuus sisältää tietojen säilyttämiseen, varmistamiseen, palauttamiseen ja tuhoamiseen liittyvät toimenpiteet. Aineistoihin lasketaan kuuluvaksi manuaalisen tietojenkäsittelyn asiakirjat sekä ATK-tulosteet. (Hakala ym. 2006, 11.)

Vahti-ohjeeseen (Vahti 5/2004, 79-80) on koottu mm. seuraavia vaatimuksia kuvauksineen tietoaineistoturvallisuuteen liittyen

- Pääsyn rajaaminen vain työntekijän tarvitsemiin tietoihin.
- Käyttöoikeusprosessit; käyttöoikeuksien myöntämisessä noudatetaan dokumentoituja prosesseja.
- Tietovälinepolitiikka; erityisesti siirrettävien tallennusvälineiden käyttäminen ja käyttörajoitukset on ohjeistettu.
- Tietoaineiston turvallinen hävitys; turvallinen ja luokituksen mukainen hävitys on ohjeistettu.
- Tietosuoja; henkilötietolakia tulee noudattaa käsiteltäessä henkilötietoja, tulee huomioida henkilötietokäsitteen laajuus.

2.2.4 Fyysinen turvallisuus

Fyysiseen turvallisuuteen kuuluvat tilojen ja laitteiden turvaaminen. Toteutuksessa käytetään esimerkiksi kulunvalvontaa (tunnistekortit omalle henkilöstölle ja vierailijoille), kameravalvontaa, lukitusta ja mekaanista suojaamista. Laitteet tulee olla suojattu ilkivallalta sekä mahdollisilta vesi- ja palovahingoilta. Myös sähkönsaantiin liittyviin poikkeuksiin tulee varautua. Esimerkkinä palvelinhuoneen fyysisestä turvallisuudesta voidaan mainita kulunvalvonta, lukitus, UPS (Uninterruptible Power Supply, varautuminen sähkönsyötön häiriöihin, kuten sähkökatkot ja virtapiikit). Fyysisestä turvallisuudesta vastaa yleensä kiinteistöhuolto, mutta esimerkiksi palvelintilojen fyysisen turvallisuuden suunnitteluun osallistuu yleensä myös tietohallinto. (Hakala ym. 2006, 11.)

2.2.5 Laitteistoturvallisuus

Laitteistoturvallisuuteen katsotaan kuuluvaksi tietokoneiden sekä tietoverkon laitteiden asianmukainen mitoittaminen, huolto, ylläpito sekä testaus. Myös laitteiden elinkaaren hallinta on huomioitava eli varaudutaan laitteiden kulumiseen ja vanhenemiseen. Laitteiden käytöstä johtuviin mahdollisiin vaaratekijöihin tulee varautua, kuten sähköiskut. Vaaraa tulee arvioida ja minimoida. (Hakala ym. 2006, 12.)

2.2.6 Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella varmistetaan organisaation käytössä olevien ohjelmistojen tarkoituksenmukaisuus, yhteensopivuus toisten ohjelmistojen kanssa, ohjelmatoimintojen luotettavuus ja virheettömyys sekä laillisuus. Uusien ohjelmistojen käyttöönottoon tulee kuulua testaus, ohjattu asetusten hallinta ja päivitykset. Ohjelmistojen ylläpitoon kuuluvat myös ohjelmistoversioiden- ja lisenssien hallinta. Ohjelmistoturvallisuus on organisaation tietohallinnon vastuulla. (Hakala ym. 2006, 12.)

2.2.7 Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan toimia, joilla pyritään saavuttamaan tietoliikenteen turvallisuus. Keinoina ovat mm. laitteistojen ja siirtoyhteyksien ylläpito, kokoonpanojen- ja verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen. Tietoliikenneturvallisuuteen kuuluvat myös tietoliikennetoimintojen ja järjestelmien suunnitteleminen ja rakentaminen hyvän tiedonhallintatavan mukaisesti, niin että siirrettävän tiedon eheys, luottamuksellisuus ja saatavuus säilyvät. (Andreasson & Koivisto 2013, 69.)

VAHTI-ohjeessa Valtionhallinnon keskeisten tietojärjestelmien turvaaminen (Vahti 5/2004, 54-55) on useita eri vaatimuksia tietoliikenneturvallisuuden toteuttamiseksi, seuraavaksi on koottu niistä muutamia:

- Dokumentointi; tietoliikenneyhteyksistä on oltava ajan tasalla olevat dokumentaatiot.

- Aktiivilaitteiden suojaus ja asetukset; laitteet on sijoitettava fyysisesti turvattuihin tiloihin, konfiguraatioiden tulee minimoida tunkeutumisen riskit.

- Ulkoisten yhteyksien turvaaminen; tietoliikenneyhteyksien tulee olla pitkälti vikasietoisia, niille on oltava varajärjestelyt. Lisäksi tärkeimmille tietoliikenneyhteyksille tulee olla varajärjestelyt.

- Tunkeutumisen havaitsemis- ja estämisjärjestelmä; tietoverkossa on oltava mekanismit tunkeutumisen havaitsemista ja estämistä varten.

2.2.8 Käyttöturvallisuus ja haittaohjelmilta suojautuminen

Hakalan ym. (2006, 12) mukaan joissakin esityksissä mukaan on otettu lisäksi käyttöturvallisuus, mutta kirjoittajat toteavat, että järjestelmän käytöstä aiheutuvat riskit ja niihin varautuminen kannattaa sisällyttää kaikkiin edellä mainittuihin osa-alueisiin.

Käyttöturvallisuuteen kuuluvat mm. käyttöoikeuksien hallinta; käyttäjille annetaan vain tarvittavat käyttöoikeudet tietoihin ja tietojärjestelmiin, käytön ja lokien valvonta, toiminnan valvonta, varmuuskopiointi ja häiriöraportointi. Lisäksi tietojärjestelmät tulee suojata haittaohjelmia vastaan. (Tietoturva – Kunnat.net, 2014)

2.3 Standardit, VAHTI-ohjeet ja JHS-suositukset

2.3.1 Yleistä

Standardointijärjestöt luovat tietoturvastandardeja tietoturvallisuuden jäsentämisen ja organisoimisen avuksi. Kansainvälisiä standardointijärjestöjä ovat maailmanlaajuisella tasolla mm. ISO (International Organization for Standardization) ja kansallisella tasolla mm. SFS (Suomen Standardisoimisliitto SFS ry).

Tunnetut standardit ovat useiden eri tahojen arvioimia, joten asioita käsitellään niissä laaja-alaisesti ja asiantuntevasti. Organisaation käyttäessä standardeja toimiensa ohjenuorana, voidaan varmistua siitä, että kaikki oleelliset tietoturvan osa-alueet on otettu huomioon. Tavoitteena voidaan pitää sitä, että tietoturvallisuus tulee kiinteäksi osaksi organisaation jokapäiväistä toimintaa ja liiketoimintaprosesseja. Sen lisäksi toiminnan tulee muotoutua määrämuotoiseksi. (Laaksonen, Nevasalo & Tomula 2006, 104.)

2.3.2 Standardien hyödyntäminen

Läheskään aina ei ole tarpeellista eikä järkevää ryhtyä noudattamaan vain tiettyä standardia. Hyvä käytännön tapa on valita muutama soveltuva standardi tai toimintamalli ja poimia niistä oman organisaation tai yrityksen toimintaan parhaiten soveltuvat osa-alueet. Näin toimien organisaatioon saadaan luotua tarpeenmukainen oma tietoturvallisuusstandardi, jota voidaan käyttää organisaation sisäisen toiminnan ja auditointien vaatimusmäärittelynä.

ISO 17799 -standardissa todetaankin, että sitä voidaan pitää organisaatiokohtaisten ohjeiden kehittämisen lähtökohtana, eivätkä välttämättä kaikki turvamekanismit ja ohjeet ole sovellettavissa.

Tässä opinnäytetyössä hyödynnetään eri standardeja ja toimintamalleja poimimalla niistä toimeksiantajan tarpeisiin soveltuvat kohdat.

2.3.3 ISO/IEC 27001

ISO 27001 on kansainvälinen standardi, joka rakentuu tietoturvallisuuden hallintajärjestelmän (Information Security Management System) ympärille. Standardissa esitetään tietoturvallisuuden hallintajärjestelmälle vaatimuksia sen luomiseen, toteuttamiseen, ylläpitämiseen ja jatkuvaan parantamiseen. Organisaation tarpeet vaikuttavat tietoturvallisuuden hallintajärjestelmän luomiseen ja toteuttamiseen. Standardissa esitetyt vaatimukset ovat yleisluonteisia, joten ne ovat soveltuvia useanlaisille ja kaikenkokoisille organisaatioille.

Tietoturvallisuuden hallintajärjestelmän avulla suojataan tiedon luottamuksellisuutta, eheyttä ja saatavuutta riskienhallintaprosessin avulla. Standardin käyt-

tö on viesti ulkoisille sidosryhmille organisaation halusta ja kyvystä täyttää sen omat tietoturvavaatimukset. Standardiin sitoutumista voidaankin pitää kilpailuetuna. ISO/IEC 27001 -standardi on luonteeltaan sitova: jos organisaatio ilmoittaa noudattavansa standardia, sen on noudatettava standardin kohdissa 4-10 esitetyt vaatimukset. (SFS-ISO/IEC 27001 2013, 6-8.)

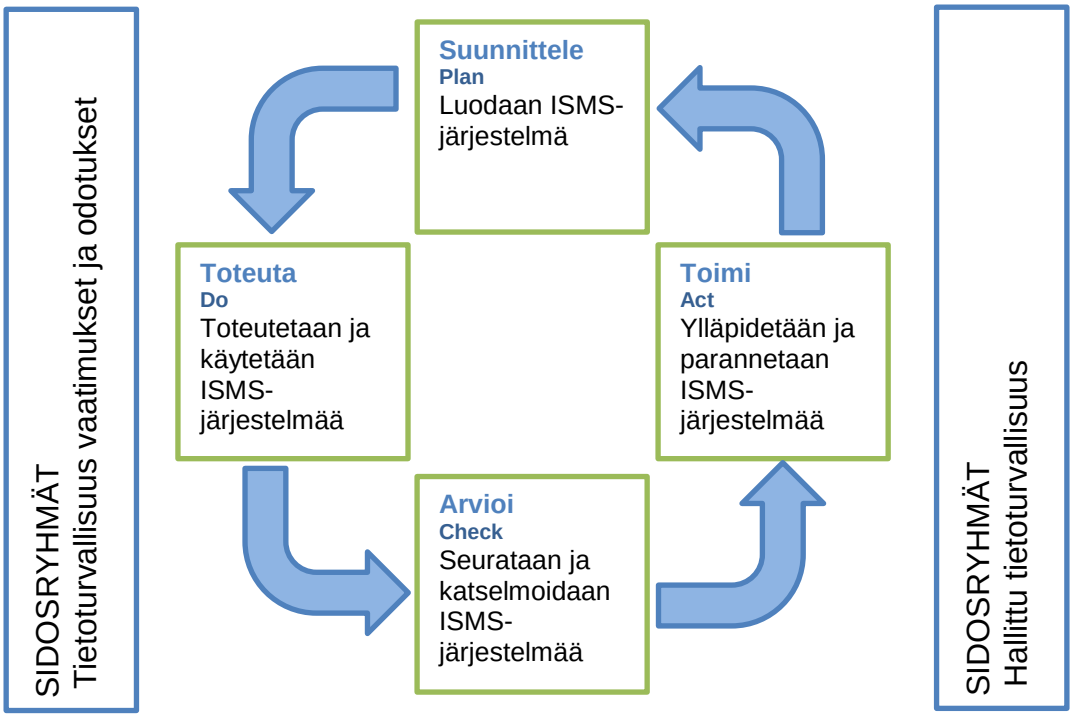
ISO/IEC 27001 -standardia on uusittu vuonna 2013. Uudistettu standardi vastaa paremmin identiteettivarkauksiin, langattomien laitteiden ja muihin verkon haavoittuvuuksiin liittyviin uhkiin. Lisäksi siinä on huomioitu nykyajan vaatimuksia liittyen sosiaalisen median, älypuhelinten ja taulutietokoneiden tietoturvan hallintaan ja ongelmien ennaltaehkäisyyn. Tietoturvatarkastukset on koottu standardin liitteeseen A. Uusittu standardi soveltuu entistä paremmin käytettäväksi muiden ylimmän tason hallintajärjestelmien kanssa. Myös riskienhallinta on uudistetussa versiossa paremmin esillä. (Uusi versio tietoturvastandardista ISO/IEC 27001 2013.)

Standardissa on seitsemän eri osa-aluetta, joita tarkastellaan yksityiskohtaisesti. Osa-alueet ovat organisaation toimintaympäristö, johtajuus, suunnittelu, tukitoiminnot, toiminta, suorituskyvyn arviointi ja parantaminen.

Standardissa painotetaan prosessimaista toimintamallia. Sitä on noudatettava kehittäessä, toteuttaessa, käytettäessä, valvoessa, katselmoidessa, ylläpidettäessä ja parannettaessa tietoturvajärjestelmää. Prosessi -termi kuvataan olevan resursseja käyttävää johdettua toimintaa, jonka tarkoituksena on panosten muuttaminen tuotoiksi. Usein yhden prosessin tuotos muodostaa suoraan panoksen uudelle prosessille. (SFS-ISO/IEC 27001:2005 2005, 6.)

PDCA-malli

ISO/IEC 27001 -standardin mukaan tietoturvallisuuden hallintajärjestelmää kehitetään prosessimaisesti. Kaikkia vaiheita seurataan ja kehitetään säännöllisesti prosessin mukaisesti. Kuviossa 1 on esitetty PDCA-mallin eri vaiheiden liittyminen toisiinsa ja sidosryhmien vaikutukset.



Kuvio 1. PDCA-mallin prosessit (ISO/IEC 27001:2005)

- Plan – Suunnittele
  Luodaan tietoturvallisuuden hallintajärjestelmä; määritellään organisaation tietoturvapolitiikka, -tavoitteet, -päämäärät, -prosessit ja menettelytavat, jotka ovat oleellisia riskien hallinnalle ja tietoturvallisuuden kehittämiselle organisaation yleisen politiikan ja tavoitteiden mukaisesti.

- Do – Toteuta
  Toteutetaan ja käytetään tietoturvallisuuden hallintajärjestelmää, noudatetaan tietoturvapolitiikkaa, turvamekanismeja, prosesseja ja menettelytapoja.

- Check – Arvioi
  Seurataan ja arvioidaan tietoturvallisuuden hallintajärjestelmää mittaamalla prosessien suorituskykyä, verrataan tuloksia tietoturvapolitiikkaan ja tavoitteisiin. Raportoidaan tuloksista johdolle katselmointia varten.

- Act – Toimi
  Ylläpidetään ja parannetaan tietoturvallisuuden hallintajärjestelmä, ryhdytään korjaaviin ja ehkäiseviin toimenpiteisiin, jos sisäisen auditoinnin tai johdon katselmusten tulokset näin vaativat.

Tietoturvallisuuden hallintajärjestelmän käyttäminen on prosessimaista, jatkuvaa työtä. Tuloksia tulee tarkastella jatkuvasti ja tarvittavat muutokset ja toimenpiteet on suoritettava poikkeamien ehkäisemiseksi. (SFS-ISO/IEC 27001:2005, 2005, 8.)

Muita 27000 -sarjan standardeja
ISO/IEC 27001 -standardia voidaan kuvata vaatimusstandardiksi, jota vasten organisaatio voi sertifioida toimintaansa, ISO/IEC 27002 standardissa kuvataan miten ISO/IEC 27001 -standardin vaatimuksiin voidaan päästä (Andreasson & Koivisto 2013, 37).

2.3.4 ISO/IEC 17799

Standardi BS 7799 eli British Standard 7799: Code of Practice for Information Security, on kaksiosainen standardi, jonka osat ovat BS 17799-1 ja BS 17799-2. ISO 17799 -standardi käsittelee ensimmäisen osan asiat.

Standardissa määritellään ohjeita ja yleisiä periaatteita organisaation tietoturvahallinnan käynnistämiseen, käyttöönottoon, ylläpitoon ja parantamiseen. Standardissa kuvailtuja tavoitteita voidaan käyttää ohjenuorana haluttaessa saavuttaa yleisesti hyväksyttyjä tietoturvan tavoitteita. Standardiin on koottu valvontatavoitteita ja turvamekanismeja, joita voidaan hyödyntää riskiarvioinnissa. Organisaatiot voivat käyttää standardia käytännön ohjeistuksena kehittäessään omia turvallisuusstandardeja ja turvallisuusjohtamisen käytäntöjä,

lisäksi se auttaa lisäämään luottamusta organisaation välisissä liiketoimissa. (SFS-verkkokauppa – Standardit kätevästi netistä.)

2.3.5 VAHTI-ohjeet

Valtiovarainministeriö on asettanut Valtionhallinnon tieto- ja kyberturvallisuuden johtoryhmän (VAHTI) julkisen hallinnon tietoturvallisuuden kehittämisen, ohjauksen ja yhteistyön elimeksi. VAHTIn tavoitteena on tieto- ja kyberturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista. Tavoitteena on myös edistää tieto- ja kyberturvallisuuden sekä ICT-varautumisen saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta sekä tietojärjestelmien, tietoverkkojen ja ICT-palvelujen kehittämistä, ylläpitoa ja käyttöä. (Tietoturvallisuus.)

VAHTIn tietoturvaohjeisto on yksi maailman kattavimmista yleisistä tietoturvaohjeistoista. VAHTI-ohjeita käytetään hallinnon lisäksi laajasti hyväksi myös kansainvälisessä tietoturva- ja yhteistyössä, elinkeinoelämässä, yrityksissä ja kunnissa sekä opetus- ja kansalaistoiminnassa. VAHTI-ohjeiden laatimiseen on osallistunut laaja joukko asiantuntijoita, joten ohjeet ovat hyvin kattavia.

Voimassa olevia VAHTI-ohjeita on saatavissa vuodesta 2000 alkaen. Ohjeita julkaistaan noin 2-5 vuodessa. Viimeisimmät ohjeet ovat vuodelta 2013, ne ovat päätelaitteiden-, henkilöstön-, toimitilojen ja sovelluskehityksen tietoturvaohjeet. VAHTI-ohjeita on saatavissa kattavasti tietoturvan eri osa-alueille, mm. hankintoihin, hankkeisiin, sosiaaliseen mediaan, tekniseen ICT-ympäristöön, johtamiseen ja sovelluskehitykseen liittyen. Usein VAHTI-ohjeissa on viite toiseen ohjeeseen, jossa asiaa on käsitelty perusteellisemmin.

VAHTI-ohjeet on luettavissa internetissä Valtiovarainministeriön internetsivuilla: www.vm.fi > Julkisen hallinnon ICT > Tietoturvallisuus > Voimassa olevat tietoturvaohjeet ja –määräykset. Uuden julkaisun julkaisusta voi tilata sähköpostiin ilmoituksen.

Opinnäytetyön toteutusosassa käytettiin VAHTI-ohjeita soveltuvilta osin. Opinnäytetyössä käytettiin seuraavia VAHTI-ohjeita:

Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa 7/2003

Ohjeessa käsitellään riskien arviointia ja hallintaa sekä niiden merkitystä organisaatiossa. Ohjeessa käydään läpi keinot uhkien ja haavoittuvuuksien tunnistamiseen ja mahdollisten toteutuneiden uhkien seurauksien vaatimat toimenpiteet. Lisäksi ohjeessa annetaan menetelmät riskien suuruuden arviointiin sekä toimenpiteiden määrittelemiseksi. Ohjeeseen sisältyy tietoriskien arviointia helpottavia työkaluja, kuten tarkastuslistoja ja linkkejä muihin VAHTI-ohjeiden tarkistuslistoihin. VAHTI-ohjeesta saa hyvän käsityksen organisaation riskienhallinnasta ja siinä tarvittavista keinoista ja menetelmistä.

Valtionhallinnon keskeisten tietojärjestelmien turvaaminen 5/2004

Ohjeessa käsitellään valtionhallinnon keskeisten tietojärjestelmien tietoturvallisuuden parantamista ja tietoturvallisuudessa huomioitavia asioita ja toimenpiteitä. Kohderyhmänä ovat johto, tietojärjestelmien omistajat ja niiden toiminnasta vastaavat henkilöt. Ohjetta voi hyödyntää myös valtionhallinnon ulkopuolella tärkeiden tietojärjestelmän turvaamisessa. Ohjeessa tavoitteena on huomioida ja käydä läpi tietojärjestelmien erityiskysymykset liittyen tietojärjestelmien turvaamiseen, ohjeessa oletetaan että tietojärjestelmän perustietoturva on jo kunnossa. Ohje ei sisällä kaikkia varsinaisia toimenpiteitä, vaan ne löytyvät ohjeessa olevista viitteistä. Ohje on vuodelta 2004, joten se on aika vanha, mutta käyttökelpoinen.

Tietoturvallisuudella tuloksia, yleisohje tietoturvallisuuden johtamiseen ja hallintaan 3/2007

Ohjeessa keskitytään tietoturvallisuuteen johtamisen näkökulmasta. Ohjeessa käydään läpi mm. tietoturvan perusteita, tietoturvatoiminnan organisointia ja seurantaa sekä raportointia. Liitteissä on mallipolitiikkoja tietoturvapolitiikalle, riskienhallintapolitiikalle. Suunnitelmarungoissa on esimerkit tietoturvallisuuden kehittämissuunnitelmasta, tietoturvaperiaatteet ja -käytännöt, valmius-

suunnitelma, jatkuvuussuunnitelma ja toipumissuunnitelma. Lisäksi liitteissä on kuvattu tietoturvavastuut rooleittain.

Teknisen ICT-ympäristön tietoturvataso-ohje 3/2012

Ohjeessa käsitellään keskeisiä vaatimuksia ICT-ympäristön tietoturvallisuuden toteuttamiseksi, suojattavien kohteiden määrittelemistä (suojattavien kohteiden määrittäminen ja rajaaminen) ja vaatimuksia tekniselle tietotekniikkaympäristölle (kuten työasemien ja päätelaitteiden vaatimukset). Ohje sisältää Excel-taulukkoon toteutettuja työvälineitä, joita työssä voi hyödyntää.

Tämä VAHTI-ohje liittyy aiemmin julkaistuun ohjeeseen nimeltä ”Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, 2/2010”, johon suositellaan ensin tutustuttavan.

Henkilöstön tietoturvaohje 4/2013

Henkilöstön tietoturvaohjeeseen on koottu tietoturvallisuuden perusasioita ja käytännön vinkkejä tietoturvan toteuttamiseen, nimenomaan henkilöstön näkökulmasta. Ohje on sovellettavissa myös kuntien henkilöstön tietoturvatyöhön. Opas on helppolukuinen ja selkeä, se soveltuukin hyvin henkilöstön käyttöön. Ohjetta käytettiin runkona laadittaessa Muuramen kunnan henkilöstön tietoturvaohjetta. Ohje on todella hyödyllinen, sitä vasten pystyi hyvin peilaamaan nykyisiä organisaation käytössä olevia käytänteitä.

2.3.6 JHS-suositukset

JUHTA- Julkisen hallinnon tietohallinnon neuvottelukunta julkaisee JHS-suosituksia. JHS-järjestelmän mukaiset suositukset koskevat valtion- ja kunnallishallinnon tietohallintoa. Sisällöltään JHS voi olla julkishallinnossa käytettäväksi tarkoitettu yhtenäinen menettelytapa, määrittely tai ohje. JHS-järjestelmän tavoitteena on parantaa tietojärjestelmien ja niiden tietojen yhteentoimivuutta, luoda edellytykset hallinto- ja sektorirajoista riippumattomalle toimintojen kehittämiselle sekä tehostaa olemassa olevan tiedon hyödyntämistä.

Yksi JHS-suositus käsittelee julkisuuslain mukaista tietojärjestelmäselosteen laadintaa. Suosituksessa on perusteet miksi tietojärjestelmäselosteet on laadittavat, tietojärjestelmäselosteen malli, jäsennys ja täyttöohje sekä selvitys millaisesta tietojärjestelmästä selosta on laadittava. Suosituksessa on myös kirjattu miten suositusta sovelletaan. Lisäksi on selvitetty asiakirjojen ryhmittely julkisuuslain näkökulmasta. (JHS-suositukset JUHTA-julkisen hallinnon tietohallinnon neuvottelukunta, n.d.)

2.4 Tietoturvan suunnittelun vaiheet

2.4.1 Riskien arviointi ja käsittely

Riskien arvioinnin vaiheen tehtävänä on yksilöidä riskit, määritellä niille suuruus ja asettaa ne tärkeysjärjestykseen suhteessa riskien hyväksymiskriteereihin ja organisaation olennaisiin tavoitteisiin. Riskien arviointia tulee suorittaa jatkuvasti, huomioiden muuttuvat tietoturvallisuusvaatimukset ja riskitilanteet. (SFS-ISO/IEC 17799, 2006, 26.)

Riskien arviointi ja käsittelyt ovat yksi tärkeä vaihe tietoturvan suunnittelussa. Siihen liittyvät kuusi päävaihetta, joiden tuloksena organisaation riskien hallinnalle saadaan suunnitelma ja toimintatavat.

Riskienhallinnan päävaiheet ovat

- Suojattavien kohteiden tunnistaminen
- Uhkien tunnistaminen ja niiden merkityksen arviointi
- Riskien torjunnan ja toimenpiteiden valinta
- Toiminta vahinkotilanteessa ja siitä toipuminen
- Tilanteen seuranta
- Toteutuneen riskin analysointi.

Seuraaviin kappaleisiin on kuvattu tarkemmin muutamaa päävaihetta.

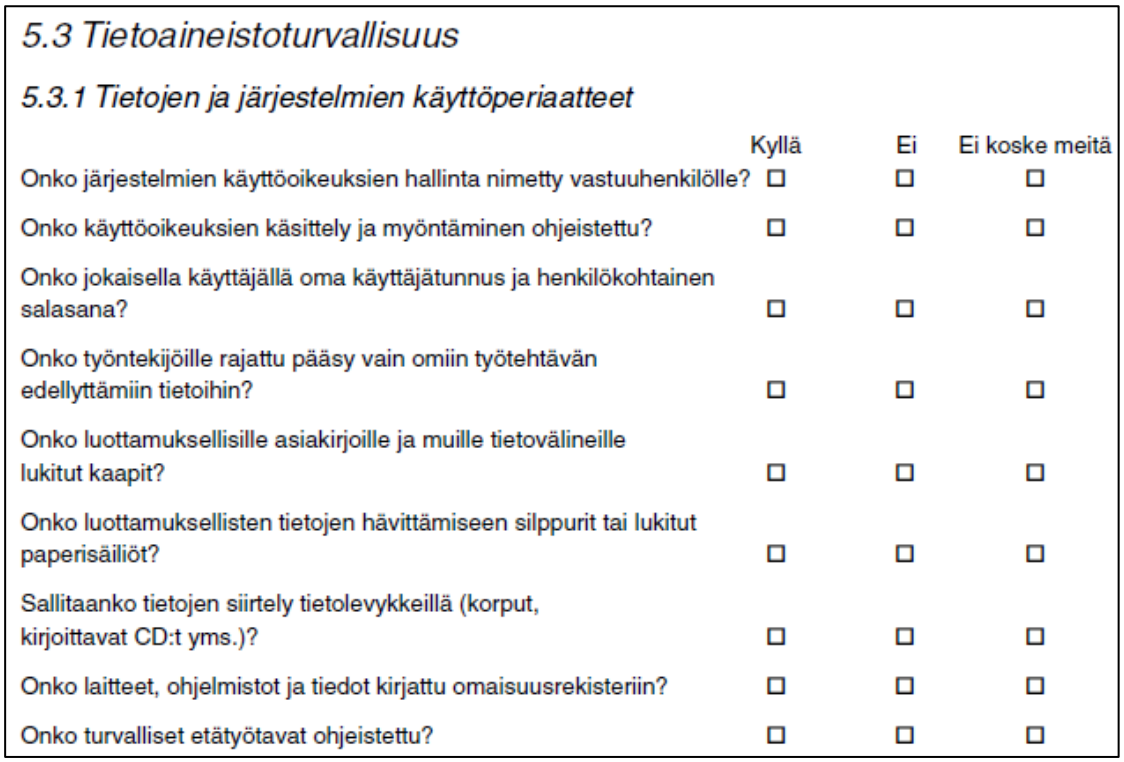
Suojattavien kohteiden tunnistaminen

Ensimmäisessä vaiheessa tulee tunnistaa organisaation suojattavat kohteet. Yleensä suojattava kohde on tieto eri muodoissa, kuten tietoaineistot paperilla ja sähköisessä muodossa. Tilat, kuten palvelintilat, työtilat, asiakastilat, työhuoneet ja arkistot. Muita kohteita ovat mm. paperien hävitys, tietojärjestelmät, sovellukset ja tietoliikenneyhteydet. (Vahti 7/2003, 17-18.)

Suojattavien kohteiden määrittelemisessä tulee selvittää niitä koskevat velvoitteet, joita ovat mm. yleinen lainsäädäntö, organisaatiota koskeva erityislainsäädäntö, viranomaismääräykset, VAHTI-ohjeet, organisaation työjärjestys, sopimukset. (Vahti 3/2012, 32-33.)

Uhkien tunnistaminen ja niiden merkitysten arviointi

Uhkien tunnistamisen vaiheessa pyritään eri menetelmiä hyödyntämällä löytämään kaikki mahdolliset toimintaa uhkaavat tekijät. Uhkien tunnistamisen riskianalyysimenetelmiä menetelmiä ovat mm. potentiaalisten ongelmien analyysi (POA), uhkapuut, skenaariomenetelmä, haavoittuvuusanalyysi. Tarkastuslistojen avulla uhkia voidaan tunnistaa karkeammalla tasolla ja löytää oman organisaation ongelmakohdat. Useissa VAHTI-ohjeissa on tarkastuslistoja, joita voi vapaasti hyödyntää. Uhkien tunnistaminen tulee kohdentaa kaikkiin tietoturvallisuuden osa-alueisiin. (Vahti 7/2003, 26-29.). Edellä mainitussa VAHTI-ohjeessa on liitteessä 2 esimerkkeinä tietoturvauhkien tunnistamisen tarkistuslistoja. Listassa käsitellään tietoliikenne-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus. Kuviossa käsitellään tietoaineistoturvallisuutta, tietojen ja järjestelmien käyttöperiaatteita.



5.3 Tietoaineistoturvallisuus

5.3.1 Tietojen ja järjestelmien käyttöperiaatteet

	Kyllä	Ei	Ei koske meitä
Onko järjestelmien käyttöoikeuksien hallinta nimetty vastuuhenkilölle?	☐	☐	☐
Onko käyttöoikeuksien käsittely ja myöntäminen ohjeistettu?	☐	☐	☐
Onko jokaisella käyttäjällä oma käyttäjätunnus ja henkilökohtainen salasana?	☐	☐	☐
Onko työntekijöille rajattu pääsy vain omiin työtehtävän edellyttämiin tietoihin?	☐	☐	☐
Onko luottamuksellisille asiakirjoille ja muille tietovälineille lukitut kaapit?	☐	☐	☐
Onko luottamuksellisten tietojen hävittämiseen silppurit tai lukitut paperisäiliöt?	☐	☐	☐
Sallitaanko tietojen siirtely tietolevykkeillä (korput, kirjoittavat CD:t yms.)?	☐	☐	☐
Onko laitteet, ohjelmistot ja tiedot kirjattu omaisuusrekisteriin?	☐	☐	☐
Onko turvalliset etätyötavat ohjeistettu?	☐	☐	☐

Kuvio 2. VAHTI-ohjeen (Vahti 7/2003) tarkistuslistan kysymyksiä liittyen tietoaineistoturvallisuuteen

Uhkia löytyy yleensä runsaasti, eikä kaikkia uhkia pystytä käsittelemään yhdellä kertaa. Sen vuoksi ensimmäisessä vaiheessa etsitään suurimmat riskit ja keskitytään niiden ratkaisemiseen. Uhkien suuruudelle saadaan arvo arvioimalla uhkan todennäköisyyttä ja toteutuneen vahingon suuruutta. Uhkan todennäköisyyden arvioinnin asteikko voi olla esimerkiksi: korkea, keskimääräinen, alhainen, ei merkitystä. Seurauksen vakavuus voidaan luokitella seuraavasti: erittäin vakava, vakava, vähäinen. Jos löydetyn uhkan/riskin arvot ovat todennäköisyydeltään korkea ja seurauksiltaan erittäin vakava, on riski otettava välittömään käsittelyyn ja siihen on löydyttävä ratkaisu- ja toimintamallit. Riskien merkityksen arvioinnissa on hyvä pitää lähtökohtana kuinka suuri toteutuneen riskin vaikutus on organisaation toimintaan. (Vahti 7/2003, 41-43.)

Kuviossa 3 on riskitaulukko, joka toimii hyvänä käytännön apuvälineenä riskien arvioinnissa.

Kriittisyys		Seurausten vakavuus		
		Vähäinen (1)	Vakava (2)	Erittäin vakava (3)
Uhkan todennäköisyys	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

Kuvio 3. Riskitaulukko (Vahti 7/2003, 43)

Seuraavaan kappaleeseen on koottu esimerkkejä sisäverkon uhkista perustuen VAHTI-ohjeeseen vuodelta 2010 nimeltä Sisäverkko-ohje (Vahti 3/2010), 41-43).

- Haittaohjelmat
- Ulkopuolinen murtautuja
- Oma työntekijä
- Yhteistyökumppanit
- Erilaiset luonnonmullistukset ja muut fyysiset tapahtumat
- Laiterikot, ohjelmistovirheet ja konfiguraatioviat.

Andreasson ja Koivisto (2013, 237) toteavat kirjassaan, että yleinen ongelma on se, että tietoturvauhkiin ei osata varautua, koska ne eivät tunnu arkipäiväisiltä ja konkreettisilta, sillä ne eivät välttämättä ole koskaan toteutuneet. Uhkien tunnistaminen ja niiden käsittely on juuri edellä mainitusta syystä erittäin tärkeässä asemassa organisaation tietoturvan suunnittelussa.

Riskien torjunnan ja toimenpiteiden valinta

Uhkien tunnistamisvaiheessa löydetyille riskeille tulee määritellä toimenpiteet. Riskienhallinnan toimintavaihtoehdot ovat riskien välttäminen, riskin poistaminen, riskin pienentäminen (estetään vahinkojen syntyminen ja vähennetään

sen seurauksia), riskin siirtäminen (esimerkiksi vakuuttamalla tai sopimuksin) tai riskin hyväksyminen eli pitäminen omalla vastuulla. Riskienhallinnassa tulee aina huomioida myös tarvittavien toimenpiteiden kustannukset.

Riskien pienentämistä voidaan toteuttaa teknisillä toimenpiteillä, organisaation toimenpiteillä tai yksilön toimintamahdollisuuksia parantavilla toimenpiteillä. Suurempien riskien kohdalla tavoitteena on riskien poistaminen tai pienentäminen. Lisäksi tulee estää vahinkojen syntyminen ja minimoida toteutuneen riskin seuraukset. Riskit voidaan kategorisoida seuraavasti: merkityksetön riski (toimenpiteitä ei tarvita), vähäinen riski (ei pakollisia toimenpiteitä, tilannetta seurataan), kohtalainen riski (vaatii toimenpiteitä riskin pienentämiseksi, mutta ei heti, saattaa vaatia lisäselvittelyä), merkittävä riski (riskin pienentämisen toimenpiteet aloitettava heti) ja sietämätön riski (riskin pienentäminen aloitettava välittömästi, riskialtista toimintaa ei voi aloittaa eikä jatkaa ennen riskin pienentämistä). (Vahti 7/2003, 45-46.)

Tilanteen seuranta

Riskien arviointi ja käsittely ovat säännöllistä ja jatkuvaa toimintaa. Tunnistetuille riskeille tulee laatia riskien hallintasuunnitelma. Siinä kuvataan riski, asetetaan tavoite riskin hallitsemiseksi, kuvataan toimenpide-ehdotus ja määrätään vastuuhenkilö ja aikataulu. (Vahti 7/2003, 47.)

Tietoturvatyön kehittämissuunnitelma

Opinnäytetyön puitteissa tehtävien tietoturvaohjeiden tekemisen jälkeen on vuorossa edellä mainittujen kartoitusten tekeminen. Jotkin tehtävät toimeksiantajan organisaatiossa on jo suoritettu, mutta ne vaatinevat lisätarkastelua ja päivittämistä. Työn lähtökohtana voidaan pitää sitä, että arvioidaan nykyinen tilanne ja käytössä olevat tekniset –ja hallinnolliset ratkaisut, samoin käytössä olevat prosessit ja ryhdytään kehittämään niitä.

Tietoturvallisuuden hallinnan suunnittelu ja toteutus voidaan jakaa seuraaviin tehtäväalueisiin:

1. Tietoturvatarpeiden ja lähtökohtien tunnistaminen

2. Tärkeiden toimintojen, riippuvuuksien ja tieto-omaisuuden tunnistaminen

3. Riskienhallinta- ja häiriötilannemenettelyiden luominen

4. Tietoturvallisuuden hallintamenettelyiden luominen.

   (Nurmi 2011, 4.)

Hyvänä apuvälineenä tietoturvan kehittämisessä ja suunnittelussa on Kirsi Nurmen, vuonna 2011 kirjoittama opas nimeltä Tietoturvallisuuden hallinnan suunnittelu ja toteutus, joka on projektiopas valtionhallinnon organisaation tietoturvallisuudesta vastaavalle. Oppaaseen on koottu selkeästi projektin vaiheet, oppaassa on huomioitu KATAKRI ja VAHTI-ohjeet.

VAHTI-ohjeessa Tietoturvallisuudella tuloksia, yleisohje tietoturvallisuuden johtamiseen ja hallintaan (Vahti 3/2007) liitteessä on mallisuunnitelmarunko tietoturvallisuuden kehittämissuunnitelmaan sekä mm. toipumis-, valmius-, jatkuvuussuunnitelmille. Myös nämä ohjeet kannattaa huomioida tietoturvan kehittämissuunnitelmaa tehdessä.

2.4.2 Tietojärjestelmäkuvaukset

Tietoturvasuunnittelun yhteydessä käytetään organisaation olemassa olevia tietojärjestelmäkuvauksia. Tietojärjestelmäkuvauksista selviää mitä tietoa tietojärjestelmissä säilytetään, miten ja kuka tietoja käyttää sekä miten tieto toimitetaan käyttäjille. Järjestelmän yleiskuvaus sisältää yleiskuvauksen järjestelmän käytöstä, kuka on järjestelmän omistaja sekä tiedon mihin toimintaprosesseihin tietojärjestelmä kuuluu. (Hakala ym. 2006, 72.)

Tietojärjestelmäluettelosta selviää kaikki organisaation käytössä olevat tietojärjestelmät.

VAHTI-ohjeessa Teknisen ICT-ympäristön tietoturvataso-ohje on liitteenä Ympäristön ja järjestelmien kuvauksen-apuväline Excel-taulukko, jota voi hyödyntää tietojärjestelmien perustietojen keräämisessä.

2.4.3 Tietoturvan auditoinnit

Auditointien avulla arvioidaan organisaation riskienhallinnan toimivuutta ja tarkoituksenmukaisuutta. Auditointien tuloksista voi ilmentyä muutoksia vaativia seikkoja organisaation prosesseissa tai infrastruktuurissa. (Kim & Solomon 2014.)

Kansallinen turvallisuusauditointikriteeristö (KATAKRI) on valmistunut vuonna 2009 viranomaisten, elinkeinoelämän ja turvallisuusalan yhteistyönä. KATAKRI:n kriteeristön avulla viranomaiset tai auditoijat todentavat arvioitavan kohteen turvallisuuden tasoa KATAKRI:n auditointikriteereihin verraten. KATAKRI:n avulla varmistetaan suomalaisten yritysten ja organisaatioiden tietoturvan taso suhteessa kansainvälisiin tietoturvan velvoitteisiin. KATAKRI:ssa on suositusosio, jota yritykset voivat käyttää apuna omaehtoisessa tietoturvatyössä. (Vahti 2012, 28-29.)

KATAKRIn turvallisuusauditointikriteeristössä on neljä osa-aluetta: hallinnollinen turvallisuus, henkilöstöturvallisuus, fyysinen turvallisuus ja tietoturvallisuus. Jokaisesta osa-alueesta on koottu kysymyssarja. Viranomaisvaatimukset on jaettu kolmeen tasoon: perustaso, korotettu taso ja korkea taso. Lisäksi erikseen ovat elinkeinoelämän suositukset sekä viittaukset standardeihin ja lisätietoihin. Kysymyksiin on myös avattu se mitä kysymyksellä arvioidaan. Turvallisuuden osa-alueet on jaettu pienempiin osakokonaisuuksiin, esimerkiksi tietoturvallisuuteen kuuluvat tietoliikenneturvallisuus, tietojärjestelmäturvallisuus, tietoaineistoturvallisuus ja käyttöturvallisuus. Käymällä kysymyssarjan läpi varmistuu siitä, että tietoturvallisuuden osa-alueet on käyty kattavasti läpi.

2.5 Tietoturvallisuuden johtaminen ja hallinnointi

2.5.1 Vastuuttaminen

Organisaatioiden johto on keskeisessä asemassa tietoturvallisuuden johtamisessa ja hallinnoimisessa. Tietoturvallisuuden kehittäminen, ylläpitäminen ja suunnitteleminen vaativat johdolta sitoutumista. Käytännössä organisaatioiden tietoturvatyö on vastuutettu nimeämällä tietoturva-asioista vastuullinen henkilö, esimerkiksi tietoturvapäällikkö, jolle osoitetaan riittävät resurssit työtehtävän hoitamiseen. Tietoturva-asioiden raportoiminen johdolle on tärkeää kehittämiskohteiden havaitsemiseksi, yleisen tietoturvatilan tiedostamiseksi sekä tietoturvavelvoitteiden toteutumisen seuraamiseksi. Johdon velvollisuutena on pitää vastuuhenkilö ajan tasalla mm. meneillä olevista hankkeista ja suunnitelmista, esimerkiksi tietojärjestelmien hankinnoista. Tietoturvaa tulisi vastuuttaa organisaatiossa myös osasto-, yksikkö- ja toimintokohtaisesti nimeämällä niihin tietoturvan vastuuhenkilöt. Tietoturvallisuus korostuu etenkin keskeisissä hallinnollisissa toimissa, kuten tieto-, henkilöstö-, talous- ja materiaalihallinnossa ja hankintatoimessa. (Andreasson & Koivisto 2013, 32-33.)

Andreasson ja Koivisto (2013, 45) toteavat kirjassaan, että tietoturvan toteuttamisen haasteena voidaan pitää resurssien vähyyttä, tarkoittaen henkilö- ja taloudellisia resursseja. Usein kunnissa on tilanne, jolloin organisaatiossa ei ole täysipäiväistä tietoturvallisuudesta vastaavaa henkilöä, vaan tietoturva-asiat hoidetaan muun työn ohessa. Näissä tilanteissa johdon on tuleekin osoittaa riittävästi resursseja, jotta tietoturvatyö tulee asianmukaisesti hoidettua. Isommissa organisaatioissa haasteeksi voi tulla toiminnan organisoiminen eli se miten henkilöstö saadaan toimimaan tietoturvaohjeiden mukaisesti. Tilannetta voidaan parantaa jo aiemmin mainitulla tavalla, eli vastuuttamalla osastoilta yhteyshenkilöt, jotka mm. hoitavat viestintää ja tiedottamista tietoturvapäällikön ja oman osaston välillä. (Andreasson & Koivisto 2013, 45.)

Tietoturvan johtamisen apuvälineiksi on olemassa ”parhaita käytäntöjä”, joiden avulla on helpompi hallita tietoturvan eri osa-alueita. Ne voivat olla esimerkiksi standardeja, muistilistoja tai muita dokumentteja, esimerkkinä VAHTI-ohjeet.

Parhaiden käytäntöjen noudattamisen etuna on saattaa tietoturvatyö määrämuotoiseksi, jolloin sen hallinnoiminen ja hahmottaminen on helpompaa. Tärkeä seikka on tietoturvatyön johtaminen osana organisaation muuta toimintaa; se ei saa olla kokonaisuudesta irrallinen tekijä. Tietoturvatyön tavoitteena voidaan pitää tietoturvan nivoutumista yhteen organisaation muun jokapäiväisen toiminnan kanssa, koskien koko organisaation henkilöstöä ja kaikkea toimintaa. Työntekijöiden tietoturvatietoisuutta voidaan lisätä järjestämällä tietoturvakoulutusta, ja ottamalla tietoturva yhtenä osana mukaan työohjeisiin, perehdytykseen ja työnohjaukseen. (Laaksonen ym. 2006, 115-116.)

VAHTI-ohjeessa Tietoturvallisuudella tuloksia, Yleisohje tietoturvallisuuden johtamiseen ja hallintaan (Vahti 3/2007, 92-94) liitteeseen on koottu tietoturvallisuuden johtamisen ja toimineenpanon tehtävät rooleittain. Muutama esimerkki rooleista ja niiden tehtävistä.

- Ylin johto

  Ylimmän johdon vastuulla ovat mm. riskienhallinta- ja tietoturvapolitiikan ja niiden periaatteiden hyväksyminen, edellytysten luominen ja takaaminen tarvittaviin resursseihin liittyen tietoturvallisuuteen ja riskienhallintaan, raportointivaatimusten määrittäminen ja riskienhallinnan nivominen osaksi johtamistoimintaa.

- Tietojärjestelmän omistaja

  Vastuulla ovat mm. tietojärjestelmäkuvausten ylläpitäminen, tietojärjestelmien tietoturvallisuuden seuranta ja tietoturvallisuuden ja mahdollisten poikkeamien raportointi.

- Tietotekninen asiantuntija, järjestelmäasiantuntija, atk-tukihenkilö

  Vastuulla ovat mm. tietoturvallisuuden raportointi, tietoturvapolitiikan soveltaminen ja toteuttaminen omaa erikoisasiantuntemusta hyödyntäen ja tietoturvatoimenpiteiden huomioiminen ja noudattaminen omalla vastuualueella.

2.5.2 Tietoturvapolitiikka

Tietoturvapolitiikka on julkinen asiakirja, johon on koottu organisaation tietoturvan päälinjaukset ja tavoitteet. Se nähdään myös organisaation johdon kannanottona ja sitoutumisen ilmauksena organisaation tietoturva-asioiden kehittämiselle. Tietoturvapolitiikka luo pohjan tietoturvaohjeistukselle ja –koulutukselle. (Laaksonen ym. 2006, 146-148.)

Tietoturvapolitiikka tulee saattaa koko organisaation tietoon ja saataville, tarvittaessa se tiedotetaan myös sidosryhmille. Usein yritykset ja organisaatiot julkaisevatkin tietoturvapolitiikkansa internetsivuillaan. Tietoturvapolitiikka tulee kirjoittaa sellaiseen muotoon, että se on helposti ymmärrettävissä. (Hakala ym. 2006, 9.)

Tietoturvapolitiikan laatimiseksi on olemassa useita malleja, jota organisaatiossa voidaan soveltaa. Malleissa kuvataan tietoturvapolitiikan runko ja siinä käsiteltävät asiat. Kansainvälisistä standardeista ISO/ETC 27001 ja ISO/ETC 27002 käsittelevät tietoturvapolitiikkaa, VAHTI-ohjeista Johdon tietoturvaopas (Vahti 2/2011) ja Tietoturvallisuudella tuloksia - yleisohje tietoturvallisuuden johtamiseen ja hallintaan (Vahti 3/2007). (Andreasson & Koivisto 2013, 34.)

VAHTI-ohjeessa Tietoturvallisuudella tuloksia - yleisohje tietoturvallisuuden johtamiseen ja hallintaan (Vahti 3/2007) on malli tietoturvapolitiikasta. Sen mukaan tietoturvapolitiikassa tulee ottaa kantaa mm. seuraaviin asioihin: tietoturvapolitiikan tavoite, tietoturvatoimintaa ohjaavat tekijät, tietoriskien hallinta, tietoturvallisuuden merkitys organisaatiolle, turvatoimien priorisointi, tietoturvallisuuden hallintajärjestelmä, tietoturvavastuut, tietoturvakoulutus ja –ohjeet, tietoturvallisuudesta tiedottaminen, tietoturvallisuuden toteutumisen valvonta ja toiminta poikkeustilanteissa ja –oloissa. (Vahti 2007, 85.)

Tietoturvapolitiikkaa tulee katselmoida säännöllisesti ja suunnitelmallisesti, lisäksi aina jos tietoturvapolitiikkaan vaikuttavia muutoksia tapahtuu. Näin varmistetaan tietoturvapolitiikan ajan tasaisuus, soveltuvuus, asianmukaisuus ja vaikuttavuus. Tietoturvapolitiikalla tuleekin olla nimetty omistaja, jolla on

hyväksytty esimiesvastuu turvallisuuspolitiikan kehittämisestä, katselmoinnista ja arvioinnista. (SFS-ISO/IEC 17799 2006, 30.)

2.5.3 Tietoturvaohjeistus

Tietoturvaohjeiden laatiminen on tärkeää, sillä niiden avulla pyritään estämään ongelmien syntyminen. Ohjeita on tarpeen laatia eri tilanteisiin, esimerkiksi sovellusten – ja tietoverkon käyttöön, erityis- ja poikkeustilanteisiin, laitteiden käyttöön, internetin käyttöön sekä mahdollisiin väärinkäyttötilanteisiin. Ohjeiden tulee olla laadittu riittävän selkeästi ja kaikki ohjeet tulee olla yhteneväisiä, jotta vältytään eri ohjeiden ristiriitaisuuksilta. Organisaation toteuttaessa teknisiä tietoturvaratkaisuja tulee samassa yhteydessä laatia myös tarvittavat ohjeistukset. (Laaksonen ym. 2006, 146.)

Työntekijöiden käytössä olevien ohjeiden ansiosta vältytään myös tietämättömyydestä johtuvista tietoturvaongelmista sekä organisaatioon saadaan yhteneväiset käytännöt mm. internetin ja laitteiden käytön suhteen. Yhteiset pelisäännöt ovat tärkeä osa tietoturvan toteuttamisessa.

Organisaation työntekijöiden motivoiminen tietoturvan noudattamiseen on ensiarvoisen tärkeää, pelkät ohjeet ja säännöt eivät ole riittäviä ilman motivointia. Henkilöstön tulee myös ymmärtää ja havaita tietoturva-asioiden ja ohjeiden tärkeys kaikissa toimissaan myös käytännön tasolla. Organisaation johdon ja muun henkilöstön esimerkillinen tietoturvaohjeiden noudattaminen lisää koko henkilöstön motivaatiota noudattaa ja toimia annettujen ohjeiden mukaisesti. Yksilön tietoturvakäyttäytymiseen vaikuttavat mm. työntekijän henkilökohtaiset arvot ja asenteet, työntekijän suhtautuminen työnantajaan ja ohjeiden noudattamisen vaatima aika ja työ. (Laaksonen ym. 2006, 249-251.)

Tietoturvapolitiikka – ja ohjeet muodostavat perustan henkilöstön toimintatavoille, ohjeistuksen ansiosta organisaatioon muodostuu sen hyväksymä tietoturvallisuuden käyttäytymismalli. Työssä eteen tulevat tietoturvallisuuteen liittyvät tilanteet on pyrittävä hoitamaan organisaation käytänteiden mukaisesti. (Laaksonen ym. 2006, 249.)

2.5.4 Tietoturvakoulutus

Tietoturvakoulutuksen tarkoituksena on ohjeistaa henkilökunta toimimaan organisaation tietoturvavaatimusten tavalla. Perustana pidetään tietoturvapolitiikkaa, tietoturvaohjeistusta, prosessikuvauksia ja mahdollisesti havaittuja tietoturvakäyttäytymisen puutteellisuuksia. Henkilöstön motivaatio on tärkeää huomioida tietoturvakoulutuksia suunnitellessa. Motivoitunut henkilöstö omaksuu ohjeet ja neuvot paremmin. Motivaatio voi olla sisäistä tai ulkoista, sisäisesti motivoitunut työntekijä on kiinnostunut asioista ja oppiminen sen ansiosta helpompaa. Ulkoista motivaatiota voi herätellä esimerkiksi kilpailuasemalla. (Laaksonen ym. 2006, 254.)

Tietoturvakoulutuksissa henkilöstölle tulee antaa tarvittava ohjeistus omista työtehtävistä suoriutumiseen tietoturvan näkökulmasta, jokaisen tulee ymmärtää työhönsä liittyvät riskit ja keinot niiden minimoimiseksi. Koulutuksessa kannattaa painottaa mihin ohjeistetuilla toimintatavoilla pyritään, niin että kaikki ymmärtävät tietoturvan perimmäisen merkityksen. (Laaksonen ym. 2006, 255.)

3 Työn toteutus

3.1 Tavoitteet

Opinnäytetyön tavoitteena oli laatia koko organisaation kattava tietoturvapolitiikka sekä tarvittavia tietoturvaohjeita, joita ovat mm. mobiililaitteiden tietoturvaohje ja henkilöstön tietoturvaohje. Tehtäviin kuului myös tietojärjestelmäluettelon päivittäminen ja tarkempien tietojärjestelmäkuvausten luominen tietojärjestelmistä. Henkilöstön intranetin tietoturvasivujen päivittäminen tehtiin samassa yhteydessä.

3.2 Laaditut ohjeet

3.2.1 Tietoturvapolitiikka

Tietoturvapolitiikasta on laadittu luonnos, joka odottaa ylimmän johdon hyväksyntää. Tietoturvapolitiikassa määritellään Muuramen kunnan tietoturvallisuuden linjaukset ja tavoitteet. Hyväksytty tietoturvapolitiikka annetaan tiedoksi koko henkilöstölle ja asetetaan saataville mm. intranetiin. Tietoturvapolitiikan luomiseen ovat osallistuneet ATK-henkilöstö sekä toimialajohtajat. Tietoturvapolitiikan laatimisen ansiosta organisaatiossa on määritelty tarkemmin tietoturvallisuuteen liittyviä yksityiskohtia ja käytänteitä sekä vastuita.

Tietoturvapolitiikka sisältää mm. seuraavat aihealueet:

- Tietoturvan päämäärät

  Kappaleessa on määritelty mitä tietoturvallisuudella tarkoitetaan ja mikä on sen tavoite sekä kuvataan määritelmät luottamuksellisuus, eheys, käytettävyys, kiistämättömyys ja pääsynvalvonta. Lisäksi kuvataan tietoturvatyöhön liittyvät toiminnat.

- Toteuttamiskeinot

  Kappaleessa kuvataan keinot yleisellä tasolla tietojärjestelmien ja tietoverkkojen turvallisuuden toteutuksesta.

- Vastuut ja organisointi

  Kappaleessa on määritelty organisaation toimijoiden vastuualueet.

- Tiedottaminen ja koulutus

  Kappaleessa on määritelty tietoturvaan liittyvän tiedottamisen vastuutahot sekä henkilöstön tietoturvatietoisuuden ylläpitämisen keinot.

- Seuranta ja ongelmatilanteet

  Kappaleessa otetaan kantaa miten tietoturvan tasoa seurataan ja miten mahdollisissa ongelmatilanteissa toimitaan. Lisäksi kappaleessa on toimintamalli tietoturvarikkomustilanteeseen.

3.2.2 Tietoturvaohjeet

Tietoturvallisuuteen liittyviä ohjeita on laadittu suunnitelman mukaisesti: tietoturvaohje matkapuhelimen kadotessa, mobiilikäyttäjän tietoturvaohje sekä henkilöstön tietoturvaohje. Vaikka ohjeisiin kootut käytänteet ovatkin olleet käytössä aiemmin, nyt ne on kirjattu virallisiksi ohjeiksi. Ohjeet on pyritty tekemään mahdollisimman selkeiksi ja havainnollisiksi. Uusista ohjeista on tiedotettu henkilöstölle ja ne ovat nyt kaikkien saatavilla intranetissä. Vanha tietoturvan yleisohje oli osittain vanhentunut, nyt se on uudistettu vastaamaan nykyajan vaatimuksia huomioiden myös mobiililaitteet ja niiden käyttäjät, samassa yhteydessä ohjeen nimi muutettiin henkilöstön tietoturvaohjeeksi. Ohjeiden laatimisen yhteydessä olemassa olevia käytänteitä tarkastettiin ja täsmennettiin, joitakin löytyneitä epäkohtia myös muutettiin vastaamaan nykypäivän vaatimuksia. Lisäksi ohjeissa huomioitiin viimeaikoina lisääntyneet mobiililaitteet, kuten iPad:it ja älypuhelimet.

Muuramen kunnan henkilöstön Intranetin tietoturvaosio uudistettiin ja uudet ohjeet lisättiin Tietoturvaohjeet-sivulle, lisäksi lisättiin linkkejä tietoturvaa käsitteleville sivuille, joista henkilöstö voi itsenäisesti hankkia lisätietoa tietoturvallisuuteen liittyen.

Henkilöstön tietoturvaohje sisältää mm. seuraavia osa-alueita:

- Tietoturvallisuuden määritelmä, joka on myös kuvattu käytännön tasolla.

- Käyttöoikeudet, tunnukset ja salasanat

  Määrittelyssä kuvataan Muuramen kunnan tietoverkon ja tietojärjestel-

mien käyttämisen perusperiaatteet ja tarvittavat käyttöoikeudet. Kappaleessa kuvataan käyttöoikeuksiin liittyvät periaatteet ja käytännöt.

- Työvälineiden käyttö

  Kappaleessa on kuvattu Muuramen kunnan omistamien työvälineiden käytön periaatteet ja säännöt. Ohjeistus sisältää myös työtiedostojen tallentamisen kohteet ja periaatteet. Poistuvien tietoteknisten laitteiden kierrättämis- ja poistokäytännöt on niin ikään kerrottu.

- Internet- ja viestintäratkaisut

  Kappaleessa kuvataan Muuramen kunnan internet- ja viestintäratkaisujen käytön periaatteet.

- Sosiaalinen media

  Kuvataan sosiaalisen median käyttämisen perusperiaatteet erillisessä ohjeessa nimeltä ”Ohjeita sosiaaliseen mediaan”.

- Etätyö ja etäkäyttö

  Kuvataan Muuramen kunnan periaatteet etätyön ja etäkäytön suhteen. Lisäksi ohjeistetaan miten toimitaan matkoilla ja julkisissa paikoissa liittyen organisaation omistaman tiedon käsittelyn suhteen.

- Mobiililaitteet

  Mobiililaitteiden käytön perusperiaatteet, sekä mm. ohjeistus miten estää laitteen luvaton käyttö, toimintaohje mobiililaitteen kadotessa sekä ohjeistus mobiiililaitteiden hankintaan liittyen.

- Ongelmatilanteet

  Kuvataan miten ongelmatilanteissa toimitaan. Niitä voivat olla esimerkiksi organisaation omistaman laitteen katoaminen tai rikkoutuminen tai epäilys tietoturvarikkomuksesta.

- Seuraamukset

  Kappaleessa on määritelty seuraamukset mahdollisissa tietoturvarikkomustilanteissa.

- Lisätietoa

  Kappaleeseen on koottu linkkejä ulkopuolisiin tahoihin, joista saa lisätietoa tietoturvallisuuteen liittyen.

3.2.3 Tietojärjestelmäkuvaukset

Tietojärjestelmäkuvauksia varten tehtiin taulukko soveltaen VAHTI-ohjeissa olevaa mallia. Tietojärjestelmäkuvaukseen on koottu tietojärjestelmistä kaikki tärkeä tieto, kuten järjestelmän perustiedot, elinkaari, pääkäyttäjien ja toimittajan yhteystiedot sekä tukipalvelutiedot. Taulukko toimii samalla tarkastuslistana tietojärjestelmän kriittisille tekijöille, kuten miten varmistukset on hoidettu ja miten palvelinalustan vikasietoisuus on varmistettu. Täyttäessäni taulukkoa havahduinkin muutamaan epäkohtaan, joka paljastui juurikin taulukon valmiiden kysymysten ansiosta. Taulukkoa voisi ehkä vielä joltain osin parantaa, mutta se on tehtävissä myöhemmin.

Muuramen kunnan tietojärjestelmien tietojärjestelmäluettelo, johon on koottu kaikki käytössä olevat sovellukset, päivitettiin samalla ajantasalle, käytöstä poistuneet sovellukset poistettiin luettelosta ja uudet lisättiin, myös pääkäyttäjätiedot päivitettiin samalla. Luettelo laitetaan esille intranetiin. Luettelosta henkilöstö voi tarkastaa sovellusten pääkäyttäjätiedot esimerkiksi käyttöoikeuksia tarvitessa.

4 Pohdinta

Opinnäytetyön toteuttaminen onnistui kokonaisuutena melko hyvin. Tietoturvallisuuden ollessa laaja käsite, työn rajaaminen tuntui aluksi haasteelliselta. Reunaehdot opinnäytetyölle asetti toimeksiantajan tarpeet, jotka olivat tietoturvapolitiikan laatiminen ja tietoturvaohjeet.

Opinnäytetyön tavoitteena oli laatia organisaation tarvitsemat ohjeistukset tietoturvaan liittyen. Ohjeista tuli mielestäni selkeät ja ymmärrettävät. Ohjeiden laatiminen oli pääpiirteissään helppoa, koska tunnen organisaation käytänteet ja toiminnan. Henkilöstön tietoturvaohjeen laatimisessa haasteeksi muodostui kaikkien tietoturvan osa-alueiden huomioiminen niin, että ohjeen selkeys ja luettavuus säilyivät. Liian pitkässä ohjeessa asian omaksuminen voi vaikeutua.

Tulevaisuudessa tietoturvaan liittyviä ohjeita pidetään ajan tasalla sekä laaditaan uusia tarvittavia ohjeita. Henkilöstön tietoturvatietoisuuden tasoa tullaan mittaamaan esimerkiksi kyselyin. Kyselytulosten perusteella tietoturvatietoisuutta voidaan lisätä ja täsmentää koulutuksilla. Henkilöstön tietoturvaohje on todella hyödyllinen koko organisaatiolle, koska siihen on kerätty organisaation tietoturvakäytänteitä ja toimintatapoja laajasti. Ohjeen avulla henkilöstölle selviää organisaatiossa käytössä olevat tietoturvan pelisäännöt ja käytänteet. Myös muista ohjeista on organisaatiolle konkreettista hyötyä, joka näkyy mm. henkilöstön tietoturvatietoisuuden lisääntymisenä. Tietoturvapolitiikka on niin ikään organisaatiolle tarpeellinen ja tärkeä tuotos, jonka päälle määrätietoinen tietoturvatyö rakentuu.

Yleensä tietoturvan suunnitteleminen alkaa erilaisten kartoitusten tekemisellä, kuten uhkakartoituksella. Opinnäytetyön toimeksiantaja piti kuitenkin tärkeänä tietoturvapolitiikan ja henkilöstön tietoturvaohjeiden laatimisen, jonka vuoksi työn ulkopuolelle jäivät erilaiset tietoturvan kartoitukset, kuten uhkakartoitus ja riskien arviointi. Työn teoriaosassa niiden tekemisen periaatteet on käyty läpi, joten sen pohjalta kartoitusten tekeminen on helppo aloittaa myöhemmässä vaiheessa. Tietoturvan kehittämissuunnitelma- kappaleeseen on koottu kar-

kealla tasolla tietoturvallisuuden hallinnan suunnittelun ja toteutuksen vaiheet sekä lähteitä, joista on apua työn tekemisessä.

Opinnäytetyön puitteissa kerättiin tiedot muutamasta tietojärjestelmästä tietojärjestelmäkuvaukseen. Lopuista tietojärjestelmistä työ on vielä tekemättä, mutta se tehdään myöhemmin. Samalla tietojärjestelmätaulukkoon tehtäneen pieniä parannuksia. Tavoitteena on saada taulukosta mahdollisimman informatiivinen ja helposti ylläpidettävä.

Työn kirjoittamisen aikana olen tutustunut useaan VAHTI-ohjeeseen. Tulen varmasti myöhemmin hyödyntämään ohjeita työssäni, samoin kuin muutakin opinnäytetyön lähdekirjallisuutta. Aineistoa tietoturvaan liittyen löytyy todella paljon, pelkästään VAHTI-ohjeita on paljon. Haasteena olikin löytää sopivat lähteet runsaasta tarjonnasta. Lisäksi ohjeiden lukeminen vaati aikaa ja keskittymistä, joka oli varsinaisen työn ohella haasteellista. VAHTI-ohjeet ovat laajoja kokonaisuuksia, joissa on viittauksia toisiin VAHTI-ohjeisiin. Standardeihin tutustuminen oli hyödyllistä, vaikka kovin paljon niitä ei käytetty ohjeiden tekemisen lähteinä.

Opinnäytetyön ansiosta ymmärrykseni tietoturvatyön laajuudesta ja monipuolisuudesta lisääntyi. Tietoturvallisuus ei liity pelkästään laitteisiin ja tietojärjestelmiin vaan koskee laajasti koko organisaation kaikkia toimintoja.

Lähteet

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

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

JHS-suositukset JUHTA- julkisen hallinnon tietohallinnon neuvottelukunta. Viitattu 6.11.2014. http://www.jhs-suositukset.fi/web/guest/jhs

Kim, D. & Solomon, M. 2014. Fundamentals of Information Systems Security, Second Edition. Jones & Bartlett Learning.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja. Helsinki: Edita publishing Oy.

Muurame Info. N.d. Muuramen kunnan internetsivut. Viitattu 22.4.2014. http://www.muurame.fi/fi/muurame_info/

Muuramen kunnan henkilöstökertomus 2013. 2013.

Muuramen kunnan talousarvio vuodelle 2014 ja taloussuunnitelma vuosille 2015-2016. 2013.

Nurmi, K. 2011. Tietoturvallisuuden hallinnan suunnittelu ja toteutus. Viitattu 20.10.2014. http://www.tietoturvatalkoot.fi/projektiopas.pdf

SFS-ISO/IEC 17799:fi. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Standardi. Suomen Standardisoimisliitto SFS.

SFS-ISO/IEC 27001:2005. 2005. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Standardi. Suomen Standardisoimisliitto SFS.

SFS-ISO/IEC 27001. 2013. Informaatioteknologia. Turvallisuustekniikat. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Standardi. Suomen Standardisoimisliitto SFS.

SFS-verkkokauppa – Standardit kätevästi netistä. Suomen standardoimisliitto SFS ry. Tuotetiedot. N.d. SFS ry:n verkkokauppa. Viitattu 24.3.2014. http://sales.sfs.fi/sfs/servlets/ProductServlet?action=productInfo&productID=184287

Tietoturva – Kunnat.net. 2014. Viitattu 8.3.2014. http://www.kunnat.net/fi/asiantuntijapalvelut/tyk/tietohallinto/tietoturva/Sivut/default.aspx

Tietoturvallisuus. N.d. Valtionhallinnon tietoturvallisuuden johtoryhmä. Viitattu 19.3.2014. http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp

Uusi versio tietoturvastandardista ISO/IEC 27001. 2013. Tuoteuutiset SFS:n verkkosivuilla. Viitattu 20.3.2014. http://www.sfs.fi/ajankohtaista/tuoteuutiset/tuoteuutiset_2013/uusi_versio_tietoturvastandardista_iso_iec_27001.1777.news

Vahti 7/2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. Valtionhallinnon tietoturvallisuuden johtoryhmä.

Vahti 5/2004. Valtionhallinnon keskeisten tietojärjestelmien turvaaminen. Valtionhallinnon tietoturvallisuuden johtoryhmä.

Vahti 3/2007. Tietoturvallisuudella tuloksia, yleisohje tietoturvallisuuden johtamiseen ja hallintaan. Valtionhallinnon tietoturvallisuuden johtoryhmä.

Vahti 3/2010. Sisäverkko-ohje. Valtionhallinnon tietoturvallisuuden johtoryhmä.

Vahti 3/2012. Teknisen ICT-ympäristön tietoturvataso-ohje. Valtionhallinnon tietoturvallisuuden johtoryhmä.

Vahti 4/2013. Henkilöstön tietoturvaohje. Valtionhallinnon tietoturvallisuuden johtoryhmä.