LAUREA AMMATTIKORKEAKOULU Uuden edellä

Tietoturvallisuuden kehittäminen Yritys Oy:ssä

Vesalainen, Tapio

2011 Leppävaara

Laurea-ammattikorkeakoulu
Leppävaara

Tietoturvallisuuden kehittäminen Yritys Oy:ssä

Tapio Vesalainen
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Huhtikuu, 2011

Sisällys

Laurea-ammattikorkeakoulu **Tiivistelmä**
Leppävaara
Turvallisuusalan koulutusohjelma

Tapio Vesalainen

Tietoturvallisuuden kehittäminen Yritys Oy:ssä

Vuosi 2011 Sivumäärä 56

Tämän toiminnallisen opinnäytetyön tarkoitus on ollut selvittää, mitä asioita kohdeyrityksen on huomioitava, kun laaditaan tietoturvallisuuden hallintajärjestelmää. Tarve opinnäytetyölle ilmaantui, kun Yritys Oy (nimi muutettu) tunnisti tietoturvallisuuden kehittämistarpeensa. Hankkeen tarkoituksena oli kehittää yrityksen yleistä toiminnan laatua, parantaa kilpailukykyä ja vastata asiakkaiden muuttuviin tietoturvatarpeisiin. Hankkeessa tunnistettiin organisaation tietoturvallisuustavoitteet ja määriteltiin organisaation tietoturvapolitiikka. Siihen liittyy turvamekanismien luominen sekä niiden käyttö tietoturvariskien hallintaan.

Opinnäytetyön teoreettinen viitekehys koostuu turvallisuusjohtamisen, riskienhallinnan sekä tietoturvallisuuden hallintajärjestelmän tutkimuksesta. Viitekehyksenä hallintamallissa on käytetty soveltaen ISO 27001 ja 17799 -standardeja. Tässä toiminnallisessa opinnäytetyössä yhdistyvät käytännön toteutus ja kehittäminen tutkimuksellisten työkalujen avulla työelämäkontekstissa ja työn raportointi tapahtuu tutkimusviestinnän keinoin.

Tietoturvallisuus on ennen kaikkea yrityksen johdon asia ja se oli mukana, kun määriteltiin tietoturvallisuuden hallintajärjestelmän kattavuus ja rajat. Työssä tunnistettiin yrityksen riskit sekä analysoitiin ja arvioitiin riskien vaikutukset. Yritykselle luotiin ja otettiin käyttöön riskienhallintasuunnitelma, jonka avulla saavutetaan tunnistetut valvontatavoitteet ja joka ottaa huomioon kustannukset sekä osoittaa roolit ja vastuut. Liiketoiminnan jatkuvuuden hallintaan liittyen tietoturvallisuus sisällytettiin liiketoiminnan jatkuvuuden hallintaprosessiin. Sen avulla otettiin käyttöön suunnitelmat, joilla yrityksen liiketoiminta saadaan ylläpidettyä ja palautettua sekä tiedon saatavuus varmistettua vaaditulla tasolla ja vaadituissa aikarajoissa kriittisten liiketoimintaprosessien keskeytymisen tai toimintahäiriön jälkeen.

Asiasanat: ISO 27001, riskien hallinta, tietoturvallisuus, tietoturvallisuuden hallintajärjestelmä, turvallisuusjohtaminen

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Security Management

Tapio Vesalainen

Development of information security in Company X

Year 2011 Pages 56

The purpose of this functional thesis was to discover what issues the target company has to consider when establishing an information security management system (ISMS). This information was needed when Company X (name changed) identified its information security development needs. The purpose of this development project is to improve the company's overall quality of operations and improve the competitiveness and meet customers' changing security needs. The objective of this project was to understand an organization´s information security requirements and the need to establish a policy and objectives for information security. It involves implementing and operating controls to manage an organization´s information security risks.

The theoretical framework of reference contains the research of corporate security management, risk management and information security management system. The framework of the ISMS comprises of two international standards ISO 27001 and ISO 17799. This functional thesis combines the practical implementation and development of the research tools in the context of work and reporting is conducted using research communications methods..

Security is first and foremost the responsibility of the company's management and it was involved when the scope and boundaries of the information security management system were defined. This project identified the risks and analyzed and evaluated the risks. A risk treatment plan was implemented for the company in order to achieve the indentified control objectives, which includes consideration of funding and allocation of roles and responsibilities. Relating to business continuity management, information security was included in the business continuity management process. It allows the introduction of plans implemented to maintain or restore operations and ensure the availability of information at the required level and in the required time scales following interruption to or failure of the critical business process.

Keywords: information security management system, ISO 27001 standard, risk management, security management

1 Johdanto

Globalisaation myötä yritykset hallinnoivat, tallentavat ja antavat asiakkaiden ja sidosryhmien käyttöön yhä enemmän tietoa sähköisessä muodossa. Yritysten monimuotoinen toiminta ei enää tunne valtioiden rajoja, joten myös tietoverkkojen hyödyntäminen tukee tätä kehitystä. Laajenevia tietoverkkoja ja uusia tietojärjestelmiä hyödyntävä toimintatapa on yritysten operatiivisessa liiketoiminnassa keskeinen toiminto, jonka uusimmat ulottuvuudet yltävät uuden sosiaalisen median hyödyntämiseen. Tässä kehityksessä yritystoiminnan toimintakulttuuri on sosiaalisen median myötä muuttumassa verkostoitumiseen ja monesta monelle periaatteeseen. Uuteen toimintatapamalliin liittyy niin Internet-palvelujen sekä mobiliteetin käytön tuntuva lisääntyminen, joka on yhä tärkeämpi osa liiketoimintaa. Sosiaalisen mediaan myötä on yritysten maineenhallinta siirtynyt tietoverkkoihin. Yritykset ovat yhä haavoittuvampia verkossa olevan tiedon vuoksi. ”Sosiaalinen vuorovaikutus muuttuu tietoverkkovälitteiseksi. Always-on-yhteiskunta laajenee, ja online presence - ja yhteisöpalveluja käytetään entistä enemmän. Yksilöillä on enemmän kuin yksi identiteetti”. (VTT 2010, 21.)

Tiedon turvaaminen on yhä tärkeämpää, kun tietoverkkoja ja -tekniikkajärjestelmiä käytetään yhä enemmän tiedon tallentamiseen, käsittelyyn ja jakamiseen. Yritysten liiketoiminnalle on keskeistä se, että varmistetaan tietotekniikan luotettavuus-, toimintavarmuus- ja käytettävyysvaatimukset. Tietoturvallisuuden hyvä hoitaminen on edellytys yritysten toimintojen ja palveluiden laadulle, tehokkuudelle, kilpailukyvylle ja asiakkaiden luottamukselle yhtiöiden toimintaan. (ISO/IEC 17799 2006, 14.)

Information Security Forum (ISF) on maailman johtavia riippumattomia, voittoa tuottamattomia tietoturvayhteisöjä. ISF on kyselyiden ja tutkimuksen avulla määritellyt tietoturvaa koskevan tietämyksen seuraavasti:

"Jatkuva, vastaanottajille merkityksellinen oppimisprosessi, joka tuottaa organisaatiolle mitattavissa olevia etuja käyttäytymisen pysyvän muuttumisen kautta".

Edellä lainattu kannanotto on ollut keskeinen periaate tehdessäni Yritys Oy:lle kehityshanketta tietoturvallisuuden kehittämiseksi. Opinnäytetyön toiminnallisuudesta johtuen oma asiantuntijuuteni on kehittynyt ja työn eteneminen on ollut samalla oppimisprosessi tutkivaan ja kehittävään työskentelyyn, koska Yritys Oy on toiminnassaan kohdannut edellä kuvattuja uusia haasteita, joita muuttuva toimintakulttuuri, uusi sosiaalinen kanssakäyminen ja alati kehittyvä globaali tietoverkkorikollisuus kohdistaa yritysten tietopääomaa kohtaan.

2 Kohdeyrityksen esittely

Kohdeyritys on monipalveluyhtiö, jonka liiketoiminta muodostuu erilaisista henkilöstöpalveluista, kiinteistön vuokraus- sekä ulkoistammispalveluista. Yritys toimii teollisuus-, rakennus-, logistiikka-, toimisto-, informaatioteknologia-, kiinteistö- ja hoivatoimialoilla. Suomessa se toimii usealla paikkakunnalla ja sillä on myös ulkomaantoimintoja niin Euroopassa kuin Aasiassa. Se on alallaan yksi Suomen suurimmista yrityksistä. Vuonna 2010 yrityksen liikevaihto oli yli 120 miljoonaa euroa ja se työllisti yli 6000 työntekijää. Nopeasti useiden yrityskauppojen avulla kasvanut yritys on perustanut laajentumisensa vahvan toimialaosaamisensa avulla. Yrityksessä on tiedostettu, että tietoturvallisuuden hyvä hoitaminen on edellytys Yritys Oy:n liiketoimintojen ja palveluiden laadulle, tehokkuudella ja asiakkaiden luottamukselle yhtiön toimintaan. Johtoryhmän työskentelyssä on tullut esille, että tarvitaan dynaamisen toiminnan edellyttämä tietoturvallisuuspolitiikka ja – suunnitelma, jolla ohjataan tietoturvallisuutta tärkeänä osana johtamista, osaamista, riskienhallintaa sekä liiketoimintaa. Tähän viitta myös BSI Standard 100-1 standardi, joka mukaan riittävän resursoinnin löytäminen on välttämätön edellytys tietoturvallisuuden kehittämiselle ja ylläpidolle (BSI 100-1 2008,18).

3 Opinnäytetyön merkitys kohdeyritykselle

Opinnäytetyön tutkimus ja tulokset kohdistuvat Yritys Oy:n tietoturvallisuuden hallintajärjestelmän kehittämiseen ja toteuttamiseen. Yrityksessä on käyty keskusteluja siitä, miten kattava, dokumentoitu tietoturvapolitiikka olisi laadittava ja aidosti otettava käyttöön yrityksen liiketoiminnassa. Aiheeseen liittyvät hyvään turvallisuustasoon suuntaavat tietoturvallisuuden järjestelyt sekä tietoturvallisuusorganisaation määrittely. Yritys on aidosti joutunut liiketoiminnan yhteydessä sopimusneuvottelujen keskellä vastaamaan liikekumppanien kysymyksiin siitä, onko organisaation tietoturvallisuudella johdon tuki ja miten johtaminen vaikuttaa tietoturvallisuuden toteuttamiseen? Viranomaisten sekä lainsäädännön asettamat vaatimukset ovat aiheuttaneet tarpeen käsitellä henkilötietoja vaatimusten mukaisesti. Liiketoiminnan laajeneminen ulkomaille ja uusien työntekijöiden tuleminen yhtiöön on saanut turvallisuudesta vastaavat tarkastelemaan tietoturvavaatimuksia uudella tavalla. Yrityksessä havahduttiin turvallisuutta ohjaavan kokonaisuuden puuttumiseen.

Opinnäytetyö jakaantuu yhdeksään päälukuun. Ensimmäisessä ja toisessa luvussa kuvataan opinnäytetyön taustaa sekä kohdeyritystä. Kolmas luku keskittyy opinnäytetyön kohdeyritykselle tuottaman merkityksen käsittelyyn sekä lähtökohtien ja rajausten linjaukseen. Tämän toiminnallisen opinnäytetyön tiedonhankinta ja siihen liittyvien menetelmien kuvaus on neljännessä luvussa. Viides luku käsittää kirjallisuuskatsauksen tietoturvallisuuden johtamisesta. Riskien hallinta ja sen liittyminen tietoturvallisuuteen määritellään kuudennessa luvussa. Seitsemäs luku paneutuu tietoturvallisuuden hallintajärjestelmän ja tekijöiden käsittelyyn.

Työn tulokset Yritys Oy:n tietoturvallisuuden kehittämisestä tuodaan esille kahdeksannessa luvussa. Yhdeksäs luku päättää käsittelyn pohdinnan, johtopäätösten, kehitysehdotusten ja reflektion kautta.

Käsittelen opinnäytetyössä tietoturvaa ja siihen liittyvää toimintaa yrityksessä johdon näkökulmasta. Toiminnallisen vaiheen aikana olin kylläkin tekemisessä hyvin yksityiskohtaisten ongelmien ka kysymysten kanssa, mutta niiden avulla pyrin rakentamaan tarkastelukulmaa yrityksen johdon suuntaan. Marinka Lanne toteaa (2007, 22) turvallisuusjohtamisesta, että se ei kuitenkaan ole erillinen toiminto, vaan luonnollinen osa yrityksen johtamista: taloutta, tavoitteita ja toimintaa. Turvallisuusjohtaminen on siis mukana kaikissa organisaation elinkaaren eri vaiheissa ja yhtyy myös organisaation strategiseen päätöksentekoon. Edelleen Lanne havaitsee, että turvallisuusjohtaminen voidaan nähdä organisaation johtamisena, jossa otetaan huomioon yritysturvallisuuden näkökulma. Laadun kehittämisessä johdon keskeisinä tehtävinä nähdään strategioiden luominen ja hallinta, strateginen johtaminen, politiikan laadinta, politiikan viestiminen sekä politiikan sisäistämisestä ja ymmärtämisestä huolehtiminen. (Lanne 2007, 22-23.)

Åbergin (2006) mukaan päätäntä on prosessi, jossa ongelman havaitseminen, ratkaisuvaihtoehtojen etsintä sekä niiden arviointi ja vertailu muodostavat toisiaan seuraavan ketjun. Tämän tuloksena syntyy valinta, toimintasuunnitelman laadinta ja toteutus sekä valvonta. Åberg toteaa edelleen, että prosessinäkemys korostaa valintaa edeltäviä ja seuraavia tapahtumia. Päätännän laatuun vaikuttavat hänen mukaansa ennen valintaa olevat vaiheet. Johtajan valinnan jälkeiset tapahtumat vaikuttavat siihen, toteutuvatko tehdyt päätökset. Strateginen viestintä jakaantuu neljään vaiheeseen: strategian kuvaukseen, tulkintaan, tulkinnan tarkistukseen sekä strategian jalkautukseen. (Åberg 2006, 120 - 121.)

Opinnäytetyön kohteen Yritys Oy:n tärkein tuotannon tekijä on tieto – ei teknologia. Suojattavia tietoja ovat Yritys Oy:ssä esimerkiksi asiakastietojärjestelmän sisältö ja liiketoimintasuunnitelmat. Niitä voi kuitenkin kohdata erityyppisiä uhkia ja haavoittuvuuksia. Tieto, oli se sitten missä muodossa tahansa Yritys Oy:n käytössä, tulee olla suojattuna koko sen elinkaaren ajan. Ennakointi tietoturvaa kohtaavista uhkista on saatava johdon tietoisuuteen ja turvallisuusvaatimusten luomisen pohjaksi, sillä muutoin haavoittuvuudet, häiriöt ja muut uhkatekijät eivät ole hallinnassa. (ISO/IEC 17799 2006, 14.) Yritys Oy:n tietoturvallisuuden hallintajärjestelmän suunnittelu ja käyttöön ottaminen on johdon strateginen päätös. Johdon päätöksillä laaditaan ne tarpeet, tavoitteet ja tietojen käsittelyyn liittyvät periaatteet, jotka liiketoiminnan kannalta täyttävät keskeisimpien menestystekijöiden suojauksen. (ISO/IEC 27001 2006, 6.)

VTT:n mukaan tietoturvan parantaminen vaatii selkeitä, helppokäyttöisiä ja tehokkaita työkaluja ja käytäntöjä, jotka voidaan ottaa käyttöön organisaatiossa kaikilla tarvittavilla osa-alueilla liiketoiminnan kannalta kriittisten järjestelmien toiminnan jatkuvuuden varmistamiseksi. (VTT 2010, 3.)

3.1 Opinnäytetyön lähtökohdat ja rajaus

Tämän toiminnallisen opinnäytetyön tarkoitus on ollut selvittää, mitä asioita kohdeyrityksen on huomioitava, kun laaditaan tietoturvallisuuden hallintajärjestelmää. Tarve opinnäytetyölle ilmaantui, kun Yritys Oy (nimi muutettu) tunnisti tietoturvallisuuden kehittämistarpeensa. Hankkeen tarkoituksena oli kehittää yrityksen yleistä toiminnan laatua, parantaa kilpailukykyä ja vastata asiakkaiden muuttuviin tietoturvatarpeisiin. Hankkeessa tunnistettiin organisaation tietoturvallisuustavoitteet ja määriteltiin organisaation tietoturvapolitiikka. Siihen liittyy turvamekanismien luominen sekä niiden käyttö tietoturvariskien hallintaan.
Opinnäytetyössä toteutuu Laurean Learning by Developing oppimismalli, jonka kohteena on aidosti työelämän kehittämistilanne. Tässä opinnäytetyössä Learning by Developing –mallilla haetaan vastausta sellaiseen ongelmaan, jonka ratkaiseminen vaatii uuden tiedon luomista. Tutkimuksen aikana oppiminen on vaatinut perehtymistä tietoturvallisuuden hallintajärjestelmään, riskienhallintaan, organisaation prosesseihin ja tiedon soveltamista hallintamallin luomiseen ja käyttöönottoon kohdeyrityksessä. (Fränti & Pirinen 2005, 55.)

Yritys Oy:n tulee liiketoiminnassaan tunnistaa ja johtaa monia toimintoja toimiakseen vaikuttavasti ja tuloksekkaasti. Resurssien käyttö ja tehokas johtaminen mahdollistaa panosten muuttumisen tuotoksiksi. Tämä toimintatapa voidaan mieltää olevan prosessi. Usein yhden prosessin tuotos muodostaa suoraviivaisesti panoksen seuraavalle prosessille. Kansainväliset standardit esittävät tietoturvallisuuden hallinnan prosessimaiseksi toimintamalliksi. Prosessijärjestelmän soveltamisella yrityksen tietoturvallisuuden rakentamisen keskeisiksi asioiksi muodostuvat ISO/IEC 27001 mukaan yrityksen tietoturvavaatimusten ymmärtäminen ja tietoturvapolitiikan sekä tietoturvatavoitteiden määrittäminen. Tätä seuraa turvamekanismin luominen ja käyttö yrityksen tietoturvariskien hallintaan yleisten liiketoimintariskien puitteissa. Prosessin edetessä tarvitaan myös tietoturvallisuuden hallintajärjestelmän valvontaa ja sen suorituskyvyn katselmointia. Jatkuva parantaminen edellyttää objektiivisen mittaamisen käyttöä sekä mahdollisesti ulkopuolista auditointia (ISO/IEC 27001 2006, 6.)

Tässä opinnäytetyössä etsitään ratkaisuja ISO/IEC 27001 standardin pohjalta seuraaviin seikkoihin:

- tietoturvatavoitteiden ja tietoturvapolitiikan määrittäminen
- organisaation tietoturvavaatimusten tunnistaminen

- turvamekanismien luominen sekä käyttö tietoturvariskien hallintaan

Kohdeorganisaation selkeä tahtotila työtä varten on Yritys Oy:n tietoturvallisuuden kehittäminen. Työn pohjalta syntyvän tietoturvallisuuden hallintajärjestelmän tarkoituksena on tietojen sekä niiden käsittelyn, hallinnan ja käytön turvaaminen. Tietoturva on osa Yritys Oy:n konsernin kokonaisturvallisuutta. Tietoturvallisuus kattaa kaikki yrityksen tietojenkäsittelytehtävät koko tiedon elinkaaren ajalta riippumatta siitä millä tavalla tai millä välineillä tietoa käsitellään. Tietoturvallisuus liittyy kaikkiin prosesseihin, joiden avulla pyritään asetettuihin tavoitteisiin yhtiön pitkäjänteisessä ja tuloshakuisessa kumppanuudessa asiakkaiden kanssa.
Tämän tietoturvallisuuden kokonaisnäkymän keskellä opinnäytetyö rajattiin Yritys Oy:n turvallisuuspäällikön hyväksymän suunnitelman pohjalta koskemaan tietoturvallisuuden suunnittelua, riskien arviointia ja turvallisuuspolitiikan luomista.
Tutkimuksen havainnointiosiossa lisäksi myös haastateltiin Yritys Oy:n eri toiminnoissa työskenteleviä henkilöitä ja selvitettiin yrityksen omistaman ja hallinnoiman tiedon luottamuksellisuus, tiedon käsittelytavat ja käyttöoikeudet, arkistointi, tiedon hävittäminen sekä menettelytavat häiriötilanteissa. Havaittujen tulosten ymmärrettäviksi tekeminen edellyttää teoreettista perustelua ja teorian sekä käytännön havaintojen vertailua (Eskola & Suoranta 2005, 82).

3.2 Opinnäytetyön keskeiset käsitteet

Tässä luvussa esittelen opinnäytetyön aiheeseen liittyvät keskeiset käsitteet. Ne perustuvat tietoturvallisuuden hallintajärjestelmän vaatimuksia kuvaavaan ISO/IEC 27001:fi standardin käyttämiin määritelmiin (ISO/IEC 27001, 10).

Eheys on ominaisuus siitä, että suojattavien kohteiden oikeellisuus ja täydellisyys turvataan (ISO/IEC 13335-1, 2004). Tämä ominaisuuden tarkoituksena on varmistaa, että tietoa ei päästä muuttamaan, poistamaan tai niihin ei ole lisätty mitään ilman asianmukaista valtuutusta. Eheyden saamiseksi tarvitaan teknisiä toimenpiteitä kuten salaus.

Käytettävyys on ominaisuus olla saatavilla ja käyttökelpoinen valtuutetun tahon niin vaatiessa (ISO/IEC 13335-1, 2004). Käsitteenä käytettävyydellä tarkoitetaan yleensä järjestelmien teknistä toimivuutta ja toimivuusastetta. Siinä arvioidaan sitä, kuinka suuren osan käyttöajasta järjestelmä ja sen sisältämä tai tuottama tieto on toiminnassa ja käyttäjien saatavilla. Tiedon arvo on usein sidottu aikaan. Tästä on hyvä esimerkki suurissa pörsseissä noteerattujen yhtiöiden pörssitiedotteet, joiden sisältämä tieto on tarkoitettu julkaista tarkoin määrättynä aikana.

Luottamuksellisuus on ominaisuus, että tietoa ei anneta tai paljasteta luvattomille henkilöille, tahoille tai prosesseille (ISO/IEC 13335-1, 2004). Tähän käsitteeseen liittyy paljon julkisen

vallan vaatimuksia, koska esimerkiksi oikeus luottamukselliseen viestintään on turvattu perusoikeutena Suomen perustuslaissa. Viestintäsalaisuuden loukkaaminen on säädetty rangaistavaksi rikoslaissa.

Tietoturvahäiriö on yksi tai useampi epätoivottu tai odottamaton tietoturvatapahtuma, joka merkittävällä todennäköisyydellä vaarantaa liiketoiminnot ja uhkaa tietoturvallisuutta (ISO/IEC TR 18044, 2004)

Tietoturvallisuuden määrittelee standardi ISO/IEC 17799 siten, että se on tiedon luottamuksellisuuden, eheyden ja käytettävyyden säilyttämistä. Lisäksi tähän voi sisältyä muita ominaisuuksia, kuten aitous, vastuullisuus, kiistämättömyys ja luotettavuus (ISO/IEC 17799, 2005)

Tietoturvallisuuden hallintajärjestelmä on osa yleistä toimintajärjestelmää, joka liiketoimintariskien arviointiin perustuen luodaan ja toteutetaan ja jota käytetään, valvotaan, katselmoidaan, ylläpidetään ja parannetaan tavoitteena hyvä tietoturvallisuus. (ISO/IEC 27001, 2006.)

4 Tiedon hankinta ja käytetyt menetelmät

Pinnallisella tai kertaluonteisella tiedolla ei voi ratkaista vähäänkään monimutkaisempaa ongelmaa. Tutkimusprosessille on usein tyypillistä, että se täytyy aloittaa ennen kuin hallussa on täydellistä tietoa tutkimuksen kohteena olevista asioista. Tutkimusprosessin lähtökohtana on silloin, että jokin hyvin yleinen tai epätarkka kysymys on prosessin keskiössä. Vaikka tutkimusprosessin dynamiikkaan kuuluukin se, että nämä epätarkat kysymykset ja epäselvät teoriat tarkentuvat prosessin kuluessa, niin vaarana on kuitenkin yleisten kysymysten aiheuttama ongelmien tai vaihtoehtojen rajautuminen ulos prosessista. (Hakkarainen, Lonka & Lipponen 2004, 337.)

Korsman toteaa tutkimuksen ongelma-asettelusta, että laajaan tutkimusaiheeseen on löydettävissä useita erilaisia ongelmia. Hän esittääkin mielekkäältä tuntuvan näkökulman etsimistä, jonka perusteella tutkimustyölle voidaan asettaa tavoitteet (1999, 9.) Hän tuo esille edelleen, että tutkimustyön alkuosassa rakennetaan teoriakehikko tai käsitejärjestelmä, jota käyttäen tutkimuksellinen aineisto kerätään ja käsitellään. Tutkimuksessa käytetään kokeellista metodia, jossa aineisto voidaan kerätä esimerkiksi havainnoimalla, kyselyllä, tai haastattelulla. Metodin tarkoituksenmukaisuutta tulee pohtia aineiston keruun yhteydessä. Parhaat mahdollisuudet saada sopivin aineisto on silloin, kun käytetään ns. primääriaineistoa eli aineisto kerätään suoraan halutusta kohdejoukosta. (Korsman 1999, 10.)

Sirkka Lauri käsittelee käytännöllisen lähestymistavan ja toimintatutkimuksen luonnetta Paunonen & Vehviläinen-Julkusen teoksessa (2006). Hän esittää toimintatutkimuksen luonnetta tutkimukselliseksi lähestymistavaksi, jossa pyritään teoriatietoa ja käytännön kokemuksellista tietoa yhdistämällä ratkaisemaan organisaatiossa olevia tai myöhemmin ilmeneviä ongelmia. Käytännöllistä lähestymistapaa hän kutsuu vastavuoroiseksi lähestymistavaksi, jossa tutkija ja kohdeorganisaatio yhdessä määrittelevät ongelmat ja niiden taustan. Lauri tarkastele kehittämistyön ideoita käytännön ongelmien valossa ja havaitsee, että tähän lähestymistapaan ei välttämättä kuulu tieteellistä tutkimusta. Tavoitteen asettamiseen sisältyy käytännön kehittäminen olemassa olevin resurssein. Laurin mukaan toimintatutkimus voidaan kuvata syklisenä prosessina. siinä kohdeorganisaatiossa vallitseva tilanne sekä esiintyvät ongelmat kartoitetaan ensimmäiseksi. Seuraavaksi selvitetään esiin tulleiden ongelmien käsittely ja tiedostaminen. Toiminnan uudelleensuuntautumiseen sitoutuminen sekä konkreettinen muutoksen suunnittelu ja toteuttaminen seuraavat prosessissa tämän jälkeen. (Paunonen & Vehviläinen-Julkunen 2006, 114 – 119.)

Toiminnallinen opinnäytetyö tavoittelee tekijän työkokemuksen sekä ammatillisen taidon, alan tietopohjan ja teorian kautta käytännön toiminnan ohjaamista, opastamista sekä toiminnan järjestämistä. Käytettävän toimintatapamallin tai tietopohjan vuoksi sitä on vaikeaa määritellä tutkimukselliseksi prosessiksi. Tärkeää on kuitenkin se, että toiminnallisessa opinnäytetyössä yhdistyvät käytännön toteutus ja kehittäminen tutkimuksellisten työkalujen avulla työelämäkontekstissa ja työn raportointi tapahtuu tutkimusviestinnän keinoin. (Vilkka & Airaksinen 2003, 9.)

Toiminnallisessa opinnäytetyössä toimintatapaan kuuluu tutkimuksellinen selvitys. Työ on opiskelijalle oppimiskokemus, jonka aikana oma henkilökohtainen ja ammatillinen tieto joutuu vuorovaikutukseen ja koetukselle toimeksiantajan toiveiden, kohderyhmän tarpeiden ja ammattikorkeakoulun opinnäytetyötä koskevien vaatimusten välillä. Opiskelijalle asetetaan vaatimukset etsiä, löytää, ratkaista ja pohtia ratkaisujen seurauksia. Opinnäytetyöprosessin ja oppimiskokemuksen kautta ymmärrys ja asiantuntijuus omasta aiheesta kehittyvät, koska toimeksiantajan käytännön työelämä erityispiirteineen opettaa objektiivisen tiedon lisäksi käytännönläheistä näkökulmaa. (Vilkka & Airaksinen 2003, 56 - 58.)

Laurean LbD-mallissa opiskelija osallistuu todellisiin työelämän kehittämishankkeisiin, joissa edellytetään halua ja kykyä hyödyntää tutkivaa ja kehittävää työotetta oppimistehtävissä. Tarkoituksena on tuottaa uutta osaamista niin opiskelijoiden pääomaksi, kuin työelämän ja alueen kehittämiseksi. Työskentelyssä noudatetaan hyvää tutkimuksen käytäntöä, johon kuuluvat järjestelmällisyys, systemaattisuus ja kurinalaisuus. Työskentelyprosessin aikana on oleellista oppia löytämään käsiteltävänä olevan kohteen ja ongelman ydinilmiöt ja niihin liittyvät käsitteet, joiden avulla ilmiötä voidaan jäsentää. (Laurea Fakta 2010 – 2011.)

Toiminnallisessa opinnäytetyöprosessissa voidaan hyödyntää laadullista tutkimusmenetelmää, kun tavoitteena on käsiteltävän aiheen kokonaisvaltainen ymmärtäminen. Laadullinen tutkimusasenne palvelee kirjoittamattoman faktatiedon etsinnässä. Haastattelutavan valinnassa on mietittävä tavoitetta eli tietoa siitä, millaista tietoa selvityksellä halutaan. Jonkin ilmiön tilaa arvioidessa on yksilöllinen teemahaastattelu usein käytetty menetelmä. Sen on vapaa tapa kerätä aineistoa ja toimii toiminnallisessa opinnäytetyössä, mikäli tavoitteena on kerätä tietoa jostain teemasta tai tehdä kohdeorganisaatiolle konsultaatiota. Työn toiminnallisen osuuden onnistumien kannalta on aineiston laatu keskeisempää kuin määrä. (Vilkka & Airaksinen 2003, 63 - 64.)

Tämän opinnäytetyön tietoturvallisuuden teoriakehikko ja käsitejärjestelmä rakentuu kansainvälisten standardien ja kansallisten tietoturvaohjeiden varaan. Kohdeyrityksen tietoturvallisuuden tilaa arvioidessa haetaan kyselyjen ja haastatteluiden avulla tietoa siitä, mitä tutkittavat henkilöt havaitsevat kohdeyrityksessä ja mitä he ajattelevat, tuntevat ja uskovat. Havainnoinnin avulla haetaan tietoa siitä, mitä todella tapahtuu kohdeyrityksessä ja sen toimintaprosesseissa tietoturvallisuuden johtamisen kannalta.

5 Tietoturvallisuuden johtaminen

Tässä luvussa kuvaan sitä, mistä näkökulmista ja miten aihetta on lähestytty aiemmin sekä sitä, millaisiin turvallisuusalan näkemyksiin opinnäytetyö liitetään. Tieto on yritykselle hyödyke, kuten muutkin tärkeät tuotantoon ja liikeomaisuuteen kuuluvat asiat. Tieto on välttämätöntä yrityksen toiminnassa ja tämän vuoksi se on suojattava. Suojaaminen on erityisen tärkeää liiketoiminnan ollessa lisääntyvässä määrissä sidoksissa yrityksen ulkopuoliseen maailmaan. Liiketoiminnan siirtyminen tietoverkkoihin johtaa tiedon altistumiseen yhä monipuolisempien uhkien ja haavoittuvuuksien vaikutuksen alle. Tietoturvallisuus on siten tietojen suojaamista näiltä uhkilta ja haavoittuvuuksilta, jotta liiketoiminnan jatkuvuus, liiketoiminnan riskien minimointi, sijoitetun pääoman tuoton maksimointi ja liiketoiminnan mahdollisuuksien turvaaminen onnistuu. Tietoturvallisuus saavutetaan toteuttamalla sopivia ohjaustoimenpiteitä, kuten politiikkoja, prosesseja, menettelyjä, organisaatiorakenteita ja ohjelmistojen ja laitteistojen toimintoja. Nämä kontrollitoimet perustetaan, pannaan täytäntöön, valvotaan, tarkistetaan ja tarvittaessa parannetaan yrityksen johtamisprosessissa (ISO/IEC 17799 2005, 8.)

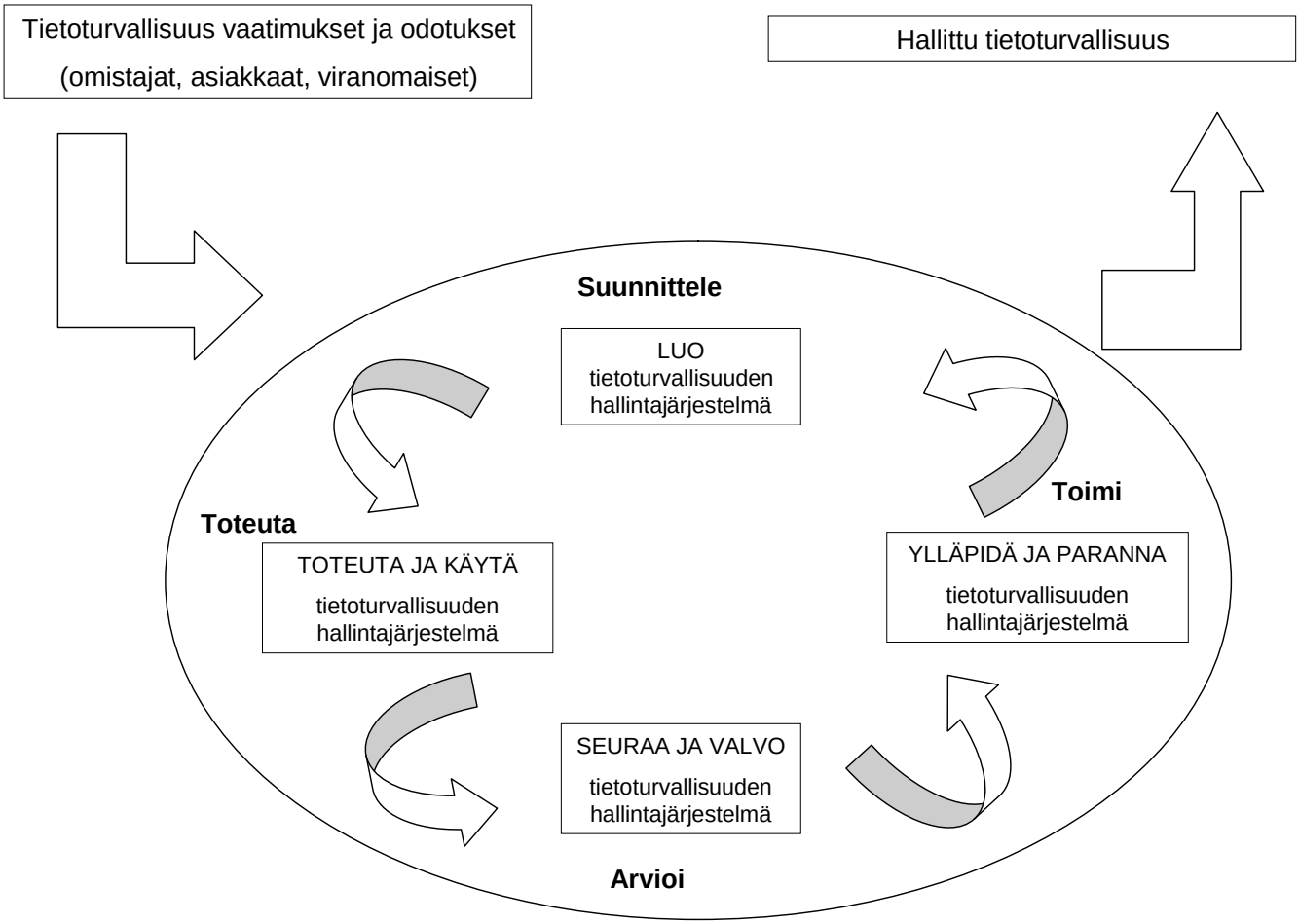
Yrityksen turvallisuustoimintaa ohjaavat periaatteet keskittyvät organisaation ylimmän johdon toimiin ja osuuteen turvallisuustoiminnan määrittelyissä. Johdon hyväksymä turvallisuuspolitiikka ohjaa turvallisuustyön tavoitteita, riskien tunnistamista ja hallintaa, turvallisuusorganisaation toimia ja vastuun jakaantumista. Organisaation turvallisuusdokumentaation tulee

vastata toiminnan ja tuotteiden laajuutta ja toimintatapaa sekä niihin liittyviä turvallisuusriskejä. Organisaation johdolla on selvä toimintatapa valvoa turvallisuuspolitiikan perusteiden mukaista toimintaa. Johdolla on myös vastuu siitä, että turvallisuustoimintaa koskeva lainsäädäntö tunnetaan ja lainsäädännön vaatimukset on huomioitu turvallisuusohjeissa. Perusta sille on se, että turvallisuuspolitiikan sisältö tiedotettu kaikille työntekijöille, jotta heillä on selvä kuva omista turvallisuuteen liittyvistä velvollisuuksistaan ja vastuistaan. (KATAKRI 2009, 8 - 10.)

PDCA-mallilla tarkoitetaan jatkuvaa johtamisen prosessia ja keskeisiä menettelyitä, joilla tuetaan toiminnan suunnittelua, toteutusta, seurantaa ja toiminnan arviointia sekä johtopäätösten tekemistä (Plan – Do – Check – Act). PDCA-malli on otettu perustaksi johtamisen ja laadunhallinnan ISO 9000 -sarjan standardeihin sekä useisiin muihin johtamisjärjestelmästandardeihin. Tutkimuksessa yrityksen tietoturvallisuuden hallintaa pyritään ymmärtämään syklimäisenä ilmiönä. Tämän ymmärrys edellyttää sekä tietoturvallisuuden hallintaan että riskien arviointiin liittyvien käsitteiden pohtimista. Tietoturvallisuuden hallintajärjestelmän keskeisimmät osat ovat ajantasainen tietoturvapolitiikka ja siihen liittyvät asiakirjat sekä säännöllinen, toistuva riskienhallinta. Hallintajärjestelmä on siten osa yrityksen operatiivisista työvälineistä, joilla toteutetaan yrityksen strategiaa (ISO/IEC 27001 2006, 8.)

Tietoturvallisuuden hallintaprosessi eli tietoturvallisuuden kehittämisen ja ylläpitämisen prosessi, jonka tavoitteena on tuottaa hallittu tietoturvakokonaisuus, on PDCA-kehä. Se on kaikessa johtamisessa tärkeä jatkuvan laadun parantamisen mallin menetelmänä. Tietoturvallisuudessa se muodostaa käytännössä kehän sijasta spiraalin, joka kierroksittain kohoaa korkeammalle, mikäli prosessi on toteutunut sille asetettujen tavoitteiden mukaisesti. Menetelmän käyttö tietoturvallisuuden kehittämisen johtamisessa edellyttää laatujärjestelmien ymmärtämistä.

ISO 9000 laatujärjestelmän standardi kuvailee PDCA-mallia koordinoiduksi toimenpiteiksi organisaation suuntaamiseksi ja johtamiseksi. Se on siis johtamisen perusmalli, jonka kehää ja sen kierrosta on esitetty kuviossa 1. Siinä suunnittelun tavoite on luoda tietoturvallisuuden hallintajärjestelmä. Tavoitteen toteuttamisessa kohdeorganisaatio käyttää hallintajärjestelmää tietoturvallisuuden ylläpidossa. Tarkistusvaiheessa arvioidaan toimintaa ja hallintojärjestelmän toimivuutta. Toimi-vaiheessa käydään läpi kaikki vaiheet ja tehdään mahdolliset parannukset seuraavaa vaihetta varten.



Kuvio 1: PDCA-mallin soveltaminen tietoturvallisuuden hallintajärjestelmässä (ISO/IEC 27001 2006, 8)

Opinnäytetyössä hyödynnetään PDCA-mallia (Suunnittele-Toteuta-Arvioi-Toimi) tietoturvallisuuden hallintajärjestelmän hallintarakenteiden prosesseissa. Tietoturvallisten prosessien PDCA-mallin ylläpito- ja kehittämissykliin kuuluu hallintajärjestelmän suunnittelu ja rakentaminen (Plan), sen toimeenpano ja noudattaminen (Do), seuranta ja arviointi (Check) sekä ylläpito ja kehittäminen (Act). Mallin kierros edellyttää organisaatiolta aktiivista toimintaa ja sen tarkoituksena on johtaa toiminnan jatkuvaan parantamiseen.

Tietoturvallisuuden hallintajärjestelmän suunnitteluvaiheessa määritellään tietoturvallisuuden kehittämisen kannalta oleelliset tekijät eli tietoturvapolitiikka, -tavoitteet, -päämäärät, prosessit ja –menettelytavat. Edellä kuvatut ovat yrityksen yleisen toimintapolitiikan ja tavoitteiden mukaiset. PDCA-mallin toteuttamisvaiheessa käytetään tietoturvallisuuden hallintajärjestelmää eli tietoturvapolitiikka, turvamekanismeja, prosesseja ja menettelytapoja. Arviointivaiheessa seurataan ja katselmoidaan tietoturvallisuuden hallintajärjestelmää. Siinä seurataan ja mitataan prosessien suorituskykyä, vertaillaan tuloksia tavoitteisiin ja raportoidaan yrityksen johdolle. Mallin toimintavaiheessa ylläpidetään ja parannetaan tietoturvalli-

suuden hallintajärjestelmää. Auditoinnin ja johdon katselmuksen perusteella ryhdytään korjaaviin ja ennaltaehkäiseviin toimenpiteisiin. (ISO/IEC 27001 2006, 8)

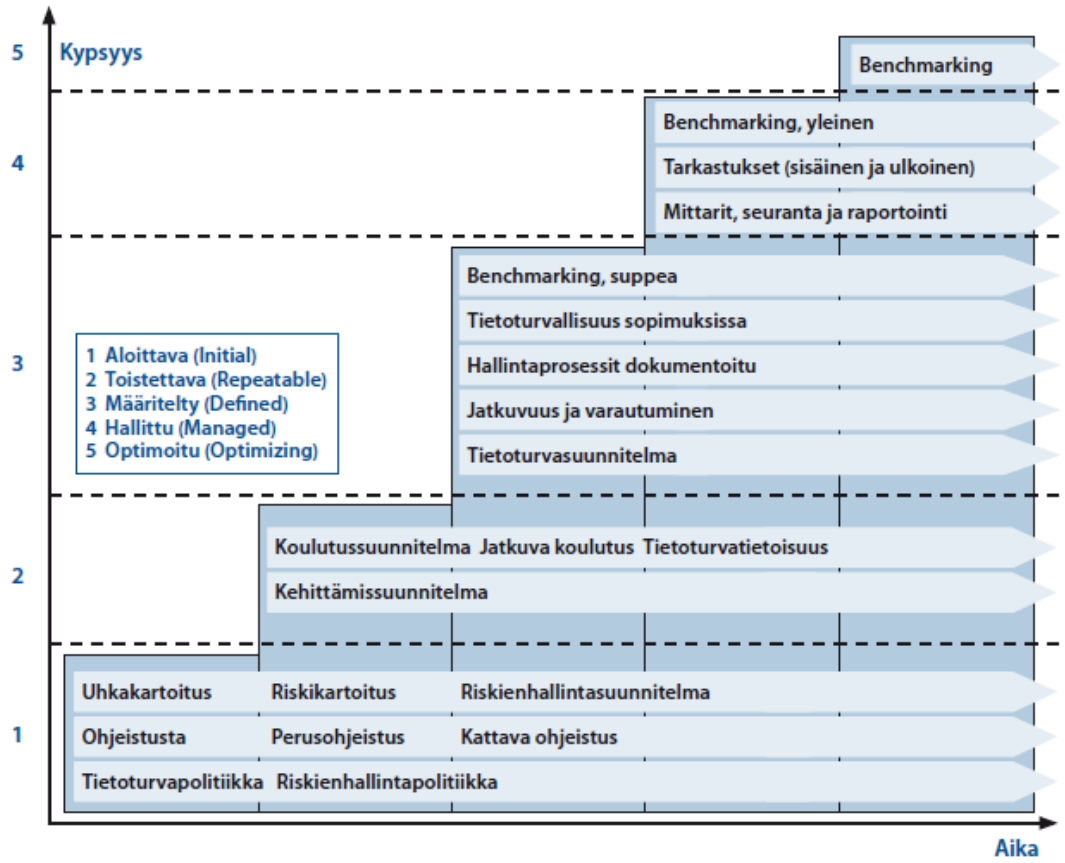
Kuviossa 1 esitetään miten tietoturvallisuuden hallintajärjestelmä käyttää panoksena omistajien, asiakkaiden ja viranomaisten tietoturvavaatimuksia ja odotuksia. Tarvittavien toimenpiteiden ja prosessien tuotoksena syntyy tietoturvatuotoksia, jotka täyttävät asetetut vaatimukset ja odotukset (ISO/IEC 27001 2006,10.)

Tietoturvallisuus on kiinteä osa yrityksen johtamistoimintaa. Perustan onnistuneelle tietoturvallisuudelle luo kyky tunnistaa ja arvioida yrityksen toimintaan liittyvät tietoturvallisuusriskit. Johto voi tämän pohjalta päättää niistä toimenpiteistä, jotka pitää toteuttaa. ”Riskejä hallitessa lähtökohdaksi on otettava organisaation toiminnan kehittäminen, kuten esimerkiksi toimintatavat, osaaminen ja johtaminen. Sen jälkeen tulevat tekniset suojauskeinot”. (VAHTI 7 2003, 10).

Tietoturvallisuuden ja riskienhallinnan luonne on jatkuvaa ja kehittyvää. Ne tulee sisällyttää osaksi organisaation toimintaprosesseja, jotta ne toteutuisivat käytännön toiminnassa. Tietoturvallisuudessa tavoitetason saavuttaminen on yleensä monivuotinen kehityshanke, jonka tavoitteet kuvataan strategisissa toimintasuunnitelmissa ja jaetaan useammalle vuodelle. Lisäksi tietoturvallisuuden kehittyminen ositetaan niin, että vuositasolla kehitystoiminnalle pystytään asettamaan mitattavat tavoitteet sekä osoittamaan tavoitteiden saavuttamiseksi tarvittavat resurssit (VAHTI 3 2007, 38.)

Tietoturvallisuuden kehittymisen yhteydessä voidaan puhua sen kypsyystasoista. Aloittavan tason ominaisuuksia ovat ne, että tietoturvatoimenpiteet perustuvat reaktiiviseen tilannehallintaan, harva toiminto on selkeästi määritelty ja tietoturvallisuuden tulokset saattavat riippua yksilön onnistumisesta. aloittavalla tasolla johtamisen kannalta toimenpiteet ovat tunnistamisen tasolla. Organisaation toistettavan tason tietoturvaprosessit ovat määriteltyjä ja niitä seurataan. Johto tukee ja ohjaa suoraan prosessia. Prosessia voidaan jossakin määrin toistaa. Määritelty kypsyystaso sisältää mallinnetut tietoturvaprosessit, jotka ovat vakiintuneet ja integroitu organisaation menettelyihin. Johtamistoimet ovat osallistumista ja tilan valvontaa. Hallitun kypsyystason tietoturvatoiminnalla on mittarit, tuotokset ja prosessit ovat toiminnassa ja niitä valvotaan ja mitataan. Organisaation johto aidosti johtaa ja suunnittelee tietoturvallisuustoimintaa. Korkeimman kypsyystason eli optimoidun tason ominaispiirteitä ovat esimerkiksi ne, että jatkuva tietoturvan parantaminen on käytössä ja se perustuu kvantitatiivisiin mittareihin, palautteisiin ja innovatiivisiin uusiin ideoihin ja teknologioihin. Johto huolehtii toimintaedellytyksistä ja ennen kaikkea motivoi organisaation toimintaa. Kuviossa 2 tarkastellaan kypsyystason kehittymistä aikaan verrattuna ja siinä on kuvattu esimerkkejä kypsyys-

tasojen tuotoksista.



Kuvio 2: Esimerkki kypsyystason soveltamisesta (VAHTI 3 2007, 42).

Kuviosta voidaan huomata, että kypsyystason portaittainen nousu edellyttää myös konkreettisia tuotoksia, jotka luovat mahdollisuuden seuraavan tason saavuttamiselle.

6 Riskien hallinta

VTT:n yleisen määritelmän mukaan riskillä tarkoitetaan vaaran tai uhkan aiheuttaman haitan mahdollisuutta. Riski on siis mahdollisen vahingon uhkan muodostama todennäköisyys. Riski kostuu aina kahdesta tekijästä: haitasta (sen suuruus ja vahingollisuus) ja haitan toteutumisen todennäköisyydestä. Riskille voidaan antaa matemaattinen kuvaus eli riski on haitan aiheuttavan tapahtuman todennäköisyyden ja haitan suuruuden tulo. Riskin määritelmä rajaa selvästi käsitteen ulkopuolelle haitalliset tapahtumat, jotka tapahtuvat varmasti tai eivät varmasti tapahdu (VTT 2003.)

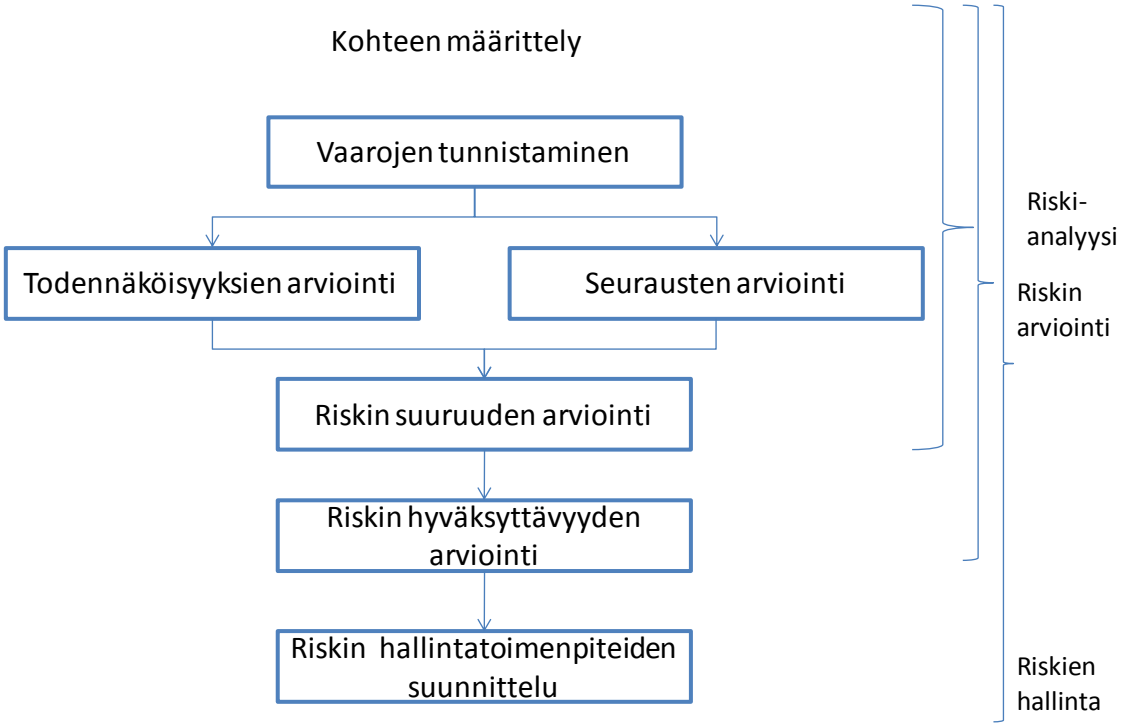
Riskianalyysi voidaan VTT:n mukaan määritellä siten, että se on saatavissa olevan tiedon järjestelmällistä käyttämistä vaarojen tunnistamiseksi sekä riskin suuruuden arviointi. Tämän päättelyketjun tarkoituksena on ymmärtää riskin luonne ja päätellä riskin taso. Edelleen riskin merkityksen arviointi määritellään prosessiksi, jossa tehdään päätökset riskien siedettä-

vyydestä riskianalyysin perusteella. Riskianalyysi luo perustan riskien arvioinnille ja riskien hallintaan liittyvälle päätöksenteolle (VTT 2009, 9.)

Kokonaisuudessaan riskienhallintaan sisältyvät yrityksen toimintakulttuuri, liiketoiminnan prosessit ja organisaatiorakenteet, jotka edistävät mahdollisten edullisten tapahtumien kulkua ja joiden avulla voidaan hallita haitallisia tapahtumia (VTT 2009, 9.)

Käsiteltäessä riskien tunnistukseen, arviointiin ja kontrolleihin liittyviä seikkoja, voidaan esittää kysymys siitä, onko organisaatiolla menetelmät tunnistaa ja arvioida turvallisuusriskit? Luonteva jatkokysymys on näiden menetelmien kattavuudesta normaalin toiminnan sekä erityistilanteiden osalta. Hyvän riskienhallintapolitiikan mukaisesti arvioitavat riskit sisältävät laaja-alaisesti koko organisaation toiminta-alueen. Riskienarviointi tulee olla määritelty osaksi organisaation johtamisprosessia. (KATAKRI 2009, 16 – 17.)

Standardi IEC 60300-3-9 (2006) antaa ohjeita riskianalyysin tekniikoiden valitsemiseksi ja toteuttamiseksi. Kuviossa 3 on riskien hallinnan osien kuvaus, josta voidaan tunnistaa prosessin kolme päävaihetta: analyysi, arviointi ja hallinta.



Kuvio 3 Riskienhallinnan osat standardin SFS-IEC 60300-3-9 (2006) mukaan

Riskejä voidaan hallita monin eri keinoin. Ensimmäinen vaihe riskien hallinnassa on uhkien tunnistaminen. Toisessa vaiheessa tunnistettujen uhkien toteutumisen todennäköisyys ja seu-

raukset arvioidaan. Tämän jälkeen voidaan suunnitella ja päättää riskien hallitsemisen toimenpiteistä. Tässä voidaan nähdä muutama keskeinen vaihtoehto. Ensimmäinen vaihtoehto on riskien välttäminen. Se on todennäköisesti mahdollista vain silloin, kun kyseessä olevasta toiminnasta pidättäydytään erossa. Toinen vaihtoehto on riskin poistaminen, mutta tähän liittyy mahdollisuus uusien riskien syntymisestä. Monimutkaisissa ja yrityksen toiminnassa toisiinsa liittyvissä prosesseissa voidaan yksittäinen riski poistaa kokonaan, mutta tämä toimenpide saattaa aiheuttaa mahdollisesti uusia riskejä. Kolmas keino on riskin pienentäminen. Siinä pyritään estämään ensisijaisesti vahinkojen syntyminen tai niiden seurausten vähentämiseen. Tämä tapahtuu erilaisten kontrollien avulla, jolloin seurausten vakavuuden tai tapahtuman todennäköisyyden avulla saavutetaan toivottu tulos. Riskin siirtäminen on neljäs keino, jonka avulla esimerkiksi sopimuksin tai vakuutusten avulla siirretään tai jaetaan riskikuormaa. Viides yleinen keino on riskin pitäminen omalla vastuulla, jolloin otetaan tietoinen riski siitä, että uhka voi toteutua. Tämä keino valitaan silloin, kun riski kannattaa pitää tai se joudutaan pitämään omalla vastuulla. (VAHTI 3 / 2003, 21.)

Potentiaalisten ongelmien analyysi (POA) on uhkien tunnistusmenetelmä. Sen tavoitteena on löytää määritellyn kohteen keskeisimmät ongelma-alueet sekä keskeisimpiin vaaroihin liittyvät onnettomuustekijät. Tarkastelussa ei etukäteen rajata mitään ongelmatyyppiä analyysin ulkopuolelle. POA on luovan ideoinnin ja työryhmäkäsittelyn yhteistyössä käytettävä menetelmä. Ongelmien analyysissä on useita eri vaiheita. Merkittävien häiriöiden ja vaikutuksiltaan vakavien vaarojen tunnistaminen hiljaisessa aivoriihessä tuottaa vaaraluettelon. Työskentely voi tapahtua myös keskustelun avulla ideoita läpikäyvässä aivoriihessä, jossa edetään järjestelmällisesti arvioitavan toiminnan tai tapahtumien mukaisesti. Häiriöiden ja vaarojen arvioinnissa saadaan tuotoksena alustavat analyysilomakkeet, joissa on käsiteltäviksi valittujen vaarojen syiden ja seurausten selvitys ja riskin suuruutta kuvaavat arvot. Näiden pohjalta luodaan tarvittavat ehdotukset niistä toimenpiteistä, joiden avulla varaudutaan työryhmässä esille tulleisiin uhkiin ja vaaroihin. Toimenpide-ehdotusten kehittäminen tapahtuu seuraavaksi järjestelmällinen tarkastelu arvioinnin yhteydessä. Lopuksi analyysin loppuraportti sisältää lopullisen häiriö- ja vaaraluettelon ja analyysilomakkeet. (VTT 2003.)

Tietoturvallisuuden hallintajärjestelmän luomisen yhteydessä organisaation tulee määritellä liiketoiminnan ominaispiirteiden, organisaation, suojattavien kohteiden ja teknologian perustella ne kriteerit, joita vastaan riskit arvioidaan. Riskien arvioinnin toimintatapaa määriteltäessä organisaation tulee valita sellainen riskien arvioinnin menettelytapa, joka on sopiva tietoturvallisuuden hallintajärjestelmän ja tunnistettujen liiketoimintaa koskevien lakisääteisten ja tietoturvavaatimusten kannalta. Keskeistä on myös se, että organisaatio kehittää sisällään sovitun riskien hyväksymiskriteerin. Samalla on määriteltävä hyväksyttävä riskitaso. Suunnitteluprosessin tarkoituksena on taata valitun riskien menettelytavan toiminta niin, että riskien arvioinnit tuottavat vertailukelpoisia ja toistettavia tuloksia. Riskienhallinnassa organisaation

tehtävänä on tunnistaa riskit, analysoida ja arvioida riskien vaikutukset, jonka jälkeen voidaan tunnistaa ja arvioida riskien käsittelyn vaihtoehdot. Riskien tunnistamisessa keskitytään tietoturvallisuuden hallintajärjestelmään kuuluviin suojattaviin kohteisiin. (ISO/IEC 27001 2006, 15.)

7 Tietoturvallisuuden hallintajärjestelmä

Standardi ISO/IEC 27001 tarjoaa mallin tietoturvallisuuden hallintajärjestelmän rakentamiseen ja hallintaan sekä aihekokonaisuudet, joiden avulla tietoturvallisuutta voidaan arvioida ja katselmoida. Yleensä hallintajärjestelmän katsotaan sisältävän ainakin tietoturvapolitiikan ja – strategian, riskien arvioinnin toimintatavan, tietoturvakäytännöt, kehittämissuunnitelman, tietoturva-arkkitehtuurit eli ratkaisujen peruskuvaukset sekä jatkuvuussuunnitelman (ISO/IEC 27001, 14.)
Arviointiin perustuen organisaation johto voi määritellä asianmukaiset tietoturvallisuuden turvamekanismit, hallintatoimenpiteet, niiden tärkeysjärjestyksen sekä valvontamekanismien käyttöönoton. Näiden toimien tavoitteena on hyvä tietoturvallisuus. Tietoturvallisuuden hallintajärjestelmä kattaa organisaatiorakenteen ja liiketoimintaprosessit sekä kaikki ne johtamismenettelyt, joilla johdetaan, ohjataan ja valvotaan tietoturvallisuusvaatimusten toteuttamista. Johto edistää tavoitteiden saavuttamista ja hallitsee epävarmuuksia suunnitelmilla, päätöksillä, toimenpiteillä ja valvonnalla, jotka ovat osa toiminnan yleistä systemaattista johtamista. Kokonaisuutena voidaan tietoturvallisuuden hallintajärjestelmää käsitellä johtamisjärjestelmän viitekehyksenä, joka on aina sovitettava organisaatiokohtaisesti riippuen tietoturvariskien merkityksestä ja tietoturva-asioiden kehitysvaiheesta organisaatiossa (VAHTI 6 / 2006, 19).

7.1 Tietoturvallisuuspolitiikka

Johdon on tuettava ja ohjattava tietoturvallisuudella liiketoimintatavoitteiden ja asiaankuuluvien lakien ja asetusten mukaisesti organisaationsa toimintaa. Turvallisuuspolitiikassa tietoturvallisuudella on johdon ehdoton tuki. Onnistunut ja asiakkaiden arvostama tietoturvallisuus on yrityksen menestyksen laatu- ja kilpailutekijä. Tietoturvallisuuspolitiikassa yrityksen sisällä on keskeistä johdon ja yksittäisten työntekijöiden ehdoton sitoutuminen turvallisuuspolitiikkaan. Se tulee myös julkaista ja tiedottaa kaikille työntekijöille sekä merkittäville ulkopuolisille sidosryhmille. Tietoturvapolitiikka tulee katselmoida suunnitellusti tai mikäli merkittäviä muutoksia tapahtuu yrityksen toimintaympäristössä. Johdon tulee täten varmistaa politiikan jatkuva soveltuvuus, asianmukaisuus ja vaikuttavuus (ISO/IEC 27001 2006, 32).

Tietoturvallisuuden organisoiminen on keskeinen osa tietoturvallisuuden hallinnassa. Johto ilmoittaa aktiivisesti sitoutumisen tietoturvallisuuteen osoittamalla selkeää suuntaa, näkyvää

sitoutumista ja tietoturvavastuiden selkeää ja yksiselitteistä jakamista. Organisaation eri osien toimijoille on annettava selkeät roolit, joihin tietoturvallisuuteen liittyvät toimet koordinoidaan. Sidosryhmiin ja muihin ulkopuolisiin tahoihin liittyvä tietoturvallisuuden hallinta kuvataan politiikassa niin, että organisaatio pystyy ylläpitämään tiedon ja tietojenkäsittelyn turvallisuutta, kun ulkopuoliset tahot pääsevät näkemään, käsittelemään tai jopa hallinnoimaan organisaation omistamaa tietoa (ISO/IEC 27001 2006, 34).

7.2 Suojattavien kohteiden hallinta

Tietoturvallisuuden hallintajärjestelmän keskeisenä tehtävänä on osoittaa ja saavuttaa organisaation suojattavien kohteiden riittävä suojaus. Turvamekanismi rakentuu kaikkien suojattavien kohteiden selkeästä yksilöinnistä ja luetteloinnista. Jokaiselle kohteelle, niin tiedolle kuin tietojenkäsittelytapahtumalle, määritellään yksiselitteinen omistajuus. Kohteiden käytön määrittelyt ja säännöt yksilöidään ja dokumentoidaan osaksi tietoturvallisuuden hallintajärjestelmää.

Suojattavien kohteiden hallintaan kuuluu myös tiedon luokitus, jossa tieto luokitellaan sen arvon, lakisääteisten vaatimusten, arkaluonteisuuden ja kriittisyyden perusteella. Organisaation omien käyttöönsä määrittelemien luokitteluperiaatteiden mukaisesti ohjeistetaan tiedon merkitseminen ja käsittely (ISO/IEC 27001 2006, 34.)

Tavoitteena on saavuttaa organisaation omat sekä yleiset ja lainsäädännössä määritellyt vaatimukset tietoturvallisuuden osalta sekä varmistaa menettelyt käsiteltäessä salassa pidettäviä ja käytöltään rajoitettuja tietoaineistoja, jolloin asiakkaiden ja sidosryhmien luottamus organisaation ja sen tietojenkäsittelyyn säilyy hyvänä.

7.3 Henkilöstöturvallisuus

Henkilöstöturvallisuus on henkilöstöön liittyvien riskien hallintaa. Se määritellään koskemaan niin organisaation omia työntekijöitä kuin ulkopuolisia tiedon käyttäjiä. Tavoitteena on varmistaa, että työntekijät sekä tietoturvallisuuteen liittyvät ulkopuoliset käyttäjät ymmärtävät velvollisuutensa ja vastuunsa. Heidän tulee olla tietoisia tietoturvallisuuteen kohdistuvista uhkista ja niiden merkityksestä yritykselle. Työntekijöiden tulee osata tukea yrityksen turvallisuuspolitiikkaa tehdessään normaalia päivittäistä työtään. Tämä pitää sisällään kyvyn vähentää inhimillisen erehdyksen mukanaan tuomaa riskiä. Henkilöstöturvallisuus levittäytyy koskemaan koko toiminta-aikaa, jonka työntekijä tai ulkopuolinen henkilö on sidoksissa organisaation toimintaan. Yrityksen tulee määritellä ja dokumentoida turvallisuuspolitiikan mukaisesti työntekijöiden, toimittajien ja ulkopuolisten käyttäjien roolit ja vastuut. Henkilöstöturvallisuudesta huolehtiminen alkaa rekrytoinnin yhteydessä tehtävistä taustatarkistuksista ja turvallisuusselvityksistä. Kaikkien työnhakijoiden, toimittajien ja ulkopuolisten käyttäjien tausta tulee tarkistaa noudattaen asiaan liittyviä lakeja, määräyksiä ja eettisiä normeja. Tar-

kistusten tavoitteena on varmistaa, että henkilö on sopiva erityistä luotettavuutta edellyttävään tehtävään. Suuri osa henkilöstöturvallisuudesta muodostuu ihmisten asenteista ja toiminnasta. Työsuhteen aikana tietoturvaohjeistus, sääntöjen tiedottaminen ja valvonta sekä koulutus ovat niitä menettelyjä, joita käyttämällä organisaation johto voi edellyttää työntekijöitä, toimittajia ja ulkopuolisia käyttäjiä noudattamaan tietoturvallisuutta organisaatioon luotujen periaatteiden ja menettelytapojen mukaisesti (ISO/IEC 27001 2006, 36.)

Valtiovarainministeriön Vahti-ohjeessa todetaan, että usein uhkana pidetään pelkästään organisaation oman henkilöstön aiheuttamia vahinkoja, tahallisia (ei-tuottamuksellisia) tai tahattomia (tuottamuksellisia), mutta on muistettava myös se, että organisaation rakenteella ja sen panostuksella tietotekniikkaan on suuri merkitys (VAHTI 2/2008, 20). Valtionvarainministeriön ohjeesta voidaan edelleen huomata, että karkeasti ottaen noin puolet kaikista tietoturvarikkomuksista liittyy organisaation menettelytapoihin. Henkilöstöturvallisuuden tarkastelun kohteena kannatta käsitellä teknologian, organisaation, ihmisen, työtehtävän ja työympäristön välistä yhteyttä.

7.4 Fyysinen turvallisuus

Fyysisen turvallisuuden kokonaisuus sisältää organisaation tuotanto- ja toimitilojen fyysiseen suojaamiseen liittyvät asiat, joiden tavoitteena on estää luvaton tunkeutuminen organisaation toimitiloihin ja tietoaineistoihin. Tavoitteena on myös estää toimitilojen ja tietoaineistojen vahingoittuminen sekä toiminnan häiriintyminen. Fyysisen tietoturvallisuuden osa-alueeseen kuuluvat mm. kulunvalvonta, tekninen valvonta ja vartiointi, palo-, vesi-, sähkö-, ilmastointi ja murtovahinkojen torjunta sekä tietoaineistoja sisältävien lähetysten turvallisuus (VAHTI 1/2002, 7).

Fyysinen turva-alue rajataan turvasulkujen avulla kuten esimerkiksi seinillä, kulunvalvontakorttien avulla valvotuilla kulkuporteilla tai miehitetyillä vastaanottopisteillä. Näillä turvarajoilla suojataan alueita, joilla on tai sijaitsee tietoa ja tietojenkäsittelypalveluita. Ulkoisia ja ympäristön aiheuttamia uhkia vastaan tarvitaan myös fyysinen suojaus. Turvamekanismit suunnitellaan ja rakennetaan riskianalyysin pohjalta tulipalojen, tulvien, maanjäristysten, räjähdysten, mellakoiden ja muiden luonnollisten tai ihmisen aiheuttamien katastrofien varalta. ISO/IEC 27001- standardi käsittelee turvamekanismeja ja se koskee julkista pääsyä organisaation tiloihin, toimituksia sekä kuormausalueita. Standardin mukaan kulkualueita, kuten toimitus- ja kuormausalueita sekä muita pisteitä, joissa luvattomat henkilöt saattavat päästä tiloihin, tulee valvoa ja ne tulee mahdollisuuksien mukaan eristää tietojenkäsittelyprosessista (ISO/IEC 27001 2006, 38.)

Organisaation tietojenkäsittelyyn liittyvät laitteistot tulee sijoittaa tai suojata siten, että ympäristövaarojen ja luvattoman tunkeutumisen riskejä vähennetään. Nämä laitteistot suojataan sähkökatkoilta ja muilta toiminnan peruspalvelujen katkosten aiheuttamilta häiriöiltä. Laitteisiin liittyvä sähkökaapelointi sekä tieoja siirtävä tai tietotekniikka palveluita tukeva tietoliikennekaapelointi suojataan salakuuntelulta ja vaurioilta. Laiteturvallisuuteen kuuluu myös se, että laitteistoja huolletaan asianmukaisesti käytettävyyden ja eheyden ylläpitämiseksi. Mikäli organisaatiolla on tarvetta työskennellä omien tilojen ulkopuolella, on turvallisuusvaatimusten koskettava myös tilojen ulkopuolelle vietyjä laitteita. Laitteita, tietoaineistoja eikä ohjelmia ei saa siirtää pois organisaation tiloista ilman ennalta saatua valtuutusta (ISO/IEC 27001 2006, 38.)

7.5 Tietoliikenneturvallisuus

Hyvään tietoturvallisuuden hallintajärjestelmään kuuluu kyky varmistaa tietojenkäsittelypalvelujen asianmukainen ja turvallinen käyttö. Tietoliikenteen turvallisuuteen liittyvät kaikki ne uhat, jotka voivat liittyä verkon yksittäiseen laitteeseen tai muuhun osaan tai niiden käyttämiseen. Näitä yleisiä uhkia ovat esimerkiksi inhimilliset vahingot, osaamattomuus, kokemattomuus, laitteistojen kokoonpano- ja määrittelyvirheet, datan korruptoituminen sekä ohjelmisto- ja siirtovirheet (VAHTI 2/2001, 4.)

Tietoliikenteen ja käyttäjätoimintojen hallintaan tarvitaan kirjalliset menettelyohjeet. Nämä tulee dokumentoida ja niitä tulee ylläpitää. On myös huolehdittava siitä, että ne ovat sellaisten organisaation jäsenen saatavilla, jotka tarvitsevat niitä toiminnassaan. Mahdollisia tietojenkäsittelypalvelujen ja –järjestelmien muutoksia tulee valvoa. Organisaatiossa kehitettävänä, testattavina ja tuotantokäytössä olevat palvelut tulee erottaa toisistaan, jotta pienennetään tuotantojärjestelmän luvattoman käytön tai muutosten riskiä. Ulkopuolisten palvelujen hallinnassa tulee varmistaa, että ulkopuolinen palveluntuottaja toteuttaa, käyttää ja ylläpitää sovittuja turvamekanismeja, palvelumäärittelyjä ja toimitustasoja. Ulkopuolisen tahon toimittamia palveluita, raportteja ja tallenteita tulee tarkkailla ja katselmoida säännöllisesti. Mikäli palveluihin tulee muutoksia, tulee muutos hallita ottaen huomioon kyseisen liiketoimintajärjestelmän kriittisyys riskien arvioinnin kannalta. (ISO/IEC 27001, 40-42.)

7.6 Käyttöturvallisuus

Käyttöturvallisuudella luodaan ja ylläpidetään tietoverkkojen, -koneiden sekä –ohjelmistojen turvallisen käytön edellyttämät toimintaolosuhteet. Käyttöturvallisuuden varmistamiseksi laaditaan tietojärjestelmien pääsynvalvonnan toimintaperiaatteet liiketoiminta- ja turvallisuusvaatimusten perusteella. Toimilla on varmistettava valtuutettu käyttäjien pääsy ja samalla estettävä luvaton pääsy tietojärjestelmiin. Kaikissa usean käyttäjän tietojärjestelmässä

tulee olla käyttöoikeuksien rekisteröinnistä menettelyohjeet. Varsinkin etäoikeuksien jakamista ja käyttöä pitää rajoittaa ja valvoa. Jaettavien salasanojen myöntämistä on valvottava määritellyllä hallintaprosessilla. Kaikilta käyttäjiltä tulee vaatia hyvän turvallisuuskäytännön noudattamista salasanan valinnassa ja käytössä. Papereita ja siirrettäviä tallennusvälineitä koskeva puhtaan pöydän politiikka, jossa jokainen on velvollinen huolehtimaan osaltaan tietoa sisältävien papereiden ja sähköisten tallennusvälineiden huolellisesta säilyttämisestä, otetaan käyttöön. Verkkoon pääsyn valvonnan tarkoituksena on estää luvaton pääsy verkkopalveluihin. Etäkäyttäjien pääsynvalvonnan tulee käyttää tarkoituksenmukaisia todennusmenetelmiä. Pääsyä käyttöjärjestelmiin on valvottava turvallisen sisäänkirjausmenettelyn avulla. Jokaisella käyttäjällä tulee olla yksilöllinen tunniste vain käyttäjän henkilökohtaiseen käyttöön. Lisäksi tulee valita soveltuva todennuskeino, jolla varmennetaan käyttäjän väitetty henkilöllisyys. Salasanojen hallintajärjestelmän tulee olla vuorovaikutteinen ja varmistaa salasanojen laatu. Tietokoneen matkakäytössä tulee ottaa käyttöön määritellyt toimintaperiaatteet ja turvamekanismit, joilla suojaudutaan tietokoneen matkakäytön ja etäyhteyksien aiheuttamilta riskeiltä. Samalla tulee etätyötä varten kehittää ja ottaa käyttöön periaatteet, toimintasuunnitelmat ja menettelytavat. (ISO/IEC 27001, 48 - 50.)

7.7 Liiketoiminnan jatkuvuuden hallinta

Yrityksen varautuminen toiminnassaan olevien tietojärjestelmien sekä tietoliikenneyhteyksien keskeytyksiin on tärkeää. Keskeytyksen vaikutus voi koskea laaja-alaisesti koko yhteiskuntaa. Tietoturvallisuuden hallintaa ja ohjausta varten yrityksillä tulee olla toimintaansa liittyvä jatkuvuussuunnitelma, jonka tarkoituksena on ehkäistä liiketoiminnan keskeytyminen ja suojata kriittisiä liiketoimintaprosesseja tietojärjestelmien merkittävien häiriöiden tai onnettomuuksien vaikutuksilta ja taata prosessien viiveetön jatkuminen.
Liiketoimintaprosessit mahdollisesti keskeyttävät tapahtumat tulee yksilöidä samoin kuin tällaisten keskeytysten todennäköisyys, vaikutukset ja seuraukset tietoturvallisuuden kannalta. Yrityksen toimintaan tai tietojenkäsittelytiloihin voi kohdistua vakavia onnettomuustilanteita, joita voivat aiheuttaa tulipalot, vesivahingot, räjähdykset, kaasuvuodot sekä luonnonvoimien aiheuttamat myrskyt, maanjäristykset sekä tulvat. Arvioitaviin uhkiin kuuluu myös itse tietotekniikan laajat vahingot tai niihin kohdistuvat ulkoiset uhkat kuten laajamittaiset verkkohyökkäykset. (VAHTI 3 / 2007, 75.)

Tietoturvallisuuden sisältävien jatkuvuussuunnitelmaan sisällytetään kaikki ne toimenpiteet, joilla liiketoiminta saadaan ylläpidettyä keskeytystilanteessa siihen asti, kunnes se saadaan palautettua alkuperäiselle käyttöasteelle. Tämä edellyttää, että tiedon saatavuus pitää var-

mistaa ja pystyä palauttamaan vaaditulle tasolle vaaditussa aikarajoissa kriittisten liiketoiminnallisten prosessien keskeytymisen tai toimintahäiriön jälkeen (ISO/IEC 27001, 54).

8 Yritys Oy:n tietoturvallisuuden kehittäminen

Kun tarkastelen ajassa taaksepäin ensimmäistä tapaamista Yritys Oy:n edustajien kanssa, niin keskeiseksi asiaksi nousi tarve tuottaa yritykselle konkreettisia tuotteita, joilla yritys pystyisi parantamaan kykyä puuttua mahdollisiin tietoturvaongelmiin ennaltaehkäisevästi. Tavoitteiden asettaminen oli selkeä prosessi. Minulta odotettiin toteuttamisvaiheen aikana uutta tietoa yrityksen käyttöön selvitysten, ohjeiden ja suunnitelmien muodossa. Tavoitteena kaikille tuotteille on niitä hyödyntämällä ehkäistä Yritys Oy:n mahdollisista tietoturvapoikkeamista aiheutuvia haitallisia vaikutuksia.

Opinnäytetyön toteuttamisvaihe jakaantui useaan osaan Yritys Oy:n edustajien kanssa. Työn ja tavoitteiden suunnittelussa olivat mukana talousjohtaja, liiketoimintajohtaja, turvallisuuspäällikkö ja tietoliikennejohtaja. Yrityksen johto tuki ja ohjasi työn toteuttamista. Työn organisointi tapahtui turvallisuuspäällikön johdolla. Tapaamiset olivat havaintojen kirjaamista yrityksen eri toimipisteissä, tietojärjestelmien, dokumentaation ja toimitilojen läpikäyntejä, työ- ja toimintatapatarkasteluja, videoneuvotteluja sekä haastatteluja osoitettuina yrityksen liiketoimintajohdolle ja prosessivastaaville. Avoimilla kysymyksillä pyrittiin laadullisen tutkimuksen tapaan saamaan vastaajat pohtimaan syvällisemmin esitettyjä tutkimuskysymyksiä ja esittämään kehitysehdotuksia ja uusia näkökulmia. Osa haastatteluja perustui suljettuihin kysymyksiin, jotka perustuivat tarkistuslistojen tapaisiin havaintoihin. Kokonaisuudessaan opinnäytetyön toteuttamisvaiheen aikana tutkimuksellisen aihepiirin kysymykset ja havaintokohteet pohjautuivat tietoturvallisuuden standardiin ISO/IEC 27001 sekä Kansallisen turvallisuusauditointikriteeristöön (KATAKRI). Valtiovarainministeriö asettaman Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) antamia ohjeita ja suosituksia käytettiin hyväksi varsinkin henkilöstöturvallisuutta ja hallinnollista turvallisuutta koskevissa tutkimusvaiheissa.

Yhteenvetona tuloksista voidaan havaita, että opinnäytetyön toiminnallisen vaiheen aikana syntyi Yritys Oy:n käyttöön tietoturvallisuuden hallintajärjestelmän tuotteita, joita yritys käyttää päivittäisessä toiminnassaan. Keskeisin tuote on tietoturvallisuussuunnitelma, joka pitää sisällään riskienhallinnan. Tietoturvallisuussuunnitelmassa käsitellään standardin ISO/IES 27001 pohjalta turvallisuudelle asetettuja vaatimuksia hallinnollisen tietoturvallisuuden, henkilöstöturvallisuuden, fyysisen tietoturvallisuuden, tietoliikenneturvallisuuden, käyttöturvallisuuden sekä tietoaineistoturvallisuuden näkökulmista. Suunnitelma sisältää myös tietojärjestelmien jatkuvuussuunnitelman sekä suunnitelman mahdollista poikkeustilanteesta toipumiseen.

Yritys Oy:lle laadittiin opinnäytetyön toiminnallisen osan aikana tietoturvallisuuspolitiikka, jonka yrityksen ylin johto hyväksyi käyttöön otettavaksi. Kaikki opinnäytetyön toiminnallisen vaiheen aikana syntyneet arvioinnit, suunnitelmat ja dokumentit syntyivät kohdeyrityksen toimintaympäristössä ja ovat kohdeyrityksen omaisuutta. Yritys Oy on ottanut ne käyttöön ja tallentanut ne säilytettäväksi omassa sisäisessä tietoverkossaan.

Käsittelen seuraavissa luvuissa toiminnallisen työvaiheen aikana syntyneitä tuotteita, niiden laatimiseen liittyneitä tutkimustuloksia sekä prosesseja.

8.1 Hallinnollinen tietoturvallisuus

Toiminnallisen osuuden alussa keräsin tietoa Yritys Oy:n tietoturvallisuuden nykytilasta. Perehtyessäni konsernin eri liiketoiminta-alueiden toimintatapoihin ja niihin liittyvien haastattelujen kautta kävi ilmi, että Yritys Oy:llä ei ole kirjoitettua tietoturvapolitiikkaa, joten suurimmat ongelmakohdat kohdistuvat pääasiassa hallinnolliseen turvallisuuteen. Strategian ja politiikan puuttumisen myötä tietoturvatyön organisoiminen ja vastuunjako ontuu kuten myös strateginen suunnittelu ja dokumentointi. Samoin yhteinen tietoturvallisuusohjelma ja käytännön ohjeet kuten esimerkiksi työntekijöille jaettavat menettelytapaohjeet puuttuivat. Nopeasti kasvaneen ja toimintaansa eri liiketoiminta-alueille laajentaneen yrityksen tietoturvallisuuden hallintajärjestelmän kehittämisen aloitustilanteessa ei ollut henkilöä, joka olisi vastannut tietoturvallisuudesta ja sen toimeenpanosta systemaattisesti. Tietoturvallisuuden hallinnallinen prosessi oli hajanaista, muutama ohje sähköpostin ja Internetin käytöstä sekä salasanoista ja tietojärjestelmän pääkäyttäjän tehtävistä. Tietoturvallisuuden hallinta oli reaktiivista eikä perustunut riskien hallintaan.

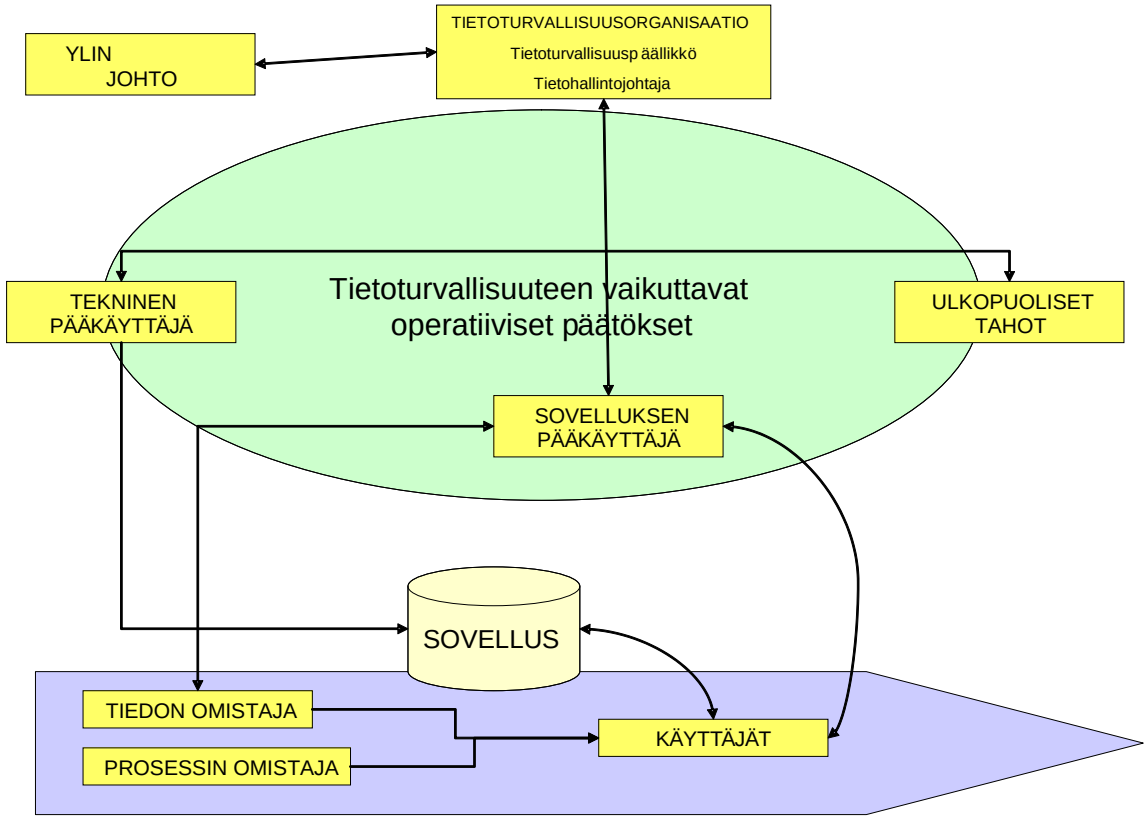
Johtoryhmän kanssa tietoturvallisuuden hallintajärjestelmää ja sen rakentamista suunniteltaessa kävi ilmi, että rakennettavassa Yritys Oy:n turvallisuuspolitiikassa tietoturvallisuudella on johdon ehdoton tuki. Onnistunut ja asiakkaiden arvostama tietoturvallisuus on yrityksen menestyksen laatu- ja kilpailutekijä. Johto linjasi tavoitteeksi sitoutumisen standardien mukaisiin hallintajärjestelmiin. Yritys Oy:n tietoturvallisuusorganisaation tehtävänä ovat luoda kehys, josta liiketoimintayksiköille voidaan muodostaa soveltuvat ohjeistukset. Tietoturvallisuusorganisaatio suunnittelee asiantuntijoiden kanssa teknisen suojauksen rakenteen sekä valvoo, että tietoturvallisuus otetaan riittävässä määrin huomioon kaikissa prosesseissa. Samalla seurataan, että toimijat toteuttavat velvoitteita ja että tietoturvallisuuteen liittyvät seikat on asianmukaisesti otettu huomioon toiminnassa. Seuraavassa taulukossa on esitetty tietoturvallisuuden johtamisen ja hallinnan yleisohjeen (VAHTI 3/2007, 92-96) mukaisesti keskeiset tietoturvallisuuden johtamisen ja toimeenpanon tehtävät rooleittain sovitettuna Yritys Oy:n organisaatioon.

Taulukko 1: Tietoturvallisuuden johtamisen ja toimeenpanon tehtävät rooleittain (VAHTI 3 / 2007)

Rooli	**Vastuu ja toimenpiteet**
Yritys Oy:n ylin johto **Toimitusjohtaja**	• hyväksyy riskienhallinta- ja tietoturvapolitiikan sekä niihin liittyvät periaatteet • vahvistaa tietoturvallisuuden ja riskienhallinnan päälinjaukset • vastaa tietoturvallisuuden ja riskienhallinnan toteutumisesta • nivoo riskienhallinta osaksi johtamistoimintaa • sisällyttää tietoturvallisuus osaksi riskienhallintaa • luo edellytykset ja taata tietoturvallisuuden ja riskienhallinnan tarvitsemat resurssit
Hallintojohtaja **Henkilöstöpäällikkö**	• määrittelee henkilötietojen käsittelyyn liittyvät tehtävät ja niiden vastuualueet erityisesti tietoturvallisuutta ja tietosuojaa koskien • vastaa henkilöstön perehdyttämis- ja tietoturvakoulutuksen järjestämisestä • vastaa henkilöstöhallintoprosessien sisällön määrittelyistä ja ylläpidosta
Turvallisuuspäällikkö	• osallistuu riskienhallinta-, turvallisuuspolitiikan ja -periaatteiden sekä tietoturvapolitiikan määrittelyyn • kehittää riskienhallinta- ja turvallisuuspolitiikan mukaisesti turvallisuuden kokonaistoimintoa ml tietoturvallisuus • ohjaa turvallisuuden käytännön toteutusta tiedon, henkilöstön, toiminnan ja omaisuuden turvaamiseksi ja niihin kohdistuvien riskien hallitsemiseksi • määrittelee perussuojaustason • sidosryhmäyhteyksien hoitaminen viranomaisiin tietoturvallisuusasioissa • tietoturvallisuuden poikkeustilanteiden johtaminen • raportoi ylimmälle johdolle turvallisuudesta, riskeistä ja uhista.
Tietohallintopäällikkö **Järjestelmäasiantuntija**	• tietohallintoon ja tietotekniikkaan liittyvän tietoturvapolitiikan valmistelu ja esittely • hallinnonalan tai organisaation tietoturvallisuuden kehittämistoimenpiteiden ohjaus • tietoturvallisuuden toteutumisen varmistaminen tietohallinnossa sekä • tietoturvallisuuden toteutumisen valvonta ostetuissa tietopalveluissa.

Tietoturvallisuusjohtaja	• kehittää tietoturvallisuutta turvallisuuspolitiikan mukaisesti • huolehtii henkilöstön turvallisuustietoisuuden lisäämisestä ja tietoturvakoulutuksen järjestelystä • ohjaa tietoturvallisuuden käytännön toteutusta ja siihen liittyvää riskienhallintaa ja raportoi ylimmälle johdolle tietoturvallisuudesta, riskeistä ja uhista.

Tietoturvallisuudesta vastaa toimitusjohtaja ja tietoturvallisuutta johtaa tietohallintopäällikkö. Tietoturvallisuuspolitiikka tarkistetaan vuosittain ja tarkistukset dokumentoidaan sekä hyväksytetään Yritys Oy:n johtoryhmässä. Jatkossa yritys pystyy sisäisten ja ulkoisten auditointien tuloksilla osoittamaan, että se kaikilla tasoilla sitoutuu tietoturvallisuustyön vaatimuksiin ja niiden toteuttamiseen. Johdon hyväksymällä turvallisuuspolitiikalla toimitusjohtajan johdolla ohjataan vuotuinen tietoturvallisuuden toimintaohjelma, tietoturvallisuustyön tavoitteet ja painopisteet. Yritys Oy:n tietojärjestelmät jakaantuvat useaan sovellukseen, joilla on omat pääkäyttäjät. Yrityksen liiketoimintaprosessissa käsiteltävällä tiedolla on omistaja. Kuviossa 4 kuvataan pääkäyttäjien ja prosessien tiedon omistajien yhteyttä yrityksen johdosta turvallisuusorganisaation kautta tulevaan turvallisuuteen vaikuttavaan operatiiviseen ohjaukseen.



Kuvio 4: Yritys Oy:n tietoturvallisuuteen vaikuttavien toimijoiden yhteydet

Tietoturvallisuuspolitiikassa yrityksen sisällä on keskeistä johdon ja yksittäisten työntekijöiden ehdoton sitoutumisen tarve turvallisuuspolitiikkaan. Koko konsernin kohdalla lähdetään siitä, että ihmiset tekevät tietoturvallisuuden ja samalla korostetaan, että se on jokaista henkilöä koskeva asia, joka toisaalta velvoittaa yksilöä ja toisaalta myös takaa häiriöttömän toiminnan ja työn jatkumisen. Todennäköisimmät tietoturvauhat ja niistä aiheutuvat riskit ovat käyttäjälähtöisiä. Tietoturvaongelmat voivat syntyä tahattomasti tai tahallisesti. Käyttäjät voivat toimia varsin itsenäisesti ja sivuuttaa Yritys Oy:n oman toimintayksikön tarjoamat tietoturvallisuuden hallinnolliset ja tekniset ratkaisut.

Hallintojohtajan ja turvallisuuspäällikön haastattelujen tuloksena voitiin päätellä, että globalisaatio ja vuorovaikutteinen toimintakulttuuri edellyttää jokaiselta Yritys Oy:n työntekijältä osaamista toimia tietoverkoissa turvallisuusajattelun mukaisesti. Tietoturvallisuuteen kohdistuvat haasteet koostuvat ensisijaisesti Internet-toiminnasta sekä asiakasrajapinnoista. Uusia haasteita tuovat sosiaalinen media sekä verkostoitumisen kautta tapahtuva tietoverkkorikollisuus. Uudet riskit (haittaohjelmat, kalasteluyritykset sekä roskaposti), jotka johtuvat sosiaalisen median palveluihin tuotettuun sisältöön tai jotka johtuvat verkostoitumisesta ja sosiaalisesta kanssakäymisestä sosiaalisen median palveluissa, ovat keskeisessä asemassa tietoturvallisuuden kannalta.

Verkostoituminen ulkoisten toimittajien kanssa lisää saatavilla olevan tiedon määrää sekä nopeuttaa liiketoimintaa ja päätöksentekoa. Verkossa liikkuvan tiedon arvoa tai oikeellisuutta ei aina voi mitata. Verkostot ovat Yritys Oy:n omia sekä palveluntuottajien palveluverkostoja, ja uhkia tietoturvallisuudelle syntyy tietojen siirrosta toimintayksiköiden välillä sekä toimintayksiköiden käyttöoikeuksista toistensa järjestelmiin. Oikeuksien hallinta on nopeatempoista ja tilannekohtaista. Eri osapuolten tietoturvallisuustaso saattaa poiketa toisistaan merkittävästi, eikä erojen selvittäminen ole aina ongelmatonta. Vastuunjakoon on tietoturvallisuuden takaamiseksi kiinnitettävä tällaisessa yhteistyössä erityistä huomiota. Verkostoituminen luo toisaalta myös edellytykset tietoturvallisuuden parantamiselle siten, että tieto hyväksi havaituista toimintatavoista leviää yrityksen sisällä nopeasti.

8.2 Riskien arviointi ja riskianalyysi

Kehityshankkeen edetessä turvallisuuspäällikön kanssa käydyn neuvottelun tuloksena todettiin, että laadin yritykselle tietoturvallisuuden riskienhallinta mallin. Siitä tulee Yritys Oy:ssä jatkuva prosessi, joka sisältää riskin tunnistamisen, todennäköisyyden ja vaikuttavuuden arvioinnin, tarvittavat toimenpiteet, vastuut ja aikataulut. Tietoturvallisuuden riskienarvioinnit toteutetaan säännöllisesti taulukon 1 vastuiden mukaisesti.

Riskienhallintaprosessi on perustana yrityksen tietoturvallisuustyön priorisoinnille. Arvioitavat riskit sisältävät laaja-alaisesti yrityksen koko liiketoiminnan ja mahdolliset erityistilanteet. Ne liittyvät osin yleiseen yritysturvallisuuteen, mutta laadittu riskienhallinnan malli kattaa vain tietoturvallisuuden näkökulmasta riskejä ja niiden vaikutusta. Riskeihin liittyvät asiat otetaan huomioon myös normaalitoiminnasta poikkeavien tilanteiden ja tarvittavien sidosryhmien osalta.

Neuvottelussa todettiin myös se, että kaikki riskit eivät löydy yhdellä menetelmällä. Riskianalyyseissä käytetään useita toisiaan täydentäviä menetelmiä: yksi karkean tason tunnistusmenetelmä, yksi menetelmä teknisen järjestelmän tarkasteluun ja yksi menetelmä ihmisten työtehtävien tarkasteluun. Käytetyt riskianalyysimenetelmät perustuvat usean ihmisen tietojen hyödyntämiseen ja yhteistyössä ideointiin ja pohtimiseen. Oman aihepiirinsä vastuussa olevien henkilöiden tulee tuntea tietoturvallisuuden kannalta analysoitavaa kohdetta eri näkökulmista.

Standardin ISO/IEC 27001 mukaisen tietoturvallisuuden osa-alueiden jaottelu ja niihin liittyvät riskienhallintavastuut Yritys Oy:n organisaation sisällä on esitetty taulukossa 2. Vastuun jako on tehty koskemaan koko konsernin osuutta, riippumatta siitä missä yksittäisessä liiketoiminnan yksikössä esimerkiksi henkilöstöturvallisuuden riskienhallinta tapahtuu.

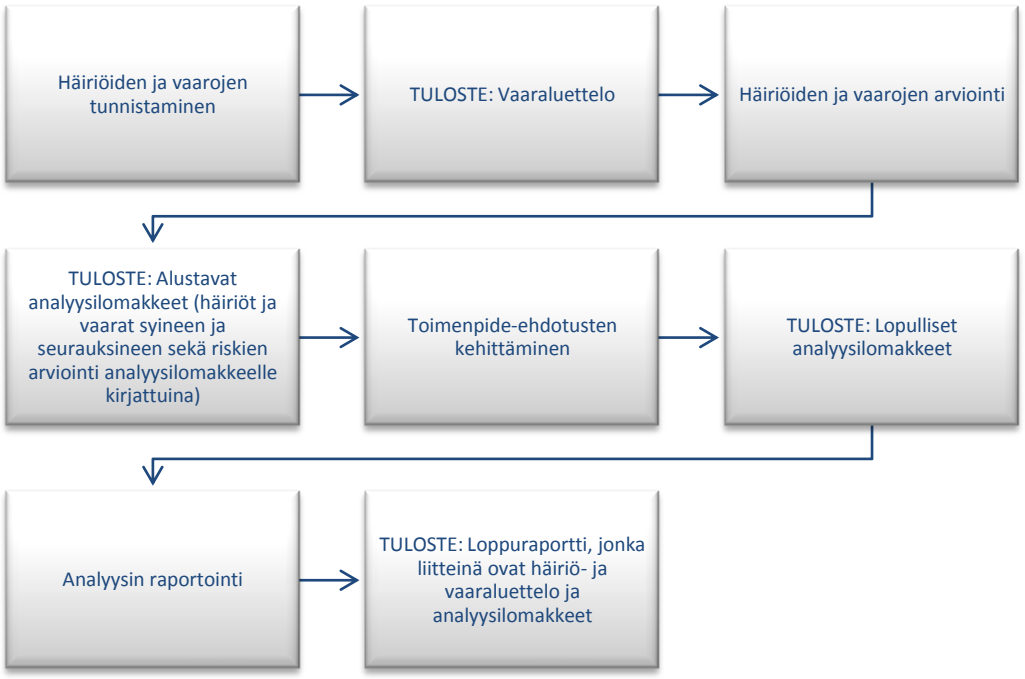
Taulukko 2: Tietoturvallisuuden riskienhallintavastuut Yritys Oy:ssä

Riskityyppi	***Vastaa kartoituksesta***
Henkilöstöturvallisuus	Henkilöstöpäällikkö
Fyysinen tietoturvallisuus	Turvallisuuspäällikkö
Tietoliikenneturvallisuus	Järjestelmäasiantuntija
Käyttöturvallisuus	Hallintojohtaja
Tietoaineistoturvallisuus	Hallintojohtaja
Laiteturvallisuus	Järjestelmäasiantuntija

Riskianalyysi aikataulutetaan niin, että valmius vaikutusten arviointeihin ja tarvittaviin toimenpiteisiin saavutetaan vuosittain maaliskuun alkuun mennessä. Tietoturvallisuuteen liittyviä uhkia ja vaaroja tunnistettaessa sekä arvioitaessa ei haeta syyllisiä, vaan syitä. Kaikkien Yritys Oy:n riskien analyysiin osallistuvien on oivallettava tämä, vaikka jossain yksittäisessä tapauksessa riskit saattavat liittyä yrityksen yksittäisten henkilöiden tekemiin tai tekemättä jättämiin toimenpiteisiin. Pohdittaessa vaarojen tunnistamista on lähtökohtana avoimuus ja rehellisyys, jolloin riskienarviointi on osa laadukasta turvallisuustoimintaa, joka tähtää jatkuvaan toiminnan tason parantamiseen.

On tärkeää tunnistaa, mikä kohteessa on keskeistä ja mitkä riskit ovat suurimmat ja tärkeimmät torjua. Riskit priorisoidaan selvittämällä niiden merkittävyys. Tämä määräytyy mahdollisten vahinkojen suuruuden ja vahingon todennäköisyyden perusteella. Keskitytään siihen, mikä on tärkeää ja saadaan tuloksena perusteet riskienhallinnan toimenpiteiden valinnalle, tärkeysjärjestykselle ja kiireellisyydelle.

Riskianalyysit ja niiden taustalla olevat tiedot dokumentoitiin taulukkolaskennan avulla lomakkeille. Lomakkeet on laadittu ISO/IEC 27001 standardin mukaisesti jaoteltuina tietoturvallisuuden eri osa-alueille. Prosessi eteni vaiheittain kuvion 5 esittämällä tavalla.



Kuvio 5 Tietoturvallisuuden riskienhallintaprosessi Yritys Oy:ssä

Riskien arviointia ja analyysiä varten laadin liitteenä 1 olevan lomakkeen. Sen avulla käsiteltiin vastuuhenkilöiden kanssa kanssa jokaisen ISO/IEC 27001 standardin mukaisen tietoturvallisuuden osa-alueen riskitekijät. Arvioinnissa luokiteltiin taulukkojen avulla tunnistetut riskit niiden vaikuttavuuden ja todennäköisyyden pohjalta. Vaikutusten arvioinnissa otettiin huomioon riskin mukanaan tuoman vaikutuksen liiketoimintaan, aiheutuviin kustannuksiin sekä tietopääomaan. Ongelmaksi muodostui arvioida riskin todennäköisyyttä. Mahdollisuudet epätodennäköisyyden ja todennäköisyyden välillä päädyttiin lopulta kuvaamaan lineaarisesti arvon 0 ja 1 välillä prosenttilukuna. Riski-indeksin laskennassa painotettiin kuitenkin vaikutuksen neliöllä lopullista arvolukua. Yritys Oy ei voi vaikuttaa riskin olemassaolon todennäköisyyteen. Vaikuttavuuden arvioinnin kautta voidaan nostaa konkreettiset uhkat paremmin esille ja antamalla niille korkeampi painoarvo saadaan riski-indeksin kautta luokiteltua esille yrityksen toiminnan kannalta tärkeimmät tietoturvallisuuden uhkatekijät.

Tietoturvallisuuden riskianalyysin pohjalta kerättiin Yritys X:n toiminnan kannalta kriittisimmistä kohteista tietoturvallisuuden liitteenä 2 oleva kehittämissuunnitelma, jossa käsitellään riskin hallinnan toimenpiteet sekä aiheutuvat kustannukset. Kehittämissuunnitelma laadittiin jokaisesta tietoturvallisuuden osa-alueesta. Samalla se muodosti toimenpideohjelman ja kustannuslaskelman tietoturvallisuuden hallintajärjestelmään.

8.3 Henkilöstöturvallisuus

Yritys Oy:n henkilöstöhallinnossa tietoturvallisuuden kannalta keskeiseksi tavoitteeksi havaittiin suunnitelmallinen ja järjestelmällinen henkilöstön kehittämien, johtaminen ja henkilöstöasioiden hallinto. Hallintojohtajan ja turvallisuuspäällikön kanssa laaditun selvityksen pohjalta voitiin todeta, että henkilöstöturvallisuus on ennen kaikkea henkilöstöön liittyvien riskien hallintaa. Arvioitavina kohteina käytettiin henkilöstön soveltuvuutta, toimenkuvia, sijaisjärjestelyjä, tiedonsaanti- ja käyttöoikeuksia sekä valvontaa.

Tietoturvallisuuden hallintajärjestelmän teknisten ja toiminnallisten menetelmien käytön lisäksi suuri rooli jää henkilöstölle ja sen asenteille sekä toiminnalle. Opinnäytetyön yhteydessä laaditulla tietoturvallisuusohjeella määritetään yksikäsitteisesti henkilöiden tietoturvallisuuteen liittyvät vastuut ja velvollisuudet. Jokaiselle työntekijälle jaetaan laadittu tietoturvallisuusohje, jonka jälkeen työntekijä allekirjoittaa sitoumuksen noudattaa yrityksen turvallisuuspolitiikkaa. Tämän lisäksi erityisiä vastuita määritellään yrityksen avainhenkilöiden osalta erillisten työsopimusten tai muiden vastaavien sitoumusten perusteella. Henkilöiden vastuuja velvollisuuskuvauksissa on määritelty muun muassa salassapitovelvollisuuksiin, henkilöstöja asiakastoimintaan liittyvien tietojen käsittelyyn sekä muiden erityisluontoisten tietoaineistojen käsittelyyn liittyvät velvoitteet.

Henkilöstöturvallisuuteen liittyvässä riskien arvioinnissa tarkasteltiin seuraavia tekijöitä mahdollisten vahinkojen määrän rajoittamiseksi. Mahdollisen vahingon tapahtumisen todennäköisyyden pienentämiseksi arvioitiin henkilöstön sijoittelua. Turvallisuuden kannalta paras periaate olisi tiedon tarpeen määrittely niin, että se on vain tarvittavissa määrin käytettävissä niiden kohdalla, jotka sitä työssään tarvitsevat. Yritys Oy:n kohdalla tietojärjestelmien sisältö sekä sisäisen tietoverkon rakenne poikkesivat tästä mallista. Osa henkilöstöstä, joka pääsi käyttämään tietovarantoja, oli konsultti-suhteessa Yritys Oy:n palveluksessa. He eivät siis kuuluneet vakituiseen henkilökuntaan.
Yrityksen eri toimitiloissa liikkumisen ja toiminnan rajoituksia oli käytössä, mutta ne kohdistuivat lähinnä yrityksen ulkokehään. Kulunvalvonta organisaation tiloihin oli järjestetty asiallisesti. Osassa toimitiloja oli kulunvalvontapisteen jälkeinen tila vailla erityistä valvontaa. Tiloja ei oltu myöskään jaettu toiminnallisiin osiin, vaan tiloja käytettiin ristiin eri toiminnoissa, jolloin asiakkaat joutuivat liikkumaan tiloissa, jotka eivät olleet säännöllisesti asiakastiloja. Tietoturvallisuuden kannalta korostui tietoa sisältävien aineistojen ja laitteiden asianmukainen hallinta ja säilytys tiloja käytettäessä. Yrityksessä ei ollut käytössä erilaisia käyttäjärooleja ja niiden mukaista tietojen saatavuutta tietojärjestelmissä. Yrityksen tilojen valvontalaitteistot, tietojärjestelmien lokitiedostot ja niiden automatisoitu valvonta olivat käytössä, mutta niitä ei kohdistettu estämään tietojen väärinkäytön yrityksiä ja paljastamaan mahdollisesti tapahtuneita väärinkäytöksiä.

Avainhenkilöihin kohdistuvat riskit arvioitiin riskienhallintataulukoilla ja toipumissuunnitelman tarpeisiin laadittiin henkilöstösuunnitelma, jossa kuvattiin taulukon 3 avulla. Avainhenkilöiden merkitys oli keskeinen tarkastelun kohde, koska tehtävänkuvaus ei aina ilmaissut riittävän selvästi henkilön merkitystä yrityksen liiketoiminnan kriittisten toimintojen kannalta. Liiketoimintaprosessit ja niiden tietojärjestelmien kriittisyys määrittelivät henkilön korvattavuuden merkityksen. Samalla määriteltiin se aika, joka yritykseltä menee avainhenkilön menetyksen aiheuttaman vajeen korjaamiseen toipumisaikana.

Taulukko 3: Yritys Oy:n avainhenkilöt

Nimi	Tehtävä	Merkitys	Korvattavuus / toipumisaika
N			
N^x			

Riskienhallintatoimenpiteiden painopiste on yrityksen rekrytointiprosessissa sekä henkilön työsuhteen päättymisen aikana. Yritys Oy on keskittynyt näihin toimintoihin hyvin. Henkilöstön työhönoton aikana on varmistettu, että uuden työntekijän pääsy tietoon, tietojenkäsittelylaitteisiin ja liiketoimintaprosesseihin on ollut tietoturvallisuuden vaatimusten kannalta kontrolloitua. Myös yrityksen muuttuvan liiketoiminnan vaatimukset asettavat jokaisen uuden tehtävän arvioinnin piiriin. Yritys Oy:ssä kaikkien tietojärjestelmän käyttäjien valtuuttamisprosessi käydään lävitse ennen kuin heille annetaan pääsyoikeuksia tietojärjestelmiin. Jokainen henkilö allekirjoittaa tietoturvallisuuteen sitouttavan sitoumuksen. Kaikkien, jotka tarvitsevat saada käsiteltäväkseen tai tietoonsa vähintään luottamuksellisia tietoja, luotettavuus selvitetään asiaan kuuluvalla tavalla turvallisuusselvityksen avulla. Selvitys tehdään myös yrityksessä niiden henkilöiden osalta, joiden tehtäviin kuuluu turvaluokiteltuja tietoja sisältävien tieto- tai tietoliikennejärjestelmien tekninen käyttö tai kunnossapito. Turvallisuusselvitys tehdään voimassa olevan lainsäädännön mukaisesti henkilön yksityisyyden suojaa kunnioittaen. Tarkoituksena on saada varmuus siitä, että henkilö on taustaltaan luotettava ja hän on elämäntavoiltaan ja toimintatavoiltaan sellainen, että hänen käsiteltäväkseen voidaan työtehtävissä uskoa luottamuksellisia tietoja. Mikäli henkilöllä on työtehtäviensä vuoksi oikeus päästä Yritys Oy:n tehtävien kannalta oleellisiin liiketoiminnan tietoihin tai tietoliikennejärjestelmiin ja näin tilaisuus päästä merkitykseltään keskeiseen tai suureen määrään turvaluokiteltua tietoa, kohdistetaan häneen mahdollisimman tehokkaasti hyväksi taustatutkimustekniikkaa. Henkilöstön luotettavuuden selvittäminen toteutetaan pääasiallisesti turvallisuusselvitysmenettelyllä, laki turvallisuusselvityksistä (177/2002) mukaisesti. Yrityksellä on palveluksessaan myös sellaisia henkilöitä, jolla ei ole tehtävien mukaista valtuutusta päästä luotta-

muksellisiin tai salassa pidettäviin tietoihin. Näitä ovat esimerkiksi lähetit, kiinteistön kunnossapitohenkilöstö sekä siivoojat. He ovat työtehtävissään kuitenkin tekemisissä turvaluokiteltujen tietojen kanssa liikkuessaan tiloissa, jossa näitä tietoja käsitellään tai säilytetään. Rekrytoitaessa näitä henkilöitä on luotettavuus ensin asiaan kuuluvasti selvitettävä.

Henkilöstöturvallisuuden kokonaisuuden tarkastelemiseksi laadin opinnäytetyön toiminnallisen vaiheen aikana liitteenä 3 olevan taulukon. Sen tarkoituksena on antaa turvallisuuspäällikölle ja hallintojohtajalle kokonaiskuva henkilöstön käyttöoikeuksista ja sitoumuksista yrityksessä, joka toimii usealla paikkakunnalla eri liiketoimintayksiköissä ja monissa tietojärjestelmissä. Kokonaiskuvan avulla voidaan tarkastella henkilön käytössä olevia tietojärjestelmiä ja verrata niitä hänen todelliseen tehtävänkuvaukseen. Mahdolliset työtehtäviin kuulumattomat käyttöoikeudet poistetaan. Turvallisuuspäällikkö valvoo etenkin ns. admin-oikeuksilla olevien toimintaa tietojärjestelmissä. Henkilöstöturvallisuuden riskiarvioinnissa tarkastelun kohteina olivat myös monitasoinen turvajärjestelyn käyttö, vaarallisten työyhdistelmien välttäminen sekä usean henkilön yhtäaikainen läsnäolo kriittisissä toiminnoissa. Yritys Oy on järjestänyt toimenpiteillään henkilöstöturvallisuuden näiltä osin toimivaksi, joten riskienhallinnan arvioinnissa esille ei noussut uhkaavia vaaroja tältä osin.

Yritys Oy:llä on liiketoiminnassaan useita ulkopuolisia työntekijöitä sekä palveluntuottajia ostopalveluiden kautta. Palveluyritysten kanssa tulee tehdä turvallisuus- tai salassapitosopimus. Turvallisuussopimus on laajempi koko palveluntuottajayritystä ja sen tietoturvallisuutta koskeva sopimus. Salassapitosopimuksella huolehditaan erityisesti henkilöstöturvallisuusjärjestelyistä. Yksittäisten ulkopuolisten työntekijöiden kanssa on Yritys Oy tehnyt salassapitosopimuksia.

8.4 Fyysinen tietoturvallisuus

Fyysinen turvallisuus liittyy yrityksen kokonaisturvallisuuteen. Tietoturvallisuuden näkökulmasta huolella toteutettu fyysinen turvallisuus on yksi turvallisuuden perustekijöistä, joka takaa muiden tietoturvallisuuteen kuuluvien osien toiminnan. Yritys Oy:ssä käytetään tilaturvallisuusluokkia, jossa turvattavat tilat, tilaryhmät ja alueet jaetaan turvallisuusryhmiin. Yrityksen toimitilojen ulkokehän jälkeen ovat yleiset tilat, tilaryhmät ja alueet. Näitä ovat esimerkiksi asiakasneuvonnan tilat sekä neuvotteluhuoneet ja sosiaalitilat. Työntekijöiden huoneet ja konsulttien käyttämät työpisteet kuuluvat valvottuihin työtiloihin. Rajoitettujen tilojen ryhmään kuuluvat yrityksen arkistotilat. Yritys Oy on siirtänyt tietojärjestelmien palvelimet ulkopuolisen palveluntuottajan tiloihin. Tämä huolehtii siitä, että niissä tilat kuuluvat erityistiloihin, joiden kulunvalvonta sisäänkäynnissä tai kaikilla turvarajoilla on tunnisteen ja salasanan muodostaman tunnisteen suojaama. Muissa yritys Oy:n toimitiloissa on kulunvalvon-

ta sisäänkäynnissä, joissa vastaanottovirkailija valvoo henkilön tunnistamisen kuvallisten henkilökorttien avulla.

Yritys Oy:n kriittiset tietotekniset laitteistot, jotka vaativat katkotonta sähkön syöttöä, dokumentoitiin ja käsiteltiin riskienarvioinnissa. Tärkeimmät varasähkön piiriin kuuluvat laitteet ovat palvelimet, jotka sijaitsevat palveluntuottajien tiloissa. Arvioinnin perusteella niille suunnitellaan varasähkö kaikkien järjestelmien hallittuun alasajoon varsinaisen sähkönsaannin häiriintymisen aikana. Kaikki Yritys Oy:n toimitilat ovat suojassa luonnonmullistusten aiheuttamilta myrsky- ja tulvatuhoilta. Rakennustekniikan aiheuttamat vesivahingot havaittiin riskien arvioinnissa uhkatekijäksi useassa toimipisteessä. Riskien arvioinnin kautta selvisi, että osassa yrityksen toimitiloja puuttuivat vesi- ja palo- ja rikosvahinkoja suojaavat turvamekanismit. Tietoturvallisuutta kehitettiin suojaamalla asiakirjat, salkkutietokoneet, älypuhelimet sekä muistitikut palo- ja murtosuojattuihin kaappeihin työskentelyn päättyessä. Riskien kartoituksen yhteydessä huomattiin, että normaalin toimistoajan ulkopuolisesta kulunvalvonnasta ja mahdollisista havainnoista yrityksen tiloissa tapahtuvasta poikkeavasta toiminnasta ei tullut ulkoistetun vartioinnin kautta tietoja yrityksen turvallisuuspäällikölle.

8.5 Tietoliikenne- ja tietojärjestelmäturvallisuus

Toiminnallisen vaiheen aikana tutustuin kahteen eri otteeseen Yritys Oy:n tietoliikenneturvallisuuteen. Päällimmäiseksi kuvaksi jäi se, että monet asiat on toteutettu hyvin kuten esimerkiksi tekniset suojaukset jokapäiväisessä toiminnassa. Yritys Oy:n tietoliikennettä ja verkon turvallisuutta arvioitiin riskien hallinnan avulla tekemällä laajamittainen haastattelu Yritys Oy:n eri toimipisteissä. Haastattelu pohjautui ISO/IEC 27001 standardin asettamiin vaatimuksiin. Dokumentaatio katselmoitiin sen varmistamiseksi, että kaikki dokumentaatio vastaa nykyistä konfiguraatiota ja toimintaprosesseja. Turvallisuuden hallintajärjestelmän vaatimusten mukaisesti riskien hallinnan menetelmät suunniteltiin siten, että Yritys Oy voi varmistua siitä, että kaikki dokumentaatio päivitetään kolmen kuukauden kuluessa muutoksista ja että se vastaa kaikkia verkkoon tai kontrolleihin tehtyjä muutoksia. Samoin pääsynvalvonnan lokia ylläpidetään vähintään kolme kuukautta sekä raportoitujen tietoturvatapahtumien dataa on säilytetty vähintään kolme vuotta.

Yritys Oy:n tietoverkko on jaettu vyöhykkeisiin ja segmentteihin asianmukaisesti. Eri tietoturvatason järjestelmät on sijoitettu erillisille verkko-alueille. Vyöhykkeiden välistä liikennettä valvotaan ja rajoitetaan palomuurien ja vastaavien liikennettä suodattavien laitteiden avulla. Liikenteen säännöstöt ovat hyvien tietoturvaperiaatteiden mukaisia. Verkkojen ja tietojärjestelmien (ml. palvelimet, työasemat, verkkolaitteet ja vastaavat) hallintaliikenne on eriytettyä ja/tai salattua. Verkon aktiivilaitteet on kovennettu Yritys Oy:n yhtenäisen menettelyta-

van mukaisesti. Langattomien verkkojen käyttö sallitaan vain tunnistetuille ja valtuutetuille käyttäjille. Yritys Oy käyttää tarvittaessa haittapostin torjumiseen itse ylläpitämiään palvelinkohtaisia pääsylistoja (access list). Listan avulla voidaan sulkea tilapäisesti tai pysyvästi erillisiä toimialueita, lähettäjiä, vastaanottajia, yksittäisiä verkko-osoitteita tai kokonaisia aliverkkoja, mikäli se on välttämätöntä muun liikenteen turvaamiseksi tai yksittäisen henkilön häirinnältä suojaamiseksi.

Tietojärjestelmät

Yritys Oy:n tietoverkoissa tunnistaminen ja todentaminen on järjestetty luotettavalla tavalla. Käytössä olevassa menettelytavassa uudet järjestelmät kuten työasemat, kannettavat tietokoneet, palvelimet, verkkolaitteet, verkkotulostimet ja vastaavat asennetaan järjestelmällisesti siten, että lopputuloksena on kovennettu asennus, jolla varmistutaan, ettei Yritys Oy:n verkoissa ole luvattomia laitteita tai järjestelmiä. Tunnistamisessa syntyneiden tallenteiden kattavuus on riittävä tietomurtojen tai niiden yritysten jälkikäteiseen todentamiseen.
Opinnäytetyöhön liittyen riskienhallinnan yhteydessä käsiteltiin tietojärjestelmien sekä turvattavien tietojen luokittelua niiden kriittisyyden kannalta. Tarkastelun tuloksena syntyi seuraava luokittelu:

Taulukko 4: Yritys Oy:ssä noudatettavan tietojärjestelmien ja turvattavien tietojen kriittisyyden luokittelu

Järjestelmän kriittisyysluokka	Kriittinen järjestelmä	Tärkeä järjestelmä	Melko tärkeä järjestelmä	Ei tärkeä järjestelmä
Järjestelmän kuvaus	Liittyy keskeisesti Yritys Oy:n toimintaan, joka ei voi jatkua ilman järjestelmää, erittäin suuri strateginen tai taloudellinen merkitys yrityksen omalle tai asiakkaan liiketoiminnalle	Tukee keskeisiä liiketoimintaprosesseja. Toiminta voi jatkua jonkin aikaa ilman tämän toimivuutta.	Ei tarvita ydinliiketoimintaan, mutta tukee sitä.	Tukijärjestelmä, jota ei tarvita liiketoiminnan ylläpitämiseksi.

Sallittu keskeytysaika	< 5 min	< 5 tuntia	< 5 päivää	< 1 Viikko
Tietojen kriittisyys	Tietojen säilyminen, prosessointi ja saatavuus turvattava aina.	Tietojen säilyminen, prosessointi turvattava, saatavuudessa mahdollinen 5 tunnin viive.	Tietojen säilyminen, prosessointi pyritään turvaamaan, menettäminen ei kriittistä.	Tietojen säilyminen, prosessointi pyritään turvaamaan, menettäminen ei kriittistä.
Korkean käytettävyyden ratkaisut / kahdennus	Pakollisia	Tarpeellisia	Ei pakollisia	Ei järkevää

Yrityksen toiminnassa merkittävä liikkuvuuden mukanaan tuoma uhka on luvaton pääsy laitteisiin tallennettuun tietoon ja niissä oleviin ohjelmiin. Tietojenkäsittely- ja viestintälaitteita käytetään paljon yrityksen eri toimintayksiköiden ulkopuolella. Laitteen katoamisesta voi aiheutua tiedon joutuminen valtuudettomaan käyttöön, koska niistä on suora etäyhteys yrityksen sisäisiin tietojärjestelmiin. Tietojenkäsittely- ja viestintälaitteiden valtuudettoman käytön estämiseksi on niihin asennettava suojausohjelmat, joiden avulla torjutaan katoamistilanteessa laitteen käyttö.

8.6 Tietoaineistoturvallisuus

Yritys Oy:ssä tarkasteltiin tietoaineistoturvallisuutta ja siihen liittyviä turvallisuusuhkia Valtiovarainministeriön Tietoaineistoturvallisuus valtionhallinnossa ohjeen tavoitteiden avulla. Yrityksellä on tavoitteena saavuttaa ohjeen mukaiset ja lainsäädännössä erikseen määritellyt perustietoturvatason vaatimukset tietoturvallisuuden osalta sekä varmistaa menettelyt käsiteltäessä salassa pidettäviä ja käytöltään rajoitettuja tietoaineistoja, jolloin asiakkaiden ja sidosryhmien luottamus yhtiöön ja sen tietojenkäsittelyyn säilyy hyvänä. Opinnäytetyön kehityshankkeessa päädyttiin siihen, että Yritys Oy:ssä tiedot luokitellaan jatkossa niiden merkittävyyden tai lakisääteisten vaatimusten perusteella. Kaikkea salassa pidettäviä tietoa sisältäviä aineistoja ja tietovälineitä säilytetään turvallisesti, salassa pidettävän aineiston kopiointi ja tulostus on järjestetty turvallisesti sekä luottamuksellisia ja salaisia tietoja sisältävät aineistot hävitetään luotettavasti.

Listatessa tiedon luokittelua on muistettava, että yrityksen määritelmä salaiselle tiedolle voi poiketa viranomaisen antamasta tiedon määrityksestä, joka perustuu lakiin ja asetukseen. Keskeiseen liiketoimintaan kuuluvat asiakastiedot, toimitussopimukset, hinnoittelulaskelmat ja sisäisen laskennan tunnusluvut ovat Yritys Oy:n kannalta salassa pidettäviä tai luottamuksellisia tietoja. Yritys Oy on liiketoiminnassa kohdannut kuitenkin tarpeen luokitella tieto suojaustasojen mukaisesti, jolloin esimerkiksi liiketoimintaan oleellisesti liittyvät turvallisuussopimukset ovat laadittavissa yhteismitallisesti julkista tahoa edustavan liikekumppanin kanssa. Sosiaalisen median kannalta on tärkeää muistaa varmistaa tiedon eheys, vaikka se olisikin julkista, koska maineenhallinta vaarantuu yritystietojen vapaasta käytöstä.

Taulukko 5: Tietoluokkien kriittisyyden määrittely

Tiedon turvaluokitus	Julkinen tieto	Sisäinen tieto	Luottamuksellinen tieto	Salainen tieto
Tiedon joutuminen ulkopuolisille	Ei haittaa	Mahdollisesti vähäistä haittaa	Vahingollista	Erittäin vahingollista
Kenellä oikeus / pääsy tietoon	Kaikille	Yritys Oy:n sisällä	Rajattu joukko joiden työhön kuuluu, Asiakasprojektit, henkilötiedot	Erikseen nimetyt
Suojaus	Suojataan siten, että eheys varmistetaan	Pääsy vain Yritys Oy:n sisällä, tarvittaessa sidosryhmillä	Henkilökohtaiset pääsyoikeudet, salataan tarvittaessa	Vahva suojaus, salataan aina, tarvittaessa erityisjärjestelmät
Kuvaukset	Yritys Oy:n www-sivut, Facebook, Twitter, esitteet, tiedotteet, vuosikertomukset, tilinpäätös	Koulutus, ohjeet, menettelytavat, sisäinen puhelinluettelo	Asiakastiedot, henkilötiedot, palkkauksen tiedot, hinnoittelutiedot, tarjoukset	Yrityskaupat, taloudelliset tiedot, turvallisuustiedot

8.7 Toipumis- ja jatkuvuussuunnitelma

Opinnäytetyön yhteydessä kävi Yritys Oy:n kohdalla selville se seikka, että kaikilla käytettävillä keinoilla riskianalyysissä ei voida koskaan löytää tai määrittää kaikkia riskejä, varautua niihin, estää niiden toteutumista tai poistaa riskejä kokonaan. Yritys Oy:ssä varaudutaan siihen, että joskus riskit toteutuvat ja niihin pitää osata silloin reagoida. Vakavassa onnettomuus- tai muussa poikkeustilanteessa turvallisuuteen liittyvät tekijät korostuvat aina selvästi. Tilanteesta, onnettomuuden laajuudesta ja menetyksistä riippumatta Yritys Oy:n omistaman ja hallitseman tiedon eheyden ja luottamuksen tulee säilyä. Kriittisen tiedon käytettävyys on oltava myöskin lyhyitä katkoksia lukuun ottamatta aukotonta. Toipumis- ja jatkuvuussuunnitelman tarkoitus on taata, että jokaisesta liiketoiminnan osa-alueesta löydetään ne alueet, joiden jatkuvuus tulee taata. Hyvällä suunnittelulla voidaan varmistaa, että onnettomuuden, luonnonmullistuksen tai muun katastrofin sattuessa Yritys Oy:ssä osataan toimia suunnitelmallisesti, eikä päätöksiin ajauduta, vaan ne voidaan tehdä proaktiivisesti yrityksen liiketoiminnan etujen kannalta parhaalla tavalla.
On tärkeää huomata, että kyseessä ei ole pelkästään tietotekninen toimenpide, vaan kysymys on koko liiketoiminnasta. Tällöin toipumis- ja jatkuvuussuunnitteluprosessia ei saa jäädä vain yhden yksikön, kuten IT:n hoidettavaksi, vaan Yritys Oy:n jokaisen liiketoimintayksikön osallistumista tarvitaan.

Toipumissuunnitelman tarkoitus on suuren onnettomuuden sattuessa haittojen minimointi ja mahdollisimman nopea toipuminen. Toipumissuunnitelma otetaan käyttöön, kun riski (tunnistettu tai tunnistamaton) toteutuu ja normaali liiketoiminta on vielä sekaisin.

Yritys Oy:ssä opinnäytetyön yhteydessä laaditun suunnitelman mukaisesti tietoturvallisuuden kannalta onnettomuus, poikkeus tai katastrofitilanteita varten määritellään seuraavat tekijät

- RPO = paljonko dataa voidaan menettää (Recovery Point Objective)
- RTO = kuinka kauan palauttaminen saa kestää (Recovery Time Objective)

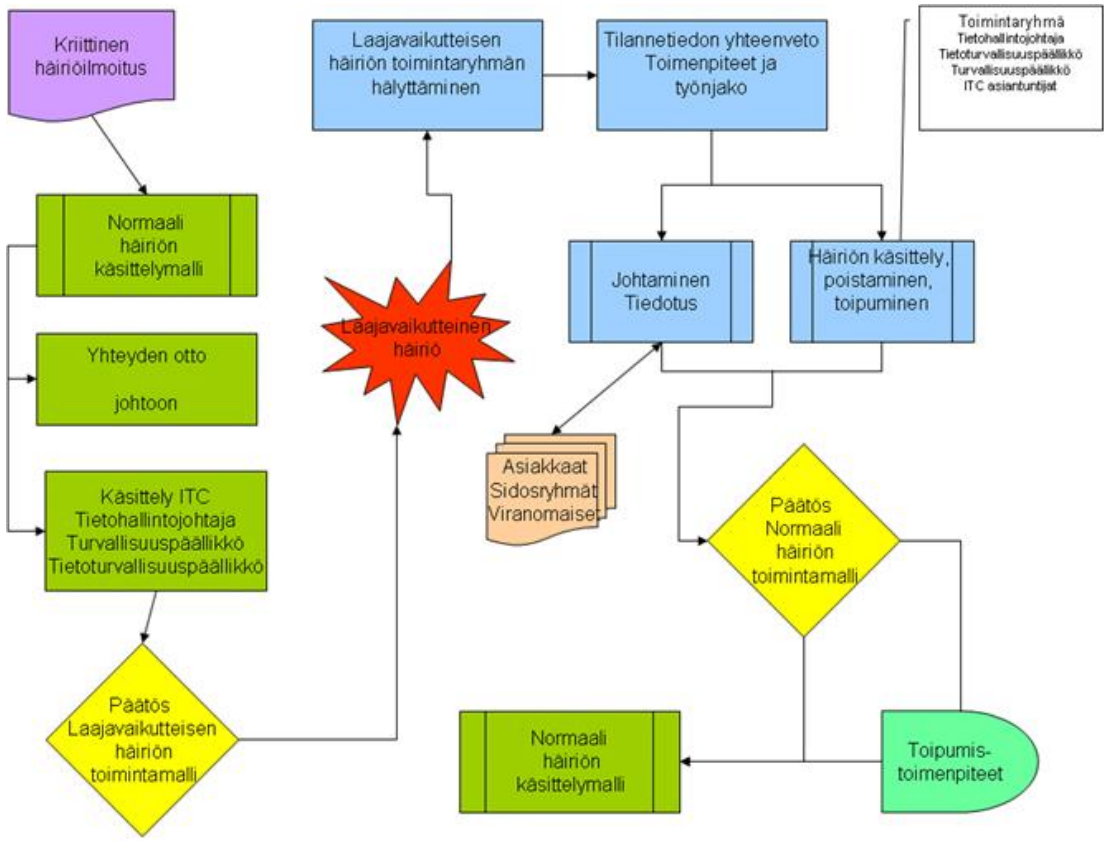
Taulukossa 4 on määritelty Yritys Oy:n n tietojärjestelmien kriittisyys ja sallittu keskeytysaika normaalioloissa. Tämän kriittisyyden pohjalta on määritelty poikkeustilanteiden vaatimukset toipumista varten taulukossa 6. Tietojärjestelmien luokitteluun osallistuivat toimialajohtajat jokaisen Yritys Oy:n liiketoiminta-alan osalta. Tietojärjestelmien luokittelu onnistui osallistujien syvällisesti perehdyttyä toimialaansa kuuluvan tietojärjestelmän sisältämään tietoon ja sen merkitykseen yritykselle ja sen liiketoiminnalle. Taulukossa on merkitty vain luokitus ja sen vaatima datan ja ajan määre.

Taulukko 6: Tietojärjestelmien luokittelu toipumis- ja jatkuvuussuunnitelmaa varten

Luokitus	Tietojärjestelmä	Tieto	RPO	RTO
Kriittinen järjestelmä			< 2 min	< 5 min
Tärkeä järjestelmä			< 4 tuntia	< 1 päivä
Melko tärkeä järjestelmä			<2 päivää	<4 päivää
Ei tärkeä järjestelmä			< viikko	< viikko

Pohdittaessa tietoturvallisuuden jatkuvuussuunnitelman vaatimuksia nousi esille myös kysymys laajavaikutteisen häiriön mahdollisuudesta. Opinnäytetyön toiminnallisen vaiheen aikana syntyi kuviossa 6 oleva laajavaikutteisen häiriötilanteen toimintamalli sekä siihen liittyvä liitteessä 4 oleva toimenpidelista.

Tämän opinnäytetyöprosessin aikana on maailmassa tapahtunut useita äkillisiä muutoksia niin ihmisten kuin luonnon aiheuttamana. Laajavaikutteinen häiriötilanne ja sen edellyttämät jatkuvuussuunnitelmat eivät ole Japanin maanjäristystuhojen valossa kovin epätodennäköinen vaihtoehto. Nämä traagiset tapahtumat ovat herätelleet yrityksiä pohtimaan toimintaansa laajamittaisessa häiriötilanteessa. Yksittäinen laaja onnettomuus tai luonnontuho voi verkottuneessa maailmassa levittää nopeasti vaikutuksensa moneen suuntaan. Yritys Oy on halunnut kuvata toimintatapamallinsa valmiiksi, jolloin perussuunnitelmat ovat olemassa siltä varalta, että yritys joutuu jonain päivä tuhon kohteeksi tai heijastusvaikutusten piiriin. Kuvio kuusi esittää toimintatapamallin, johon Yritys Oy on valmistautunut.



Kuvio 6: Laajavaikutteisen häiriötilanteen toimintamalli (mukailtu Vihonen, L. Large Scale Incident malli. 2007)

Laajavaikutteisen häiriön toimintamalli otetaan Yritys Oy:ssä käyttöön, kun normaali häiriönhallinnan malli on riittämättön. Kriteerejä laajavaikutteisen häiriön toimintamallin käyttöönottoon ovat tilanteet, joissa tietoliikenneverkko ei ole käytettävissä, useita prioriteetiltaan kriittisiä järjestelmiä on alhaalla, ulkoistetuissa käyttöpalveluissa on laajoja toimintahäiriöitä, suurin osa työasemista ei toimi tai yritykseen kohdistuu vakava tietoturvaongelma kuten esimerkiksi virustartunta tai kohdistettu monipistehyökkäys. Kaikki edellä kuvatut tilanteet ovat laajasti asiakkaille, sidosryhmille tai viranomaisille näkyvä tietojärjestelmähäiriö. (Vihonen 2007.)

9 Johtopäätökset ja tulosten arviointi

Tietoturvallisuuden kehittäminen Yritys Oy:ssä oli kokonaisuudessaan muuta kuin yhden turvallisuussuunnitelman laatiminen. Kohdeyrityksessä toimiessani törmäsimme yrityksen turvallisuuspäällikön kanssa johtamisen ongelmiin, riskien hallinnan epäselvyyteen sekä itse tietoturvallisuuteen kaikkine osatekijöineen. Lopulta tärkein eli yrityksen tietoturvallisuuden hallintajärjestelmä alkoi hahmottua ja sai tässä työssä kuvatun muotonsa.

Tietoturvallisuuden kehittyminen

Tietoturvallisuuden hallintajärjestelmä on tässä toiminnallisessa opinnäytetyössä nähty tavoitteellisena tilana, johon pyritään sisällyttämällä tietoturvallisuuden hallinta yrityksen normaaliin toimintaan. Kirjallisuuskatsaus nosti esiin strategisen ja operatiivisen johtamisen merkityksen tietoturvallisuuden tavoitteiden saavuttamisessa. Johdon strategiset ratkaisut ohjaavat tietoturvallisuuden tavoitetasoa ja Yritys Oy:n johdon päätöksenteko luo pohjan riskienhallintaan. Tietoturvallisuusorganisaation operatiivisella johtamisella varmistetaan asetettujen toimenpiteiden toteuttaminen ja tavoitteiden saavuttaminen.

Yritys Oy:n toiminnassa oli monet tietoturvallisuuteen liittyvät asia hoidettu hyvin ja niiden avulla yritys on onnistunut suojaamaan tietopääomaansa. Opinnäytetyön tulokset nostivat kuitenkin tietoturvallisuuden hallintajärjestelmän kokonaisuuden tarkastelun kautta esille puutteita ja kehitettäviä asioita. Lähtökohtana opinnäytetyön tarpeellisuudelle Yritys Oy:n kannalta oli selvittää kolme keskeistä kohtaa tietoturvallisuuden hallintajärjestelmän viitekehyksessä. Ensimmäinen päätavoite oli tietoturvatavoitteiden ja tietoturvapolitiikan määrittäminen. Opinnäytetyön toiminnallisen vaiheen tulosten perusteella on selvää, että Yritys Oy:n suurimmat kehitystarpeet tietoturvallisuuden kannalta ovat nimenomaan yrityksen hallinto- ja johtamisjärjestelmässä. Tietoturvallisuuden strateginen suunnittelu ja dokumentointi olivat tietoturvallisuuden kypsyysmallia vasten tarkasteltuina vasta aloittavalla tasolla. Johdon strategisiin tavoitteisiin pohjautuva tietoturvapolitiikka ja riskienhallintapolitiikka ovat keskeiset turvallisuuden rakentamisen kulmakivet. Niiden pohjalta voi yritys vasta tehdä riskikartoituksen ja tarkastella sitä tunnistetun uhka-arviomallin kanssa. Toiminnallisen vaiheen aikana valitsin tämän prosessin läpikäymisen keskeisimmäksi tavoitteeksi, jonka pohjalle aloin laatia varsinaista turvallisuussuunnitelmaa siihen liittyvine dokumentteineen.

Toinen työlle asetettu tavoite oli tutkia organisaation tietoturvavaatimusten ymmärtämistä ja tunnistaa tietoturvavaatimukset. Opinnäytetyön tulosten pohjalta syntyneen kokonaiskuvan sanoma viestitti samaa kuin yrityksen tehtävän antovaiheessa käytyjen keskustelujen sisältö. Yrityksen mahdollisuudet toimia lakisääteisten vaatimusten mukaisesti, toiminta tietoturvapoikkeamien kohdalla tai kaikkien käyttäjien pääsy- ja käyttöoikeuksien hallinta hyvän tiedonhallintatavan mukaisesti ovat esimerkiksi tilanteita, joissa edellytetään johdonmukaista dokumentoitua tietoturvavaatimusten kuvausta ja ymmärtämistä menettelytapojen perustaksi. Työssä nousi esille tarve saada yrityksen johdon ehdoton tuki sekä johdon hyväksymät tietoturvaperiaatteet ja – käytänteet viestitettyä läpi Yritys Oy:n organisaatiorakenteen, jolloin kaikilla oli tiedossaan keskeiset tietoturvavaatimukset. En ollut käyttäjänä yrityksen sisäisessä intranet-verkossa, mutta jakelu onnistui havaintojeni pohjalta hyvin ja aiheutti välittömästi muutosta toimintatavoissa.

Kolmas opinnäytetyön päätavoite kohdeyrityksen puolesta oli turvamekanismien luominen sekä käyttö tietoturvariskien hallintaan. Työn toiminnallisen vaiheen aikana siirryttiin yrityksessä tietoturvallisuuden hallintajärjestelmän kokonaiskuvassa aloittavasta tasosta määriteltyyn toimintaympäristöön. Ottaessani tietoturvapolitiikan luomisen ensimmäiseksi tavoitteeksi oli syynä selkeästi puutteet tietoturvatyön organisoimisessa ja vastuunjaossa. Nopeasti kasvaneessa yrityksessä on vaarana yritysturvallisuuden hallintaan liittyvän vastuun ja tehtävien jakaantuminen pirstoutumalla useille eri toimijoille: ylimmälle johdolle, sisäisille asiantuntijoille, linjajohdolle, työntekijöille sekä ulkoisille toimijoille. (Lanne 2007, 91 - 92.)
Yritys Oy:ssä ulkoisten toimijoiden kanssa tehtävä laaja yhteistyö aiheutti ongelmia sisäisten toimijoiden kanssa olevassa yhteistyö- ja vuorovaikutustarpeissa. Tämä johtui yhteisen tietoturvapolitiikan puuttumisesta.

Tämän toiminnallisen opinnäytetyön päätulos, Yritys Oy:n tietoturvallisuuden kehittäminen ja hallintajärjestelmän suunnitelma, kuvaa ja jäsentää yrityksen eri toimijoiden kuten ylimmän johdon, linjajohdon, tietoturva-asiantuntijoiden, työntekijöiden sekä ulkoisten toimijoiden välistä vastuuta ja vaatimuksia tietoturvallisuuden hallinnan eri vaiheissa. Työn tuloksen pohjalta voi Yritys Oy:ssä syntyä ja kehittyä johdon ohjaama tietoturvallisuuskulttuuri, jossa jokainen tekijä on tietoinen tekemiensä toimien vaikutuksesta turvallisuuteen. Tärkein tekijä tietoturvallisuudessa on edelleenkin yrityksen työntekijä, hänen arvomaailmansa ja eettinen vastuunsa työtavoistaan. Yritys Oy voi työn pohjalta kehittää tietoturvallisuutensa kypsyystasoa toistettavuuden kannalta, jolloin jokainen riskienarviointikierros tuo uutta tietoa hallintaprosessiin.

Tarvittavaa tietoturvallisuuden tasoa ja sen riittävyyttä on vaikeaa mitata konkreettisesti.
Tämä toiminnallinen opinnäytetyö pystyi antamaan perustason tietoa tietoturvallisuuden hallintajärjestelmän tilasta sekä avaamaan Yritys Oy:ssä keskustelun hallintajärjestelmän kehittämisestä. Selkeä jatkokehityksen tavoite on saada tietoturvallisuuden hallintajärjestelmä vakiinnutettua toistettavuuden avulla hallitulle tasolle, jolloin tietoturvallisuus näkyy kaikessa operatiivisessa liiketoiminnassa. Se voidaan sisällyttää työskentelytapojen prosessikuvauksiin, menettelytapojen sisältöön, koulutussuunnitelmiin sekä jatkuvuussuunnitelmiin. Tietoturvallisuuden kehittämisen kannalta on tärkeää luoda soveltuvat mittarit, seurantametodit ja raportointijärjestelmä. Ulkoiset auditoinnit ja benchmark nostavat yrityksen tietoturvallisuuden tason optimoidulle tasolle.

Työn arviointi

Opinnäytetyön kehityshankkeen kokemuksia pohtiessani keskeisin havainto on ollut se, että sama vaikutus minkä havaitsin kohdeyrityksen johtamiskulttuurin muutoksessa on koskenut myös itseäni. Johtamisella on keskeinen vaikutus toiminnan syntymisessä, mutta sama koskee

myös omaa toimintatapamallia ja työskentelyotetta. Oman itsensä johtaminen ja päämäärien asettelu tuo toivottuja tuloksia. Jokaisessa toiminnassa tarvitaan visio ja strategia, jonka toteuttamiseen tarvitaan johdonmukainen ohjaus ja valvonta.

Työelämälähtöisen opinnäytetyön laatua voidaan arvioida sen pohjalta, tuottiko opinnäytetyö sellaista tietoa, joka on työelämärelevanttia, ajankohtaista ja sillä on yritykselle konkreettinen merkitys. Tämä opinnäytetyö toi Yritys Oy:lle konkreettista ja relevanttia tietoa yrityksen tietoturvallisuuden tilasta ja sen kehittämistarpeista. Myös opinnäytetyön sisällöillä ja tuloksilla on merkitystä ammattialan näkökulmasta, koska tuotettu kehittämistieto on syntynyt monialaisessa yhteistyössä yrityksen sisällä palvellen kuitenkin erityisesti turvallisuusalaa.

Opinnäytetyön toiminnallisen vaiheen aikana käydyissä neuvotteluissa Yritys Oy:n edustajien kanssa sain palautetta työn edistymisestä. Toin heidän toimintakulttuuriin oman turvallisuusorganisaatioissa hankitun työkokemuksen kautta ansaitun asiantuntemuksen lisättynä Laureassa turvallisuusalan koulutusohjelmassa opitulla tiedollisella tiedolla. Näitä molempia, kokemuksen tuomaa hiljaista osaamista sekä tiedollisia taitoja, käytin tutkivan ja kehittävän työskentelytavan periaatteilla saadakseni hyviä turvallisuustapoja noudattavan tuotoksen aikaiseksi Yritys Oy:n käyttöön. Työn mukanaan tuoman vuorovaikutuksen ansiosta niin oma kuin työhön osallistuneiden Yritys Oy:n kumppaneiden kehittyminen on osoitettavissa.
Pelkästään oma itsearviointi ei riitä tuottamaan täyttä kuvaa Yritys Oy:n tietoturvallisuuden kehittämisen laadusta, vaan yritys tarvitsee myös ulkopuolista arviointitietoa.

Työn alkaessa oli edessä suuri ja tuntematon tietoturvallisuuden kenttä. Sen tutkiminen ja selvittäminen edellytti käytössä olleiden käsitteiden ja teorioiden hyödyntämistä ja soveltamista kohdeyrityksen toimintakulttuuriin. Laadittu kehityshanke sisälsi laajoja kokonaisuuksia, joiden jokaisen kohdalla syvyyttä ei voi ottaa liikaa johtuen työn rajallisesta koosta. Puhuttaessa tietoliikenneturvallisuudesta mennään jo osin hyvin teknisiin sovelluksiin ja niiden muodostamaan verkkoon, jolloin tarvittavien turvallisuuskontrollien selvittäminen vaatii laajaa yhteistyötä työyhteisön sisällä.

Opinnäytetyön alussa käytin lainausta, jossa tietoturvallisuus kuvattiin jatkuvaksi ja merkityksselliseksi oppimisprosessiksi, jonka odotetaan mitattavissa olevia etuja käyttäytymisen pysyvän muutoksen kautta. Itselleni opinnäytetyöprosessi on ollut oppimisprosessi, joka on saanut aikaan konkreettista ammatillisen osaamisen kasvua.

Lähteet

BSI 100-1. 2008. Bundesamt für Sicherheit in der Informationstechnik. Tulostettu 28.2.2011. https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

Eskola, J. & Suoranta, J. 2005. Johdatus laadulliseen tutkimukseen. Jyväskylä: Vastapaino.

Fränti, M. & Pirinen, R. 2005. Tutkiva oppiminen integratiivisissa oppimisympäristöissä Bar-Laurea ja REDLabs. Espoo: Laurea.

Hakkarainen, K. Lonka K. & Lipponen, L. 2005. Järki, tunteet ja kulttuuri oppimisen synnyttäjänä. Porvoo: WS Bookwell Oy.

Hirsjärvi, S., Remes, P. & Sajavaara, P. 2008. Tutki ja kirjoita. Helsinki: Tammi.

ISO/IEC 13335-1. 2004. Information technology. Security techniques. Management of information and communications technology security. Helsinki. Suomen Standardisoimisliitto SFS.

ISO/IEC 17799. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintaa koskeva menettelyohje. Helsinki. Suomen Standardisoimisliitto SFS.

ISO/IEC 27001. 2006. Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät. Vaatimukset. Helsinki. Suomen Standardisoimisliitto SFS.

ISO/IEC TR 18044. 2004. Information technology. Security techniques. Information security incident management. Helsinki. Suomen Standardisoimisliitto SFS.

KATAKRI. Kansallinen turvallisuusauditointikriteeristö. 2009. Helsinki. Puolustusministeriö.

Korsman, U. 1999. Tutustuminen tutkimuksen tekemiseen Ohjeita pienimuotoisten tutkimusraporttien laatimista varten. Pori: Porin korkeakouluyksikkö.

Kupi E, Keränen J & Lanne M. Riskienhallinta osana pk-yritysten strategista johtamista. Viitattu 29.3.2011. http:// http://www.vtt.fi/publications/index.jsp)

Lanne, M. 2007. Yhteistyö yritysturvallisuuden hallinnassa. Tutkimus sisäisen yhteistyön tarpeesta ja roolista suurten organisaatioiden turvallisuustoiminnassa. Helsinki: Edita Prima Oy.

Paunonen, M. Vehviläinen-Julkunen, K. 2006. Hoitotieteen tutkimusmetodiikka. Helsinki: WSOY.

SFS-IEC 60300-3-9. 2006. Luotettavuusjohtaminen. Osa 3: Käyttöopas. Luku 9: Teknisten järjestelmien riskianalyysi. Helsinki. Suomen Standardisoimisliitto SFS.

Valtiovarainministeriö. 2003. Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa. VAHTI 7/2003. Helsinki: Edita Prima Oy.

Vihonen, L. 2007. Toipumissuunnitelma laajavaikutteisten häiriöiden varalle. Viitattu 5.4.2011.
http://www.tieke.fi/mp/db/file_library/x/IMG/21340/file/LSI_20070322.pdf

Vilkka, H. & Airaksinen, T. 2003. Toiminnallinen opinnäytetyö. Gummerus Kirjapaino Oy. Jyväskylä.

VTT. Riskianalyysit. Viitattu 29.3.2011. http://www.vtt.fi/proj/riskianalyysit/index.jsp

Åberg, L. 2000. Viestinnän johtaminen. Helsinki: Inforviestintä.

Kuviot

Taulukot

Liitteet

Liite 1

RISKIENHALLINTASUUNNITELMA
Tietoturvallisuus

Yritys Oy

5 = Erittäin vakavat
3= Vakavat
1 = Vähäiset

Henkilöstöturvallisuus	
Fyysinen tietoturvallisuus	
Tietoliikenneturvallisuus	
Käyttöturvallisuus	
Tietoaineistoturvallisuus	
Laiteturvallisuus	

Riski-indeksi= todennäköisyys*(vaikutus)^2

Riski-indeksi	Tunnistetut riskit	Syy riskin olemassaoloon	Todennäköisyys %	Vaikutusindeksi (1-5)			Riskin vaikutus	Riskin minimointi- ja/tai hallintakeinot	Vastaa	Aikataulu
				Liiketoiminta	Kustannukset	Tietopääoma				
0,000			0,0000 %							
0,000			0,0000 %							
0,000			0,0000 %							
0,000			0,0000 %							
0,000			0,0000 %							
0,000			0,0000 %							
0,000			0,0000 %							
0,000			0,0000 %							
0,000			0,0000 %							

Liite 2

Tietoturvan kehittäminen

Toimenpiteiden valinta ja toteutus

Riskianalyysi xx.11.2010 Yksikkö: X

Riskityyppi X	
Tunnistetun riskin vaikutus (kriittisyys) x	
Riskin minimointi ja hallinta (Riski voidaan välttää luopumalla tietystä toiminnasta, välttäminen kahdentamalla, välttää ulkoistamisella, vaikutuksen minimointi, siirtäminen, hyväksyminen) x	
Henkilökustannukset x	**Euroa**
Palvelut, vuokraukset x	**Euroa**
Koneet, laitteet x	**Euroa**
Vakuutukset x	**Euroa**

Liite 3

Henkilöstöturvallisuus / käyttöoikeudet

Nimi	Tehtävä	Yksikkö	Käyttäjäsitoumuksen allekirjoitus pvm	Turvallisuusselvitys kyllä / ei sekä pvm	Tarkistettu turvallisuusselvitys pvm	ID numero	Admin-oikeudet kyllä / ei	Käyttöoikeudet tietojärjestelmiin			
								Kriittinen järjestelmä x	Kriittinen järjestelmä y	Järjestelmä x	Järjestelmä y

Liite 4

Toimenpiteet vakavassa häiriö / poikkeustilanteessa

JOHDANTO

Tämä dokumentti on toteutussuunnitelma Yritys Oy:n toiminnasta vakavassa tietoturvallisuutta uhkaavassa tilanteessa. Uhka voi ilmetä esimerkiksi siten, että tietoliikenneverkko ei ole käytettävissä, järjestelmien prioriteettilistan sovelluksista on useita alhaalla, ulkoistetuissa käyttöpalveluissa laajoja toimintahäiriöitä tai suuri osa työasemista ei toimi. Häiriö voi johtua onnettomuudesta, luonnonmullistuksesta tai rikollisesta toiminnasta (minipistehyökkäys).

Edellä kuvattujen ongelmien ilmetessä toimitaan seuraavan kuvauksen mukaisesti.

HÄLYTYS / ILMOITUS

Vakavasta häiriötilanteesta ilmoitetaan puhelimella seuraaville

Nimi	*Puhelin*

Tiedottaminen

Yritys Oy:n toiminnasta vakavassa tietoturvallisuutta uhkaavassa tilanteessa tiedottaa asiakkaille, sidosryhmille tai viranomaisille yhtiön toimitusjohtaja. Onnettomuuden, tulipalon tai muun kriisitilanteen yhteydessä tietoturvallisuudesta tiedottaminen liittyy yhtiön muuhun kriisitiedottamiseen.

ITC -toiminnan TILANTEEN SELVITTÄMINEN

Laajavaikutteisen häiriötilanteen toimintamallin käyttöönoton jälkeen tietohallintojohtaja sekä tietoturvallisuuspäällikkö kokoavat tilannekuvan sekä varmistavat seuraavat toimintaan liittyvät tekijät

ITC -tilojen fyysiset olosuhteet

Osoite	*Kuvaus*

Varmistaa alihankkijoiden toimintakyvyn; kopiot kaikista huoltoon ja muuhun alihankintaan liittyvistä sopimuksista (ml. ns. service level agreementit)

Alihankkija / puhelin	*Merkitys*

Varmistaa tarvittavien konsulttien / palveluntuottajien toimintamahdollisuudet

Konsultti / puhelin	*Merkitys*

Inventoivat ITC -materiaalin ja tietojärjestelmien toimintakunnon sekä tietovarastojen kunnon

Tietojärjestelmä	*ITC materiaali*	*Toimintakunto %*

Tietovarasto	*Käytettävyys %*

Selvittävät voimassa olevat vakuutukset

Vakuutus / Yhtiö / numero	*Kattavuus*