LAUREA AMMATTIKORKEAKOULU Uuden edellä

Tietoturvallisuuden kehittäminen yrityksen toiminnassa

Mansikkamäki, Pasi

2014 Leppävaara

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Tietoturvallisuuden kehittäminen yrityksen toiminnassa

Pasi Mansikkamäki
Turvallisuusalan koulutusohjelma
Opinnäytetyö
Lokakuu, 2014

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Turvallisuusalan koulutusohjelma

Pasi Mansikkamäki

Tietoturvallisuuden kehittäminen yrityksen toiminnassa

Vuosi 2014 Sivumäärä 38

Tässä opinnäytetyössä käsitellään tietoturvallisuuden kehittämistä yritystoiminnassa. Opinnäytetyön tavoitteena on muodostaa selkeä käsitys tietoturvallisuuden vaikutuksesta yritystoimintaan sekä kuvata kattavasti tietoturvallisuutta ohjaavaa lainsäädäntöä, kansainvälisiä standardeja sekä kansallisia ohjeistuksia. Lisäksi työn tavoitteena on tuottaa selkeä ja toimialasta riippumatta sovellettava prosessikuvaus tietoturvallisuuden kehittämiseen ja siten madaltaa yritysten kynnystä lähteä kehittämään toimintansa turvallisuutta.

Työ on toiminnallinen opinnäytetyö, jonka lähtötilanteessa oletetaan, ettei sitä hyödyntävä taho ole suorittanut mitään toimenpiteitä tietoturvallisuuden kehittämiseksi. Työssä on tutustuttu kattavasti tietoturvallisuutta ohjaavaan kansalliseen lainsäädäntöön sekä luotu teoreettinen viitekehys perehtymällä tietoturvallisuuden, yritysturvallisuuden ja turvallisuusjohtamisen aiheista kirjoitettuihin teoksiin. Tietoturvallisuustoiminnan kehittämisen teoriapohjaa on lisäksi vahvistettu tutustumalla kansainvälisiin standardeihin sekä valtionhallinnon ohjeisiin.

Työn tuotoksena syntyi toimialasta riippumattomasti sovellettavissa oleva yksinkertainen prosessimalli, jota seuraamalla lähes mikä tahansa yritys pystyy kehittämään toiminnassaan käsittelemänsä tiedon suojaamista. Malli perustuu jatkuvaan kehitykseen ja turvallisuuden tason parantamiseen.

Työ sisältää myös kuvauksen tietoturvallisuuden kehittämishankkeesta, joka on toteutettu työharjoitteluna keskisuuressa markkinointialan yrityksessä. Hankkeessa sovellettiin työssä esiteltyä tietoturvallisuuden kehittämisen prosessia, jonka eteneminen on kuvattu alkaen kehittämistarpeen tunnistamisesta ja päättyen hankkeessa syntyneisiin tuotoksiin. Tämän opinnäytetyön tuotoksena syntynyt yksinkertaistettu prosessimalli tietoturvallisuuden kehittämiseen havaittiin hankkeen yhteydessä erittäin käyttökelpoiseksi ja helposti toteutettavaksi. Yritystä ei työssä yksilöidä eikä sen henkilöstöä mainita nimeltä.

Asiasanat: Tietoturvallisuus, riskienhallinta, fyysinen turvallisuus, henkilöstöturvallisuus

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Security Management

Pasi Mansikkamäki

Development of information security in corporations

Year 2014 Pages 38

This thesis addresses the development of information security in corporate context. The objective was to establish a comprehensive understanding about the meaning of information security to business operations and also to create an inclusive description of the legislation, international standards and national guidelines concerning information security. The purpose of this thesis was to produce a simplified process description for the development of information security, which can be universally applied to all companies regardless of their line of business.

As a starting point for the thesis it was assumed that no methods or systems to manage information security have yet been implemented in the company or organization in question. The theoretical frame of reference for the thesis was established by studying multiple publications about information security, corporate security and security management. The theoretical framework was also substantiated with international standards.

The outcome of this thesis is a universally applicable process model, which can be used to improve information security in almost every company or organization. The process model is based on the idea of continuous improvement and development.

Included in the thesis is also a report of a development project in which the process model was used. The project was a part of an internship in a medium sized marketing company. The report illustrates the progress of the project from recognizing the need for improvement to the outcomes of the project. The process model for improving information security produced in this thesis was found very useful and easy to apply. The company in question or its employees are not identified in this thesis.

Keywords: Information security, risk management, physical security, personnel security

Sisällys

1 Johdanto

Tässä opinnäytetyössä esittelen tietoturvallisuuden kehittämisen ja ylläpitämisen prosessina, joka pohjautuu ISO/IEC 27001- ja 27002-standardeissa esitettyihin vaatimuksiin ja toimintamalleihin tuettuna turvallisuusjohtamisesta, riskienhallinnasta ja tietoturvallisuudesta julkaistuihin teoksiin. Painotan prosessissa hallinnollisen ja fyysisen turvallisuuden sekä henkilöstöturvallisuuden kehittämistä, sillä tämän opinnäytetyön tarkoitus on olla enemmän yleisluontoinen opas tietoturvallisuuden hallinnasta ja kehittämisestä kuin tarkka kuvaus teknisistä suojausmenetelmistä. Lisäksi hallinnollisten perusasioiden tulisi olla kunnossa ennen kuin teknisistä suojausmenetelmistä saadaan täysi hyöty (Laaksonen, Nevasalo & Tomula 2006, 15).

1.1 Tausta, tarkoitus ja tavoitteet

Lähtökohtana tälle opinnäytetyölle oli suorittamani työharjoittelujakso, jolla tehtävänäni oli kehittää toimeksiantajayritykseni tietoturvallisuuden hallintaa. Työharjoittelujaksolla yrityksen edustajien kanssa keskustellessani kävi ilmi, että tietoturvallisuuden ylläpitäminen koettiin vaikeaksi ja raskaaksi toiminnaksi, johon ei löytynyt resursseja tai osaamista. Lisäksi tietoturvallisuus ymmärrettiin lähinnä sen teknisen ulottuvuuden kautta hallinnollisten asioiden jäädessä täysin huomiotta. Tästä sain ajatuksen tälle opinnäytetyölle. Opinnäytetyön lähtötilanteessa oletan, että kohteena olevalla yrityksellä tai organisaatiolla ei ole käytössä järjestelmää tai toimintamalleja tietoturvallisuuden hallinnoimiseksi ja ylläpitämiseksi.

Tämän opinnäytetyön tarkoituksena on tuottaa yleisluontoinen, toimialasta riippumatta sovellettavissa oleva prosessikuvaus tietoturvallisuuden kehittämisestä. Lisäksi tarkoituksena on valottaa tietoturvallisuuden suhdetta yrityksen muuhun turvallisuustoimintaan, esimerkiksi fyysiseen turvallisuuteen. Tässä opinnäytetyössä kerron tietoturvallisuuteen liittyvästä lainsäädännöstä sekä turvallisuustoimintaa ohjaavista standardeista. Standardien, esimerkiksi ISO 27001, sisältämien ohjeiden noudattamisesta on hyötyä yrityksen toiminnalle, vaikka yritys ei tavoittelisi niiden mukaista sertifiointia. Tuotoksena olevassa prosessikuvauksessa esittelen eri viitekehyksissä esille nostetut, hyväksi havaitut toimintamallit tietoturvallisuuden kehittämiseksi.

Opinnäytetyön tavoitteena on tuottaa konkreettista hyötyä tietoturvallisuuttaan kehittäville yrityksille selkiyttämällä tietoturvallisuuden monista säädöksistä ja standardeista muodostuvaa monimutkaista kokonaisuutta. Lisäksi tavoitteena on madaltaa pienenpienkin yritysten kynnystä tietoturvallisuuden kehittämiseen ja siten kilpailukykynsä ja toimintansa jatkuvuuden turvaamiseen. Tavoitteenani on myös syventää omaa osaamistani ja tietopohjaani tietoturvallisuuden kehittämisen alalta sekä oppia tulkitsemaan ja soveltamaan standardien ja lainsäädännön vaatimuksia.

1.2 Rajaus

Edellä esitetyn opinnäytetyön tarkoituksen perusteella rajasin työn kattamaan tietoturvallisuuden johtamisen ja riskienhallinnan osa-alueet sekä henkilöstöturvallisuuden ja fyysisen turvallisuuden näkökohdat. En käsittele työssäni tietoturvallisuuden teknisiä osa-alueita, kuten tietojärjestelmiä, tietoverkkoja tai ohjelmistoja. Perusteena rajaukselle on opinnäytetyön tavoitteeksi asetettu riippumattomuus toimialoista. Opinnäytetyöhön sisältyvät aihealueet ovat sovellettavissa kaikilla toimialoilla, kun taas ulkopuolelle rajatut osa-alueet ovat hyödyksi vain tietoteknisiä järjestelmiä käyttävissä yrityksissä.

1.3 Tietoturvallisuuden perusteet

Jokainen yritys ja organisaatio tarvitsee toiminnassaan tietoa suorittaakseen tehtävänsä. Yrityksillä tämä tehtävä on useimmiten tuottaa taloudellista tulosta tarjoamalla palveluita tai tuotteita asiakkailleen. Muilla organisaatioilla, esimerkiksi julkishallinnossa, tehtävä ei välttämättä ole niinkään tuottaa rahallista voittoa kuin palveluita yhteiskunnalle. Tieto on yritykselle omaisuutta siinä missä irtaimisto, toimitilat tai pääomakin, ja siitä syystä sitä tulee suojata asianmukaisesti. Myös lainsäädäntö asettaa vaatimuksia tiedon suojaamiselle.

Tieto voi esiintyä monessa muodossa. Se voi olla painetussa tai kirjoitetussa muodossa, sähköisesti varastoituna, esitettynä kuvallisesti tai videolla tai yksinkertaisesti puhuttuna keskusteluissa ja palavereissa. Tiedon muodosta riippumatta se tulisi aina suojata arvonsa mukaisella tavalla. (ISO/IEC 2005.)

Tietoturvallisuustoiminnalla yritykset ja organisaatiot pyrkivät suojaamaan käsittelemäänsä tietoa ja siten varmistamaan sen luottamuksellisuuden, eheyden ja käytettävyyden. Tietoturvallisuus koostuu monista osakokonaisuuksista; hallinnollinen turvallisuus, fyysinen turvallisuus, henkilö-, tietoaineisto-, ohjelmisto-, laitteisto- ja tietoliikenneturvallisuus. (Hakala, Vainio & Vuorinen 2006, 10.)

Tietoturvallisuus on parhaimmillaan kiinteä osa organisaation kulttuuria ja jokapäiväistä toimintaa. Kun tietoturvallisuustoiminta on sulautettu kiinteäksi osaksi organisaatiokulttuuria, kaikki organisaatiossa toimivat ymmärtävät sen merkityksen ja ylläpitävät sitä jokapäiväisessä työssään. Huolellisesti suunniteltuina ja määrätietoisesti johdettuina teknisinä ja hallinnollisina toimina saavutettava ja jatkuvasti ylläpidetty tietoturvallisuuden taso on yritykselle kilpailuetu, joka realisoituu muun muassa liiketoiminnan jatkuvuuden edellytysten paranemisena. (Laaksonen ym. 2006.)

1.4 Käsitteet ja määritelmät

Seuraavassa esittelen tässä opinnäytetyössä käytettäviä keskeisiä käsitteitä. Käsitteet ja määritelmät perustuvat niin kansainvälisiin standardeihin kuin kansallisiin, Valtiovarainministeriön antamiin VAHTI-ohjeisiinkin. Lisäksi mukana on kirjallisuudessa esiteltyjä käsitteitä.

Tietoturvallisuus käsittää Valtionhallinnon tietoturvasanasto VAHTI 8/2008:n (Valtiovarainministeriö 2008) mukaan "järjestelyt, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus". Lisäksi sanastossa mainitaan tietoturvallisuuden olevan riskienhallintaa ja osa yritysturvallisuutta.

Käytettävyys on tiedon ominaisuus olla saatavilla ja käyttökelpoinen valtuutetun tahon niin vaatiessa (ISO/IEC 2006).

Eheys tarkoittaa suojattavan tiedon oikeellisuutta ja täydellisyyttä (ISO/IEC 2012, 5).

Luottamuksellisuus tarkoittaa sitä, ettei kukaan sivullinen saa tietoa, ts. tieto on vain siihen oikeutetun tahon käytettävissä.

Hallinnollisella tietoturvallisuudella tarkoitetaan tietoturvallisuuteen tähtääviä hallinnollisia keinoja, kuten organisaatiojärjestelyt, tehtävien ja vastuiden määrittely sekä henkilöstön ohjeistus, koulutus ja valvonta. (Valtiovarainministeriö 2008.)

Fyysinen turvallisuus on rakennusten ja niihin sijoitettujen laitteiden ja muun omaisuuden suojaamista fyysisiltä uhkilta, kuten murroilta, sekä ympäristöuhkilta, kuten vesi- ja palovahingoilta. Fyysinen turvallisuus käsittää myös suojautumisen kiinteistöteknisten järjestelmien häiriöiltä, kuten sähkökatkoilta. (Hakala ym. 2006.)

Henkilöstöturvallisuus käsittää ne toimet, joilla varmistetaan tietoja käsittelevien ihmisten toimintakyky sekä rajataan heidän mahdollisuuksiaan käsitellä tietoja (Hakala ym. 2006, 11). Valtionhallinnon VAHTI-ohjeen (Valtiovarainministeriö 2008) mukaan "Tietoturvallisuuden alaterminä henkilöstöturvallisuudella tarkoitetaan henkilöstöön liittyvien salassapito- ja käytettävyysriskien hallintaa tietoja ja tietojärjestelmiä käytettäessä".

Tietoaineistoturvallisuus käsittää " tietoturvallisuuteen tähtäävät toimet asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden ylläpitämiseksi keinoina muun muassa tietoaineistojen luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen" (Valtiovarainministeriö 2008).

2 Tietoturvallisuustoimintaa ohjaava lainsäädäntö ja standardit

Yritysten tietoturvallisuustoimintaa ohjaavaa tai sääntelevää säännöstöä ja ohjeistusta on olemassa sekä kansainvälisellä että kansallisella tasolla. Kansainväliset viitekehykset, esimerkiksi EU-direktiivit, eivät suoraan velvoita tai ohjeista yksittäistä yritystä tai yhteisöä, vaan edellyttävät toimenpiteitä kansallisilta lainsäätäjiltä. Tämän opinnäytetyön viitekehyksen kannalta olennaisimpia direktiivejä ovat Euroopan Yhteisön tietosuojadirektiivi (1995/46/EY) sekä Sähköisen viestinnän tietosuojadirektiivi (2002/58/EY), jotka on suoraan implementoitu Suomen kansalliseen lainsäädäntöön. EU-direktiivien lisäksi merkittävänä kansainvälisen tason ohjeistuksena voidaan pitää OECD:n (The Organisation for Economic Co-operation and Development) antamaa ohjeistusta tietojärjestelmien ja tietoverkkojen tietoturvaperiaatteista, joka päivitetyssä, vuonna 2002 julkaistussa versiossaan esitteli mm. käsitteen tietoturvallisuuskulttuuri. Ohjeistuksessa korostetaan korkean prioriteetin asettamista turvallisuuden suunnittelulle ja johtamiselle sekä turvallisuustarpeiden ymmärtämiselle kaikilla organisaation tahoilla (OECD 2002, 8). OECD:n ohjeistus sisältää lisäksi yhdeksän tietoturvaperiaatetta, joissa tietoturvallisuuden kehittäminen ja ylläpitäminen nähdään prosessina. Prosessimainen tietoturvallisuuden hallinnan malli on otettu vahvasti huomioon ISO 27000-sarjan standardeissa. OECD:n ohjeistus on Suomessa otettu huomioon sekä lainsäädännössä että Valtiovarainministeriön alaisen VAHTI-ryhmän ohjeistuksissa.

Kansallisella tasolla Suomessa ei ole yhtä yksittäistä erillislakia tietoturvallisuudesta, vaan yrityksille asetettuja vaatimuksia ja velvoitteita tietojen käsittelyyn ja suojaamiseen liittyen löytyy useista säädöksistä. Tämä osaltaan vaikeuttaa tietoturvallisuustyön toteuttamista käytännön tasolla. Tietoturvan lainsäädännöllinen kehys alkaa Suomessa perustuslaista (1999/731), joka määrittelee yksityisyyden suojan osaksi jokaiselle kuuluvia perusoikeuksia, joista ei voida poiketa kuin lain perusteella (Laaksonen ym. 2006, 28). Seuraavassa listaus muista olennaisista yritysten tietoturvallisuustoimintaan vaikuttavista laeista ja säädöksistä sekä kuvaukset niiden vaikutuksista yritysten toimintaan:

Henkilötietolaki (1999/523) sisältää määräykset koskien henkilötietojen käsittelyä. Henkilötietolaki on merkittävä, sillä lähes poikkeuksetta kaikki yritykset käsittelevät toiminnassaan henkilötietoja, kuten nimiä ja henkilötunnuksia. Lain tarkoituksena on ”- - toteuttaa yksityiselämän suojaa ja muita yksityisyyden suojaa turvaavia perusoikeuksia henkilötietoja käsiteltäessä sekä edistää hyvän tietojenkäsittelytavan kehittämistä ja noudattamista” (Henkilötietolaki 1999, 1 §). Laki sisältää yritysten kannalta merkittävän huolellisuusvelvoitteen (Henkilötietolaki 1999, 2. luku, 5 §), jossa henkilötietoja käsittelevää (rekisterinpitäjä) velvoitetaan toimimaan siten, ettei rekisteröidyn yksityiselämän suojaa ja muita yksityisyyden suojan turvaavia perusoikeuksia rajoiteta ilman laissa säädettyä perustetta. Käytännössä tämä tarkoit-

taa henkilötietojen riittävää suojaamista käsittelyn ja säilyttämisen yhteydessä. Henkilötietolain 7. luvun 32 §:ssä velvoitetaan henkilötietoja käsittelevä toteuttamaan ” tarpeelliset tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomalta pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta, siirtämiseltä taikka muulta laittomalta käsittelyltä”. Edellä mainittu pykälä toimii tehokkaana perusteena yrityksen tietoturvallisuuden kehittämiselle. Huomionarvoista on, että laki ei suoraan aseta tarkkoja vaatimuksia, vaan suojaustason ja menetelmät päättää lähtökohtaisesti rekisterinpitäjä eli yritys itse. Suojaustason valinnan tulisi riippua käsiteltävien henkilötietojen laadusta; ei ole tarkoituksenmukaista suojata pelkkiä nimiä ja osoitteita samalla tavalla kuin esimerkiksi potilastietoja.

Laki yksityisyyden suojasta työelämässä (2004/759) sisältää mm. henkilötietolakia tarkemmin työntekijää koskevien tietojen käsittelyn vaatimuksia ja edellytyksiä sekä kameravalvonnalle sekä muulle työpaikalla tapahtuvalle tekniselle valvonnalle asetettavia vaatimuksia. Tietoturvan toteuttamisen kannalta erityisen merkittävä on lain 6.luku, jossa säädetään työnantajan oikeudesta hakea esille tai avata työntekijän käyttöön osoitettuun sähköpostiosoitteeseen lähetettyjä tai työntekijän siitä osoitteesta lähettämiä sähköpostiviestejä. Luvussa säädetään edellytykset edellä mainitun oikeuden käyttämiselle sekä työnantajan velvollisuuksista oikeutta käyttäessään.

Sähköisen viestinnän tietosuojalaki (2004/516) on säädetty turvaamaan mm. sähköisen viestinnän luottamuksellisuuden ja yksityisyyden suojan toteutumista sekä edistämään sähköisen viestinnän tietoturvaa (Sähköisen viestinnän tietosuojalaki 2004, 1 §). Soveltamisalastaan johtuen lakia voidaan soveltaa lähes kaikkiin yrityksiin, koska ne lähes poikkeuksetta käsittelevät viestintäverkoissaan työntekijöidensä tunnistamistietoja ja luottamuksellisia viestejä (Laaksonen ym. 2006, 54). Huomionarvoista on, ettei lakia sovelleta yrityksen sisäisiin verkkoihin, kuten Intranet-verkkoihin muutoin kuin pykälissä neljä ja viisi tarkoitettujen tietojen luottamuksellisuuden, salassapidon ja hyväksikäyttökiellon osalta. Laissa määritellään sähköisessä viestiverkossa lähetetyt viestit, tunnistetiedot ja paikkatiedot luottamuksellisiksi sekä asettaa yritykselle velvoitteet huolehtia verkon käyttäjien tunnistamistietojen ja paikkatietojen käsittelyn tietoturvasta (Sähköisen viestinnän tietosuojalaki 2004, 4 § & 19 §). Lain 19 § velvoittaa yritystä tai yhteisöä toteuttamaan uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin suhteutetut suojaustoimet toiminnan turvallisuuden, tietoliikenneturvallisuuden, laitteisto- ja ohjelmistoturvallisuuden sekä tietoaineistoturvallisuuden varmistamiseksi. Tietoturvallisuuden hallinnan kannalta laki on sikäli merkittävä yrityksille, että se antaa yritykselle tarvittaessa oikeuden käsitellä luottamuksellisia tietoja väärinkäytösten tai yrityssalaisuuksien paljastamisen ehkäisemiseksi (Sähköisen viestinnän tietosuojalaki 2004, 13 a §).

1.1.2015 voimaan tuleva **Turvallisuusselvityslaki (2014/726),** jolla kumotaan aikaisempi Laki turvallisuusselvityksistä (2002/177), pyrkii parantamaan ” - - mahdollisuuksia ennakolta ehkäistä toimintaa, joka voi vahingoittaa valtion turvallisuutta, maanpuolustusta, Suomen kansainvälisiä suhteita, yleistä turvallisuutta tai muuta niihin verrattavaa yleistä etua taikka erittäin merkittävää yksityistä taloudellista etua taikka edellä tarkoitettujen etujen suojaamiseksi toteutettavia turvallisuusjärjestelyjä” (Turvallisuusselvityslaki 2014). Laissa määritellään henkilöstä tai yrityksestä ja sen vastuuhenkilöistä tehtävät turvallisuusselvitykset sekä edellytykset ja menettelytavat niiden laatimiselle.

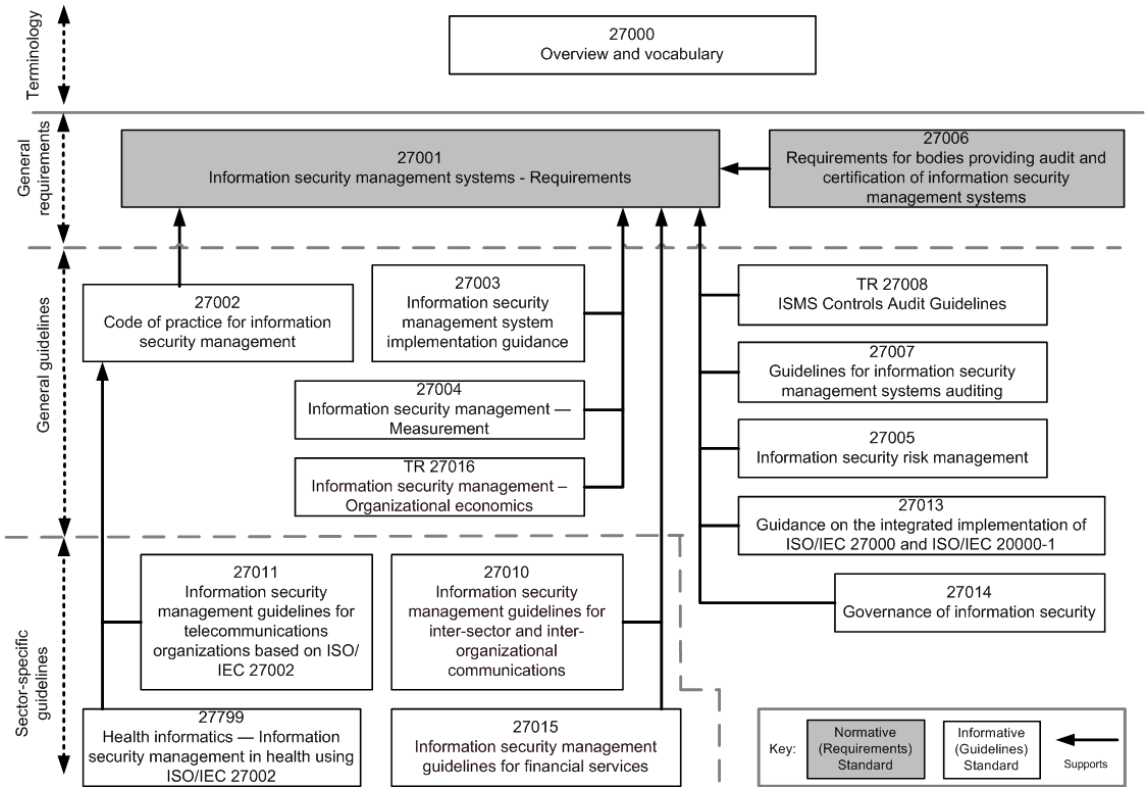
Yritys voi hakea turvallisuusselvitystä palvelukseensa tulevasta henkilöstä tämän nuhteettomuuden tai luotettavuuden varmistamiseksi. Lisäksi turvallisuusselvitys voidaan tehdä yrityksestä ja sen vastuuhenkilöistä niiden luotettavuuden, yrityksen tietoturvallisuuden tason sekä sitoumustenhoitokyvyn arvioimiseksi, mikäli lain edellytykset selvityksen tekemiselle täyttyvät. Turvallisuusselvityksien käyttö on sallittua vain silloin, kun siihen on selvityksen kohteen kirjallinen suostumus ja kun se voidaan perustella erittäin merkittävien taloudellisten etujen tai niiden suojaamiseksi käytettävien turvallisuusjärjestelyjen suojaamisella (Turvallisuusselvityslaki 2014, 1§). Selvitystä haetaan työnantajan toimesta tapauskohtaisesti, ja sen tuloksia saa käyttää vain kyseessä olevaan tarkoitukseen. Selvityksen tulokset on säilytettävä siten, että niitä voivat käsitellä vain niitä tehtävissään välttämättä tarvitsevat, ja hävitettävä, kun ne eivät ole enää tarpeellisia hakemuksessa ilmoitetun käyttötarkoituksen kannalta.

Turvallisuusselvitykset ovat tehokas keino pienentää henkilöstöstä aiheutuvia riskejä jo rekrytointivaiheessa, ja tietyissä yhteyksissä, esimerkiksi turvallisuusluokitelluissa toimeksiannoissa, välttämättömiä.

Laki kansainvälisistä tietoturvallisuusvelvoitteista (2004/588) määrittelee tietoturvallisuusvelvoitteet yrityksille ja niiden henkilöstölle niissä tapauksissa, kun yritys on sopimusosapuolena turvallisuusluokitellussa sopimuksessa tai osallistuu tällaista sopimusta edeltävään hankintakilpailuun tai toimii tällaisen elinkeinonharjoittajan alihankkijana. Nimensä mukaisesti lakia sovelletaan sellaisiin yrityksiin, jotka sopivat tai suorittavat sellaista toimeksiantoa kansainvälisillä markkinoilla, jossa käsitellään erityissuojattavaa tietoaineistoa. Laki velvoittaa suorittamaan sellaiset tietoturvallisuustoimenpiteet, joita erityissuojattavan tietoaineiston suojaamiseksi kansainvälisessä tietoturvallisuusvelvoitteessa vaaditaan. Tällaisia toimenpiteitä ovat esimerkiksi tietoaineiston luokittelu sekä tilojen suojaus kansainvälisen tietoturvallisuusvelvoitteen määritelmien mukaisesti.

2.1 ISO/IEC 27000-sarja

ISO/IEC 27000-sarja on standardiperhe, jonka yhteinen otsikko on "Informaatioteknologia. Turvallisuus. Tietoturvallisuuden hallintajärjestelmät". Standardiperheen tarkoituksena on auttaa kaiken kokoisia ja tyyppisiä organisaatioita kehittämään ja käyttämään tietoturvallisuuden hallintajärjestelmä (ISO/IEC 2012). Standardiperhe koostuu alla kuvassa 1 esitetyistä standardeista. Tässä opinnäytetyössä esitettävän prosessimuotoisen tietoturvallisuuden kehittämisen kannalta olennaisimpia ovat sarjan kolme ensimmäistä osaa; 27000, 27001 sekä 27002.

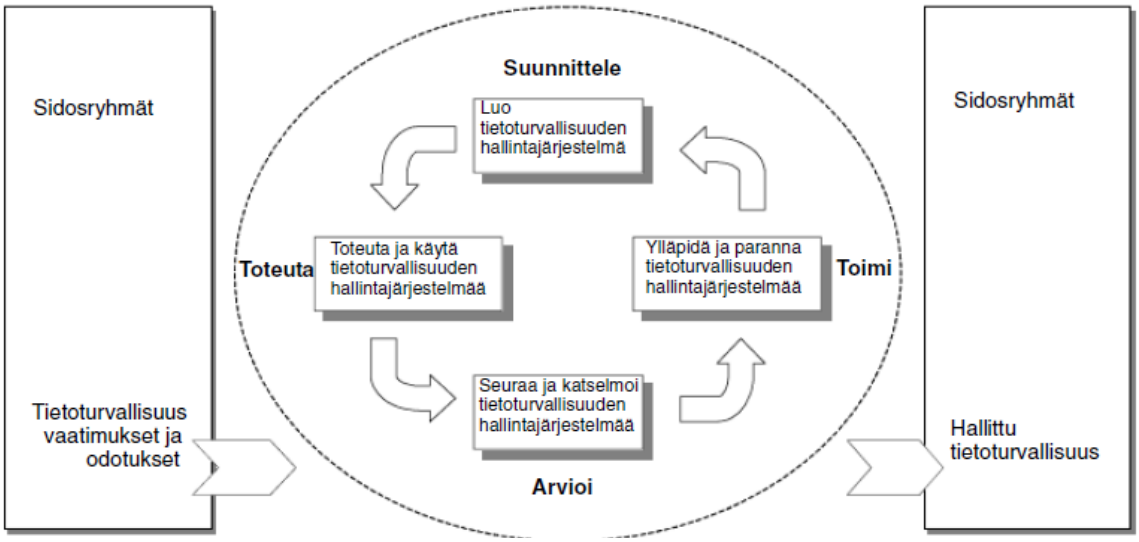


Kuvio 1: ISO/IEC 27000-sarjan standardien suhteet (ISO/IEC 27000 2012, 18)

Sarjan ensimmäinen osa, ISO/IEC 27000, sisältää yleiskatsauksen sarjan standardeihin sekä sanaston. Toinen osa, ISO/IEC 27001, määrittelee vaatimukset ja mallin tietoturvallisuuden hallintajärjestelmälle sekä sen kehittämiselle, toteuttamiselle, käyttämiselle, valvomiselle, katselmoinnille, ylläpitämiselle ja parantamiselle (ISO/IEC 2006, 6). Standardi esittelee prosessimallisen, "Suunnittele-Toteuta-Arvioi-Toimi" -mallin (Plan-Do-Check-Act, PDCA), jonka tavoite on tietoturvallisuuden jatkuva parantaminen. Toimintamallissa painotetaan organisaatioiden tietoturvavaatimusten ymmärtämistä sekä tietoturvapolitiikan ja tietoturvatavoitteiden määrittämistä, turvamekanismien luomista ja käyttöä organisaation tietoturvariskien hallintaan yleisten liiketoimintariskien puitteissa, tietoturvallisuuden hallintajärjestelmän val-

vontaa ja sen suorituskyvyn ja vaikuttavuuden katselmointia sekä objektiiviseen mittaamiseen perustuvaa jatkuvaa parantamista. (ISO/IEC 2006, 6.)

Kuviossa 2 on esitetty PDCA-malli sovellettuna tietoturvallisuuden hallintajärjestelmään suhteessa sidosryhmien asettamiin tietoturvavaatimuksiin.



Kuvio 2: PDCA-mallin soveltaminen tietoturvallisuuden hallintajärjestelmään (ISO/IEC 2006, 8)

Standardiperheen kolmas osa, ISO/IEC 27002, sisältää yleisesti hyväksyttyjä tavoitteita sekä yleisiä periaatteita tietoturvallisuuden hallinnalle, sen suunnittelulle, toteuttamiselle ja ylläpitämiselle. Standardissa tietoturvallisuus alkaa riskien arvioinnista ja hallinnasta, ja sen jälkeen on jaettu 11 pääkohtaan: tietoturvallisuuspolitiikkaa, organisointi, omaisuuden hallinta, henkilöstöturvallisuus, fyysinen sekä ympäristöturvallisuus, käytönhallinta, pääsynvalvonta, tietojärjestelmiin liittyvät asiat kuten hankinta, kehittäminen ja ylläpito, tietoturvatapahtumien hallinta, liiketoiminnan jatkuvuuden hallinta sekä tietoturvallisuustoiminnan yhteensopivuus.

2.2 BSI Standard 100-1 ja 100-2

Bundesamt für Sicherheit in der Informationstechnik (BSI) on Saksan valtiollinen tietoturvallisuudesta vastaava virasto. Sen pääasiallisena tehtävänä on pitää yllä tilannekuvaa tietoturvallisuutta kohtaavista uhkakuvista ja kehittää sekä ennaltaehkäiseviä että reaktiivisia tiedon suojausmenetelmiä. BSI on keskeinen tietoturvallisuuspalveluiden tuottaja Saksan hallitukselle. (Bundesamt für Sicherheit in der Informationstechnik 2013.)

BSI on laatinut yhteensä neljä tietoturvallisuusstandardia, joista kaksi ensimmäistä, 100-1 ja 100-2, ovat keskeisimmät tämän opinnäytetyön aiheen kannalta. Standardeista ensimmäinen

käsittelee tietoturvallisuuden hallintajärjestelmää, ja on täysin yhteensopiva ISO/IEC 27001-standardin (ks. luku 2.1) kanssa. Se on kuitenkin osin yksityiskohtaisempi ja ehkä helppolukuisempi kuin ISO/IEC 27001. BSI-standardisarjan toinen osa, BSI Standard 100-2, esittelee käytännönläheisen, askel askeleelta etenevän toteutustavan tietoturvallisuuden hallinnalle. Myös 100-2 on täysin yhteensopiva ISO/IEC 27000-sarjan standardien kanssa, ollen kuitenkin yksityiskohtaisempi ja esitellen pelkkien vaatimusten sijasta käytännön ohjeita niihin vastaamiseen. (Bundesamt für Sicherheit in der Informationstechnik 2013.)

2.3 Valtiovarainministeriön VAHTI-ohjeet

Valtionhallinnon tietoturvallisuuden johtoryhmä (VAHTI) on Valtiovarainministeriön asettama hallinnon tietoturvallisuuden yhteistyöstä, ohjauksesta ja kehittämisestä vastaava elin. ”VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta, jatkuvuutta, laatua, riskienhallintaa ja varautumista sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi hallinnon toimintaa, johtamista ja tulosohjausta.” (Valtiovarainministeriö 2013.)

Vaikka VAHTI toimii valtionhallinnon tietoturvallisuutta kehittävänä elimenä, ovat sen valtion virastoille antamat ohjeet suurelta osin käyttökelpoisia ja sovellettavissa myös yksityisen sektorin organisaatioihin. Tämän opinnäytetyön tarkoituksen ja tavoitteiden kannalta erityisen hyödyllisinä voidaan pitää Valtionhallinnon tietoturvasanastoa (VAHTI 8/2008), Johdon tietoturvaopasta (VAHTI 2/2011), Toimitilojen tietoturvaohjetta (VAHTI 1/2013), Hankkeen tietoturvaohjetta (VAHTI 9/2008) sekä henkilöstön roolia tietoturvallisuudessa käsittelevää ohjetta Tärkein tekijä on ihminen - Henkilöstöturvallisuus osana tietoturvallisuutta (VAHTI 2/2008). Edellä mainittujen lisäksi Tietoturvallisuudella tuloksia - Yleisohje tietoturvallisuuden johtamiseen ja hallintaan (VAHTI 3/2007), joka sisältää muun muassa tässä opinnäytetyössä usein mainittavan prosessimallisen tietoturvallisuuden hallintatavan, on erittäin hyödyllinen yleisohje tietoturvallisuustoiminnan kehittämiseen. VAHTI-ohjeissa on paljon yhteneväisyyksiä edellä mainittuihin ISO/IEC 27000-sarjan standardeihin, muun muassa yllä mainittu prosessimallinen ajattelu sekä tietoturvallisuuden osa-alueiden jaottelu.

3 Tietoturvallisuuden johtaminen ja osa-alueet

Tietoturvallisuuden, kuten kaiken yrityksen turvallisuustoiminnan, johtaminen yritystoiminnassa on tärkeä osa yritystoiminnan johtamisen kokonaisuutta. Turvallisuusjohtamisen tulisi ulottua kaikille organisaation johtamisen tasoille, alkaen strategisesta ja operatiivisesta johtamisesta jatkuen aina yksittäisen työntekijän johtamiseen. Yrityksen turvallisuuden johtamisen tulisi olla yhtenevä sen strategisten tavoitteiden kanssa, toisin sanoen turvallisuustoiminnan tulee tukea yrityksen olemassaolon tarkoitusta sekä kehitystä. Operatiivisella tasolla hyvällä turvallisuusjohtamisella tuetaan yrityksen prosesseja sekä varmistetaan tuotannon häiriötön toteutuminen ja toiminnan jatkuminen. (Leppänen 2006).

Olennainen osa turvallisuusjohtamista on turvallisuustoiminnan tavoitteiden määrittely ja asettaminen. Huomionarvoista on, että turvallisuustoiminnan tavoitteet eivät voi olla ristiriidassa yrityksen liiketoiminnan tavoitteiden kanssa. Turvallisuustoiminta on kuitenkin tukitoiminto, jolla organisaatio pyrkii varmistamaan tavoitteidensa toteutumisen, eikä niinkään itsetarkoituksellinen organisaation osa, joka on olemassa vain itseään varten. Turvallisuustoiminnan johtamisen kannalta olennaista on, että asetetut tavoitteet ovat mitattavissa ja niiden toteutuminen seurattavissa. Ilman selkeästi asetettuja, mitattavia tavoitteita jatkuvan parantamisen mallin (PDCA-malli) toteuttaminen on käytännössä mahdotonta. Myös tavoitteiden määrittelyyn on hyvä kiinnittää huomiota, esimerkiksi vahinkotapausten määrän vähentäminen on tavoitteena helposti mitattavissa, mutta ei välttämättä auta organisaatiota pidemmällä aikavälillä, sillä vahinkotapausten syihin ei puututa (Leppänen 2006). Tehokkaampi tapa onkin mitata niin sanottujen turvallisuuspoikkeamien määrää, esimerkiksi vaarallisia työtapoja tai, tietoturvallisuuden kontekstissa, lukitsemattomia työasemia. Tällöin turvallisuusjohtamisella voidaan saavuttaa konkreettisia parannuksia organisaation toiminnassa.

Tietoturvallisuuden johtamisen toteuttamista määrittää suurelta osin kyseessä olevan yrityksen toiminnan luonne ja tiedon merkitys tavoitteiden toteutumiselle. Ääripäinä voidaan mainita toisessa päässä yritys, jonka toiminnan kannalta tarkoituksenmukaista on ainoastaan täyttää lainsäädännön asettamat vaatimukset, ja toisena ääripäänä yritys, jolle tiedon suojaaminen ja hallinta on elinehto ja toiminnan jatkuvuuden ja toimialalla menestymisen edellytys. Luonnollisesti edellä mainitut ääripäät vaativat erilaisen tietoturvallisuuden tason ja sen myötä tietoturvallisuuden johtamistavat. Tietoturvallisuustoiminnan toteuttamisen perusedellytys on suojattavan tiedon tunnistaminen ja arvottaminen. Perusajatuksena voidaan ajatella, että mitä suurempi merkitys tiedon suojaamisella on yritykselle ja sen toiminnalle, sitä enemmän resursseja tietoturvallisuustoimintaan on osoitettava. Toimintaympäristö, jossa yritys toimii, vaikuttaa olennaisesti alla käsiteltävien tietoturvallisuuden hallintajärjestelmän sekä tietoturvallisuuspolitiikan sisältöön sekä laajuuteen.

3.1 Tietoturvallisuuden hallintajärjestelmä

Standardisarjassa ISO/IEC 27000 esitellään tietoturvallisuuden hallintajärjestelmä, joka voidaan käsittää työkaluna tietoturvallisuuden johtamiselle. Standardin mukaan tietoturvallisuuden hallintajärjestelmän laatiminen on strateginen päätös, ja järjestelmän sisällön ja laajuuden määrittävät organisaation tavoitteet ja tarpeet, turvallisuusvaatimukset sekä koko ja rakenne (ISO/IEC 2006). Tietoturvallisuuden hallintajärjestelmä koostuu organisaation sisäisistä politiikoista, toimintamalleista, ohjeista sekä niihin liittyvistä resursseista ja toiminnoista, joilla pyritään yrityksen tiedon suojaamiseen. Hallintajärjestelmä sisältää systemaattisen lähestymistavan tietoturvallisuuden tavoitellun tason saavuttamiseksi ja ylläpitämiseksi (ISO/IEC 2012).

Tehokkaan ja toimivan tietoturvallisuuden hallintajärjestelmän perusedellytyksiä ovat tietoturvallisuustoiminnan tarpeen tunnistaminen, vastuiden onnistunut määrittely ja jakaminen sekä johdon sitouttaminen turvallisuustoimintaan. Lisäksi olennaista on yrityksen toiminnan kannalta tärkeiden sidosryhmien, kuten asiakkaiden ja yhteistyökumppanien tarpeiden ja vaikutusten huomiointi. Hallintajärjestelmän luominen tulee aloittaa tunnistamalla suojattavat arvot, eli mitä tietoa yritys toiminnassaan käsittelee, minkälaista arvoa sillä on yritykselle tai miten suuri merkitys sillä on toiminnan jatkuvuudelle, ja mitä sen vuotaminen tai tuhoutuminen aiheuttaisi yritykselle tai sidosryhmille. Edellä mainittujen kriteerien perusteella tiedolle määritellään suojausvaatimukset, joihin hallintajärjestelmällä pyritään vastaamaan. Toinen tärkeä osa hallintajärjestelmän luomista on riskien tunnistaminen ja arviointi. Riskienarvioinnin tulosten perusteella määritellään ja toteutetaan tarpeelliset suojaustoimenpiteet tunnistettujen tietoriskien hallitsemiseksi. (ISO/IEC 2012).

Hallintajärjestelmälle tulee määrittää viitekehys, jossa määritellään sen laajuus ja rajaukset. Viitekehyksessä kuvataan kyseessä olevan organisaation toimiala ja liiketoiminta, organisaatiorakenteet ja toimipaikat, aineellinen ja aineeton omaisuus (suojattavat arvot) sekä käytettävissä olevat tekniikat ja järjestelmät. Mikäli hallintajärjestelmän ulkopuolelle rajataan joitain organisaation osia tai toimintoja, on rajaukset perusteltava.

3.1.1 Tietoturvallisuuspolitiikka

Tietoturvallisuuspolitiikka on yrityksen ylimmän johdon hyväksymä ylätason asiakirja, jossa määritellään strategiset suuntaviivat, tavoitteet ja rajaukset yrityksen tietoturvallisuustoiminnalle. Politiikan merkitys yrityksen tietoturvallisuuden kehittämiselle ja ylläpidolle on suuri, sillä se osoittaa johdon sitoutumisen ja tahtotilan turvallisuuden ylläpitämiseen. On huomionarvoista, että tietoturvallisuuspolitiikassa ei kuvata yksityiskohtaisia tiedon suojausmenetelmiä tai edes suojattavaa tietoa, vaan tietoturvallisuuden merkitys organisaatiolle

yleisellä tasolla sekä turvallisuustoiminnan tavoitteet. Tietoturvallisuuspolitiikkaa laadittaessa on otettava tämä huomioon, sillä politiikka on julkiseksi luokiteltava asiakirja, joka tulee olla jaettavissa tarvittaessa myös yrityksen ulkopuolelle. Hyvin laaditulla tietoturvallisuuspolitiikalla yritys voi osoittaa yhteistyökumppaneilleen sitoutumisensa tiedon suojaamiseen ja vastuulliseen käsittelyyn, ja siten vahvistaa positiivista yrityskuvaansa.

Laaksosen ym. (2006, 147) mukaan tietoturvallisuuspolitiikan tulisi sisältää ainakin tietoturvallisuustoiminnan tavoitteet ja niihin liittyvät toimet, roolit ja vastuut, kuvauksen tietoturvallisuuskoulutuksesta ja tietojenkäsittelyn suojaamisesta, yleiset linjaukset jatkuvuus- ja toipumissuunnittelun toteuttamisesta sekä seuraukset tietoturvallisuuspolitiikan laiminlyönnistä.

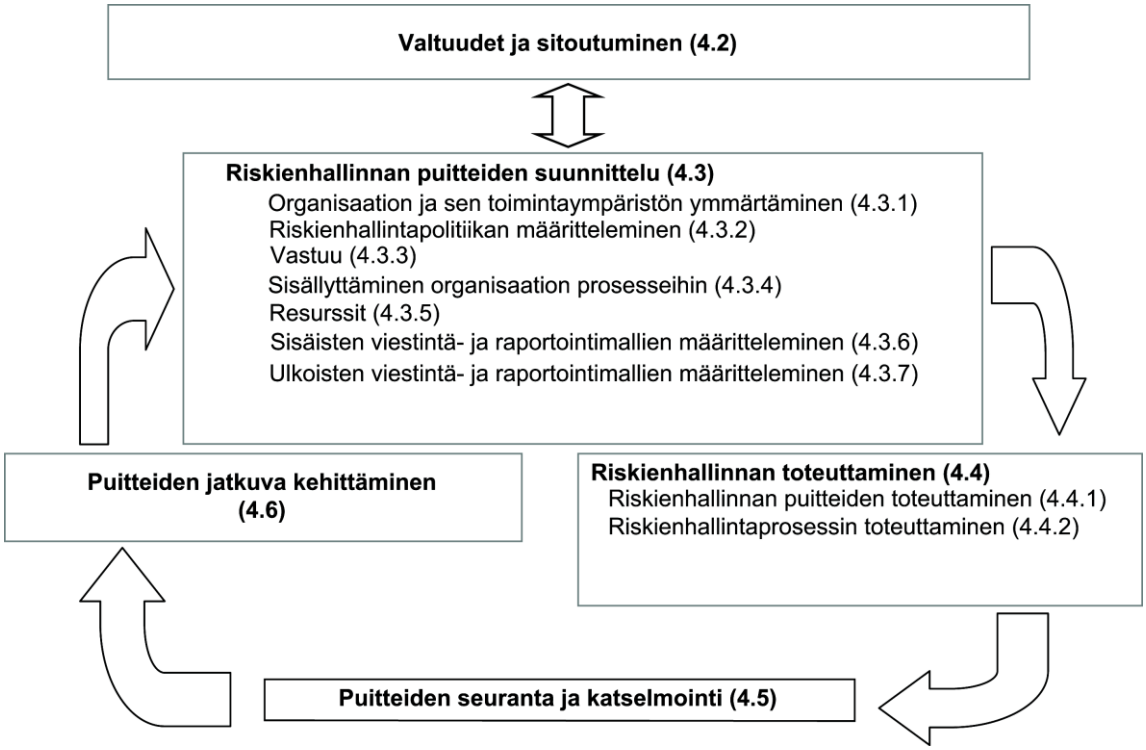
ISO/IEC 27001-standardi asettaa tiettyjä vaatimuksia tietoturvallisuuspolitiikalle osana tietoturvallisuuden hallintajärjestelmää, mutta ei ota tarkemmin kantaa sen sisältöön. Standardi määrittelee politiikalle tavoitteeksi ”Tarjota johdon ohjaus ja tuki tietoturvallisuudelle liiketoimintatavoitteiden ja asiaankuuluvien lakien ja asetusten mukaisesti” (ISO/IEC 2006, liite A, 32). Standardi ISO/IEC 27002 määrittelee sisältöä tarkemmin, mutta ei kuitenkaan tarjoa määrämuotoista mallia politiikan luomiselle.

Standardin mukaan politiikan tulisi sisältää tietoturvallisuuden määritelmät ja tavoitteet, ilmaista johdon sitoutuminen liiketoiminnan strategisia tavoitteita tukevien tietoturvallisuuden tavoitteiden ja periaatteiden tukemiseen, määrittää riskien arvioinnin ja hallinnan toteutuksen sisältävä valvontatavoitteiden sekä valvontamenetelmien viitekehys sekä selvittää organisaatiolle tärkeät muut turvallisuuspolitiikat, periaatteet ja standardit sekä määräystenmukaisuuden. Edellä mainittujen lisäksi tietoturvallisuuspolitiikassa tulisi määrittää tietoturvallisuuden hallinnan yleiset ja tehtäväkohtaiset vastuut sekä selvittää viittaukset muihin politiikkaa täydentäviin asiakirjoihin, esimerkiksi turvallisuusohjeisiin.

Molemmat edellä mainitut standardit painottavat tietoturvallisuuspolitiikan julkaisun ja tiedottamisen tärkeyttä koko organisaatiolle. Tietoturvallisuuspolitiikka tulisi lisäksi katselmoida ja päivittää suunnitelluin aikavälein tai aina kun tapahtuu merkittäviä muutoksia organisaation toimintaympäristössä.

3.2 Tietoriskien tunnistaminen, arviointi ja hallinta

Riskienhallinta koostuu neljästä osasta: Riskien tunnistaminen, riskien analysointi ja arviointi sekä varsinaiset riskien hallintatoimet, joita ovat riskin pitäminen, riskin pienentäminen, riskin siirtäminen ja riskin poistaminen. Riskienhallintaa ohjaava kansainvälinen standardi ISO 31000 suosittelee riskienhallinnan sisällyttämistä yrityksen jokapäiväisiin prosesseihin sen sijaan, että se pidettäisiin erillisenä toimintona. Lisäksi standardissa korostetaan riskienhallinnan jatkuvuutta PDCA-mallin mukaisesti, kuten alla olevasta kuviosta voidaan havaita.



Kuvio 3: Riskienhallinnan jatkuva kehittäminen (SFS-ISO 2009, 26)

Tietoriskien, kuten kaikkien yrityksen toimintaan kohdistuvien riskien, hallinta alkaa toimintaympäristön määrittelystä, jossa rajataan riskienhallinta koskemaan tiettyä organisaation osaa tai tietojärjestelmää, sekä suojattavien arvojen tunnistamisesta, jossa tarkastellaan yrityksen omistamaa ja yrityksessä käsiteltävää tietoa. Tiedot ja tietojärjestelmät tulee luokitella niiden tärkeyden perusteella kriittisyysluokkiin. Karkeasti ilmaistuna tiedon kriittisyydellä tarkoitetaan tiedon tärkeyttä yritykselle sekä sen tuhoutumisesta tai vuotamisesta aiheutuvien vahinkojen suuruutta. Kun tiedot on tunnistettu, tulee yrityksen systemaattisesti kartoittaa ja luetteloida kuhunkin tietomateriaaliin tai -järjestelmään kohdistuvat uhat. Tätä vaihetta kutsutaan riskien tunnistamiseksi. Riskien tunnistamiseen on olemassa useita erilaisia työkaluja, joita esitellään mm. kansainvälisessä standardissa ISO/IEC 31010. Yksi tietoriskien kartoitukseen hyvin soveltuva tekniikka on esimerkiksi standardissa kuvattu Brainstorming, joka

on yksinkertaisimmillaan ryhmäkeskustelu, jossa keskustellaan avoimesti mahdollisista ongelmatilanteista. Keskustelu voi olla muodollinen tai vapaamuotoinen. Muodollisessa keskustelussa osallistujat valmistautuvat etukäteen ja keskustelulle on määritelty selkeät tavoitteet ja säännöt. Kaikki keskustelussa esiin tulevat uhkakuvat ja mahdollisuudet kirjataan ylös todennäköisyydestä riippumatta. Näin saavutetaan mahdollisimman kattava ja monipuolinen käsitys erilaisista uhkakuvista. Keskusteluun osallistujilla tulee olla monipuolisesti tietoa, kokemusta ja näkemystä käsiteltävästä aiheesta, tässä tapauksessa tiedon käsittelystä ja tietojärjestelmistä. Lisäksi keskustelun ohjaajalla täytyy olla riskienhallinnan osaamista. (ISO/IEC 2009.)

Kun riskien tunnistamisvaiheessa on kartoitettu yrityksen tietoon kohdistuvat uhkakuvat, ne voidaan jakaa erilaisiin ryhmiin niiden jatkokäsittelyn ja vastuunjakamisen helpottamiseksi. Erilaisia ryhmiä voivat olla esimerkiksi fyysiset riskit, henkilöriskit, ympäristöstä aiheutuvat riskit sekä teknisiin järjestelmiin liittyvät riskit. Tunnistetut uhkakuvat tulee kartoituksen jälkeen analysoida ja arvioida. Analysoinnilla saadaan selville kaksi asiaa: miten uhkakuva realisoituessaan vaikuttaa yritykseen (seurauksien vakavuus) sekä miten todennäköistä realisoituminen on (tapahtuman todennäköisyys). (ISO/IEC 2009.)

Näiden kahden osatekijän perusteella suoritetaan riskien arviointi, jossa kullekin riskille määritetään numeerinen riskitaso, jota ilmaistaan Riskiluvulla (RL). Todennäköisyyttä (T) ilmaistaan arvolla 1-5, jossa 1 on erittäin epätodennäköinen ja 5 erittäin todennäköinen tapahtuma. Tapahtuman seurausten vakavuutta (S) ilmaistaan samoin arvolla 1-5, jossa 1 on vähäinen ja 5 sietämätön.

Riskianalyysissä painotetaan riskejä seurauksen vakavuuden mukaan, eli mitä vakavampi riskin seuraus, sitä suurempi riskiluku sille muodostuu.
Riskiluku lasketaan kaavalla **$RL = T*S^2$**
Tunnistetut riskit voidaan sijoittaa taulukkoon, kuten alla taulukossa 1. Saadun riskiluvun perusteella riskit asetetaan järjestykseen, josta nähdään minkä riskin käsittely vaatii eniten huomiota.

Riskin kuvaus	**T**	**S**	**RL**
Sisäisen palvelimen ongelmat			
Ulkoiset palvelinongelmat, palvelunestohyökkäykset			
Irtisanomisen yhteydessä tapahtuva tietovarkaus			
Avainhenkilön poistuminen			

Taulukko 1: Riskien arviointi ja riskiluku

Kun riskit on tunnistettu ja arvioitu, tulee niille määritellä hallintatoimenpiteet. Hallintatoimenpiteeksi määritellään riskin suuruuden mukaan joko riskin poistaminen, jossa riskin sisältävästä toiminnasta luovutaan kokonaan, riskin pienentäminen eli todennäköisyyden tai seurausten rajoittaminen, riskin siirtäminen toi toisen osapuolen kannettavaksi esimerkiksi vakuutus- tai alihankintajärjestelyin, tai riskin pitäminen, jolloin riski päätetään hyväksyä osaksi toimintaa, eikä se johda toimenpiteisiin.

Yllä listatuista toimenpiteistä riskin pienentäminen vaatii eniten käytännön toimenpiteitä yrityksen sisällä. Riskien hallintatoimenpiteiden toteuttaminen vaatii aina tarkan suunnitelman, josta ilmenee suoritettava toimenpide, resurssit ja aikataulu sekä toimenpiteistä vastuussa oleva taho. Kaikkia havaittuja riskejä ei tarvitse eikä ole edes taloudellisesti kannattavaa käsitellä. Näitä riskejä kutsutaan hyväksyttäviksi riskeiksi. Yrityksen johdon tulee määritellä kriteerit, joilla riskit luokitellaan hyväksyttäviksi. Kriteerinä voidaan käyttää esimerkiksi riittävän pientä riskilukua.

Tunnistettujen riskien hallintatoimenpiteiden suunnittelussa ja toteutuksessa voidaan käyttää aiemmin esittelemääni 11 kohdan listausta, jossa esitän tietoturvallisuuden osa-alueet. Hallintatoimien jakaminen eri osa-alueisiin helpottaa vastuiden jakamista sekä resursointia. Seuraavissa kappaleissa käsittelen henkilöstöturvallisuuden ja fyysisen turvallisuuden osa-alueille soveltuvia riskienhallinta- ja turvallisuustoimenpiteitä.

3.3 Henkilöstöturvallisuus

Henkilöstöturvallisuus on tietoturvallisuuden osa-alue, jolla tarkoitetaan henkilöstön toiminnasta aiheutuvien tietoturvauhkien hallintaa. Henkilöstöturvallisuustoiminnalla pyritään eliminoimaan niin tahalliset väärinkäytökset kuin tahattomasti aiheutetut vahingotkin. Henkilöstöturvallisuus voidaan jakaa karkeasti työsuhteen elinkaarta noudattaen rekrytointivaiheessa, työsuhteen aikana sekä työsuhteen päättyessä suoritettaviin toimenpiteisiin. (Laaksonen ym. 2006.) Alla mainitut toimenpiteet ja vaiheet ovat sovellettavissa myös alihankintana toteutettavan työn henkilöstöturvallisuuden hallintaan.

3.3.1 Työsuhteen alku

Työsuhteen alkuvaiheessa keskeistä on palkattavan henkilön soveltuvuus tehtävään. Oleellista on myös henkilön luotettavuus ja nuhteettomuus. Työhön otettavan henkilön taustoja tarkastelemalla voidaan luoda käsitys henkilön soveltuvuudesta ja luotettavuudesta, esimerkiksi hakijan työ- ja koulutushistoriaan kannattaa tutustua henkilön pätevyyden varmistamiseksi. Lisäksi työnantaja voi teettää hakijasta Suojelupoliisilla turvallisuusselvityksen, mikäli lain asettamat edellytykset sille täyttyvät. Suppea turvallisuusselvitys antaa työnantajalle käsityk-

sen siitä, voiko hakijalle myöntää oikeuden luottamuksellisen tiedon käsittelyyn. Mikäli työntekijä on välittömässä taloudellisessa vastuussa tai häneltä vaaditaan erityistä luottamusta, voi työnantaja tehdä hakijasta myös luottotietokyselyn. Sekä turvallisuusselvitykseen että luottotietokyselyyn vaaditaan kirjallinen hyväksyntä niiden kohteelta, eli tässä tapauksessa työnhakijalta.

Työsuhteen alkuvaiheessa olennainen asia ovat myös työsopimus ja salassapitosopimukset. Työsopimus tulisi aina tehdä kirjallisena, ja siihen tulee kirjata vähintään työnantajan ja -tekijän tiedot, sopimuksen laatu, kuvaus työtehtävistä sekä palkanmaksun perusteet. Muilta osin voidaan viitata työehtosopimuksiin ja lakiin. Salassapitosopimus voidaan sisällyttää työsopimukseen tai se voidaan tehdä erikseen. Salassapitosopimukseen tulee aina sisällyttää sen rikkomisesta aiheutuvat sanktiot, joiden tulee olla riittävän raskaat sopimuksen tehokkuuden varmistamiseksi. (Laaksonen ym. 2006.) Työntekijän tulee myös olla selvillä vastuistaan, velvollisuuksistaan ja oikeuksistaan.

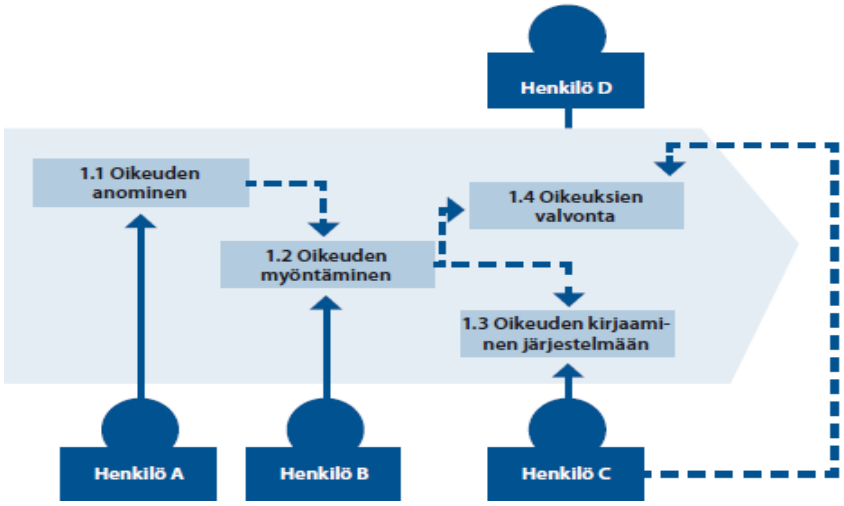
Ennen työntekijän sijoittamista tehtäviinsä, tulee hänet asianmukaisesti perehdyttää tehtäviensä lisäksi myös organisaation tietoturvapolitiikkaan sekä -ohjeisiin. Ohjeisiin ja politiikkaan sitoutumisesta ja niiden noudattamisesta voidaan vaatia kirjallinen suostumus.

3.3.2 Työsuhteen aikana

Työsuhteen aikana keskeistä on työntekijän toimenkuvan ja tehtävien onnistunut määrittely. Olennaista on, että työntekijällä on riittävä perehdytys tehtäviinsä sekä organisaation tietoturvallisuusohjeisiin, käytäntöihin ja politiikkaan. Oikein suunnitellulla ja toteutetulla tietoturvakoulutuksella annetaan työntekijälle riittävät tiedot ja taidot toimia tehtävissään oikein ja turvallisesti.

Työntekijä tarvitsee työnsä suorittamiseksi pääsyn yrityksen tietoihin. Tietoturvallisuuden ylläpitämiseksi on siksi keskeistä määritellä kullekin työntekijälle pääsyoikeudet tietojärjestelmiin ja tietoaineistoihin. Pääsyoikeuksien määrittelyssä tulee noudattaa Valtiovarainministeriön VAHTI-ohjeessa ”Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta” (Valtiovarainministeriö 2008) määriteltyä salassapidon periaatetta; tiedon käsittelijöiden ja tiedon määrän rajaaminen vain työtehtävästä johtuvan tarpeen mukaan ja oikeuksien lokeroiminen nimetylle henkilöryhmälle. Toisin sanoen yrityksen on hallinnollisesti huolehdittava siitä, että vain niillä henkilöillä, jotka tarvitsevat tietoa työssään, on mahdollisuus saada tai muokata sitä. Näin varmistetaan tietoturvallisuuden kolmen päätavoitteen; luottamuksellisuus, eheys ja saatavuus, toteutuminen.

Yksi tärkeimmistä mekanismeista henkilöstöturvallisuuden hallinnassa on vaarallisten työyhdistelmien välttäminen eli tehtävien eriyttäminen. Sillä tarkoitetaan yksinkertaistettuna sitä, että sama henkilö ei voi olla vastuussa useasta tietoturvallisuuden kannalta kriittisestä tehtävästä. Esimerkkinä henkilö, joka tarvitsee pääsyoikeuden tiettyyn tietojärjestelmään. Hän ei voi myöntää sitä itselleen, vaan hän tarvitsee ensin oikeutuksen pääsyyn toiselta henkilöltä ja mahdollisesti vielä kolmannen henkilön luomaan hänelle pääsyoikeudet järjestelmään. Valtionhallinnolle suunnatussa VAHTI-ohjeessa (Valtiovarainministeriö 2008.) sama asia on esitetty seuraavasti:



Kuvio 4: Tehtävien eriyttäminen pääsyoikeuksien hallinnassa (Valtiovarainministeriö 2008.)

Yllä olevassa kuviossa Henkilö A tarvitsee pääsyoikeuden tietoon, jolloin hän anoo sitä henkilöltä B. B:n myönnettyä pääsyoikeuden, Henkilö C järjestää sen esimerkiksi kulunvalvontajärjestelmää käyttämällä. Henkilöt B ja C myös valvovat myönnetyn pääsyoikeuden käyttöä. Henkilö D valvoo prosessia ja tietoaineistoon tehtyjä muutoksia osallistumatta siihen itse. Yllä kuvatulla tehtävien eriyttämisellä ehkäistään virheiden ja väärinkäytösten mahdollisuutta tietojen käsittelyssä.

3.3.3 Työsuhteen päättyessä

Riippumatta työsuhteen päättymisen syistä tai sen päättäjästä, on työsuhteen päättyessä tarpeen varmistua, ettei henkilön poistuminen yrityksen palveluksesta aiheuta haittaa tai uhkaa yrityksen tietoturvallisuudelle. Erityisesti avainhenkilön poistuessa yrityksestä, on keskeistä, että tämän seuraaja perehdytetään asianmukaisesti ja seuraajalla on käytössään hyvin dokumentoitu tietopääoma jota hän työssään tarvitsee. Tällä varmistetaan yrityksen toiminnan häiriötön jatkuminen. Poistuva työntekijä voidaan velvoittaa kouluttamaan itselleen seuraaja ennen poistumistaan. Itse poistuvan henkilön kannalta keskeisiä asioita ovat erilaiset salassapitositoumukset. Poistuvan työntekijän tulee olla tietoinen salassapitositoumuksen kestosta sekä sen rikkomiseen liittyvistä mahdollisista sanktioista. Salassapitositoumuksen lisäksi voi-

daan tietyissä tapauksissa laatia myös kilpailukieltosopimus, jolla rajoitetaan poistuvan työntekijän mahdollisuutta käyttää tehtävässään hankkimaansa tietoa kilpailevan yrityksen hyödyksi. Tämä on erityisen tarpeellista, mikäli poistuva henkilö työskenteli arkaluontoisen tiedon parissa, esimerkiksi tuotekehityksessä.

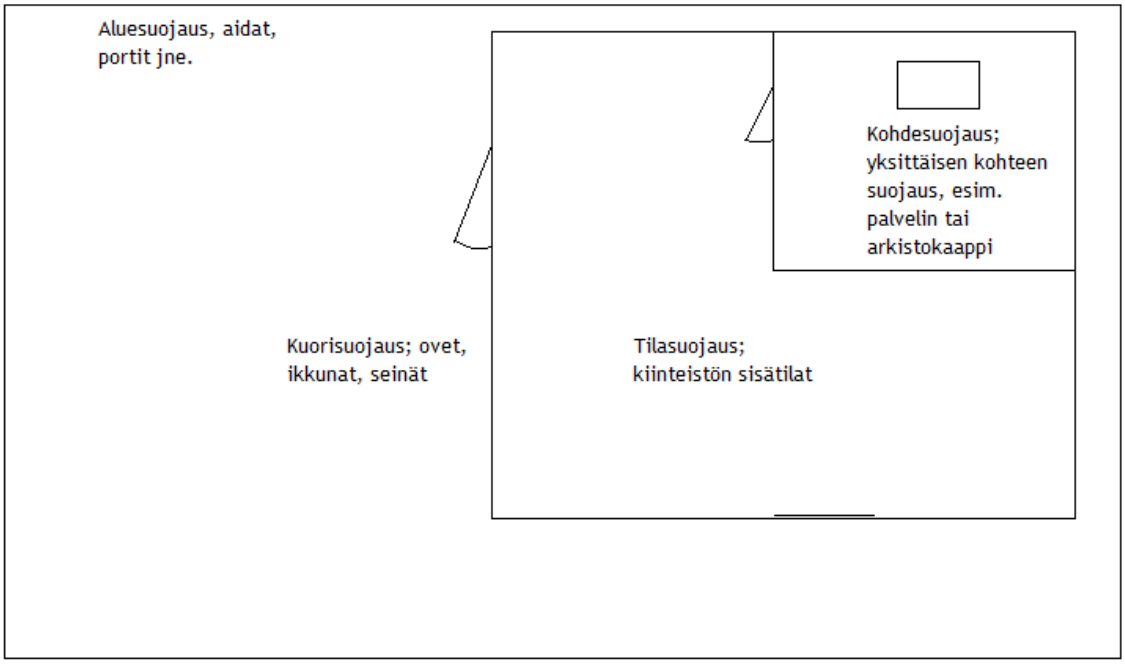
Luonnollisesti olennaista on huolehtia poistuvan henkilön käyttö- ja kulkuoikeuksien hallinnasta jo irtisanomisaikana. Henkilön pääsyä arkaluontoiseen tietoon voidaan jo ennalta rajoittaa, mikäli se on mahdollista henkilön työn suorittamisen kannalta. Kun henkilö poistuu yrityksestä irtisanomisajan päätteeksi, tulee kaikki käyttö- ja kulkuoikeudet poistaa ja kaikki henkilön hallussa oleva materiaali, esimerkiksi kirjalliset dokumentit ja siirrettävät muistilaitteet, hankkia takaisin. Lisäksi luonnollisesti kulku- ja henkilökortit sekä fyysisen lukituksen avaimet tulee saada takaisin. Poistuvan henkilön yrityssähköposti tulee myös sulkea, ja siellä oleva materiaali käsitellä asianmukaisesti. Henkilön poistumisesta tulee myös tiedottaa koko yrityksen henkilöstölle mahdollisten väärinkäytösten ehkäisemiseksi. (Valtiovarainministeriö 2008.)

3.4 Fyysinen turvallisuus

Fyysisellä turvallisuudella tarkoitetaan yrityksen toimitilojen ja kiinteistöjen suojaamista erilaisin teknisin, mekaanisin tai fyysisin järjestelyin sekä onnettomuuksilta että rikoksilta. Perinteisimpiä esimerkkejä fyysisen turvallisuuden ratkaisuista ovat aidat, portit ja mekaaniset lukitukset. Tietoturvallisuuden kannalta fyysisellä turvallisuudella on keskeinen rooli niin rikos- kuin vahinkoriskien torjunnassakin. Hyvin suunnitellulla ja oikein toteutetulla toimitilojen suojauksella voidaan estää tai ainakin vaikeuttaa tiloihin tunkeutumista, rajoittaa vahinkoja tulipalo- tai muussa onnettomuustilanteessa sekä estää yrityksen sisäisiä väärinkäytöksiä.

3.4.1 Kehäsuojausperiaate ja tilojen luokittelu

Yrityksen toimitilojen suojaamisessa perusajatuksena voidaan käyttää niin sanottua kehäsuojausperiaatetta, jossa tiloja lähestytään ulkoa sisäänpäin ja kokonaisuus jaetaan neljään suojaustasoon; aluesuojaus, kuorisuojaus, tilasuojaus ja kohdesuojaus. Aluesuojauksella pyritään estämään tai havaitsemaan asiaton oleskelu yrityksen tontilla tai kiinteistön välittömässä läheisyydessä, kuorisuojauksella estetään yrityksen tiloihin tunkeutuminen, tilasuojauksella havaitaan asiaton liikkuminen tiloissa, ja kohdesuojauksella suojataan yksittäinen kohde varkaudelta tai vaurioitumiselta. (Koskenranta 2006.)



Kuvio 5: Kehäsuojausperiaate (Koskenranta 2006.)

Kullekin mainitulle suojaustasolle on olemassa useita suojaustapoja, jotka tulee suunnitella ja toteuttaa vähintään Finanssialan keskusliiton suojeluohjeiden mukaisesti mitoitettuna kiinteistön luokituksen mukaan. Kiinteistön luokitus määritellään Finanssialan keskusliiton Toimialaluettelon (Finanssialan keskusliitto 2007.) mukaan asteikolla 1-3, jossa 1 on vaatimustasoltaan matalin ja 3 korkein.

Esimerkkejä aluesuojauksessa käytettävistä menetelmistä ovat mm. aidat ja portit sekä niiden lukitus, kameravalvontajärjestelmät sekä sähköinen kulunvalvontajärjestelmä. Kuorisuojauksessa käytettäviä menetelmiä ovat mm. mekaaninen ja sähköinen lukitus, salvat ja puomit, erilaiset kalterit ja ristikot sekä sähköiset turvallisuusjärjestelmät kuten kulunvalvonta-, rikosilmoitin- ja kameravalvontajärjestelmät. Tilojen suojaus kiinteistön sisällä voidaan järjestää esimerkiksi rikosilmoitin-, kulunvalvonta- ja kameravalvontajärjestelmiä käyttämällä. Yksittäisen kohteen suojaukseen tehokkaita keinoja ovat rikosilmoitin- ja kameravalvontajärjestelmien käyttö sekä rakenteelliset suojausmenetelmät kuten paloturvakaapit. Kaikkien edellä mainittujen kehäsuojausperiaatteen suojaustasojen suojaamiseen voidaan käyttää myös hyväksytyltä vartioimisliikkeeltä tilattua vartiointipalvelua, jonka tulee perustua toimeksiantosopimukseen ja olla mitoitettu yrityksen tarpeiden mukaisesti.

Yrityksen tulee luokitella käyttämänsä toimitilat niiden tärkeyden mukaan. Tilojen tärkeys voidaan määritellä perustuen joko niissä säilytettävään omaisuuteen ja sen rahalliseen tai toiminnalliseen arvoon, tai tilojen kriittisyyteen yrityksen toiminnalle. Esimerkiksi yrityksen tiloissa sijaitseva palvelinkeskus luokitellaan tärkeämmäksi kuin henkilökunnan taukotila, ja tuotekehitysosasto luokitellaan tärkeämmäksi kuin myyntiosaston tilat. Tilojen tärkeysluoki-

tuksen avulla voidaan valita ja kohdentaa suojaustoimenpiteet tehokkaasti ja taloudellisesti, sekä määrittää esimerkiksi henkilöstön kulkuoikeudet, joista tarkemmin seuraavassa kappaleessa.

3.4.2 Pääsyoikeudet ja kulunvalvonta

Yrityksen tilojen ja niissä käsiteltävien tai säilytettävien tietojen suojaamisen kannalta olennaista on kyetä valvomaan, kuka tiloissa liikkuu. Yrityksen oman henkilöstön liikkumisen valvontaan voidaan käyttää esimerkiksi sähköistä kulunvalvontajärjestelmää, joka mahdollistaa oikein käytettynä tehokkaan henkilöstön tiloissa liikkumisen ohjauksen ja valvonnan. Lisäksi useimmat kulunvalvontajärjestelmät mahdollistavat lokitietojen tallennuksen, joista voidaan myöhemmin todentaa yksittäisen henkilön liikkuminen tiloissa. Järjestelmä mahdollistaa myös reaaliaikaisen pääsyoikeuksien muokkauksen sekä yksittäisten ovien tai oviryhmien ohjauksen.

Kansallinen Turvallisuusauditointikriteeristö KATAKRI (Puolustusministeriö 2011.) määrittelee vaatimuksia kulunvalvontajärjestelmän käytölle korotetulla (III) ja korkealla (II) tasoilla. Yksinkertaistettuna kriteeristön vaatimuksilla pyritään suojaamaan organisaation tietoja siten, että vain hankkeeseen tai projektiin oikeutetuilla henkilöillä on pääsy tiloihin joissa tietoaineistoa käsitellään, ja että tiloihin kulku on myöhemmin todennettavissa. Korkealla tasolla vaaditaan tämän lisäksi myös kaksoistunnistusta, eli esimerkiksi fyysisen kulkutunnisteen tai biometrisen tunnisteen lisäksi PIN-koodia. Käytännössä tämä on mahdollista toteuttaa erittäin pienellä vaivalla lähes kaikilla markkinoilla olevilla kulunvalvontajärjestelmillä.

Kulunvalvontajärjestelmä on kuitenkin hyödytön, ellei sitä hallinnoida ja käytetä asianmukaisesti. Seuraavassa on listattu kuusi hyvän kulkuoikeuksien hallinnoinnin ominaisuutta, jotka pätevät myös perinteisen, mekaanisin avaimin toteutetun kulkemisen hallinnointiin ja avainhallintaan:

1. Kulkuoikeuksien hallintaan, myöntämiseen ja käsittelyyn on nimetty vastuuhenkilö
2. Käyttäjillä on vain ne oikeudet, joita he tarvitsevat työnsä suorittamiseksi, ja oikeudet ovat voimassa vain tavanomaisina työskentelyaikoina
3. Oikeuksien myöntämisen yhteydessä varmistutaan, että henkilö jolle oikeuksia myönnetään, kuuluu henkilöstöön tai on muutoin oikeutettu (esimerkiksi ulkoistetun huollon työntekijä, siivooja tms.) Kulkuoikeudet myös katselmoidaan säännöllisesti.
4. Oikeuksien käsittely ja myöntäminen on ohjeistettu
5. On olemassa selkeä ja toimiva tapa henkilöstössä tapahtuvien muutosten ilmoittamiseksi asiaankuuluville tahoille sekä toimiva tapa tarvittavien muutosten tekemiseen
6. Jokaisesta myönnetystä kulkuoikeudesta ja luovutetusta kulkutunnisteesta tai avaimesta jää joko fyysinen tai sähköinen dokumentti. Myös palautetut tunnisteet ja poistetut oikeudet tulee dokumentoida.

3.4.3 Onnettomuuksilta suojautuminen

Yrityksen toiminnalle tärkeät tiedot on suojattava myös vahinkoriskeiltä. Tässä yhteydessä vahinkoriskeillä tarkoitetaan niin sanottuja Force Majeure-tilanteita, esimerkiksi tulipaloja, vesivahinkoja tai sähkökatkoksista aiheutuvia tiedon menetyksiä. Kaikkien vahinkoriskien hallinnassa olennaista on riskien tunnistaminen ja arviointi sekä oikeiden hallintatoimenpiteiden käyttöönotto. Lisäksi yrityksellä tulee olla suunnitelma vahingosta toipumiseksi.

3.4.4 Paloturvallisuus

Paloturvallisuudesta huolehtiminen on olennainen osa jokaisen yrityksen toimintaa, ja sillä on merkittävä rooli myös tietoturvallisuuden ylläpidossa. Tulipalo yrityksen tiloissa voi aiheuttaa paitsi henkilövahinkoja ja katkoksen yrityksen toimintaan, myös peruuttamatonta vahinkoa yrityksen hallinnoimalle tietoaineistolle, ellei asianmukaisia turvatoimia ole käytössä. Paloturvallisuuden hallinnan tärkeimpiä työkaluja on Pelastuslain (30.12.2013/1171) sekä Valtioneuvoston asetuksen 5.5.2011/407 vaatimukset täyttävä pelastussuunnitelma, joka sisältää muun muassa riskienarvioinnin sekä kuvauksen yrityksessä toteutetuista omatoimisista varautumistoimenpiteistä.

Paloturvallisuuden ylläpitoon on olemassa lukuisia keinoja, joista tärkeimpinä voidaan pitää tiloja käyttävän henkilöstön kouluttamista ja ohjeistamista. Hyvin koulutettu ja ohjeistettu henkilöstö osaa päivittäisessä toiminnassaan ottaa huomioon paloturvallisuuden sekä toimia tulipalotilanteissa oikein. Henkilöstö tulisi ohjeistaa ja kouluttaa toimimaan tulipalotilanteissa siten, että vahingot jäisivät mahdollisimman vähäisiksi. Esimerkiksi ovien ja ikkunoiden sulkeminen palon leviämisen estämiseksi sekä asiakirjojen suojaaminen paloturvakaappeihin ennen tiloista poistumista tulisi olla itsestäänselvyys. Lisäksi alkusammutusvälineiden käyttö tulisi kouluttaa koko henkilöstölle.

Paloturvallisuutta voidaan parantaa myös teknisillä ratkaisuilla, kuten automaattisilla paloilmoitin- ja sammutinjärjestelmillä. Automaattinen paloilmoitinjärjestelmä tekee tulipalotilanteessa hälytyksen sekä paikallisesti että suoraan aluehälytyskeskukseen. Automaattinen sammutusjärjestelmä havaitsee tulipalossa tapahtuvan lämpötilan nousun ja sammuttaa tiloissa syttyneen palon joko vedellä tai muulla sammutusaineella. Vettä käyttävän sammutusjärjestelmän käyttö ei luonnollisesti tule kysymykseen tiloissa, joissa on kosteudelle herkkiä laitteita tai muuta materiaaleja. Serverihuoneita, laitetiloja tai arkistohuoneita varten voidaan käyttää esimerkiksi kaasusammutuslaitteistoja. Finanssialan keskusliiton suojeluohjeessa H1 (Finanssialan keskusliitto 2002) mainittuja erilaisia kaasusammutuslaitteistoja ovat hiilidioksi-

dilaitteistot ja inerttejä sammutuskaasuja käyttävät laitteistot. Kaasuja käyttävät laitteistot soveltuvat vain tiloihin joissa ei oleskella, koska kaasut ovat ihmisille vaarallisia.

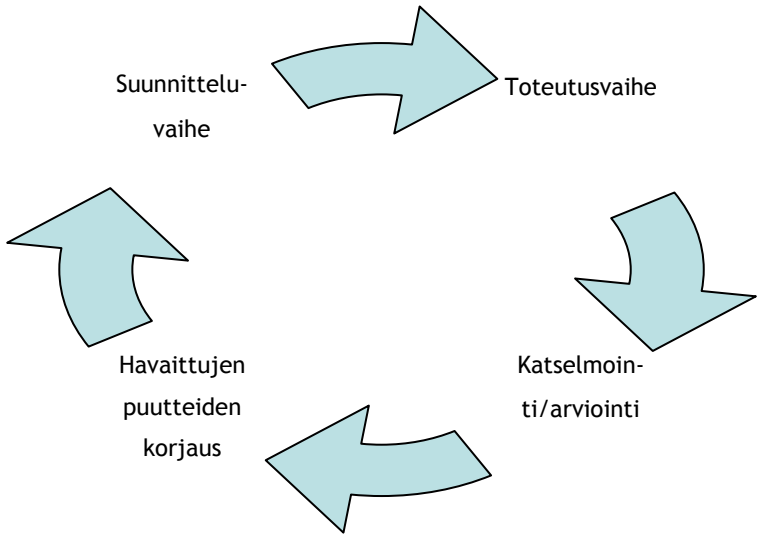
3.4.5 Vesi- ja vuotovahingot sekä sähkönjakelun häiriöt

Erityisesti laitetiloissa, kuten palvelinhuoneissa, tulee varautua vesi- ja vuotovahinkoihin. Varautuminen alkaa jo tilojen sijoittelulla ja suunnittelulla. Putkirikoista tai luonnonilmiöistä johtuvat vesivahingot ovat yleisimpiä rakennusten pohja- ja kellarikerroksissa, joten kosteudelle herkät laitteet tulisi sijoittaa ylempiin kerroksiin mikäli mahdollista. Tiloissa säilytettävät ja käytettävät laitteet tulisi lisäksi sijoittaa irti lattiapinnoista. Mikäli tiloissa on lattiakaivot, tulisi ne varustaa takaiskuventtiileillä tulvimisen ehkäisemiseksi. Laitetiloissa tulisi olla myös kosteusilmaisimet sekä vuotoveden poistolaitteisto, mikäli tila on sijoitettupohjaveden keskipinnan alapuolelle. (Valtiovarainministeriö 2002.)

Sähkönjakelun häiriöt, riippumatta niiden aiheuttajasta, voivat olla tuhoisia tietojenkäsittelylle. Äkillinen sähkökatko saattaa johtaa merkittäviin tiedon menetyksiin, ja esimerkiksi salamaniskusta aiheutuva virtapiikki saattaa vaurioittaa laitteita. Sähkönjakelussa esiintyviin häiriöihin, kuten hetkellisiin katkoksiin tai yli- ja alijännitteisiin, voidaan varautua UPS-laitteilla (Uninterruptible Power Supply). UPS-laitteen kapasiteetti tulee mitoittaa siten, että sillä voidaan pitää ATK-laite käynnissä sen hallittuun alasajoon tarvittava aika. Pidempiaikaisiin sähkökatkoihin voidaan varautua varavoimakoneilla. (Valtiovarainministeriö 2002.)

4 Tietoturvallisuuden kehittämisen prosessi

Tietoturvallisuuden kehittäminen ei ole yksittäinen toimenpide, vaan jatkuvasti ylläpidettävä ja kehitettävä toiminto, jolla pyritään pitämään turvallisuuden taso jatkuvasti riittävän korkealla tasolla. Tästä syystä tietoturvallisuuden kehittämiseen sovelletaan PDCA-mallia, jossa turvallisuustoimenpiteiden suunnittelua ja toteutusta seuraa katselmointi ja toimenpiteiden vaikutusten arviointi. Katselmoinnin perusteella havaitut puutteet tai kehityskohteet käynnistävät prosessin alusta.



Kuvio 6: Tietoturvallisuuden jatkuva kehittäminen

Tietoturvallisuuden kehittäminen alkaa toimintaympäristön määrittelyllä. Tähän sisällytetään kohdeorganisaation oman fyysisen ympäristön lisäksi sen toimintaan liittyvät sidosryhmät, kuten asiakkaat, alihankkijat ja yhteistyökumppanit. Tässä vaiheessa tehdään myös rajaus, jolla määritellään koskeeko kehittäminen koko organisaatiota vai jotain osaa siitä. Toimintaympäristön määrittelyn jälkeen valitaan viitekehys jossa toimitaan. Viitekehyksen valintaan vaikuttaa esimerkiksi organisaation toimiala, toivottu vaatimustenmukaisuus esimerkiksi valtionhallinnon kanssa toimittaessa sekä halutaanko tietoturvallisuustoiminnalle sertifiointi. Mahdollisia viitekehyksiä ovat esimerkiksi ISO 27000-sarjan standardit sekä Kansallinen turvallisuusauditointikriteeristö KATAKRI. Viitekehys asettaa toiminnalle puitteet sekä vaatimukset. Mikäli organisaatio ei pyri saamaan esimerkiksi sertifiointia, vaan ainoastaan kehittämään omaa toimintaansa, voidaan eri viitekehyksiä yhdistellä, kuten tässä opinnäytetyössä on tehty.

Seuraava vaihe prosessissa on suojattavien arvojen tunnistaminen. Suojattavilla arvoilla tarkoitetaan tässä yhteydessä yrityksen toiminnassaan käsittelemää tietoa riippumatta missä muodossa se on. Eri tiedot sijoitetaan alaryhmiin ja tärkeysluokkiin, joiden perusteella tiedoille asetetaan suojausluokitus. Suojausluokitus voidaan määrittää esimerkiksi alla taulukossa 2 esitetyllä tavalla. Taulukossa on esitetty neliportainen tiedon luokitusjärjestelmä, kunkin tasoisen tiedon leviämisen ja tuhoutumisen vaikutukset yritykselle sekä pääsyoikeuksien perusteet. Lisäksi taulukossa on esimerkkejä kuhunkin luokkaan kuuluvasta tiedosta.

Aineiston luokitus:	**I. Julkinen**	**II. Sisäinen**	**III. Luottamuksellinen**	**IV. Salainen**
Leviämisen vaikutukset	Ei vahinkoa, jopa tarkoituksellista	Vähäisiä haittoja tai ei haittaa	Taloudellisia haittoja, asiakkaiden menetyksiä ja/tai oikeudellisia seurauksia	Vakavia taloudellisia vahinkoja, oikeudellisia seurauksia, uhkaa ihmisille
Tuhoutumisen vaikutukset	Lievä haitta julkisuuskuvalle	Lievä haitta toiminnalle	Vakavia toiminnan häiriöitä, osittainen keskeytys	Keskeyttää toiminnan kokonaan
Pääsyoikeus	Kaikilla	Yrityksen henkilöstö, (asiakkaat ja muut sidosryhmät)	Vain työssään tietoa tarvitsevat yrityksen työntekijät	Erittäin rajallinen, vain välttämättömät työntekijät
Esimerkkejä	Internet-sivut, lehdistötiedotteet	Ohjeet, toimintamallit,	Asiakas- ja henkilötiedot (lainsäädäntö), tarjousten yksityiskohdat jne.	Turvallisuusjärjestelyt, tuotekehitystiedot jne.

Taulukko 2: Tietoaineiston luokittelu

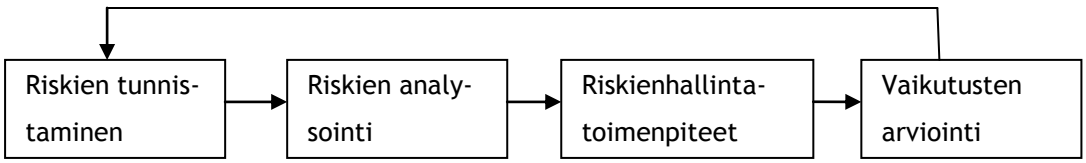
Tietoaineiston luokittelussa on otettava huomioon myös lainsäädännön asettamat vaatimukset ja toisaalta rajoitukset tiedon julkisuudesta. Esimerkiksi pörssiyhtiöillä on velvollisuus julkaista tietoja toiminnastaan, kun taas toisaalta henkilötiedot on pidettävä salassa. Lisäksi tiedon käytettävyysvaatimuksen tulee täyttyä, eli tieto tulee luokitella ja pääsyoikeudet määritellä siten, että työssään tietoa tarvitseva myös pääsee siihen käsiksi.

Prosessin seuraavassa vaiheessa kartoitetaan suojattavia arvoja uhkaavat riskit. Riskien tunnistamiseen soveltuva menetelmä on esimerkiksi Brainstorming, jossa toimialaan ja yrityksen toimintaan perehtyneet henkilöt pyrkivät listaamaan toiminnassa esiintyviä uhkia ja vaaratilanteita (ISO/IEC 2009, 27). Tunnistetut riskit analysoidaan. Riskianalyysissä arvioidaan eri riskien toteutumisen todennäköisyyttä asteikolla 1-5 (1=erittäin epätodennäköinen ja 5=erittäin todennäköinen) sekä vahinkojen vakavuutta asteikolla 1-5 (1=vähäinen ja 5=sietämätön). Riskin todennäköisyyden ja vakavuuden mukaan riskille lasketaan riskiluku (**RL**). Riskiluku muodostuu kertomalla riskin todennäköisyys (T) riskin seurauksen vakavuudella^2 (**S**^{2}). Alla taulukossa 3 on esimerkki riskianalyysin tuloksista.

Riskin kuvaus	**T**	**S**	**RL**
Työntekijä vuotaa kampanjan yksityiskohtia ennen julkaisua	3	4	48
Sisäisen palvelimen ongelmat	2	4	32

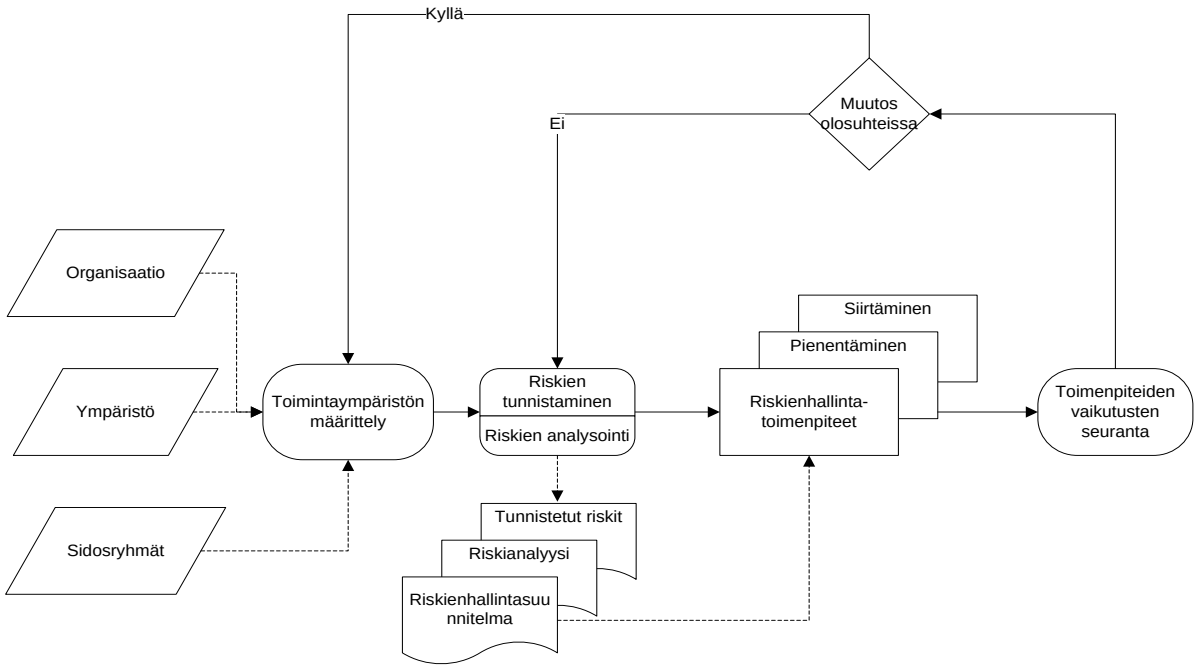
Taulukko 3:Riskianalyysi

Seuraavassa vaiheessa riskeille määritellään hallintatoimenpiteet ja tavoiteaikataulu niiden vakavuus huomioiden. Toimenpiteet, aikataulu ja toteutuksesta vastuussa oleva taho kirjataan riskienhallintasuunnitelmaan, joka noudattaa samaa jatkuvan kehittämisen mallia.



Kuvio 7: Riskienhallinnan jatkuva prosessi

Kuviossa 7 on kuvattu, miten hallintatoimenpiteiden ja tietoturvallisuustoimenpiteiden käyttöönoton jälkeen toimenpiteiden vaikutusta organisaation tietoturvallisuuden tasoa seurataan ennalta määritellyin mittarein. Mikäli joku mittareista osoittaa turvallisuustason heikentyneen, tai organisaation toimintaympäristössä tapahtuu muutoksia, kehitysprosessi käynnistetään uudelleen. Alla kuviossa 8 on havainnollistettu koko kehitysprosessi alkaen toimintaympäristön määrittelystä.



Kuvio 8: Tietoturvallisuuden kehittämisprosessi

5 Esimerkkihanke

Käytän tässä opinnäytetyössä esimerkkihankkeena suorittamaani työharjoittelujaksoa, jossa tehtävänäni oli kartoittaa ja kehittää toimeksiantajayrityksen tietoturvallisuustilannetta. Toimeksiantajani oli media- ja markkinointialalla toimiva, noin 30 henkilöä työllistävä yritys, joka toimii Helsingissä. Lähtötilanteena hankkeelle oli yrityksessä havaittu, yrityksen toiminnassaan käsittelemien tietojen luonteesta johtuva, tarve tietoturvallisuuden kehittämiselle. Yritys käsittelee toiminnassaan muun muassa henkilötietoja sekä asiakkaiden liiketoimintaan liittyviä salassa pidettäviä tietoja. Toimeksiantajani toivoi saavuttavansa hankkeen tuloksena tietoturvallisuuden tason, jolla voidaan varmistua toiminnan laadun ja jatkuvuuden ylläpidosta sekä saavuttaa tiettyjä kilpailuetuja.

Hanke käynnistyi palaverilla yrityksen johdon kanssa. Palaverissa kävimme läpi näkemyksiämme hankkeen tavoitteista ja etenemisestä. Sovimme hankkeen rajaukseksi hallinnollisen tietoturvallisuuden kehittämisen. Esittelin ajatukseni hyödyntää hankkeessa soveltuvin osin ISO 27001-standardin mukaista tietoturvallisuuden hallintajärjestelmää, ja edetä hankkeessa sertifiointiprosessin mukaisesti. Yrityksen edustajat hyväksyivät ajatukseni, ja hanke voitiin aloittaa. Tässä vaiheessa hankkeelle määritettiin myös aikataulutus ja tarvittavat resurssit.

5.1 Toimintaympäristön määritys ja rajaukset

Varsinaisen hankkeen toteutuksen aloitin toimintaympäristön määrittelyllä, jossa rajasin hankkeen kattamaan ainoastaan toisen yrityksen kahdesta yksiköstä. Lisäksi sisällytin hankkeeseen myös ulkopuolisia sidosryhmiä siltä osin, kuin ne olivat elintärkeitä yrityksen toiminnalle. Tällaisia toimijoita löytyi analyysissä ainoastaan yksi, vuokrapalvelin- ja pilvipalveluita yritykselle tarjoava alihankkija. Fyysisen turvallisuuden osalta määrittelin toimintaympäristöksi yrityksen toimitilat Helsingin Ruoholahdessa. Fyysisen turvallisuuden osalta sidosryhmäksi löytyivät kiinteistön ylläpito- ja vartiointipalvelut, joihin yritys ei itse voi vaikuttaa, vaan ne toteutetaan kiinteistön omistajan ja isännöinnin taholta.

5.2 Turvallisuuspolitiikka

Toimintaympäristön määriteltyäni aloin laatimaan yritykselle tietoturvallisuuspolitiikkaa, jossa linjasin tavoitteet tietoturvallisuustoiminnalle yrityksessä, turvallisuustoiminnan toteutuksen yleiset periaatteet sekä toteutuksen vastuut ja organisoinnin. Tietoturvallisuuspolitiikka hyväksyttiin yrityksen toimitusjohtajan toimesta yrityksessä sovellettavaksi ohjeeksi.

Osana tietoturvallisuuspolitiikkaa määrittelin yrityksen käsittelemälle tiedolle neliportaisen luokitusjärjestelmän, jonka perusteella kaikki fyysinen ja sähköinen tietoaineisto ja data tultaisiin luokittelemaan ja suojaamaan.

5.3 Riskienhallinta

Riskienhallintatoimenpiteet käynnistin laatimalla ensin yleisen ohjeen yrityksen johdolle, jota seuraamalla yritys voisi jatkossa itsenäisesti viedä läpi riskianalyysin ja riskien arvioinnin. Tämän jälkeen järjestin yrityksessä riskien tunnistuspalaverin, jossa etsimme potentiaalisia ongelmia yrityksen toiminnassa sekä keskustelimme riippuvuuksista yrityksen ulkopuolisiin toimijoihin.

Palaverissa esille tulleiden asioiden perusteella laadin yritykselle riskienhallintasuunnitelman, jossa määrittelin hallintatoimenpiteet tunnistetuille riskeille (poistaminen, pienentäminen, siirtäminen, pitäminen), riskienhallinnan resurssit ja vastuut sekä toteutusaikataulun tunnistettujen riskien hallintatoimenpiteille. Suunnitelmassa jaottelin riskit henkilö- toimitila- ja sopimusriskeihin vastuiden jaon helpottamiseksi.

5.4 Toimenpiteet

Pisteytin riskienarviointiprosessissa tunnistetut riskit niiden todennäköisyyden ja vahinkojen vakavuuden mukaan. Määrittelin tämän jälkeen kullekin riskille hallintatoimenpiteet. Valitut hallintatoimenpiteet perustuivat pitkälti Saksan tietoturvallisuusviranomaisen BSI:n IT-Grundschutz-luettelossa (Bundesamt für Sicherheit in der Informationstechnik 2005.) esiteltyihin toimiin. Toimenpiteitä olivat esimerkiksi pääsyoikeuksien hallinta, palvelintilojen fyysinen suojaus, reaaliaikainen varmuuskopiointi ja etävalvonta sekä erilaiset keskeytys- ja vastuuvakuutukset sekä sopimustekniset asiat alihankkijoiden osalta.

5.5 Hankkeen lopputulokset

Hanke saatettiin päätökseen edellä mainittujen toimenpiteiden toteutuksella ja vaikutusten seurannalla. Laatimiani ohjeita ja suunnitelmia hyödyntäen yrityksessä pystytään toteuttamaan jatkuvan parantamisen PDCA-mallin mukaista kehittämistä. Välittömiä hyötyjä hankkeesta olivat ennen kaikkea tietoisuuden lisääntyminen, kun yrityksessä oli aiemmin jätetty tietoturvallisuus lähinnä virustorjuntaohjelmien varaan, nyt se osattiin ottaa huomioon kaikessa jokapäiväisessä toiminnassa. Lisäksi yrityksen toimintamalleissa esimerkiksi paperijätteen käsittelyssä tapahtui merkittäviä parannuksia jo hankkeen aikana. Yritys sai käyttöönsä hankkeen aikana laaditun työkalupakin tietoturvallisuuden jatkuvalle kehittämiselle, sisältäen muun muassa riskienhallintaohjeita, asiakirjojen luokittelujärjestelmän sekä tietoturvallisuuspolitiikan.

6 Yhteenveto ja arviointi

Tietoturvallisuus on osa jokaisen yrityksen kokonaisturvallisuutta, ja liittyy kiinteästi lähes kaikkeen yrityksen toimintaan. Tietoturvallisuuden irrottaminen omaksi asiakokonaisuudekseen on käytännössä mahdotonta, koska monet muut yritysturvallisuuden osa-alueet, kuten fyysinen turvallisuus ja henkilöstöturvallisuus, vaikuttavat myös tietoturvallisuuteen. Tietoturvallisuutta voi siis osittain kehittää muita yritysturvallisuuden osa-alueita kehittämällä. Onnistunut ja tehokas tiedon suojaaminen yrityksessä vaatii kuitenkin jatkuvaa katselmointia ja olosuhteiden muutoksiin reagoimista, ja jokaisella yrityksellä ja organisaatiolla on omanlaisensa tarve suojata tietoa ja erilaiset uhkakuvat.

Tässä opinnäytetyössä esitetty prosessimalli pohjautuu suurelta osin kansainvälisiin standardeihin sekä valtionhallinnolle suunnattuihin VAHTI-ohjeisiin, mutta sitä on yksinkertaistettu huomattavasti verrattuna esimerkiksi ISO 27000-sarjassa esitettyihin prosesseihin. Tästä syystä se ei varmastikaan kata kaikkia mahdollisia käsitellyissä viitekehyksissä esitettyjä alueita, mutta on kuitenkin sovellettavissa siten, että sitä seuraamalla saavutetaan parannuksia tietoturvallisuuteen ja sen hallintaan organisaatioissa, joissa siihen ei ole ennestään panostettu. Tämä huomattiin luvussa 5. kuvatun esimerkkihankkeessa, joka noudatti tässä työssä esiteltyä prosessimallia. Prosessi havaittiin myös helposti läpikäytäväksi, sillä hankkeen kohdeorganisaatio pystyi jatkamaan sitä ilman lisäresursseja. Tätä taustaa vasten pidän opinnäytetyöni tuotosta onnistuneena ja alkuperäistä tavoitetta vastaavana.

Itse työprosessi ei sujunut täysin tavoitteitani vastaavasti, erityisesti aikataulu pitkittyi huomattavasti. Lisäksi työn teoriapohjaa olisi ollut syytä laajentaa sekä sisällyttää siihen tutkimuksellisia elementtejä nykyisen kirjallisuuskatsauksen tueksi. Tästä huolimatta oppimistavoitteeni täyttyivät tyydyttävästi, koen pystyneeni hankkimaan merkittävästi tietoa työni aiheesta ja oppineeni myös soveltamaan sitä tehokkaasti.

Lähteet

Bundesamt für Sicherheit in der Informationstechnik. 2005. IT-Grundschutz Catalogues. Bonn: BSI.

Finanssialan Keskusliitto. 2002. Suojeluohje H1: Sammutuslaitteistot - Yleinen ohje.

Finanssialan Keskusliitto. 2007. Toimialaluettelo.

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

Henkilötietolaki 22.4.1999/523.

ISO/IEC 27000. 2012. Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva: ISO/IEC.

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

ISO/IEC 27002. 2005. Information technology - Security techniques - Code of practice for information security management. Geneva: ISO/IEC.

ISO/IEC 31010. 2009. Risk Management - Risk assessment techniques. Geneva: ISO/IEC.

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

Laki kansainvälisistä tietoturvallisuusvelvoitteista 24.6.2004/588.

Laki yksityisyyden suojasta työelämässä 13.8.2004/759.

Laki turvallisuusselvityksistä 8.3.2002/177.

Leppänen, J. 2006. Yritysturvallisuus käytännössä. Helsinki: Talentum Media.

OECD. 2002. Guidelines for the Security of Information Systems and Networks - TOWARDS A CULTURE OF SECURITY. Paris: OECD Publications.

Pelastuslaki 30.12.2013/117.

Puolustusministeriö. 2011. Kansallinen Turvallisuusauditointikriteeristö KATAKRI, versio II. Helsinki: Puolustusministeriö.

SFS-ISO 31000. 2009. Riskienhallinta. Periaatteet ja ohjeet. Helsinki: Suomen Standardisoimisliitto SFS.

Suomen Perustuslaki 11.6.1999/731.

Sähköisen viestinnän tietosuojalaki 16.6.2004/516.

Turvallisuusselvityslaki 19.9.2014/726.

Valtioneuvoston asetus pelastustoimesta 5.5.2011/407.

Valtiovarainministeriö. 2008. VAHTI 8/2008 - Valtionhallinnon tietoturvasanasto. Helsinki: Edita Prima.

Valtiovarainministeriö. 2008. VAHTI 2/2008 - Tärkein tekijä on ihminen - henkilöstöturvallisuus osana tietoturvallisuutta. Helsinki: Edita Prima.

Sähköiset lähteet

Bundesamt für Sicherheit in der Informationstechnik 2013. BSI: BSI-Standards. Viitattu 2.7.2013. https://www.bsi.bund.de/EN/Publications/BSIStandards/standards.html

Bundesamt für Sicherheit in der Informationstechnik 2013. BSI: History. Viitattu 2.7.2013. https://www.bsi.bund.de/EN/TheBSI/History/history_node.html

Bundesamt für Sicherheit in der Informationstechnik 2013. BSI: Functions. Viitattu 2.7.2013. https://www.bsi.bund.de/EN/TheBSI/Functions/functions_node.html

Koskenranta, H. 2006. Henkilöstö- ja toimitilaturvallisuus. Viitattu 28.10.2014. https://www.tml.tkk.fi/Opinnot/T-110.5610/2006/kuorisuojaus-6.pdf

Valtiovarainministeriö. 2002. VAHTI 1/2002 - Tietoteknisten laitetilojen turvallisuussuositus. Viitattu 18.8.2014. https://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20020101Tietot/turvallisuussuositus.pdf

Valtiovarainministeriö. 2013. Valtiovarainministeriö: Tietoturvallisuus. Viitattu 9.7.2013. http://www.vm.fi/vm/fi/16_ict_toiminta/009_Tietoturvallisuus/index.jsp

Kuviot

Taulukot