TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄN LUOMINEN PK-YRITYKSISSÄ

11. Turvallisuusjohdon koulutusohjelma Aalto-yliopiston teknillinen korkeakoulu
Koulutuskeskus Dipoli
Tutkielma 27.3.2011
Mika Pekkala

Sisällysluettelo

1. JOHDANTO

1.1. Taustaa

Elämme tietoyhteiskunnassa, jossa tietoa käytetään monin erin tavoin. Aloittavan, pienen tai keskisuuren yrityksen toiminta vaatii tietoa, joka on yrityksen voimavara, joka tulee suojata aivan kuten kiinteä omaisuus. Häiriöt tietoturvallisuudessa voivat olla haitallisia maineelle, niillä voi välittömiä tai välillisiä taloudellisia vaikutuksia, voivatpa ne jopa aiheuttaa uhkia henkilöstön turvallisuudelle. Tärkeä on ymmärtää mitä tietoa tulee suojata, tavat miten suojataan, rakennetaan tilanteen mukaan. Jokaisen yrityksen tulee rakentaa oma tietoturvallisuutensa itse, yhtä valmista ja oikeaa ratkaisua ei ole. Tietoturvallisuus on osa koko yrityksen riskienhallintaa ja tekninen tietoturva on osa tietoturvallisuuden kokonaisuutta.

1.2. PK -yritykset Suomessa

PK -yritykset muodostavat Suomen talouselämän perustan huolimatta muutaman suuryrityksen korostuneesta näkyvyydestä tiedotusvälineissä. Vuonna 2009 alle 50 työntekijän yrityksiä oli 99,1 % ja alle 250 työntekijän yrityksiä 99,8 % kaikista Tilastokeskuksen yritysrekisterin yrityksistä.

PK -yritysten palveluksessa oli vastaavia rajoja käyttäen 48 % tai 64 % kaikkien yritysten henkilöstöstä (2009). Liikevaihtoa kertyi alle 50 työntekijän yrityksissä 35 % ja alle 250 työntekijän yrityksissä 51 % kaikkien yritysten liikevaihdosta. Palkoista alle 250 työntekijän yrityksissä maksetaan yli puolet, 57 % (2009).

PK -yritysten osuus on merkittävä myös Suomen vientikaupassa. Alle 250 työntekijän yrityksistä 20 prosentilla on vientitoimintaa. Viennin

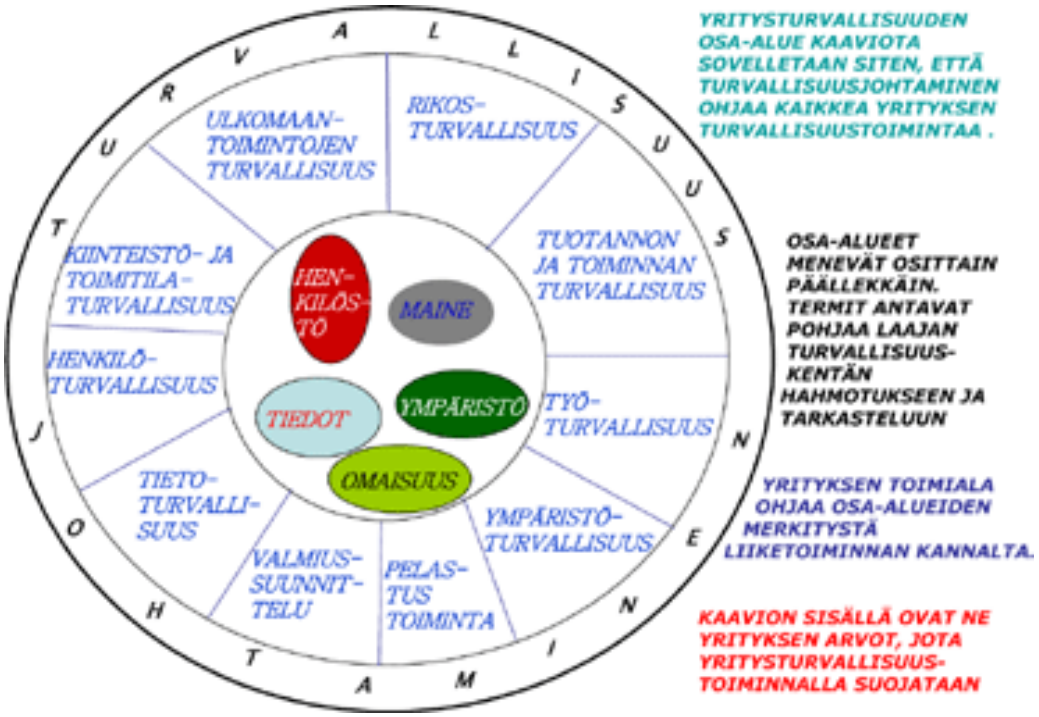
harjoittaminen on keskimäärin sitä yleisempää, mitä suuremmasta yrityksestä on kyse. Näillä yrityksillä viennin osuus liikevaihdosta on keskimäärin kolmasosa. (Elinkeinoelämän keskusliitto: 2011)

1.3. Tavoite

Pyrkimyksenä on kiteyttää ne osa-alueet, jotka pk-yrityksen tulee huomioida omassa toiminnassaan, jotta yritykseen syntyy prosessi, joka kehittää tietoturvallisuutta yrityksessä valmistaen sitä kohtaamaan tulevaisuuden haasteet. Pk-yrityksessä vähäiset resurssit on yleensä keskitetty puhtaasti liiketoimintaan, jolloin riskienhallinta jää vähäiseksi. Tietoturvallisuus mielletään myös usein vain tekniseksi tietoturvaksi, jota hoitaa IT-osasto tai –henkilö.

2. YRITYSTURVALLISUUS JA TIETOTURVALLISUUS

2.1. Yritysturvallisuus



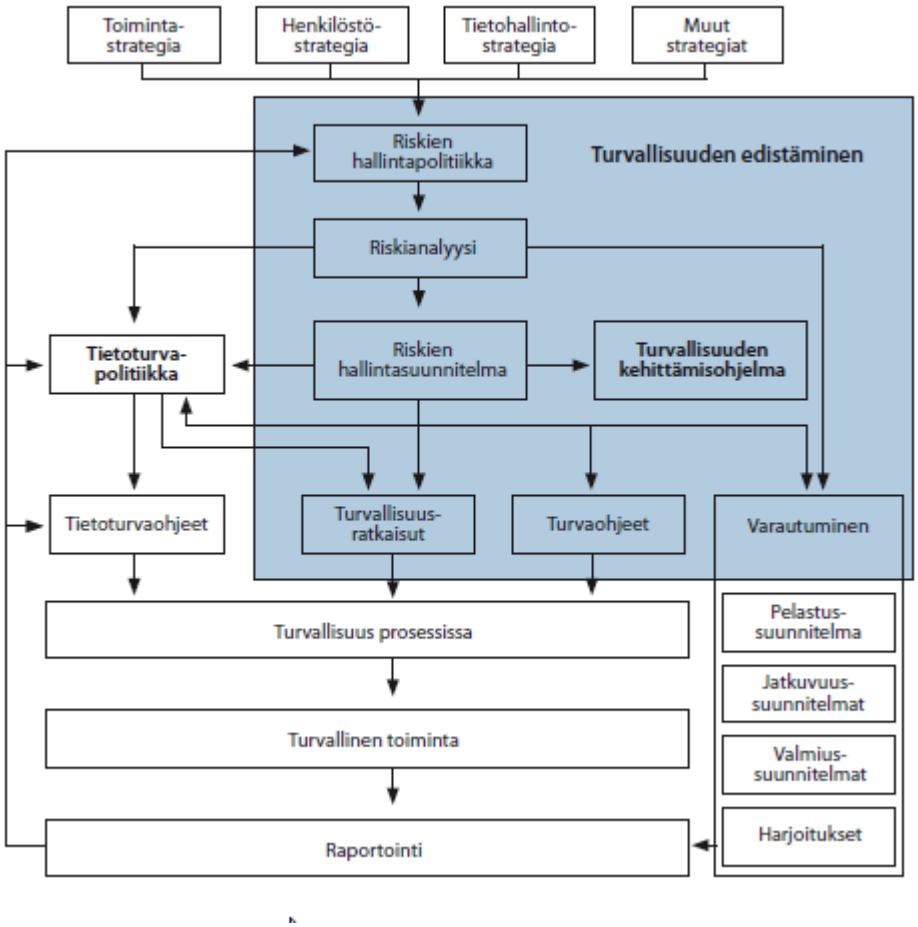
Kuva 1. Yritysturvallisuuden osa-alueet (EK Yritysturvallisuus Oy: 2009)

Tietoturvallisuus määritellään usein yhdeksi osaksi perinteistä yritysturvallisuuskokonaisuutta. Yritysturvallisuus tulee nähdä osana yrityksen riskienhallintaa, joka tukee yrityksen tavoitteita ja liiketoimintaa. Tietoturvallisuus tulee ottaa huomioon kaikessa yrityksen toiminnassa, eikä sitä voida erottaa yrityksen prosesseista, vaan sen täytyy tukea liiketoimintaa.

2.2. Mitä on tietoturvallisuus?

Tietoturvallisuudella tarkoitetaan yleisesti järjestelyitä, joilla pyritään varmistamaan tiedon käytettävyys, eheys ja luottamuksellisuus. Käytettävyys tarkoittaa tietoturvallisuuden yhteydessä sitä, että tieto on siihen oikeutettujen henkilöiden hyödynnettävissä haluttuna aikana. Eheys tarkoittaa tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa ja luottamuksellisuus sitä, ettei kukaan sivullinen saa tietoa. Tietoturvallisuus on riskienhallintaa ja osa yritysturvallisuutta.
(VAHTI 8/2008,108)

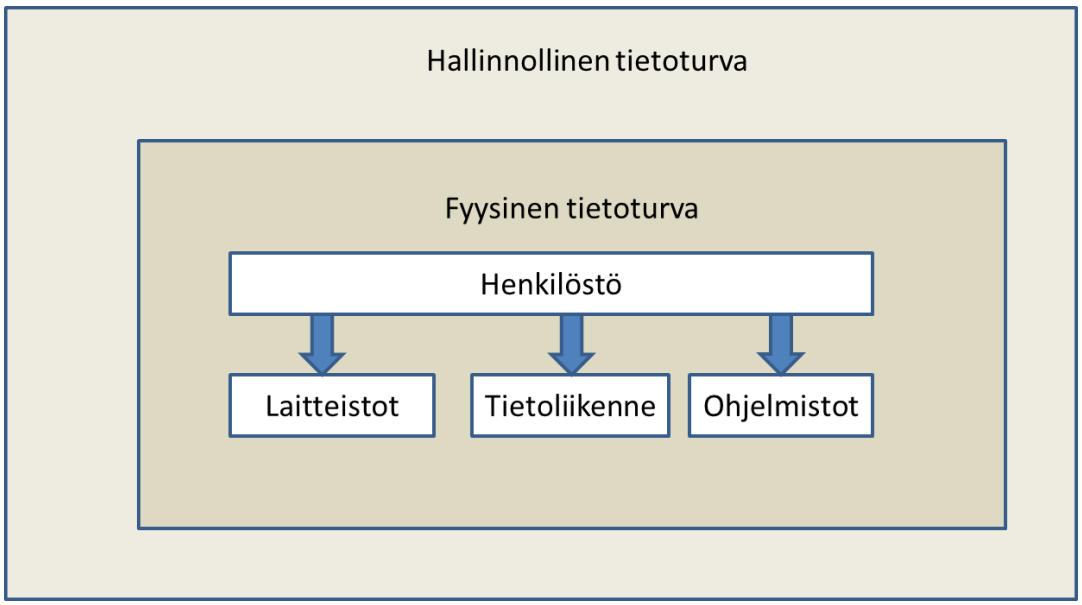
Tietoteknisellä turvallisuudella tarkoitetaan organisaation tietotekniikkaan kuten tietoliikenteeseen, laitteistoihin, ohjelmistoihin ja niiden käyttöön liittyvää tietoturvallisuutta. (VAHTI 8/2008, 106)



Kuva 2. Tietoturva- ja turvallisuussuunnitelmien keskinäiset suhteet (Vahti 3/2007, 44)

3. TIETOTURVALLISUUDEN JAOTTELU

VAHTI –ohjeistus jaottelee tietoturvallisuuden hallinnolliseen tietoturvallisuuteen, henkilöstö-, fyysiseen -, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuuteen. Kansallisessa auditointikriteeristössä (KATAKRI) jaottelu on samanlainen poikkeuksena tietojärjestelmäturvallisuus, johon sisältyy sekä laitteisto- että ohjelmistoturvallisuus. Tänä päivänä näiden erottaminen on vaikeaa, joten on loogista käsitellä niitä myös yhtenä kokonaisuutena. Tietoturvallisuuden jaottelulle ei kuitenkaan ole yhtä oikeaa mallia, vaan tämä kahdeksan osa-alueen malli antaa hyvän näkökulman tietoturvallisuudelle.



Kuva 3. Tietoturvallisuuden osa-alueet

3.1. Hallinnollinen tietoturvallisuus

Hallinnollinen tietoturvallisuus tarkoittaa niitä hallinnollisia toimenpiteitä, jotka tähtäävät organisaation tietoturvallisuuden parantamiseen. Tämä voidaan toteuttaa esimerkiksi organisaatiojärjestelyiden, tehtävien ja vastuiden määrittelyn, ohjeistuksien, koulutuksen sekä valvonnan kautta. Johdon sitoutuminen on oleellista, jotta tietoturvallisuutta voidaan kehittää. Tietoturvapolitiikka on yrityksen johdon kannanotto tietoturvallisuus asioihin. Se sisältää esimerkiksi tietoturvallisuuden yleistavoitteet organisaatiossa, lakeihin ja sopimuksiin liittyvät vaatimukset tietoturvalle, organisaation turvallisuuskoulutuksen vaatimukset, liiketoiminnan jatkuvuuden vaatimukset turvallisuudelle, turvallisuuspolitiikan rikkomusten seuraamukset, tietoturvallisuuteen liittyvien velvollisuuksien määrittelyn, poikkeustilanteiden raportointikäytännöt, ja viittaukset politiikkaan liittyviin asiakirjoihin, kuten lakeihin ja turvasuunnitelmaan. Tietoturvasuunnitelma määrittelee yksityiskohtaisesti kehittämisen aikataulut sekä toimenpiteet tietoturvapolitiikassa määriteltyjen tavoitteiden saavuttamiseksi. Näiden lisäksi on usein erillistä tietoturvasuunnitelmaa täydentäviä ohjeita, esimerkiksi ohjeet poikkeamiin reagoimiseksi, ylläpitopolitiikka,

sähköpostipolitiikka ja säännöt esimerkiksi kuolemantapausten varalle. (Tietoturva-ammattilaisen osaamistarvekartoitus)

3.2. Henkilöstöturvallisuus

Henkilöstöturvallisuus tarkoittaa oman organisaation sekä ulkopuolisten henkilöiden inhimillisestä toiminnasta aiheutuvien tietoturvariskien hallintaa. Riskejä aiheuttavat tahallisen toiminnan (esimerkiksi anastukset, yritysvakoilu, petos ja kavallus) lisäksi myös osaamattomuus ja erehdykset Tärkeitä asioita henkilöstöturvallisuuteen liittyvässä riskienhallinnassa ovat toimintatavat, rekrytointi, toimenkuvat, käyttöoikeudet, koulutus, opastaminen ja valvonta. Kriittisiä toimenkuvia suunniteltaessa tulee lähtökohtana olla, että kriittisiä tehtäviä suoritettaessa, läsnä on vähintään kaksi henkilöä ja useampi kuin yksi henkilö on tietoinen asioista. Henkilöstöturvallisuudessa on myös huomioitava sijaisjärjestelyt. Yrityksen toiminta ei saa pysähtyä esimerkiksi yhden avainhenkilön poistuttua yrityksen palveluksesta. (Tietoturva-ammattilaisen osaamistarvekartoitus)

3.3. Fyysinen turvallisuus

Fyysisellä turvallisuudella tarkoitetaan laitteiden käyttöympäristöjen suojaamista esimerkiksi lukituksilla, kulunvalvonnalla, vartioinnilla ja muilla tilojen suojaustoimilla. Tarkoituksena on estää ja hidastaa esimerkiksi palo-, vesi-, sähkö-, ilmastointi- ja murtovahinkoja. Fyysisen turvallisuuden huolehtiminen on aiheellista paitsi työpaikalla, myös muissa toimitiloissa ja etätyöpisteissä, esimerkiksi henkilön kotona. (Tietoturva-ammattilaisen osaamistarvekartoitus)

3.4. Tietoliikenneturvallisuus

Tietoliikenneturvallisuudella tarkoitetaan siirrettävän tiedon ja tietoa siirtävien laitteiden fyysistä turvallisuutta. Sen avulla pyritään varmistamaan tietojen muuttumattomuus, luottamuksellisuus ja todentamaan lähettävät ja vastaanottavat osapuolet

Tietoliikenneturvallisuudessa tarkastellaan tiedonsiirtovälineitä, tiedonsiirtoprotokollia, verkkotopologioita, tietoturvatuotteita ja salausalgoritmeja. Tietoliikenneverkkojen turvallisuudessa on kiinnitettävä huomiota erityisesti eri organisaatioiden verkkojen liityntäpisteisiin, koska laitteistot, politiikat, osaamistasot ja suhtautuminen tietoturvallisuuteen vaihtelevat suuresti organisaatioittain. Tietoliikennetuotteiden nopea kehitys aiheuttaa sen, että verkossa on usein eri-ikäisiä, standardien eri versioita noudattavia laitteita, minkä seurauksena pitää varautua siihen, että kaikki laitteiden ominaisuudet eivät ole käytettävissä kaikkien laitteiden yhteydessä. (Tietoturva-ammattilaisen osaamistarvekartoitus)

3.5. Laitteistoturvallisuus

Laitteistoturvallisuuden piiriin kuuluvat laitteet ja laitteisiin liittyvät laitteiden omat ohjelmistot eli laitekohtaiset käyttöjärjestelmät. Laitteistoihin liittyviä turvallisuusominaisuuksia ovat tunnistaminen, todentaminen, osastointi, pääsynvalvonta, itsetarkkailu, tiedon luokittelu ja valmistajan laaduntarkkailu. Laitteistojen turvaamiseen käytöstä poiston yhteydessä on syytä tehdä suunnitelma. Laitteistoturvallisuuden tietokonearkkitehtuuri muodostaa rajapinnan ohjelmistoturvallisuudelle. (Tietoturva-ammattilaisen osaamistarvekartoitus)

3.6. Ohjelmistoturvallisuus

Ohjelmistoturvallisuudella tarkoitetaan käyttöjärjestelmiin ja sovelluksiin liittyvää tietoturvallisuutta. Ohjelmistoturvallisuuteen vaikuttavia asioita ovat mm. tietokonearkkitehtuurit, käyttöjärjestelmät, kääntäjät, sovellukset, haittaohjelmat ja virukset sekä ohjelmavirheet ja näiden tietoturvapuutteet. Ohjelmistojen tietoturvavaatimukset on otettava huomioon jo suunnitteluvaiheessa, sillä jälkikäteen tietoturvallisuuden rakentaminen on hyvin mutkikasta ja kallista. (Tietoturva-ammattilaisen osaamistarvekartoitus)

On syytä myös huomioida, että ohjelmistokehityksen tietoturvallisuuteen liittyy sekä ohjelmistokoodin suojaaminen kehityksen aikana että itse ohjelmiston turvallisuus tuotannossa.

3.7. Tietoaineistoturvallisuus

Tietoaineistoturvallisuudella tarkoitetaan ainoastaan tietoihin kohdentuvaa turvallisuutta. Tiedot voivat olla missä muodossa tahansa. Tietoaineistoturvallisuus on tietojen ja tietovälineiden tunnistamista, turvallisuusluokitusta, säilytystä, varmistamista, käsittelyä ja tarpeettoman tiedon tuhoamista. Tarkoituksena on turvata tietojen eheys, muuttumattomuus, aitous, saatavuus ja luottamuksellisuus. Tiedon turvaluokittelu on olennainen osa tietoaineistoturvallisuutta. Tiedon luokittelussa on huomioitava, että tiedon turvaluokka saattaa muuttua ajan kuluessa. Tiedon eheyden kannalta on tärkeää, että tietojen versionhallinta on kunnossa. (Tietoturva-ammattilaisen osaamistarvekartoitus)

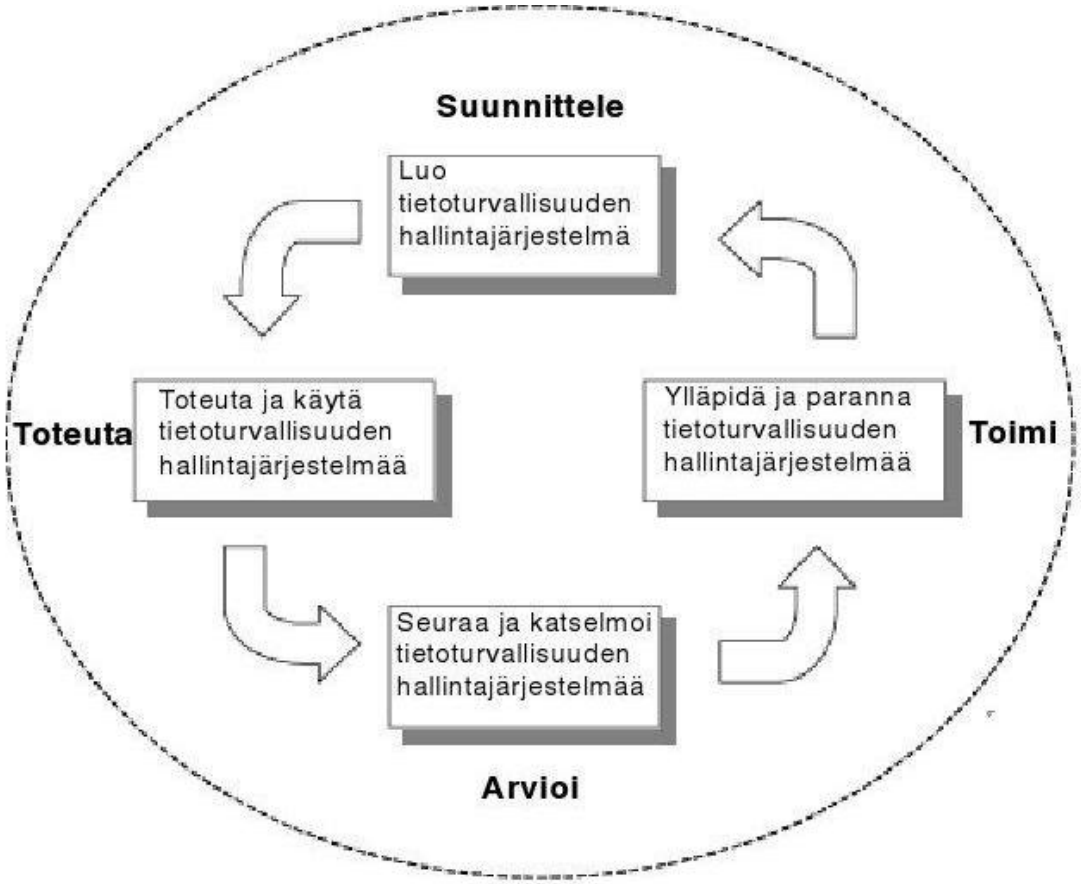
3.8. Käyttöturvallisuus

Käyttöturvallisuudella tarkoitetaan turvallisen käyttötavan, käyttöympäristön, tapahtumien valvonnan ja toiminnan jatkuvuuden hallintaa. Turvallinen käyttötapa edellyttää järjestelmien asennukselta ja ylläpidolta organisaation tietoturvasuunnitelman mukaista toimintaa. Turvallinen käyttöympäristö muodostuu järjestelmän fyysisen - ja laitteistoturvallisuuden ylläpidosta. Tapahtumien valvonnalla tarkoitetaan esimerkiksi järjestelmän tapahtumien kirjaamista lokeihin ja niiden seuraamista. Ongelmien aiheuttajat ovat näin jäljitettävissä ja niiden vaikutukset voidaan minimoida ja ehkäistä tulevat ongelmat. Jatkuvuuden hallinnalla tarkoitetaan dokumentointia ja jatkuvuussuunnitelman laadintaa. Jatkuvuussuunnitelma sisältää viittaukset dokumentteihin, josta löytyvät toipumissuunnitelma, pääsynvalvonnan toteutus, järjestelmien mahdollisten lokitiedostojen sijainnit ja muut suojaustoimenpiteet. (Tietoturva-ammattilaisen osaamistarvekartoitus)

4. TIETOTURVALLISUUDEN HALLINTAJÄRJESTELMÄ

4.1. PDCA -malli

Tietoturvallisuuden hallintajärjestelmä on dokumentoitu, rakenteellinen kuvaus organisaation käytännöistä lähtökohtana organisaation toiminta ja siihen liittyvät liiketoimintariskit. Tietoturvallisuuden hallintajärjestelmän kehittämiseen soveltuu hyvin PDCA -malli (Plan, Do, Check, Act), joka on myös ISO/IEC 27001–standardin perusajatuksena. Malli kuvaa hyvin jatkuvan oppimisen prosessia, jossa jokaisen kierroksen jälkeen ollaan hieman lähempänä tavoitetta, koska käytettävissä on aiemmilta kierroksilta saatu tieto.



Kuva 4. PDCA-malli sovellettuna tietoturvallisuuden hallintajärjestelmän prosesseihin (ISO/IEC 27001, 8)

Suunnittele (Luo tietoturvallisuuden hallintajärjestelmä)	Määrittele tietoturvapolitiikka, -tavoitteet, -päämäärät, -prosessit ja – menettelytavat, jotka ovat oleellisia riskien hallinnalle ja tietoturvallisuuden kehittämiselle organisaation yleisen politiikan ja tavoitteiden mukaisesti.
Toteuta (Toteuta ja käytä tietoturvallisuuden hallintajärjestelmää)	Toteuta ja käytä tietoturvapolitiikkaa, turvamekanismeja, prosesseja ja menettelytapoja.
Arvioi (Seuraa ja katselmoi tietoturvallisuuden hallintajärjestelmää)	Seuraa ja mittaa soveltuvin osin prosessien suorituskykyä, vertaa tuloksia tietoturvapolitiikkaan, tavoitteisiin ja käytäntöön ja raportoi tulokset johdolle katselmointia varten.
Toimi (Ylläpidä ja kehitä tietoturvallisuuden hallintajärjestelmää)	Suorita korjaavat ja ehkäisevät toimenpiteet sisäisen tietoturvallisuuden hallintajärjestelmän auditoinnin ja johdon katselmusten tulosten tai muun olennaisen tiedon perusteella, jotta tietoturvallisuusjärjestelmä kehittyy.

Kuva 5. PDCA -mallin vaiheiden selitykset (ISO/IEC 27001, 8)

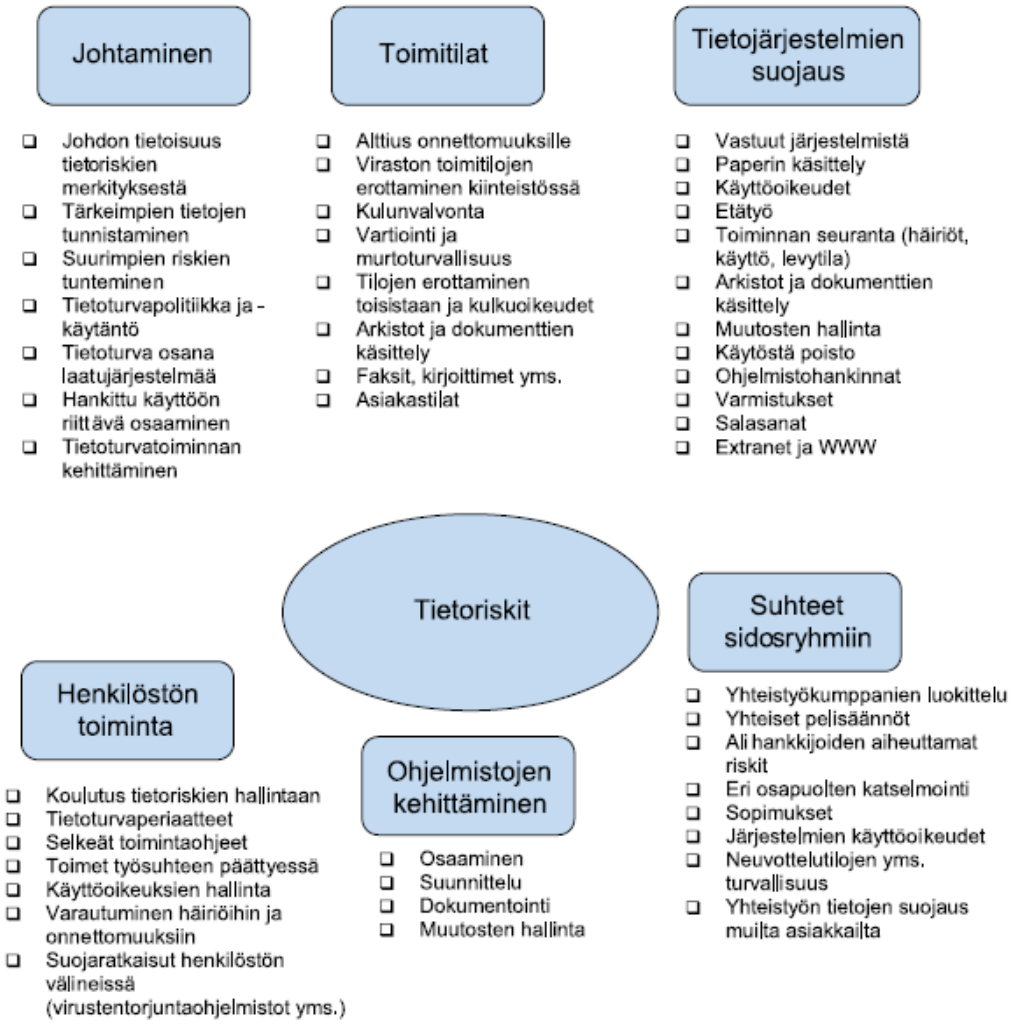
4.2. Järjestelmän suunnittelu

4.2.1. Riskikartoitus

Tietoturvallisuuden hallintajärjestelmän luominen lähtee liikkeelle tunnistamalla tieto, jolla on arvoa yritykselle. Tiedoille tulee määrittää omistajat eli yleensä prosessien vastuuhenkilöt. Seuraavaksi pyritään

löytämään tietoihin ja järjestelmiin kohdistuvat uhat ja niiden merkitystä lisäävät haavoittuvuudet. Viimeiseksi arvioidaan vaikutukset luottamuksellisuuden, eheyden tai käytettävyyden menetyksestä johtuen. (Hakala, Vainio, Vuorinen 2006, 108)

Riskikartoituksessa voidaan hyödyntää riskikarttaa (Kuvio 4), jonka avulla voidaan tarkastella tietoturvallisuuden eri osa-alueita. Kartoituksessa on hyvä olla edustajia yrityksen eri organisaatioista, jotta erilaiset näkökulmat saadaan hyödynnettyä.



Kuva 6. Esimerkki riskikartasta. (Vahti 7/2003)

4.2.2. Tietojen luokittelu

Samalla tiedot tulee luokitella, jotta niille voidaan rakentaa oikeantasoinen suojaus. Tietojen luokittelu vaikuttaa suoraan tietojen käsittelyyn. Eri luokille luodaan erilaiset käsittelysäännöt, joita henkilöstön tulee noudattaa. Järjestelmien osalta luokittelu on tärkeää laadittaessa jatkuvuus- ja toipumissuunnitelmaa. Toisaalta luottamuksellisuuden mukaan tärkeimmät tiedot järjestelmät tulee suojata parhaiten tietomurtoja vastaan, mutta ne eivät välttämättä ole tärkeimpänä mietittäessä järjestelmien toipumissuunnitelmaa. Tietojen luokittelun tekee tiedon omistaja. Luokittelun pohjana olevat tietojen turvaluokat tulee sopia yhteisesti. Määrittelyyn ei ole olemassa valmista tai yhtä oikeaa tapaa eikä missään ole määrätty käytettäväksi tiettyä luokittelua. Perussääntönä voidaan pitää, että luokkia ei tulisi olla enempää kuin neljä, jotta luokittelu olisi helpompaa. (Laaksonen, Nevasalo, Tomula 2006: 157)

Tiedon tärkeysluokka/ käsittelysääntö	**Julkinen**	**Sisäinen**	**Luottamuksellinen**	**Salainen**
Merkintä	Merkintä Julkinen vähintään dokumentin etusivulla	Merkintä Sisäinen vähintään dokumentin etusivulla	Merkintä Luottamuksellinen vähintään dokumentin etusivulla	Merkintä Salainen dokumentin jokaisella sivulla
Tiedonjakelu	Kaikille halukkaille	Kaikille yrityksen työntekijöille	Rajoitetulle joukolle yrityksen työntekijöistä	Erittäin rajoitetulle joukolle yrityksen työntekijöistä
Tiedon salaus	Ei pakollista	Ei pakollista	Pakollista, jos kuljetetaan tai lähetetään yrityksen ulkopuolelle	Aina pakollista
Lähetys sähköpostilla	Sallittu	Sallittu	Sallittu salattuna	Sallittu salattuna
Tietojen	Ei	Yrityksen	Yrityksen	Yrityksen

tallennus	rajoituksia	keskitetyissä tietojärjestelmissä	keskitetyissä tietojärjestelmissä, asianmukaiset käyttöoikeudet	keskitetyissä tietojärjestelmissä, asianmukaiset käyttöoikeudet ja tiedon salaus
Tietojen tallennus siirrettävillä muistivälineillä	Sallittu	Sallittu, salaus suositeltava	Sallittu salattuna	Sallittu salattuna

Kuva 7. Esimerkki tietojen luokittelusta. (Laaksonen, Nevasalo, Tomula 2006, 157)

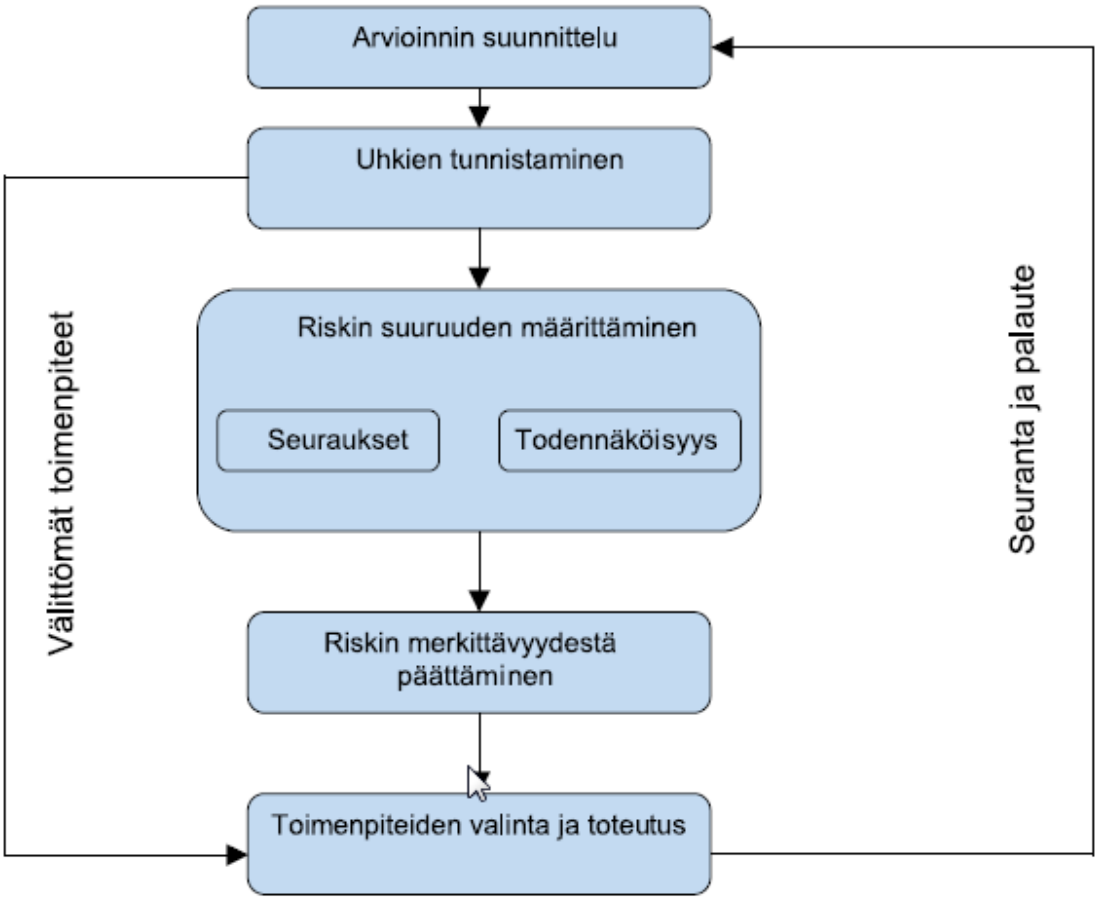
Tärkeysluokka /ominaisuus	**Kriittinen järjestelmä**	**Tärkeä järjestelmä**	**Melko tärkeä järjestelmä**	**Ei tärkeä järjestelmä**
Järjestelmän kuvaus	Järjestelmä joka liittyy erittäin keskeisesti yrityksen toimintaan. Toiminta ei voi jatkua ilman kyseistä järjestelmää	Järjestelmä joka tukee yrityksen keskeisiä liiketoimintaprosesseja. Toiminta voi jatkua jonkin aikaa ilman kyseistä järjestelmää (järjestelmä kykenee suorittamaan esim. eräajoja)	Järjestelmä, jota ei välttämättä tarvita yrityksen ydinliiketoimintaan, mutta joka helpottaa toimintaa	Tukijärjestelmä jota ei välttämättä tarvita liiketoiminnan ylläpitoon.
Järjestelmän omistaja	Tulee määritellä	Tulee määritellä	Tulee määritellä	Tulee määritellä
Sallittu keskeytysaika	< 5 minuuttia	< 4 tuntia	< 5 päivää	< 1 kuukausi
Järjestelmän sisältämien tietojen kriittisyys	Tietojen säilyminen, oikea prosessointi ja saatavuus tulee turvata kaikissa tilanteissa	Tietojen säilyminen, oikea prosessointi ja saatavuus tulee turvata, tietojen saatavuudessa voi olla max. 4 tunnin viive.	Tietojen säilyminen, oikea prosessointi ja saatavuus tulee pyrkiä turvaamaan, mutta tietojen menettäminen ei ole kriittistä	Tietojen säilyttäminen, oikea prosessointi ja saatavuus tulee pyrkiä turvaamaan, mutta tietojen menettäminen

			liiketoiminnalle.	ei ole kriittistä liiketoiminnalle
Huolto-sopimukset	Huomioivat järjestelmän luokituksen	Huomioivat järjestelmän luokituksen	Huomioivat järjestelmän luokituksen	Huomioivat järjestelmän luokituksen
Järjestelmien kahdennus/ korkean käytettävyyden ratkaisut	Pakollisia	Tarpeellisia	Ei pakollisia	Ei pakollisia

Kuva 8. Esimerkki järjestelmien luokittelusta. (Laaksonen, Nevasalo, Tomula 2006: 159)

4.2.3. Riskien analysointi

Seuraavaksi arvioidaan mitä vaikutuksia riskeillä on yrityksen liiketoimintaan, jos riskit realisoituvat. Kunkin riskin realistinen todennäköisyys on pystyttävä arvioimaan huomioiden erilaiset uhkatekijät ja haavoittuvuudet. Näiden perusteella pitää syntyä selkeä käsitys riskitasosta, jonka perusteella voidaan päättää tarvitaanko suojaavia toimia vai voidaanko riski hyväksyä. (Hakala, Vainio, Vuorinen 2006, 108) Riskin käsittelyssä on löydettävä sopivat vaihtoehdot ja arvioitava vaihtoehtojen soveltuvuus tilanteeseen. Objektiivisen arvioinnin jälkeen voidaan päätyä tietoisesti riskin hyväksymiseen. Hyväksyminen on mahdollista, kun riskin todennäköisyys on pieni ja vaikutus alhainen. Jotta varmistutaan, että kontrolli on riittävä, kannattaa jäännösriski hyväksyttää yrityksen johdolla. Muita keinoja ovat riskin siirtäminen toiselle organisaatiolle, riskin välttäminen esim. luopumalla toiminnoista, joihin sisältyy riskejä. Mikäli päädytään siirtämään riski toiselle organisaatiolle, tulee varmistua tämän kyvystä käsitellä riski asianmukaisella tavalla. Yleensä kuitenkin riskeihin varaudutaan ja niiden todennäköisyyttä pyritään pienentämään rakentamalla erilaisia riskinhallintakontrolleja. (Hakala, Vainio, Vuorinen 2006, 108)



Kuva 9. Riskien arvioinnin ja hallinnan vaiheet. (Vahti 7/2003)

4.2.4. Tietoturvapolitiikka

Riskienhallinnan kautta muodostuva kokonaiskuva on hyvä perusta luoda yritykselle tietoturvapolitiikka. Riskienhallinta ja tietoturvallisuuden linjaukset kuuluvat ylimmälle johdolle. Nämä korkean tason linjaukset esitetään yleensä tietoturvapolitiikan muodossa. Sen avulla johto osoittaa tukensa ja sitoutumisensa turvallisuuden kehittämiseen. Politiikka toimii myös pohjana yrityksen tietoturvasuunnitelmalle, -ohjeistukselle ja –koulutukselle.

Tietoturvapolitiikan tulisi ottaa kantaa seuraaviin asioihin:

- Tietoturvallisuuden tavoitteet sekä niihin liittyvät toimenpiteet. Tietoturvapolitiikassa esitellään johdon näkemys tietoturvallisuuden

vaikutuksista yrityksen toimintaan ja luodaan perusta asenteille tietoturvallisuutta kohtaan.

- Tietoturvallisuuden roolit ja vastuut. Tietoturvapolitiikassa määritellään tahot, joiden vastuulla asetettujen tavoitteiden saavuttaminen on. Politiikassa tulee määritellä yrityksen linjaus, miten tietoturvallisuus tulee huomioida sopimuksissa ja muissa juridisissa asioissa.
- Tietoturvallisuuskoulutus. Tietoturvapolitiikassa tulee määritellä tietoturvallisuuskoulutuksen vaatimukset. Koulutuksen avulla henkilöstön on mahdollista ymmärtää ja sisäistää tietoturvapolitiikan tavoitteet ja toimenpiteet tavoitteiden saavuttamiseksi.
- Tietojenkäsittelyn suojaaminen, Tietoturvapolitiikassa ei luetella suojaamisen keinoja, vaan määritetään suuntaviivat, joita suojaamisessa noudatetaan. Tällainen on esimerkiksi päätös tietosisällön luokittelusta.
- Yleiset linjaukset ottavat kantaa liiketoiminnan jatkuvuus- ja toipumissuunnittelun toteuttamiseen.
- Seuraukset tietoturvapolitiikan laiminlyönnistä. Politiikassa tulee ottaa kantaa mahdollisiin kurinpitotoimenpiteisiin ja sanktioihin.

Tietoturvapolitiikalle ei ole valmista mallia, vaan jokaisen yrityksen tulee luoda oma politiikkansa, jotta siitä on hyötyä. Käytyään keskustelun em. asioista, johdon tulee laatia keskustelusta dokumentti, joka toimii yrityksen tietoturvapolitiikkana. Valmista tai toisen yrityksen tietoturvapolitiikkaa käytettäessä, johdon sitoutuminen ei välttämättä ole ehdotonta eikä sisältöä ymmärretty, mikä vaikuttaa tietoturvaohjelman toimivuuteen. Politiikan tulee olla selkeä ja lyhyt ja se tulee kirjoittaa niin yleisellä tasolla, että jokainen lukija ymmärtää lukemansa. Tietoturvapolitiikan tulee olla jaettavissa myös yrityksen ulkopuolelle, esimerkiksi alihankkijoille tai asiakkaille. Tarvittaessa ulkopuoliset sidosryhmät, joilla on pääsy yrityksen tietojärjestelmiin, tulee sitouttaa tietoturvapolitiikkaan. Tämän vuoksi

politiikassa ei tule kuvata käytettyjä suojausmenetelmiä tai muita yksityiskohtaisia asioita. (Laaksonen, Nevasalo, Tomula 2006: 146-148)

4.2.5. Tietoturvallisuussuunnitelma

Tietoturvallisuuspolitiikkaan ei kirjata yksityiskohtia eikä käytäntöjä, miten tietoturvallisuutta toteutetaan, vaan ne tulisi kirjata tietoturvallisuussuunnitelmaan. Siinä määritellään yksityiskohtaisesti työmenetelmät ja ratkaisut, joita käytössä olevissa tietojärjestelmissä käytetään. Tietoturvasuunnitelma perustuu tietoturvallisuuspolitiikkaan, joka on pidempiaikainen ja antaa suuntaviivat ja reunaehdot. Organisaatiot, toimintaprosessit ja teknologia kehittyvät jatkuvasti, mikä edellyttää tietoturvasuunnitelman jatkuvaa päivittämistä. Suunnitelma tulisi tarkistaa vähintään kerran vuodessa ja aina tietojärjestelmissä tai työmenetelmissä tapahtuvien olennaisten muutosten yhteydessä. Tietoturvallisuussuunnitelman laativat organisaation turvallisuudesta huolehtivat tahot yhdessä tietohallinnon, tietojenkäsittelyn ja tietotekniikan ammattilaisten kanssa. Suunnitelman sisältämien yksityiskohtaisesti kuvattujen menetelmien ja teknisten ratkaisujen vuoksi dokumentti tulee luokitella vähintään luottamukselliseksi. Mikäli organisaatiolla on käytössä esim. standardiin perustuva laatujärjestelmä, tulee tietoturvasuunnitelma liittää osaksi laatukäsikirjaa. (Hakala, Vainio, Vuorinen, 2006: 9)

4.3. Roolit ja vastuut

4.3.1. Johto

Yrityksen ylin johto aloittaa sitoutumisen tietoturvallisuusasioihin laatimalla tietoturvapolitiikan. Sitoutumisella tarkoitetaan näkyvää ja vahvaa osallistumista tietoturva-asioihin niin, että henkilöstö on siitä myös tietoinen. Turvallisuusasioista tulee tiedottaa avoimesti henkilöstölle ja heillä tulee olla myös mahdollisuus osallistua turvallisuusasioiden valmisteluihin. Tämä edesauttaa henkilöstön sitoutumista johdon määrittelemään tietoturvapolitiikkaan ja helpottaa asetettujen tavoitteiden

saavuttamista. Johdon tehtävä on myös varata riittävät resurssit tietoturvallisuuden kehittämiseksi.

Johdon tulee ymmärtää tietojen suojaustarpeet, tietoriskit ja niiden hallintaan liittyvän työn laajuus sekä ymmärrys tietoturvallisuuden kehityksen suuntaviivoista. On syytä muistaa, että varsinaista vastuuta ei voi delegoida, mutta toteuttamisen voi. Johdon on kuitenkin varmistuttava, että organisaatio toimii tietoturvapolitiikan mukaisesti.

Johdon tehtäviä ovat:

- riskianalyyseihin osallistuminen
- tavoitteidenasetanta perustuen tuoreimpaan arvioon tietoturvariskeistä
- suunnitella ja organisoida tietoriskien hallinta
- perehtyä lakien, sidosryhmien ja asiakkaiden tietoturvavaatimuksiin
- päättää tietoturvallisuuden painopistealueet
- varmistaa riittävät resurssit tietoturvallisuustyöhön
- seurata tietoturvapolitiikan noudattamista.

(Laaksonen, Nevasalo,Tomula 2006: 129-130)

4.3.2. Tietoturvaorganisaatio

Tietoturvaorganisaation muodostavat ne henkilöt, jotka vastaavat tietoturvapolitiikan ja ohjeistuksen laatimisesta ja järjestävät tarvittavan koulutuksen tietoturvallisuuden jalkauttamiseksi. Se valvoo toimintaa ja raportoi toiminnasta johdolle. Tietoturvallisuusorganisaatio on liiketoiminnan tukiorganisaatio ja sen määrittelee yrityksen johto antaen samalla riittävän toimivallan ja resurssit tehtävien suorittamiseksi. Resursoinnissa voidaan hankkia omaa asiantuntemusta tai käyttää ulkopuolista apua. Tietoturvaorganisaatio tulee määritellä tarkasti ja se tulee tiedottaa henkilöstölle, jotta he osaavat ottaa yhteyttä oikeisiin henkilöihin tietoturvallisuusasioissa. Mikäli näin ei toimita, jää moni tietoturvallisuuden kannalta oleellinen asia tekemättä.

Vaikka vastuu tietoturvallisuuden organisoinnista kuuluu siihen nimetylle ryhmälle, tulee jokaisen vastata tietoturvallisuudesta omien tehtäviensä

osalta. Esimiehet vastaavat lisäksi tietoturvapolitiikassa ja ohjeistuksessa kirjattujen linjauksien noudattamisesta. Liiketoimintavastuulliset tehtäviin kuuluu arvioida ja seurata tietoturvan toteutumista omalla vastuualueellaan ja raportoida toiminnasta joko suoraan johdolle tai tietoturvaorganisaation välityksellä.

Organisaation ei tarvi olla kovin suuri ja usein tehtäviä hoidetaan oman toimen ohella. Pienemmissä yrityksissä yksikin nimetty henkilö voi olla riittävä, kunhan henkilöllä riittää kiinnostusta ja valmiuksia tehtävään.

Tietoturvaorganisaation tehtäviä:

- kehittää ohjeistus sopivaksi eri organisaatioille
- suunnitella tekninen suojaus yhdessä teknisten asiantuntijoiden kanssa sekä tietoturvallisuuden toteutumisen valvonta kaikissa projekteissa
- huomioida tietoturva-asiat käytettävissä sopimuksissa
- valvoa velvoitteiden noudattamista myös sopimuskumppanien osalta
- huolehtia tietoturvallisuuden jalkauttamisesta
- valvoa toimintaa ja raportoida siitä
- seurata yleistä tietoturvakeskustelua ja alan kehitystä

(Laaksonen, Nevasalo, Tomula 2006: 131-132)

4.3.3. Tietojen omistajat

Tiedon omistajat ovat yleensä ne, jotka luovat tai tuottavat tiedon. Tiedon omistaja määrittää tiedon julkisuuden ja oikeudet käsitellä tietoa. Omistaja on vastuussa käytettävän tiedon luotettavuudesta ja siitä, että tieto on niiden henkilöiden käytettävissä, jotka sitä tarvitsevat. Koulutuksen yhteydessä tulee kertoa myös tiedon omistajan määrittelyt tiedon luokittelusta. Tiedon käsittelijöitä määriteltäessä tulee huomioda lainsäädäntö, kuten henkilötietolaki, laki yksityisyyden suojasta työelämässä ja sähköisen viestinnän tietosuojalaki. Lähtökohtaisesti tietojen käsittely on kuitenkin mahdollista, kun se liittyy käsittelijän työtehtävien hoitamiseen. Tiedon omistajan tulee huomioida toiminnan

jatkuvuus häiriötilanteissa ja osallistua aktiivisesti liiketoiminnan jatkuvuussuunnitteluun.

Tiedon omistajien tehtäviä:

- luokitella tieto ja määritellä suojaustarpeet
- varmistaa käyttäjien koulutus
- päättää käyttöoikeudet omalta vastuualueeltaan
- tarkastaa käyttöoikeudet säännöllisesti
- määrittää ja varmistaa riittävä tietoturvallisuustaso

(Laaksonen, Nevasalo, Tomula 2006: 132-133)

4.3.4. Prosessien omistajat

Liiketoimintaprosesseille nimetään omistaja, joka on yleensä operatiivisessa vastuussa prosessista. Omistajien vastuulla on, että tietoturvallisuus on huomioitu prosessin kaikissa eri vaiheissa. Tietoturvallisuuden merkitys kasvaa, kun tietoa prosessiin tuotetaan eri organisaatioissa tai kun prosessissa on mukana ulkopuolisia toimijoita. Tietoturvauhkien todennäköisyys kasvaa, kun tietoa liikkuu eri organisaatioiden välillä ja vastuu tietoturvasta hämärtyy.

Prosessin omistajan tehtäviä:

- riskikartoitukset
- päättää asianmukaisesta prosessin suojauksesta
- luokitella suojattavat kohteet
- laatia ja testata jatkuvuussuunnitelmat yhdessä tietoturvaorganisaation ja tietohallinnon kanssa
- tietää käytetyt tiedonkäsittelytavat omalla vastuualueella
- yhdistää tietoturvallisuuden ja liiketoiminnan tavoitteet
- yhdistää tietoturvallisuuden ja prossesien kehittäminen
- varmistaa henkilöstön osaaminen
- määritellä, seurata ja raportoida poikkeamat

- raportoida ja seurata säännöllisesti (Laaksonen, Nevasalo, Tomula 2006: 134)

4.3.5. Järjestelmien pääkäyttäjät

Jokaiselle käytettävälle sovellukselle tulisi nimetä pääkäyttäjä, joka vastaa sovelluksen toimivuudesta ja sen prosessoiman tiedon luotettavuudesta. Lisäksi pääkäyttäjän tehtäviin voi kuulua myös muiden käyttäjien koulutus. Tietoturvallisuuteen liittyen pääkäyttäjä hallinnoi sovelluksen käyttöoikeuksia, mutta ei päätä niistä.
Lisäksi tietohallinto voi tarvittaessa nimetä teknisen pääkäyttäjän, jonka tehtävä on tukea sovellusta ja sen vaatimaa laitteistoa.
Pääkäyttäjien tehtäviä:

- tuntea käyttäjät
- seurata järjestelmän käyttöä
- luoda ja ylläpitää käyttöoikeuksia annettujen ohjeiden mukaisesti
- huolehtia tietojen varmistamisesta ja säilytyksestä
- päivittää ja ylläpitää järjestelmää

(Laaksonen, Nevasalo, Tomula 2006: 134-135)

4.3.6. Tietohallinto

Tietohallinto keskittyy tietojärjestelmien käytettävyyteen ja tukijärjestelmien rakentamiseen ja ylläpitoon. Järjestelmien pääkäyttäjät kuuluvat yleensä tietohallintoon. Tietohallinto vastaa tietoturvallisuuden teknisestä toteutuksesta ja ylläpidosta, mutta järjestelmien ja tiedon suojaustason päättävät tiedon, prosessien ja järjestelmien omistajat. Lisäksi tietohallinto vastaa usein laitetilojen suojauksesta, kulunvalvonnasta ja seurannasta. Tietohallinto kerää myös lokitietoja sovelluksista, aktiivilaitteista ja muista tietojärjestelmän osista, avustaa niiden analysoinnissa. Analysoinnissa tulee huomioida tunnistamistietojen käsittelyä koskevat määräykset.
Tietohallinnon tehtäviä:

- ylläpitää ajantasalla olevaa tietoa tietoturvallisuuden teknisen suojauksen keinoista ja välittää tietoa asianosaisille
- huolehtia pääsykontrollien asianmukaisuudesta
- noudattaa käyttöoikeusmenettelyitä
- varmistaa tietojärjestelmät
- turvata tiedonsiirto
- kerätä ja säilyttää lokitietoja
- testata muutokset järjestelmissä ennen käyttöönottoa

(Laaksonen, Nevasalo, Tomula 2006: 135-136)

4.3.7. Sisäinen tarkastus

Sisäisen tarkastuksen tehtävä on toiminnan epäkohtien kartoitus ja toimintaedellytysten turvaaminen, ei siis virheiden etsiminen ja niistä rankaiseminen. Sisäisen tarkastus on yhdysside eri yksiköiden välissä ja se arvioi myös tietoturvallisuuden tasoa ja sitä, miten tietoturvapolitiikkaa noudatetaan. Se voi myös arvioida teknisten ja toiminnallisten turvaratkaisujen toimivuutta.

Sisäisen tarkastuksen tehtäviä:

- arvioida tietojenkäsittelyn oikeellisuutta ja kontrolliympäristön toimivuutta
- raportoida havainnot johdolle
- laatia kehitysehdotuksia ja toimenpidesuosituksia.

(Laaksonen, Nevasalo, Tomula 2006: 136)

Sisäisen tarkastuksen organisointi voi olla haasteellista pienessä yrityksessä esim. resursoinnin tai väärien ennakkoluulojen takia. Vaihtoehtona voi olla esim. laatupäällikkö tai yritysturvallisuudesta vastaava taho, kunhan huomioidaan tahon riippumattomuus.

4.3.8. Työntekijät

Tietoturvallisuuspolitiikan tavoitteiden saavuttamisesta on jokainen työntekijä vastuussa. Jotta tavoitteet saavutetaan, on työntekijällä oltava riittävä tietämys ja ymmärrys tietoturvallisuudesta ja edellytykset soveltaa tietoturvaohjeita ja –toimintatapoja käytännössä.

Henkilöstön tehtäviä:

- luokitella ja käsitellä tietoja ohjeiden mukaisesti
- käsitellä, siirtää ja säilyttää luokiteltua tietoa asianmukaisesti
- huolehtia omien salasanojen turvallisesta käytöstä
- noudattaa ohjeita
- tiedottaa ja kouluttaa varahenkilö
- raportoida havaitut heikkoudet ja puutteet sovitun mukaisesti.

(Laaksonen, Nevasalo, Tomula 2006: 137)

4.3.9. Ulkoiset sidosryhmät

Yrityksen johto vastaa myös käytettävien ulkopuolisten palveluntuottajien toiminnasta. Palveluita ostettaessa, pitää yrityksen johdon pystyä arvioimaan ulkopuolisten toimijoiden pätevyyttä. Samoin arvioidaan toimintaan liittyvät tietoturvariskit yhdessä palvelusta vastaavien organisaatioiden omien asiantuntijoiden kanssa.

Sidosryhmien tehtäviä:

- kommunikoida avoimesti organisaation kanssa
- noudattaa sopimuksia
- tunnistaa ja kommunikoida kehitysehdotukset ja mahdollisuudet.

4.4. Malli soveltamisesta

	Yrityksen koko (henkilöä)			
Järjestelmän osa-alue	**1-10**	**11-30**	**31-100**	**101-250**
Tietoturvapolitiikka	Ei välttämätön	Ei välttämätön	Suositeltava, toimiala ja koko huomioiden.	Suositeltava, toimiala ja koko huomioiden.
Tietoturvasuunnitelma	Ei välttämätön	Suositeltava, toimiala ja koko huomioiden.	Välttämätön	Välttämätön
Tietoturvaohjeet	Välttämätön	Välttämätön	Välttämätön	Välttämätön
Riskikartoitus	Välttämätön	Välttämätön	Välttämätön	Välttämätön
Tietojen luokittelu	Suositeltava, toimiala ja koko huomioiden.	Suositeltava, toimiala ja koko huomioiden.	Suositeltava, toimiala ja koko huomioiden.	Suositeltava, toimiala ja koko huomioiden.
Riskianalyysi	Suositeltava, toimiala ja koko huomioiden.	Suositeltava, toimiala ja koko huomioiden.	Suositeltava, toimiala ja koko huomioiden.	Välttämätön
Henkilöstöryhmien osallistuminen				
Johto	Oltava tietoinen riskeistä	Oltava tietoinen riskeistä	Oltava tietoinen riskeistä, osallistuttava suunnitteluun	Oltava tietoinen riskeistä, osallistuttava suunnitteluun
Tietohallinto	Huolehtii teknisestä tietoturvasta, osallistuu suunnitteluun	Huolehtii teknisestä tietoturvasta, osallistuu suunnitteluun	Huolehtii teknisestä tietoturvasta, osallistuu suunnitteluun	Huolehtii teknisestä tietoturvasta, osallistuu suunnitteluun
Tietoturvaorganisaatio	Vastuu tietoturvallisuudesta, ei välttämättä oma organisaatio	Vastuu tietoturvallisuudesta, ei välttämättä oma organisaatio	Vastuu tietoturvallisuudesta, toimialasta riippuen tulisi nimetä vastuullinen	Vastuu tietoturvallisuudesta, toimialasta riippuen tulisi nimetä vastuullinen
Tiedon omistajat	Ei välttämätön	Ei välttämätön	Toimialasta riippuen tulisi nimetä omistajat, jotka osallistuvat suunnitteluun	Toimialasta riippuen tulisi nimetä omistajat, jotka osallistuvat suunnitteluun
Prosessin omistajat	Ei välttämätön	Ei välttämätön	Toimialasta riippuen tulisi nimetä omistajat, jotka osallistuvat suunnitteluun	Toimialasta riippuen tulisi nimetä omistajat, jotka osallistuvat suunnitteluun
Järjestelmien pääkäyttäjät	Laatii tietoturvaohjeet	Laatii tietoturvaohjeet	Laatii tietoturvaohjeet, osallistuu suunnitteluun	Laatii tietoturvaohjeet, osallistuu suunnitteluun
Sisäinen tarkastus	Ei välttämätön	Ei välttämätön	Ei välttämätön, tulisi järjestää mahdollisuuksien mukaan	Ei välttämätön, tulisi järjestää mahdollisuuksien mukaan
Muu henkilökunta	Tietoturvaohjeistuksen noudattaminen	Tietoturvaohjeistuksen noudattaminen	Tietoturvaohjeistuksen noudattaminen	Tietoturvaohjeistuksen noudattaminen
Ulkoiset sidosryhmät	Tulee huomioida tietoturvaohjeistuksessa	Tulee huomioida tietoturvaohjeistuksessa	Tulee huomioida tietoturvaohjeistuksessa	Tulee huomioida tietoturvaohjeistuksessa

Kuva 10 Esimerkki järjestelmän suunnittelusta ja vastuista

Oheisessa taulukossa (Kuva 10) on pyritty kuvaamaan mitä eri kokoisissa yrityksissä tulisi tehdä ja mitkä henkilöstöryhmät tulisi osallistaa tietoturvallisuuden hallintajärjestelmän suunnitteluun. Yhtä ja oikeaa mallia ei ole, koska yritykset ovat erikokoisia ja niiden toiminta on hyvin erilaista. Yritysten, jotka havaitsevat riskikartoituksessa tietoturvariskejä, tulisi huomioida tietoturvallisuus vähintään tietoturvaohjeistuksen muodossa ja luoda säännöllinen prosessi riskien hallitsemiseksi.

5. YHTEENVETO

PK-yritykset kamppailevat nykypäivänä monien haasteiden parissa. Aika ja raha ei riitä kaikkeen, jolloin on keskityttävä vain ja ainoastaan ydinliiketoimintaan ja vain välttämättömiin tukitoimintoihin. Yrityksen prosessit eivät kehity, vahinkoja sattuu, tehdään asioita moneen kertaan ja kaikki toiminnan kehittäminen, turvallisuus ja laadun parantaminen ovat kulueriä.

Tietoturvallisuus, kuten muukin turvallisuus on osa yrityksen toiminnan laadun parantamista. Kun riskit tunnistetaan ja niihin puututaan, yrityksen toiminta kehittyy ja tehostuu, mikä parantaa tuottavuutta ja luo kilpailukykyä.

Tietoturvallisuuden hallintajärjestelmä on osa yrityksen kokonaisturvallisuutta ja kokonaisturvallisuus lähtee riskienhallinnasta. Nämä eivät ole irrallisia kokonaisuuksia, vaan ne on nähtävä osana yrityksen prosesseja, jotka tukevat liiketoiminnan tavoitteisiin pyrkimistä. Tässä työssäni olen pyrkinyt löytämään tärkeimmät asiat, joihin tietoturvallisuudessa tulee keskittyä, kun tavoitteena on aloittaa tietoturvallisuuden kehittäminen. Tavoite ei ole ISO/IEC 27001 – sertifikaatti, vaan käytäntöjen kehittäminen ja varsinkin kehittämisen aloittaminen. PDCA-prosessi vie kierros kierrokselta eteenpäin ja valmiudet jopa ISO/IEC 27001 -sertifiointiin paranevat. Tarkastelussa voi käyttää matkan varrella esim. KATAKRIn kriteeristöä tai PK-RH – kyselylomakkeita (www.pk-rh.fi). Perusta kaikissa ISO/IEC 27001-

standardi mukaan lukien on sama ja se on pyritty kuvaamaan tässä työssä.

Tärkeintä on kuitenkin ihmiset ja ihmisten toiminta. Ihmiset rakentavat järjestelmät, käyttävät niitä ja tekevät virheitä. Vaikuttamalla ihmisiin ja saamalla henkilöstön ymmärtämään mitä vaikutusta turvallisuudella on, toiminta lähtee muuttumaan kuin itsestään. Haasteena on miten vaikuttaa ihmisiin ja asenteisiin.

6. LÄHDELUETTELO

Elinkeinoelämän keskusliitto: 2011, www.ek.fi/www/fi/yrittajyys_ja_pk/pk_yritykset/Merkitys_kansantaloudessa_ja_eussa.php.

EK Yritysturvallisuus Oy: 2009, www.ek.fi/ytnk08/fi/yritysturvallisuus.php,

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

Laaksonen M., Nevasalo T., Tomula K. 2006.Yrityksen tietoturvakäsikirja. Edita Publishing Oy.

ISO/IEC 27001:fi,

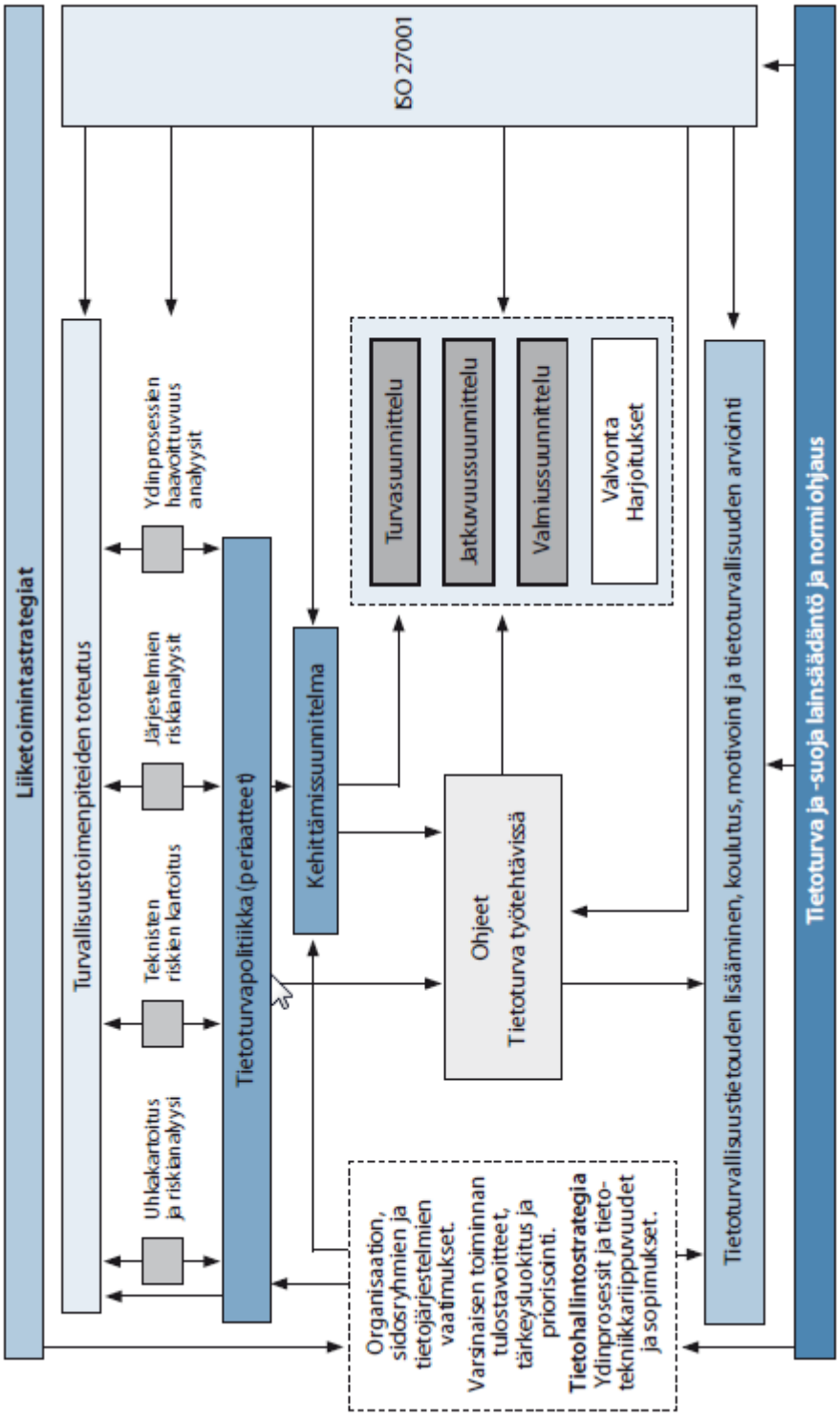
Tietoturva-ammattilaisen osaamistarvekartoitus – diplomityö. Sulosaari A. 2004.

VAHTI 3/2007: Yleisohje tietoturvallisuuden johtamiseen ja hallintaan.

VAHTI 7/2003: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa.

VAHTI 8/2008: Valtionhallinnon tietoturvasanasto.

7. LIITTEET



Liite 1. Tietoturvallisuuden hallintajärjestelmän malli (VAHTI 3/2007,4)