1

LAUREA

Tietoturvallisuuden kehittäminen yrityksessä

Seppänen, Olli

2012 Leppävaara

2
3

Laurea-ammattikorkeakoulu
Laurea Leppävaara

Tietoturvallisuuden kehittäminen yrityksessä

Seppänen, Olli
Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
Toukokuu, 2012

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Leppävaara
Tietojenkäsittelyn koulutusohjelma

Seppänen, Olli

Tietoturvallisuuden kehittäminen yrityksessä

Vuosi 2012 Sivumäärä 49

Tietoturvallisuus on nykyaikana elintärkeä osa turvallista ja tehokasta yritystoimintaa. Verkkorikollisuus ja tietomurrot ovat arkipäivää, joten yritykset ovat valmiita tekemään kaikkensa suojatakseen liiketoiminnan kannalta arvokkaita tietoja ja resursseja.

Tietoturvallisuuden toteutuminen on aina kiinni ihmisistä. Parhaatkaan tekniset ratkaisut eivät hyödytä jos tietoturvallisuuden pelisääntöjä ei tiedetä. Yrityksellä on siis oltava selkeä tietoturvapolitiikka ja tietoturvaohjeet, jotka toimivat tietoturvallisen toiminnan perustana.

Asiakasyrityksenä toimivasta SGN Group Oy:stä annettiin tehtäväkseni uuden tietoturvapolitiikan sekä ohjeistuksen laatiminen. Tällä tavoin toimeksiantajan henkilökunnan tietoturvatietoisuutta ja –osaamista voidaan kehittää. Tietoturvapolitiikka sekä ohjeistus on suunniteltu mahdollisimman yleisluontoisiksi, jolloin niiden muokattavuus säilyy ja ne toimivat pohjana tarkemmille ohjeille.

Opinnäytetyössä käsitellään tietoturvallisuutta yritystoiminnan näkökulmasta tarkasteltuna. Teoriaosuudessa esitellään tietoturvallisuuden yleismääritelmää, tärkeimpiä standardeja, tietoturvapolitiikkoja, tietoturvallisuuden johtamis- ja hallintajärjestelmää sekä tietoturvaohjeita.

Tulokset on koottu opinäytetyön loppuun kolmeksi eri liitteeksi.

Asiasanat: tietoturvallisuus, tietoturvapolitiikka, tietoturvaohjeistus

Laurea University of Applied Sciences **Abstract**
Laurea Leppävaara
Bachelor's Degree Programme in Business Information Technology

Seppänen, Olli

Developing information security in a company

Year 2012 Pages 49

Information security is today a vital part of safe and efficient business. Cybercrime and hacking are an everyday problem, so companies are willing to do everything to protect valuable business information and resources.

Implementation of information security always depends on how people act. Even the best technical solutions are not beneficial if the knowledge of the safety rules is unclear. The company must therefore have a clear security policy and security guidelines, which operate as a basis for secure actions.

This thesis was commissioned by SGN Group Ltd., assigning a new information security policy as well as guidelines to be prepared. In this way, security skills and awareness of the personnel of the target company can be developed. Security policy and guidelines are designed to be generic in order to maintain their malleability and at the same time they serve as a basis for more precise instructions.

This thesis addresses information security from a business perspective. The theoretical section presents a general definition of information security, the most important standards, security policies, information security management, control system and security guidelines.

The results are compiled into three different annexes at the end of this thesis.

Key Words: information security, information security policy, information security instructions

Sisällys

1 Johdanto

Tietoturvallisuus on elintärkeä liiketoimintaan sitoutuva osa-alue nykyaikaisissa yrityksissä. Yritykset käsittelevät päivittäin erilaista tietoa, josta suurin osa voidaan luokitella salaiseksi tai luottamukselliseksi. Tällaisen tiedon joutuminen vääriin käsiin voi aiheuttaa tiedon omistavalle yritykselle muun muassa taloudellisia tappioita. Tietoturvallisuuden on sulauduttava täydellisesti osaksi yritysten liiketoiminnallisia prosesseja, jotta voidaan varmistua tietojen oikeanlaisesta ja ennenkaikkea turvallisesta käsittelystä. Tietoturvallisuus ei ole pelkästään teknistä toteuttamista. Täytyy huomioida myös ihmisten työskentelytavat ja tottumukset. Yrityksissä tapahtuvan tietoturvakoulutuksen yksi päätavoitteista onkin ihmisten motivaation kasvattaminen tietoturvallisuusasioita käsiteltäessä (Nykänen 2011, 20). Merkille pantavaa on myös se tosiasia, että tiettyjen tietojen turvaamiselle yrityksissä on olemassa lainsäädännöllisiä velvoitteita, esimerkiksi henkilötietolaki.

Tässä opinnäytetyössä esitellään ja pohditaan tietoturvallisuutta sekä sen merkitystä yritysten toiminnassa ja suunnitellaan kohdeyritykselle uusi tietoturvapolitiikka, tietoturvaohjeistus sekä uusien tietoturvaohjeiden jalkauttaminen henkilökunnalle. Tarkoituksena on kohottaa kohdeyrityksen kokonaisvaltaista tietoturvan tasoa sekä henkilökunnan tietoturvatietoisuutta. Kohdeyritys ottaa käyttöönsä tämän työn tuloksina syntyneet tietoturvaohjeet.

Työ on jaettu seitsemään lukuun. Johdantoluvussa luodaan yleiskatsaus tietoturvallisuuteen sekä kerrotaan tämän opinnäytetyön tarkoituksesta. Toinen luku kertoo asiakkaana toimivasta kohdeyrityksestä, työn rajauksesta, tavoitteista sekä menetelmistä. Kolmannessa luvussa käsitellään tietoturvallisuutta yrityksen näkökulmasta. Neljäs luku puolestaan keskittyy tietoturvapolitiikkoihin ja niiden merkitykseen yritystoiminnassa. Viidennessä luvussa analysoidaan tietoturvallisuuden johtamis- ja hallintajärjestelmän toimintaa. Kuudes luku kertoo yrityksen tietoturvaohjeista, henkilöstön motivoinnista, kouluttamisesta, tietoturvatietoisuudesta sekä tietoturvakäyttäymiseen vaikuttavista seikoista. Viimeisessä luvussa kerrotaan työn tuloksista yhteenvedon muodossa.

2 Opinnäytetyön tavoite ja lähtökohdat

Opinnäytetyön tavoitteena on ratkaista kohdeyrityksen ongelma. Tällä hetkellä voimassaoleva tietoturvapolitiikka on riittämätön lähes jokaiselta osa-alueeltaan ja se on tarkoitettu lähinnä kohdeyrityksen vanhoja toimitiloja varten. Myöskään erillistä henkilökunnalle tarkoitettua tietoturvaohjetta ei ole olemassa. Tarkoituksena on siis kehittää uudenlainen yleispätevä tietoturvapolitiikka, johon on selkeästi määritelty tarpeelliset kohdeyrityksen tietoturvaa koskevat osa-alueet. Henkilökunnan tietoturvaohjeella pyritään kohottamaan henkilökunnan tietoturvatietoisuuden tasoa sekä minimoimaan ongelmatilanteiden syntymistä. Varsinaisena tutkimusongelmana tässä työssä on uusien tietoturvaohjeiden jalkauttaminen kohdeyritykseen. Jalkauttaminen tullaan osaksi toteuttamaan seminaarityyppisellä tilaisuudella kohdeyrityksessä tämän opinnäytetyön avulla. Henkilökunta tullaan myös sitouttamaan uusiin tietoturvaohjeisiin sekä niiden noudattamiseen.

2.1 Työn rajaus

Opinnäytetyö on rajattu koskemaan uutta tietoturvapolitiikkaa, ohjeistusta sekä näiden jalkauttamista kohdeyritykseen. Lisäksi tarkastellaan tietoturvallisuutta yleisesti, sen määritelmiä ja toteuttamista yritysympäristöissä.

Tässä työssä esiteltävä tietoturvapolitiikka perustuu osittain kohdeyrityksen nykyiseen politiikkaan, mutta myös toisten yritysten politiikkoja sekä lähdeaineistoa on käytetty apuna. Henkilökunnan tietoturvaohje noudattaa pääpiirteittäin Valtionhallinnon marraskuussa vuonna 2006 julkaisemaa henkilöstön tietoturvaohjetta, jota voidaan soveltaa lähes kaikissa yrityksissä. Tutkimusongelman ratkaisu taas lähtee liikkeelle ongelman ymmärtämisestä ja kartoittamisesta. Lopputuloksena esittelen teorioiden ja tutkimustulosten pohjalta rakennettun ehdotuksen, jonka avulla tietoturvaohjeiden jalkauttaminen voidaan suorittaa tehokkaasti.

2.2 Tutkimusmenetelmä ja kohdeyrityksen perustiedot

Menetelmänä käytetään konstruktiivista tutkimusta, jolle on ominaista muun muassa tutkimusongelmien liittäminen tai sitominen aiempaan tietämykseen ja lähteisiin. Konstruktiivisella tutkimusotteella pyritään tuottamaan ratkaisuja aitoihin reaalimaailman ongelmiin ja tällä tavoin luomaan kontribuutioita sille tieteenalalle, johon sitä sovelletaan. Konstruktiivista tutkimusta voidaan pitää eräänlaisena menetelmäoppina, jonka pääasiallisena tarkoituksena on tuottaa innovaatiivisia konstruktioita. Tutkimusote on myös yksi case-tutkimuksen muoto. Tyypillistä tälle tutkimusotteelle on myös kattava liikkuminen teorian ja käytännön välillä sekä tutkijan suorittamien interventioiden käyttäminen tutkimusmetodina.

Tärkeää on myös se, että löydetty ratkaisu toimisi parhaimmassa tapauksessa myös muualla kuin esimerkiksi vain kohdeorganisaatiossa. Yleensä kuitenkin konstruktion toimivuuden testaus vaatii lisätyötä. Opinnäytetöissä sekä muissa vastaavissa kehittämistöissä joudutaan usein lisäksi miettimään, miten selvä näyttö tai ratkaisu rakenteen toimivuudesta tarvitaan. Konstruktiivisessa tutkimuksessa kohdeorganisaatio saa puolueettoman ja teoreettiseen tietämykseen perustuvan ratkaisun tutkimusongelmaan. Siinä korostuu myös tutkimuksen hyödyntäjän ja toteuttajan välinen kommunikaatio. Konstruktiivinen tutkimus tulee siis kyseeseen kun tutkimusongelman ratkaisuun tarvitaan ehdottomasti teoreettista tietämystä. Tämän lisäksi konstruktiivisessa tutkimusotteessa voidaan käyttää monenlaisia menetelmiä, koska lähestymistapa ei sinällään rajaa ulos mitään menetelmää. (Metodix & Ojasalo, Moilanen & Ritalahti 2009, 65-66, 68.)

Ojasalo ym. (2009, 67) ovat jakaneet konstruktiivisen tutkimusmenetelmän vaiheet kuuteen vaiheeseen:

1. Mielekkään ongelman etsiminen.
2. Syvällisen teoreettisen ja käytännöllisen tiedon hankinta tutkimuksen ja kehittämisen kohteesta.
3. Ratkaisujen laatiminen.
4. Ratkaisun toimivuuden testaus ja konstruktion oikeellisuuden osoittaminen.
5. Ratkaisussa käytettyjen teoriakytkentöjen näyttäminen ja ratkaisun uutuusarvon osoittaminen.
6. Ratkaisun soveltamisalueen laajuuden tarkastelu.

Tutkimusongelman luonteen vuoksi oli tarkoituksenmukaista valita konstruktiivinen tutkimusmenetelmä. Tutkimuksen tarkoituksena on löytää ratkaisu, joka kehittää kohdeyrityksen tietoturvallista toimintaa. Ongelman ratkaisu perustuu osaltaan yritykseltä saatuihin dokumentteihin, joita tutkimalla olen saanut riittävän käsityksen tutkimusongelman laadusta. Apuna on myös käytetty aiheeseen liittyvää teoriaa sekä omaa tietämystäni. Kohdeyrityksen kanssa on sovittu, että ongelma ratkaistaan päivittämällä yrityksen tietoturvapolitiikka, luomalla henkilöstölle tietoturvaohjeet sekä suunnittelemalla ehdotus, jonka avulla tietoturvaohjeet on järkevintä jalkauttaa kohdeyritykseen.

Kuten kappaleessa kaksi todetaan; kohdeyrityksen nykyinen tietoturvapolitiikka on riittämätön ja suunniteltu yrityksen vanhoja toimitiloja varten. Henkilöstölle ei ole suunniteltu yleispätevää tietoturvaohjetta teknisten ohjeiden rinnalle. Kohdeyrityksen kannalta tärkein kysymys on se, että miten nämä tietoturvadokumentit saadaan tehokkaasti jalkautettua henkilöstön pariin. Kohdeyrityksen kanssa sovittiin, että tietoturvapolitiikasta luodaan uusi versio, joka palvelee yrityksen toimintaa aiempaa tehokkaammin tietoturvallisuuden saralla. Teknisten tietoturvaohjeiden rinnalle rakennetaan yleiset ohjeet,

joita henkilöstö sitoutuu noudattamaan päivittäisissä töissään. Uusittujen ohjeiden täytyy täten nostaa yleistä tietoturvatietoisuutta ja tietoturvallisuuden tasoa, joten päätimme vielä, että suunnittelen kohdeyritykselle ohjeiden jalkauttamiseen sopivan koulutussuunnitelman.

Työ aloitettiin aiheanalyysillä, jossa määriteltiin muun muassa aihealuetta yleisesti, tutkimusongelman laatu sekä perusteltiin sen tutkimusarvoa. Tämän lisäksi aiheanalyysissä käytiin läpi varsinaisessa työssä käytettävää materiaalia ja arvioitiin soveliasta lähestymistapaa ja tutkimusmenetelmää. Aiheanalyysin jälkeen tein vielä tutkimussuunnitelman, jonka tarkoituksena oli jäsentää alkavaa opinnäytetyötä sekä antaa kattava kokonaiskuva opinnäyteen sisällöstä. Sekä aiheanalyysi, että tutkimussuunnitelma hyväksytettiin tämän työn ohjaajalla ja kohdeyrityksessä. Varsinainen opinnäytetyö tehtiin yhteistyössä kohdeyrityksen kanssa.

Tutkimusprosessi käynnistettiin selvittämällä tutkimusongelman piirteet sekä sen laajuus. Ja tähän liittyen kartoitettiin myös kohdeorganisaation nykytila sekä odotukset ja työn vaatimat resurssit suhteessa tutkimusongelmaan. Kohdeyritystä koskevaa tutkimusongelmaa ei voitu ratkaista perinteisillä tiedonhakutavoilla, vaan oli perehdyttävä yrityksen toimintaan. Konkreettisten tulosten saavuttamiseksi tarvittiin pohjatietoa sekä teoreettista tietämystä. Pohjatietoa sain suoraan kohdeyrityksen edustajilta sekä yrityksen internetsivuilta. Teoreettista tietämystä liittyen tutkimusongelmaan löytyi sekä minulta että yrityksen edustajilta. Tämän lisäksi hankittiin vielä aiheeseen liittyvää kirjallisuutta sekä haettiin tietoa tavanomaisilla menetelmillä.

Tutkimusongelman ratkaisuun tarvittavan tiedon hankinnan jälkeen työtä jatkettiin muutamalla suunnittelupalaverilla, joihin osallistuivat tämän työn tekijä sekä yrityksen edustajat. Palavereissa keskusteltiin sopivien ratkaisumallien kehittämisestä, jotka parhaiten sopivat yrityksen toimenkuvaan ja nykytilaan. Ideoita ja tietoa vaihdettiin molemminpuolisesti ja sovittiin edellä mainittujen kolmen tietoturvallisuusdokumentin luomisesta. Palaverien lisäksi tiedonvaihtoa ja keskustelua käytiin myös sähköpostin välityksellä. Tutkimusprosessin aikana lähetin opinnäytetyön säännöllisin väliajoin sekä muina sovittuina aikoina kohdeyritykseen arvioitavaksi ja kommentoitavaksi. Saadun palautteen ja arvioinnin perusteella kehittämistyötä oli loogista jatkaa eteenpäin. Kehittämistyön tuloksina syntyivät uusi tietoturvapolitiikka, yleinen henkilöstön tietoturvaohje sekä näiden jalkauttamissuunnitelma, jotka kohdeyritys ottaa käyttöönsä.

Työn tilaaja sekä toimeksiantaja on SGN Group Oy, joka on kotimarkkinoilla sekä lähialueilla toimiva tukkukaupan alan perheyritys. SGN Groupin toimialat koostuvat urheilu- ja vapaa-ajan tuotteista, maataloudesta, ympäristönhoidosta sekä teollisuuslaitteista. Sen palveluksessa on

160 työntekijää ja liikevaihto on noin 170 miljoonaa euroa. SGN Group sijaitsee Vantaan Koivuhaassa. (SGN Group, 2008)

3 Yleistä yritysten tietoturvasta

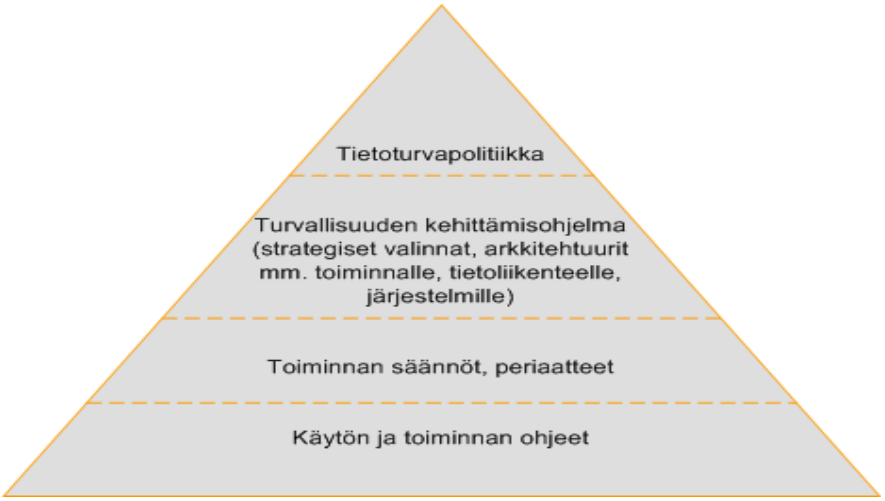
Tietoturvallisuus yrityksissä on tärkeä osa menestyksekästä liiketoimintaa. Ilman toimivaa tietoturvaa ei voi olla menestyvää yritystä. Tässä kappaleessa käydäänkin läpi tietoturvallisuuden perusasiat ja valotetaan niiden merkitystä yritystoiminnassa.

Tietoturvallisuuden määritelmä perustuu pitkälti tiedon kolmen perusominaisuuden turvaamiseen, joita ovat: eheys, käytettävyys sekä luottamuksellisuus. (Laaksonen, Nevasalo & Tomula 2006, 17.) Eheydellä viitataan tiedon oikeellisuuteen ja täydellisyyteen. Jos tieto muuttuu tai sitä muutetaan hallitsemattomasti, eheys menetetään. Käytettävyyden määritelmänä voidaan pitää sitä, että tietoon oikeutetut pääsevät siihen käsiksi vaaditulla tavalla ja haluttuna ajankohtana. Luottamuksellisuudella tarkoitetaan sitä, että tietoon pääsevät käsiksi vain ne, jotka ovat oikeutettuja pääsyyn. Pääsyllä tässä yhteydessä tarkoitetaan tiedon lukemista tai kopiointia.

Tietoturvallisuudella pyritään siis suojaamaan asianmukaisesti yrityksen erilaiset tiedot, tietojärjestelmät sekä palvelut niin, että niiden eheyteen, luottamuksellisuuteen ja käytettävyyteen liittyvät riskit ovat hallinnassa. Tällainen toiminta on osa yrityksen toiminnan laatua. Käytäntöön tuotuna tällä tarkoitetaan esimerkiksi sitä, että osaa tiedoista ja tietojärjestelmistä voivat käyttää vain niiden käyttöön oikeutetut henkilöt. Tällöin sivulliset eivät voi muuttaa, kopioida tai poistaa tietoja. Tietojen käsittelyyn oikeutetut saavat käyttää tietoja ja tietojärjestelmiä vain työtehtäviensä hoitamiseen tarvittavilla oikeuksilla. Tietojen, tietojärjestelmien sekä palveluiden täytyy olla myös ajantasaisia, luotettavia sekä oikeita. Ne eivät saa paljastua, tuhoutua tai muuttua hallitsemattomalla tavalla esimerkiksi asiattoman toiminnan, haittaohjelmien tai laitteisto- tai ohjelmistovikojen takia. Tietojen, tietojärjestelmien sekä erilaisten palveluiden on oltava saatavilla ja toimintakuntoisia silloin kun niitä tarvitaan. Nykyään sähköinen asiointi erilaisissa palveluissa on hyvinkin yleistä, joka tuo lisävaatimuksia tietoturvallisuudelle. Sähköisen asioinnin osapuolet täytyy pystyä tunnistamaan luotettavasti sekä myös asiointitapahtumat ja niiden sisällöt tulee voida todistaa jälkikäteen. (VAHTI 10: Henkilöstön tietoturvaohje 2006, 10.)

Tietosuojan ja tietoturvan merkitykset on hyvä osata erottaa toisistaan, mikä ei aina ole helppoa. Tietosuoja suojaa ihmisen tiedollista itsemääräämisoikeutta sekä yksityisyyttä. Tietosuojaa voidaan ylläpitää tietoturvan tarjoamin keinoin sekä toimintamallein. Ymmärtämistä voidaan helpottaa ajatusmallilla, jossa ajatellaan, että tietoturva on muuri suojattavan tiedon ympärillä. Tietoturvallisuudella on suuri merkitys yritysten

organisaatiokulttuurissa ja se onkin pieniä tekoja osana jokapäiväistä toimintaa. Tällöin tietoturvallisuuden merkitys ymmärretään paremmin ja sen saavuttamiseksi ja ylläpitämiseksi työskennellään tehokkaammin. Tietoturvallisuus rakentuu teknisistä ja hallinnollisista komponenteista, joiden suunnittelu ja toteutus tulee tehdä huolella, koska huomioon joudutaan ottamaan muun muassa lainsäädännön vaatimukset ja rajoitukset. Näiden vaikutuksia on hyvä seurata toiminnan kehittämisen kannalta. (Laaksonen ym. 2006, 17.)



Kuva 1: Tietoturvallisuuden arkkitehtuuri (Yliopistojen IT.)

Hyvän tietoturvallisuustason määrittäminen, ylläpitäminen ja saavuttaminen yrityksessä vaatii määrätietoista toimintaa ja johtamista. Tietoturva tulisi nähdä ennenkaikkea kilpailuetuna liiketoiminnallisesti ajateltuna, joten sen on siis toimittava liiketoiminnan asettamien vaatimusten mukaisesti. Tällainen kilpailuetu voi realisoitua esimerkiksi liiketoiminnallisten edellytysten kehittymisenä, jos yrityksen tietoturvakulttuuri on sulautettu käytössä olevaan liiketoimintaympäristöön. Kilpailuetua on myös hyvä ajatella tarjouskilpailuiden voittamisen kannalta, koska nykypäivänä niissä saattaa esiintyä vaatimuksia koskien tietoturvallisuutta. (Laaksonen ym. 2006, 17-18.)

3.1 Lainsäädännölliset velvoitteet ja vaatimukset

Laaksonen ym. 2006 (18), sekä tietoturvaopas.fi –sivusto käsittelevät yrityksen lainsäädännöllisiä velvoitteita sekä vaatimuksia kattavasti ja helposti ymmärrettävällä tavalla. Erityisesti kannattaa huomioida, että monet asetukset ja lait sisältävät säännöksiä, jotka liittyvät tietoturvallisuuden järjestämiseen yrityksessä, esimerkiksi henkilötietojen suojaamisesta määrätään laissa. Kotimainen sekä ulkomainen lainsäädäntö asettaakin yrityksille erilaisia suoria tai epäsuoria velvoitteita tietoturvallisuuteen liittyvien asioiden hoitamiseksi. Huomattavaa on kuitenkin se, että yleensä tällaiset velvoitteet ovat luonteeltaan yleisiä. Yritykset joutuvat itse huolehtimaan riittävästä tietoturvallisuuden tason

määrittelystä sekä käytännön toteutuksista. Yritys on itse vastuussa toimintansa lainmukaisuudesta ja sen vastuulla on myös henkilöstön ohjeistus.

Jos asiaa ajatellaan yritysten näkökulmasta, on hyvä selventää muutama asia. Varsinkin ne lakiin perustuvat säädökset, jotka vaikuttavat tietoturvan suunnittelun, ylläpidon sekä kehittämisen ohjaukseen, on hyvä kartoittaa ennakkoon: esimerkiksi sähköisen viestinnän tietosuojalain toteutusta valvoo Viestintävirasto. Lainsäädännön lisäksi on tärkeää myös oppia tunnistamaan erilaisiin sopimuksiin kuuluvat tietoturvavelvoitteet ja oikeudet. Tästä on hyötyä esimerkiksi silloin, kun sopimusasioissa tai sopimuskiistoissa joudutaan miettimään ongelmakohtien sopivaa tarkastelunäkökulmaa. (Laaksonen ym. 2006, 18.)

Kansallisesta tietoturvastrategiasta puhuttaessa voidaan nostaa esille yksi hyvin tärkeä seikka. Yhteiskunta yrittää tukea yhteisöjä ja yrityksiä asettaen niille samanlaiset tavoitteet tietoturvallisuuden totetuttamiselle. Tällä pyritään kohti tietoturvallisempaa yhteiskuntaa, jossa on huomioitu niin yritysten kilpailuasema kuin yksittäisenkin kansalaisen oikeudet yksityisyyden suojaan. Viime aikoina on lainsäädäntöön luotu suuri määrä uusia tietoturvaan liittyviä säädöksiä, joiden perimmäisenä tarkoituksena on tietoturvatoimenpiteiden määritteleminen erilaisissa tilanteissa. Esiin voidaan kuitenkin nostaa muutamia ongelmia, jotka saattavat aiheuttaa vaikeuksia. Esimerkiksi voidaan verrata teknisen tietoturvan toteuttamista sekä lainsäädäntöä. Tekninen tietoturva on varsin täsmällistä toteuttamista kun taas lainsäädäntö on luonteeltaan yleistä sekä tulkinnanvaraista. Ongelmia aiheuttaa myös tekniikan ja sovellusten vauhdikas kehitys, joka saattaa aiheuttaa tilanteita, joihin laissa ei ole edes varauduttu. (Laaksonen ym. 2006, 18.)

Erityistä tietoturvaan liittyvää erillislakia ei ole säädetty Suomessa. Tässä yhteydessä erillislailla tarkoitetaan sellaista lakia, jossa olisi kattavasti säädelty muun muassa yhteisöjen sekä yksilöiden tietoturvaoikeuksista ja –velvollisuuksista. Julkisuudessa on silloin tällöin nostettu esiin tällaisen erillislain tarpeellisuus, mutta vastaanotto on ollut penseää yritysten ja lainsäätäjien keskuudessa. Yhtenäisenä mielipiteenä onkin ollut se, ettei lisää lakeja haluta. Tämä on johtanut siihen, että joissakin yrityksissä on jopa mietitty erillisistä tietoturvaohjeista luopumista, koska ne voitaisiin integroida osaksi muita toimintaohjeita. Suomen laista löytyy kuitenkin yleiset reunaehdot erilaisten tietoteknisten palveluiden tuottamiselle, ylläpidolle, käyttäjille sekä molempien ryhmien oikeuksille ja velvollisuuksille. Keskeisimmät tietoteknisiä palveluita ja niiden käyttöä koskevat lait ovat rikoslaki, henkilötietolaki, sähköisen viestinnän tietosuojalaki ja laki yksityisyyden suojasta työelämässä. (Laaksonen ym. 2006, 21; Helsingin yliopiston tietotekniikkapalvelut, 2010.)

Yritykset toivovat yhä enemmän selviä ohjeita ja kannanottoja viranomaisilta liittyen siihen, mitä saa tai tulisi tehdä, jotta tietoturvaan liittyvät toimenpiteet saataisiin hoidetuksi lain

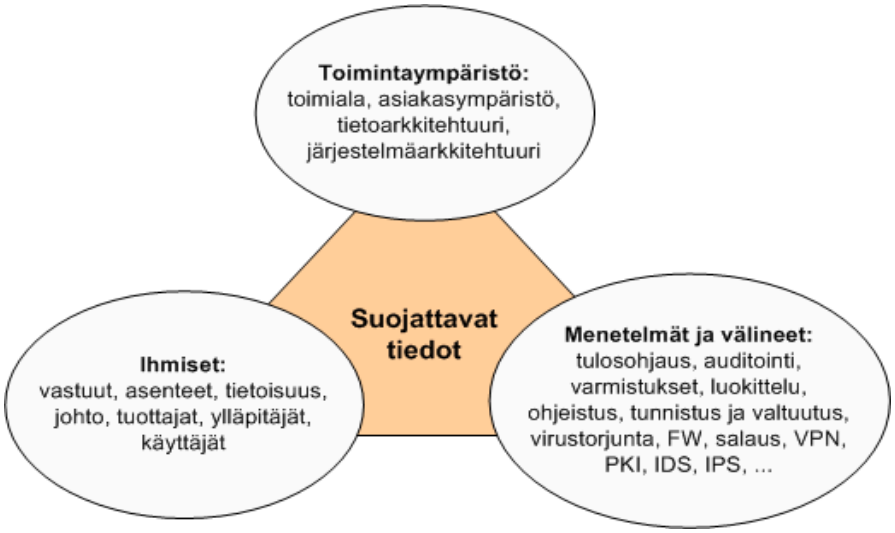
edellyttämällä tavalla jokaisen osapuolen parhaita intressejä palvellen. Ongelmia aiheuttaa kuitenkin tietoturvan käytännönläheisyys. Usein on pakko toimia ensin vahinkojen minimoimiseksi ja tarkastella lakeja vasta sen jälkeen. Tämä ei tietenkään palvele lain alkuperäistä tarkoitusta. (Laaksonen ym. 2006, 21.)

Tekniikan valtavan nopea kehittyminen on johtanut siihen, että kilpailu markkinoilla kiristyy avaten uusia tapoja käsitellä tietoa yhteisöissä ja yrityksissä. Yritysten kannalta tämä on ongelmallista, koska samanaikasesti on säädetty uusia yksilön yksityisyyden suojaa koskevia lakeja, jotka osaltaan rajaavat tietojärjestelmien tehokasta käyttöä koskevia teknisiä keinoja. Järjestelmäresurssien käytön ohjaaminen ja valvonta saattavat kärsiä tiukkojen yksityisuuden suojaa koskevien lakien takia. Yritysten kannalta nähtynä tämä on ongelmallista varsinkin tietohallinnon osalta, koska sen on huolehdittava asioiden teknisestä toteuttamisesta liiketoiminnallisten sekä lainsäädännöllisten vaatimusten mukaisesti. Nämä samat ongelmat koskevat tietysti myös yrityksen johtoa ja tietoturvaorganisaatioita, koska lopullinen vastuu on heillä. (Laaksonen ym. 2006, 21.)

3.2 Liiketoiminnallisten tarpeiden suhde tietoturvaan

Heikko ja huonosti toteutettu tietoturva ei aiheuta pelkästään taloudellisia tappioita vaan sillä on myös vaikutusta yrityksen imagoon ja liiketoimintaan. Useat yritykset ovatkin vasta viime vuosina havahtuneet tähän. Yrityksen maine sekä markkinaluottamus ovat vähintäänkin yhtä tärkeitä kuin tietojärjestelmien sisältämä tieto. (Laaksonen ym. 2006, 19; tietoturvaopas.fi.) Tietoturvallisuutta kehnosti hoitavan yrityksen kanssa on hankalaa ja kannattamatonta harjoittaa liiketoimintaa, koska tällöin kaikkien osapuolten tiedot ja tietojärjestelmät vaarantuvat oleellisesti.

Tietoturvallisuus on keskeinen osa yritysten liiketoimintaa sekä tietojärjestelmiä, koska liiketoiminta hoidetaan nykyään lähes sataprosenttisesti erilaisten tietojärjestelmien avulla. Yritysten toimintakyky sekä tehokkuus ovat melkein aina riippuvaisia tietojärjestelmistä sekä niiden tietoturvallisuudesta. Jokainen on osaltaan vastuussa tietoturvallisesta käyttäytymisestä yrityksessä. Parhaatkaan tekniset sekä fyysiset tietoturvaratkaisut eivät takaa esimerkillistä tietoturvallisuuden tasoa, koska viimekädessä tietoturvan toteutumisesta vastuussa ovat ihmiset sekä heidän toimintatapansa. (Laaksonen ym. 2006, 19.) Juurikin ihmisten asenteisiin ja toimintatapoihin vaikuttamalla voidaan nostaa yleistä tietoturvallisuuden tasoa ja parantaa tietoturvallisuuden toteutumista, koska motivoituneet ja koulutetut ihmiset toimivat tietoturvallisesti ja tällöin myös tekniset ratkaisut toimivat oikealla tavalla.



Kuva 2: Turvallisuuskolmio (Yliopistojen IT.)

Jotta yritys voisi toimia oikealla tavalla se tarvitsee ajan tasalla olevaa tietoa, jonka pitää olla oikeaa ja luotettavaa sekä oikeiden henkilöiden tai tahojen saatavilla. Yrityksen toimintaa koskevien tietojen tulee vastata liiketoiminnan asettamia vaatimuksia. Usein nämä vaatimukset kohdistetaan koskemaan myös eri sidosryhmiä kuten esimerkiksi alihankkijoita tai asiakkaita. Erilaiset liiketoimintaympäristöt muuttuvat kokoajan ja uusia tietoturvallisuutta koskevia vaatimuksia saattaa nousta esiin yllättäviltäkin tahoilta, joten liiketoimintaympäristöjen seuraaminen onkin kannattavaa myöskin tietoturvamielessä. Täytyy myös muistaa, että tietoturvallisuusosaajilta vaaditaan liiketoiminta- ja prosessiosaamista ja näitä tulee vaatia myös palveluiden tarjoajilta. (Laaksonen ym. 2006, 19-20; Karttunen 2005, 26.)

Markkinoilla vallitsevan kilpailun koveneminen voidaan nähdä haasteena tietoturvallisuuden kehittämiselle ja käyttöönotolle, koska suuri osa yritysten ajasta kuluu operatiivisten tehtävien hoitamiseen. Tämä voi aiheuttaa sen, että yrityksissä on vaikeuksia löytää riittävästi resursseja ja henkilöstöä huolehtimaan tietoturvallisuudesta. Yritysjohdon on kuitenkin tilanteesta riippumatta kyettävä osoittamaan ja varamaan riittävät resurssit, jotta tarvittavat tietoturvallisuuden vaatimukset voidaan toteuttaa. (Laaksonen ym. 2006, 20.)

3.3 Tärkeitä standardeja

Tietoturvallisuuteen liittyvät keskeiset standardit ovat nykyään ISO-standardeja. Niiden perustana on käytetty usein joitain muita kansallisia standardeja. ISO-standardit ovat levinneet laajasti sekä ne ovat myös tunnustettuja, koska ISO:n jäseninä on noin 150:n maan kansalliset standardointielimet. Merkittävimpiä standardeja ovat ISO 17799, ISO 27001, BS 7799 sekä ISF:n tietoturvallisuusstandardi. (Laaksonen ym. 2006, 85.)

Standardien merkitys korostuu muun muassa yritysten välisessä liiketoiminnassa. Jos yrityksen käytössä on jokin tietty standardi niin samanlaista tietoturvallisuuden laatutasoa saatetaan vaatia myös potentiaalisilta tai uusilta yhteistyöyrityksiltä. Näin ollen yhteistyöyritys joutuu sopimusten kautta hankkimaan saman standardin tai ainakin noudattamaan standardin edellyttämää toiminnan tasoa. (Laaksonen, ym. 2006, 85.)

ISO 17799

ISO/IEC 17799 on ehkä parhaiten tunnettu standardi heti BS 7799:n jälkeen. ISO 17799 sopii niin pienten kuin suurtenkin yritysten tarpeisiin. Se on laadittu BS 7799 –standardin osan yksi pohjalta vuonna 2003 ja uusi versio julkaistiin vuonna 2005. ISO/IEC muodostuu seuraavista termeistä: Information technology – Security Techniques – Code of practice for information security. Nimi kuvastaa hyvin sen, mistä standardissa on kyse. Kyseessä on siis tietoturvallisuuden hallinnointiin tarkoitettu standardi. Standardista löytyy yleiset periaatteet ja ohjeet, joiden mukaan tietoturvallisuuden hallinta yrityksessä voidaan aloittaa sekä täten myös ylläpitää ja hallita.ISO 17799 –standardia ei voi käyttää sertifioinnin perustana, joten näin ollen mikään yritys ei voi olla ISO 17799 –sertifoitu. ISO 17799 huomioi myöskin OECD:n vuonna 1992 laatiman ohjeistuksen koskien tietojärjestelmien ja tietoverkkojen tietoturvaperiaatteita. Vuonna 2002 ohjeistusta päivitettiin, jolloin esiteltiin käsite tietoturvakulttuuri. (Laaksonen ym. 2006, 86; International Organization for Standardization.)

ISO:n standardit on pääasiallisesti suunniteltu yksityisen sektorin käyttöön, mutta niitä voidaan soveltaa hyvin myös julkisyhteisöissä. Yleensä julkisyhteisöille on useissa maissa omat ohjeensa sekä standardinsa. Suomessa tällaisia ovat Valtionvarainministeriön VAHTI-ohjeet. Ne on tarkoitettu ohjeeksi valtionhallinnon tietoturvatoimepiteitä ja niiden kehittämistä varten. (Laaksonen ym. 2006, 86.)

BS 7799

BS 7799 kehitettiin Englannissa vuonna 1993 Department of Trade and Industryn toimesta. Vuonna 1995 tämä standardi nimettiin BS 7799:ksi. Tähän standardiin kuuluva osa 1 määritteli tietoturvallisuuden hallinnan menettelyt, joten sen perusteella laadittiin ISO 17799 – standardi. Tietoturvallisuuden hallintajärjestelmän vaatimukset, joita vastaan sertifointi on mahdollista suorittaa esitetetään osassa 2. Nykyään sertifointi suoritetaan ISO 27001 – standardia vastaan, joka korvaa BS 7799 –standardin osan 2. Nykypäivän yritysten ei kannata enää harkita tietoturvallisuuden hallintajärjestelmien kehitystä tai sertifioinnin suorittamista BS 7799 –standardin pohjalta, koska se alkaa olemaan jo vanhentunut. (Laaksonen ym. 2006, 88.)

ISO 27001/ISO 27002

ISO/IEC 27001 on julkaistu 10/2005 ja se perustuu BS 7799 –standardin osaan 2. Sitä on kuitenkin päivitetty niin, että se on enemmän yhtenevämpi ISO 17799 –standardin kanssa. Standardien numeroinnissa ISO on varannut tietoturvallisuuden hallinnalle 27000-sarjan. Tästä johtuen myös ISO 17799 nimettiin uudelleen huhtikuussa 2007, jotta se saadaan sopimaan 27000-sarjaan. ISO 27001 –standardiin on määritelty tietoturvallisuuden hallintajärjestelmän vaatimukset, joten sitä voidaan käyttää tietoturvallisuuden hallintajärjestelmien sertifioinnin perustana. ISO 17799:n uudeksi nimeksi tuli ISO/IEC 27002: 2007. Nimenmuutoksen vahvisti ISO-standardista vastaava komitea JTC 1/SC27 omalla lausunnollaan 4.4.2007. Tämän lisäksi tammikuussa 2007 vahvistettiin myös uusi ISO 27006 –sertifiointiohje. ISO 27002 –standardi käsittää tietoturvallisuuden hallinnan parhaat käytännöt, hallintatavoitteet sekä hallintatoimenpiteet. (Laaksonen ym. 2006, 88-89; DNV Oy, 2010, International Organization for Standardization & Yhteiskunnan tieto 2007.)

ISF -tietoturvastandardi

ISF tulee sanoista Information Security Forum. Se on kansainvälinen järjestö, jonka jäsenenä on noin 300 yritystä. Suomalaisia yrityksiä on mukana noin 15 ja ne ovat lähes kaikki yksityisen sektorin yrityksiä. ISF:llä on monenlaista toimintaa kuten esimerkiksi erilaiset tutkimukset, benchmarking, parhaiden käytäntöjen edistäminen ja tunnistaminen sekä vuotuiset kongressit. (Laaksonen ym. 2006, 90.)

Foorumin tuottamiin tutkimusraportteihin saa pääsyn vain liittymällä sen jäseneksi. Tärkein foorumin tuotos on ehdottomasti Standard of Good Practice for Information Security –standardi. Tämän standardin voivat ottaa käyttöönsä kaikki yritykset ja yhteisöt ja se on ladattavissa ilmaiseksi foorumin www-sivuilta. Standardi tarjoaa liiketoimintalähtöisen lähestymistavan tietoturvallisuuden kehittämiseksi. Standardin ensimmäinen versio julkaistiin jo vuonna 1996 ja sitä päivitetään joka toinen vuosi, jotta se vastaisi parhaiten yritysten erilaisia vaatimuksia alati muuttuvissa toimintaympäristöissä. (Laaksonen ym. 2006, 90.)

ISF –tietoturvastandardin tarkoituksena on ehdottaa parhaita käytäntöjä tietoturvallisuuden eri osa-alueille. Täten se myös vastaa periaatteiltaan ISO 17799 –standardia ja yhtenä ydinajatuksena on se, että kaikki sen tarjoamat suositukset tulisi ottaa käyttöön ellei joidenkin poisjättämiselle ole erityistä liiketoiminnallista perustetta tai syytä. Tässä standardissa on myös mietitty erilaisia teknisiä toteutuskeinoja kuten esimerkiksi mac-suodatuksen vaikutuksia langattomassa verkossa tai mitä protokollia ei ole suotavaa käyttää. Täten se siis eroaa hieman ISO 17799 –standardista. Sertifiointia ei voi hakea ISF:n standardin

perusteella. Sen suosituksia noudattamalla voi kuitenkin verrattain helposti luoda tietoturvallisuuden hallintajärjestelmän, joka täyttää ISO 27001 –standardin vaatimukset. (Laaksonen ym. 2006, 90-91; Kallio 2003, 8.)

4 Tietoturvallisuuden johtamis- ja hallintajärjestelmä

Yrityksen johtamisen yksi tärkeimmistä vastuualueista on tietoturvallisuuden hallinta. Kappaleessa viisi esitellyt ISO-standardit luovat kansaivälisellä tasolla yhteisen perustan tietoturvallisuuden lähestymiselle ja kehittämiselle. Yritysten yleisten johtamismallien avulla myös tietoturvallisuutta voidaan johtaa tehokkaasti yhdessä normaalin johtamistoimen rinnalla. Tietoturvallisuudesta sekä sen käytännön toteuttamisesta on saatavilla paljon tuki- ja ohjemateriaalia. Tärkeimpinä viitejulkaisuina pidetään ISO-standardeja, jotka ovat myös kansainvälisesti arvostettuja. (Anttila & Kajava 2006, 43.)

Tietoturvallisuuden johtamisen kannalta merkittävimmät ISO-standardit ovat ISO/IEC 27001:2005, ISO/IEC 17799:2005, ISO/IEC 27002:2007 sekä ISO/IEC 11770-1:1996. Kyseessä olevien standardien tarkoituksena on painottaa sitä, että tietoturvallisuuden hallinnan toteuttamisessa täytyy huomioida yrityksen toiminnalliset sekä strategiset tarpeet sekä niissä tapahtuvat muutokset. (Anttila & Kajava 2006, 43 & Yhteiskunnan tieto 2009.)

Tietoturvallisuuden johtamisjärjestelmä pitää sisällään sellaiset johtamiseen liittyvät menettelyt, joiden tarkoituksena on ohjata sekä valvoa tietoturvallisuuden toteuttamista. Johtamisjärjestelmän osia ovat esimerkiksi:

- tietoturvallisuusstrategia
- tietoturvallisuuspolitiikka ja toimintaperiaatteet
- riskianalyysi
- tietoturvallisuussuunnitelma ja –ohjeet
- jatkuvuus- ja toipumissuunnitelma
- tietojenkäsittelyn poikkeusolojen valmiussuunnitelma
- tietoturvallisuuden tulosohjaus
- tietoturvallisuuden toteutustapa, organisaatio ja vastuut
- vuosisuunnitelma, budjetit ja raportointi

(VAHTI: Tietoturvallisuuden hallintajärjestelmän arviointisuositus 2003, 13-14.)

4.1 Tietoturvallisuuden hallintajärjestelmä

Tietoturvallisuuden hallintajärjestelmä puolestaan on osa johtamisjärjestelmää, joka pohjaa riskien analysointiin ja niiden hallintaan. Hallintajärjestelmän avulla tietoturvallisuutta

voidaan suunnitella, toteuttaa, noudattaa, seurata, arvioida, ylläpitää ja kehittää. (VAHTI: (VAHTI: Tietoturvallisuuden hallintajärjestelmän arviointisuositus 2003, 15.)

Tietoturvallisuuden hallintajärjestelmän osatekijät ja periaatteet määritetään ISO 27000 –standardisarjassa. Hallintajärjestelmä koostuu alla olevista osatekijöistä:

- tietoturva- ja riskienhallintapolitiikkojen sekä tietoturvallisuusorganisoinnin määrittely, joiden lähtökohtana on toiminnan strategiset tavoitteet
- tietoturvallisuusarkkitehtuuri sekä tietoturvallisuustavoitteet
- edellisten osatekijöiden tuominen käytäntöön prosessi-integraation sekä tietoturvallisuusosaamisen kautta
- tietoturvallisuuteen liittyvät arviointiprosessit ja niihin liittyvä tiedon hallinta ja raportointi

(Yhteiskunnan tieto 2009, 1.)

4.2 ISO 27000 –standardin mukaiset arvokkaat kohteet

Tietoturvallisuutta kohdennetaan arvokkaiden kohteiden perusteella, jotka määrittelevät tietoturvallisuuden hallintajärjestelmää koskevan sovellusalueen. Arvokkaat kohteet inventoidaan. Tämän lisäksi niiden arvo organisaation ja tietoyhteiskuntapalvelun kannalta määritellään. (Yhteiskunnan tieto 2009, 1.)

ISO 27000-standardin luokittelemat arvokkaat kohteet:

- Tiedot, tietämysaineistot, tietoaineistot
- Tietoliikenneverkkojen ja –palveluiden, ohjelmistojen sekä laitteistojen muodostama käyttöympäristö
- Fyysinen ympäristö
- Inhimilliset resurssit
- Ulkoisten palveluiden käyttö ja hankinnat

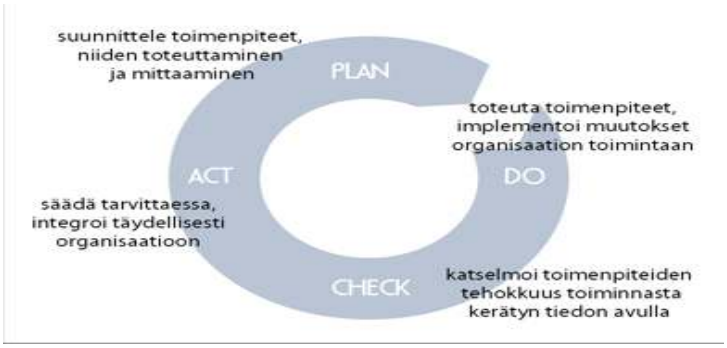
(Yhteiskunnan tieto 2009, 1.)

Kuva 3: ISO 27000:n mukaiset arvokkaat kohteet (Yhteiskunnan tieto 2009.)

Tärkeimpinä turvaamisen kohteina pidetään tietoaineistoja (information assets). Jos tietoaineistot liittyvät henkilöön ja toimintaan, ne sisältävät myös hiljaisen tiedon ja niiden perusteella määriteltävät tietokohteet (knowledge assets). Tietoturvallisuus sulautetaan sellaiseen ympäristöön, jonka muodostavat käyttöympäristö sekä fyysinen ympäristö yhdessä. Tällaisessa ympäristössä tietoa tuotetaan, siirretään ja säilytetään. (Yhteiskunnan tieto 2009, 1-2.)

4.3 PDCA-malli

Kappaleessa kahdeksan esiteltyjen standardien pohjalta organisaation tietoturvallisuuden käytännön toteutuksen johtamismalliksi suositellaan PDCA-mallia ja sen soveltamista osana yleistä johtamisjärjestelmää. PDCA-malli on tullut osaksi tietoturvallisuuden hallintastandardeja ISO 9000 –sarjan (laadunhallinta) standardien kautta. PDCA-malli on yksi laajimmista ja pisimpään käytössä olleista johtamismalleista. Malli määrittelee toiminnan kehittämisen, ohjauksen ja suunnittelun. (Anttila & Kajava 2006, 43.)



Kuva 4: PDCA-malli (Veini 2008.)

ISO 27001 –standardi suosittelee Plan-Do-Check-Act prosessiin perustuvaa lähestymistapaa tietoturvallisuuden hallintajärjestelmässä. (Tipton & Krause 2008, 20.)

PDCA-mallin kaikkia mahdollisuuksia ei ole täysipainoisesti hyödynnetty erilaisissa tietoturvallisuuden hallintaan tarkoitetuissa standardeissa. Joissakin tapauksissa PDCA-mallin piirteet ja käyttömahdollisuudet on esitetty harhaanjohtavasti eri tavoilla. Viime vuosikymmenten aikana PDCA-mallin käyttötarkoituksia ja toimintoja varten on kehitetty erilaisia johtamistyökaluja. Kuitenkaan niiden yhteyttä tietoturvallisuuden lähteisiin ei nähdä. Nämä johtamisen työkalut ovat kaikesta huolimatta laajassa käytössä maailmanlaajuisesti erilaisissa organisaatioissa toisten johtamisen osa-alueiden kehittämisessä. Joten tällä perusteella ei ole mitään syytä olettaa, etteikö niitä voisi käyttää myöskin tietoturvallisuuden hallinnassa. (Anttila & Kajava, 2006, 45-46.)

4.4 Tietoturvallisuuden hallinnan kehittäminen ja organisaation oppiminen

Koko organisaation kattava tietoturvallisuuden kehittäminen tarkoittaa sen kykyä oppia toimimaan paremmin tietoturvallisuuden tarpeiden ja odotusten toteuttamiseksi. Uutta luova innovatiivinen kehittäminen nähdään myös tärkeänä osana organisaation oppimisprosessia. Tietoturvallisuuden kaikkien osa-alueiden ja toimintatapojen kehittäminen ja tehokas toteuttaminen vaatii organisaatiolta ponnistuksia. Tietoturvallisuuteen liittyvien periaatteiden on oltava selkeitä ja tunnettuja ja niiden pitää vielä lisäksi soveltua liiketoiminnan asettamien vaatimusten mukaan. (Anttila, Kajava, Savola & Röning 2009, 22.)

Kilpailutilanteessa organisaation ainoana tavoitteena on liiketoiminnan suorituskyvyn laadukkuus ja ylivertaisuus, koska tällä tavoin on mahdollista ylläpitää kestävää kilpailukykyä. Tavoitteiden täytyy kohdistua organisaation kaikkiin suorituskykyominaisuuksiin, jolloin myös tietoturvallisuuden hallinta tulee katettua. Tietoturvallisuuden laadukkuus on suoraan sidoksissa siihen, millä tasolla organisaation kaikkien sidosryhmien tarpeet ja odotukset täytetään. Ylivertaisuus ei toteudu jos pelkästään täytetään tietyt minimivaatimukset tai ollaan samassa tilanteessa kuin muutkin organisaatiot eli täytetään keskinkertaiset vaatimukset. (Anttila ym. 2009, 22)

Suorituskyvyn hallintaan ja sen jatkuvaan kehittämiseen kuuluu jokaisessa organisaatiossa sen oma yrityskulttuuri ja tarpeiden mukaan syntynyt organisaatiokohtainen toteutusratkaisu. Kokonaisvaltainen toteuttaminen ja siihen liittyvän jatkuvan kehittämisen pohjana on muun muassa tietoisuuden ja herkkyyden syntyminen uusia asioita kohtaan, asenteiden ja uskomusten muuttaminen sekä tietojen ja taitojen kehittäminen. Kehittyminen on yleensä jatkuvaa ja pitkäaikaista, mutta harvemmin suoraviivaista. (Anttila ym. 2009, 22-23.)

4.5 Hallintajärjestelmän hyväksyttäminen

Hallintajärjestelmä hyväksytetään organisaation ylimmällä johdolla kun sen toimintaperiaatteet ja ja sisältö on asianmukaisesti dokumentoitu ja kuvattu. Vastuukysymykset ja oikeudet on määritettävä selkeästi ja ehdottomasti sekä nimettävä tietoturvallisuudesta vastaavat henkilöt. Myöskin tietoturvallisuudesta vastaavien henkilöiden toimivalta tulee rajata asianmukaisesti ja selkeästi. Tärkeää on myös, että tietoturvallisuuteen liittyvät oikeudet määritellään ja rajataan yksiselitteisesti rooleittain. Usein riittämätön oikeuksien määrittely voi johtaa vakaviin erimielisyyksiin tietohallinnon henkilöiden ja heidän yläpuolellaan organisaatiohierarkiassa olevien henkilöiden välille. Tällaisten tilanteiden välttämiseksi tietoturvallisuudesta vastaavilla henkilöillä tulee olla oikeus puuttua myös esimiesasemassa olevien henkilöiden toimintaan jos se nämä ovat vaaraksi organisaation tietoturvallisuudelle. Ristiriitatilanteissa organisaation johdon on ilmaistava tukensa tietoturvallisuudesta vastaaville henkilöille. (Hakala, Vainio & Vuorinen 2006, 109.)

Hallintajärjestelmän laajuus olisi hyvä kuvata dokumentissa, joka tulisi laatia ennen hyväksynnän hankkimista. Dokumentista tulee käydä ilmi myös hallintajärjestelmän soveltuvuus suhteessa organisaation toimintaympäristöön sekä noudatettuun standardiin (Statement of Applicability). Siinä kuvataan käyttöönotettujen kontrollien lisäksi niiden valintaperusteet, toteutetut kontrollit sekä ne tavoitteet ja kontrollit, jotka on tarkoituksellisesti jätetty hallintajärjestelmän ulkopuolelle. Poistetut osa-alueet täytyy aina perustella huolellisesti. (Hakala ym. 2006, 109.)

5 Tietoturvapolitiikat ja niiden merkitys

Mäkisen (2003, 2-3) mukaan tietoturvallisuutta toteutetaan tietoturvapolitiikkojen avulla, jolloin ne voidaan kohdistaa tietoturva eri osa-alueille. Yrityksen johto valvoo ja ohjaa tietoturvan toteutumista juurikin tietoturvapolitiikkojen avulla. Niiden avulla myös henkilökunta saadan tietoiseksi tiedon suojaamisvaatimuksista sekä voidaan määritellä ne käytännöt, joiden avulla nämä vaatimukset voidaan täyttää.

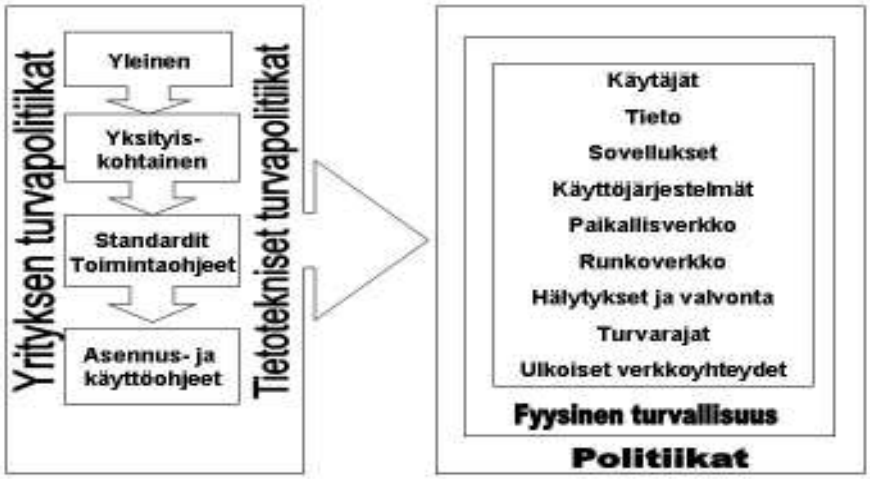
Tietoturvapolitiikka on siis luonteeltaan pysyvä tahtotila, jota tarpeen vaatiessa päivitetään. Sitä tulisi tarkastella säännöllisesti, erityisesti sen ajantasaisuutta. Jos muutoksille ilmenee tarvetta, on yritysjohdon laadittava päivitetty politiikka. Tietoturvapolitiikka on aina yritysjohdon kannanotto, jolla se osoittaa sitoutumisensa sekä tukensa yrityksen

tieoturvallisuuden kehittämiselle. Se on myös perusta yrityksen tietoturvaohjeistukselle sekä tietoturvakoulutukselle. (Laaksonen ym. 2006, 146.)

Laaksosen ym. (2006, 147) mukaan tietoturvapolitiikkaan sisältyvät seuraavat asiat:

- Tietoturvallisuuden tavoitteet sekä niihin liittyvät toimet
- Tietoturvallisuuden rooli ja vastuut
- Tietoturvallisuuskoulutus
- Tietojenkäsittelyn suojaaminen
- Yleiset linjaukset
- Seuraukset tietoturvapolitiikan laiminlyönnistä

Tietoturvapolitiikat muodostavat myös hierarkisen rakenteen (kuva 3). Ylimpänä tässä hierarkiassa on johdon laatima yrityksen tietoturvapolitiikka. Sen avulla luodaan alempien tasojen politiikat, joiden tarkoituksena on käytännön toimintaohjeiden sekä järjestelmien turvamääritykset. Tällä tavoin eri osa-aluiden turvamääritykset ulottuvat koko organisaatioon. (Mäkinen 2003, 3.)



Kuva 5: Turvapolitiikan hierarkia (Mäkinen 2003.)

Hierarkiasta selviää, että ylempien tasojen politiikat ovat aina hallinnollisia. Hallinnolliset politiikat muuttuvat alaspäin mentäessä teknisiksi politiikoiksi, toimintaohjeiksi ja asennusmäärittelyiksi. Tekniset määritykset sekä käyttäjien ohjeet tulee aina johtaa tietoturvapolitiikoista. (Mäkinen 2003, 3.)

5.1 Vaatimukset tietoturvapolitiikoille

Tietoturvapoliitiikkojen on oltava tarpeeksi kattavia ja moniulotteisia, jotta tietoturvallisuus toteutuu yrityksen jokaisella osa-alueella. Tietojen saatavuus, eheys ja käytettävyys on turvattava politiikkojen avulla kaikilla tietojenkäsittelyn osa-alueilla sekä normaali- että poikeusolosuhteissa. Vastuujako on määritettävä selvästi eri osapuolten kesken, joita yleensä ovat käyttäjät, ylläpitäjät sekä yritysjohto. (Mäkinen 2003, 5.)

Tietoturvapolitiikkoja suunniteltaessa on ensiarvoisen tärkeää ottaa huomioon niiden sitoutuminen liiketoimintaprosesseihin. Tarpeettomia rajoituksia tulisi välttää, jotta politiikoista tulisi selkeitä ja ymmärrettäviä. Tällä tavalla voidaan varmistua myös siitä, että käyttäjien helppo ymmärtää ja noudattaa politiikkoja. Jos politiikoista luodaan liian tiukkoja on vaarana se, että ne haittaavat yrityksen toimintaa. Tämä puolestaan saattaa johtaa sääntöjen noudattamatta jättämiseen tai niiden kiertämiseen. (Mäkinen 2003, 5.)

Mäkinen (2003, 6) esittää myös, että tietoturvapolitiikkojen tulee olla ajantasaisia sekä niitä on arvioitava jatkuvasti uskottavuuden takaamiseksi. Tärkeää on myös politiikoista johdettujen turva-asetusten määrittely. Riittämättömät asetukset voivat johtaa verkkojen luvattomaan käyttöön kun taas liian vahvat asetukset voivat haitata tietojärjestelmien normaalia käyttöä.

5.2 Tietoturvapolitiikkojen kerroksellisuus ja käyttöönotto

Yrityksen tietoturvapolitiikassa kuvataan yleisluontoisesti, mitä halutaan suojata. Alempien tasojen politiikoissa määritellään yksityiskohtaisesemmin tiettyjen osa-alueiden tietoturvatoimenpiteet. Tällaisia osa-alueita ovat yleensä: tietojärjestelmät, palvelinalustat, tietoliikenneverkot, langattomat verkot, kannettavat tietokoneet, työasemat sekä etäkäyttö. On myös normaalia, että suojaustavat määritellään, joita ovat muun muassa salaus, tunnistus, pääsynvalvonta. (Mäkinen 2003, 8.)

Mäkisen (2003, 8) mukaan tietoturvapolitiikat on rakennettava niin, että riittävä tietoturvallisuuden taso voidaan saavuttaa sellaisten pakollisten politiikkojen avulla, joiden tekninen toteuttaminen sekä valvonta on mahdollista. Kokonaisvaltaista tietoturvaa ei voida toteuttaa pelkästään teknisillä keinoilla. Hallinnolliset toimintaohjeet ovat hyvä keino tietoturvan tehostamiseen. Toimivat tietoturvapolitiikat auttavat henkilöstöä toimimaan oikein ja tietoturvallisesti.

Tietoturvapolitiikkojen käyttöönoton yksi tärkeimmistä vaiheista on niistä tiedottaminen. Ilman tiedottamista tietoturvapolitiikoista ei ole paljoakaan hyötyä, koska tällöin henkilöstö

ei ole niistä tietoinen eikä näin ollen osaa niitä noudattaa. Tällöin voidaan valita alue, jolla on selkeät rajat ja se tukee useita muita palveluita, esimerkiksi keskitetyt IT-toiminnot. (Mäkinen 2003, 9; Department for Business, Enterprise & Regulatory Reform 2009, 8.)

Tietoturvallisuudessa on kyse luottamuksesta sekä siitä, kehen luotetaan ja milloin. Ihmiset tekevät virheitä, vaikka yrittävät toimia oikeilla tavoilla. Myös ohjelmistoissa voi olla tietoturva-aukkoja. Tietoturvapolitiikkojen tehtävänä onkin estää tahallisesta tai vahingollisesta toiminnasta aiheutuvia haittoja. (Mäkinen 2003, 9.)

5.3 Tietoturvapolitiikkojen markkinoinnin ja koulutuksen merkitys

Tietoturvapolitiikkojen hyödyt saadaan tuotua esille vain tehokkaalla markkinoinnilla. Henkilöstölle on tehtävä selväksi, että tietoturvapolitiikoilla ei ole tarkoitus haitata tai hankaloittaa työtehtävien suorittamista, vaan niiden avulla varmistetaan liiketoimintojen mukainen avoimuus. Erityisen tärkeää tiedottamisen kannalta on mainita se, että tietoturvapolitiikkojen avulla yrityksen johto sitoutuu turvaamaan yrityksen liiketoiminnan. Tietoturvan lopullinen toteutuminen ja sen taso on suoraan sidoksissa työntekijöiden ja johdon asenteisiin ja toimintatapoihin. Tietoturvan täytyy olla osa yrityksen sisäistä kulttuuria sekä jokapäiväisiä toimintoja. (Mäkinen 2003, 10.)

Työntekijöiden kouluttaminen on kriittinen vaihe tietoturvapolitiikkojen käyttöönotossa. Ihmiset voivat jättää noudattamatta sellaisia sääntöjä, joita pitävät tarpeettomina. Tietoturvapolitiikkojen merkitystä voidaan korostaa tietoturvatietoisuuden lisäämisellä, jolloin työntekijöiden on helpompi ymmärtää tietoturvapolitiikkojen merkitys jokapäiväisessä työssä. Kouluttamisen yksi pääasiallisista tarkoituksista on saada työntekijät ymmärtämään ne syyt, minkä takia tietoturvapolitiikat ja toimintaohjeet otetaan käyttöön. Tällä tavoin niitä myös noudatetaan paremmin verrattuna pelkkien sääntöjen opettamiseen. (Mäkinen 2003, 10.)

Kouluttaminen tulee tehdä kaikentasoisille käyttäjille, joita ovat peruskäyttäjät, edistyneemmät käyttäjät sekä tehokäyttäjät. Peruskäyttäjät toimivat yleensä annettujen ohjeiden mukaan, joten niiden tulee olla asianmukaisia ja helposti ymmärrettäviä. Edistyneempien käyttäjien kohdalla voidaan puhua työskentelyn optimoimisesta, jolloin tietoturvakoulutuksen merkitystä ei voi liikaa korostaa. Puutteellinen koulutus voi saada aikaan sen, että työn tehostaminen tai optimointi tehdään keinoin, jotka eivät ole tietoturvan mukaisia. Tehokäyttäjistä puhuttaessa pitää muistaa, että usein he pyrkivät ratkomaan aktiivisesti tietojenkäsittely-ympäristössään olevia ongelmia. Ongelmien kokonaisuuksia ei aina hahmoteta eikä myöskään tietojenkäsittely-ympäristön vaatimuksia. Koulutuksessa

täytyy siis kiinnittää erityistä huomiota ongelmien ratkaisumalleihin, jotka noudattavat yrityksen tietoturvavaatimuksia. (Mäkinen 2003, 10.)

Koko yrityksen kattava tietoturvallisuuden kehittäminen koskee myös sen johtoa. Yritysjohtoa on koulutettava samanlailla kuin muitakin työntekijöitä ja heitä on tiedotettava ajankohtaisista tietoturvakysymyksistä. Tietojärjestelmien tietoturvallisuudesta puhuttaessa täytyy niistä vastaavien henkilöiden tietojen ja taitojen olla ajantasalla.
(VAHTI: Tietoturvapoikkeamatilanteiden hallinta 2005, 19.)

Koulutuksen avulla jokainen oppii oikeat toimintatavat erilaisissa tilanteissa. Koulutuksen hyviä puolia on myös se, että kaikille tietotekniikan kanssa tekemissä oleville henkilöille muodostuu selvä kuva hyväksyttävästä toiminnasta. Tiedottaminen ja koulutus yhdessä kumoavat mahdollisuuden käyttää tietämättömyyttä virheiden selittämiseksi. Asiakkaille sekä muille yhteistyökumppaneille on hyvä kertoa yrityksen tietoturvapolitiikasta sekä standardeista. (Mäkinen 2003, 10-11.)

5.4 Tietoturvapolitiikkojen valvonta sekä tarkkailu

Tietoturvapolitiikkojen oikeanlaista toteutumista suoritetaan tarkkailun ja valvonnan avulla. Tarkkailua suoritetaan jatkuvasti, koska se on osa tietoturvaa. Tarkkailun kohteina ovat yleensä haitta- ja virusohjelmien torjunta, palomuurien asetukset sekä verkon hallintatyökalut. Tarkkailun tuloksina saatuja tietoja voidaan käyttää vahingoista toipumiseen. Valvonnalla tarkoitetaan satunnaisia, mutta säännöllisiä tarkastuksia, joiden tarkoituksena on varmistaa se, että tietoturvapolitiikat ovat asianmukaisia ja noudatettavia. Yleensä tietoturvapolitiikat voidaan pakottaa käytäntöön erilaisin teknisin keinoin. Jos tällainen menettely ei ole mahdollista, voidaan tietoturvapolitiikkojen noudattamista tehostaa sanktiomäärittelyin. (Mäkinen 2003, 11.)

5.5 Peruspolitiikat yrityksessä

Yrityksen koko henkilöstö on viime kädessä vastuussa tietoturvan toteutumisesta ja toteuttamisesta. Tietoturvapolitiikkojen perusperiaatteina on kertoa peruskäyttäjille, ylläpitäjille sekä yritysjohdolle jokaisen vastuut ja velvollisuudet yrityksen tiedon sekä teknologian suojaamiseen liittyen. Tämän lisäksi ne määrittelevät keinot, joiden avulla vaatimukset voidaan toteuttaa. Yleisesti tietoturvapolitiikat voidaan jaotella käyttäjä-, ylläpitäjä- ja infrastruktuuripolitiikkoihin. Tärkeimpinä yksittäisinä politiikkoina pidetään yleisesti tietotekniikan käyttöpolitiikkaa, etäkäyttöpolitiikkaa, tiedon turvaamispolitiikkaa sekä palomuuripolitiikkaa. Mainitsemisen arvoisia politiikkoja ovat myös ylläpitäjien käyttöpolitiikka ja tietojärjestelmien ylläpitopolitiikka. (Mäkinen 2003, 13.)

Tietotekniikan käyttöpolitiikka

Tietotekniikan käyttöpolitiikkaa voidaan pitää yhtenä yrityksen tärkeimmistä politiikoista, koska se ulottuu koskemaan koko henkilöstöä. Tämä politiikka määrittelee tavat ja keinot, joilla tietotekniikka saa ja ei saa käyttää. Käyttöpolitiikassa on määritelty ohjeistukset ohjelmistoille, laitteille, tietojärjestelmille sekä tietoliikentelle. Koska käyttöpolitiikka kuvastaa käyttäjän suhdetta tietotekniikkaan, on siinä kerrottava määrättyjä asioita. Tällaisia asioita ovat esimerkiksi yrityksen tietojen sekä tietoresurssien käsittelytavat, erilaisten järjestelmien käyttäjätunnusten ja salasanojen käyttötavat sekä sähköpostin ja internet-yhteyksien käyttötavat. Tavallisesti käyttöpolitiikkaan voidaan määritellä myös, kuinka suhtaudutaan esimerkiksi yrityksen tietojärjestelmiä koskeviin ulkopuolisiin kyselyihin. Käyttöpolitiikka tulee luoda niin, että se on lukijaystävällinen sekä selkeä ja käytettävät termit ovat ymmärrettäviä. (Mäkinen 2003, 13.)

Käyttöpolitiikassa täytyy kertoa, miten henkilöstön tietotekniikan käyttöä valvotaan, esimerkiksi sähköpostin valvonnan tai internet-käytön lokitietojen keräämisen kannalta. Lisäksi käyttöpolitiikasta on selvittävä, millä tavoin ja ketkä kerättyä tietoa käsittelevät. (Mäkinen 2003, 13.)

Etäkäyttöpolitiikka on olennainen on tietotekniikan käyttöpolitiikkaa. Etäkäyttöpolitiikan tarkoituksena on määrittää, ketkä saavat käyttää etäyhteyksiä päästäkseen yrityksen tietojärjestelmiin. Tämä politiikka määrittää myös etäyhteyksien toteuttamistavat sekä suojaamisen. Etäkäytön ohella etäkäyttöpolitiikkaan liittyy muitakin politiikkoja, joita ovat esimerkiksi: salauspolitiikka, henkilökohtaisten erillisverkkojen politiikka ja langattomien verkkojen politiikka. (Mäkinen 2003, 13.)

Ylläpitäjien käyttöpolitiikat ja tietojärjestelmien ylläpitopolitiikat

Ylläpitäjien toiminnan täytyy perustua voimassa oleviin tietoturvapolitiikkoihin sekä turvallisiin menetelmiin. Tavallisesti ylläpitäjillä täytyy myös olla hyväksytty tietotekniikan käytön sekä tietoturvallisen ylläpidon politiikka, johon on määritetty ylläpitäjien oikeudet ja velvollisuudet. Ylläpitäjien käyttöoikeudet erilaisiin tietojärjestelmiin määritetään yleensä pienimmän valtuutuksen periaatteen mukaisesti työturvallisuussyistä johtuen. Ylläpitäjiltä vaaditaan myös korkeaa tietoturvaosaamista, koska heillä on työtehtäviensä puolesta lähes rajoittamaton pääsy yrityksessä olevaan tietoon. (Mäkinen 2003, 14.)

Tietojärjestelmien ylläpitopolitiikoilla voidaan estää tai vähentää hyökkäyksiä, jotka kohdistuvat joko itse tietojärjestelmiin tai yrittävät hyödyntää niissä olevia haavoittuvuuksia.

Ylläpitopolitiikat ja toimintasuunnitelmat sisältävät yleensä seuraavanlaisia asioita: tarpeettomien palveluiden poisto palvelimilta ja työasemilta, ylläpitotunnusten käyttäminen vain ylläpidollisissa tehtävissä, vakiotunnusten poistaminen tietojärjestelmistä, virustorjunnan ylläpito sekä tietoturva-aukkojen ja päivitysten säännöllinen seuranta. (Mäkinen 2003, 14.)

Tiedon turvaamisen politiikka

Tiedon turvaamisen politiikassa määritellään keinot, joilla tietoa tulee käsitellä, säilyttää ja siirtää. Tämän politiikan pääasiallisena tarkoituksena on varmistaa tiedon pysyminen muuttumattona ja paljastumattomana tarkoituksenmukaisin suojausmenettelyin. Esimerkkejä tiedon turvaamisen politiikoista ovat tunnistamiseen sekä järjestelmien käytön valvontaan liittyvät politiikat. Tiettyjen henkilöiden pääsy vain heille tarkoitettuun tietoon oikealla tavalla varmistetaan käyttöoikeus- ja tunnistuspolitiikkojen avulla. Pienimmän valtuutuksen -politiikka varmistaa sen, että jokaisella on vain työtehtäviensä vaatimat oikeudet käytössään.

Ajat, jolloin tietojärjestelmien tulee olla käytettävissä määritellään käytettävyysvaatimuksissa. Lokitietojen seuraamiseen ja keräämiseen liittyvät politiikat kuuluvat yhtenä osana tiedon turvaamisen politiikkaan. (Mäkinen 2003, 14.)

Palomuuripolitiikka

Palomuuripolitiikka määrittää palomuurien sekä muiden vastaavanlaisten laitteistojen- ja ohjelmistojen vastuut, ylläpidolliset prosessit sekä muutoksenhallinnan vaatimat toimenpiteet. Tavallisesti palomuuripolitiikassa selvitetään myös se, kenellä on oikeus saada tietoja muun muassa asetuksista sekä miten tällaisia tietoja säilytetään. Yleisesti kaikki tuleva ja lähtevä liikenne, joka ei ole nimenomaisesti sallittu yrityksen palomuuripolitiikassa, tulisi estää, koska yritys ei sitä tarvitse. Tällainen käytäntö vähentää verkkohyökkäyksen riskiä ja alentaa verkossa tapahtuvan liikenteen määrää. (Mäkinen 2003, 14; Scarfone, Hoffman 2009, 1.)

6 Tietoturvaohjeet yrityksessä

Tietoturvaohjeet perustuvat selkeään ja todelliseen kuvaa siitä, mitä varten niitä laaditaan. Tietoturvaohjelma puolestaan toteutetaan organisaation johdon, tietoturvaorganisaation sekä muiden relevanttien tahojen pohdiskelujen sekä riskikartoituksessa ilmenneiden havaintojen perusteella. Tietoturvaohjelmaan sisältyy ne periaatteet, joihin tietoturvallisuuteen sitoutuvat käytännöt perustuvat. Ohjelman ei tarvitse välttämättä olla mittava, mutta siitä on käytävä ilmi miksi se on tehty. Tietoturvaohjelmasta tulee käydä ilmi ne toimenpiteet, joilla

tietoturvallisuutta parannetaan sekä se miten nämä toimenpiteet toteutetaan. (Laaksonen ym. 2006, 146.)

Tietoturvallisuusohjelman sisältämät ohjeet tähtäävät siihen, että ongelmien syntyminen pyritään estämään. Ohjeita tarvitaan muun muassa internetin ja sähköpostin käyttöön, tietojen käsittelyyn, vierailujen järjestämiseen, laitteiden ja järjestelmien käyttöön sekä toiminnan kuvaukseen väärinkäytöstilanteissa. Ohjeet täytyy laatia myös poikkeus- ja ongelmatilanteiden varalle. (Laaksonen ym. 2006, 146.)

Tietoturvaohjeistuksen laatimisen tulisi tapahtua aina yhdessä teknisen tietoturvan rakentamisen kanssa, koska tekninen tietoturva ei yksinään voi poistaa ongelmia. Myös teknisten välineiden ominaisuuksia tukevia ohjeita tarvitaan. Ristiriitaisuuksia erilaisten ohjeiden välillä tulee välttää, jotta niiden määrien vähentäminen ja integrointi muodostaisivat toiminnan ja tulosten kannalta järkevän toimintatavan. Ohjeiden käytäntöön viemisessä selkeästi määriteltyjen vastuualueiden merkitys korostuu, koska jokaisen on tiedettävä, mistä asioista kukin huolehtii. (Laaksonen ym. 2006, 146.)

6.1 Tietoturvatietoisuus ja kouluttaminen

Jotta organisaatio voisi tehokkaasti toteuttaa tietoturvallisuutta sen täytyy luoda turvakulttuuri ja lisätä yleista tietoturvatietoisuutta. Koko henkilökunta täytyy vakuuttaa siitä, että tietoturvallisuus on välttämätön edellytys ja väline organisaation menestymiselle. Henkilöstöä täytyy myös informoida siitä, mitä heiltä odotetaan tietoturvallisuuden osalta sekä miten toimia tietoturvallisuus-kriittisissä tilanteissa. Yleensä tämä vaatii pitkäaikaista muutosta henkilökunnan käyttäytymisessä, joka voidaan saavuttaa vain asianmukaisella ja jatkuvalla prosessilla. Kertaluontoiset tai ”herättävät” kurssit eivät riitä. (IT-Grundschutz Manual 2005, 86.)

Tietoinen ja koulutettu henkilökunta on ehdoton edellytys organisaatiolle, jotta se voi saavuttaa asetetut tavoitteet. Lisäksi koulutuksilla ja kursseilla voidaan varmistaa, että henkilökunta voi arvioida toimintansa vaikutuksia ja seuraksia niin yksityis- kuin ammattiympäristössäkin. Tietoturvallisuuskoulutuksen avulla henkilökunta saavuttaa vaadittavan tietoturvallisuuden kompetenssin, jota he tarvitsevat työtehtäviensä suorittamiseen. On myös varmistettava, että koko henkilökunta on tietoinen tarvittavista menettelytavoista ja henkilöistä, joiden puoleen heidän tulee kääntyä tietoturvallisuusasioissa. (IT-Grundschutz Manual 2005, 86.)

6.2 Tietoturvakäyttäytymiseen vaikuttavat tekijät

Ihmisten käyttäytymistä koskevia tieteellisiä malleja on useita ja näitä malleja on myös sovellettu tietoturvallisuuskäyttäytymisen osa-alueella. Jotta tietojenkäsittelyä ja tietoturvariskejä voidaan hallita, vaatii se organisaation luonteen ja kulttuurin ymmärtämistä sekä visiota erilaisten toimintamallien vaikutuksista henkilöstön käyttäytymiseen. Tarvittava ymmärrys muodostuu kahdesta osasta; organisaation toimintatapojen ymmärtämisestä ja sisäistämisestä sekä siitä, miten toimintatapoja halutaan noudattaa. (Laaksonen ym. 2006, 248.)

Organisaation näkökulmasta henkilöstön tietoturvakäyttäytymiseen vaikuttaa kolme asiaa; tiedon lähteet (yrityksen arvot, tietoturvapolitiikka, toimintaohjeet, koulutus), vanhempien kollegojen näyttämä esimerkki sekä käyttäjän ”maalaisjärki” ja päätöksentekotaidot epätavallisissa tilanteissa. Tietoturvapolitiikka ja –ohjeet muodostavat selkeän perustan henkilöstön toimintatavoille. Nämä ohjeet luovat turvallisuuteen tähtäävän käyttäytymis-mallin, joka on organisaation hyväksymä. Lisäksi, käyttäytymismallin toimivuuteen vaikuttaa ohjeiden kattavuus, selkeys ja yhdenmukaisuus. Erilaiset normaali- sekä poikkeustilanteet on aina pyrittävä hoitamaan organisaation hyväksymien käytäntöjen mukaisesti. Turvallisuuden kannalta ajateltuna rutiininomaiseen toimintaan vaikuttavat johtajien sekä muun henkilöstön esimerkit, kirjallisten ohjeiden ja käytännön toimintatapojen yhtenäisyys sekä se, ovatko muut toimintamallit (esimerkiksi tiedotus, rektytointikäytännöt) yhteneviä tietoturvaohjeiden kanssa. (Laaksonen ym. 2006, 249-250.)

Yksilön tietoturvakäyttäytymiseen vaikuttaa myös omasta tahdosta riippumattomat tekijät. Nämä tekijät ovat työntekijän henkilökohtaiset arvot ja asenteet, suhtautuminen työnantajaan sekä ohjeiden noudattamiseen vaadittava työpanos. Ohjeiden laatimisen yksi päätavoitteista onkin sellaisen ratkaisun löytäminen, jonka avulla samoihin lopputuloksiin voitaisiin päästä työntekijöiden kannalta helpolla ja joustavalla tavalla. Organisaation toimintamallien hyväksyminen on helpompaa kun työntekijät uskovat niiden olevan tärkeitä työtehtävien hoitamisen kannalta sekä samassa linjassa heidän omien asenteiden ja arvojen kanssa. Organisaatiossa vallitsevien arvojen ja toimintamallien hyväksyminen useasti helpottaa työskentelyä, mutta jos ne ovat ristiriidassa työntekijän omien arvojen ja mallien kanssa, saattaa ongelmia ilmetä. Tällöin työntekijän omat arvot kiilaavat organisaation arvojen edelle. (Laaksonen ym. 2006, 250.)

Tietoturvaohjeisto ei anna yksiselitteistä neuvoa jokaiseen tilanteeseen, vaan ohjeita tulee soveltaa itsenäisesti käytäntöön. Suurin osa turvallisuutta koskevista päätöksistä tehdään vakaassa toimintaympäristössä, joka saattaa sietää suuretkin virhearvioinnit. Osa päätöksistä joudutaan kuitenkin tekemään nopeasti herkässä toimintaympäristössä ilman etukäteistietoa

päätösten jälkivaikutuksista. Tällaiset tilanteet ovat selkeä uhka tietoturvallisuudelle. Vasta kokemuksen myötä henkilöstö saavuttaa taidon tehdä nopeita, mutta oikeita päätöksiä, jotka ovat organisaation toiminnan kannalta järkeviä ja johdonmukaisia. (Laaksonen ym. 2006, 252.)

6.3 Motivoiminen tietoturvatyöhön

Useimpien tietoturva-asiantuntijoiden mukaan henkilöstön mielenkiinnon kiinnittäminen tietoturvallisuuteen voi joskus olla vaikeaa. Useimmiten ihmiset ovat kohteliaita ja ottavat muita huomioon, jolloin turvallisuusjärjestelmien toiminta voi heikentyä. Esimerkiksi ovia saatetaan avata tuntemattomille ”työtovereille” tai lainata avaimia arkistokaappien avaamista varten. Turvallisuustason parantaminen edellyttää muutosta henkilöstön käyttäytymisessä, koska sen ymmärtäminen ja ennustaminen on tärkeää tietoturvallisuuden kehittämistä ajatellen. Tietoturvasta vastaavien henkilöiden ja tahojen täytyy ymmärtää ne asiat, jotka vaikuttavat siihen tapaan, jolla henkilöstö luo itselleen kuvan organisaatiossa vallitsevasta todellisesta turvallisuuskäyttäytymisen käytännöstä sekä myös omaksuu sen. Tietoturvatietoinen ja motivoitunut henkilö havaitsee paremmin ja helpommin uhkia ja epäkohtia yrityksen toiminnassa ja pyrkii kehittämään omaa toimintaansa kohti oikeanlaista tietoturvakäyttäytymistä. (Laaksonen ym. 2006, 252-253; Nykänen 2011, 17.)

Positiivisia kannustimia voidaan käyttää palkitsemaan henkilöstöä ohjeiden ja määräysten noudattamisessa, jolloin tietoturvallisuuden taso saadaan nousemaan. Tietoturvapolitiikkaa ja –toimintaohjeita sovellettaessa käytäntöön on tavallista, että keskitytään liian helposti tarkkailemaan vain ohjeiden rikkomista. (Laaksonen ym. 2006, 253.)

Organisaation sosiaalista ilmapiiriä on muutettava niin, että henkilöstön on mahdollista tehdä yhteistyötä turvallisuuden parantamiseksi. Yhteistyö tulisi aloittaa nykytilanteen kartoituksella ja selvittää mikä on henkilöstön näkemys tietoturvallisuuden nykytasosta sekä tulevaisuuden tasosta. (Laaksonen ym. 2006, 253; Nykänen 2011, 18.)

6.4 Tietoturvaohjeiden jalkauttaminen

Tietoturvaohjeiden jalkauttaminen voidaan suunnitella esimerkiksi Yrityksen tietoturvakäsikirjassa olevien koulutusesimerkkien avulla. Niiden tarkoituksena on helpottaa kohdeyrityksen tietohallintoa suunnittelemaan tarkoituksenmukainen ja tehokas tietoturvakoulutus. Tämän osion tarkoituksena on selventää tietoturvakoulutukseen liittyvää teoriaa sekä esitellä tärkeimpiä koulutusmalleja ja esimerkkejä.

Tietoturvakoulutuksen pääasiallisena tavoitteena on opastaa ihmiset toimimaan johdon haluamalla tavalla, niin että yrityksessä oleva tieto suojataan mahdollisimman turvallisilla sekä kustannustehokkailla tavoilla. Suunniteltaessa tietoturvakoulutusta täytyy muistaa, että koulutuksen tulisi ensisijaisesti perustua voimassaolevaan tietoturvapolitiikkaan, sitä täydentäviin toimintaohjeisiin sekä yritysjohdon suorittamissa auditoinneissa havaittuihin puutteisiin tietoturvakäyttäytymisessä. Konstruktiivisen oppimiskäsityksen katsotaan soveltuvan hyvin tietoturvakoulutuksen dynaamiseen oppimismalliin, koska siinä otetaan huomioon eri osapuolten muuttuvat tavoitteet ja opetuksen lähestymistavan muutokset opetustapahtumassa syntyvien tilanteiden mukaisesti. (Laaksonen ym. 2006, 254; Nykänen 2011, 26.)

Henkilöstön motivaation taso on suoraan sidoksissa tietoturvakoulutuksen tehokkuuteen. Erilaisten motiivien vaikutusta oppimiseen tulisikin siis miettiä tarkoin. Parhaassa tapauksessa henkilöstön omaa kiinnostusta uusien asioiden omaksumisessa voidaan hyödyntää tehokkaasti, koska innostunut työntekijä levittää innostustaan myös ympärilleen. (Laaksonen ym. 2006, 254.)

Yksi hyvä keino motivoida henkilöstöä on ehdottaa heille esimerkiksi mahdollisuutta kehittää omat, nykyistä joustavammat tai järkevämmät tietoturvallisuuden pelisäännöt yhdessä tietohallinnon edustajien tai muiden tietoturvallisuudesta vastaavien henkilöiden kanssa. Tämä menetelmä on erityisen toimiva silloin, kun yrityksessä ei ole vahvaa tietoturvakulttuuria tai vakiintuneita tietoturvakäytäntöjä. (Laaksonen ym. 2006, 254.)

Henkilöstön ei odoteta tietävän kaikkea tietoturvasta. Usein riittää, että jokainen ymmärtää omaan työhönsä liittyvät riskit sekä sen, miten ne voidaan minimoida. Tietoturvan teknisten ratkaisuiden pitäisi näkyä käyttäjille mahdollisimman vähän ja ihannetilanteessa ei ollenkaan. Tietoturvallisuuden kehittämisen suurimmat virheet tehdään yleensä tietoturvallisuustoimintaa organisoitaessa ja henkilöstöä koulutettaessa. Ohjeiden jakamisen lisäksi täytyy muistaa myös korostaa toimintatapojen perimmäisiä syitä, jotta päästäisiin haluttuun lopputulokseen. (Laaksonen ym. 2006, 254-255.)

Käytännön esimerkkien avulla kouluttaminen

Käytännön esimerkkien avulla henkilöstölle avautuu parhaiten se, mitä tietoturvapolitiikalla, ohjeilla sekä toimintamalleilla todellisuudessa haetaan. Mikäli ohjeita ei viedä käytännön tasolle, yrityksen tietoturvallisuuden tasoa voi olla vaikea saada haluttujen tavoitteiden mukaiseksi. Esimerkkien avulla on tarkoitus synnyttää keskustelua erilaisista toimintatavoista sekä siitä, minkälaisiin tilanteisiin ne kulloinkin sopivat. Keskustelu tulisi myös ulottaa

koskemaan myös sitä, miten tietoturvaohjeita tulee käytännössä noudattaa sekä miksi niitä täytyy noudattaa. (Laaksonen ym. 2006, 255.)

Henkilöstön toimintatapojen pitäisi olla suhteellisen yhteneväisiä. Keskustelun yksi päätavoitteista onkin siis yhteisten pelisääntöjen määritteleminen erilaisissa tieturvallisuusasioissa. Joillekin työntekijöille eteentulevat tilanteet voivat olla entuudestaan tuttuja, joten heillä saattaa olla aikaisempaa tietämystä siitä, miten tilanteessa tulee toimia. Täten kokeneemmat työntekijät voivat jakaa kokemuksiaan muun henkilöstön kanssa, jolloin voidaan yhteisesti arvioida, ovatko toimintatavat olleet riittäviä vai voitaisiinko niitä edelleen kehittää. (Laaksonen ym. 2006, 255.)

Kysymyksien asettelulla saadaan tehokkaasti ihmiset ajattelemaan omaa päivittäistä tietoturvallisuuskäyttäytymistään. Jo yksinkertaisella kysymyksellä, kuten esimerkiksi millaista luottamuksellista tietoa henkilö päivittäin käsittelee, saadaan aikaan keskustelua siitä, minkälainen tieto on luottamuksellista tai julkista. Huomioitavaa on myös se, että päivittäisessä työssä käsiteltävää tietoa ei aina käsitetä niin luottamukselliseksi kuin esimerkiksi tietoturvaohjeistus edellyttää. (Laaksonen ym. 2006, 256.)

Esimerkki 1: Yrityksen tietoturvaroskalaatikkoa tyhjentämään tullut henkilö ei tarkalleen tiedä laatikon sijaintia. Hän kysyy neuvoa yrityksen työntekijältä. Miten tällaisessa tilanteessa tulisi toimia?
Esimerkki 2: Työntekijä on lähettänyt sopimuspohjan väärään sähköpostiosoitteeseen. Miten tässä tilanteessa tulisi toimia? Miten tilanne voidaan ehkäistä tulevaisuudessa? (Laaksonen ym. 2006, 256.)

Säännöllisyys ja vaihtelevat menetelmät

Välillä eteen tulee tilanteita, jolloin pakollista koulutusta tarvitaan esimerkiksi uusien työtehtävien hallitsemiseksi. Tällaisissa tilanteissa motivoinnin suhdetta oppimistuloksiin ei pidä unohtaa. Motivoinnin tulee olla avointa ja rehellistä. Yritysjohdon on myös selkeästi ja ennenkaikkea perustellusti täsmennettävä, että asiat on opeteltava ja ohjeita noudatettava, halusivatpa työntekijät sitä tai eivät. On hyvä muistaa, että tällaisissa tapauksissa ei pelkällä kouluttamisella välttämättä saavuteta vaadittuja tuloksia. Tehostavina apukeinoina voidaan käyttää ulkoa opettelua ja mekaaniseen harjoitteluun ”pakottamista”. (Laaksonen ym. 2006, 256.)

Organisaatiossa kouluttamisen on oltava säännöllistä. Tietoturvapolitiikan ja toimintaohjeiden vuotuinen läpikäynti on jo nykypäivää monissa yrityksissä. Myöskin uusien työntekijöiden kouluttaminen tietojärjestelmien käyttöön ja tähän liittyvä tietojenkäsittelytapojen

läpikäynti on osa peruskoulutusta. Säännöllisessä koulutuksessa on kuitenkin huomioitava se, että työntekijät eivät koe sitä pakollisena tilaisuutena, jota halutaan välttää kaikin keinoin. Tietoturvallisuuden kannalta on edullisempaa saada henkilöt ymmärtämään asioiden vaikutukset yrityksen toimintaan. Kokeilemalla kouluttaminen puolestaan saattaa johtaa ei toivottuun lopputulokseen ainakin liiketoiminnan kannalta, vaikka työntekijät kokeilusta oppisivatkin. (Laaksonen ym. 2006, 256-257.)

Esimies kouluttaa alaisensa

Yritysjohto on vastuussa siitä, että henkilöstö ymmärtää tietoturvallisuuden merkityksen yrityksen liiketoiminnalle ja maineelle. Käytännössä toimivaksi havaittu menetelmä on, että esimies selvittää alaisilleen tietoturvaohjeiden merkityksen ja sisällön. Esimies on vastuussa toiminnasta sekä sen hallinnoimisesta noudattaen yrityksen menettelytapoja ja valmentamalla työntekijät. Esimiehen tehtäviin kuuluu myös uusista käytännöistä ja ohjeista tiedottaminen sekä varajärjestelyjen luominen poikkeustilanteiden varalle. Tämä vaatii kuitenkin myös sen, että kaikki muutkin esimiehet ovat tietoisia uusista ohjeista sekä muista oleellisista dokumenteista. Tätä varten kannattaa sopia vakioidut tiedotuskanavat. (Laaksonen ym. 2006, 258.)

Yritysjohdon oma toimintatapa on aina sidoksissa siihen, miten tietoturvaan yrityksessä suhtaudutaan. Johdon on oltava perehtynyt tietoturvallisuuteen sekä sitoutunut tietoturvariskien hallintaan, jotta riskien torjunta yrityksessä onnistuu. (Laaksonen ym. 2006, 258.)

Kysymyksiä esimiehelle:

- *Tuntevatko työntekijät suurimmat tietoturvauhat?*
- *Ovatko työntekijät lukeneet tietoturvaohjeet, ovatko he ymmärtäneet ne ja mistä tämä tiedetään?*
- *Ymmärtävätkö työntekijät hyvän salasanan merkityksen?*
- *Tietävätkö työntekijät, miten henkilökohtaiset tietojenkäsittelylaitteet varmistetaan?*
- *Osaavatko työntekijät suojata tiedon myös työmatkoilla?*
- *Tietävätkö työntekijät kenelle tietoturvahavainnoista tulee ilmoittaa?*

(Laaksonen ym. 2006, 259.)

Tietoturvaorganisaation järjestämä keskitetty koulutus

Pääpiirteittäin suuri osa tietoturvakoulutuksen järjestämisestä kuuluu yrityksen tietoturvaorganisaatiolle. Tietoturvaorganisaation ei välttämättä aina itse täydy pitää koulutusta, mutta sen suunnittelu tulisi jättää tietoturvaorganisaation vastuulle. Tällä tavoin

varmistetaan se, että koulutus on yhtenäistä, vastaa tavoitteita sekä organisaatiotasoisia käytäntöjä. Tietoturvaorganisaation roolia koulutuksen kannalta voidaan luonnehtia merkittäväksi esimerkiksi tietoiskuja sekä muita koulutusluontoisia tapahtumia ajatellen. (Laaksonen ym. 2006, 259.)

Keskittettyä, jokaista koskevaa koulutusta kannattaa järjestää säännöllisesti ja silloin kun tietoturva-asioissa tai käytännöissä on merkittäviä muutoksia tai jonkin ajankohtaisen tapauksen johdosta. Tietoturvaorganisaation tehtävänä on myös varmistaa esimiesten riittävä tietämyksen taso, jotta he voivat kouluttaa omat alaisensa, mikäli tällainen toimintamalli on käytössä yrityksessä koulutuksen järjestämiseksi. (Laaksonen ym. 2006, 259.)

Tietoiskut

Tietoturvakoulutuksen ei aina tarvitse olla perinteistä opettamista. Markkinoinnin keinoja voidaan käyttää tässäkin kohtaa hyödyksi, jolloin tietoturva-asiat voidaan aika-ajoin tuoda henkilöstön ajatuksiin. Dialogin avulla saadaan ihmiset ajattelemaan asioita. Keskustelua käynnistettäessä tulee ”pelata” kysymyksillä, jotka pakottavat ajattelemaan. Tietoiskujen rakenne voidaan jakaa neljään selkeään osaan:

- Mitkä ovat tyypillisimmät tietoturvaongelmat, joita yritykset maailmanlaajuisesti kohtaavat?
    - Selvitetään lyhyesti tutkimusten valossa merkittävimmät tietoturvaongelmat, jotka ovat haitanneet yritysten operatiivista toimintaa tai aiheuttaneet muutoin suuria taloudellisia tappioita.
    - Konkreettiset esimerkit lisäävät koulutuksen ja tutkimustulosten uskottavuutta.
- Mitkä ongelmat ovat merkittäviä omaa yritystä ajatellen?
    - Käydään kattavasti ne ongelmat, jotka ovat mahdollisia sekä todennäköisiä oman yrityksen vaikutusalueella.
- Miten ongelmat voidaan välttää?
    - Selvitetään toimintamallit, joiden avulla ongelmat voidaan välttää. Samalla voidaan viitata yrityksen tietoturvaohjeisiin.
- Mitä henkilöstö hyötyy ohjeiden noudattamisesta?
    - Henkilöstön täytyy kokea hyötyvänsä ohjeiden noudattamisesta, jolloin saavutetaan konkreettisia tuloksia. Hyötynä voidaan nähdä oman työn helpottuminen tai esimieheltä saatava arvostus.

(Laaksonen ym. 2006, 260.)

Tietoiskut ovat toimiva ja tehokas tapa kun halutaan nostaa esille jokin ajankohtainen tietoturvakysymys. Edellä oleva havainto-ratkaisu-hyötymalli sopii monenlaisten tietoturvaongelmien käsittelyyn. (Laaksonen ym. 2006, 259.)

7 Yhteenveto ja tulosten analysointi

Työn saaminen valmiiksi oli pitkä prosessi. Aihealue on suhteellisen laaja, joten sen rajaaminen järkeväksi oli tehtävä kunnolla. Tarkoituksena oli luoda kohdeyritykselle tietoturvapolitiikka, ohjeet sekä suunnitelma ohjeiden kouluttamiseksi henkilökunnalle. Työn teoriaosuudessa on käsitelty tietoturvallisuutta lähinnä yrityksen näkökulmasta. Teoriaosuuteen on myös sisällytetty perustietoa yrityksen tietoturvapolitiikoista, tärkeistä standardeista, tietoturvan johtamis- ja hallintajärjestelmästä sekä tietoturvaohjeista ja niiden merkityksistä.

Tietoturvapolitiikan luomisessa on käytetty apuna kohdeyrityksen voimassaolevaa tietoturvapolitiikkaa, joka ei tällä hetkellä kunnolla vastaa yrityksen toimintaa sekä on siinä mielessä vanhentunut, että se on tarkoitettu kohdeyrityksen vanhoja toimitiloja varten. Eri yritysten tietoturvapolitiikkoja tutkiessani huomasin, että ne noudattavat pääosin samanlaista linjausta. Eroavaisuuksia ei juurikaan ole havaittavissa. Tämänkaltaisella yhteneväisyydellä on varmasti haettu jonkinlaista standardisoitumista tietoturvapolitiikkojen saralla. Lisäksi niitä on helppo muokata ja tarvittaessa uudistaa yleisluontoisuuden vuoksi. Kohdeyrityksen oman tietoturvapolitiikan lisäksi uudistetussa tietoturvapolitiikassa on vaikutteita Mänttä-Vilppulan kunnan sekä Peruspalvelukuntayhtymä Kallion tietoturvapolitiikoista, jotka ovat luonteiltaan sellaisia, että niitä voi soveltaa lähes missä tahansa yrityksessä. Kohdeyritykselle tuotetussa politiikassa on selkeästi määritelty ne osa-alueet, joista keskeiset periaatteet käytännön tietoturvatyölle muodostuvat.

Kohdeyrityksen tekniset tietoturvaohjeet ovat tällä hetkellä riittävät, joten ne katsottiin parhaaksi jättää sellaisiksi kuin ovat. Nykyisten teknisten ohjeiden täydennykseksi laadittiin erilliset henkilöstön tietoturvaohjeet, jotka ovat yleispätevät ja auttavat toimimaan tietoturvallisesti lähes kaikissa käytännön tilanteissa. Suosittelen VAHTI10/2006 –julkaisua jaettavaksi kokonaisuudessaan kohdeyrityksen henkilöstölle, koska se sisältää arvokasta tietoa henkilötasolla tapahtuvan tietoturvallisuuden toteuttamisen kannalta. Täytyy myös muistaa, että yritysjohdolle on tarjottava tietoturvakoulutusta siinä missä muullekin henkilöstölle, koska tietoturvallisuuden toteuttaminen lähtee aina liikkeelle yritysjohdosta. Esimerkiksi tietoturvapolitiikka on aina yritysjohdon kannanotto yrityksen tietoturvallisuuteen.

Varsinaisena tutkimuskysymyksenä tässä työssä oli se, että millä tavalla uudet tietoturvaohjeet tulisi jalkauttaa kohdeyritykseen. Ohjeistus jalkautukseen (liite 3) pohjautuu pitkälti Yrityksen tietoturvakäsikirjaan ja sitä on täydennetty sopivilta osin vastaamaan kohdeyrityksen tarpeita ja toimintoja. Kirjan loppuosasta löytyvien koulutusesimerkkien- ja

mallien avulla voidaan kehittää tehokas tietoturvakoulutus. Esimerkit ovat vaihtelevia ja tämän lisäksi koulutusosiossa on käsitelty aiheeseen liittyvää teoriaa riittävällä syvyydellä, jolloin koulutuksesta saatavan hyödyn määrä voidaan maksimoida. Idea infotelevisioiden käytöstä puolestaan tuli nykyisestä työpaikastani, jossa ne ovat käytössä ja toimivat erittäin hyvin.

Lähteet

Anttila, J. & Kajava, J. 2006. PDCA-malli tietoturvallisuuden integroinnissa organisaation liiketoiminnan johtamiseen. SFS-Tiedotus 38 VSK 2/2006.

Anttila, J., Kajava, J., Savola, R. & Röning J. 2009. Liiketoimintaprosessit – organisaation tietoturvallisuuden ydinaihe. Sähkö&Tele -lehti. Viitattu 20.3.2011 http://www.qualityintegration.net-a.googlepages.com/ST32009Osa1.pdf

Department for Business, Enterprise & Regulatory Reform. 2009. Information security: How to write an information security policy. Viitattu 3.4.2012. http://www.bis.gov.uk/files/file49963.pdf

DNV Oy. 2010. ISO 27001. Viitattu 15.02.2012. http://www.dnv.fi/palvelut/sertifiointi/hallinta_ja_johtamisjarjestelmat/tietoturvallisuus/iso27001/

Helsingin Yliopisto 2010. Tietotekniikan palvelut. Viitattu 16.02.2012. http://www.helsinki.fi/atk/tietoturva/politiikat.html

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

International Organization for Standardization. ISO/IEC 17799:2005. Viitattu 15.02.2012. http://www.iso.org/iso/catalogue_detail?csnumber=39612 & http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103

IT-Grundschutz Manual 2005. Federal Office for Information Security. Viitattu 14.2.2011 https://www.bsi.bund.de/EN/Topics/ITGrundschutz/ITGrundschutzCatalogues/itgrundschutzcatalogues_node.html

Kallio, T. 2003. BS7799 vs ISF Standard of Good Practices. Helsingin Yliopiston tietojenkäsittelytieteen laitos. Tietoturva nykyaikaisessa liiketoimintaympäristössä – seminaari. Viitattu 15.02.2012. www.cs.helsinki.fi/group/turvasem/papers/kallio_seminaari.rtf

Karttunen, I. 2005. TeliaSonera. Ajankohtaiskatsaus tietoturvallisuuteen. Viitattu 15.02.2012. http://tekniikka.ncp.fi/turvallisuustekniikka/files/tiva/karttunen/ismokarttunen.pdf

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen Tietoturvakäsikirja. Helsinki: Oy Nordprint Ab.

Metodix. Konstruktiivinen tutkimusote. Viitattu 14.2.2012. http://www.metodix.com/fi/sisallys/04_virtuaalikirjasto/dokumentit/aineistot/konstruktiivinentutkimusote

Mäkinen, R. 2003. Tietoturvapolitiikat. Helsingin Yliopiston tietojenkäsittelytieteen laitos. Tietoturva nykyaikaisessa liiketoimintaympäristössä –seminaari. Viitattu 19.1.2011. http://www.cs.helsinki.fi/group/turvasem/papers/makinen_tietoturvapolitiikat.pdf

Nykänen, K. 2011. Tietoturvakoulutuksen vaikuttavuuden arviointi yksilön ja organisaation tietoturvakäyttäytymiseen. Oulun yliopiston tietojenkäsittelytieteiden laitos. Viitattu 4.4.2012. http://herkules.oulu.fi/isbn9789514295713/isbn9789514295713.pdf

Ojasalo, K., Moilanen, T. & Ritalahti, J. 2009. Kehittämistyön menetelmät. Helsinki: WSOYpro Oy.

Scarfone, K. & Hoffman, P. 2009. Guidelines on Firewalls and Firewall Policy. Viitattu 3.4.2012. http://csrc.nist.gov/publications/nistpubs/800-41-Rev1/sp800-41-rev1.pdf

SGN Group Oy. 2008. SGN Groupille uudet toimitilat.Viitattu 26.11.2010. http://www.sgn.fi/uutinen?=&id=2

Tietoturvaopas.fi. Yrityksen tietoturvaopas. Viitattu 16.02.2012. http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/index.html

Tietoturvaopas.fi. Mihin laki velvoittaa?. Viitattu 15.02.2012. http://www.tietoturvaopas.fi/yrityksen_tietoturvaopas/fi/mihin_laki_velvoittaa.html

Tipton, H. & Krause, M. 2008. Information Security Management Handbook. United States of America: Auerbach Publications.

VAHTI 10/2006. Henkilöstön tietoturvaohje. Valtionvarainministeriö. Helsinki: Edita Prima Oy.

VAHTI 3/ 2003. Tietoturvallisuuden hallintajärjestelmän arviointisuositus. Valtionvarainministeriö. Helsinki: Edita Prima Oy.

Yhteiskunnan tieto. 2009. Tietoturvallisuuden hallintajärjestelmän kehittäminen. Viitattu 14.4.2011. http://www.yhteiskunnantieto.fi/tthj.pdf

Yhteiskunnan tieto. 2007. ISO 27002:2007. Viitattu 23.5.2012. http://www.yhteiskunnantieto.fi/ajankohtaista_iso27002.pdf

Kuvat ja kuviot

Liitteet

Liite 1: Tietoturvapolitiikka – SGN Group

SGN GROUP – TIETOTURVAPOLITIIKKA

Hyväksytty xx.xx.xxxx

Johdanto, päämäärä ja tavoitteet

Tietoturvapolitiikka kuvaa SGN Groupin tietoturvallisuuden tavoitteet, vastuut sekä toteutuskeinot. Tietoturvallisuus on välttämätön osa yrityksen kokonaisvaltaisen toiminnan varmistamista ja kehittämistä.

Tietojenkäsittely tukee SGN Groupin palveluiden tuottamista, ja palveluiden tehokkuus riippuu osaltaan tietojenkäsittelystä. Yrityksessä tapahtuvan tietoturvallisuustyön tavoitteena on turvata yrityksen toiminnalle tärkeiden tietojärjestelmien ja tietoverkkojen keskeytymätön toiminta, estää tietojen ja tietojärjestelmien valtuudeton käyttö, tahaton tai tahallinen tiedon tuhoutuminen, tietojen joutuminen vääriin käsiin sekä minimoida aiheutuvat vahingot. Tietoturvallisuus kattaa yrityksen kaiken tietojenkäsittelyn huomioiden eri yritysten perusluonteen ja mahdollisen tarpeen myös tietoturvallisuuden tehostamiseen.

Normaaliajan toiminnan tietojenkäsittelyn turvaamisen lisäksi varaudutaan toiminnan keskeyttäviin uhkatilanteisiin ja niistä toipumiseen.

Yrityksen tiedot, tietojenkäsittelyjärjestelmät ja -palvelut pidetään asianmukaisesti suojattuina sekä normaali- että poikkeusoloissa hallinnollisten, teknisten ja muiden toimenpiteiden avulla. Tieto on yrityksen omaisuutta ja sitä on suojattava samoin menetelmin, kuin yrityksen muutakin omaisuutta.

Yrityksen tavoitteena on, että tietoturvajärjestelyt ovat hyvää kansainvälistä ja kansallista tasoa. Jokainen yrityksen tietoja käsittelevä henkilö on omalta osaltaan velvollinen huolehtimaan tietoturvallisuudesta.

Tämä tietoturvapolitiikka on voimassa toistaiseksi ja sen voimassaolo jatkuu, ellei sitä nimenomaisesti kumota. Tarvittaessa voidaan julkaista uusi versio, joka kumoaa tämän dokumentin julkaisuhetkellä.

Tietoturvallisuus

Tietoturvallisuudella tarkoitetaan tärkeiden tietojen, palveluiden, tietojärjestelmien sekä tietoliikenteen suojaamista. Tietoturvallisuus rakentuu kolmesta osasta; tiedon eheydestä, luottamuksellisuudesta sekä käytettävyydestä. Näitä kolmea ominaisuutta täydentää yleensä vielä kiistämättömyys, tunnistus, todennus sekä pääsynvalvonta. Tietoturvallisuustoimet koskevat kaikkea tietojenkäsittelyä; sähköisessä, suullisessa ja kirjallisessa muodossa oleva tiedon säilytys, käsittely, luovuttaminen, hävittäminen, siirto sekä arkistointi.

Eheys: Tieto ja tietojärjestelmät ovat oikeellisia, luotettavia sekä ajantasaisia.
Luottamuksellisuus: Tieto ja tietojärjestelmät ovat vain niihin oikeutettujen henkilöiden saatavilla.
Käytettävyys: Tieto ja tietojärjestelmät ovat käytettävissä, kun niitä tarvitaan.
Kiistämättömyys: Tapahtuman todentaminen jälkeenpäin, tavoitteena juridinen sitovuus.
Pääsynvalvonta: Menetelmät, joilla voidaan rajoittaa tietojärjestelmien käyttöä.

Toteutuskeinot

Tämä tietoturvapolitiikka toimii tietoturvallisuuden toteuttamisen perustana ja se annetaan tiedoksi jokaiselle yrityksessä työskentelevälle henkilölle. Tietoturvallisuuden tavoitteiden toteuttaminen on jatkuva prosessi, joka tapahtuu fyysisten, hallinnollisten sekä teknisten ratkaisujen avulla. Lisäksi, käyttäjien toimintaa niihin opastetaan erilaisten käyttösääntöjen, toimintaohjeiden ja tietoturvakoulutuksen avulla.

Tietoturvan seuranta ja ongelmatilanteiden käsittely

Yrityksen tietohallinto-osasto seuraa ja kartoittaa tietojärjestelmien tietoturvallisuutta ja voi ryhtyä välittömiin toimenpiteisiin havaittujen epäkohtien korjaamiseksi kaikissa tilanteissa. Jokainen yrityksen tietoa tai tietojärjestelmiä käyttävä henkilö on velvollinen noudattamaan annettuja tietoturvallisuusohjeita sekä muita käyttösääntöjä. Tämän lisäksi jokainen käyttäjä sekä ylläpitäjä ovat velvoitettuja ilmoittamaan havaitsemistaan tietoturvallisuuspuutteista, väärikäytöksistä tai epäilemistään tietoturvallisuusrikkomuksista lähimmälle esimiehelleen tai tietohallintoon.

Vastuut, organisointi ja rikkomukset

Tietoturvallisuus on osa yrityksen kokonaisturvallisuutta. Tietoturvallisuustyötä valvotaan yrityksen johtoryhmän toimesta, joka päättää tietoturvallisuustoiminnan kehittämisestä, organisoinnista sekä tarvittavista resursseista. SGN Groupissa tietoturvallisuudesta

huolehditaan yhteisesti. Jokainen yrityksessä työskentelevä henkilö on velvollinen toimimaan tietoturvallisuutta edistävällä tavalla. Täten jokainen työntekijä on myös henkilökohtaisessa vastuussa oman toimintansa turvallisuudesta sekä sitoutuu noudattamaan työtehtäviensä turvalliseen hoitamiseen annettuja määräyksiä ja ohjeita.

Yrityksen tietohallinto-osastolla on velvollisuus selvittää tietoturvallisuuteen liittyvät rikkomukset ja väärinkäytökset. Jokainen rikkomus raportoidaan yrityksen johtoryhmälle ja rikkomuksen tekijä saatetaan edesvastuuseen teoistaan. Rikkomuksen luonne määrää tekijää vastaan toteutettavat toimenpiteet.

Liite 2: Henkilöstön yleiset tietoturvaohjeet

Tämä ohje sisältää keskeisimmät tietoturvallisuuden perusasiat. Ohjeen tarkoituksena on opastaa tietoturvalliseen toimintaan omassa työssä sekä muissa käytännön tilanteissa. Laadinnassa on sovellettu VAHTI10/2006 –ohjeistusta.

Keskeiset ohjeet:

- Seuraa tietoturvallisuuteen liittyviä ohjeita ja tiedotteita. Osallistu sinulle tarjottuun koulutukseen. Toimi saatujen ohjeiden perusteella.
- Älä jätä vierasta yksin/valvomatta työhuoneeseesi tai muihin yrityksen tiloihin.
- Pidä kuvallinen henkilökortti aina mukanasi, mikäli sellainen on annettu.
- Älä koskaan anna ulkopuolisen käyttää tietokonettasi tai muuta välinettä, esim. älypuhelinta.
- Muista puhtaan pöydän periaate. Älä säilytä työpöydälläsi arkaluontoista tai salattavaa aineistoa.
- Tietoja on aina käsiteltävä huolellisesti välineestä riippumatta – olipa tietojen välittäjänä sitten henkilö, tietokone, paperi, puhelin tai telekopio.
- Älä koskaan luovuta henkilökohtaisia käyttäjätunnuksiasi ja salasanojasi toiselle henkilölle. Älä edes tietohallintohenkilöstölle, koska he eivät niitä tarvitse.
- Salasanat tulee vaihtaa riittävän useasti ja heti kun epäilet niiden paljastuneen.
- Tietoaineistot sekä työvälineet ovat tarkoitettu vain työtehtävien hoitamiseen.
- Älä asenna ohjelmistoja tai tee niihin asetusmuutoksia, ellei se kuulu työtehtäviisi.
- Tallenna työsi aina verkkopalvelimelle, josta ne varmuuskopioidaan keskitetysti.
- Hae tulosteesi verkkotulostimelta välittömästi tulostamisen jälkeen.
- Älä unohda, että yrityksen laitetta, verkkoa tai sähköpostia käyttäessäsi näyt ja esiinnyt tietoverkkossa aina –tahtomattasikin- yrityksen edustajana.
- Huolehdi asianmukaisesta salauksesta aina kun siirrät internetin kautta salassapidettävää tietoa.
- Jos siirrät aineistoa esimerkiksi muistitikun tai vastaavan muistivälineen avulla, valvo siirtoa henkilökohtaisesti.
- Muista estää asiaton pääsy tietojärjestelmiin lukitsemalla työasemasi aina kun poistut työpisteeltäsi. Myös näytönsäästäjään saa suojattua salasanalla.
- Työpäivän lopuksi kirjaudu ulos tietojärjestelmästä sekä sammuta työasemasi yrityksen ohjeiden mukaisesti.
- Ilmoita välittömästi havaitsemistasi tietoturvallisuuteen liittyvistä ongelmatilanteista, uhista tai puutteista tietoturvavastaavalle, tietohallintoon tai esimiehellesi. Heidän velvollisuutensa on ryhtyä tarvittaviin toimenpiteisiin.

- Voit aina pyytää neuvoa tai apua yrityksesi asiantuntijoilta.
- Jos olet poissa työpisteeltäsi, älä jätä kannettavaa työasemaasi lojumaan autoon tms. vastaavaan paikkaan, josta sivullisen on helppo saada se haltuunsa.
- Huolehdi asianmukaisten salassapitosopimusten tekemisestä jos projektissa käytetään alihankkijoita tai freelancereita.
- Älä koskaan avaa epäilyttäviä sähköpostilla saapuneita liitetiedostoja. Jos et ole varma mitä pitää tehdä, voit aina pyytää apua yrityksesi asiantuntijoilta.

Liite 3: Tietoturvaohjeiden jalkauttaminen kohdeyritykseen

Tietoturvaohjeiden jalkauttaminen henkilökunnalle on tärkeää yrityksen tietoturvallisen toiminnan kannalta. Tietoturvaohjeista ei ole paljoakaan hyötyä jos henkilöstö ei niitä noudata tai sisäistä. Yrityksessä käsiteltävä tieto on arvokasta, joten sitä on suojattava kaikin keinoin. Tietoturvakoulutus tähtääkin siihen, että henkilöstö saadaan toimimaan yritysjohdon määrittelemillä tavoilla. Tärkein asia mikä tietoturvallisuusasioiden- ja ohjeiden noudattamiseen vaikuttaa on motivaatio. Tietoturvaohjeiden jalkautusta suunniteltaessa tulee muistaa, että sen tulee aina perustua kulloinkin voimassaoleviin tietoturvaohjeisiin sekä tietoturvapolitiikkaan.

Valitettavan monet ihmiset luulevat, että he ovat paremmassa turvassa kuin muut ja vahinkoa ei heille voi sattua. Huolimattomasti toimivat ihmiset ovat suurin riski yrityksen tietoturvallisuudelle. Teknisistä ratkaisuista ei ole mitään hyötyä jos tietoturvallisuuteen suhtaudutaan välinpitämättömästi. Tekniset ratkaisut toimivat yhtä turvallisesti kuin niitä operoivat käyttäjät. Useat tietokoneen käyttäjät myös uskovat olevansa niin sanottuja ”tehokäyttäjiä” ja tietävänsä ”kaiken” tietokoneista, koska he osaavat luoda tekstinkäsittely- ja taulukkolaskenta-asiakirjoja sekä esityksiä. Monet eivät kuitenkaan silti tunnu käsittävän edes perustietoturvallisuuden käsitteitä. Kyseenalaisilla internetsivuilla vierailu sekä umpimähkäisten ohjelmistojen asentaminen rikkovat yleensä myös yrityksen tietoturvallisuussäädöksiä.

Hyökkääjien ei edes kannata yrittää murtaa teknisiä tietoturvaratkaisuja, vaan helpompaa on mennä sieltä missä aita on matalin eli saada loppukäyttäjä avamaan heille ovi yrityksen tietoverkkoon. Yleisimmät tavat tähän ovat sähköpostilla lähetetyt liitetiedostot, tietojen kalastelu sekä sosiaalinen manipulointi. Esimerkkinä tästä I Love You –virus, joka aiheutti laajaa tuhoa levitessään. Puuttuminen loppukäyttäjien aiheuttamiin riskeihin on tärkeä osa mitä tahansa tietoturvaohjelmaa.

Näkisin myös, että laitteiden ja palveluiden etäkäyttö saattaa aiheuttaa tiettyjä riskejä. Ollakseen tuottavia, käyttäjät haluavat päästä käsiksi tarvitsemaansa tietoon kannettavilta työasemiltaan, kotikoneiltaan ja mobiililaitteiltaan. Tämän takia IT-osastojen on voitava synknoroida tietoja erilaisten laitteiden välillä. Ja jos tähän ei pystytä, käyttäjät voivat ottaa ohjat omiin käsiinsä. Esimerkiksi Googlen tarjoamaan Gmail-palveluun voi tallentaa seitsemän gigatavun edestä tiedostoja. Ja tähän liittyen ainakin Firefox-selaimeen saa Gspace-liitännäisen, joka tarjoaa käyttäjälle FTP-tyylisen käyttöliittymän, jonka avulla tiedostoja voidaan siirtää tietokoneelta Gmail-tilille. Tämäntyylinen mahdollisuus siirtää tietoa yrityksen ulkopuolelle ilman valvontaa vaikeuttaa yrityksen tietojen turvaamista oleellisesti.

Edellisellä sivulla olen nostanut esille mielestäni merkittäviä uhkakuvia ja esittänyt esimerkkejä siitä, millä tavoin yrityksen tietoturvallisuus voi vaarantua jos käyttäjät eivät ole perillä tietoturvaohjeistuksista. Tietoturvaohjeiden jalkauttamiseen ja kouluttamiseen on monia tapoja. Seuraavassa esitän keinot, joiden avulla jalkauttaminen mielestäni parhaiten onnistuu.

1. Tietoturvakulttuurin luominen ja henkilöstön motivointi

Henkilöstö on saatava näkemään, että tietoturvallisuus on välttämätön edellytys ja työkalu tehokkaalle liiketoiminnalle sekä yrityksen menestykselle. Tietoturvakulttuurin luominen vaatii yleensä pitkäaikaista muutosta henkilöstön käyttäytymisessä. Motivoinnin ja motivaation asemaa ei voi tässä asiassa mielestäni kyseenalaistaa. Ei-motivoitunut ja vanhoihin tapoihin juurtunut henkilöstö ei haluakaan oppia uusia tietoturvallisuuden toimintamalleja. Tietoturvakoulutuksen täytyy siis olla mielekästä ja innostavaa. Suosittelen myös jonkilaista palkitsemiskäytäntöä kun tietoturvallisuuteen liittyviä asioita ja ongelmia on käsitelty säädösten mukaisesti. Henkilöstön ei pidä kokea tietoturvallisuutta pahana asiana, joka vaikeuttaa päivittäisiä työtehtäviä ja teknisten ratkaisuiden on näyttävä mahdollisimman vähän. Työilmapiiriä on muutettava enemmän sosiaaliseksi, joka kannustaa yhteistyöhön tietoturvallisuuden parantamiseksi. Tämä kannattaa aloittaa nykytilanteen kartoituksella ja selvittää henkilöstön näkemys vallitsevasta tietoturvallisuuden tilasta. Onnistunut tietoturvakulttuurin luominen nostaa henkilöstön tietoturvatietoisuutta ja yleistä tietoturvallisuuden tasoa. Myös ihmisten arvot, asenteet ja odotukset vaikuttavat tietoturvallisuuden tasoon, joten myös yrityksen arvojen ja periaatteiden tulee olla kunnossa suhteessa tietoturvallisuuteen. Lisäksi haluan vielä korostaa, että tietoturvapolitiikka- ja ohjeet luovat vahvan perustan henkilöstön toimintatavoille.

2. Sopivien koulutumetodien valinta

Kuudennessa kappaleessa olen esitellyt erilaisia koulutusmetodeja. Metodit ovat vaihtelevia ja niitä voidaan soveltaa kaiken kokoisiin organisaatioihin. Kohdeyrityksen kanssa sovimme, että uudet tietoturvaohjeistukset tullaan esittelemään henkilöstölle seminaaritilaisuudessa ja henkilöstö tullaan myös sitouttamaan niihin. Tällöin tietoturvaorganisaation tulee huolehtia koulutuksen sisällöstä sekä toteutustavasta. Mielestäni seminaarin ei pidä olla luentotyyppinen, vaan mahdollisimman vuorovaikutteinen kaikkien siihen osallistuvien kesken. Koulutus voisi sisältää erilaisia tehtäviä ja kysymyksiä, joita henkilöstö voisi ratkoa pienissä ryhmissä. Ratkaisut tulisi lopuksi käydä yhteisesti läpi tietoturvaorganisaation kanssa. Tällainen seminaari pitäisi mielestäni järjestää säännöllisesti muutaman kerran vuodessa, erityisesti silloin kun tietoturva-asioissa tai käytännöissä tapahtuu muutoksia tai jonkin ajankohtaisen tapauksen vuoksi.

Myös esimiehet voivat kouluttaa alaisiaan tietoturva-asioissa ja tämä onkin yleisin tapa kouluttaa. Tällöin tietoturvaorganisaation vastuulla on esimiesten riittävästä tietotasosta huolehtiminen, jotta koulutus voi onnistua. Esimiesten tehtävänä on kertoa alaisilleen tietoturvaohjeiden merkityksestä sekä sisällöstä. Esimiehet tiedottavat myös uusista järjestelyistä ja ohjeista sekä luovat varajärjestelyt mahdollisten poikkeustilanteiden varalle. Esimiehen tehtäviin kuuluu myös uusien työntekijöiden perehdytys tietojärjestelmien käyttöön ja hyvän tietojenkäsittelytavan opettaminen.

Tietoiskut ovat myös tehokas tapa kun halutaan viestiä jostain ajankohtaisesta tietoturva-asiasta nopeasti. Mielestäni kohdeyritys voisi ottaa käyttöön esimerkiksi tietoturvasta kertovia julisteita, joita voitaisiin jakaa työpisteisiin. Tietoiskuihin kannattaa myös käyttää markkinoinnin keinoja, jotta tietoturvallisuuteen liittyvät seikat saadaan tehokkaasti henkilöstön ajatuksiin. Kappaleessa 6.4 esiteltyä havainto-ratkaisu-hyötymallia voidaan käyttää apuna tietoiskuja suunniteltaessa. Kohdeyritys voisi ottaa käyttöön myös eräänlaisen keskitetyn tietoiskupankin, johon voisi kerätä vaikkapa uutisartikkeleita ajankohtaisista tietoturva-asioista. Tietoiskukanavaksi suosittelen ensisijaisesti sähköpostia, mutta kohdeyritys voisi harkita myös esimerkiksi infotelevisioiden hankkimista eri osastoille tiedonvälityskanaviksi. Infotelevisioiden avulla voitaisiin kertoa esimerkiksi tulevista järjestelmäpäivityksistä ja muista yleisistä tietoturvallisuusasioista. Tietenkin infotelevisioita voisi käyttää myös muuhunkin tiedonvälitykseen.

Yhteenveto: Kohdeyrityksessä tulisi järjestää interaktiivinen tietoturvaseminaari muutaman kerran vuodessa tietoturvaorganisaation johdolla. Tämän lisäksi esimiesten tietoturvakoulutusta tulisi lisätä, jolloin he voisivat tehokkaasti kouluttaa alaisiaan aina tarpeen vaatiessa. Täten myös yritysjohdon sitoutuneisuus tietoturvallisuuteen tulee paremmin esille. Tietoiskujen avulla voidaan helposti ja tehokkaasti informoida henkilöstöä nopeasti muuttuvissa tietoturvallisuusasioissa ja –tilanteissa.