TAMPEREEN
AMMATTIKORKEAKOULU

YLEMPI AMK-TUTKINTO

OPINNÄYTETYÖRAPORTTI

Tietoturvatason nostaminen pk-yrityksissä tietoturvakulttuurin muutoksella

Toni Männistö

Yrittäjyyden ja liiketoimintaosaamisen koulutusohjelma
Huhtikuu 2007
Työn ohjaaja: Harri Hakonen

TAMPERE 2007

Tekijä: Toni Männistö

Koulutusohjelma: Yrittäjyyden ja liiketoimintaosaamisen koulutusohjelma

Opinnäytetyön nimi: Tietoturvatason nostaminen pk-yrityksissä tietoturvakulttuurin muutoksella.

Title in English: Weighting up information security in small and medium sized enterprises with changing information security culture.

Työn valmistumis-kuukausi ja -vuosi: 5/2007

Työn ohjaaja: Harri Hakonen **Sivumäärä:** 65

TIIVISTELMÄ

Tämän työn tavoitteena oli laatia pk-yritysten johtajille ja esimiehille ohje siitä, miten yrityksen tietoturvakulttuuria voidaan ohjata turvallisempaan suuntaan. Kyseinen ohje on tämän työn liitteenä. Ohje tehtiin tutkimalla ensin laajasti tutkimuksia, tieteellisiä artikkeleita, kirjallisuutta ja yleisiä artikkeleita. Näistä muodostuneet johtopäätökset ovat ohjeiden tekemisen perustana. Ohje haluttiin tehdä, koska pk-yrityksissä henkilöstön toimintaan liittyvät tietoturva-asiat eivät tutkimusten valossa ole kovinkaan hyvässä kunnossa. Työntekijöitä ei resurssien puutteen vuoksi kouluteta tietoturvalliseen toimintaan. Tietoturvaohjeita ei noudateta koska niitä ei ymmärretä tai niitä ei ole ollenkaan ja johtajat/esimiehet eivät sitoudu tietoturvan kehittämiseen.

Pk-yritysten toiminnassa on selvä ristiriita, koska pk-yritykset kuitenkin hyödyntävät nykyään yhä enemmän erilaisia tietojärjestelmiä ja tietoliikenneverkkoja liiketoiminnassaan. Jo pienimmätkin yritykset Suomessa ovat riippuvaisia tavanomaisimmista tietoteknisistä ratkaisuista. Lisäksi suuri osa pk-yrityksistä on riippuvaisia taloushallinnon ja asiakastietoon liittyvistä sähköisistä järjestelmistä.

Lisääntyvän tietotekniikan käytön myötä myös työn liikkuvuus on lisääntynyt. Työ ei olekaan enää paikkaan sidottua ja yhä useampi työntekijä tekeekin töitä kotona. Tämä lisää osaltaan tietovuotojen riskiä ja työntekijöiden vastuuta yrityksen arvokkaan tietopääoman luotettavasta kuljettamisesta ja säilyttämisestä. Kasvuhakuiset pk-yritykset myös kansainvälistyvät vauhdilla. Kansainvälistyminen tarkoittaa verkottumista uusien ulkomaisten toimijoiden ja sitä mukaa kulttuurien ja yrityskulttuurien yhteentörmäystä. Tässä tapauksessa myös tietoturvakulttuurien osalta. Onkin mielenkiintoista kuinka kansainvälisissä verkostoissa toimivien yritysten tietoturvakulttuurit saadaan yhtenäistettyä. Joka tapauksessa yritysten työntekijöillä on paljon vastuuta, koska heidän harteillaan on lopulta, kuinka laajalle yrityksen arvokas tietopääoma leviää tai ei leviä. Pelkästään huolimaton sähköpostin käyttö voi aiheuttaa esimerkiksi luottamuksellisen tiedon leviämisen kilpailijalle.

Harva pk-yritys on kuitenkaan laatinut tietoturvapolitiikkaa ja kirjallista tietoturvasuunnitelmaa. Nämä edustavat kuitenkin niitä tietoturvakulttuuriin liittyviä arvoja joilla työntekijöiden käyttäytymiseen voidaan vaikuttaa. Arvot ilmaisevat mitä pidetään toivottavana tai tavoittelemisen arvoisena käyttäytymisenä. Tietoturvapolitiikka ja tietoturvasuunnitelma pitäisi siis tehdä näiden arvojen ilmaisemiseksi.

Ohjaamista ja opastusta tulisi olla erilaisissa arkipäivän tilanteissa, kuten ryhmäpalavereissa ja työntekijöiden välisissä keskusteluissa. Myös kouluttaminen/kouluttautuminen on ehdottoman tärkeää koska vain koulutuksella varmistetaan, että työntekijät ymmärtävät tietoturvaohjeita ja toimivat tietoturvan kannalta oikealla tavalla. Erityisesti työntekijät tarvitsevat esimerkkejä oman toimintansa seurauksista, koska sillä tavalla pystytään perustelemaan miksi joku toinen tapa toimia on parempi vaihtoehto.

Pk-yritysten johtajien/esimiesten tulisi myös pyrkiä tiedostamaan omat toimintatavat tietoturvan kannalta, koska arvovaltaisina henkilöinä he näyttävät työntekijöille esimerkkiä miten tietoturvan kannalta pitäisi toimia. Johtajat/esimiehet romuttavat hyvin helposti puheillaan jo aikaansaatua tietoturvallista toimintatapaa elleivät itse tiedän miten pitäisi toimia. Pk-yritysten johtajien/esimiesten pitäisi myös käyttää pk-yritysten vahvuuksiin liittyviä asioita hyväksi paremman tietoturvakulttuurin muodostamisessa. Näitä ovat mm. matala organisaatiorakenne ja muutoksiin tottunut organisaatio.

Avainsanat: Tietoturva Tietoturvakulttuuri Pk-yritys Ohje Riski

Sisällysluettelo

1 Johdanto

Tietoturva on paljon puhuttu asia tänä päivänä. Lehdistä saa usein lukea erilaisista tietoturvavaroituksista ja/tai tietoturvarikkomuksista. Jo pelkästään Suomessa tehdään lukuisia tietoturvarikkomuksia vuosittain. Syitä tähän tilanteeseen on monia, mutta suurin syy lienee kuitenkin nopea tekniikan kehitys, joka on muuttanut oleellisesti yritysten liiketoimintaa muutaman viime vuosikymmenen aikana.

Nopeat tietoliikenneyhteydet ja tietojärjestelmät

Yritykset hyödyntävät yhä enemmän tietojärjestelmiä liiketoiminnassaan, jolloin tieto on entistä useammin sähköisessä muodossa. Tietojenkäsittelyn toiminnot ovat yhä enemmän informaatio-, raha- ja tavaravirtoja liikuttelevia tietojenkäsittelyprosesseja. Vaihtoehtoista tapaa toiminnalle ei tänä päivänä usein enää ole olemassa. (Korhonen 2006.) Kauppa- ja teollisuusministeriön pk-yritysten tietoturvakyselyssä (pk-yritysten tietoturvakysely 2006 2007:4) ilmeni, että Suomi on tietoteknistynyt merkittävästi ja pienimmistäkin yrityksistä lähes puolet ilmoitti olevansa erittäin paljon tai paljon riippuvaisia tavanomaisimmista tietoteknisistä ratkaisuista. Saman tutkimuksen mukaan esimerkiksi 46 % pk-yrityksistä oli erittäin paljon tai paljon riippuvaisia taloushallinnon sähköisistä järjestelmistä. Vastaavasti asiakastietoon liittyvistä järjestelmistä oltiin riippuvaisia erittäin paljon tai paljon 45 % yrityksistä (pk-yritysten tietoturvakysely 2006 2007:4). Pk-yritysten toiminnassa on selvä ristiriita, koska työntekijöiden tietoturvallisen toiminnan kehittämiseen ei kuitenkaan ole panostettu yhtä paljon kuin uuden tekniikan käyttöönottoon.

Työn liikkuvuus

Tänä päivänä on myös yhä helpompi tehdä etätyötä. Työ ei ole aikaan ja paikkaan sidottua. Lisäksi tietoa on helppo kuljettaa töistä erilaisilla massamuistivälineillä ja viimeistellä vaikkapa kotona seuraavan päivän koulutustilaisuutta/esitystä. Koska työ ei ole sidottu paikkaan, mahdollistaa se työnantajalle säästöjä kiinteiden kulujen osalta. Kaikille työntekijöille ei tarvitse järjestää omaa kiinteää työpistettä, vaan työtä voidaan tehdä etätyönä. Etätyötä Suomessa tekeekin noin 100 000 ihmistä ja 90 000 ihmiselle päätyöpaikka on kotitoimisto. Lisäksi palkansaajista yli 40 % eli 900 000 henkilöä tekee liikkuvaa työtä ajoittain ja yli kolmannes on enemmän kuin päivän viikossa poissa työpisteestään (Kemppainen 2007:15). Työn ja sitä kautta tiedon liikkuminen kuitenkin muodostaa erilaisia tietoturvariskejä, jotka pitäisi aina ottaa huomioon työn liikkuvuuden suunnittelussa.

Esimerkiksi Ilona Iivosen (2006:35) diplomityössä, jossa tutkittiin tietoturvallisuutta pirkanmaalaisissa tietointensiivisissä pk-yrityksissä, yritykset totesivat, että erityisesti kotona tapahtuvan työskentelyn valvonta katsottiin käytännössä mahdottomaksi. Näin ollen yritykset voivat pohtia, onko etätyöstä käytännössä mitään kustannussäästöjä, jos esimerkiksi uudet innovaatiot leviävät ”kotisohvilta” eteenpäin. Etätyöstä on yri-

tyksille nopeita välittömiä säästöjä, mutta mitkä ovat etätyön pitkäaikaisvaikutukset?

Muiden liiketoiminnan vaatimusten vaikutukset tietoturvaan

Globalisaatio vaikuttaa väistämättä tietoturvaan. Globaalissa kilpailussa mikään ei enää pysy salassa. Yritysten siirtyminen kansainväliseen toimintaan tarkoittaa verkottumista uusien toimijoiden kanssa ja uusiin kulttuureihin tutustumista ja sopeutumista. Yrityksille on tarjolla halvempaa työvoimaa, mutta toisaalta taas ongelmia esimerkiksi teollisuusvakoilun muodossa. Teollisuusvakoilu voi aiheuttaa esimerkiksi uusien innovaatioiden, tutkimus- ja kehitystyön ja uuden kilpailukykyä tuovan teknologian päätymisen kilpailijoille. Tästä on jo todisteita väärennettyjen matkapuhelimien ja hyvin kaupaksi menevien muiden länsimaisten väärennettyjen merkkituotteiden osalta. Toimintojen siirtäminen esimerkiksi Aasiaan massatuotannon maihin näyttää yksiselitteisen helpolta. Huono puoli kuitenkin on, että Suomessa vaivalla kehitetty teknologia on nopeasti kopioitavissa eteenpäin kilpailijoiden käyttöön. Käytännössä uusien teknologioiden päätyminen kilpailijoiden käyttöön tarkoittaa yhä nopeampaa uusien teknologioiden kehittämistä ja niiden lanseeraamista uusien tuotteiden muodossa. Muutosnopeus on valtavaa, mikä taas nostaa osaamisen ja oppimisen organisaatioiden tärkeimmäksi pääomaksi. Tämä tarkoittaa, että aivovoima ja uudistuminen ovat kaiken perustana.

Yksi syy verkottumiseen uusien toimijoiden kanssa on myös se, että halutaan keskittyä ydinliiketoimintaan. Tästä syystä kaikki muu ns. turha pyritään ulkoistamaan muille toimijoille. Tämä johtaa verkostojen kasvamiseen myös globaalisti ja pitkien alihankintaketjujen muodostumiseen. Kun verkostoon tulee yhä enemmän toimijoita, joilla ei ole samoja toimintatapoja, syntyy myös erilaisia riskejä kuten esimerkiksi tietoriskejä. Organisaatioiden väliset kulttuurit törmäävät toisiinsa tässä mukana tietoturvakulttuurit. Nykypäivänä tekniset puitteet toimijoiden välillä on suhteellisen helppo hoitaa tietoturvaltaan samanlaiseksi, mutta toimijoiden välisen tietoturvakulttuurin yhtenäistäminen ei olekaan enää niin helppoa.

Tänä päivänä verkottuvat yritykset tarvitsevat yhä enemmän yksityiskohtaista tietoa toisistaan, jotta ne voivat luottaa toisen yrityksen toimintatapoihin. Ydinliiketoimintaan keskittyminen onkin pakollisen verkottumisen kautta tuonut paljon erilaisia riskejä joihin on nyt varauduttava. Kaikki verkostoon mukaan tulevat toimijat lisäävät esimerkiksi tietovuotoriskejä. Siksi erityisesti työntekijöiden huolellinen toiminta tietojen käsittelyn osalta on ensisijaisen tärkeää.

Tärkeäksi kysymykseksi tietoriskien vähentämisessä muodostuukin, miten näiden sekä kansallisissa että kansainvälisissä verkostoissa toimivien yritysten/organisaatioiden tietoturvakulttuuri saadaan yhtenäistettyä. Mitkä ovat ne tavat, että yhteistyössä toimivat yritykset pystyvät toimimaan kuin yksi suurempi yritys, jolla on samanlainen tietoturvakulttuuri? Ja varsinkin, miten pk-yritykset pystyvät vastaamaan tähän haasteeseen? Pk-yrityksille kun on ominaista olla usein mukana suuremman

toimijan palkkaamana alihankkijana. Alihankkijana oleminen tarkoittaa vastuuta palvelun tai tavaran tekemisestä tilauksen mukaisesti. Tietoturvan osalta se tarkoittaa myös sitä, ettei tuotteen tekemisen yhteydessä tule tietovuotoja, jotka voisivat aiheuttaa loppuasiakkaalle liiketoiminnallisia tappioita.

Liiketoimintaan liittyvä laatutekijä

On silti merkillepantavaa, että tietoturvallisuutta ei yrityksissä nykyisin nähdä liiketoimintaan olennaisesti liittyvänä laatutekijänä, vaan se mielletään usein tietotekniikka-asiantuntijoiden hoitamaksi tekniikaksi muiden tekniikoiden joukossa (Tietoturvatietoisuutta pk-yrityksiin 2005). Tietoturva on vaarallista nähdä pelkkänä tekniikkana. Tekniikan on oltava kunnossa, koska se luo puitteet tietoturvan toteuttamiselle. Lisäksi kuitenkin henkilöstön asenne ja koulutus tietoturvan osalta on nähtävä vähintäänkin yhtä tärkeänä kuin tekniikka. Varsinkin yritysjohdolla on merkittävä rooli tietoturvallisuuden luotsaamisessa sen strategisena suunnittelijana.

Samalla, kun suunnittelutyö ja koulutus tietoturvan osalta etenevät on yritysjohdon toimittava esimerkkinä muille työntekijöille. Johdon on turha luulla, että työntekijät noudattavat sääntöjä, jos johto ei itse niitä noudata. Hyvä tietoturva on pieniä tekoja ja se lähtee yrityksen työntekijöiden toiminnasta, osaamisesta ja asenteesta. Johdon toimesta työntekijöille jalkautetut tietoturvaohjeet yksin eivät auta, jos niitä ei ymmärretä tai jos ne sisältävät suurelta osin työntekijälle epäoleellista tietoa. Työntekijät tulisi ottaa mukaan ohjeiden tekemiseen, jotta työntekijät saadaan niitä myös noudattamaan ja ymmärtämään. On siis tärkeää, että työntekijät saadaan mukaan ohjeiden laadintaan ja muuhun tietoturvan kehittämistyöhön.

Omat työntekijät parhaita tietolähteitä

Tietoturvan kehittämisen kannalta onkin merkille pantavaa, että siellä olevat työntekijät ovat parhaita tietolähteitä analysoimaan yrityksen toiminnassa olevia ja mahdollisesti syntyviä riskejä. Toisin sanoen työntekijät analysoivat omaa toimintatapaansa, koska yrityksen toiminnot koostuvat työntekijöiden toiminnoista. Joskus kuitenkin tarvitaan ulkopuolinen konsultti ohjaamaan tietoturvallisuustyön tekemistä, keskustelun kulkua ja tekemään keskustelusta yhteenveto. Usein varsinkaan pk-yrityksen sisällä ei ole ammattitaitoista henkilökuntaa tällaisen suunnittelun ohjaamiseen. Pk-yritysten johtajilta/esimiehiltä pitäisi silti vaatia tietoturvaosaamista ja tietoturvaan liittyvien asioiden käsittelyä yrityksissä.

1.1 Tutkintotyön tavoite ja metodi

Tämän tutkintotyön tavoitteena on laatia pk-yritysten johtajille ja esimiehille ohje siitä, miten yrityksen tietoturvakulttuuria voidaan ohjata tietoturvallisempaan suuntaan. Tavoitteeseen pääsemiseksi tutkintotyössä vastataan seuraaviin tutkimuskysymyksiin:

- Miten kirjoitetaan hyvä ohje?
- Miten yrityskulttuuri vaikuttaa henkilöstön tietoturvakäyttäytymiseen?
- Mitä yleisiä ongelmia yrityksissä on esiintynyt tietoturvakulttuurin edistämisessä?
- Mitkä ovat pk-yrityksen vahvuudet ja heikkoudet jotka osaltaan vaikuttavat tietoturvakulttuurin muodostumiseksi?
- Miten johtajat/esimiehet voivat toimillaan vaikuttaa paremman tietoturvakulttuurin muodostumiseen pk-yrityksissä?

Tutkintotyössä kuvataan tietoturvallisuuden ongelmia pk-yritysten henkilöstön osalta. Ongelmat esitetään jo tehtyjen tutkimusten pohjalta. Tutkimusmetodina työssä käytetään valmiiden aineistojen analyysiä. Analyysin tarkoituksena on tuoda esille olemassa olevien tutkimusten valossa, miten henkilökunta pystyy omalla toiminnallaan parantamaan yrityksen tietoturvaa. Ohje johtajille/esimiehille kirjoitetaan analyysin tuloksien perusteella.

Jatkossa tässä työssä sekä tämän työn liitteenä olevassa ohjeessa käytetään yrityksen ylimmästä johdosta ja esimiehistä lyhennetysti nimitystä esimies. Tällä pyritään helpottamaan tutkintotyön ja ohjeen luettavuutta. Luonnollisesti myös yrityksen ylin johto katsotaan esimiehiin kuuluviksi.

1.2 Tutkintotyön rajaukset

Kun kuvataan henkilöstön tietoturvalliseen käyttäytymiseen liittyviä ongelmia, voidaan niiden todeta olevan todella monimuotoisia ja jopa mahdottomia analysoida. Onhan kyse kuitenkin ihmisen tekemisestä ja käyttäytymisestä, mikä ei joka tilanteessa ole loogista. Lisäksi tekemiseen ja käyttäytymiseen vaikuttavat monet seikat. Näitä asioita voivat olla työpaineet, yleiset työolot, työkaverit, tieto-/taitotaso, perhesuhteet, esimiehen johtamistapa, yleinen asenne työntekoon jne. Tämän tutkimuksen puitteissa ei kuitenkaan ole mahdollista ottaa kantaa jokaiseen käyttäytymiseen liittyvään seikkaan, joten tutkimusta on rajattu tietyin osin. Tässä tutkimuksessa paneudutaan siihen, kuinka työntekijän tieto-/taitotasoa voidaan nostaa ja ylläpitää tietoturva-asioiden osalta sekä siihen, miten esimiehet voivat omalta osaltaan vaikuttaa työntekijöiden tietoturvallisempaan tekemiseen ja käyttäytymiseen.

Tutkimusta rajataan lisäksi koskemaan vain pk-yrityksiä. Pk-yrityksillä on tietoturvan osalta tiettyjä tunnusomaisia piirteitä, jotka erottavat ne suurista yrityksistä.

2 Ohjeistuksen kirjoittaminen

Useimmat ohjeet on kirjoitettu jonkun teknisen laitteen käyttämisen helpottamiseksi. Siksi myös suurin osa ohjeiden kirjoittamiseen liittyvistä oppaista on kirjoitettu antamaan neuvoja, miten kirjoittaa jonkun teknisen laitteen käyttöohje. Näistä oppaista löytyy kuitenkin yleishyödyllisiä ohjeita, joita voidaan soveltaa myös tässä tapauksessa ajatellun tietoturvaohjeistuksen kirjoittamiseen.

Ohjeita ja oppaita tarvitaan, kun kehitetään muun muassa uusia toimintatapoja tai tuotantomenetelmiä (Kauppinen, Nummi & Savola 2004:102). Kauppinen ym. (2004:102) toteavat, että ohjeen kirjoittajan on hyvä pitää mielessään tiettyjä ohjeen kirjoittamiseen liittyviä lähtökohtia. Ensimmäinen lähtökohta on, että kärsimättömänkin lukijan mielenkiintoa tulisi pitää yllä. Asia pitäisi esittää kirkkaasti. Lukijan tulisi pystyä etenemään vaiheesta toiseen jouhevasti, joten jonkinasteista täsmällisyyttä tulisi noudattaa. Lisäksi lukijaa tulisi osata opastaa nopeasti ja vaivatta oikean asiakohdan äärelle.

Kauppinen ym. (2004:102) toteavat myös, että usein on tarpeellista kertoa lukijalle suorasanaisesti, miksi ohjeiden lukeminen on tärkeää. Tämä johtuu siitä, että ihmisillä on yleensä taipumus ryhtyä nopeasti toimeen ja jättää ohjeet lukematta (ibid.). Suorasanainen kertominen ohjeiden tärkeydestä liittyy ehkä enemmän teknisten laitteiden ohjeisiin. Tämän tutkintotyön tuloksena syntyvässä ohjeessa tulisi kuitenkin perustella lukijalle ohjeiden tarpeellisuutta ja ennen kaikkea se, kenelle ohje on tarkoitettu.

2.1 Ennen ohjeen kirjoittamista

Ennen ohjeen kirjoittamista täytyisi ensimmäisenä miettiä laitteen rakenne ja toiminta (Kauppinen ym. 2004:104). Tässä tilanteessa ei kuitenkaan ole kysymys teknisen laitteen ohjeistuksesta, vaan enemmänkin toimintaohjeesta ja/tai suosituksesta. Silti tässä tapauksessa ohjeeseen tulisi tehdä taustatutkimusta ohjeen tulevasta käyttökontekstista. Ohjetta tullaan käyttämään pk-yrityksissä. Tulisi siis selvittää mitä yleisesti tarkoitetaan pk-yrityksellä ja mitkä asiat sanelevat ehtoja pk-yrityksen tietoturvan kehittämiselle.

Ennen ohjeen kirjoittamista tulisi myös miettiä kenelle ja mihin tarkoitukseen ohje laaditaan. Lisäksi täytyisi kuvitella ohjeen tyypillinen käyttötilanne. (Kauppinen ym. 2004:104.)

2.2 Ohjeen ulkoasu

Ohjekirjan ulkoasun on mahdollistettava asioiden nopea löytyminen ja houkuteltava selailemaan ohjetta toteavat Kylänpää ja Piirainen (2002:115). Esimerkiksi sivunumero on asemoitava paikkaan, josta sen löytää heti (ibid.). Ohjeen eri alueilla voi olla erilainen marginaalikuvio tai teksti- visuaalisena hakuvinkkinä (Kylänpää & Piirainen 2002:115).

Formaatti, silmäiltävyys ja rakenne

Ohjeen täytyy olla kätevä käyttää. Käyttämiseen kätevyyteen vaikuttavat käyttöympäristön olosuhteet mahdollisuuksineen ja rajoituksineen, joten ne on hyvä ottaa heti alkuvaiheessa huomioon toteavat Kylänpää & Piirainen (2002:115). Ohjeen suunnitteluvaiheessa tulisikin ottaa huomioon ohjeen *formaattiratkaisut*, *silmäiltävyysratkaisut* ja *rakenneratkaisut* (ibid.). *Formaattina* voi olla esim. paperipainatus, CD-julkaisu tai vaikkapa nettiohje. Ohjeen *silmäiltävyyteen* liittyvät muun muassa tekstityyppi, otsikointi, taulukointi, numerointi, erilaiset tekstimuotoilut, laatikointi, sävypohjat, värit, kuvat, kuvaajat jne. *Rakenneratkaisuissa* tulisi huomioida tarvittava tietomäärä, tietojen järjestys ja toiston riittävyys, sisällysluettelo sekä sana- ja asiahakemisto.

Ohjeen kuvitus

Ohjeen kuvituksen tulisi olla havainnollista ja informatiivista. Valokuvat, graafiset kuvaajat ja piirrokset sekä taulukot ja luettelot lisäävät tietoa ja helpottavat viestin ymmärtämistä, jos niihin ei ole ahdettu liikaa informaatiota. (Kylänpää & Piirainen 2002:116.)

Ohjetta laadittaessa on kuitenkin muistettava yksi tärkeä seikka: pelkistetty ja yksinkertainen on tyylikästä ja viestinnällisesti tehokasta.

2.3 Ohjeen jäsentäminen

Aina ensimmäisenä ohjeessa tulisi selvittää esim. laitteen normaali käyttö (Kauppinen ym. 2004:104). Materiaalin karttuessa ohjeen rakennetta tulisi hahmotella käyttötilanteiden edellyttämään järjestykseen toteavat Kylänpää ja Piirainen (2002:119). Samanaikaisesti voidaan erotella käyttötilanteen vaatimia informaatiotyyppejä, joita voivat olla esim. yleisohjeet, vaiheittain etenevät toimintaohjeet, varoitukset, huomautukset ja täsmennykset (ibid.). Ohjeosuuksien tavoite tulisi myös pitää kirkkaasti mielessä toteavat Kylänpää ja Piirainen (2002:119).

Tässä tilanteessa, kun kirjoitetaan tietoturvaohjetta pk-yrityksen esimiehille, normaali käyttö voisi vastata yleisiä tietoturvallisuuteen liittyviä asioita, jotka ainakin täytyy olla kunnossa jokaisessa pk-yrityksessä. Tämän lisäksi voidaan erotella muita mahdollisia informaatiotyyppejä, kuten tarkistuslistoja yrityksen tietoturvan tämän hetkisestä tilasta tai vaikkapa täsmennyksiä tärkeimmistä tietoturvaan liittyvistä asioista.

Lisäksi tulisi ennakoida käyttäjän tavallisimmat ongelmat (Kauppinen ym. 2004:104). Tässä ohjeessa tavallisimmat ongelmat ovat esimiehen eteen tulevia arkipäiväisiä ongelmia esim. henkilökunnan tietoturvallisuuskäyttäytymisen parantamisessa.

Ohje pitäisi vielä rakentaa johdonmukaiseksi kokonaisuudeksi ja noudattaa käyttäjän toimintojen aikajärjestystä (Kauppinen ym. 2004:104). Ehkä teknisen laitteen käyttöohjeen saa johdonmukaiseksi kokonaisuudeksi mutta, kun puhutaan laajasta ohjeesta, joka on tarkoitettu osin ajatellen

ihmisten johtamista, epäjohdonmukaisuuksia varmasti tulee eteen. Lisäksi voidaan kysyä, milloin ohje on johdonmukainen. Kaikille käyttäjille edes teknisen laitteen ohjeistusta ei välttämättä saa johdonmukaiseksi. Johdonmukaisuus on paljolti kiinni ohjeen käyttäjästä. Käyttäjän toimintojen aikajärjestys voidaan tämän ohjeen osalta saada ainakin osittain sellaiseksi, että se on kaikille käyttäjille loogisesti etenevä. Mutta ohjeessa tulee välttämättä toimia, jotka eivät ole sidottu tiettyyn aikajärjestykseen. Kuten tiedetään, hyvän tietoturvan ylläpito on jatkuva prosessi eikä yksittäinen projekti. Näin ollen toimia ei voi sitoa tiettyyn aikajanaan. Lisäksi esimerkiksi Kylänpää ja Piirainen (2002:118) toteavat, että käyttöohjeen kirjoittajan on otettava huomioon myös oletettava lukutapa. Ohjetta ei yleensä lueta kannesta kanteen, vaan sieltä haetaan ratkaisua ongelmaan tai tietoa kuten hakuteoksesta tai sanakirjasta (ibid.). Tämänkään vuoksi ohjetta ei voida täysin sitoa tiettyyn aikajärjestykseen. Mutta ohje pitäisi silti olla hyvin käytettävä toteavat Kylänpää ja Piirainen (2002:118). Ohjeesta pitäisi helposti löytyä ratkaisu ohjeen aihepiiriä koskeviin ongelmiin.

Ohjeen lopussa voidaan käyttää tarvittaessa luettelomaisia yhteenvetoja muistuttamassa aihealueen pääkohdista. Yhteenveto voi olla osittain graafinen ja osoittaa, miten aihealue liittyy kokonaisuuteen (Kylänpää & Piirainen 2002:120).

2.4 Ohjeita kirjoitettaessa

Ohjeen kieliasu

Ohjeita kirjoitettaessa tulisi käyttää mahdollisimman helppoa ja selkeää kieltä toteavat Kauppinen ym. (2004:104). Lisäksi ohje pitäisi pitää Kylänpään ja Piiraisen (2002:120) mukaan mahdollisimman lyhyenä ja yksinkertaisena, koska monimutkaisten tekstien tulkitsemisen yksiselitteisyys on vaikeaa ja jopa mahdotonta. Ymmärrettävyyden tekijäksi mielletään usein pelkästään sanasto, mutta tosiasia on, että myös lauserakenteet vaikuttavat (ibid.). Tämän vuoksi pitkät ja monista lauseista koostuvat virkkeet on lyhennettävä ja tehtävä ne helpoiksi tulkita (Kylänpää & Piirainen 2002:120). Virkerakenne pitäisi olla sellainen, että ensin kerrotaan mitä tehdään ja sen jälkeen perustellaan miksi näin tehdään (ibid.).

Jälleen on kyse esimerkiksi teknisen laitteen käyttöön liittyvästä ohjeen kirjoittamisesta. Osittain nämä samat asiat pätevät myös tämän tutkintotyön tuloksena syntyvään ohjeeseen, mutta ohjeessa tulee varmasti kohtia, jotka eivät ole yksiselitteisiä tai jotka kuuluvat enemmän suosituksen kuin yksiselitteisen ohjeen piiriin.

Viittaukset vai toisto

Viittaukset tekstistä kuviin ja päinvastoin tulisi olla selkeitä ja täsmällisiä Kylänpään ja Piiraisen (2002:116) mukaan. Lisäksi Kylänpää ja Piirainen (2002:120) toteavat, että ohjeen kirjoittajan tulisi pyrkiä tekemään ohje sellaiseksi, ettei käyttäjän tarvitse hyppiä ohjeessa edestakaisin.

Näin ollen viittaukset muihin lukuihin tulisi ohjeessa jättää mahdollisimman vähäisiksi ja keskittyä enemmän toistamaan asioita useampaan kertaan. Myös Kauppisen ym. mukaan (2004:104) toistoa pitäisi käyttää aina, kun siihen on tarvetta. Lisäksi Kylänpää ja Piirainen (2002:120) korostavat toiston tärkeyttä erityisesti silloin, kun käyttöohjeen luvut ovat itsenäisiä kokonaisuuksia, joita oletetaan käyttäjän tarkastelevan tarpeeseensa yhtä kerrallaan.

Samasta asiasta tulisi käyttää aina samaa nimitystä, esimerkiksi joko painike tai näppäin, ei molempia (Kauppinen ym. 2004:104).

Ohjeen luonnostelu ja testaus

Alkuun ohjeesta tulisi kirjoittaa luonnos, josta pyydetään palautetta ohjeen käyttäjiltä toteavat Kauppinen ym. (2004:104). Luonnosteluvaihe on pääasiassa tiedonhakua, tietojen yhteensovittamista, yhteyksien ymmärtämistä ja pyrkimystä ilmaista asioita mielekkäässä järjestyksessä ja riittävän tiiviisti, mutta aina ymmärrettävästi (Kylänpää & Piirainen 2002:118). Lopulta ohje pitäisi testata vielä tositilanteessa (Kauppinen ym. 2004:104).

3 Ohjeen sisältö

Ohjeen sisältö liittyy pk-yritysten tietoturvaan. Ohje on tarkoitettu pääasiassa pk-yrityksissä toimiville esimiehille ja muille johtavassa asemassa oleville työntekijöille. Ohjeen sisältö liittyy tietoturvaan joka tehdään työntekijöiden ja hyvän johtamisen avulla, ei niinkään tekniikan avulla. Vaikka tekniikka on tärkeässä asemassa ajatellen yrityksen tietoturvallisuutta, on yrityksen työntekijöiden omalla toiminnalla huomattavasti suurempi merkitys.

Ohjeen sisällössä käydään läpi syitä tietoturvallisuuden laiminlyöntiin. Tähän liittyvät mm. työnkuvan muuttuminen, työntekijöiden koulutuksen laiminlyönti, tietoturvaohjeiden noudattamatta jättäminen ja esimiesten toimiminen huonona esimerkkinä. Lisäksi ohjeessa kerrotaan pk-yritykselle ominaisista tietoturvallisuustyöhön liittyvistä asioista, tiedon suojaamisen lähtökohdista, tietoturvan kehittämisen lähtökohdista henkilöstön osalta, henkilöstön ohjaamisesta/johtamisesta ja kouluttamisesta tietoturvatyöhön sekä lopuksi vielä pk-yrityksen vahvuuksista paremman tietoturvakulttuurin luomisessa. Ohje esimiehille on tämän tutkintotyön liitteenä.

Miksi ohje pk-yrityksille?

Ohje tehdään pk-yrityksille, koska yleisesti ottaen tietoturva-asiat ovat pk-yrityksissä huonommin hoidettu verrattuna suuriin yrityksiin. Suurissa yrityksissä tietoturva-asiat ovat usein jo kunnossa. Tämä johtuu tietoturvaan liittyvien töiden lukuisasta määrästä, jonka vuoksi niiden hoitamiseen kannattaa erikseen palkata työntekijä/työntekijöitä. Pk-yrityksissä tilanne on erilainen johtuen mm. työntekijöiden laajasta toimenkuvasta. Yksi henkilö joutuu hoitamaan useita eri tehtäviä, jotka suuressa yrityksessä olisi annettu eri henkilöiden hoidettavaksi. Toimenkuvan laajuus aiheuttaa vain pinnallista osaamista kultakin osa-alueelta. Näin käy myös tietoturvan osalta. Osaamiskentän laajuus johtaa myös kiireeseen ja työtehtävien suunnittelemattomuuteen, jolloin tehdään se mikä on prioriteettilistalla ykkösenä. Henkilöt eivät ehdi keskittymään itsensä kehittämiseen saati sitten yrityksen sisäiseen kehittämiseen. Pk-yrityksissä on siis harvoin tietoturvaan liittyvää erikoisosaamista. Siksi varsinkin tekninen tietoturva pyritään usein ulkoistamaan erilliselle toimijalle.

Tietoteknisen tietoturvan ulkoistamisesta huolimatta pk-yritysten henkilöstön pitäisi osata toimia tietoturvallisesti. Tekniikka luo vain puitteet sille, että henkilöstö voi toimia tietoturvallisesti jos niin haluaa/osaa. Koska pk-yritysten esimiehet ovat olennainen osa pk-yritysten tietoturvallisuuden toteutumista, tämän tutkintotyön tuloksena syntyvä ohje pyrkii antamaan yksinkertaisia neuvoja pk-yritysten esimiehille tietoturvallisempaan toimintaan. Näin ainakin yksinkertaisimmat tietoturvaan liittyvät sudenkuopat saadaan karsittua yrityksen liiketoiminnasta.

4 Riski käsitteenä

Aluksi tarkastellaan riskiä käsitteenä, koska tietoturvallisuus kuuluu yrityksen yleiseen riskienhallintaan, mikä täytyy ottaa huomioon liiketoiminnassa. Tietoturvallisuuden osalta puhutaan yrityksen tietoriskeistä, kuten Tuija Kyrölä kirjassaan Esimies ja tietoriskien hallinta.

Riski tarkoittaa haitallisen tapahtuman todennäköisyyttä ja vakavuutta (Riskin arviointi 2003:6). Riski sanaa käytetään kuvaamaan sitä vaaraa ja epätietoisuutta, joka liittyy onnettomuuden mahdollisuuteen. Aikain saatossa riskin määrä ja sisältö on lisääntynyt ja riskit ovat tulleet yhä monimutkaisemmiksi (Kuusela & Ollikainen 1999:16). Alkuvaiheissa ihmisten suurimpia riskejä olivat ravinnon löytäminen ja riskien hallinnan tavoitteena olivat elossa pysyminen ja lajin säilyminen (ibid.). Riskiin liittyy tappion mahdollisuus ja menettämisen uhka. Olennainen riskiin liittyvä tekijä on *epävarmuus*. Emme varmuudella tiedä tulevia tapahtumia, vaikka tunnemme tapahtumien todennäköisyyksiä. Todennäköisyyksiin liittyy kuitenkin virhearvioinnin mahdollisuus ja joissakin tapauksissa ihmiset suhtautuvat liian luottavaisesti omiin riskiarvioihinsa. Usein riski koetaankin henkilön subjektiiviseksi näkemykseksi lopputuloksesta. Näin ollen riskiarviot vaihtelevat henkilöiden välillä. Lisäksi on selvää, että riskinäkemys muuttuu myös tietotason muuttuessa. (Kuusela & Ollikainen 1999:17.)

Riski on epävarmuutta jonkun negatiivisen asian todennäköisyydestä

Epävarmuus vaikuttaa riskin toteutumiseen monella tavalla. Riskin sanotaan olevan olemassa, kun negatiivinen lopputulos on ennalta arvaamaton ja odottamaton. Päätöksentekijät eivät usein tiedosta tai havaitse omien päätöstensä haitallisia vaikutuksia. Vaikka negatiivisten tapahtumien mahdollisuus tiedostetaan, ei voida olla varmoja, milloin ja minkä laajuisina tai suuruisena tapahtumat toteutuvat. *Epävarmuus* ulottuu täydellisestä tietämättömyydestä laskennallisiin todennäköisyyksiin. Todennäköisyydet voivat perustua muutamaan kokemusperäiseen tapaukseen tai laajaan tietopohjaan. (Kuusela & Ollikainen 1999:18.)

Osa ihmisistä on riskisietoisempia ja haluavatkin ottaa riskejä. Toiset taas pelaavat varman päälle. Jotkut aliarvioivat riskejä ja toiset taas yliarvioivat niitä. Riskien yliarviointi voi johtua esimerkiksi siitä, että tietyistä riskeistä puhutaan ja kirjoitetaan paljon. Esimerkiksi usein toistuvia ja laajasti uutisoituja riskejä yliarvioidaan. (Kuusela & Ollikainen 1999:18.) Kun yliarvioidun riskin pienentämiseen käytetään paljon voimavaroja, voi olla, että nenän edessä olevan ilmeisen riskin arviointi jää kokonaan huomioon ottamatta. Myös riskin arvioijan tietoisuustaso mahdollisista riskeistä vaikuttaa tähän. Siksi riskienhallintaan liittyy olennaisena osana aina asiantuntevat henkilöt, jotka osaavat kartoittaa riskit aiempien kokemustensa ja tietopohjansa kautta. Riskien kartoittamisen ja todennäköisyyksien arvioinnin jälkeen riskeihin on mahdollista tietoisesti varautua ja tehdä niiden varalle toimenpiteet.

5 Yrityksen riskienhallinta

Yritystoimintaan kohdistuu kaikissa olosuhteissa lukemattomia erilaisia riskejä. Yleiseen yrityksen riskienhallinnan piiriin voi kuulua esimerkiksi taulukossa 1 lueteltuja riskejä (Pk-yrityksen riskienhallinta):

Taulukko 1. Yritystoimintaan liittyviä yleisiä riskejä.

Yritystoiminnan yleisiä riskejä	
ympäristöriskit	projektiriskit
henkilöriskit	keskeytysriskit
liikeriskit	tietoriskit
tuoteriskit	rikosriskit
sopimus- ja vastuuriskit	paloriskit

Yrityksen riskienhallinta on siis erittäin laaja käsite. Varsinkin suuressa yrityksessä riskienhallinta kaikilta osin on erittäin oleellinen liiketoimintaan liittyvä tekijä. Suominen (1999:134) on todennut, että perinteisesti riskit on jaettu vahinko- ja liikeriskeiksi. Tämä jako palvelee erityisesti vakuutusratkaisuihin liittyviä tarpeita. Vahinkoriskit ovat periaatteessa vakuutuskelpoisia mutta liikeriskit eivät (ibid.).

Riskienhallinta muodostaa yrityksen omaisuutta, sen henkilöstöä, osaamista ja liikesuhteita turvaavan suojajärjestelmän. Riskienhallinta edellyttää käytännössä erilaisten riskienhallintamenetelmien tuntemista ja aktiivista käyttöä. On selvää, että riskienhallinnan tarpeet ja toteuttamistavat vaihtelevat merkittävästi yrityksen koosta ja toimialasta riippuen. Suuri monialayritys tarvitsee aivan erilaisen suojajärjestelmän verrattuna pieneen yritykseen joka valmistaa muutamaa tuotetta. (Suominen 1999:135.)

Riskienhallinta on kompromisseja ja suunnitelmallisuutta

Eri riskienhallintakeinot ovat ominaisuuksiltaan ja kustannusvaikutuksiltaan erilaisia. Usein riskien poistaminen kokonaan ei ole mahdollista, koska tällöin yrityksen tulisi oikeastaan luopua kokonaan harjoittamastaan liiketoiminnasta. Riskin välttäminen saattaa silti olla toteutettavissa ilman merkittävää panostusta. (Suominen 1999:135.)

Käytännössä liiketoiminnassa on koko ajan olemassa olevia riskejä, joita karttamalla yritys voi tehdä tuottoisampaa liiketoimintaa. Toisaalta riskienhallintakeinot ja niiden aiheuttamat kustannukset täytyy olla tasapainossa liiketoimintaan nähden tai muussa tapauksessa voi käydä niin, että riskienhallintakeinoihin käytetyt kustannukset syövät yrityksen tulosta. Riskienhallintaan ei voi käyttää määräänsä enempää resursseja, mutta kuitenkin jonkinlainen suojajärjestelmä olisi rakennettava. Käytännössä tämä tarkoittaa, että yrityksellä on aina jonkinlainen harkittu riski harteillaan. Joskus riski on pienempi ja joskus suurempi. Jossakin tapauksessa riski voi olla hyvinkin suuri, mutta suunnitelmallinen esimerkiksi tilanteessa, jossa haetaan nopeaa liiketoiminnan kasvua. Täl-

löin kyseessä on riski, jonka toteutumattomuuteen voidaan vaikuttaa suunnittelemalla riskinotto hyvin.

Riskinottoon liittyy riskin arviointi ja sen suunnitelmallinen toteuttaminen. Samalla tavalla yrityksen turvallisuusnäkökohtien osalta erilaiset turvallisuusriskit tulisi ensin listata ja sen jälkeen tehdä riskien arviointi. Riskien arviointi on laaja-alaista ja järjestelmällistä riskien tunnistamista ja niiden merkityksen arvioimista (Riskien arviointi 2003:6). Ennen kaikkea se on työpaikan normaalia toimintaa eikä harvoin tapahtuvaa konsultin erikoistoimintaa (Kerko 2001:57). Riskien arvioinnin jälkeen tehdään tulosten pohjalta vaadittavat toimenpiteet, joilla varaudutaan riskin ennalta ehkäisemiseen. Riskien toteutumiseen varautuminen voidaan taas katsoa liiketoiminnan jatkuvuuden suunnitteluksi. Tämä suunnittelutyö tulisi tehdä ainakin niille riskeille, jotka toteutuessaan voivat johtaa liiketoiminnan loppumiseen. Tämä kaikki työ kuuluu joka tapauksessa yrityksen riskienhallinnan piiriin.

6 Mitä on yritysturvallisuus?

Kuten edellä on todettu, yrityksillä on lukuisia muitakin riskejä kuin turvallisuusriskit, mutta niitä ei käsitellä tässä työssä. Riskienhallinta kuitenkin liittyy aivan samalla tavalla turvallisuusriskien arviointiin kuin mihin tahansa muiden riskien arviointiin. Riskienhallinnan keinojen avulla voidaan arvioida esimerkiksi yritysturvallisuuden tilaa. Yritysturvallisuus tarkoittaa yrityksen kaikkien turvallisuusasioiden yhtenäistä tulostavoitteita tukevaa kokonaishallintaa (Kerko 2001:21).

Yritysturvallisuuden avulla yritys pyrkii varmistamaan liiketoimintansa häiriöttömän päivittäisen jatkumisen suojaamalla henkilöstöä, asiakkaita, sidosryhmiä, tietoja, omaisuutta ja toimintaympäristöä vahingoilta, väärinkäytöiltä ja rikolliselta toiminnalta (Miettinen 2002:11). Yritysturvallisuus on kiinteä osa yrityksen toimintaa ja tukee yrityksen tulostavoitteita. Sillä on myös paljon vaikutusta yrityskuvaan, yrityksen tuotteisiin ja palvelun laatuun toteaa Miettinen (2002:11). Käytännön turvallisuustyö on Kerkon (2001:21) mukaan ennalta ehkäisevää toimintaa onnettomuus- ja vaaratilanteiden sekä vahinkojen torjumiseksi ja toimintavalmiuksien luomista näiden tilanteiden varalta.

Yritysturvallisuus kattaa koko yrityksen turvallisen toiminnan kirjon ja se voidaan jakaa useaan osa-alueeseen. Miettisen (2002:14) mukaan tärkeimmät osa-alueet ovat alla listattuna. Hänen jaottelunsa noudattelee pääpiirteissään Teollisuuden ja työnantajain keskusliitto ry:n, Palvelutyönantajat ry:n ja näiden noin 12 000 jäsenyrityksen muodostaman Yritysturvallisuuden neuvottelukunnan määrittelemää jaottelua.

1. yritysturvallisuuden johtaminen
2. kiinteistö- ja toimitilaturvallisuus
3. henkilöturvallisuus
4. vakuuttaminen
5. tietoturvallisuus
6. poikkeusoloihin varautuminen
7. paloturvallisuus ja pelastustoiminta
8. ympäristönsuojelu
9. ulkomaantoimintojen yritysturvallisuus
10. matkustusturvallisuus
11. rikosturvallisuus
12. työsuojelu
13. tuotannon ja muun toiminnan yritysturvallisuus

Kuten huomataan, tietoturvallisuus on vain yksi osa-alue yrityksen kokonaisturvallisuuden varmistajana. On kuitenkin selvää, että muut yritysturvallisuuden osa-alueet vaikuttavat merkittävästi myös tietoturvallisuuden varmistamiseen. Lisäksi kaikki yritysturvallisuuden osa-alueet

ovat toisiinsa nähden osittain sisäkkäisiä ja toimivat yhtenäisenä ketjuna. Siksi on perusteltua käydä läpi ensin yrityksen kokonaisturvallisuutta.

Yritysturvallisuus on osana yrityksen yleistä riskienhallintaa

Yritysturvallisuuden kehittämisessä ei ole kyse minkään erillisen asian kehittämisestä, vaan yritysturvallisuusasiat tulisi ottaa huomioon yrityksen jokaisessa toimintaprosessissa ja niiden kaikissa vaiheissa toteaa Miettinen (2002:23). Yritysturvallisuuden kehittäminen on jatkuva dynaaminen prosessi, joka elää yrityksen toimintaprosessien elinkaaren mukaisesti (ibid.).

Yritysturvallisuuden eri osa-alueisiin kohdistuu lukematon määrä erilaisia riskejä, ja niiden hallitsemiseksi yritys tarvitsee selkeät menettelytavat. Yrityksen yleiseen riskienhallintaan kehitetyt toimintamallit soveltuvat usein myös yritysturvallisuusriskien hallintaan, ja tätä kautta yrityksen riskienhallinta ja yritysturvallisuus usein sivuavat toisiaan läheisesti eri yhteyksissä. (Miettinen 2002:28.)

Miettinen (2002:28) toteaa myös, että yritysturvallisuusriskien hallinta on kiinteä osa yrityksen muuta riskienhallintaa, ja siksi tavoitteet tulee olla yhteneväiset yrityksen muun riskienhallinnan tavoitteiden kanssa. Tästä seuraa, että yrityksen yleisen riskienhallinnan ja yritysturvallisuuden kehittämisestä ja ylläpidosta vastaavien tulee olla yhteistyössä keskenään (ibid.).

7 Mitä on tietoturvallisuus?

Tietoturvallisuus on sisällöltään laaja ja varsin abstrakti käsite (Miettinen 2002:129). Termillä tietoturvallisuus tarkoitetaan tavoitetilaa, jossa tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojaa niin, että niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen (käytetään myös: saatavuus) kohdistuvat uhat eivät aiheuta merkittävää vahinkoa yhteiskunnalle ja sen jäsenille (Valtionhallinnon tietoturvakäsitteistö 2003:51). Tietoturvallisuus pitää sisällään myös lainsäädännön ja muut normit sekä toimenpiteet, joiden avulla tiedot, tietojärjestelmät ja palvelut pyritään varmistamaan niin normaali- kuin poikkeusoloissa (ibid.).

7.1 Tietoturvallisuuden peruselementit

Miettisen (2002:129) mukaan tietoturvallisuuden tärkeimmät peruselementit ovat eheys, luottamuksellisuus ja saatavuus. Luottamuksellisuus tarkoittaa hänen mukaansa, että yrityksen tiedot ovat ainoastaan niiden henkilöiden ja tahojen käytettävissä, jotka tarvitsevat niitä. Luottamuksellisuus tarkoittaa siis tietojen suojaamista niiden luvatonta käyttöä vastaan. Esimerkiksi tietojärjestelmien tietojen luottamuksellisuutta suojataan käyttäjätunnuksin ja salasanoin.

Miettinen (2002:129) jatkaa eheyden tarkoittavan, että yrityksen toiminnassaan tarvitsema tieto ei muodostu tai häviä itsestään ja tieto pysyy alkuperäisenä eli virheettömänä tiedon elinkaaren sekä tietojenkäsittelyn eri vaiheiden aikana. Tiedon eheyttä tietoliikenteessä suojataan esimerkiksi tietoliikenteen salaamisella eli kryptaamalla siirrettävä tieto sellaiseen muotoon ettei se ole selväkielistä.

Saatavuus Miettisen (2002:129) mukaan taas tarkoittaa, että yrityksen tarvitsemat tiedot ovat sen käytettävissä silloin, kun niitä tarvitaan ja niitä voidaan käyttää niin pitkään kuin on tarpeellista. Tiedon saatavuutta suojataan esimerkiksi peilipalvelimilla, levyjärjestelmillä ja tietoliikenneverkon varalaitteilla.

7.2 Tietoturvallisuuden jaottelu

Tietoturvallisuuden toteuttamisessa on tapana erottaa kahdeksan toimenpidealuetta: hallinnollinen, henkilöstö-, fyysinen, tietoliikenne-, laitteisto-, ohjelmisto-, tietoaineisto- ja käyttöturvallisuus (Valtionhallinnon tietoturvakäsitteistö 2003:51). Tosin näistä toimenpidealueista on olemassa myös 7-, 9- ja 10-kohtaisia määritelmiä riippuen siitä, kuka on ollut kirjoittajana tai milloin kirja tai artikkeli on kirjoitettu.

Esimerkiksi Miettinen (2002:130) jakaa tietoturvallisuuden yhdeksään osa-alueeseen, jotka ovat hallinnollinen, ohjelmisto-, laitteisto-, tietoaineisto-, tietojenkäsittelyn, tietoliikenteen-, käyttötoimintojen turvallisuus ja immateriaalioikeuksien suojaaminen sekä yksityisyyden suoja. Aiemmassa kirjassaan Tietoturvallisuuden johtaminen Miettinen (1999:5) puolestaan erottelee tietoturvallisuuden kymmeneen eri osa-alueeseen, jotka ovat hallinnollinen-, henkilö-, toimitila-, tietojenkäsittelyn-, tieto-

liikenteen-, laitteisto-, ohjelmisto-, käyttötoimintojen- ja tietoaineistoturvallisuus sekä yksityisyyden suoja.

Tämän lisäksi vielä Hakala, Vainio ja Vuorinen (2006:10) jakavat tietoturvallisuuden seitsemään eri osa-alueeseen, jotka ovat hallinnollinen, fyysinen, henkilö-, tietoaineisto-, ohjelmisto-, laitteisto- ja tietoliikenneturvallisuus. Näitä tietoturvallisuuden osa-alueita olen sekaannuksien välttämiseksi pyrkinyt vertailemaan taulukossa 2. Vertailuun on otettu Miettisen osalta vain tuoreempi vuoden 2002 jaottelu, joka kirjoittajan mielestä on varmasti relevantimpi.

Taulukko 2. Tietoturvallisuuden osa-alueiden jaottelu eri kirjoittajien kesken.

Miettinen, Juha E. Yritysturvallisuuden käsikirja (2002).	VAHTI. Valtionhallinnon tietoturvallisuuden johtoryhmä (2003)	Hakala, Mika ym. Tietoturvallisuuden käsikirja (2006).
Hallinnollinen turvallisuus	Hallinnollinen turvallisuus	Hallinnollinen turvallisuus
	Fyysinen turvallisuus	Fyysinen turvallisuus
	Henkilöstöturvallisuus	Henkilöturvallisuus
Tietoaineistoturvallisuus	Aineistoturvallisuus	Tietoaineistoturvallisuus
Ohjelmistoturvallisuus	Ohjelmistoturvallisuus	Ohjelmistoturvallisuus
Laitteistoturvallisuus	Laitteistoturvallisuus	Laitteistoturvallisuus
Tietoliikenteen turvallisuus	Tietoliikenneturvallisuus	Tietoliikenneturvallisuus
Tietojenkäsittelyn turvallisuus		
Käyttötoimintojen turvallisuus	Käyttöturvallisuus	
Yksityisyyden suoja		
Immateriaalioikeuksien suojaaminen		

7.2.1 Hallinnollinen tietoturvallisuus

Kaikissa kolmessa vertaillussa tapauksessa hallinnollinen tietoturvallisuus määritellään lähes samalla tavalla. Miettinen (2002:131) määrittelee, että hallinnollinen tietoturvallisuus on osa-alue, jossa tarkastellaan mm. yrityksen tietoturvallisuuden toimintapolitiikkaa, toiminnan linjauksia, johtamista, organisointia, sijoitusta yrityksessä, toiminnan resursointia ja tietoturvallisuuden vastuumäärittelyjä.

Valtionhallinnon tietoturvakäsitteistössä (2003:11) vastaavasti todetaan, että hallinnollinen tietoturvallisuus määrittelee tietoturvallisuuteen tähtäävät hallinnolliset keinot, kuten tehtävien ja vastuiden määrittelyt sekä henkilöstön ohjeistuksen, koulutuksen ja valvonnan.

Hakala ym. (2006:10) toteavat, että hallinnollisella turvallisuudella pyritään varmistamaan tietoturvan johtaminen ja kehittäminen. Siihen liittyvät myös yhteydenpito eri turvallisuudesta vastaaviin elimiin ja organisaation sisällä ja ulkopuolella toimiviin viranomaisiin (ibid.).

7.2.2 Fyysinen turvallisuus

Valtionhallinnon tietoturvakäsitteistön (2003:10) mukaan fyysinen turvallisuus on henkilöiden, laitteiden, aineistojen, postilähetysten, toimitilojen ja varastojen suojaamista tuhoja ja vahinkoja vastaan. Se sisältää kulun- ja tilojen valvonnan, vartioinnin, palo-, vesi-, sähkö-, ilmastointi ja murtovahinkojen torjunnan sekä kuriirien ja tietoaineistoja sisältävien lähetysten turvallisuuden.

Sen sijaan Hakalan ym. (2006:11) mukaan fyysiseen turvallisuuteen kuuluvat rakennuksen tilojen ja niihin sijoitettujen laitteiden suojaaminen erilaisilta fyysisiltä uhkilta. Fyysisen turvallisuuden ylläpidosta vastaavat yleensä kiinteistöhuollon ja vartiointialan ammattilaiset.

Lisäksi Ruohonen (2002:4) toteaa, fyysisen tietoturvallisuuden tarkoittavan niiden fyysisten tilojen suojaamista, joissa tietojärjestelmä sijaitsee. Hänen mukaansa fyysisen turvallisuuden ei välttämättä ajatella kuuluvan tietoturvallisuuteen, mutta sillä on kuitenkin olennainen merkitys tietojärjestelmän suojaamisessa. Kenen tahansa ei pidä päästä sellaisten tietokoneiden luokse, jotka sisältävät yrityksen tärkeitä liiketoimintaan liittyviä tietojärjestelmiä.

7.2.3 Henkilöstöturvallisuus

Valtionhallinnon tietoturvakäsitteistön (2003:13) mukaan henkilöturvallisuus tarkoittaa henkilöstöön liittyvien tietoturvariskien hallintaa. Siihen kuuluvat henkilöstön soveltuvuuden, toimenkuvien, sijaisuuksien, tiedonsaanti- ja käyttöoikeuksien, suojaamisen, turvallisuuskoulutuksen ja valvonnan hallinta.

Hakalan ym. (2006:11) mukaan henkilöstöturvallisuuteen kuuluvat puolestaan toimet, joilla varmistetaan tietojärjestelmän käyttäjien toimintakyky ja rajataan heidän mahdollisuuksiaan käyttää organisaation tietoja ja tietojärjestelmiä. Näihin toimiin kuuluvat varamiesjärjestelyt, tietojärjestelmiin liittyvän koulutuksen järjestäminen, tietojärjestelmiä koskevien vastuiden ja oikeuksien määrittely sekä erityistapauksissa mahdollisten taustatietojen selvittäminen.

Ruohosen (2002:5) mukaan henkilöturvallisuus tarkoittaa tietojärjestelmän suojaamista sen käyttäjien aiheuttamilta uhilta. Tähän kuuluvat mm. käyttäjien opastaminen tietojärjestelmän käyttämiseksi sekä käyttäjän taustojen tarkastaminen, jotta esimerkiksi petoksesta tuomittu henkilö ei pääse vastaamaan ei-julkisten tietojen varmuuskopioinnista (ibid.).

Miettinen (2002:103) ei pidä henkilöturvallisuutta tietoturvallisuuden osa-alueena, vaan yritysturvallisuuden osa-alueena. Myös tietoturvallisuus on yksi yritysturvallisuuden osa-alue, joten Miettinen oikeastaan rinnastaa henkilöturvallisuuden ja tietoturvallisuuden. Miettinen selvittää henkilöturvallisuutta varsin seikkaperäisesti teoksessaan. Hänen mukaansa siihen kuuluvat henkilön taustatietojen tarkastaminen, toimenpiteet työ- tai sopimussuhteen alkaessa ja päättyessä, uhkaustilanteiden kä-

sittely, henkilön fyysisen koskemattomuuden suojaus, avainhenkilöiden suojaaminen ja salassapitosopimukset.

7.2.4 Tietoaineistoturvallisuus

Kaikissa kolmessa vertaillussa tapauksessa mainitaan tietoaineistoon liittyvä turvallisuus (tietoaineistoturvallisuus tai aineistoturvallisuus). Miettisen (2002:132) mukaan tietoaineistoturvallisuus liittyy yrityksen käyttämien tietoaineistojen tunnistamiseen ja varsinkin tietojen suojaamiseksi toteutettu tietojen turvaluokituskäytäntö eli käytännössä tietojen järjestelmällinen luokittelu esim. salaisiin, julkisiin, luottamuksellisiin jne.

Valtionhallinnon tietoturvakäsitteistön (2003:1) mukaan aineistoturvallisuus on asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden ylläpitämiseksi keinoina muun muassa tietoaineistojen luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen. Valtionhallinnon tietoturvakäsitteistön määrittelemä aineistoturvallisuus on Miettisen määrittelyä laajempi. Tietoaineiston hävittäminen kuuluu Miettisen määrittelyn mukaan tietojenkäsittelyn turvallisuuteen (ks. tietojenkäsittelyn turvallisuus).

Hakala ym. (2006:11) ovat esittäneet, että tietoaineistoturvallisuuteen kuuluvat tietojen säilyttämiseen, varmistamiseen ja palauttamiseen sekä tuhoamiseen liittyvät toimet. Tiedon luokittelusta ei kuitenkaan ole mainintaa Hakalan ym. (2006:11) tietoaineistoturvallisuuden määrittelyssä.

7.2.5 Ohjelmistoturvallisuus

Miettinen (2002:168) on kirjoittanut, että ohjelmistoturvallisuudessa tarkastellaan tietokoneohjelmien suojaamiseen liittyviä asioita kuten: ohjelmiston pääsynvalvonta, ohjelmiston tapahtumatietojen seuranta, tietojen ja ohjelmien varmuuskopiointi, asianmukainen dokumentaatio, ohjelmien ylläpito- ja huoltosopimukset ja rekisteröityjen ohjelmistojen käyttö. Valtionhallinnon tietoturvakäsitteistön (2003:28) mukaan ohjelmistoturvallisuus on käyttöjärjestelmiin ja muihin ohjelmistoihin kohdistuvien toimien, kuten ohjelmistojen tunnistamis-, eristämis-, pääsynvalvonta- ja varmistusmenettelyt, tarkkailu- ja paljastustoimet, lokimenettelyt ja laadunvarmistus sekä ohjelmistojen ylläpitoon ja päivitykseen liittyvät toimet tietoturvallisuuden parantamiseksi.

Hakala ym. (2006:11) ovat maininneet, että ohjelmistoturvallisuuteen kuuluvat sovellusten sopivuus suunniteltuun käyttötarkoitukseen, ohjelmistojen keskinäinen yhteensopivuus ja toiminnan luotettavuus ja virheettömyys sekä ohjelmistoversioiden ja lisenssien hallinta. Ohjelmistoturvallisuuden osalta näiden kolmen lähteen voi todeta olevan lähes yhteneviä. Kaikkein lähimpänä toisiaan ovat kuitenkin Valtionhallinnon tietoturvakäsitteistön ja Miettisen määritelmät.

7.2.6 Laitteistoturvallisuus

Laitteistoturvallisuudessa tarkastellaan Miettisen (2002:166) mukaan teknisten laitteiden suojaamista. Laitteistoturvallisuus kattaa kaikki yrityksen tekniset laitteet. Laitteistoturvallisuuden tärkeimmät perussuojausmenetelmät ovat pääsynvalvonta laitteeseen, laitteiston tapahtumatietojen kerääminen, luotettava varaosien saanti, laitteiden varmentaminen kriittisissä kohteissa, laitteiden energiansaannin varmistaminen, asianmukainen laitteistodokumentaatio sekä huolto- ja ylläpitosopimukset (ibid.).

Valtionhallinnon tietoturvakäsitteistön (2003:23) mukaan laitteistoturvallisuus on puolestaan tietojenkäsittely- ja tietoliikennelaitteiden ja tilojen käytettävyyteen, toimivuuteen, kokoonpanojen määrittelyyn ja pääsynvalvontaan sekä varaosien ja tarvikkeiden saatavuuteen liittyvät toimet tietoturvallisuuden toteuttamiseksi.

Hakala ym. (2006:12) ovat todenneet, että laitteistoturvallisuuteen liittyvät tietokoneiden ja muiden tietojärjestelmään kytkettyjen laitteiden tarkoituksenmukainen mitoitus, toiminnan testaus, huollon järjestäminen sekä varautuminen laitteiden kulumiseen ja vanhenemiseen.

Myös nämä tietoturvan osa-alueet vastaavat vertailluissa lähteissä pääosin toisiaan.

7.2.7 Tietoliikenneturvallisuus

Tietoliikenteen suojaamisella yritys pyrkii varmistamaan, ettei sen tietoliikenneyhteyksiä ja -palveluita käytetä väärin, toteaa Miettinen (2002:144). Tietoliikenteen turvallisuuteen liittyy kiinteän puhelinverkon turvallisuus esimerkiksi tietoliikenteen salaaminen yleisessä televerkossa. Lisäksi siihen liittyvät lanka- ja GSM puhelimien sekä telefaxin ja sähköpostin turvallinen käyttäminen. Miettinen (2002:145) antaa ohjeita tietoliikenneturvallisuuden osalta jopa puhelinvastaajan käyttöön ja tilanteisiin, joissa puhutaan puhelimeen työasioista julkisella paikalla.

Valtionhallinnon tietoturvakäsitteistön (2003:48) mukaan tietoliikenneturvallisuus on tavoitetila, jossa tietoturvallisuus on toteutettu tietoliikenteen laitteiden, järjestelmien ja niissä kulkevien tietojen osalta. Tietoliikenteen turvallisuuteen kuuluvat myös lainsäädäntö, normit ja toimet, joilla tietoliikenteen turvallisuus pyritään aikaansaamaan (ibid.). Tietoliikenneturvallisuuden toteuttamiseen liittyviä keinoja ovat laitteistojen ja siirtoyhteyksien ylläpito ja niiden kokoonpanojen hallinta, verkonhallinta, pääsynvalvonta, tietoliikenteen käytön valvonta ja tarkkailu, ongelmatilanteiden kirjaaminen ja selvittäminen, viestinnän salaus ja varmistaminen sekä tietoliikenneohjelmien testaus ja hyväksyminen.

Hakala ym. (2006:12) ovat kirjoittaneet, että tietoliikenneturvallisuudessa huolehditaan tiedonsiirtoratkaisujen, kuten lähi- ja laajaverkkoyhteyksien sekä muiden viestintäjärjestelmien turvallisuudesta.

Kaikki lähteet ajavat pääosin samaa asiaa tietoliikenneturvallisuuden osalta. Tekniikan lisäksi Miettinen on kuitenkin ottanut omaan tietoliikenneturvallisuuden määrittelyynsä mukaan ihmisten tietoturvalliseen käyttäytymiseen liittyviä seikkoja, jotka useampien muiden määrittelyjen kuten Valtionhallinnon tietoturvakäsitteistön ja Ruohosen mukaan kuuluvat henkilöstöturvallisuuden osa-alueelle.

7.2.8 Tietojenkäsittelyn turvallisuus

Miettinen (2002:137) on todennut, että tietojenkäsittelyn turvallisuus käsittää työasemien suojaamisen, tietokonevirusten torjunnan ja tietoaineiston käytöstä poiston sekä hävittämisen. Muut aikaisemmin mainitsemani lähteet eivät käsittele tietojenkäsittelyn turvallisuutta erillisenä tietoturvallisuuden osa-alueena.

7.2.9 Käyttötoimintojen turvallisuus tai käyttöturvallisuus

Miettinen (2002:158) on sanonut, että käyttötoimintojen turvallisuudessa tarkastellaan kaikkia ihmisen suorittamia manuaalisia ja atk-järjestelmillä hoidettavia yrityksen päivittäisen käyttötoiminnon rutiineja. Yrityksen tietojenkäsittelyn rutiinien hoito tulisi tapahtua asianmukaista huolellisuutta noudattaen valvotusti kaikissa tilanteissa. Tällä turvallisuuden osa-alueella on Miettisen (2002:159) mukaan yhtymäkohtia laitteisto- ja ohjelmistoturvallisuuteen. Käyttötoimintojen turvallisuuteen liittyy käyttöoikeuksien hallinta, laitteisiin ja järjestelmiin kytkeytyminen, salasanojen hallinnointi, laitteiden ja järjestelmien käytön valvonta, kriittisten tehtävien hajautus ja varmuuskopiointi (ibid.).

Valtionhallinnon tietoturvakäsitteistö (2003:22) käyttää tästä tietoturvallisuuden osa-alueesta termiä käyttöturvallisuus. Sen mukaan käyttöturvallisuus on tietotekniikan käyttöön, käyttöympäristöön, tietojenkäsittelyyn ja sen jatkuvuuteen sekä tuki-, ylläpito-, kehittämis- ja huoltotoimintoihin liittyvät keinot tietoturvallisuuden parantamiseksi.

Ruohonen (2002:5) määrittelee käyttöturvallisuuden tarkoittavan, että tietojärjestelmää käytetään turvallisesti. Hänen mukaansa käyttöturvallisuus liittyy suoraan henkilöstöturvallisuuteen, sillä järjestelmää huolimattomasti ja/tai ohjeiden vastaisesti käyttävät henkilöt heikentävät käyttöturvallisuutta. Tämä saattaa johtaa esimerkiksi siihen, että järjestelmässä on helposti murrettavia salasanoja.

7.2.10 Yksityisyyden suoja

Ainoastaan Miettinen (2002:170) on määritellyt yksityisyyden suojan kuuluvaksi tietoturvallisuuden osa-alueeseen. Verrattuna ovat olleet lähteet Miettinen (2002), Ruohonen (2002), Valtionhallinnon tietoturvakäsitteistö (2003) ja Hakala ym. (2006). Miettinen (2002:170) on todennut, että yksityisyyden suoja (tietosuoja) on osa-alue, jossa tarkastellaan erityisesti yrityksen toimintaan liittyvien henkilöiden henkilötietojen suojaamista. Näitä henkilöitä voivat olla mm. yrityksen henkilöstö, asiakkaat ja yhteistyökumppanit. Suomessa yksityisyyden suojaa säädellään

melko tarkasti lainsäädännössä. Lainsäädäntö asettaakin erityisvaatimuksia yrityksille niiden käsittelemien henkilötietojen suojausten suunnittelulle, toteutukselle ja ylläpidolle.

7.2.11 Immateriaalioikeuksien suojaaminen

Ainoastaan Miettinen (2002:171) on määritellyt myös immateriaalioikeuksien suojaamisen kuuluvaksi tietoturvan osa-alueisiin. Jälleen on verrattu keskenään lähteitä Miettinen (2002), Ruohonen (2002), Valtionhallinnon tietoturvakäsitteistö (4/2003) ja Hakala ym. (2006). Miettisen (2002:171) mukaan immateriaalioikeuksien suojaaminen tarkoittaa, että yritys tai yksityishenkilö hyödyntää lainsäädännön mahdollisuuksia kohteen omistus- ja hallintaoikeuden suojaamisessa muiden menetelmien lisäksi. Immateriaalioikeuksien suojalla pyritään estämään esimerkiksi kohteen tai sen osan luvaton kopiointi tai jäljentäminen (ibid.). Immateriaalioikeuksien suojalla yritys voi vaatia suojaamiensa tuotteiden käytöstä korvauksia itselleen, jos toinen yritys haluaa käyttää suojattua kohdetta omassa toiminnassaan.

Lisäksi Miettinen (2002:171) on kirjoittanut, että immateriaalioikeuksien peruskäsitteitä ovat patentti, hyödyllisyysmalli, mallisuoja, tuotemerkki, tekijänoikeus ja liikesalaisuus. Jokaisella maalla on omat menettelytapansa immateriaalioikeuksien suojaamiseen (ibid.). Tämä tuokin varmasti huomattavan paljon haasteellisuutta kansainväliseen liiketoimintaan.

7.2.12 Lähteiden vertailu ja luotettavuus

Tietoturvallisuuden osa-alueet on eri lähteissä määritelty toisaalta hyvin samalla tavalla, mutta erojakin löytyy, kuten edellä nähtiin. Eräät lähteet määrittelevät ja käsittelevätkin tietoturvallisuutta yksinomaan tietoteknisestä näkökulmasta. Toiset puolestaan ottavat mukaan myös muita yrityksen tietoturvallisuuteen kuuluvia asioita, kuten edellä oleva immateriaalioikeuksien suojaus. Lähteiden eroavaisuus tulee esille tilanteessa, jossa tarkastellaan kirjoittajan ammatillista suuntautuneisuutta. Toisaalta myös kohderyhmällä, eli kenelle kirja on kirjoitettu, on vaikutusta kirjoitusnäkökulmaan. Joka tapauksessa tietoteknisesti suuntautunut tarkastelee lähes ainoastaan yrityksen tietoturvaan liittyviä riskejä tietoteknisestä näkökulmasta. Näin on tehnyt esimerkiksi Ruohonen (2002) kirjassaan Tietoturva, kuten myös Hakala ym. (2006) kirjassaan Tietoturvallisuuden käsikirja.

Tietoturvallisuuden ammattilainen osaa ottaa huomioon kuitenkin koko tietoturvallisuuden kirjon, josta yrityksen tulisi pystyä huolehtimaan. Esimerkiksi Miettinen (2002) on erittäin ansiokkaasti kirjoittanut koko yrityksen tietoturvallisuuteen liittyvistä asioista eikä tarkastele pelkästään yrityksen tietoteknistä puolta, mikä kuitenkin on erittäin tärkeässä asemassa tietoturvan ylläpitämisessä. Juha E. Miettinen on toiminut mm. Soneran yritysturvallisuusjohtajana. Sittemmin häntä on tosin syytetty törkeästä viestintäsalaisuuden rikkomisesta.

VAHTI on Valtionhallinnon tietoturvallisuuden johtoryhmä. Johtoryhmän ohjeet löytyvät Valtiovarainministeriön sivuilta www.vm.fi. VAHTI toimii valtion tietoturvallisuuden kehittämisohjelmassa ja sen ohjeistoa täydennetään jatkuvasti. VAHTI johtoryhmään kuuluu useita tietoturvapäälliköitä ja tietoturva-asiantuntijoita. Johtoryhmän tavoitteena on parantaa valtionhallinnon toimintojen luotettavuutta ja jatkuvuutta tietoturvallisuutta kehittämällä sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi valtionhallinnon kaikkea toimintaa (Valtionhallinnon tietoturvallisuuden johtoryhmä.) Johtoryhmän toiminnasta ja ohjeiden ansiokkuudesta kertoo mm. vuonna 2006 saatu Tieturin Data Security Award -palkinto (Vuoden 2006 Tieturi Data Security Award Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI:lle).

8 Mitä tieto on?

Aiemmin on käsitelty riskiä terminä. Nyt on hyvä käsitellä vielä termiä tieto ja sitä mitä tieto on, jotta saamme kokonaiskuvan tietoriskeistä. Useissa tietojohtamisen kirjoissa erotellaan tieto, informaatio ja data toisistaan. Esimerkiksi Grönroos (2003:116) on todennut, että data on tiedon pienin rakennusosa. Data on mikä tahansa merkki tai merkkijono, joka sisältää informaatiota. Data voi olla vaikkapa pitkiä ykkösen ja nollan sarjoja tai kiinankielen symboleja. Kummatkaan eivät sano mitään sellaiselle henkilölle, joka ei osaa tulkita niitä. Ja vaikka osaisimme tulkitakin niitä, niin tulkitsemallamme informaatiolla ei ole mitään arvoa, ellemme osaa soveltaa sitä käyttöömme. Tämä tarkoittaa sitä, että ensin merkit täytyy osata tulkita informaatioksi, minkä jälkeen saamamme informaatio täytyy osata soveltaa vielä tiedoksi. Tämän jälkeen voimme jalostaa soveltamamme tiedon edelleen informaatioksi, joka on käyttökelpoista tietyssä ympäristössä tai tehtävässä.

8.1 Inhimillinen tieto jaetaan kolmeen osaan

Tietojohtamisessa inhimillinen tieto voidaan jakaa edelleen kolmeen lajiin jotka ovat: eksplisiittinen, hiljainen ja uusi tieto. Eksplisiittinen tieto on informaatiota. Tämä tarkoittaa käytännössä sitä, että se on tietoa joka on helppo ymmärtää eikä vaadi selittämistä tai tulkintaa. Informaation vastaanottajan on helppo yhdistää informaatio oman kokemusmaailmansa kanssa ilman kenenkään apua. Voimme sanoa esimerkiksi, että tietokone käsittelee dataa bitteinä. Tällöin vastaanottajalla täytyy olla tietysti tietyt perustiedot. Hänen tulee tietää, mitä tarkoitetaan tietokoneella, datalla ja bitillä. Muussa tapauksessa tämä informaatio on hänelle hyödytöntä. Eksplisiittinen tieto (informaatio) on siis tietoa, jota voimme omaksua painetusta sanasta kuten kirjasta, tietokoneen ruudulta ja lehdistä. (Grönroos 2003:117.)

Toinen inhimillisen tiedon osa on hiljainen tieto. Grönroosin (2003:117) mukaan hiljainen tieto on henkilösidonnaista ja sitä on vaikea siirtää muille. Hiljainen tieto voi olla vaikkapa käden taitoa, ongelmien ratkaisukykyä ja muuta sellaista, mitä henkilö osaa ja mitä on vaikea kirjoittaa paperille tai jakaa muille työntekijöille vaivattomasti. Hiljainen tieto on siis tietoa, jota olemme opetelleet ja osaamme teknisesti. Joku on oppinut soittamaan pianoa, toinen taas pelaamaan biljardia, kolmas taas osaa jonkun uuden laitteen käyttämisen jne. Hiljaisen tiedon ominaisuuksiin kuuluu, että sitä on vaikea tai jopa mahdoton siirtää muille. Työntekijät voivat olla lisäksi haluttomia siirtämään tällaista tietoa muille henkilöille, koska katsovat, että ovat sen tiedon ja taidon vuoksi vielä töissä ja saavat nauttia palkkaa.

8.2 Arvokas tieto

Yllä olevien määritelmien mukaan kaikkein arvokkainta tietoa on periaatteessa hiljaisen tiedon ja eksplisiittisen tiedon yhdistelmä tietyssä oikeanlaisessa ympäristössä, jossa on esimerkiksi oikeat työkalut ja muut välineet. Jos joku näistä kolmesta puuttuu, niin esimerkiksi tuotetta tai palvelua ei pystytä tekemään tai kehittämään. Tässä tapauksessa myös ympäristö sisältää tietoa. Esimerkiksi pelkästään jo työympäristöstä eli työkaluista (laitteista ja muista välineistä) voidaan saada selville, mitä yrityksessä tutkitaan ja kehitetään.

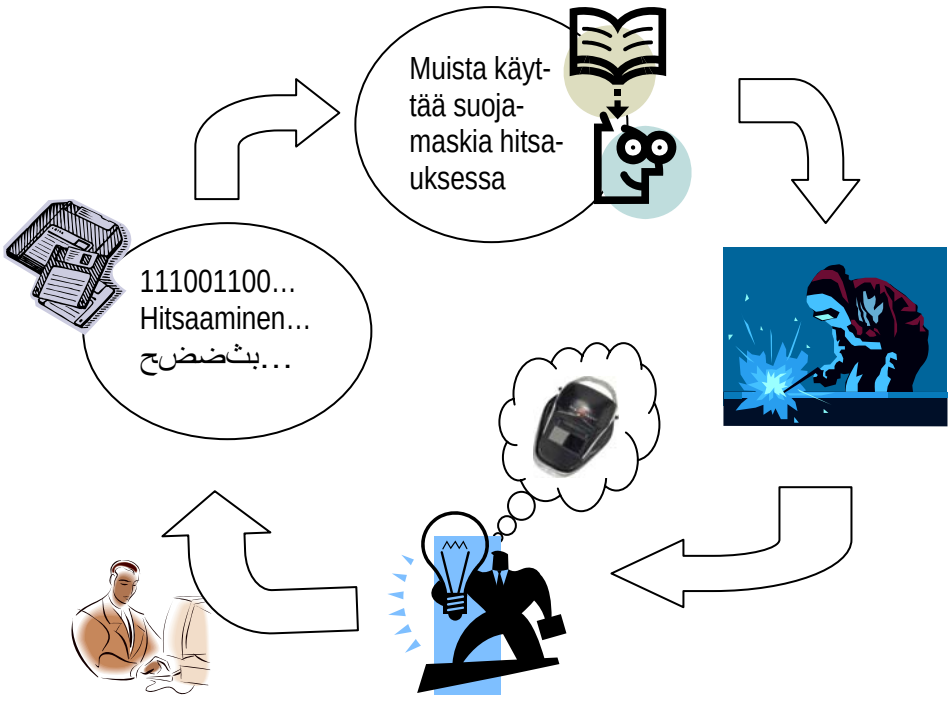
Kuvio 1. Tiedon erilaiset olomuodot (mukaillen Tuija Kyrölää 2001:25).

Yritystoiminnassa muodostuu välttämättäkin yrityksen liiketoimintaan liittyvää arvokasta tietoa, jota on kuvattu yllä olevassa kuviossa 1. Jos ei tällaista tietoa muodostu, voidaan kysyä, miksi yritys ylipäätään on olemassa. Yritystoiminnan alussa tieto voi olla eksplisiittisessä muodossa ja julkisesti saatavilla, mutta kun tämä tieto yhdistetään oikeanlaisessa työympäristössä tietynlaiseen osaamisalueeseen eli hiljaiseen tietoon, jota palkatuilla työntekijöillä on, alkaa yritykselle muodostua hiljalleen arvokasta yrityksen käyttöön jalostettua tietoa. Tämä tieto voi olla esimerkiksi jonkin tuotteen tai palvelun kehittämiseen liittyvää tietoa. Tämä jalostettu tieto muuttuu yrityksessä edelleen fyysiseen tai sähköiseen olomuotoon eli eksplisiittiseksi tiedoksi. Kun edelleen tämä eksplisiittinen tieto yhdistetään oikeanlaiseen hiljaiseen tietoon ja työympäristöön, saadaan lisää edelleen jalostettua tietoa.

Kuvion 2 kiertokulku kuvaa kyseistä tiedon kiertoa. Kun tämä kiertokulku toistuu tarpeeksi monta kertaa, niin yritykselle muodostuu palvelu tai tuote jota voidaan myydä eteenpäin. Ennen kuin mitään päästään kuitenkaan myymään on yrityksen oltava hereillä esimerkiksi tällaisen tuotekehitysprosessiin liittyvien tietoriskien osalta. Onhan tämän kaiken tie-

don tuottamiseen käytetty suuri määrä resursseja. On palkattu työntekijöitä, ostettu/vuokrattu toimitilat, ostettu oikeanlaiset työvälineet ja tietolähteet ja maksettu kaikenlaisia muita kuluja, joita yritystoimintaan kuuluu. Lisäksi on voitu hakea toiminnan rahoittamiseksi vielä julkista rahoitusta. Rahoittajina voivat olla pääomasijoittajat, piensijoittajat, TEKES, Suomen itsenäisyyden juhlarahasto (SITRA) tai muita vastaavia rahoittajia. Jos tällaisessa tapauksessa kehitetyn tuotteen tiedot joutuvat vääriin käsiin voi kyseessä olla jo kansallinen ongelma, eikä pelkästään yhden yrityksen ongelma.

Näin ollen näitä kaikkia tiedon osa-alueita on suojattava tavalla tai toisella, ettei yrityksen kilpailukyky heikkene tai liiketoiminta keskeydy. Työympäristön ja työkalujen sekä myös hiljaisen tiedon suojaamiseen käytetään yritysturvallisuuden kuten esimerkiksi vakuuttamiseen ja toimitila- ja kiinteistöturvallisuuteen liittyviä keinoja. Eksplisiittisen tiedon turvaamiseen käytetään tietoturvallisuuden kuten esimerkiksi ohjelmistoturvallisuuteen, laitteistoturvallisuuteen ja tietoaineistoturvallisuuteen liittyviä keinoja.



Kuvio 2**.** Tiedon kiertokulku, jossa hitsaamisessa opitaan ensin käyttämään suojamaskia, jonka jälkeen työtä helpottamaan kehitetään maski, jota ei tarvitse pitää kiinni toisella kädellä.

8.3 Tietoja on monessa muodossa

Kuten kuviosta 1 huomataan, tieto ei ole pelkkää kirjoitettua eksplisiittistä tietoa, joka sijaitsee esimerkiksi yrityksen tietojärjestelmässä. Tietoa on paljon eri muodossa. On henkilökohtaista osaamista ja kokemus-

tietoa, asiakirjoja, sopimuksia, ohjeita, suunnitelmia, palkkatietoja, asiakastietoja, tilaustietoja jne. Lisäksi tietojen tuottamisessa ja käsittelyssä käytetään erilaisia välineitä, ohjelmistoja ja ulkoisia palveluntarjoajia toteaa Kyrölä (2001:24). Käsiteltävät tiedot täytyy osata tunnistaa ja suojata tärkeät tiedot muuttumiselta, asiattomalta käsittelyltä, häviämiseltä ja paljastumiselta (ibid.). Tämä edellyttää Kyrölän (2001:24) mukaan, että tietoa käsittelevillä henkilöillä on kyky tunnistaa ja luokitella tietoja ja tietoa oikeanlaisista käsittelytavoista.

9 Tietoturva lähtee yritys-/organisaatiokulttuurista

Yrityksen tietoturva lähtee yrityskulttuurista. Yrityskulttuuri on sateenvarjo, jonka alle liittyvät mm. ihmisten käyttäytyminen, motivaatio, asenteet ja johtaminen, jos tarkastellaan ihmisten toimintaa yrityksen/organisaation osalta. Organisaatiokulttuuri on organisaation jäsenten muovaama ja omaksuma yhteinen käsitysmaailma (Karvinen 2004:10)[1]. Yrityksen osalta puhutaan yrityskulttuurista, mutta periaatteellisella tasolla samasta asiasta kuin organisaatiokulttuuri. Yrityskulttuuri ilmentää, millaisia uskomuksia ja toimintatapoja yrityksessä on ajan oloon omaksuttu (Yrityskulttuuri 2006 selvitys:1). Yrityskulttuuri on siis ajan saatossa työntekijöiden yhdessä omaksuttuja toimintatapoja, joiden pohjalta työntekijät toimivat usein myös tiedostamattaan. Yhteiset kokemukset ja oppiminen synnyttävät ajattelun, uskomukset ja arvot eli kulttuurin ryhmälle (Karvinen 2004:11). Yrityskulttuuri kehittyy pitkän ajan kuluessa ja vaikuttaa kaikkeen toimintaan työyhteisössä (Karvinen 2004:10). Tämän kulttuurin tunteminen on erittäin tärkeää, jotta yrityksen toimintoja voidaan kehittää eteenpäin. Yrityskulttuurilla on myös monia osa-alueita ja sitä voidaan tarkastella eri näkökulmista. Näitä osa-alueita Karvisen (2004:20) mukaan ovat johtamiskulttuuri, työkulttuuri, laatukulttuuri, palvelukulttuuri, viestintäkulttuuri jne. Tietoturvan osalta puhutaan tietoturvakulttuurista.

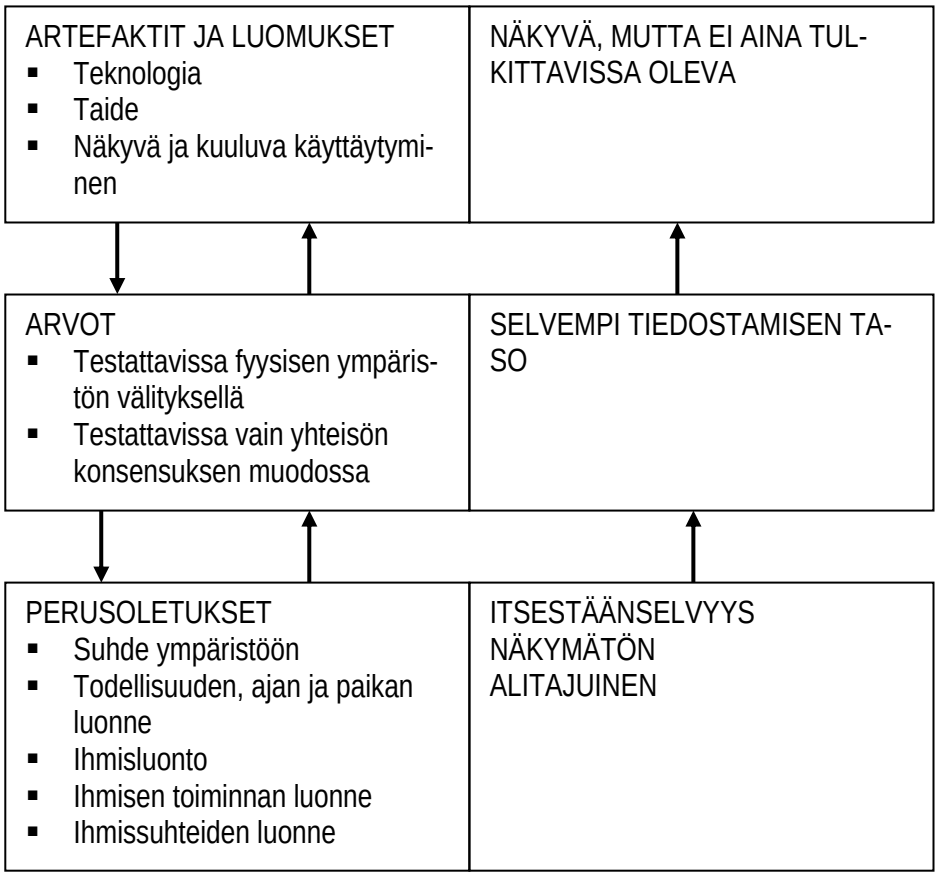
9.1 Yrityskulttuurin muodostuminen

Ennen paneutumista tarkemmin tietoturvakulttuuriin on hyvä tarkastella vielä yrityskulttuurin muodostumista. Yrityskulttuuri voidaan Scheinin (2001:30) mukaan jakaa kolmeen eri osaan. Nämä osat ovat näkyvä osa eli *artefaktit*, heti pinnan alla oleva osa eli *arvot* ja näkymätön osa eli *perusoletukset*.

Näkyvä osa eli artefaktit (ks. kuvio 3) tarkoittavat näkyvää osaa, joka ilmenee selvästi ulospäin työympäristöstä. Artefakteja voidaan löytää, kun tarkkaillaan ympäristöä ja ihmisten toimintaa. Niitä ovat näkyvät rakenteet kuten toimintatavat, työskentelytilat ja ihmisten havaittu käyttäytyminen esimerkiksi miten ihmiset käyttäytyvät toisiaan kohtaan. (Karvinen 2004:25, Petrow, Karsisto & Väänänen 2004:14.)

Syvemmälle yrityskulttuurissa päästään tutkimalla arvoja (ks. kuvio 3). Nämä arvot ovat kirjoitettuja arvoja ja usein julkisesti esillä esimerkiksi yrityksen nettisivuilla ja vuosikertomuksissa. Arvoissa voidaan mainostaa mm. henkilöstön tehokasta tiimityöskentelyä, vaikka asia olisi täysin päinvastoin. Nämä arvot siis ilmentävät sitä, miltä yritys haluaisi näyttää ulospäin. Työntekijät kertovat, että nämä ovat niitä arvoja joiden mukaan meillä toimitaan. Usein kuitenkin havaitaan näiden ulospäin näkyvien arvojen olevan vain mainoskikkoja ja eroavan todellisuudesta hyvinkin paljon. Arvoilla voidaan kuitenkin vaikuttaa ihmisten käyttäytymiseen, koska ne ilmaisevat, mitä pidetään toivottavana tai tavoittelemisen arvoisena käyttäytymisenä. (Karvinen 2004:26, Petrow ym. 2004:14.)

[1] Alkuperäinen lähde: Ahonen, Jorma & Pohjanheimo, Esa 2000. Asian ytimessä. Työkulttuurin kehittäminen oppivassa organisaatiossa. Helsinki: Yliopistopainotalo.



Kuvio 3. Scheinin kolme kulttuurin tasoa (Matikainen 1999:31)[2].

Perusoletukset (ks. kuvio 3) ovat sellaisia asioita, joita työntekijät eivät itsekään kyseenalaista tai eivät osaa tunnistaa. Siitä huolimatta työntekijät toimivat näiden perusoletusten mukaisesti. Perusoletukset ovat yhdessä opittuja ja sisäistettyjä ja niitä pidetään yrityksessä itsestään selvinä asioina. Nämä ovat ns. ”näinhän me ollaan aina toimittu” –asioita. Tällaiset ajattelu- ja toimintatavat syntyvät uskomuksista ja oletuksista, jotka on havaittu joskus toimiviksi. Myös uusi työntekijä oppii nopeasti nämä samat perusoletukset. Näiden perusolettamusten muuttaminen on erittäin vaikeaa, koska ne määrittelevät työntekijöiden käyttäytymisen säännöt ja niiden oletetaan ilman muuta olevan totta. (Karvinen 2004:26, Petrow ym. 2004:15.)

9.2 Tietoturvakulttuuri

Tietoturvakulttuuri on osa yrityskulttuuria, mutta sitä ei kuitenkaan voida pitää yrityskulttuurista erillisenä osa-alueena. Tietoturvakulttuurissa kuten myös organisaatio-/yrityskulttuurissa voidaan huomata kulttuuritasot eli artefaktit, arvot ja perusoletukset. Artefaktitasolla tietoturvallisuuskulttuuria voidaan tulkita ihmisten näkyvänä käyttäytymisenä, kuten käyttäjätunnusten ja salasanojen yhteiskäyttönä, salasanojen kirjoitteluna liimalapuille monitorin viereen tai luottamuksellisten paperidokumenttien jättäminen pöydille ilman huolta. Varsinkin ulkopuolinen havainnoit-

[2] Alkuperäinen lähde: Schein, Edgar H. 1987. Organisaatiokulttuuri ja johtaminen. Espoo: Weilin+Göös.

sija voi helposti havaita näitä epäkohtia, mutta siitä, miksi ihmiset näin käyttäytyvät onkin jo vaikeampi tehdä analyysiä. (Petrow ym. 2004:16.)

Arvojen osalta tietoturvallisuuskulttuuri näkyy työntekijöiden vaalimina arvoina. Työntekijät voivat mainostaa, kuinka paljon heidän yrityksessään panostetaan tietoturvaan ja kuinka motivoituneita he ovatkaan yrityksen tietoturvaohjeita noudattamaan. Kuten yllä todettiin, usein todetaan, että nämä yrityksestä ulospäin näkyvät arvot voivat vain olla mainoskikkoja ja ne voivat erota todellisuudesta hyvinkin paljon. Vaikka tietoturvamyönteistä ajattelutapaa vaalitaankin, työntekijät voivat silti käyttäytyä ristiriitaisesti arvoihin verrattuna. (Petrow ym. 2004:16.)

Ristiriitainen käyttäytyminen ei välttämättä ole silti tietoista, vaan se voi perustua juuri perusoletuksiin, joita työntekijät eivät itsekään kyseenalaista tai eivät osaa tunnistaa. Kun joku sitten asiaa kysyy, niin todetaan, että näinhän asiat on aina tehty. (Petrow ym. 2004:16.) Tällaisessa tilanteessa yritykseen tarvittaisiin joku ulkopuolinen henkilö herättelemään työntekijöitä. Itse opitut rutiinit, joita ei ole loppuun asti ajateltu voivat olla tietoturvan kannalta kohtalokkaita. Eri asia tietysti on, millä työntekijät saadaan tilanteeseen heräämään. Siihen voi auttaa pelkkä koulutus tai toisaalta voidaan käynnistää tietoturvaprojekti, joka annetaan tietyn vastuuhenkilön/-ryhmän hoidettavaksi. Joka tapauksessa yrityksessä yhdessä opitut perusoletukset ovat voimakkaimmin työntekijöiden käytöstä ohjaavia voimia. Näiden yrityskulttuuriin pinttyneiden tapojen muuttaminen on erittäin vaikeaa, mutta mahdollista (Petrow ym. 2004:16).

Tietoturvakulttuurin muuttaminen vaatii vähintäänkin aloitteen yrityksen johtoportaasta. Tietoturvallisen toimintaan johtavan ajattelutavan leviäminen vaatii asemansa puolesta tärkeän esimiehen aloitetta ja/tai tukea. Lisäksi se vaatii kaikkien työntekijöiden hyväksynnän ja tuen. Työntekijöiden hyväksyntää ei tänä päivänä kuitenkaan välttämättä saada enää ylhäältä päin ohjeita sanelemalla, vaan esimerkiksi perustelemalla asioita ja osallistamalla työntekijöitä tietoturvallisten toimintatapojen suunnitteluun.

Tietoturvakulttuurin muuttaminen on sitä vaikeampaa, mitä vanhemmasta yrityskulttuurista on kyse ja mitä kauemmin työntekijät ovat saaneet ”puuhata omiaan”. Tämä johtuu siitä, että pinttyneiden perusoletusten muuttaminen tarkoittaa uuden oppimista ja epämukavuusalueelle menemistä. Kaikkein pahinta kuitenkin lienee vanhasta pois oppiminen. Joku työntekijöiden mielestä itse opittu ja hyvä toimintatapa saakin nyt jäädä ja tilalle otetaan uusi tapa toimia saman asian kanssa. Tämä voi tuoda työntekijöiden keskuudesta vastustusta, varsinkin silloin, kun ylhäältä tunnutaan puuttuvan pienimpäänkin epäkohtaan työntekijän ”omassa” työssä. Tässä jälleen voisi olla kohdallaan työntekijöiden kuunteleminen ja kouluttaminen, jotta he voivat itse suunnitella esimerkiksi ulkopuolisen asiantuntijan ja esimiesten johdolla työnsä mahdollisimman järkevällä tavalla. On edelleen muistettava, että työntekijä on oman työnsä paras asiantuntija, mutta ulkoinen asiantuntija voi tuoda hyviä ajatuksia siihen, miten työtä voidaan tehdä tietoturvallisemmaksi. Joka tapauksessa-

sa tärkeintä olisi, että työ saataisiin mahdollisimman joutuisaksi huolimatta tietoturvallisista toimintatavoista.

9.2.1 Tietoturvallisuuskulttuurin muodostuminen

Basie von Solms (2000:615) esittää tietoturvallisuuskulttuurin muodostumisen kolmena aaltona. Ensimmäinen aalto on tekninen aalto, joka tuli tietoisuuteen jo aikaisin 80-luvulla eli suurien keskuskoneiden aikana. Tällöin tietoturva oli pääasiassa teknisten ihmisten käsissä, jotka huolehtivat järjestelmän tietoturvasta pääsylistoin, käyttäjätunnuksin ja salasanoin. Toisena aaltona on johtamisaalto 80-luvulta 90-luvun puoliväliin. Toisen aallon aikana tietoturvallisuus nousee myös johdon mielenkiinnon kohteeksi. Muodostetaan tietoturvallisuuspolitiikkoja, tietoturvallisuuspäälliköt tulevat kuvioihin ja organisaatiorakenteita suunnitellaan tietoturvan kannalta. Kolmas aalto on institutionalisointiaalto. Tämän aallon aikana muodostetaan tietoturvallisuuskulttuuria, joka tukee muodostettuja tietoturvallisuuspolitiikkoja, tietoturvaohjeita, tietoturvallisia menettelytapoja jne. Kolmannessa aallossa tietoturvallisuus tulee osaksi päivittäisiä rutiineja. (von Solms 2000:615.)

Toisaalta myös yrityksissä voidaan tietoturvakulttuurin ajatella muodostuvan samalla periaatteella kolmessa aallossa lähtien teknisistä puitteista ja päätyen lopulta tilanteeseen, jossa tietoturvallisuus muodostuu normaaleiksi rutiineiksi työntekijöiden työtavoissa ja käyttäytymisessä. Kauppa- ja teollisuusministeriön pk-yritysten tietoturvallisuuskysely 2006 (2007) antaakin viitettä tähän, jos tarkastellaan kyselyn tuloksia. Kuten taulukosta 3 näkyy, suurella osalla pk-yrityksiä tekniset tietoturva-asiat on hoidettu kohtuullisen hyvin. Lisäksi nähdään taulukosta 4, että joissakin pk-yrityksissä on alettu jo muodostamaan tietoturvapolitiikkoja ja tietoturvasuunnitelmia. Eli voidaan sanoa johtamisaallon tällä hetkellä kulkevan ainakin osassa pk-yrityksiä, mutta varsinaista rutiineihin vaikuttavaa tietoturvallista tietoturvakulttuuria ei voida sanoa muodostuneen moneenkaan pk-yritykseen.

Taulukko 3. Tietoteknisten turva-asioiden hoito pk-yrityksissä (Pk-yritysten tietoturvallisuuskysely 2006 [2007:10]).

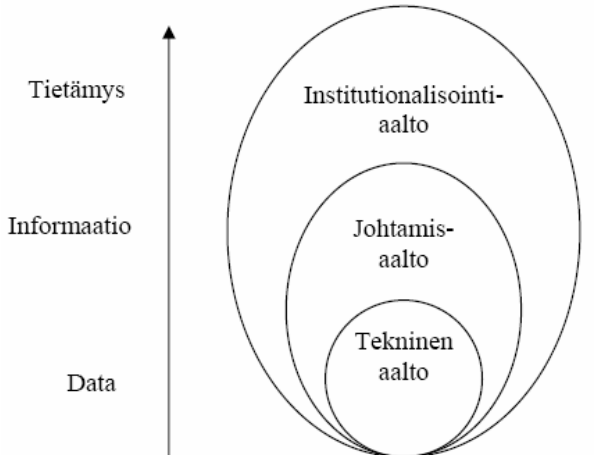
		Ei	Kyllä	Ei osaa sanoa	Yhteensä
Onko yrityksenne Internet-yhteydet suojattu palomuurilla?	n=3637	3 %	95 %	2 %	100 %
Onko tietokoneissanne automaattisesti päivittyvät virustentorjunta-ohjelmat?	n=3637	4 %	94 %	3 %	100 %
Onko kannettavat tietokoneenne varustettu laitekohtaisilla palomuureilla (kysyttiin vastaajilta, joilla on käytössä kannettava tietokone)?	n=2330	14 %	78 %	8 %	100 %
Päivitetäänkö tietokoneidenne käyttöjärjestelmät säännöllisesti?	n=3637	13 %	84 %	4 %	100 %
Onko tietokoneidenne käyttö suojattu säännöllisesti vaihdettavin salasanoin?	n=3637	47 %	49 %	4 %	100 %
Otetaanko yrityksessänne tietokoneille tallennetuista tiedoista varmuuskopiot säännöllisesti?	n=3637	29 %	68 %	3 %	100 %
Onko yrityksenne tärkeitä tietojärjestelmiä varten vararatkaisu?	n=3637	48 %	47 %	4 %	100 %
Ostatteko tekniseen tietoturvaan liittyvät palvelut muualta?	n=3637	30 %	68 %	3 %	100 %

Taulukossa 4 on merkille pantavaa, että vain 21 % pk-yrityksistä on laatinut tietoturvapolitiikan ja 14 % kirjallisen tietoturvasuunnitelman. Tietoturvapolitiikka ja -suunnitelma kuitenkin edustavat niitä esimiesten luomia tietoturvallisuuskulttuurin arvoja, jotka ilmaisevat, mitä pidetään toivottavana tai tavoittelemisen arvoisena käyttäytymisenä. Näillä arvoilla on siis mahdollista vaikuttaa työntekijöiden käyttäytymiseen. Tietoturvallisuuskulttuuri voi arvoista, koulutuksesta, johtamisesta jne. huolimatta olla kuitenkin olemassa, mutta on asia erikseen, onko kulttuuri muodostunut ajan saatossa sellaiseksi, että sitä voidaan hyvällä omalla tunnolla sanoa tietoturvalliseksi.

Taulukko 4. Tietoteknisten turva-asioiden hoito pk-yrityksissä henkilöstön kannalta (Pk-yritysten tietoturvallisuuskysely 2006 [2007:26]).

	Ei	Kyllä	Ei osaa sanoa	Yhteensä
Onko yrityksellenne laadittu tietoturvapolitiikka?	74 %	21 %	4 %	100 %
Onko yrityksessänne kirjallinen tietoturvasuunnitelma?	82 %	14 %	4 %	100 %
Onko yrityksessänne varmistettu, että henkilöt ymmärtävät oman tietoturvavastuunsa?	26 %	68 %	6 %	100 %
Onko yrityksessänne nimetty ja henkilöstölle tiedotettu tietoturva-asioiden vastuuhenkilö?	52 %	43 %	4 %	100 %
Onko yrityksenne henkilökunta perehdytetty tunnistamaan liiketoiminnan kannalta luottamukselliset tiedot?	24 %	71 %	5 %	100 %
Onko yrityksenne henkilökunta perehdytetty tunnistamaan tietojärjestelmiin liittyviä riskejä?	33 %	61 %	6 %	100 %
Tietääkö yrityksenne henkilökunta, miten ja milloin voidaan antaa ulkopuolisille yritystoiminnan kannalta luottamuksellisia tietoja?	13 %	82 %	6 %	100 %

Tietoturvallisuuden aallot voidaan nähdä kehittyvän myös sen mukaan, minkälaista tietoa yrityksessä pääosin suojataan (Iivonen 2006:24)[3]. Aallot liittyvät tiedon eri tasoihin, dataan, informaatioon ja tietämykseen (ks. kuvio 4).



Kuvio 4. Tietoturvallisuuden aallot ja tiedon tasot (Iivonen 2006:24).

Ensimmäisen eli teknisen aallon aikana suojaustoimenpiteet kohdistuvat Iivosen (2004:24)[3] mukaan lähinnä dataan ja tietokoneiden suojaamiseen. Johtamisaallon mukana pyritään suojaamaan yrityksen kaikkea informaatiota sekä tietokoneilla että fyysisessä muodossa olevaa. Institutionalisointiaallon kautta mukaan tulee vielä työntekijöiden tietämyksen suojaaminen.

Tietoturvallisuuskulttuuri voi muodostua esimiesten laatimista arvoista, tietoturvapolitiikasta, tietoturvallisuusohjeista, koulutuksesta jne. Joka tapauksessa toisaalta jokaiseen yritykseen muodostuu jonkinlainen tietoturvakulttuuri. Onko kulttuuri hyvä vai huono, on eri asia. Voi olla, että kulttuuriin on muodostunut erilaisia perusoletuksia tiettyjen toimintojen osalta, jotka aiheuttavat tietoturvaongelmia. Eräässä kirjastossa esimerkiksi kirjastovirkailija luovutti henkilökohtaisen käyttäjätunnuksen ja salasanan asiakkaalle, jotta asiakas pääsi käsiksi kirjaston tietokantoihin. Virkailija varmasti ajatteli palvelevansa asiakasta mahdollisimman hyvin, mutta ei tullut ajatelleeksi mitä asiakas olisi voinut virkailijan tunnuksella verkossa tehdä. Voi jopa olla, että tämä sama perusoletus on useilla kirjastovirkailijoilla. Toimintapa on muodostunut itsestään selvyydeksi. Näin tehdään, että pystytään palvelemaan asiakkaita mahdollisimman hyvin.

Tietoturvakulttuurin tietoturvallisuuden ratkaisee erittäin monet asiat, kuten ihmisten motivaatio, asenteet, koulutus, yhteistyö, yhdessä sovitut toimintatavat ja johtaminen. Edellä mainitussa esimerkissä kirjastossa toimimisen ratkaisi luultavasti yhdessä sovittu kirjoittamaton sääntö joka oli sovittu virkailijoiden kesken. Tässä huomataan, että esimiesten olisi kaikkein tärkeintä pyrkiä vaikuttamaan kulttuurin syvimpään tasoon niin, että tietoturvallisuus muodostuisi työntekijöiden päivittäiseksi rutiiniksi (Thomson & von Solms 2005:73). Esimiesten tulisi siis pyrkiä vaikuttamaan perusoletuksiin. Työntekijöiden tietoturvattoman toimin-

[3] Alkuperäinen lähde: Kuusisto, T; Slay, J.;Kuusisto, R. 2004. Information security culture approach to knowledge security. Proc. Of 5th Australian conference on information warfare and IT security.

nan takana voi olla väärin opittuja työtapoja ja vääriä oletuksia siitä, kuinka rutiinit pitäisi hoitaa, kuten edellä olevassa esimerkissä. Näistä vääristä toimintatavoista pitäisi oppia pois tavalla tai toisella. Tässä työntekijöiden koulutus on keskeisessä asemassa, kuten myös yritykselle laadittu tietoturvapolitiikka, yhteiset säännöt, erilaiset tietoturvaan liittyvät keskustelut esimiesten ja työntekijöiden kesken ja ylimmän johdon tuki tietoturvan kehittämiseksi.

9.2.2 Tietoturvakulttuuri eri ikäisten yritysten osalta

Eri ikäisten yritysten tietoturvakulttuuriin vaikuttaminen on erilaista. Nuoren yrityksen toimintatavat ovat muotoutuneet pääasiassa yrityksen perustusvaiheessa perustajajäsenten kautta. Nuoressa yrityksessä tietoturvakulttuuri on kehitysvaiheessa ja siihen vaikuttaminen on varmasti suhteellisen helppoa, jos siihen vain halutaan vaikuttaa. Nuoren yrityksen osalta tietoturvakulttuuriin muodostumiseen pitäisikin heti alkuun kiinnittää huomiota. (Petrow ym. 2004.)

Nuoren yrityksen ominaisuuksiin kuuluu, ettei toimintatavat ole vielä muodostuneet rutiineiksi, minkä vuoksi niitä pystytään vielä helposti muuttamaan. Nuoreen yritykseen ei ole vielä ehtinyt syntyä ”näinhän me ollaan aina toimittu” –toimintatapoja. Myös tietoturva-ajattelu voi olla jokseenkin hajanaista, koska ihmiset voivat olla eri ikäisiä, tulevat erilaisista taustoista ja ovat ehkä jo aiemmin työskennelleet erilaisissa muissa yrityksissä. Nuoren yrityksen on erittäin tärkeää jo varhaisessa vaiheessa keskittyä yhtenäisen tietoturvakulttuurin muodostamiseen, koska tietoturvakulttuurin muuttaminen myöhemmin on erittäin vaikeaa sekä rahallisesti että muutosvastarinnan vuoksi. (Petrow ym. 2004.)

Keski-ikäisen yrityksen osalta tietoturvakulttuuri on jo päässyt muodostumaan. Tietyistä toimintavoista on muodostunut rutiineja. Työntekijöille on muodostunut kuva siitä, miten tietoturva-asiat omassa työpaikassa hoidetaan. He tietävät miten kulunvalvonta toimii, miten tietokoneita ja muistivälineitä käsitellään tietoturvallisesti, miten asiakirjoja käsitellään jne. Kuitenkin jos tietoturvakulttuuria tutkitaan syvemmälle, saattaakin löytyä vakavia puutteita. Tietoturvakulttuuriin on jo muodostunut selkeitä itsestäänselvyyksiä eli ”näinhän me ollaan aina tehty” -toimintatapoja. Näiden toimintatapojen muuttaminen saattaa vaatia jo ulkopuolista konsultaatiota ja selkeitä perusteluja miksi näin tehdään. Jos yritys on vielä laajentunut eri alueille esim. maantieteellisesti, niin myös tietoturvakulttuuri koko yrityksen osalta on jakautunut luultavasti eri alakulttuureihin. Tässä tapauksessa myös nämä alakulttuurit pitäisi saada yhtenäistettyä saman tietoturvakulttuurin alle. Esimiesten tehtävä ei olekaan enää niin helppo kuin nuoremman yrityksen osalta, minkä takia voidaan tarvita hyvin suunniteltu ja johdettu kulttuurinmuutos. Joka tapauksessa varmasti törmätään samoihin ongelmiin kuin muutoksessa normaalisti eli ihmisillä ei ole aikaa muutokselle ja muutosta vastustetaan. (Petrow ym. 2004.)

Kypsään ikään ehtineessä yrityksessä on aina vain vaikeampi tehdä muutoksia ja joskus ne ovat jopa mahdottomia. Tällaisessa yrityksessä

yrityskulttuuri vaikuttaa erittäin voimakkaasti yksilöön työympäristössä. Totuttujen toimintatapojen vaikutus toimintaan on erittäin vahvaa ja vaikeasti muutettavissa. Pitkän historian omaavan yrityksen henkilöstön voidaan sanoa kasvaneen kiinni yrityksen kulttuuriin. Toivoa ei kannata silti menettää, sillä myös vanhoissa yrityksissä viedään koko ajan erilaisia muutoksia läpi. Tietoturvakulttuurin muutokseen täytyy vain lähteä samalla tavalla kuin keski-ikäänkin ehtineen yrityksen osalta eli aluksi kartoitetaan lähtötilanne ja määritellään tärkeät kehityskohteet. Erityisen suurien muutosten tekeminen on kuitenkin erityisen vaikeaa, mutta ne näyttäisivät onnistuvan siinä tapauksessa, jos muutosten taakse saadaan kriittinen massa. Toisaalta voidaan vetää johtopäätös, että kovin suuria muutoksia kypsän yrityksen tietoturvaprosessiin ei luultavasti tarvitse tehdä, jos se on jo ehtinyt kypsään ikään. (Petrow ym. 2004.)

9.3 Toimintakulttuurin muutoksesta tietoturvakulttuurin muutokseen

Vanhasta savupiipputeollisuudesta lähtöisin oleva toimintakulttuuri on ikävä kyllä joissakin yrityksissä/organisaatioissa vielä arkipäivää. Tällöin organisaatio on hyvin hierarkinen ja käskyvaltainen. Ihmisiä johdetaan rahalla, vallalla ja pelolla. Ylhäältä päin on asetettu normit, joista seuraa rangaistus. Työt on organisoitu siten, että jokaisella on omat työt eikä muiden asioihin sotkeuduta. Työtä tehdään esimiehelle, joka on vastuussa töiden sujumisesta. Virheiden tekijää ja sääntöjen rikkojaa rankaistaan minkä vuoksi virheiden syy löytyy aina jostain muualta tai virheitä piilotellaan mahdollisimman pitkään. Esimiesten ja työntekijöiden välillä on luottamuspula ja kumpikin osapuoli yrittää saada yrityksen tuottamasta tuloksesta mahdollisimman suuren osan. (Kari Laine.) Tällaista toimintakulttuuria Laine nimittää epäluottamuksen kulttuuriksi (ks. kuvio 5).

Apunen ja Pokkinen toteavat Aamulehden pääkirjoituksessaan (11.4.2007:A2) työntekijöiden yhä useammin olevan oman työnsä koulutettuja asiantuntijoita, joiden johtamiseen pätevät erilaiset tavat kuin ennen. He toteavat myös yhteiskunnan arvojen muuttuneen niin paljon, ettei tarkkaa nokkimisjärjestystä pidetä enää tarpeellisena. Silti Apusen ja Pokkisen kirjoituksen mukaan Tampereen yliopiston johtamistieteiden laitoksen professori Marja Eriksson on arvioinut työpaikkoja johdettavan edelleen pelolla. Hän perustaa väitteensä arkihavaintoihin. Erikssonin mukaan pelolla johtaminen jopa yleistyy työpaikoilla ja esimiestyön keinoiksi taipuvat nöyryyttäminen, tiedon panttaaminen ja jopa uhkailu. Useimmin pelottelua käytetään hierarkkisilla työpaikoilla, joita ovat sairaalat, seurakunnat ja yritykset, jotka elävät globalisaation takia myllerryksessä. Apunen ja Pokkinen (11.4.2007:A2) toteavatkin, ettei asiantuntijoista voi saada parhaita tehoja irti uhkailulla. Heidän mukaansa pelon ilmapiiri tuhoaa käytännön innovaatiot, joita monella alalla tarvitaan.

Luottamuksen kulttuurissa työt on organisoitu tiimeille ja niitä johdetaan osallistavaa johtamistapaa noudattaen. Vastuu on yhtä hyvin esimiehellä kuin tiimilläkin eikä työtä tehdä esimiehelle, vaan asiakkaalle. Tällaisen organisaation jäsenet ymmärtävät oman vastuunsa vuorovaikutuksen on-

nistumisessa. Tässä kulttuurissa myös työntekijöillä ja esimiehillä on luottamus toisiinsa. (Kari Laine.) Toisaalta Schein (2001:36) toteaa, että kirjallisuudessa esitettävät väitteet muuttumisesta tiimiperustaisemmaksi tai oppivan organisaation luomisesta tai työntekijöiden valtuuttamisesta ovat kaikki pätemättömiä, elleivät ne osoita, miten näiden ns. uusien arvojen pohjana olevat perusoletukset sopeutuvat organisaation toimintaympäristöön. Käytännössä tämä tarkoittaa, että esimerkiksi tiimiperustaisen työskentelytavan pitäisi sopeutua pätevällä tavalla organisaation toimintaympäristöön. Uudella työskentelytavalla pitäisi näin ollen saada enemmän asioita aikaan eli sen pitäisi tehostaa työskentelyä.

Scheinin (2001:36) mukaan joillakin markkinoilla ja joidenkin teknologioiden yhteydessä tiimityö ja työntekijöiden valtuuttaminen ovat olennaisia asioita ja ainoa keino organisaation menestyksen jatkumiseen. Hänen (Schein 2001:36) mukaansa taas toisissa markkina- ja teknologiaympäristöissä tiukka kuri ja järjestys sekä erittäin jäsentyneet suhteet ovat välttämättömiä menestymisen edellytyksiä. Esimerkiksi sairaaloissa lienee ehdottoman tärkeää noudattaa tiukasti sääntöjä ja määräyksiä, onhan kyse kuitenkin ihmishengistä. Tarkoittaen, vaikka organisaatio-/yrityskulttuuri onkin hierarkinen ja käskyvaltainen ja se on saatu aikaan kurilla ja kontrollilla, ei sitä silti voida sanoa epäluottamuksen kulttuuriksi, kuten Laine esittää (ks. kuvio 5).

On kuitenkin selvää, että lähtisin kehittämään tietoturvakulttuuria mieluummin luottamuksen kulttuurissa. Luottamuksen kulttuuri ei kuitenkaan välttämättä ole yhteydessä siihen, kuinka hierarkinen tai käskyvaltainen johtamisjärjestelmä on. Pääasia on, että kaikkien samassa ryhmässä tiiviisti työskentelevien työntekijöiden välillä on luottamus ja että työnteko on haasteellista, mielenkiintoista ja motivoivaa. On silti mielenkiintoista pohtia, miten luottamus/epäluottamus vaikuttaa organisaatio-/ryhmäkulttuuriin ja siinä työskenteleviin työntekijöihin.

Epäluottamuksen kulttuuri	Luottamuksen kulttuuri
▪ Hierarkinen, käskyvaltainen ▪ Johdetaan rahalla, vallalla ja pelolla ▪ Saatu aikaan kurilla ja kontrollilla, ”omat työt” ▪ Seurauksia: kielteisiä asenteita, virheiden siirtoa seuraaville, rangaistuksia ja pakoa todellisuudesta	▪ Matalat rakenteet, yhteistyövaltainen ▪ Johdetaan toiminnallisuudella, tuottavuudella, oikeudenmukaisuudella, tasa-arvolla ja samoilla mahdollisuuksilla ▪ Saatu aikaan vastuullisilla omatoimisilla tiimeillä, valmentavalla johtamisella, yhteisiä pelisääntöjä sopimalla, kurinalaisuudella ja sitoutumisella ▪ Seurauksia: avoimuutta, vastuunottoa, oikeudenmukaista palkitsemista, myönteisiä asenteita

Kuvio 5. Laineen esittämä luottamuksen ja epäluottamuksen kulttuuri (Kari Laine).

En väitä, että pk-yrityksissä olisi edellä mainitun kaltaista pelolla johtamista, mutta korostan sitä, että johtamistavat täytyisi olla kunnossa ennen kuin työntekijöiden luottamusta on mahdollista saada. Uusilla esimiehillä onkin melkoinen työsarka sellaisen toimintakulttuurin muokkaamisessa, jota on aiemmin johdettu huonosti ja työntekijöiden luottamus on menetetty. Vanhemmilla työntekijöillä kun on kokemusta aiemmista yritys-/organisaatiokulttuureista, joissa he ovat olleet johdettavana. Näin ollen esimiehistä on muodostunut tietty näkemys (ennakkoasenne), jota on vaikea muuttaa uuden esimiehen aloittaessa työt. Tätä ennakkoasennettaan yrityksessä/organisaatiossa kauemmin työskennelleet työntekijät levittävät aina kun yritykseen/organisaatioon tulee uusi työntekijä. Toisin sanoen, uusi työntekijä opetetaan talon tavoille mentaliteetilla uskallapas erottua porukasta. Tämä pätee sekä johtoportaaseen, että työntekijöihin.

Organisaation historian painolasti vaikuttaa siis merkittävästi uuteen työntekijään ainakin pitkällä aikavälillä. Miten siis uusia johtamistapoja edustava esimies tai työntekijä voi toteuttaa itseään? Grönroos (2003:60) toteaakin organisaation kulttuuria olevan hyvin vaikea muuttaa, eikä oikeastaan mikään organisaatio ole ikinä saanut ravistettua historian painolastia harteiltaan. Tässä mielessä Grönroosin (2003:60) mukaan kaikilla organisaatioilla on organisaation muisti, joka toimii sekä hyvässä että pahassa. Hän (Grönroos 2003:61) toteaa myös, että organisaation muisti ja arvot muodostavat organisaation kulttuurin, johon kaikki eivät välttämättä sopeudu. Tämä onkin eräs tavallisimmista työssä jaksamiseen vaikuttavista tekijöistä (Grönroos 2003:61).

Miten siis esimerkiksi uudenaikaiset esimiehet ja vanhat huonosti johdetut työntekijät sopivat yhteen? Onko niin, että vanhat työntekijät näkevät aikansa koittaneen ja hyödyntävät tilaisuutta yrittää vaikuttaa uuteen esimieheen, luistaa vastuusta ja valittaa epäkohdista. Vai pystyykö uusi esimies kenties luomaan itsestään sellaisen kokonaiskuvan, että uusi johtamistyyli on saapunut taloon, luottakaa minuun. Kaiken kaikkiaan olisi erittäin tärkeää, että pk-yritysten esimiehet tunnistavat oman yrityksensä toimintakulttuurin ennen kuin mitään lähdetään muuttamaan. Kulttuuri sanelee sen, miten muutosta johdetaan ja miten eri työntekijät voivat käyttäytyä muutoksessa. On selvää, että ennen tietoturvakulttuurin kehittymistä oikeaan suuntaan myös yrityksen toimintakulttuuri täytyy olla kunnossa.

10 Ongelmia tietoturvakulttuurin edistämisessä?

Tietoriskien hallinta on tietoturvallisuustyötä ja se on haaste yrityksen johdolle, joka vastaa toimintansa tuloksesta ja resurssien oikeasta kohdentamisesta sekä luotettavasta, laadukkaasta ja yrityksen omaisuutta kunnioittavasta toiminnasta toteaa Kyrölä (2001:23). Yrityksen johdolla on esimerkiksi osakeyhtiölain mukaan vastuu liiketoiminnan jatkuvuuden varmistamisesta, toiminnan turvaamisesta ja valvonnan organisoinnista, mitä tietoriskien hallinta osaltaan on (ibid.). Tietoriskejä pyritään hallitsemaan tietoturvan keinoin. Henkilöstön tietoturvalliseen käyttäytymiseen voidaan ajatella vaikuttavan henkilöstöturvallisuuden ja hallinnollisen turvallisuuden määrittelemin keinoin.

Hallinnollinen tietoturvallisuus ottaa kantaa mm. yrityksen tietoturvallisuuden toimintapolitiikkaan, toiminnan linjauksiin, johtamiseen, organisointiin, sijoitukseen yrityksessä, toiminnan resursointiin ja tietoturvallisuuden vastuumäärittelyihin. Henkilöstöturvallisuus puolestaan liittyy henkilöstön soveltuvuuteen, toimenkuviin, tiedonsaanti- ja käyttöoikeuksiin, turvallisuuskoulutukseen ja valvonnan hallintaan.

Omat työntekijät, yrityksen suurin tietoriski

Monissa artikkeleissa, tutkimuksissa ja muissa kirjoituksissa todetaan, että suurin tietoturvaa koetteleva uhka löytyy organisaatioiden sisältä sen omista työntekijöistä. Esimerkiksi Helen L. James on (1996:10) artikkelissaan esittänyt, että IT-ala keskittyy liikaa pelkästään tietoturvan tekniseen näkökulmaan ja katsoo läpi sormien inhimillistä osatekijää. James on (1996:10) todennut monien tutkimusten näyttävän, että suurin osa tietokoneiden väärinkäytöstä tulee oman organisaation sisältä, organisaatioiden työntekijöiden ja myös alihankkijoiden keskuudesta. Ihmiset ovat tietoturvan päätekijöitä, koska he käyttävät ja hallitsevat tietojärjestelmiä päivittäin. Näin ollen ihmiset ovat myös tietoturvarikkomusten ja -vahinkojen tekijöitä kuten myös rikkomusten uhreja toteaa James (1996:10).

On helppoa todeta, että omat työntekijät ovat yritysten suurin tietoriski. Tästä asiasta on kirjoitettu monessa tietoturvaa käsittelevässä artikkelissa ja kirjassa. Yksinkertainen selitys sille kuitenkin on, että työntekijät tekevät työn eli käyttävät tietojärjestelmiä, koneita, laitteita, ohjelmia ja muita välineitä, joilla työ tehdään. Sanonta ”tekevälle sattuu” sopii erittäin hyvin tähän yhteyteen. Jos tietoriskit halutaan kokonaan poistaa voimme samalla lopettaa työnteonkin. Niin kauan kuin yrityksissä on ihmisiä töissä (eikä koneita), on myös erilaisia tietoriskejä. Ihmiset nimittäin hermostuvat, tekevät erehdyksiä, unohtavat asioita, ahnehtivat, pettävät, ottavat riskejä, loukkaantuvat jne. Näiden kautta johtuvista tunnetiloista syntyy toimia, jotka eivät varmasti ole niitä asioita, joita odotetaan rationaalisesti, järkevästi ja tunnollisesti toimivalta työntekijältä. Vielä vähemmän näitä asioita odotetaan esimiesasemassa olevalta henkilöltä.

On selvää, että tietoriskien toteutumiseen voidaan vaikuttaa eri tavoin. Tärkeimmät näistä lienee ihmisten hyvä johtaminen, tietoisuuden lisääminen ja ihmisten motivaatio ja asenne. Ei ole täysin samantekevää, miten työntekijöitä johdetaan tietoturvalliseen toimintaan. Ensinnäkin esimiesten on hyvä näyttää omalla esimerkillään tietoturva-asioiden olevan tärkeitä. Erilaisiin tietoturvaa käsitteleviin koulutuksiin ja kokouksiin tulisi osallistua, jotta esimiehet itsekin oppivat oikeat tietoturvalliset toimintatavat. Esimiesten sitoutuminen tietoturvaan tulisi näkyä kaikella tavalla, myös tietoturvaan satsattavina resursseina. Työntekijöitä olisi myös tarpeen ottaa mukaan tietoturvallista toimintaa koskevaan suunnitteluun. Nämä kaikki yhdessä vaikuttavat oikeanlaisen tietoturvakulttuurin syntymiseen.

10.1 Esimiehet eivät sitoudu tietoturvaan

Esimiehet eivät välttämättä tiedosta omaa käyttäytymistään tietoturvallisen toiminnan osalta. Esimerkiksi konsulttiyhtiö Ernst & Youngin vuonna 2004 tehdyn tietoturvaselvityksen mukaan yritysjohtajat tiedostavat tietoturvariskit, mutta eivät tee asioiden eteen tarpeeksi toteaa Kuivalainen (2004) digitoday verkkolehdessä. Samassa artikkelissa on todettu myös, että yritykset pitävät käyttäjien tietoturvatietoisuuden puutetta merkittävänä riskinä. Siitä huolimatta vain 28 % vastaajista kertoi vuonna 2004, että käyttäjien tietoisuuden nostaminen olisi keskeinen kehityshanke samana vuonna. Ernst & Youngin tietoturva-asiantuntija toteaa samassa artikkelissa, että asenne muutokseen pitää olla peräisin ylimmästä johdosta ja hallituksesta. Sama Ernst & Youngin tietoturvaselvitys tehtiin ensimmäistä kertaa 11 vuotta sitten. Tietoturva-asiantuntija Väisäsen mukaan yksi asia on pysynyt muuttumattomana näiden vuosien aikana. Edelleen yritykset tekevät jotakin vasta sitten, kun jotakin ikävää tapahtuu.

Esimiesten tulee ymmärtää myös että, saavutettu tietoturvataso ei pysy halutulla tasolla ilman asianmukaista panostusta tietoturvan jatkuvaan kehittämiseen. Tietoturva tulee ymmärtää jatkuvana prosessina, eikä pelkästään yksittäisenä projektina jolla tietoturva saatetaan kuntoon. Tietoturva voidaan laittaa kuntoon yksittäisellä projektilla, mutta sen jälkeen sitä täytyy jatkuvasti ylläpitää ja siihen tarvitaan jatkuvaa resursointia.

10.2 Tiedot, taidot ja koulutus eivät vastaa tietoturvan vaatimuksia

Koulutus on yksi suurimpia ongelmia varsinkin tietoteknistä tietoturvaa ajatellen. Yrityksissä satsataan tekniseen infrastruktuuriin, mutta henkilöstöä ei kuitenkaan kouluteta käyttämään sitä tehokkaasti. Griffin on (1990:437) todennut, että työntekijän suorituskyky voidaan jakaa kolmeen osatekijään:

- kyky (ability)
- työympäristö (the work environment)
- motivaatio

Toisin sanoen, jos työntekijältä puuttuu kyky, niin ei hänellä myöskään ole suorituskykyä hoitaa työtä. Käytännössä tämä tarkoittaa, että työntekijä täytyy jollakin tavalla saada opiskelemaan uusia asioita. (ibid.)

Tietoturvallisuuspolitiikka voi olla tehokas ainoastaan, jos henkilöstö tietää, ymmärtää ja hyväksyy tietoturvaan liittyvät varokeinot (Furnell, Gennatou & Dowland, 2002:352). Hyvän tietoturvakulttuurin vaaliminen vaatii kuitenkin henkilöstön koulutusta ja tietoisuutta tietoturvaan liittyvistä asioista (ibid.).

10.2.1 Henkilöstön tietoturvallisuuskoulutusta laiminlyödään

Tietoturva vaatii ihmisten tietoisuutta oman toimintansa seurauksista toteaa Petri Puhakainen (2005:16). Tietoisuuden lisääminen ja asenteiden muokkaaminen on välttämätöntä organisaatioiden arvokkaan tietopääoman suojaamiseksi (ibid.). Puhakaisen (2005:16) mukaan kuitenkin jopa sellaiset yritykset, joilla tietoturva on muuten korkealla tasolla, saattavat laiminlyödä henkilöstön tietoturvakoulutuksen ja erityisesti koulutuksen vaikutuksen mittaamisen.

Tili- ja lakitoimistojen tietoturvallisuus – tutkimus 2006

Samansuuntaisia tuloksia on saatu tuoreesta koulutusyritys Granite Partners Oy:n vuonna 2006 teettämästä tutkimuksesta, tili- ja lakitoimistojen tietoturvallisuudesta. Tutkimuksen mukaan henkilöstön tietoturvallisuuskoulutusta tulisi lisätä (Tili- ja lakitoimistojen tietoturvallisuudessa parantamisen varaa 2006). Markkinatutkimuksessa kohderyhmänä oli 270 yli 5 henkilöä työllistävää eteläsuomalaista alan yritystä, joista 75 vastasi kyselyyn.

Tutkimuksen mukaan noin puolet yrityksistä vastaa tarvitsevansa lisää koulutusta tietoturva-asioista ja yli 30 % vastaajista ilmoittaa, ettei tietoturvakoulutuksesta ole vielä huolehdittu juuri lainkaan. Syynä koulutuksen puutteellisuuteen olivat mm. perinteisten koulutusmetodien ongelmat ja hankalat järjestelyt tai ajanpuute. Pieni osa koki koulutuksen myös liian kalliiksi suhteessa saavutettuihin hyötyihin. Lisäksi kolmannes yrityksistä, joissa koulutusta ei ole järjestetty, ilmoittaa syyksi sen, ettei tietoturvakoulutusta koeta tärkeäksi. Silti jopa 54 % vastanneista kertoo luottamuksellisuuden ja muiden tietoturva-asioiden olevan erittäin kriittisiä heidän asiakkailleen ja muille sidosryhmilleen. Lähes puolelta yrityksistä sidosryhmät olivatkin tiedustelleet yrityksen tietoturva-asioiden hoidosta. Ehkä tämän takia useassa yrityksessä on kuitenkin ymmärretty tietoturvan merkityksen tärkeys yrityksen toiminnalle.

Tutkimukseen osallistui 75 yli 5 henkilöä työllistävää yritystä. Lehdistötiedotteessa ei kuitenkaan kerrottu kuinka moni näistä yrityksistä lukeutuu pk-yrityksiin ja miten tietoturva oli hoidettu nimenomaan pk-yrityksissä. Toisaalta yleinen trendi on ollut, että nimenomaan pk-yrityksissä tietoturva-asiat on hoidettu yleisesti ottaen kaikkein heikoiten.

Tietoturvallisuus pirkanmaalaisissa tietointensiivisissä pk-yrityksissä

Ilona Iivonen on tutkinut diplomityössään tietoturvallisuutta pirkanmaalaisissa tietointensiivisissä pk-yrityksissä. Hän on todennut työssään (2006:36), että henkilöstön tietoturvallisuustietoutta pidetään yllä lähinnä ajankohtaisista asioista sähköpostitse tiedottamalla. Tietoturvaan liittyviä asioita voi olla esillä myös esimerkiksi viikkopalavereissa. Tiedotetut tietoturva-asiat ovat kuitenkin lähinnä teknisiä ja liittyvät esimerkiksi käyttöjärjestelmien turva-aukoista tiedottamiseen ja virussuojaukseen. Varsinaista tietoturvallisuuskoulutusta yrityksissä ei ole kuitenkaan järjestetty. Ainoa tietoturvaan liittyvä koulutus yrityksissä oli perehdytysvaiheessa, jonka aikana tutustuttiin tekniseen toimintaympäristöön. Esim. ohjeistuksiin tutustuminen oli osa tätä perehdytystä. Ainoastaan kolmessa yrityksessä todettiin, että laajemmalle ja systemaattiselle tietoturvakoulutukselle olisi tarvetta. Yhdessä yrityksessä haastateltava epäili, että korkeasti koulutetut tietotekniikan ammattilaiset tuskin olisivat motivoituneita osallistumaan koulutukseen. Tutkimukseen osallistui 16 yritystä, joiden koko vaihteli 6 ja 120 työntekijän välillä. Kymmenessä näistä yrityksistä työntekijämäärä oli 10 - 30 välillä ja viidessä työntekijöitä oli yli 30. (Iivonen 2006:36.)

Kauppa- ja teollisuusministeriön tietoturvakysely pk-yrityksille 2006

Kauppa- ja teollisuusministeriö teki pk-yritysten tietoturvakyselyn vuonna 2006. Yhteenveto kyselystä valmistui alkuvuonna 2007. Kyselyn kohderyhmänä olivat pk-yritykset (alle 250 henkilöä työllistävät). Otoskoko oli 4000 kohderyhmän vaatimukset täyttävää yritystä. Aineisto kerättiin puhelinhaastattelulla 8.5. – 22.6.2006 välisenä aikana ja tietoturva-asioihin liittyvät kysymykset kysyttiin niiltä yrityksiltä, joilla oli käytössään tietokone ja Internet-yhteys. Näitä yrityksiä oli 3637 yritystä. Selvityksestä ilmeni, että 82 % yrityksistä ilmoitti henkilökuntansa tietävän miten ja milloin ulkopuoliselle taholle voidaan antaa luottamuksellisia tietoja. Kuitenkin vain 71 % vastaajista ilmoitti perehdyttäneensä henkilökunnan tunnistamaan, mitkä ovat yritykselle luottamuksellisia tietoja, todetaan selvityksessä (2007:3). Käytännössä tämä tarkoittaa sitä, että 11 % vastanneista luottaa työntekijöidensä tietävän automaattisesti, mitkä tiedot ovat luottamuksellisia ja milloin niitä voidaan ulkopuolisille antaa. (Pk-yritysten tietoturvakysely 2006 [2007:2-3])

Samassa kauppa- ja teollisuusministeriön selvityksessä (2007) kysyttiin myös pk-yritysten tietoturvallisuusosaamisen ja ylläpitämisen varmistamisesta. Kysymys kuului: ”Miten yrityksessänne varmistetaan tietoturvallisuusosaaminen ja sen ylläpitäminen?” Kysymys oli avoin kysymys eli vastausvaihtoehtoja ei annettu valmiiksi. 15 eniten vastattua vastausta ovat alla olevassa luettelossa. Kaikista kyselyyn osallistuneista ainoastaan 464 hoiti tietoturvallisuusosaamisen ja sen ylläpitämisen kouluttamalla, kouluttautumalla tai kursseilla. Tämä on ainoastaan 12,8 % kaikista kyselyyn osallistuneista yrityksistä. Täytyy kuitenkin huomioida, että 637 mainintaa olivat ulkoistettuna palveluna/ostopalveluna eikä tiedetä, mitä ulkoistettu palvelu / ostopalvelu pitää sisällään. Se voi pitää sisällään myös koulutusta. Suurin osa pk-yrityksistä (912 kpl) mainitsi,

että osaaminen ja sen ylläpitäminen hoidetaan omilla resursseilla / hoidetaan itse. Tämä ei liene kovin yllättävä vastaus, sillä pk-yritykset eivät mielellään investoi työntekijöidensä koulutukseen, jos resurssit ovat vähäisiä. Tosin vastauksesta ei selviä, miten tietoturvaosaaminen ja sen ylläpitäminen hoidetaan itse.

Samaan kysymykseen oli seuraavia vastauksia (Pk-yritysten tietoturvakysely 2006 2007:31):

- hoidetaan omilla resursseilla / hoidetaan itse (912 mainintaa)
- ulkoistettuna palveluna / ostopalveluna (637 mainintaa)
- kouluttamalla / kouluttautumalla / kurssit (464 mainintaa)
- sisäinen tiedotus / yhteiset palaverit / keskustelemalla (170 mainintaa)
- omilla resursseilla ja ulkoistettuna palveluna (159 mainintaa)
- yrityksessä oma vastuuhenkilö / tietoturva-vastaava / tukihenkilö / avainhenkilö (146 mainintaa)
- ammattiapua / konsulttiapua käytetään tarvittaessa (71 mainintaa)
- ystävä / kaveri / sukulainen / poika / aviomies hoitaa / auttaa (57 mainintaa)
- seuraamalla alan kehitystä (46 mainintaa)
- ammattilehtiä / alan julkaisuja lukemalla (33 mainintaa)
- itseopiskelu / omaehtoinen opiskelu (32 mainintaa)
- päivitysten kautta (15 mainintaa)
- tiedot ovat yhdellä henkilöllä / vain yksi pääsee koneelle (12 mainintaa)
- konsernin kautta (10 mainintaa)
- luottamus / keskinäinen luottamus (10 mainintaa)

Edelleen samassa kauppa- ja teollisuusministeriön selvityksessä (Pk-yritysten tietoturvakysely 2006 2007:58) kysyttiin, mitkä ovat suurimmat puutteet tietotekniikka-/tietoturva-asioissa. Kysymys kuului seuraavasti: ”Mitkä ovat yrityksessänne suurimmat puutteet tietotekniikka/tietoturva-asioissa?” Kysymys oli avoin kysymys ja siihen saatiin alla olevia vastauksia. Monien avoimien vastauksien vuoksi olen ottanut vain kuusi eniten vastattua.

- osaaminen / tietämättömyys / tiedon puute / ammattitaidottomuus (199 mainintaa)
- oma / yrittäjän osaaminen / ammattitaito (191 mainintaa)
- henkilökunnan / käyttäjien atk-osaaminen (115 mainintaa)
- varmuuskopiointi / varmistukset (65 mainintaa)
- koulutuksen puute / vähyys (52 mainintaa)
- ajan tasalla pysyminen / kehityksessä mukana pysyminen (48 mainintaa)

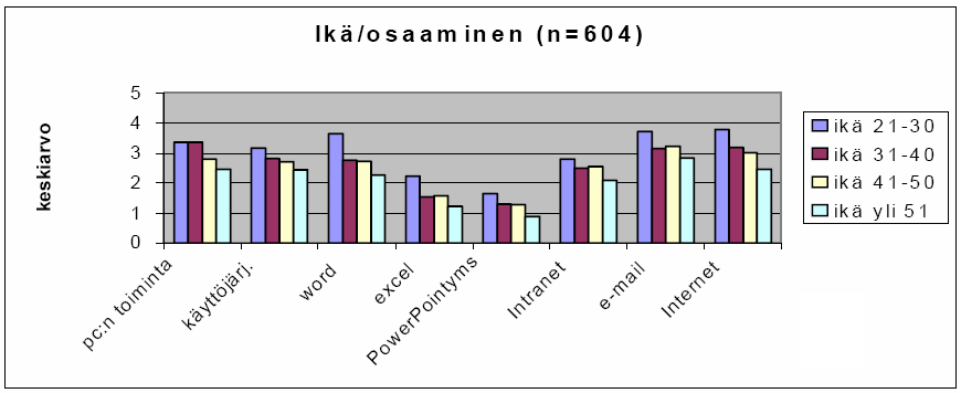
Ainakin 605:n vastauksen osalta, poislukien varmistukset, asiat saataisiin kuntoon pelkästään henkilökunnan koulutuksella. Lisäksi tutkiessani muita vastauksia, joita tässä ei ole esitetty, tuli ilmi, että samansuuntaisia vastauksia oli lisäksi useita muitakin.

10.2.2 Työntekijöiden tietotekninen tieto-/taitotaso vaihtelee

Tietotekniikka on tullut jäädäkseen. Yhä enenevässä määrin yritykset/organisaatiot ottavat erilaisia tietoteknisiä välineitä ja sovelluksia käyttöönsä helpottaakseen/tehostaakseen esimerkiksi sidosryhmien välistä tiedonsiirtoa ja liiketoimintaprosessejaan. Tietoteknisin välinein tietoa on helppoa liikutella myös sellaisille tahoille, joille se ei välttämättä kuuluisi ollenkaan. Vaikka tietoturvaa ei saisi nähdä pelkkänä tekniikkana, näyttelee tekniikka tietoturvan osalta kuitenkin melkoisen suurta osaa. Voidaanhan toisaalta ajatella, että jos tekniikkaa ei olisi, ei olisi myöskään tekniikan käyttäjiä ja tekniikkaa osaamattomien käyttäjien tuomia tietoturvaongelmia.

Selvää on, että työntekijöiden tietotekninen osaamistaso vaihtelee varsin paljon. Mutta toisaalta sekä osaamattomuus että osaaminen kummatkin voivat aiheuttaa tietoturvaongelmia. Tietoteknisessä osaamattomuudessa on kyse siitä, ettei välineitä osata käyttää, jolloin tietoa voi joutua vahingossa vääriin käsiin. Tietoteknisessä osaamisessa taas voi olla kyse moraalisista ongelmista ja asenteesta. Tässä tapauksessa vaikka osataan ja tiedetään, niin salaista tai luottamuksellista tietoa voidaan haluta käyttää esimerkiksi omaksi hyväksi tai jonkun muun henkilön hyväksi. Toisaalta edes tietotekninen osaaminen ei välttämättä takaa teknisenkään tietoturvan osaamista, mutta ainakin helpottaa tekniseen tietoturvaan liittyvien asioiden kouluttautumista.

Kuopion yliopistossa tehdyn pro gradu -tutkielman (2005) mukaan, jossa selvitettiin potilaan hoitoon osallistuvan henkilöstön tietoteknistä osaamista ja koulutustarvetta eräässä Helsingin ja Uudenmaan sairaanhoitopiirin sairaalassa, todettiin iällä olevan vaikutusta tietotekniseen osaamiseen. Iän ja tietoteknisen osaamisen vertailun perusteella nuoremmat hallitsevat paremmin tietotekniset ohjelmistot ja sovellukset kuin vanhemmat työntekijät (von Fieandt 2005:2). Kuviosta 1 voidaan nähdä kaaviokuva kyseisestä tutkimuksesta. Tutkimuksessa käytettiin asteikkoa 0-5 osaamisen arvioinnista. Asteikossa 0 tarkoitti ei lainkaan, 1 huonosti, 2 melko huonosti, 3 kohtalaisesti, 4 hyvin ja 5 erittäin hyvin.



Kuvio 6. Vastaajien ikä ja tietotekninen osaaminen (von Fieandt 2005:34).

Tutkimusta ei tietenkään voida yleistää koskemaan kaikkia organisaatioiden/yritysten palveluksessa olevaa henkilökuntaa, mutta myös oman opettajakokemukseni osalta voisin sanoa, että tulos on vähintäänkin suuntaa antava myös suuremmassa mittakaavassa. Käytännössä tämän suuntainen tulos tarkoittaisi, että tietoteknisen tietoturvakoulutuksen lisäksi vanhemmille henkilöille pitäisi antaa ensin koulutusta tietoteknisestä perusosaamisesta. Onhan selvääkin, että vanhemmalla sukupolvella ei voi olla yhtä pitkälle kehittyneitä tietoteknisiä taitoja verrattuna nuorempaan. Tämä johtuu siitä, että vanhemman sukupolven on täytynyt nämä taidot opetella vasta myöhemmällä iällä. Täytyy kuitenkin ottaa huomioon se tosiasia, että vanhempaan ikään ehtineillä on yleensä enemmän muita yrityksen/organisaation menestymiseen tarvittavia taitoja.

Lisäksi samasta pro gradu -tutkielmasta selviää, että tietoteknisessä osaamisessa on eroja myös ammattiryhmittäin. Onhan selvää, että päivät työssään tietokonetta käyttävät osaavat tietotekniset taidot paremmin kuin sellaiset henkilöt, jotka käyttävät tietokonetta harvoin. Lisäksi tähän vaikuttaa myös harrastuneisuus. Joka tapauksessa koulutukseen lähtevien henkilöiden osaamistasoa pitäisi pystyä jollakin tavalla mittaamaan, jonka jälkeen henkilöt jaetaan eri tasoisiin osaajaryhmiin. Tällaista osaamistason mittausta ja henkilöiden jakamista eri ryhmiin voi mielestäni vaatia myös kouluttajalta, ettei yrityksen tarvitse käyttää siihen voimavarojaan.

10.3 Tietoturvaohjeita ei ymmärretä

Työntekijät eivät aina ymmärrä ohjeistuksen tosiasiallista tarkoitusperää organisaation kannalta. Mikä merkitys ohjeilla on? Mitä ohjetta noudattamalla saavutetaan?

Usein ohjeistus myös kirjoitetaan liian teknisestä näkökulmasta, asioita kuvataan yksityiskohtaisesti ja vaikeilla termeillä, joita on vaikea ymmärtää. Tämä johtuu siitä, että usein ohjeiden kirjoittaminen annetaan organisaatiossa tietoteknisille henkilöille. Näin ollen henkilön, joka ei ole tekniikkaorientoitunut, on vaikea ymmärtää ohjeen tosiasiallista sisältöä. (Karin Höne & J.H.P. Elof 2002:15.)

Lisäksi Kyrölän (2001:30) mukaan tietoturvallisuuteen suhtaudutaan leväperäisesti, koska tietoturvallisuuteen liittyviä ohjeita on paljon, eikä tietoa etsivä pysty helposti löytämään häntä velvoittavia ohjeita.

Siponen (2000:36) puolestaan on todennut, että usein ongelmana on, että työntekijät tietävät tietoturvaohjeistuksesta ja ohjeistakin, mutta syystä tai toisesta eivät onnistu noudattamaan niitä. Käytännössähän tämä tarkoittaa, että työntekijät eivät osaa soveltaa ohjeita omaan työhönsä. Tähänkin vastauksena on koulutus. On siis turha käydä tietoturvaohjeita läpi ja kouluttaa työntekijöitä pelkästään noudattamaan ohjeita. Työntekijöille pitäisi näyttää kädestä pitäen, miten kutakin tietoturvaohjetta sovelletaan käytännössä. Siponen (2000:36) onkin korostanut, että

menestyvä tietoturvavalveutuneisuuden koulutus vaatii enemmän kuin ohjeiden antamisen työntekijöille.

Siponen (2000:36) on myös esittänyt, että ohjeiden ongelmana on usein, ettei ohjeita perustella relevantisti. Hänen mukaansa ohjeet pitäisi aina perustella koska vain sillä tavalla ihmisten kognitiivista eli tiedollista tilaa voidaan muuttaa. Tällöin on myös todennäköisempää, että ihmisten asenne ja motivaatio ohjeita kohtaan muuttuu. Ohjeiden perusteluksi ei toki riitä vain sanoma siitä, että näin on määrätty tekemään tai näin on vain aina tehty tai että muuallakin tehdään tällä tavalla.

Yksi tietoturvaohjeiden noudattamisen vaikeus varmasti tulee esille siinä, että esim. teknisillä laitteilla verkossa liikennöitäessä ihminen ei näe, miten tietoturvaohjeiden laiminlyöminen käytännössä realisoituu. Tarkoittaen sitä, että ihminen ei näe konkreettisesti, mitä voi tapahtua, jos jätän tämän ohjeen noudattamatta. Mutta jos esimerkiksi hitsaat koko päivän ilman suojamaskia, niin tiedät seuraavana päivänä varmasti rikkoneesi työturvallisuussääntöjä. Sillä silmiä kirveltää, ne valuvat vettä ja ovat auringonlaskun punaiset. Tämän jälkeen aivan varmasti käytät suojamaskia. Kun tietoturvaohjeiden noudattamatta jättäminen realisoituu, sitä ei välttämättä huomata heti. Voi mennä puoli vuotta tai vuosi ennen kuin todetaan esim. yrityksen palvelimella sijaitsevan väärää tietoa. Silloin voi olla jo myöhäistä edes reagoida tilanteeseen. Jäljityskään tuskin enää onnistuu.

10.4 Työntekijöitä ei oteta mukaan suunnitteluun – standardit asetetaan työntekijöiden edelle

James (1996:10) on todennut tietoturvan hallintaan ja suunnitteluun olevan monia tieteen keinoin luotuja tavanomaisia menettelytapoja. Tavallisesti nämä tavat ovat strukturoituja arviointikäytäntöjä ja matemaattisesti painotettuja arviointitapoja ja malleja. Nämä menettelytavat jakaantuvat Jamesin mukaan neljään pääryhmään, joita ovat: auditointi- ja tarkistuslistat, riskianalyyseihin perustuvat metodit, kustannuksiin keskittyneet metodit ja korkean tason käsitteellisiin johtamismalleihin perustuvat metodit. Nämä mallit eivät ole kuitenkaan toisiaan pois sulkevia, vaan niitä on käytetty monien suunnitelmien osalta yhdessä.

Jamesin mukaan nämä tavanomaiset mallit eivät kuitenkaan näytä toimivan, sillä niille kaikille on yhteistä se, että ihmisiä ei oteta mukaan suunnitteluun, menettelytapojen joustamaton rakenne, esimiesten puutteellinen tuki tai osallistuminen. Lisäksi menettelytavat voivat olla akateemisia ja teoreettisia, niitä on vaikea soveltaa käytäntöön ja ne perustuvat tieteellisiin metodeihin, jotka eivät ole sopivia ihmisiin liittyvissä järjestelmäympäristöissä. Eniten James on huolissaan juuri vähäpätöisestä ihmisten mukaan ottamisesta.

Myös Siponen (2006:41) on todennut, että erilaisissa tietoturvaan liittyvissä standardeissa kuten BS7799 tai ISO/IEC 17799 heikkoutena ovat oletukset, joilla ohjataan kaikki organisaatiot tietyn yleisen ratkaisun pariin. Tietoturvan kehittämisen todellisen kysymyksen tulisi kuitenkin

lähteä siitä, pitäisikö yksittäisen organisaation tehdä oma erityinen omia toimintojaan vastaava tietoturvan vaatimuslista? Tämä tarkoittaa käytännössä sitä, että tietoturvaan liittyviä suojauksia ei tule tehdä turhissa kohteissa, vaan täytyy ymmärtää milloin suojaus on tarpeellinen ja milloin se on rahanhukkaa. Standardien idea usein Siposen (2006:42) mukaan onkin, että tietoturva on kuin tavaraa, jota voi ostaa kaupan hyllyltä, vaikka todellisuudessa tietoturva on monimutkainen organisaatiokohtainen kysymys. Toteuttamalla tietoturvaa pelkästään sen takia, että se esiintyy standardissa tai tarkistuslistassa aiheuttaa luultavasti työntekijöiden tyytymättömyyttä, koska yleispätevä suojaus ei vastaakaan käyttäjien vaatimuksiin, organisaatiokulttuuriin tai liiketoiminnan päämääriin (ibid.). Standardien ja tarkistuslistojen heikkoja kohtia ovat Siposen mukaan nimenomaan niiden yleispätevyys sekä sosiaalisten kysymysten lähestyminen kuin ne olisivat teknisiä tietoturvaongelmia.

10.5 Yksi henkilö tai osasto sanelee ehdot, joilla tietoturvaa tehdään

Yhden henkilön tai tietotekniikkaosaston näkemyksen mukaan toimivaa norsunluutornista johdettavaa tietoturvakulttuuria on erittäin vaikea toteuttaa missään organisaatiossa. Tietoturvan vaatimuksia ei ole kartoitettu työntekijöiden kanssa, vaan on otettu käyttöön tekniikka, joka on perusteltu tietotekniikkaosaston näkemyksen mukaan ja laitettu se kentälle käytettäväksi. Tämä johtaa väistämättä erilaisiin ongelmiin. Varsinainen tuottelias työnteko voi häiriintyä ja työntekijät ottavat käyttöön erilaisia omia keinoja, joilla voivat kiertää työntekoa hidastavan ohjelman tai laitteen.

Tietoturvaa suunnittelevien henkilöiden on otettava tarkemmin huomioon kentällä työskentelevien työntekijöiden tarpeet ja suunnitella tietoturvaan liittyvät toimenpiteet vasta tarpeiden määrittelyn jälkeen. Siksi on erittäin tärkeää, että työntekijät, jotka lopulta käyttävät tietoturvaan liittyviä ohjelmia, välineitä yms. otetaan mukaan tietoturvan suunnitteluun. Tietoturvan suunnitteluprosessi täytyisi olla kuten mikä tahansa tietojärjestelmän suunnitteluprosessia vastaava tapahtuma, jossa tehdään yhdessä loppukäyttäjien kanssa vaatimusmäärittely ja vasta vaatimusmäärittelyn jälkeen suunnitellaan ja toteutetaan.

Toisaalta yrityksessä voidaan kuvitella tietoturvallisuuden olevan ”tietoturvallisuusvastaavan” murhe, jolloin yksittäisen työntekijän ei tarvitse tietoturva-asioilla vaivata päätään. Tällaisessa tapauksessa yksilön oma vastuu tulisi määritellä selkeästi. Lisäksi uhkakuvat tulisi osoittaa sekä positiivisten että negatiivisten esimerkkien avulla henkilön oman työn kautta. (Koivunen 2002:14.)

10.6 Riskien vakavuutta ei osata arvioida

Riskit ovat jokapäiväistä elämäämme. Teemme jatkuvasti päätöksiä kohdatessamme erilaisia riskejä. Onko turvallista ylittää tie? Voinko luottaa luottokorttini tarjoilijalle? Onko jonkun tavaran tai tuotteen osto hyvä investointi? Lista riskeihin liittyvistä päätöksistä on loppumaton. Kuitenkin samalla, vaikka olemme hyviä tekemään arkipäivän valintoja, on

vaikeaa arvioida riskejä työelämässä. Erityisen vaikeaksi riskien arviointi tulee tilanteessa, jossa on tekniikkaa mukana. Jokainen tietää, että riskejä on, mutta ei osaa arvioida, kuinka suuresta riskistä on kyse tai ei tiedä kuinka riskiä voisi lieventää. (Stanton 2006:18.)

Havana ja Roning (2004) ovat tehneet tutkimuksen jossa tutkittiin Rotuaari hankkeen neljän eri ryhmän asenteita ja käsityksiä tietoturvasta. It-ammattilaisten ja maallikoiden ero tietoturvan osalta on, että vaikka maallikot ovat valveutuneita tietojärjestelmien riskeistä, he eivät silti pysty analysoimaan mahdollisesti toteutuvien riskien vakavuutta. Lisäksi maallikoilla oli epävarmuutta vastuistaan tietoturvan osalta ja varsinkin omista kyvyistään olla vastuussa tietoturvaan liittyvistä asioista. Maallikoille ei ollut selvää, milloin tietoturvaan liittyviä asioita pitäisi ottaa huomioon. Myös it-ammattilaiset olivat yhtä mieltä siitä, että vaikka tiedettäisiin tietoturvallisuudesta paljon, omaan tietoturvatasoonsa ei välttämättä ole mahdollisuutta vaikuttaa.

10.7 Tietojärjestelmät ja tietoturva ovat abstrakteja käsitteitä

Ongelmana on, että tietojärjestelmät on abstrakti käsite. Tietojärjestelmien tietoturva ei ole nähtävissä eikä kosketeltavissa oleva. Siksi ihmisillä on vaikeuksia ymmärtää ja käsitellä riskejä, joita liittyy tietojärjestelmien tietoturvaan (Havana & Roning 2004). Tietoturvasta on vaikea saada konkreettista ja/tai näkyvää esimerkkiä. Ongelmaksi tulee, että työntekijän aikaansaamat toimenpiteet eivät näy työntekijälle itselleen konkreettisesti. Tämä johtaa väistämättä sellaiseen tilanteeseen, kun mitään näkyvää ei kerran tapahdu, niin oletetaan asioiden olevan kunnossa. Toisin asia on kuitenkin esimerkiksi kiinteistön suojauksessa. Suojaamiseen käytetään lukkoja, kulkuoikeuksia ja hälytysjärjestelmiä. Kiinteistön suojaus onkin huomattavasti helpompi perustella ja esittää konkreettisesti ja näkyvästi. Juuri tietoturvan abstraktiuden takia on varmasti tilanteita, jolloin johdossa ei oteta tietotekniikkariskejä vakavasti. Ollaan siinä uskossa, että kaikki on hyvin, kun mitään ei tapahdu.

10.8 Motivaatio ja asenne eivät ole kohdallaan

Tietoturvallisuus taataan pienin teoin muistuttaa Petri Puhakainen Turvallisuus lehden artikkelissa (Koskivirta 2006:14). Puhakaisen mukaan tietoturvallisuudesta pieni osa hoidetaan tekniikan avulla. Suurin osa tietoturvallisuudesta hoidetaan henkilöstön tietoturvallisen käyttäytymisen avulla. Tämän vuoksi henkilöstöä on Puhakaisen mukaan tärkeää motivoida käyttäytymään tietoturvallisesti. Henkilöstön motivaation lisäämisessä on tärkeää, että esimerkiksi tietoturvasäännöt sovitaan yhteisesti henkilöstön ja esimiesten kesken. Tietoturvasääntöjen jalkauttaminen ylhäältä alaspäin ei ole Puhakaisen mielestä välttämättä tuloksellisin vaihtoehto. (Koskivirta 2006:14.)

Suorituskyky riippuu kyvystä/taidosta tehdä jotakin, motivaatiosta ja työoloista. Nämä asiat ovat jatkuvasti vuorovaikutuksessa toistensa kanssa. Motivaation vaikutus suorituskykyyn riippuu kyvystä/taidosta tai kyvyn/taidon vaikutus suorituskykyyn riippuu motivaatiosta. Motivaati-

olla on taipumus olla dynaaminen eli kestää minuuteista viikkoihin kun taas asenne on enemmänkin staattinen ja sisäistetty ja voi kestää kuukausista vuosiin. Asenne vaikuttaa pääasiassa toiminnan laadukkuuteen samalla kun motivaatio korreloi toiminnan tason kanssa.

Mitä tulee esimerkiksi tietoturvaohjeiden noudattamiseen, niin usein työntekijät noudattavat ohjeita, kun niin on sanottu. Tällöin he ovat ulkoisesti motivoituneita. Sisäisen motivaation vallitessa ihmiset ovat vapaita tekemään omia valintojaan eli heillä on oikeus päättää ”omista” asioistaan. Tämä tarkoittaa yleensä sitä, että ihmiset perustelevat tekemisensä omiin pyrkimyksiin perustuen. Pohjimmiltaan itsemääräämisoikeus on ratkaiseva tekijä määrittelemään, onko joku ulkoisesti vai sisäisesti motivoitunut. Peruskysymys tietoturvaohjeiden kannalta onkin, että vaikuttavatko omat pyrkimykset, kyvyt ja delegoidut tietoturvaohjeet yksilön vapauteen. Tarkoittaen siis, miten tietoturvahenkilöt voivat iskostaa käyttäjien ajatuksiin sellaisen vapauden tunteen, että he rohkenevat ottaa aktiivisesti osaa tietoturvan kehittämiseen siitä syystä, että tuntevat olevansa osallisena tietoturva-asioihin liittyvässä päätöksen teossa. (Siponen, Mikko T. & Kajava, Jorma:1998.)

11 Pk-yritysten paremman tietoturvakulttuurin muodostumiseen liittyvät heikkoudet ja vahvuudet

Pk-yrityksillä on tiettyjä vahvuuksia mutta myös heikkouksia paremman tietoturvakulttuurin muodostumiseen verrattuna suurempiin yrityksiin. Näitä vahvuuksia ja heikkouksia esittelen tässä kappaleessa.

Ennen kuin näitä vahvuuksia pystytään kartoittamaan, täytyy määritellä mitä ovat pk-yritysten erityispiirteet. Ilona Iivonen on tutkimuksessaan (2006:2)[4] määritellyt näitä pk-yrityksille ominaisia erityispiirteitä seuraavasti:

- *Taloudellinen suoriutuminen*. Pk-yritykset tekevät kokoonsa suhteutettuna parempaa tulosta kuin suuret yritykset.
- *Innovaatiot*. Pienissä yrityksissä ympäristö on avoimempi luovuudelle ja uusille ideoille. Henkilöstön toimenkuvat ovat laajempia, mikä myös osaltaan antaa tilaa innovatiivisuudelle.
- *Kasvu ja työpaikkojen luominen*. Pienet yritykset luovat kasvun kautta uusia työpaikkoja suhteessa enemmän kuin suuret yritykset.
- *Alihankintasuhteet*. Pienet yritykset ovat usein toimitussuhteessa isoihin organisaatioihin.
- *Toimintaympäristö*. Pienet yritykset ovat alttiita markkinoiden muutokselle. Selvitäkseen niiden pitää kyetä nopeisiin muutoksiin.
- *Organisaatiorakenne*. Pienen työntekijämäärän vuoksi organisaatio on matala, ja ylimmätkin esimiehet lähellä alaisiaan.
- *Infrastruktuurin tarve*. Pienten yritysten käytössä olevat tietojärjestelmät ovat yksinkertaisempia kuin isojen yritysten.
- *Budjetti*. Koska yritysten koko on pieni ja liikevaihtokin siksi rajallinen, muuhun kuin suoraan tuottavaan työhön budjetoitavat varat ovat rajallisia.
- *Toiminnan kontrolli*. Koska yrityksissä on matala organisaatio, ei päivittäisten toimintojen ohjaus ole niin hierarkista.

Nämä listatut erityispiirteet ovat tietoturvakulttuurin muodostumisessa joko vahvuuksia tai heikkouksia. Seuraavaksi pohdintaa näistä heikkouksista ja vahvuuksista lueteltujen erityispiirteiden osalta.

11.1 Vahvuudet erityispiirteiden osalta

Luovuudelle ja uusille ideoille avoin ympäristö tarjoaa mielestäni erittäin hyvät puitteet tietoturvakulttuurin muutokselle parempaan suuntaan. Jos ympäristö on avoin, niin henkilöstö pystyy muutokseen paremmin ja nopeammin verrattaessa vanhoihin tapoihin pinttynyttä suurta yritystä. Ongelmaksi voi kuitenkin tulla jo muodostuneet toimintatavat varsinkin jos yrityksellä on pitkä historia. Pk-yrityksen selvä vahvuus on kuitenkin matala organisaatiorakenne, jossa ylimmätkin esimiehet ovat lähellä alaisiaan. Tämä vaikuttaa esimerkiksi nopeaan viestin perille menoon vaikkapa tietoturvaohjeiden päivitysten yhteydessä. Matalasta organisaa-

[4] Alkuperäinen lähde: Botha, J ja von Solms, R 2004. A cyclic approach to business continuity planning. Information Management & Computer Security 12 (4), 328-337.

tiorakenteesta johtuva esimiesten ja työntekijöiden suora suusta suuhun kommunikointi voi ainakin mahdollistaa, että työntekijät noudattavat esimiesten toiveita tietoturvan suhteen paremmin verrattuna siihen, että esimiesten ja työntekijöiden välillä olisi vain epäsuoraa kommunikointia. Toki työntekijöiden ohjaaminen tietoturvalliseen toimintaan tarkoittaa myös sitä, että esimiehillä täytyy olla jonkinlaista näkemystä tietoturvakulttuurin muodostumisesta ja siitä millainen yrityskulttuuri omassa yrityksessä tällä hetkellä vallitsee.

Voisi kuvitella, että tapoihinsa urautuneen yrityskulttuurin osalta tarvitaan hiukan järeämpiä otteita, jotta viesti saadaan menemään perille, siten kuin esimiehet haluavat. Toisaalta paljon merkitsee myös se, millainen suhde esimiesten ja työntekijöiden välille on vuosien saatossa muodostunut. Jos esimiehet nauttivat työntekijöidensä arvostusta ja luottamusta, niin viestin perille menemisessä ei luultavasti ole ongelmia. Suora suusta suuhun kommunikointi esimiesten ja työntekijöiden välillä on omiaan luomaan juuri tällaista arvostusta ja luottamusta esimiesten ja työntekijöiden välille. Suurien yritysten osalta suora kommunikointi ei ole von Solmsin ja von Solmsin (2004:275-279) mukaan yleensä mahdollista kahdesta syystä. Ensimmäinen syy on suuri työntekijäjoukko, joka on mahdollisesti vielä fyysisesti levinnyt laajalle alueelle. Toinen syy on suurten yritysten/organisaatioiden johtoportaat. Ylimmillä esimiehillä on harvemmin mahdollisuutta olla suorassa puheyhteydessä työntekijöiden kanssa hierarkisuuden vuoksi.

Matala organisaatiorakenne ja toiminnan kontrolli mahdollistavat myös nopeiden muutosten tekemisen eli sutjakkaan liikkumisen toimintaympäristössään. Lisäksi jos yritys on jo oppinut liikkumaan toimintaympäristössään nopeasti muuttuvilla markkinoilla, niin yritys on tottunut jatkuvaan muutokseen, jolloin muutos tietoturvakulttuuriinkaan ei ole välttämättä kovin ahdistava.

Elisa Oyj:n toimitusjohtajan Veli-Matti Mattilan (Panda Software viikkotiedote 7/2006) mukaan pk-yritykset ovat usein alihankkijana arvoketjussa. Alihankkijana oleminen voi olla vahvuus paremman tietoturvakulttuurin muodostumiselle, koska tällöin pk-yrityksen on yleensä pakko kehittää tietoturvaansa vähintään asiakkaan vaatimusten mukaisesti. Turvallisuus lehden (1/2007) artikkelissa todetaan, että yhä useampi pääurakoitsija vaatii alihankkijoiltaan näyttöä tietoturvallisesta toiminnasta (Kihl 2007:32). Tämä onkin ymmärrettävää, sillä alihankintaketjut ovat usein pitkiä ja ulottuvat useisiin maanosiin (Kihl 2007:32). Toisaalta jos halutaan, toiminta voidaan vain saada näyttämään tietoturvalliselta asiakkaan suuntaan. On täysin eri asia, onko yrityksellä todellista halukkuutta tietoturvansa kehittämiseen vai halutaanko tietoturvasta tehdä vain kulissi asiakkaan suuntaan? Toisaalta jos halukkuutta ei ole, niin yritys syö yleensä vain omaa leipäänsä.

11.2 Heikkoudet erityispiirteiden osalta

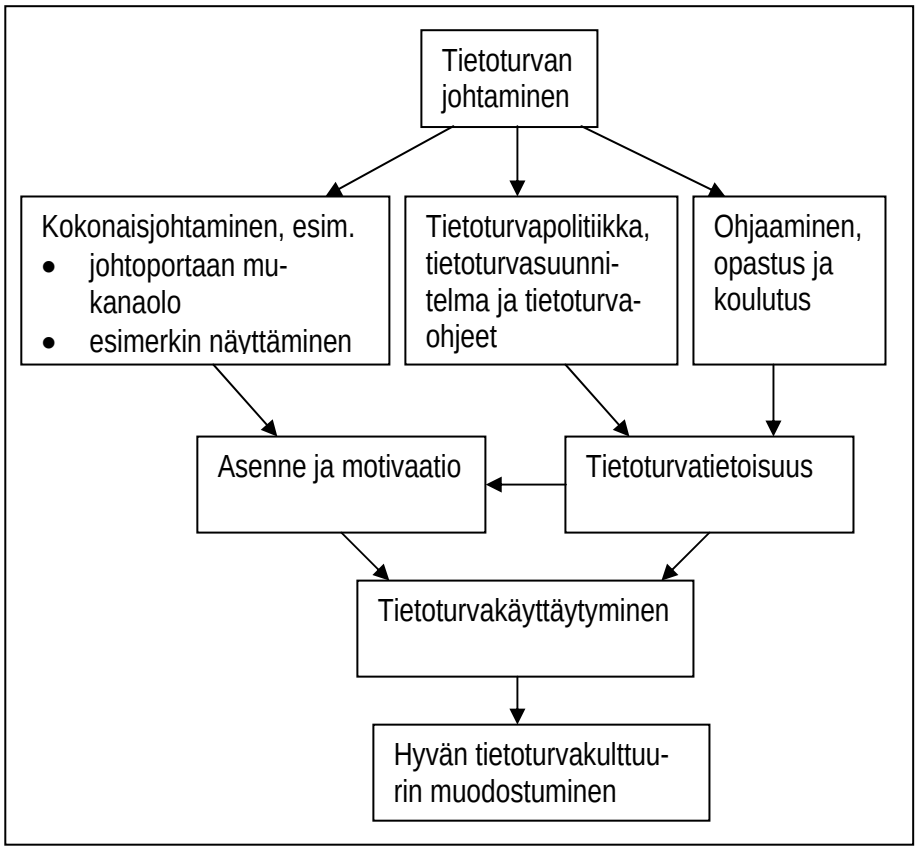
Pk-yrityksen heikkoutena tietoturvakulttuurin muodostumiseen ovat mm. resurssien riittävyys sisäisen toiminnan kehittämiseen, toimintaympäristön muutokset ja henkilöstön toimenkuvien laajuudet.

Pk-yrityksissä muuhun kuin suoraan tuottavaan työhön budjetoitavaa rahaa on vähemmän kuin suuremmissa yrityksissä. Toimintaympäristön nopeisiin muutoksiin on totuttu, mutta useat muutokset voivat vähentää esimerkiksi tuotteiden tai palveluiden kehittämishalua. Kun muutoksilta tulee hengähdystauko, halutaankin tehdä välillä vain rutiininomaisia asioita. Henkilöstön toimenkuvien laajuus johtaa osaltaan siihen, ettei työntekijöillä ole aikaa keskittyä kuin oman toimensa hoitamiseen. Asioihin ei ehdi kunnolla perehtymään ja niitä täytyy saattaa eteenpäin nopeilla ja harkitsemattomilla päätöksillä. Toimenkuvien laajuudet johtavat siis väistämättä kiireeseen. Siispä tingitään koulutuksesta ja uuden oppimisesta. Kehittämiseen ja oman osaamisen täydentämiseen/laajentamiseen ei ole aikaa.

Pk-yrityksien tietoturvaongelmat liittyvät resurssiongelman myötä osaamisen puutteeseen. Pk-yrityksen ei kannata palkata henkilöä, joka huolehtii tietokoneiden ja tietoverkon ylläpidosta saati sitten tietoturva-asiantuntijaa. Mahdollisuudet jäävät yleensä siihen, että joku työntekijä huolehtii näistä asioista muun työnsä ohella. Tämän lisäksi vaativammat työt on usein ulkoistettu. Suurissa yrityksissä asiantuntijan palkkaaminen tietoturvan ylläpitämiseen onnistuu, koska hoidettavien asioiden määrä kasvaa sen verran lukuisaksi, että työntekijä kannattaa palkata. Kuten kauppa- ja teollisuusministeriön selvityksessä (Pk-yritysten tietoturvakysely 2006 [2007:58]) todettiin, suurin puute tietotekniikka-/tietoturva-asioissa olivat osaaminen, tietämättömyys, tiedon puute ja ammattitaidottomuus. Toiseksi suurin heikkous oli oma/yrittäjän osaaminen ja ammattitaito. Kolmanneksi suurin vaje oli henkilökunnan ja käyttäjien atk-osaaminen.

12 Paremman tietoturvakulttuurin muodostaminen pk-yrityksiin esimiesten toimilla

On selvää, että tietoturvakulttuuriin voidaan vaikuttaa hyvällä johtamisella, arvojen laatimisella ja ohjaamisella, koulutuksella ja opastuksella. Tietoturvallisuuden arvot eli tietoturvapolitiikka ja tietoturvasuunnitelma on yksi keino vaikuttaa paremman tietoturvakulttuurin muodostamiseen. Tietoturvakulttuurissa arvot ilmaisevat, mikä on toivottavaa tietoturvallista käyttäytymistä työntekijöiden taholta. Lisäksi koulutuksella, ohjaamisella ja opastuksella voidaan vaikuttaa, että työntekijät varmasti osaavat toimia näiden arvojen mukaan ja kokonaisjohtamisella vielä tuetaan toivottua arvojen mukaista käyttäytymistä (ks. kuvio 7).



Kuvio 7. Hyvä tietoturvakulttuuri muodostuu hyvästä johtamisesta, johtajien luomista arvoista ja tietoturvatietoisuuden lisäämisestä.

12.1 Tietoturvapolitiikka ja tietoturvasuunnitelma

Pk-yritysten esimiesten tulisi tiedostaa, että ensimmäinen asia jolla työntekijöiden käyttäytymistä pystytään ainakin jonkin verran ohjaamaan tietoturvallisempaan suuntaan, on tietoturvapolitiikan ja tietoturvasuunnitelman luominen ja näiden jalkauttaminen tavalla tai toisella työntekijöiden tietoon. Kauppa- ja teollisuusministeriön tietoturvallisuuskyselyn mukaan vain 21 % Suomen pk-yrityksistä on laadittu tietoturvapolitiikka ja vain 14 % on kirjallinen tietoturvasuunnitelma (Pk-yritysten tietoturvakysely 2006 [2007:26]). Tässä olisi huimasti parantamisen varaa.

Tietoturvallisuuskulttuuri muodostuu kolmesta tasosta, kuten kappaleessa 9 on todettu. Nämä tasot ovat artefaktit, arvot ja perusoletukset. Arvot ovat kirjoitettuja arvoja ja edustavat sitä, millaiselta yritys haluaisi tietoturvallisuuden tilan yrityksessä olevan. Näillä arvoilla on mahdollista vaikuttaa ihmisten käyttäytymiseen, koska ne ilmaisevat, mitä pidetään toivottavana tai tavoittelemisen arvoisena tietoturvakäyttäytymisenä. Olisi kuitenkin erittäin tärkeää, että nämä esimiesten laatimat arvot osattaisiin tuoda oikealla tavalla työntekijöiden tietoisuuteen ja perustella niiden tärkeyttä ja niiden mukaan toimimista. Vielä tärkeämpää kuitenkin on, että esimiehet osaavat laatia nämä arvot oikein, koska arvojen perusteella työntekijöiden tulisi laatia itselleen tietoturvaohjeet esimiesten ja esimerkiksi ulkopuolisen konsultin johdolla. Myös esimiesten kannattaa käyttää arvojen laatimisessa ulkopuolista apua, ellei oma ammattitaito tunnu riittävän. Toisaalta jo arvojen laatimiseen kannattaa käyttää myös työntekijöiden ammattitaitoa, koska heiltä voi tulla hyviä ehdotuksia. Lisäksi kun arvot tulevat työntekijöiden keskuudesta, niihin sitoudutaan paremmin verrattuna siihen jos esimiehet olisivat ne laatineet.

12.2 Kokonaisjohtaminen

Sanotaan, että tietoriskien hallinnasta 20 % taataan teknisin ratkaisuin ja 80 % taataan työntekijöiden toiminnan ja esimiesten johtamisen tuloksena (Kyrölä 2001: 28). Siksi ennen kaikkea työntekijöiden johtamistavat tietoturvalliseen käyttäytymiseen tulisi olla kunnossa. Työntekijät täytyisi saada itse arvioimaan ja ajattelemaan omaa toimintaansa tietoturvan kannalta. Oman työnteon ohessa pitäisi pystyä jatkuvasti myös kehittämään tietoturvallisia toimintatapoja. Ei riitä, että yksi noudattaa sääntöjä, vaan kaikkien on sitouduttava yhteiseen asiaan. Työntekijöiden sitoutuminen tietoturvaan vaatii esimiehiltä esimerkin antamista ja taitavaa johtajuutta. Toki tietoturvallinen käyttäytyminen vaatii myös työntekijöiltä tietynlaisia tietoja ja taitoja, jotka kuitenkin on mahdollista saavuttaa koulutuksella. On yrityksen edun mukaista, että eri osaajat pystyvät vastuualueellaan tunnistamaan arkityön tietoriskit (Kyrölä, 2001:137).

Esimiesten tietoturvaan sitoutuminen tulisi näkyä myös heidän omassa käyttäytymisessään. Kiireestään huolimatta muun henkilöstön kanssa pitäisi osallistua tietoturvaa koskeviin koulutuksiin ja muihin tilaisuuksiin. Ohjeita ja sääntöjä täytyy noudattaa aivan samalla tavalla kuin muukin henkilöstö tekee. Esimerkkiä on siis näytettävä. Lisäksi vahingossakaan

ei saisi omilla sanomisillaan antaa ristiriitaisia viestejä tietoturvan suhteen. Muussa tapauksessa esimiehet voivat hyvinkin tehokkaasti romuttaa henkilöstön jo omaksumat tietoturvaperiaatteet. Henkilöstö tarkkailee esimiesten toimia ja tekee hyvin helposti ja nopeasti johtopäätöksiä (myös vääriä) kaikesta, mitä esimiehet tekevät tai sanovat. On turha luulla, että muu henkilöstö käyttäytyisi tietoturvallisesti, jos talon esimiehetkään eivät noudata sääntöjä tai antavat ristiriitaisia signaaleja toiminnallaan ja puheillaan.

Tämän vuoksi olisi ajoittain erittäin tärkeää esimiesten vahvistaa omaa viestiään henkilöstölleen tietoturvan tärkeydestä erilaisissa kahvipöytäkeskusteluissa ja kokouksissa. Tietoturvallisuuden johtamisessa, kuten niin monessa muussakin johtamisessa kyse on ihmisten johtamisesta eikä asioiden johtamisesta. Kyrölä (2001:30) on todennut, että tieto syntyy ihmisten toiminnan tuloksena. Lopulta kyse onkin siitä, miten johtaa ihmisiä tietoturvalliseen käyttäytymiseen.

Pk-yritysten esimiesten olisi tärkeää käyttää pk-yrityksen vahvuuksiin liittyviä asioita hyväksi. Suora kommunikaatio esimerkiksi esimiesten ja työntekijöiden kesken on tällainen vahvuus. Vääriin toimintatapoihin päästään heti puuttumaan ja niitä on rakentavasti keskustelemalla suhteellisen vaivaton kehittää tietoturvallisemmaksi. Lisäksi organisaatiorakenteen mataluuden ja muutoksiin tottuneen organisaation vuoksi muutoksia on suhteellisen helppo tehdä, koska työntekijät ovat tottuneet niihin. Näin ollen muutosvastarintaa ei välttämättä esiinny kovin paljoa. Ennen muutokseen ryntäystä esimiesten olisi kuitenkin syytä pysähtyä miettimään, millainen yrityskulttuuri yrityksessä tällä hetkellä vallitsee. Vanha yritys on jo usein tottunut hyviksi todettuihin toimintatapoihin, joita voi olla vaikea muuttaa. Siksi muutokseen liittyvä strategian luominen on esimiehille erittäin tärkeää.

Työntekijöiden osallistaminen

Mitä ovat sitten ne johtamistavat, joilla työntekijät saadaan miettimään ja kehittämään omaa toimintaansa? Petri Puhakainen puhuu henkilöstön motivoinnista käyttäytymään tietoturvallisesti (Koskivirta 2006:14). Puhakaisen mukaan esimerkiksi tietoturvasäännöt tulisi sopia yhteisesti henkilöstön ja esimiesten kesken. Jos tietoturvaohjeistusta yritetään jalkauttaa vain ylhäältä annettuna, niin tulos on huono. Puhakaisen mukaan (Koskivirta 2006:14) henkilöstö pitää motivoida tekemään pieniä ja tärkeitä tietoturvallisuutta edistäviä toimenpiteitä. Motivaation lisäämisessä on aina kyse ihmisten eikä asioiden hyvästä johtamisesta. Puhakaisen mukaan hyvän johtamisen näkee henkilöstön käyttäytymisestä. Jos henkilöstö käyttäytyy tietoturvallisesti, niin se yleensä paljastaa, että esimiehet ymmärtävät tietoturvallisuudesta ja ovat motivoituneita sitä toteuttamaan. Puhakainen painottaa esimiesten esimerkkiä tietoturvasääntöjen noudattamisessa. On turha luulla, että henkilöstö käyttäytyisi tietoturvallisesti, jos talon esimiehetkään eivät noudata sääntöjä.

Kvistin, Miekkavaaran ja Poutasen (2004:31) mukaan ihmiset motivoituvat onnistumisista ja saavutuksista, huomiosta, kehittymismahdollisuuksista ja mielenkiintoisesta työstä. Sitoutumisella eli myönteisellä tunteella työtä kohtaan on merkittävä vaikutus suorituksiin (Kvist ym. 2004:31). Sitoutuminen syntyy, jos ihmisen henkilökohtaiset tarpeet ja tavoitteet otetaan tavoiteasettelussa oikein huomioon. Kvist ym. toteaa myös, että joukkueen jäsenellä on oltava riittävästi osaamista, jotta hän kykenee suorittamaan työtehtävänsä hyvin, mutta myös työympäristön on tarjottava hänelle mahdollisuudet hyviin suorituksiin. Eniten Kvistin ym. (2004:31) mukaan suorittajan toiminnan määrään ja laatuun vaikuttaa kuitenkin hänen motivaationsa, halunsa tehdä työtä. Sisäinen motivaatio liittyy tilaisuuteen käyttää omia kykyjä, kokea saavutuksia ja toimia itsenäisesti.

12.3 Ohjaaminen, opastus ja koulutus

Tietoturvallisuuskoulutus tietoturvalliseen toimintaan täytyy hoitaa Puhakaisen mielestä erilaisissa arkipäivän tilanteissa, kuten ryhmäpalavereissa, kehityskeskusteluissa ja työntekijöiden välisissä keskusteluissa. Tässä varsinkin pk-yrityksen matalasta organisaatiorakenteesta on hyötyä. Viesti saadaan perille kaikille työntekijöille nopeasti ja tehokkaasti ja/tai mahdollisesti vielä henkilökohtaisesti suoralla kommunikoinnilla esimieheltä työntekijälle.

Puhakainen toteaa artikkelissaan (2005:17), että tietoturvaa ei voida merkittävästi parantaa muuttamalla vain muutamien henkilöiden käyttäytymistä. Muutos pitäisi viedä läpi koko organisaation. Puhakainen (2005:17) on myös todennut, että yrityksissä tietoturvakoulutukseen ei useinkaan ole käytössä kovin paljoa resursseja. Siksi koulutuksessa pitäisikin keskittyä kunkin työntekijäjoukon kannalta olennaisiin asioihin. Tavoitteiden saavuttamisessa auttaa Puhakaisen (2005:17) mukaan systemaattinen suunnittelu, joka ottaa huomioon työntekijöiden erilaiset tehtävänkuvat, tiedollisen ja taidollisen lähtötason, ennakkoasenteet, yrityksen liiketoiminnan sanelemat tietoturvatarpeet ja käytettävissä olevat resurssit. Koulutuksen tavoitteena tulisi olla myös työntekijöiden motivointi tietoturvaa kohtaan ja tätä kautta pysyvä asenteiden muuttuminen toteaa Puhakainen.

Lisäksi Puhakainen (2005:18) jatkaa, että pelkkä passiivinen tiedon vastaanottaminen ei kuitenkaan tähän riitä. Vain aktiivinen ajattelu ja yhdessä osallistuminen tuottaa pysyviä asennemuutoksia. Esimerkiksi pitkät kalvosarjat tai passiivinen verkko-opetus eivät yleensä tuota oppimista, joka näkyisi käyttäytymisen muutoksena. Puhakaisen (2005:18) mukaan eräs mahdollinen motivoinnin keino on tehdä opetettavasta asiasta merkityksellistä esimerkiksi koulutettavan ryhmän jokapäiväiseen toimintaan liittyvien tietoriskien ja niiden ikävien vaikutusten tunnistamisella.

Puhakainen on kouluttamisesta täysin oikeassa. Missä tahansa koulutuksessa olisi ensin määriteltävä koulutuksen tarve eli mitä pitäisi kouluttaa/opettaa ja koulutukseen osallistuvien lähtötaso. Lisäksi on selvää,

ettei passiivinen opettajan äänen kuuntelu ole parasta oppimista, vaan opiskelijan on aktiivisesti otettava asioista itse selvää. Nykypäivänä kun tietoa on erittäin paljon, opettaja/kouluttaja koetaankin enemmän tiedon lähteelle opastajana ja tekemisen ohjaajana. Puhakainen on myös täysin oikeassa siinä, että opetettavasta asiasta on tehtävä merkityksellinen opetettavalle ryhmälle ja tällä tavoin pyrkiä motivoimaan ryhmää. Tosin tehtäessä asioista merkityksellisiä joudutaan asioihin paneutumaan erittäin syvällisesti. Tällaisessa tapauksessa myös opiskelijoiden taustoja täytyisi selvittää, jotta koulutus voidaan kytkeä oikeaan kontekstiin. Tämä johtaa kuitenkin siihen, ettei kovin laajaa koulutusta pystytä järjestämään kuin suurilla resursseilla, jolloin uudelleen ja uudelleen palataan siihen tosiseikkaan, onko yrityksellä varaa järjestää tällaista koulutusta omalle henkilökunnalleen. Joka tapauksessa koulutukset pitäisivät olla räätälöityjä paketteja tietyille ryhmille yrityksessä. Kaikkea kaikille opetusta kannattaisi välttää. Lisäksi suurissa ryhmissä yksittäiseen opiskelijaan ei saada välttämättä hyvää kontaktia saati, että saataisiin keskustelua aikaiseksi.

13 Johtopäätökset

Pk-yritysten esimiesten täytyisi pystyä käyttämään pk-yrityksen vahvuuksiin liittyviä asioita hyväksi paremman tietoturvakulttuurin muodostamisessa. Esimerkiksi organisaation mataluus johtamisen kannalta on selkeä vahvuus. Esimies pystyy nopeasti vaikuttamaan väärien toimintatapojen korjaamiseksi. Suora viestiminen suusta suuhun on siis nopeaa ja mielekästä sekä esimiehelle että työntekijälle. Näin ei tule epäsuoralle viestinnälle tyypillisiä vääriä johtopäätöksiä. Myös kokonaisjohtaminen ja ajansaatossa muodostunut organisaatiokulttuuri vaikuttavat tietoturvakulttuurin muodostumiseen. Esimiesten pitäisikin ensimmäisenä tiedostaa, millainen organisaatiokulttuuri tällä hetkellä on ja valita oma johtamistyylinsä muutokseen sen mukaan. Lisäksi esimiesten omat toimintatavat tietoturvan suhteen pitäisi ensimmäisenä kyseenalaistaa tai vähintäänkin tiedostaa. Esimiesten täytyy tarkkailla omia toimintatapojaan ja sanomisiaan tietoturvan suhteen tarkasti ja ottaa asioista selvää, että oikean esimerkin näyttäminen työntekijöille onnistuu. Tietoturvakoulutukseen hakeutuminen kannattaa, koska se maksaa itsensä moninkertaisesti takaisin. Tietoturvapolitiikka ja tietoturvasuunnitelma tulisi laatia, koska ne edustavat tietoturvakulttuurin luomiseen liittyviä arvoja, joilla kulttuurin muodostumiseen voidaan vaikuttaa. Näillä arvoilla voidaan vaikuttaa ihmisten käyttäytymiseen, koska ne ilmaisevat, mitä pidetään toivottavana tai tavoittelemisen arvoisena käyttäytymisenä. Ohjaamista ja opastusta tulisi olla erilaisissa arkipäivän tilanteissa esimerkiksi ryhmäpalavereissa, kehityskeskusteluissa ja työntekijöiden välisissä keskusteluissa. Lisäksi kouluttaminen/kouluttautuminen on ehdottoman tärkeää oikeiden tietoturvallisten toimintatapojen muokkaamiseksi. Koulutuksessa kannattaa kuitenkin välttää kaikkea kaikille tyylistä koulutusta. Ennemminkin kannattaa pyrkiä jakamaan työntekijät erilaisiin ryhmiin osaamisensa perusteella ja antaa koulutusta näille ryhmille kohdennetusti. Myös kouluttajalta voi tätä vaatia. Ennen kaikkea koulutuksella tulisi pyrkiä tilanteeseen, jossa työntekijät näkevät, mitä tietoturvaongelmia omista toimintavoista seuraa. Tällä tavalla perustellaan väärät toimintatavat, minkä jälkeen henkilöstöä voidaan kouluttaa hallitsemaan yhä paremmin tietoturvaan liittyviä tilanteita.

Lähteet

Ahonen, Jorma & Pohjanheimo, Esa 2000. Asian ytimessä. Työkulttuurin kehittäminen oppivassa organisaatiossa. Helsinki: Yliopistopainotalo.

Apunen, Matti & Pokkinen, Jorma 2007. Pelottava paluu pokkurointiin. Aamulehti 11.4.2007.

Furnell, Steven M., Gennatou Maria & Dowland Paul S. 2002. A prototype tool for information security awareness and training. Logistics Information Management 15 (5), 352 - 357.

Griffin, Ricky W. 1990. Management, 3rd edition. Dallas: Houghton Mifflin Company.

Grönroos, Mauri 2003. Mahdollisuuden aika – kohti virtuaalista organisaatiota. Tampere: Transatlanta Oy.

Hakala, Mika, Vainio, Mika & Vuorinen, Olli 2006. Tietoturvallisuuden käsikirja. Jyväskylä: Docendo Finland Oy.

Havana, Tiina & Roning, Juha 2004. Attitudes and Perceptions Related to Information Security - Case: Rotuaari. Euromicro Conference, 538 - 543.

Höne, Karin & Elof J.H.P. 2002. What makes an effective information security policy? Network Security 6, 14 - 16.

Iivonen, Ilona 2006. Tietoturvallisuus pirkanmaalaisissa tietointensiivisissä pk-yrityksissä. eBRC Research Reports 35. Tampere: Tampere University of Technology and University of Tampere.

James, Helen L. 1996. Managing information systems security: a soft approach. Perth, Australia: Curtin University, School of Information Systems.

Karvinen, Eija 2004. Arvot ja toimintatavat apteekin yrityskulttuurin ilmentäjinä. Kuopion yliopiston koulutus- ja kehittämiskeskus.

Kauppinen, Anneli, Nummi, Jyrki & Savola, Tea 2004. Tekniikan viestintä - kirjoittamisen ja puhumisen käsikirja. Helsinki: Edita Publishing Oy.

Kemppainen, Kari 2007. Joustotyö lisää tehoja. ITviikko 4.1.2007, 15. Taloussanomat Oy.

Kerko, Pertti 2001. Turvallisuusjohtaminen. Porvoo: PS-kustannus. WS Bookwell Oy.

Kihl, Merja 2007. Miten osoitat, että yrityksen tietoturva on kunnossa? Hanki hyödyllinen sertifikaatti. Turvallisuus 1.

Koivunen, Erka 2002. Tietoturvallisuuden johtaminen. Johtamisen ja työpsykologian seminaari. Helsingin Teknillinen korkeakoulu. Tietoliikennetekniikan osasto. [online] [viitattu 5.4.2007]
users.tkk.fi/~ekoivune/Studies/Tu-53.104_v1.1.pdf

Korhonen, Heikki 2006. Tietoturvallisuuden johtaminen, yritysjohdon strateginen valinta. [online] [viitattu 29.3.2006].
www.tapiola.fi/www/Yritysasiakkaat/Asiakkaana+Tapiolassa/Asiakastilaisuudet/Tietoturvallisuuden+johtaminen+yritysjohdon+strateginen+valinta.htm

Koskivirta, Paula 2006. Näin motivoit henkilöstön käyttäytymään tietoturvallisesti. Turvallisuus 3, 14 - 17.

Kuivalainen, Jaakko 2004. Yritysjohto laiskottelee tietoturvassa. Digitoday 30.9.2004. [online] [Viitattu 2.9.2006].
www.digitoday.fi/page.php?page_id=14&news_id=200414212

Kuusela, Hannu & Ollikainen, Reijo 1999. Riskit ja riskienhalllinta. Tampere: Tampereen yliopisto.

Kvist, Hasse, Miekkavaara, Arto & Poutanen, Eeva-Maria 2004. Valmentajan polku – valmentamalla huippusuorituksiin. Performance Power Associates.

Kylänpää, Esa & Piirainen, Eeva 2002. Liike-elämän kirjallinen viestintä. Mac Laser Oy.

Kyrölä, Tuija 2001. Esimies ja tietoriskien hallinta. Helsinki: WSOY.

Laine, Kari. Organisaatiokulttuuri osallistavan johtamisen yhteydessä. QPR Software, osallistavan johtamisen akatemia.

Matikainen, Janne 1999. Organisaatiokulttuuri muutoksessa. [online][viitattu 6.4.2007].
www.valt.helsinki.fi/blogs/jmatikai/organisaatiokulttuurinmuutos.pdf

Miettinen, Juha E. 1999. Tietoturvallisuuden johtaminen – näin suojaat yrityksesi toiminnan. Helsinki: Kauppakaari Oyj.

Miettinen, Juha E. 2002. Yritysturvallisuuden käsikirja. Talentum Media Oy.

Panda Software viikkotiedote 7/2006. Tietoturvapäivän huippuseminaarissa korostettiin luottamuksen tärkeyttä. [online] [viitattu 2.9.2006].
www.swbusiness.fi/portal/news/?id=9202&area=7

Petrow, Jouni, Karsisto Timo & Väänänen, Antti 2004. Yrityksen tietoturvakulttuuri. Tietoturvallisuuden kehittämisprosessi – seminaarityö. Otaniemi: Teknillinen korkeakoulu.

Pk-yrityksen riskienhallinta. VTT. [online] [viitattu 11.12.2006].
http://www.pk-rh.com/

Pk-yritysten tietoturvakysely 2006 2007. Kauppa- ja teollisuusministeriö. [online] [viitattu 5.4.2007]. ktm.elinar.fi/ktm_jur/ktmjur.nsf/12b74ae4d1122aadc22565fa003211a6/e546d8a775141f0ac225727b003e0ae9/$FILE/Pk-yritystentietoturvakysely.pdf

Puhakainen, Petri 2005. Tutkimus tietoturvakoulutuksen vaikuttavuudesta. Ylivuoto 1/2005. Oulu: Oulu University Secure Programming Group.

Riskin arviointi 2003. Sosiaali- ja terveysministeriö, työsuojeluosasto. Tampere: Kirjapaino Öhrling.

Ruohonen, Mika 2002. Tietoturva. Jyväskylä: Docendo Finland Oy.

Schein, Edgar H. 2001. Yrityskulttuuri – selviytymisopas. Tietoa ja luuloja kulttuurimuutoksesta. Helsinki: Suomen Laatukeskus Koulutuspalvelut Oy.

Siponen, Mikko T. & Kajava, Jorma 1998. Ontology of organizational IT security awareness – from theoretical foundations to practical framework**.** Proceedings of the 7th Workshop on Enabling Technologies: Infrastructure for Collaborative Enterprises, 327-333. Washington DC: IEEE Computer Society.

Siponen, Mikko T. 2000. A conceptual foundation for organizational information security awareness. Information management & computer security 8/1. MCB University Press.

Siponen, Mikko T. 2006. Secure-system design methods: evolution and future directions. IT Professional 8 (3), 40-44. IEEE Xplore.

Stanton, Ray 2006. Weighing up security measures. Computer Fraud & Security 2006 (1), 17 - 20. ScienceDirect.

Suominen, Arto (1999). Riskienhallinnan mahdollisuudet ja kehityshaasteet. Teoksessa Kuusela, Hannu & Ollikainen, Reijo (toim.) Riskit ja riskienhallinta. Tampere: Tampereen yliopisto.

Thomson, Kerry-Lynn & von Solms, Rossouw 2005. Information security obedience: a definition. Computers and security 24, 69 - 75. ScienceDirect.

Tietoturvatietoisuutta pk-yrityksiin 2005. Kauppa- ja teollisuusministeriö. [online] [viitattu 11.12.2006]. www.tietoyhteiskuntaohjelma.fi/ajankohtaista/vuoden_2005_uutiset/fi_FI/1126862413567/

Tili- ja lakitoimistojen tietoturvallisuudessa parantamisen varaa 2006. Granite Partners Oy. [online] [viitattu 24.1.2007] www.granitepartners.fi/uploads/File/Press_GranitePartners_2006-04-04.pdf

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI. Valtiovarainministeriö. [online] [viitattu 1.12.2006].

www.vm.fi/vm/fi/13_hallinnon_kehittaminen/09_Tietoturvallisuus/01_tietoturvaryhma_VAHTI/index.jsp

Valtionhallinnon tietoturvakäsitteistö 2003. Valtiovarainministeriö. Hallinnon kehittämisosasto. Valtionhallinnon tietoturvallisuuden johtoryhmä. Helsinki: Edita Prima Oy.

von Fieandt, Noora 2005. Henkilöstön tietotekninen osaaminen ja koulutustarve terveydenhuollossa. Kuopion yliopisto, yhteiskuntatieteellinen tiedekunta terveyshallinnon- ja talouden laitos, terveyshallintotiede, sosiaali- ja terveydenhallinnon tietohallinto.

von Solms, Basie 2000. Information security – the third wave? Computers and security 19, 615 - 620. ScienceDirect.

von Solms, Rossouw & von Solms, Basie 2004. From policies to culture. Computers and security 23, 275 - 279. ScienceDirect.

Vuoden 2006 Tieturi Data Security Award Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI:lle. Tieturi. [online] [viitattu 1.12.2006] www.tieturi.fi/tieturi/DataSecurity-palkinto.asp

Yrityskulttuuri 2006 selvitys 2006. Keskuskauppakamari.[online][viitattu 7.4.2006]. www.henryorg.fi/data/dokumentit/tutkimukset/Yrityskulttuuri_2006.pdf

Liitteet

Liite 1: Henkilöstö mukaan luomaan pk-yrityksen tietoturvaa

Henkilöstö mukaan kehittämään pk-yrityksen tietoturvaa

Arvoilla, koulutuksella ja hyvällä johtamisella tuloksiin

Toni Männistö

2007

1 JOHDANTO

Pk-yritysten teknisiin tietoturvaongelmiin löytyy nykyään suhteellisen helposti edullisiakin ratkaisuja. Oikeilla teknisillä työkaluilla monet tarpeettomat tietoturvaa vastaan tehdyt rikkomukset voidaankin estää melko tehokkaasti varsinkin silloin, kun työkaluja käytetään oikein. Erilaisten työkalujen käyttö vaatii kuitenkin koulutusta ja ohjaamista. Lisäksi organisoitu tietoturvatyö ja tietoturvakulttuurin muodostuminen vaatii hyvää johtajuutta. Erilaisten teknisten tietoturvaratkaisujen hankkiminen asiantuntijan johdolla pk-yritykseen on kohtalaisen helppoa. Vaikeaksi tietoturvatyön tekevät yrityksen omat työntekijät. Heidän kun pitäisi käyttäytyä mahdollisimman turvallisesti ja tiedostaa omissa toimissaan yrityksen tietoturvaa uhkaavat tekijät. Miten saada työntekijät toimimaan työssään mahdollisimman turvallisesti? Tähän kysymykseen annetaan vinkkejä tässä ohjeessa.

Ohjeen kohderyhmät ja rakenne

Tämä ohje on tarkoitettu erityisesti pk-yritysten esimiehille ja johtavassa asemassa työskenteleville. Ohje sisältää vinkkejä tietoturvan kehittämiseen pk-yrityksissä työntekijöiden johtamisen ja koulutuksen avulla. Ohjeessa käydään läpi myös yrityskulttuurin muodostumista ja sen vaikutuksia tietoturvakulttuurin muodostumiseen. Ohje tehtiin, koska pk-yrityksissä henkilöstön toimintaan liittyvät tietoturva-asiat eivät tutkimusten valossa ole kovinkaan hyvässä kunnossa.

2 SYITÄ TIETOTURVALLISUUDEN LAIMINLYÖNTIIN

Syyt tietoturvallisuuden laiminlyöntiin ovat hyvin moninaiset. Tutkimusten mukaan tärkein syy kuitenkin löytyy yleensä organisaation sisältä, omista työntekijöistä. Ongelmana voi olla, että työvälineitä ei osata käyttää tai ei osata edes ajatella, mitä voi seurata jos tietoa joutuu vääriin käsiin. Uhkaa ei ymmärretä tai sitä ei tiedosteta lainkaan.

2.1 TYÖNKUVA ON MUUTTUNUT

Suurena ongelmana on viime vuosikymmeninä ollut erittäin nopeasti muuttuva työnkuva. Melkein millä tahansa alalla, työhön on tullut lisää asioita, joissa vaaditaan tietoteknisiä taitoja. Näiden taitojen osaaminen tai opettelu ei kuitenkaan ole itsestään selvää kaikkien työntekijöiden suhteen. Varsinkin vanhemman sukupolven osalta on selvää, että oppiminen on hidastunut ja mielenkiinto työn muuttamiseen ei houkuttele. On mukavampaa pysytellä tutussa ja turvallisessa.

Vanhempien työntekijöiden taitoja ei pidä kuitenkaan väheksyä. Pikemminkin pitäisi löytää sellaisia ratkaisuja, joissa tärkeä vanhemmilla oleva hiljainen tieto tuotaisiin yrityksen käyttöön ennen kuin he siirtyvät eläkkeelle. Olisiko työpaikoilla jopa tarpeellista luoda työpareja, joissa vanhempi ja nuorempi työntekijä työskentelevät oppipoika-mestari mallin mukaisesti? Hyödyt tästä olisivat moninaiset. Vanhemmat työntekijät voisivat oppia tärkeitä tietoteknisiä ja muita nykypäivän työtä helpottavia taitoja nuoremmilta ja nuoret saisivat vanhemmilta tärkeää liiketoimintaan liittyvää hiljaista tietoa

pystyäkseen menestyksekkäästi jatkamaan yrityksen palveluksessa.

Työ muuttuu myös tietoteknisten välineiden hankinnan mukana. Työntekijöille hankitaan kannettavia tietokoneita ja mukana kannettavia massamuistivälineitä. Näin työn tekeminen siirtyy yhä enemmän myös kotioloihin. Käytännössä tämä tarkoittaa, että yrityksen tärkeitäkin tietoja kannetaan koko ajan mukana. Ennen kuin tällaiseen ns. joustotyöhön tulisi minkään yrityksen lähteä, tulisi myös tarkasti ohjeistaa työntekijät, mitä työntekoon liittyvää tietoa työntekijä saa viedä mukanaan kotioloihin. Lisäksi tulisi suunnitella ja toteuttaa ratkaisut, joilla kotiin kannettava tieto suojataan. Työntekijöiden ”kotikonttoreissa” kun voi olla tietoturva-aukkoja, joista yrityksen tärkeää tietoa pääsee vuotamaan henkilöille, joille tieto ei ole tarkoitettu. Tästä esimerkkinä vaikkapa suojaamattomat langattomat yhteydet, haittaohjelmia sisältävät kotikoneet, pöydillä makaavat paperidokumentit ja helposti hukkuvat pienet massamuistivälineet. Kuka valvoo työntekijän työtä kotona? Työ täytyy myös kotona tehdä tietoturvasäännösten mukaisesti, mutta työnantajalla ei ole lupaa tulla kotiin tarkistamaan, millaisissa oloissa ja millaisilla välineillä yrityksen tietoja käsitellään.

- *Usealla alalla vaaditaan nykyään tietotekniikkataitoja.*
- *Tietotekniikan taidot eivät ole itsestään selvyyksiä varsinkaan vanhemmalle sukupolvelle.*
- *Työn tekeminen siirtyy yhä enemmän kotioloihin. Miten yrityksen tietoturva vastaa tähän?*
- *Kuka valvoo työntekijän tietojen käsittelyä kotikonttorissa?*

2.2 TYÖNTEKIJÖITÄ EI KOULUTETA

Vaikka työnkuva muuttuu, työntekijät eivät saa koulutusta tärkeisiin tietoteknisiin taitoihin, eivätkä varsinkaan tietoturvataitoihin. Tutkimusten mukaan varsinkaan pk-yrityksissä työntekijöille ei järjestetä tarpeeksi tietoturvakoulutusta. Tämän vuoksi työntekijät eivät edes tiedosta uhkaa olevan olemassa. Koska varsinkin tietotekniset asiat ovat varsin abstrakteja, ei ymmärretä mitä seurauksia tietoturvasääntöjen rikkomisella voi olla. Lisäksi jos tietoturvasääntöjä ei edes ole, niin tietoturvan laiminlyövää asiaa ei edes pidetä tietoturvauhkana. Abstrakteilla asioilla tarkoitetaan, että ei täysin ymmärretä, mitä voi seurata vaikkapa netistä ladatun ohjelman asennuksen myötä tai vaikkapa virustorjuntaohjelmiston päivityksen laiminlyönnistä. Tämä ymmärtämättömyys johtuu siitä, että esimerkiksi virustorjuntaohjelmiston päivittämisen laiminlyönnistä ei ole heti näkyvää konkreettista seurausta. Sen sijaan ihmiset kyllä ymmärtävät, mitä voi seurata, jos kadotan työpaikan avaimen tai asiakkaan tärkeitä papereita.

Toisaalta joskus ei kuitenkaan edes ilmiselvää tietoturvan laiminlyöntiä nähdä välinpitämättömänä toimintana. Tämä johtuu siitä, että on totuttu tietynlaisiin rutiineihin, jotka on opittu tekemään itse omalla tavalla. Nämä itse opitut tavat eivät välttämättä kuitenkaan ole niitä oikeita tapoja, joilla esimerkiksi työtehtäviä täytyisi tehdä. On erityisen ongelmallista, että näiden omalla tavalla tehtyjen rutiinien määrä kasvaa sitä mukaa, kun työhön tulee uusia välineitä, joihin ei anneta koulutusta. Sitten kun koulutusta lopulta järjestetään, niin näistä itse opituista rutiineista täytyy päästä eroon eli poisoppia. Tästä on seurauksena, että kouluttaminen ja oppiminen voi olla erityisen haasteellista.

Joka tapauksessa työntekijät tarvitsevat työhönsä itse opittujen rutiinien tilalle koulutusta erityisesti omien toimiensa seurauksista. Onnistunut tietoturvavalveutuneisuuden koulutus vaatii enemmän kuin tietoturvaohjeiden delegoimisen työntekijöille.

- *Tietoturvakoulutus on vähäistä erityisesti pk-yrityksissä.*
- *Usein ei ymmärretä, mitä seurauksia tietoturvasääntöjen rikkomisella voi olla.*
- *Jotkut tietoturvaan liittyvät asiat ovat abstrakteja eivätkä siis konkreettisia.*
- *Itse opittujen rutiinien tilalle tarvitaan koulutusta omien toimien seurauksista.*

2.3 TIETOTURVAOHJEITA JÄTETÄÄN NOUDATTAMATTA

Huonosti laadittuja tai huonosti saatavilla olevia tietoturvaohjeita on vaikea noudattaa. Ohjeet voivat olla mm. yrityksen verkossa saatavilla, mutta niitä on silti vaikea löytää, koska ne ovat esimerkiksi vaikean ja syvän hakemistorakenteen takana. Lisäksi jos ohjeet ovat vielä vaikeaselkoiset ja sisältävät paljon sellaisia ohjeita, jotka eivät liity työntekijän työn tekemiseen, on ohjeista vaikea hakea itseä velvoittavat ohjeet. Ongelmana voi myös olla että ohjeita ei yksinkertaisesti onnistuta noudattamaan tai ohjeiden merkitystä oman työn tekemisen kannalta ei ymmärretä.

Jos ohjeiden noudattaminen lisäksi todetaan työtä hankaloittavana ja paljon aikaa vievänä tekijänä, niin on turha ajatella, että työntekijät noudattaisivat ohjeita. Varsinkin kiireessä ohjeet voivat jäädä noudattamatta. On mahdollista, että työssä, jossa on kovat tulosvaatimukset tai työ on urakkaluonteista, ohjeita jätetään herkästi noudattamatta. Jos palkka on kiinni kovasta tuloksen tekemisestä, saattaa olla, että vaadittua tulosta tehdään sitten vaikka tietoturvaohjeita kiertämällä. Varsinkin jos ohjeiden noudattamista ei ole millään tavalla sidottu tuloksen tekemiseen. Ohjeita voidaan myös kiertää, jos huomataan, että työvälineet eivät tue työtä niin kuin pitäisi tai ne eivät toimi toivotulla tavalla. Näin ollen työvälineiden toimimiseen etsitään omia ratkaisuja, jotka eivät aina ole välttämättä parhaita mahdollisia tietoturvan kannalta.

- *Ohjeiden tulisi olla työntekijöille helposti saatavilla.*
- *Vaikeaselkoisia tai erityisen pitkiä ohjeita on hankala noudattaa.*
- *Ohjeiden merkitystä oman työn tekemiseen ei ymmärretä.*
- *Ohjeita voidaan kiertää, jos huomataan, että työvälineet eivät toimi odotetulla tavalla.*

2.4 ESIMIEHET EIVÄT TOIMI ESIMERKKINÄ

Tietoturvaohjeiden noudattamiseen ja tietoturvalliseen käyttäytymiseen liittyy myös huomattava sosiaalinen paine. Tämän vuoksi yritykseen pitäisi saada yhtenäinen tietoturvakulttuuri, joka painottaa tietoturvallista toimintaa työn tekemisessä. Esimiehet eivät välttämättä aina toimi esimerkillisesti tietoturvaohjeiden noudattajina. Näin ollen toimillaan tai puhumisillaan he voivat antaa alaisilleen viestin, että ohjeita ei tarvitse noudattaa. Tietoturvakulttuurin luomisessa on erityisen tärkeää, että esimiehet näyttävät toimillaan tietoturvan olevan tärkeä liiketoimintaan liittyvä asia. Siposen ja Pahnilan (2006:c8) mukaan olosuhteilla, tietämyksellä sekä esimiehen ja tietoturvahenkilöstön tuella, on huomattava merkitys tietoturvaohjeiden noudattamisessa.

- *Esimiehet eivät aina toimi esimerkillisesti tietoturvaohjeiden noudattajina.*
- *Esimiehet voivat puhumisillaan antaa sellaisen kuvan, että ohjeista ei tarvitse välittää.*

3 PK-YRITYKSEN TIETOTURVALLISUUSTYÖ

Pk-yrityksen tietoturvallisuustyö on erittäin haastavaa monestakin syystä. Tärkeimmät syyt tutkimusten mukaan ovat osaamisvaje ja resurssien riittämättömyys. Teknologian täysmittainen hyödyntäminen liiketoiminnan tukena kompastuu osaamisvajeeseen. Tietoturvallisuustyö on ammattilaisten työtä, eikä suurimmalla osalla pk-yrityksistä ole tällaisia ammattilaisia palkkalistoillaan. Pk-yrityksen ei kannata välttämättä tällaista osaajaa palkatakaan ellei hänellä ole muuta pk-yrityksen liiketoimintaan liittyvää osaamista. Tämä johtuu siitä, että tietoturvatyö pk-yrityksessä ei ole yleensä kokopäivätyötä.

Lisäksi tietoturvallisuustyöhön ei yksinkertaisesti ole aikaa ja rahaa. Työntekijöiden osaamiskenttä on laaja ja yhden työntekijän vastuulla on monenlaisia tehtäviä. Tämä johtaa kiireeseen ja lopulta siihen, että yrityksen sisäisiä asioita ei pystytä kehittämään eteenpäin. Kiireenkin keskellä pitäisi kuitenkin pystyä yrityksen sisäisten toimintojen kehittämiseen. Varsinkin pk-yrityksille on ominaista olla alihankintasuhteessa suurempiin organisaatioihin ja yrityksiin. Tämä vaatii pk-yritykseltä omien tietojen suojaamisen lisäksi myös asiakkaan tietojen suojaamista. Pk-yritys on alihankkijana vastuussa toisten yritysten tiedoista, ei ainoastaan omistaan. Jotkut liiketoimintaansa liittyviä tietoja luovuttavat asiakkaat vaativatkin nykyään alihankkijalta tietoturva-asioiden hoitoa. Tietoturva-asioiden hoidosta takeena voi olla esimerkiksi ISO/IEC 27001 –standardin mukainen tietoturvasertifikaatti. Suurten alihank-

kijoita työllistävien yritysten pitäisi silti miettiä, onko yksin sertifiointi riittävä tae hyvästä tietoturvallisuudesta. Tietoturvan auditointikäytännöt ratkaisevat aika pitkälle tämän asian. Tehdäänkö auditointia tarpeeksi usein ja onko auditoinnissa mitattavat asiat sellaisia, jotka ovat riittäviä takaamaan vaikkapa asiakkaan luovuttamien tietojen säilymisen vain alihankkijan tiedossa?

Tietoturvallisuuden kehittäminen, kuten minkä tahansa muun asian kehittäminen, vaatii yritykseltä resursseja. Vaikka tietoturvallisuustyötä tehtäisiin konsultin tai muun ulkopuolisen tietoturva-ammattilaisen avustuksella, täytyy yrityksen silti kuluttaa omia resurssejaan työn tekemiseen. Yrityksen ulkopuolinen ammattilainen ei voi tietää yrityksen tietojen käsittelyyn liittyviä toimintoja niin hyvin, että voisi omin voimin kehittää hyvän suunnitelman yrityksen tietojen suojaamiseen. Näiden tietojen käsittelyn toimintojen kuvaamiseen tarvitaan aina yrityksen omia työntekijöitä. Ulkopuolinen asiantuntija on sitä varten, että hän laittaa työn alulle, organisoi sitä ja johdattaa työntekijät tietoturvatyön pariin.

Kaikkein tärkeintä tietoturvatyössä olisi siis ottaa työntekijät laajasti mukaan yrityksen tietoturvan kehittämiseen. Vain työntekijät tietävät, miten he itse käsittelevät yrityksen tietoja, kuten asiakkaiden tilaus- ja laskutustietoja, palkkatietoja, tarjouskilpailuun liittyviä tietoja ja tutkimus ja kehitys -tietoja. Kun tiedetään, miten työntekijät käsittelevät yrityksen tietoja, voidaan vasta sitten määritellä, miten näitä tietoja suojellaan

erilaisissa tietojen käsittelyn vaiheissa. Ei ole kuitenkaan täysin samantekevää, miten tätä prosessia johdetaan. Miten saadaan työntekijät innostumaan yrityksen tietoturvan ja oman tietoturvavalveutuneisuuden kehittämisestä? Tämä lienee perustavaa laatua oleva kysymys kaikessa yritysten sisäisen toiminnan kehittämiseen liittyvissä toimissa.

- *Pk-yritys on alihankkijana vastuussa myös asiakkaan tietojen suojaamisesta.*
- *Ulkopuolisen asiantuntijan palkkaaminen tietoturvan kehittämiseen vaatii pk-yrityksen resursseja.*
- *Tietoturvatyössä olisi tärkeää ottaa työntekijät laajasti mukaan yrityksen tietoturvan kehittämiseen.*
- *Miten saadaan työntekijät innostumaan oman tietoturvavalveutuneisuuden kehittämisestä, on peruskysymys tietoturvan kehittämiseksi yrityksissä.*
- *Hyvin suunniteltu ja toteutettu tietoturvallisuus parantaa yrityksen tietojen käsittelyyn liittyviä rutiineja ja antaa asiakkaalle luotettavan kuvan alihankkijasta.*

4 VASTUU YRITYKSEN TIETOTURVASTA

Yrityksen tietoturvasta vastuussa ovat kaikki yrityksen työntekijät, sillä jokainen työntekijä käsittelee yrityksen tietoja tavalla tai toisella. Työntekijät ovat vastuussa nimenomaan tietoturvasta annettujen sääntöjen ja käytäntöjen noudattamisesta. Kokonaisvastuu tietoriskeistä on silti yrityksen esimiehillä. Tämä vastuu on pysyvä, sitä ei voida siirtää. Vaikka ohjeet on annettu työntekijöille ja tietoturvan palveluita on ulkoistettu ulkopuoliselle yritykselle, ovat esimiehet silti viime kädessä vastuussa yrityksen tietojen turvallisuudesta.

Tietoturvaan liittyvä työ on yksi osa esimiesasemassa työskentelevien esimiesten toimintaa. He vastaavat tiedon suojaamisesta, liiketoimintaa uhkaavien riskien ja tietoriskien tunnistamisesta sekä henkilöstön osaamisen ajantasaisuudesta ja toimintavalmiuksista. Ylin johto tekee tietoriskien hallinnan ja keinojen kehittämispäätökset, jotka perustuvat heille esitettyihin riskeihin ja toiminnan kehittämisehdotuksiin. (Kyrölä, 2001:208-209.) Yrityksen johtajisto vastaa osakeyhtiölain mukaan yrityksen toiminnan turvaamisesta, liiketoiminnan jatkuvuuden varmistamisesta ja valvonnan organisoinnista (Suominen, 2003:81).

- *Viime kädessä yrityksen tietoturvasta on vastuussa yrityksen johto.*
- *Johtajat eivät voi siirtää vastuuta tietoriskeistä delegoimalla ohjeita tai ulkoistamalla toimintoja.*

5 TIEDON SUOJAAMISEN LÄHTÖKOHDAT

Tiedon suojaamisessa on tärkeä ymmärtää, millaisissa muodoissa tietoa esiintyy. Tämä täytyy tietää, että osataan suojata eri muodoissa oleva tieto asianmukaisilla välineillä ja keinoilla. Tieto pitää suojata *sähköisessä* ja *fyysisessä* olomuodossa sekä *ihmisen muistissa*. Lisäksi tulisi yrityksestä riippuen suojata myös työympäristö ylimääräisiltä katseilta.

5.1 TIEDON SÄHKÖINEN JA FYYSINEN OLOMUOTO

Sähköisessä olomuodossa tietoa löytyy yrityksen tietokoneista ja massamuisteista. Nykyisillä tehokkailla järjestelmillä ja välineillä tietoa on erittäin helppo muokata, lähettää eteenpäin, tulostaa paperille ja ottaa mukaan massamuistivälineille kuten usb-tikuille. Juuri tiedon sähköinen olomuoto on tehnyt tiedon suojaamisesta erittäin haastavan, koska tietoa on helppo liikutella paikasta toiseen mm. sähköpostitse, kannettavalla tietokoneella ja massamuistivälineillä. Myös matkapuhelimissa on nykyään erittäin suuri muistikapasiteetti. Lisäksi matkapuhelimessa on mitä erilaisempia mahdollisuuksia muodostaa yhteyksiä muihin laitteisiin kuten bluetooth-, infrapuna- tai wlan-yhteys.

Näin ollen yrityksen arvokasta tietopääomaa voi löytyä yllättävistäkin paikoista. Riskitilanteita myös syntyy kun, työntekijät unohtelevat näitä työvälineitään julkisiin tiloihin ja kulkuneuvoihin. Lisäksi työvälineitä kuten kannettavia tietokoneita varastetaan mm. autojen takapenkeiltä. Huolimatta edellä mainituista riskeistä tiedon sähköisellä olomuodolla

on kuitenkin erittäin paljon positiivisia vaikutuksia. Erilaiset sähköiset järjestelmät ovat nimittäin huimasti tehostaneet tiedon käyttöä yrityksissä.

Fyysisessä olomuodossa tietoa on mm. asiakirjoina, käsikirjoina ja toimintakuvauksina. Myös näitä tietoja kuljetetaan tilanteesta riippuen mukana työpaikalta muihin yrityksiin neuvotteluihin, yksityisiin koteihin etätyötä varten jne. Fyysisen tiedon mukaan ottaminen on kuitenkin huomattavasti vaikeampaa kuin tiedon mukaan ottaminen sähköisenä. Tämä johtuu siitä, että kukaan ei jaksa kantaa sellaista tietomäärää mukanaan paperisena, mitä mahtuu esimerkiksi 250 Megatavun muistitikulle. Paperisten asiakirjojenkin kanssa täytyy siltä olla varovainen.

- *Suuren tietomäärän mukana kuljettaminen on nykypäivänä erittäin helppoa erilaisten pienten massamuistivälineiden avulla.*
- *Yrityksen arkaluonteista tietoa voi löytyä yllättävistäkin paikoista, koska ihmiset unohtelevat ja hukkaavat pieniä tiedonsiirtovälineitä.*
- *Tiedon sähköinen olomuoto ja sen siirtäminen paikasta toiseen on turvattava asianmukaisin keinoin.*

5.2 TYÖNTEKIJÖIDEN MUISTISSA OLEVA TIETO

Työntekijöiden muistissa voi olla erittäin arkaluonteista tietoa esimerkiksi yrityksen palveluista ja tuotteista. Tiedon arkaluonteisuus yleensä riippuu, millaisissa tehtävissä työntekijä yrityksessä toimii. Työntekijällä voi olla tietoa yrityksen toiminnasta yleisellä tasolla ja/tai esimerkiksi tavaran tai palvelun kehitysprosessista, ominaisuuksista ja työmenetelmistä. Työntekijällä on siis yrityksestä omaksuttua tietoa, jota hän voi käyttää hyväksi esimerkiksi toisessa saman alan yrityksessä. Lisäksi työntekijä yleensä omaa suuren määrän erilaista hiljaista tietoa, joka liittyy työntekijän oman työn tekemiseen. Hiljainen tieto on yleensä henkilösidonnaista ja sitä on vaikea siirtää muille. Se voi olla kädentaitoa, ongelmanratkaisukykyä ja muuta, mitä on vaikea kirjoittaa paperille tai jakaa muille työntekijöille.

Ihmisen muistissa olevan tiedon suojaaminen on kaikkein vaikeimmin suojeltavissa. Tätä tietoa kuitenkin pyritään suojaamaan mm. erilaisin salassapitosopimuksin. On kuitenkin erittäin vaikea todistaa työpaikkaa kilpailijalle vaihtaneen henkilön käyttänee aiemmasta työpaikasta saatua tietoa uuden työnantajan hyväksi.

- *Yrityksen palveluksessa olevalla työntekijällä voi olla erittäin kattava tietomäärä yrityksen arkaluonteistakin tietoa.*
- *Työntekijöiden muistissa olevan tiedon suojaaminen on erittäin haastavaa mille tahansa organisaatiolle.*

5.3 TYÖYMPÄRISTÖN TIETO

Riippuen yrityksen toimintaympäristöstä myös yrityksen työympäristössä voidaan ajatella olevan tietoa. Saman alan työntekijän päästessä tarkastelemaan esimerkiksi kilpailevan yrityksen työmenetelmiä tai laitteita, voi tärkeääkin tietoa vuotaa kilpailevan yrityksen tietoon. Sopivat tiedot omaava henkilö saattaa pystyä päättelemään työympäristöstä vaikkapa koko tuotteen valmistusketjun ja käyttämään tätä tietoa kilpailevan yrityksen lukuun. Alasta tietämätön henkilö ei kuitenkaan pysty tällaista tarkkailua ja tiedon soveltamista tekemään.

- *Myös yrityksen työympäristössä on tärkeää tietoa, joka on suojattava asiattomilta katseilta.*
- *Varsinkin saman alan tiedon omaava henkilö pystyy päättelemään kilpailevan yrityksen toimintoja.*

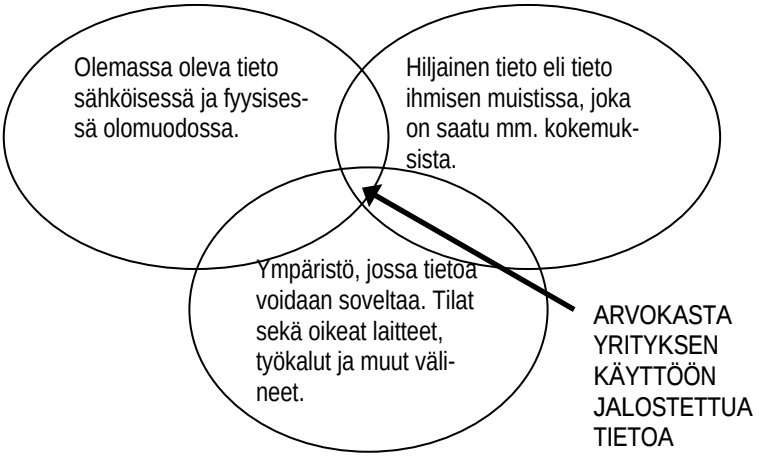
5.4 ARVOKAS TIETO

Kaikkein arvokkain tieto yritykselle syntyy, kun työntekijät työskentelevät yrityksessä käyttäen hyväksi koulutustaan, kokemuksiaan, olemassa olevaa tietoa ja yrityksen hankkimia työkaluja (ks. kuva 1). Näiden yhdistelmästä syntyy työntekijöiden toimet eli työ yrityksissä, ovat ne sitten asiakkaan palveluun tai tuotteen kehittämiseen liittyviä toimia. Näihin toimiin liittyvä tieto ja tiedon käsittely pitäisi suojata oikeassa tilanteessa ja oikealla tavalla, koska palvelun kehittämisen yhteydessä yritykseen on syntynyt uutta arvokasta tietoa, johon on voitu käyttää merkittävä määrä yrityksen resursseja. Tä-

män tiedon, työntekijöiden ja työympäristön avulla yritys joko kehittyy tai jää kehittymättä.

Tuskin kenenkään intresseissä on ensimmäisenä vuotaa suurilla resursseilla yrityksessä kehitettyä tietoa kilpailevan yrityksen tietoon. Näin voi kuitenkin käydä jos esimerkiksi erilaisia sähköisiä tietojenkäsittelyn työvälineitä käsitellään huolimattomasti tai avaintyöntekijä vaihtaa työpaikkaa kilpailevaan yritykseen.

- *Arvokas yrityksen käyttöön kehitetty tieto syntyy yritykseen työntekijöiden käyttäessä osaamistaan, olemassa olevaa tietoa sekä yrityksen hankkimia työkaluja ja työympäristöä.*



Kuva 1. Tiedon erilaiset olomuodot (mukaillen Tuija Kyrölää 2001:25).

6 MISTÄ LÄHTEÄ LIIKKEELLE TYÖNTEKIJÖIDEN OHJAAMISESSA TIETOTURVALLISEMPAAN TOIMINTAAN

Työntekijöiden ohjaaminen tietoturvallisempaan toimintatapaan on puuttumista heidän luomiinsa ”hyviksi havaittuihin” työrutiineihinsa. Käytännössä se tarkoittaa muutosta toimintatapoihin. Urautuneelle työntekijälle muutos saattaa olla pitkä prosessi jota on vaikea sisäistää. Yrityksessä on totuttu pitkän ajan kuluessa tiettyihin hyviksi havaittuihin toimintatapoihin, miksi siis muuttaa niitä: ”näinhän meillä on aina tehty”.

6.1 YRITYSKULTTUURI

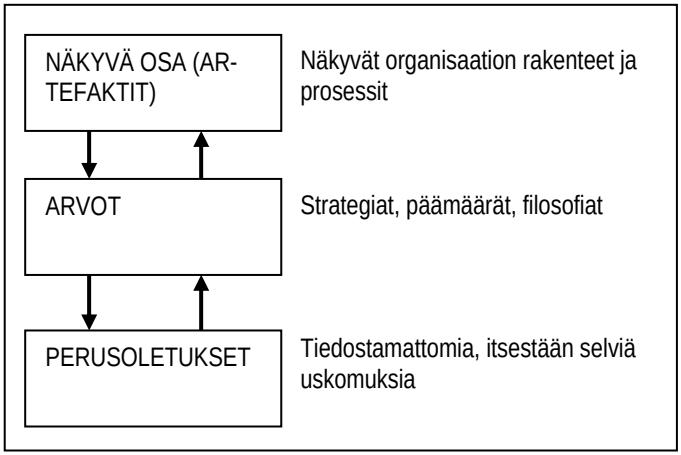
Esimiesten on ensiarvoisen tärkeää tunnistaa, millainen yrityskulttuuri heidän johtamassaan yrityksessä on. Yrityskulttuurilla tarkoitetaan ajan saatossa työntekijöiden yhdessä omaksumia toimintatapoja, joiden pohjalta työntekijät toimivat usein myös tiedostamattaan. Yhteisten kokemusten ja oppimisen kautta syntyy tapoja ajatella, uskomuksia ja arvoja, joista yrityskulttuuri lopulta syntyy. Työntekijät siis muodostavat yrityksen kulttuurin.

Mitä pidemmälle yrityskulttuuri saa toimia samojen toimintatapojensa ehdoilla, sitä vaikeammaksi vakiintuneiden ja hyviksi koettujen toimintatapojen muuttaminen käy. Ihmiset muodostavat opituista toimintatavoista itselleen rutiineja, joista on pitkällä tähtäimellä vaikea irrottautua eli pois oppia. Mikäli yritykset eivät ikääntyessään kehity, sopeudu ja muuta kulttuurinsa elementtejä, ne kasvavat yhä sopeutumattomammiksi, ja kulttuurista tulee rajoite oppimiselle ja muutokselle

(Schein 2001:27). Se kulttuuri, joka loi menestyksen, tekee yrityksen jäsenille vaikeaksi havaita ympäristöstä muutoksia, jotka vaativat uusia reaktioita (Schein 2001:27). Loppujen lopuksi kulttuurista muodostuu rajoite yrityksen strategialle, toteaa Schein (2001:27). Näin voi tapahtua tietoturvakulttuurin osalta myös yrityksen tietoturvastrategialle. Ja vaikka strategiaa ei olisikaan, jonkinlainen tietoturvakulttuuri yritykseen syntyy joka tapauksessa. Eri asia on, onko tietoturvakulttuuri hyvä vai huono. Seuraavat kappaleet selvittävät, miten yrityskulttuuri jakautuu eri tasoihin. Nämä tasot on hyvä tietää, jotta voi tulkita oman yrityksensä kulttuuria.

Yrityskulttuuri jakautuu kolmeen tasoon

Yrityskulttuuri muodostuu kolmesta tasosta (ks. kuva 2). Nämä tasot ovat *näkyvä osa*, *arvot* ja *perusoletukset*. Näkyvällä osalla tarkoitetaan työympäristöstä ulospäin näkyvää osaa. Kuten nimikin sanoo, näkyvän osan yrityksessä voi nähdä siihen tutustuessaan. Näkyvä osa tarkoittaa yrityksen näkyviä rakenteita, kuten työympäristöä, ihmisten havaittua käyttäytymistä ja toimintatapoja. Vaikka näet, mitä ympärilläsi tapahtuu, ja kuinka ihmiset käyttäytyvät toisiaan kohtaan, et silti oikeastaan tiedä, mitä tämä merkitsee. Pelkästään tarkkailemalla ympäristöä ei voi tulkita, mitä yrityksessä todella tapahtuu. Siksi yrityksen/yhteisön jäsenien kanssa täytyy keskustella asioista, joita he havaitsevat ja tuntevat. Tämän keskustelun pitäisi johtaa kulttuurin seuraavalle tasolle eli arvoihin.



Kuva 2. Scheinin kolme kulttuurin tasoa (Schein 2001).

Arvot ovat asioita, joita yritys arvostaa. Arvot vastaavat kysymykseen, miksi yrityksessä tehdään juuri niitä asioita joita he tekevät? Miksi yrityksessä esimerkiksi arvostetaan tiimityöskentelyä tai miksi yrityksessä on avoimet työtilat sermein eroteltuna eikä esimerkiksi suljetut huoneet? Arvot ovat yleensä myös yrityksen kirjoitettuja arvoja, joita löytyy vuosikertomuksista ja nettisivuilta. Nämä arvot ainakin kertovat, miltä yritys haluaisi ulospäin näyttää, mutta ne eivät kerro lopullista totuutta.

Arvot ovat johtajien ja yrityksen perustajajäsenten luomia. Ne ilmaisevat työntekijöille, mitä pidetään toivottavana ja tavoittelemisen arvoisena käyttäytymisenä. Yleensä myös työntekijät toistavat näitä kirjoitettuja arvoja kertoessaan esimerkiksi yhteistyötahoille toimittavan niiden mukaan. Joskus kuitenkin havaitaan ristiriitaisuuksia näkyvän käyttäytymisen ja arvojen

välillä. Ristiriitaisuudet kertovat ajattelun ja käsitysten syvemmän tason ohjaavan näkyvää käyttäytymistä. Tämä syvempi taso siis voi olla yhdenmukainen arvojen kanssa, mutta aina näin ei ole.

Yrityskulttuurin syvin taso on perusoletukset. Nämä ovat asioita, joita työntekijät eivät itsekään kyseenalaista tai eivät osaa tunnistaa. Jos yritys on vanha, niin historia heijastuu perusoletuksissa. Niissä heijastuvat mm. yrityksen perustajien ja keskeisten johtajien arvot, uskomukset ja oletukset. Perusoletukset ovat yhdessä opittuja ja sisäistettyjä ja niitä pidetään itsestään selvinä asioina: ”näinhän meillä on aina toimittu”.

Perusoletukset ovat voimakkaimmin työntekijöiden käytöstä ohjaavia voimia. Myös nuorelle yritykselle syntyy hyvin nopeasti tietty tapa toimia, asenteet ja ilmapiiri. Mutta nuoren yrityksen kulttuuria on vielä helpompi muokata verrattuna vanhaan yritykseen. Kaiken kaikkiaan kulttuuria on vaikea muuttaa, mutta se on mahdollista. Kulttuurin muutoksen vaikeus liittyy ihmisten tapaan muodostaa pysyviä rakenteita ja toimintatapoja, joista luopuminen on erittäin vaikeaa. Tästä syystä monet työntekijät suhtautuvat muutokseen yleensä vastahakoisesti, olkoon kyse yksinkertaisesta toimintatavan muutoksesta tai monimutkaisemmasta prosessista. Voi olla, että yrityksen johtajat yrittävät viedä muutoksen läpi vain sanelemalla arvot joiden mukaan pitäisi toimia. Uusia arvoja yritetään siis jalkauttaa ylhäältä päin käskettynä. Tosiasia kuitenkin on, että jos jokin näistä johtajien sanelemista arvoista on

ristiriidassa yrityksessä kauan vallinneen kulttuurin kanssa, aiheuttavat ne turhautumista ja yrityksen työtekijöiden välien tulehtumista.

- *Yritys-/organisaatiokulttuuri jaetaan näkyvään osaan, arvoihin ja perusoletuksiin.*
- *Näkyvä osa on sananmukaisesti näkyvää kuten rakenteet, työympäristö ja ihmisten havaittu käyttäytyminen.*
- *Arvot ovat asioita, joita yrityksessä arvostetaan esimerkiksi tiimityöskentely. Arvot ilmaisevat, mitä pidetään toivottavana tai tavoittelemisen arvoisena käyttäytymisenä.*
- *Perusoletukset ovat yhdessä opittuja ja sisäistettyjä asioita. Ne ohjaavat voimakkaimmin työntekijöiden käytöstä.*

Kaikilla ryhmillä on kulttuurinsa

Missä ikinä on ryhmiä, joilla on yhteisiä kokemuksia, on myös kulttuuri tai vähintään se alkaa muodostua yhteisten kokemusten mukana. Yrityksissä kulttuuria esiintyy osastoissa, tiimeissä, erilaisissa ryhmissä ja organisaatioyksiköissä. Kulttuureja on myös eri hierarkian tasoilla. Lisäksi sitä esiintyy koko organisaation tasolla, jos vain yhteistä historiaa on tarpeeksi.

- *Yrityksissä kulttuuria esiintyy osastoissa, tiimeissä ja organisaatioyksiköissä.*

6.2 TIETOTURVAKULTTUURI

Tietoturvakulttuuri on osa yrityskulttuuria. Siksi siihen vaikuttavat samat asiat kuin yrityskulttuuriin. Myös tietoturvakulttuurissa on näkyvä osa, arvot ja perusoletukset. Näkyvä osa tarkoittaa sitä, kuinka havaitaan työntekijöiden käyttäytyvän tietoturvan osalta. Miten työntekijät esimerkiksi toimivat luottamuksellisten tietojen kanssa? Jätetäänkö luottamukselliset dokumentit pöydille ajelehtimaan tai lähetetäänkö niitä sähköpostin liitteenä yrityksen ulkopuolelle? Miten käyttäydytään salasanojen kanssa? Onko salasanat kirjoitettu esimerkiksi paperilapuille, jotka löytyvät näppäimistön alta?

Arvot puolestaan muodostuvat esimerkiksi yhdessä sovituista päätöksistä, kuinka joku asia tietoturvan osalta tehdään (kirjoittamattomista säännöistä) tai esimiesten laatimista säännöistä, joita tulisi noudattaa. Työntekijät voivat ilmaista noudattavansa tietoturvan osalta yrityksen yhteisiä sääntöjä ja mainostavat, kuinka hyvin heidän yrityksessään sääntöjä noudatetaan. Tosiasia voi olla kuitenkin huomattavasti karumpi. Työntekijät voivat käyttäytyä tietoturvasääntöjen osalta varsin ristiriitaisesti, mikä voi johtua siitä, että ohjeita ei tosiasiassa ymmärretä tai ohjeista on monta eri tulkintaa. Ohjeiden ymmärtämättömyys ja eri tulkinnat voivat puolestaan johtua kouluttamattomuudesta ja ohjeiden huonosta jalkauttamisesta. Tällöin työntekijät joutuvat itse tulkitsemaan ohjeita milloin asioista voi tulla vääriä käsityksiä. Toki ohjeetkin voivat olla huonosti laadittu, mikä voi entistä enemmän johtaa vääriin tulkintoihin. Toisaalta perusoletukset voivat olla niin voimak-

kaita, että työn tekeminen mielletään joutuisammaksi ilman ohjeiden noudattamista periaatteella: ”näinhän olen aina tehnyt, tämä on nopea tapa tehdä ja saan paljon enemmän aikaiseksi omalla tavallani”. Tällaiset yhdessä opitut perusoletukset ovat voimakkaimmin työntekijöiden käytöstä ohjaavia voimia. Perusoletuksia ei muuteta pelkästään tekemällä ohjeita ja kertomalla työntekijöille, että näitä pitää noudattaa. Tietoturvallisen ajattelutavan leviäminen vaatii asemansa puolesta tärkeän esimiehen tukea kaikin eri tavoin. Ensimmäinen porras esimiehillä on kuitenkin kyseenalaistaa omat toimintatapansa. Ovatko ne tarpeeksi tietoturvallisia? Näytänkö työntekijöilleni oman toimintani suhteen sellaista esimerkkiä, että voin jollekin työntekijöistä huomauttaa hänen toiminnastaan?

Esimiesten tulisi pyrkiä vaikuttamaan nimenomaan kulttuurin syvimpään tasoon eli perusoletuksiin. Tähän voidaan vaikuttaa omalla esimerkillä, tukemisella, koulutuksella ja osallistamalla työntekijöitä. On kuitenkin muistettava, että ennen muutoksen tai uusien asioiden tekemistä on luotava tarpeelliset puitteet mahdollistamaan toimiminen.

- *Perusoletukset ohjaavat työntekijöiden toimintaa erittäin voimakkaasti. Tämän vuoksi esimerkiksi tietoturvaohjeista voi olla monta eri tulkintaa.*
- *Esimiesten tulisi tiedostaa ensimmäisenä omat toimintatapansa.*
- *Esimiesten tulisi pyrkiä vaikuttamaan kulttuurin syvimpään tasoon omalla esimerkillään, tukemisella, koulutuksella ja osallistamalla työntekijöitä.*

7 HENKILÖSTÖN OHJAAMINEN JA JOHTAMINEN TIETOTURVATYÖHÖN

Esimiesten on hyvä muistaa tietoturvan kehittämistyön alkaessa, että heidän sitoutumisensa muutokseen on kaikkein tärkeintä. Esimiesten on oltava mukana omalla esimerkillään. Lisäksi muutokseen on uhrattava resursseja ja ne on osattava kohdentaa oikein. On turha luulla, että asiat etenevät omalla painollaan. Henkilöresurssien kohdentamisessa on hyvä muistaa, että tietoturvan kehittämistä ei jätetä vain yhden henkilön varaan eikä ainakaan ainoastaan IT-osaston tai tietoteknisesti suuntautuneen henkilön varaan. Tietoturvan kehittämisessä pitäisi olla mukana henkilöitä jokaisesta liiketoimintayksiköstä. Yksittäinen henkilö tai useampikaan henkilö samasta liiketoimintayksiköstä ei osaa arvioida kaikkea sitä tietoon liittyvää käsittelyä, mitä kaikissa muissakin liiketoimintayksikössä tapahtuu. Siksi jokaisen liiketoimintayksikön tulisi miettiä tietojen käsittelyn prosessit omalta kohdaltaan, ja tehdä niitä vastaavat toimenpiteet turvallisen tietojen käsittelyn varmistamiseksi.

7.1 ESIMIESTEN SITOUTUMINEN TIETOTURVAN KEHITTÄMISEEN

Tärkein asia tietoturvan kehittämisessä on esimiesten sitoutuminen asiaan. Ellei tietoturvan kehittämiseen ole ylemmän tahon tukea, sitä on turha lähteä kehittämään. Esimiehet ovat avainasemassa tietoturvallisuuden kehittämisen alkuunsaattamisessa ja tietoturvallisuuden toteutumisessa. He asettavat tietoturvalle tavoitteet ja organisaatiolle riittävän tietoturvata-

son. He myös määrittelevät vastuut ja resurssit tärkeälle tietoturvallisuutta edistävälle työlle. Näistä edellä mainituista toimista syntyy yrityksen tietoturvapolitiikka. Esimiesten laatima tietoturvapolitiikka voidaan toteuttaa toimintaohjeiden tietoturvaperiaatteiden, oppaiden ja koulutuksen avulla.

Joka tapauksessa tietoturvapolitiikka käsittää esimiestahon laatimat arvot tavoitteelliselle tietoturvalliselle toiminnalle. Nämä arvot edustavat sitä, minkälaisen tietoturvallisuuden tilan esimiehet haluaisivat yrityksessä olevan. Näillä arvoilla voidaan vaikuttaa työntekijöiden käyttäytymiseen, sillä ne ilmaisevat, mitä pidetään toivottavana ja tavoittelemisen arvoisena tietoturvakäyttäytymisenä.

Esimiehiltä tarvitaan esimerkillistä toimimista ja näkyvää sitoutumista niin, että koko yrityksen henkilöstö on siitä tietoinen. Koulutuksiin täytyy osallistua samalla tavalla kuin muidenkin työntekijöiden. Osallistuminen tietoturvan kehittämiseen yleisesti on erittäin tärkeää. Näin voidaan osoittaa työntekijöille, että esimiehet ovat tosissaan ja vahvasti muutoksessa mukana. Lisäksi heidän tukeaan ja näkemyksiään tarvitaan keskusteluihin ja kehittämiseen aivan samalla tavalla kuin muiltakin työntekijöiltä. Pahin virhe on koulutuksesta tai keskusteluista pois oleminen, koska niissä esitetyt asiat tulee myös esimiesten hallita. Samalla esimiehet varmistuvat siitä, että tietoturvallinen käyttäytyminen heidän osaltaan näkyy työntekijöille, kuten koulutuksessa on opetettu. Esimiehet romuttavat vääränlaisella käyttäytymisellään vai-

valla aikaansaadut tulokset tietoturvan osalta nopeasti, jos eivät itse osaa käyttäytyä tietoturvallisesti. Työntekijät nimittäin tarkkailevat, miten esimiehet käyttäytyvät. Esimiesten sanomisia ja käyttäytymistä tarkkaillaan suurennuslasilla, eikä mikään jää alaisilta huomaamatta. Siksi tietoturvallisen käyttäytymisen muutoksen tulee lähteä liikkeelle esimiehistä.

Esimies

- *Määrittele yrityksen tietoturvapolitiikka, sillä se asettaa tietoturvakulttuurin kirjoitetut arvot, jotka ilmaisevat työntekijöille toivottavan ja tavoittelemisen arvoisen tietoturvakäyttäytymisen.*
- *Nimeä vastuut ja anna resurssit.*
- *Ole esimerkkinä alaisillesi. Näytä sitoutuneisuutesi tietoturvan kehittämiseen. Osallistu koulutuksiin ja keskusteluihin.*
- *Varmistu, että käyttäydyt itse tietoturvallisesti.*
- *Esimiehenä olet tarkkailun kohteena, jos olet muutoksen alkuunpanija. Käyttäytymistäsi ja sanomisiasi seurataan jatkuvasti.*

7.2 TYÖNTEKIJÄT MUKAAN TIETOTURVAN KEHITTÄMISEEN

Yrityksen työntekijöiden ohjaaminen ja johtaminen ovat erittäin merkityksellisiä tekijöitä työntekijän tietoturvallisen käyttäytymisen kannalta. Työntekijä, joka käsittelee yrityksen tietoja, tulisi ottaa mukaan kaikkein ensimmäisenä yrityksen tietoturvan kehittämiseen. Yrityksen työntekijät tietävät parhaiten toiminnot, joita tulisi kehittää tietoturvan osalta. Työn-

tekijät eivät välttämättä suoranaisesti osaa kertoa, missä kehittämiskohteet ovat, mutta tietoturvan ammattilainen osaa kysyä sellaiset kysymykset, että kehittämiskohteet saadaan tietoon. On siis erittäin tärkeää, että yrityksen tietoturvan kehittäminen tehdään jonkun yrityksen ulkopuolisen asiantuntijan johdolla varsinkin silloin, jos osaamista ei ole omasta takaa. Samaan aikaan kun kehittämiskohteita otetaan selville, myös työntekijän tieto- ja taitotaso paranee. Näin työntekijät voivat itse kehittää tapojaan käsitellä tietoa. Ennen kaikkea tällaisessa kartoituksessa kuitenkin saadaan tärkeää tietoa siitä, miten yrityksen työntekijät käsittelevät tietoja. Tämän jälkeen näille rutiineille voidaan kehittää parhaat mahdolliset suojaukset ja kouluttaa ja ohjeistaa työntekijät käyttämään niitä.

Tietoturvan kehittämistä ei saisi missään nimessä kuitenkaan antaa pelkästään esimerkiksi yrityksen tietohallintoväen tehtäväksi. Tällöin voi olla riskinä, että tietoturvaan tulee liian suppea tekninen lähestymistapa. Tietoturvan kehittämisessä täytyy aina olla mukana henkilöitä useasta liiketoimintayksiöstä. Näin asioihin saadaan monipuolinen kokonaiskuva.

Esimies

- *Yrityksen omat työntekijät tietävät parhaiten, miten tietoturvaa tulisi kehittää.*
- *Käytä tietoturvan kehittämiseen liittyvään keskusteluun tarvittaessa ulkopuolista asiantuntijaa.*
- *Älä anna tietoturvan kehittämiseen liittyvää työtä pelkästään tietohallintoväen tehtäväksi.*

8 KOULUTUS

Työntekijöiden koulutus on erittäin tärkeässä asemassa tietoturvan kehittämisessä. Monissa tutkimuksissa on tullut ilmi, että yritykset laiminlyövät henkilöstön tietoturvallisuuskoulutuksen ja erityisesti koulutuksen vaikutuksen mittaamisen. Teknisen infrastruktuurin lisäksi tulisi satsata merkittävässä määrin myös työntekijöiden koulutukseen. Hyvät työvälineet yksinään eivät riitä tehokkaaseen ja tietoturvalliseen työskentelyyn varsinkaan silloin, kun niitä ei osata käyttää tarkoituksenmukaisella tavalla. Joka tapauksessa tietoturva vaatii tietoisuutta ihmisten oman toiminnan seurauksista ja siitä tullaan tietoiseksi vain kouluttautumalla ja itse aktiivisesti opiskelemalla.

8.1 PEREHDYTYS

Ensimmäinen koulutus/ohjaus tietoturva-asioiden pariin työntekijälle tulisi olla siinä vaiheessa, kun hän tulee uutena työntekijänä yritykseen töihin. Perehdytyksellä henkilö saatetaan talon tavoille. Perehdytyksen antavalla esimiehellä on merkittävä vaikutus siihen, miten uusi työntekijä tulee jatkossa käyttäytymään tietoturvan osalta. Esimiehen on korostettava sellaista toimintakulttuuria, jossa ollaan koko ajan tietoisia erilaisista tietoriskeistä. Tietoturvaa kannattaa painottaa työntekijälle heti työuran alusta alkaen. Tosin sama painotus täytyisi jatkua myös työkavereiden keskuudessa, jotta hyvät elkeet tietoturvallisen käyttäytymisen osalta eivät unohdu heti, vaan ne tulisivat luontevaksi osaksi työtä. Uudelle työntekijäl-

le perehdytys on alkusignaali sille, kuinka yritys toimii ja kuinka siellä tulisi käyttäytyä. Ristiriitaiset signaalit, joita uusi työntekijä voi saada esimieheltä verrattuna työkavereihinsa, täytyisi saada poistettua. Kauemmin talossa olleet työntekijät saattavat vähätellä esimiesten antamia ohjeita uudelle työntekijälle, varsinkin jos tietoturvakäyttäytymiseen liittyvää muutosta ollaan juuri viemässä läpi koko talon tasolla. Tähän auttaa vanhemman työntekijäkaartin motivointi ja kouluttaminen tietoturvan pariin.

Esimiehen on tärkeää käydä monia työn luonteeseen liittyviä tietoturvallisuusseikkoja läpi uuden työntekijän kanssa. Näitä ovat Kyrölän (2001:155) mukaan seuraavat asiat:

- Vaitiolo- ja salassapitosopimusten merkitys
- Työsuhteen tekijänoikeudelliset seikat
- Käytettävien järjestelmien ja muiden välineiden käyttöohjeet
- Käsiteltävien tietojen arvo yritykselle ja asiakkaille
- Tietojen luokittelun periaatteet
- Sellaisten luottamuksellisten tietojen konkretisointi, joista puhuminen on kielletty
- Esimerkein kerrottuna, mitä ovat tilanteet, joissa on oltava huolellinen.
- Mitä tarkoittaa tietoturvarikkomus?

8.2 KOULUTUS JA OSAAMISEN ARVIOIMINEN

Työntekijöiden koulutus on yksi yrityksen tietoturvan peruskivistä. Koulutuksen avulla voidaan päästä pois sellaisista tietoturvattomista toimintatavoista, jotka ovat ajan saatossa muodostuneet rutiininomaisiksi perusoletuksiksi. Kaiken kaikkiaan on erittäin tärkeää, että työntekijät oppivat tiedostamaan erilaiset tietoturvauhat, koska muuten niitä ei pystytä ehkäisemään. Koulutuksella on merkittävä asema juuri tietoturvauhkien tiedostamisessa. Kuten aiemminkin on jo todettu, jokainen työntekijä on omalta osaltaan vastuussa tietoturvauhkien torjunnassa. Tämä pitäisi näkyä koulutuksessa opittujen asioiden soveltamisessa ja annettujen ohjeiden noudattamisessa. Aina näin ei kuitenkaan ole, sillä koulutus ei aina välttämättä onnistu toivotulla tavalla.

Koulutuksen epäonnistuminen voi johtua siitä, että koulutus ohittaa kohderyhmän tarpeet. Koulutus on esimerkiksi liian teoreettinen, tekninen tai laaja. Tällöin opetellut asiat jäävät epäselviksi tai kokonaan teoreettiselle tasolle ilman, että niitä pystytään tehokkaasti soveltamaan käytäntöön. Työntekijät eivät siis saa toivomaansa koulutusta juuri heidän työtään koskevista seikoista. Tietoturvakoulutus pitäisikin järjestää siten, että se liittyisi mahdollisimman paljon suoraan työntekijän tekemään työhön eli niihin rutiineihin, joissa tietoa käsitellään. Usein tämä ei kuitenkaan ole täysin mahdollista, mutta koulutuksen tilaajan ja koulutuksen järjestäjän yhteistyöllä voitaneen välttyä suurimmilta epäonnistumisilta. Räätälöity koulutus kuitenkin vaatii sen, että kouluttaja esimerkiksi

käy yrityksessä analysoimassa mahdollisia tietoturvapuutteita niin työympäristössä kuin työntekijöiden tietojen käsittelyn osalta.

Esimies

- *Tietoturvakoulutus on yksi tietoturvallisen toiminnan peruskivistä.*
- *Koulutuksella ”rikotaan” tietoturvattomia toimintatapoja, jotka ovat muuttuneet ajan saatossa selviksi rutiineiksi eli perusoletuksiksi.*
- *Työntekijöiden tulisi oppia tiedostamaan työtehtävissään piilevät tietoturvauhat.*
- *Koulutus olisi hyvä olla suoraan työntekijän työhön liittyvää myös koulutuksen mielenkiinnon ylläpitämisen takia.*

Tilaajan ja järjestäjän kannattaa tehdä yhteistyössä myös jonkinlainen osaamiskartoitus siitä, mitä pitää ja kannattaa opettaa ja mikä on kohderyhmä. Työntekijöitä ei tule kouluttaa vain kouluttamisen vuoksi, vaan koulutukselle tulisi asettaa jonkinlainen tavoite ja vaatimukset. Lisäksi tulisi muistaa, että työntekijät lähtevät kouluttautumaan kukin omalta tasoltaan. Ei pidä ajatella, että koko työyhteisöllä on sama osaaminen ja kaikki lähtevät samalta viivalta. Samalla kun kouluttaudutaan ja kun koulutus on saatu päätökseen, niin asetettujen tavoitteiden saavuttamista tulisi myös arvioida. Myös koulutuksen onnistumisen mittaamiselle löytyvät keinot koulutuksen järjestäjän ja tilaajan yhteistyöllä. Näistä arvioin-

tikeinoista voidaan sopia jo ennen koulutuksen aloittamista. Eräs tietoturvakoulutuksen parhaista onnistumisen mittareista on kuitenkin se, miten opittuja tietoja osataan soveltaa ja noudattaa käytännössä.

Mitä työntekijän sitten pitäisi tietoturvan osalta osata ja millaiseen koulutukseen työntekijän pitäisi hakeutua, jotta tietoturvaan liittyvät asiat selviävät? Tämä riippuu ennen kaikkea siitä, millaista tietoa työntekijä työssään käsittelee. Työntekijöiden työnkuvat voivat olla hyvinkin erilaisia. Joidenkin työntekijöiden osalta tietoturvataso kohentuu jo muutamien asioiden huomioimisella. Sen sijaan joidenkin työntekijöiden tulee huomioida useita eri seikkoja, jotta tietoturva toteutuisi mahdollisimman hyvin. Erityisen tärkeää työntekijälle on saada tietoa hänen oman toimintansa seurauksista. Tässä kaiken perustana on työntekijöiden käsittelemä tieto ja ne tavat ja rutiinit, joilla tietoa käsitellään. Erityisesti rutiinityön osalta erilaiset tietoturvan laiminlyöntiin liittyvät virheet pitäisi pyrkiä minimoimaan.

Esimies

- *Työntekijöitä ei pidä laittaa koulutukseen vain kouluttautumisen vuoksi. Koulutukselle on asetettava tavoite ja vaatimukset.*
- *Kunkin työntekijän pitäisi saada koulutusta oman tasonsa mukaisesti.*
- *Työntekijän pitäisi saada ennen kaikkea tietoa hänen oman toimintansa seurauksista. Tällä tavoin uuden toimintatavan*

Koulutuksen järjestäminen

Riippuen koulutettavasta asiasta koulutus voidaan järjestää joko yrityksen omissa tiloissa tai kouluttajan järjestämässä paikassa. Koulutuspaikan valintaan vaikuttaa koulutettava asia. Ellei koulutuksen tilaajalla ole tarpeellisia tiloja ja laitteita teknisen tietoturvan koulutukseen, työntekijöitä on turha yrittää kouluttaa käyttämään laitteita ja sovelluksia turvallisesti. Tällöin koulutus tietysti pyritään järjestämään kouluttajan tiloissa. Huomioitavaa kuitenkin on, että kouluttajan ympäristöllä ja laitteilla voidaan usein opettaa vain yleisiä tietoturvallisuuteen liittyviä asioita. Tämän jälkeen opetettu asia pitäisi pystyä vielä soveltamaan omaan työympäristöön. Tässä voi tulla ongelmia, varsinkin jos käytössä on erilaisia sovelluksia ja laitteita verrattuna kouluttajan ympäristön laitteisiin ja sovelluksiin.

Koulutus voidaan järjestää myös yrityksen tiloissa. Yrityksen tiloissa suoritettava koulutus voi liittyä suoraan työntekijöiden työtehtäviin ja niiden tietoturvan parantamiseen tai esimerkiksi yrityksessä laadittujen tietoturvaohjeiden noudattamiseen liittyvään koulutukseen. Koulutus voi olla esimerkiksi kouluttajan ja osaston työntekijöiden välinen keskusteleva koulutus joka etenee seuraavasti (mukaillen Puhakainen 2006):

- Koulutettavat esittelevät kouluttajalle omaa työnkuvaansa, työtehtävissään käsittelemäänsä tietoa ja sitä miten he tietoa käsittelevät.
- Koulutettavat analysoivat käsittelemäänsä tietoa ja etsivät siitä yritykselle arvokasta tietoa.

- Koulutettavien seuraavana tehtävänä on miettiä, mitä haittaa yritykselle on, jos arvokas tieto tavalla tai toisella joutuu vääriin käsiin tai tuhoutuu.

- Tämän jälkeen mietitään, miten työtä voidaan muuttaa ja mitä työvälineitä mahdollisesti täytyy käyttää, jotta arvokas tieto ei joudu vääriin käsiin tai tuhoudu

Tällaiseen analyysiin ei välttämättä tarvita edes ulkopuolista kouluttajaa. Työntekijät pystyvät itsekin miettimään, mikä on yritykselle arvokasta tietoa. He voivat myös pohtia, miten heidän on muutettava omaa työtään, jotta tämä arvokas tieto ei joudu vääriin käsiin. Joka tapauksessa tällaisen koulutuksen tarkoituksena on nimenomaan auttaa työntekijöitä tiedostamaan, millaisia tietoturvariskejä omat työtehtävät voivat aiheuttaa.

Esimies

- *Tietoteknisiin tietoturvataitoihin liittyvä koulutus täytyy yleensä järjestää kouluttajan tiloissa johtuen tiloista ja välineistä.*
- *Yrityksen tiloissa tapahtuva koulutus voi liittyä suoraan yrityksessä käsiteltäviin tietoihin ja niiden arviointiin.*

8.3 PALAVERIT JA YLEINEN KESKUSTELU

Työpaikan palavereissa kannattaa ottaa esille ajankohtaisia tietoturvaan liittyviä asioita. Käsiteltävät aiheet voivat olla esimerkiksi tietoturvaohjeiden kertausta, painotusta tai päivitystä työntekijöille. Toisaalta asiasisällöt voivat olla myös tietoja viimeisimpien haittaohjelmien leviämisestä ja tietokoneisiin ajettavista tietoturvapäivityksistä. Palavereissa ja yleisessä keskustelussa tietoturva-asiat tulisi pitää esillä koko ajan, jotta tärkeät tietoturvalliset työskentelytavat eivät unohdu. Palavereissa ja yleisessä keskustelussa kerratut asiat alkavat vähitellen luoda yritykseen tietoturvallisia toimintatapoja ja sitä myöden myös vaikuttavat tietoturvakulttuurin muodostumiseen. Mitä suurempi työntekijäjoukko tietoturvallisia työskentelytapoja noudattaa, sitä parempi asia se on yrityksen liiketoiminnalle.

Esimies

- *Tietoturvaan liittyviä asioita on tarpeen usein ottaa esille arkisissa tilanteissa.*

9 PK-YRITYKSEN VAHVUUDET PAREMMAN TIETOTURVAKULTTUURIN LUOMISESSA

Pk-yrityksillä on joitakin vahvuuksia, joita ne voivat käyttää paremman tietoturvakulttuurin muodostamiseen. Pk-yritysten vahvuuksia ovat mm. matala organisaatiorakenne, luovuudelle ja uusille ideoille avoin ympäristö ja toiminnan kontrolli. Matalan organisaation vahvuus on, että johtajat ovat lähellä alaisiaan. Tämä vaikuttaa nopeaan viestien perille menoon eli johdon toiveisiin ja tavoitteisiin voidaan nopeasti vastata. Johdosta ei tule myöskään mikään näkymätön ”mörkö”, jonka syyksi keskijohdon on mahdollista laittaa kaikki negatiiviset asiat, joita yrityksessä tapahtuu. Suora suusta suuhun kommunikointi vahvistaa viestien perille menoa, koska suorassa kommunikoinnissa myös eleet ovat mukana. Lisäksi pienissä yrityksissä on mahdollista saada koko työntekijäporukka nopeasti kokoon ja kertoa heille ajatuksistaan. Suurissa yrityksissä tämä ei onnistu, sillä työntekijät voivat olla levittäytyneet maantieteellisestikin eri toimipisteisiin.

Toinen pk-yritysten vahvuus on luovuudelle ja uusille ideoille avoin ympäristö. Esimiehelle on helppo mennä esittämään omia ideoitaan ja ajatuksiaan toiminnan kehittämisestä. Yleensä esimiehellä on vielä valta päättää toteutetaanko idea vai ei. Esimiesten kannattaa käyttää tätä voimavaraa hyväksi myös tietoturvallisten toimintatapojen kehittämisessä kannustamalla työntekijöitä kehittämään niitä. Suuressa organisaatiossa tällaisten toimintaan liittyvien ideoiden kehittely saattaa jäädä lähimmän esimiehen laiskuuteen viedä asiaa eteenpäin

päättävään johtoportaaseen. Jäykän hierarkian takia suuressa organisaatiossa voi käydä jopa niin, että ylin johto ikään kuin eristäytyy omaksi hallinnolliseksi yksiköksi ja vieraantuu varsinaisesta tuottavasta toiminnasta.

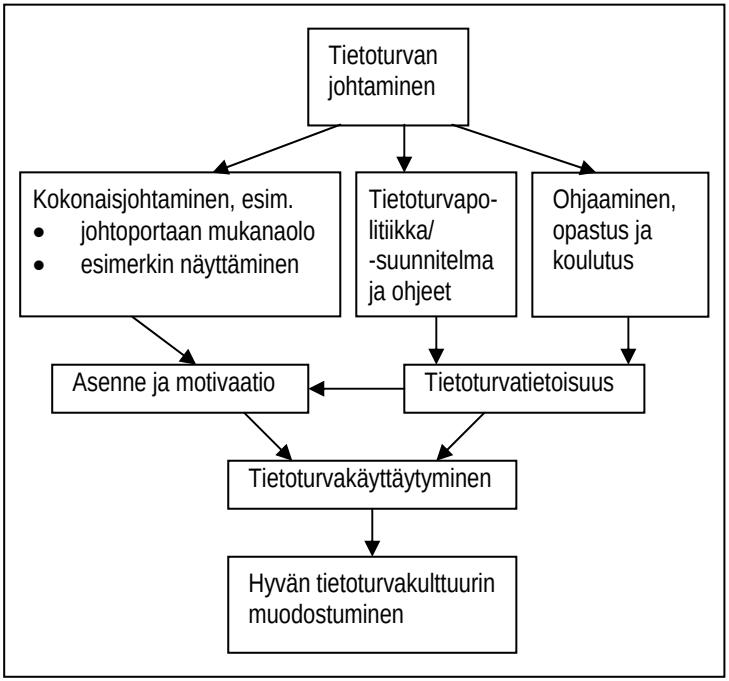
Kolmas vahvuus, joka jo edellä mainittiin, on toiminnan kontrolli. Matalan organisaation vuoksi päivittäisten toimintojen ohjaus ei ole hierarkista. Näin ollen toiminnan kontrolli mahdollistaa nopeiden muutosten ja päätösten tekemisen eli nopean liikkumisen toimintaympäristössään. Pk-yritykset ovatkin nopeita liikkumaan toimintaympäristössään johtuen niiden tottuneesta toiminnasta nopeasti muuttuvilla markkinoilla. Tätä etua kannattaa hyödyntää myös tietoturvallisen toiminnan kehittämisessä ja ylläpitämisessä. Koska pk-yritysten yrityskulttuurissa on totuttu muutoksiin, muutos tietoturvallisempaan toimintaankaan ei välttämättä ole kovin hankalaa.

Esimies

- *Käytä hyväksi pk-yrityksen vahvuuksia tietoturvallisen toiminnan kehittämisessä ja ylläpitämisessä.*
- *Näitä vahvuuksia ovat matala organisaatiorakenne, ideoille avoin ympäristö ja toiminnan kontrolli.*

10 JOHTAMISELLA JA KOULUTUKSELLA TUETAAN YRITYKSEN MUODOSTAMIA TIETOTURVALLISIA ARVOJA

Hyvä tietoturvakulttuuri muodostuu kokonaisjohtamisesta, tietoturvapolitiikan, -suunnitelmien ja -ohjeiden laatimisesta sekä ohjaamisesta, opastuksesta ja koulutuksesta (ks. kuva 3). On selvää, että myös nykytilan yrityskulttuuri vaikuttaa tietoturvakulttuuriin. Yllä mainituilla seikoilla on kuitenkin mahdollisuus vaikuttaa paremman tietoturvakulttuurin muodostumiseen, kun taas yrityskulttuuri on jo olemassa oleva ja usein jopa painolastina uudistusten edellä.



Kuva 3. Hyvä tietoturvakulttuuri muodostuu hyvästä johtamisesta, johtajien luomista arvoista ja tietoturvatietoisuuden lisäämisestä.

10.1 ARVOT HYVÄN TIETOTURVAKULTTUURIN PERUSTANA

Tietoturvallisuuden arvot eli tietoturvapolitiikka, tietoturvasuunnitelma ja näistä muodostuvat ohjeet vaikuttavat paremman tietoturvakulttuurin muodostumiseen. Tämä johtuu siitä, että ne ilmaisevat, mikä on toivottavaa tietoturvallista käyttäytymistä. Arvot vaikuttavat myös tietoturvatietoisuuden kehittymiseen. Tietoturvatietoisuuden kautta arvoilla on vaikutusta myös asenteisiin ja motivaatioon. Onhan selvää, että parempi tietoturvatietoisuus motivoi tietoturvallisempien toimintatapojen noudattamiseen. Lisäksi asenteet muuttuvat, kun on ymmärretty, miksi näitä arvoja tulee noudattaa.

Käytännössä tietoturvapolitiikka määrittelee yrityksen tietoturvallisuuden tavoitteet, vastuut ja toimenpiteet, joilla tavoitteet saavutetaan. Tietoturvapolitiikka on yleensä julkinen dokumentti, joka on tarkoitettu koko yrityksen henkilöstölle, asiakkaille ja muille yhteistyökumppaneille. Se voidaan antaa asiakkaille ja yhteistyökumppaneille osoituksena siitä, että yrityksellä on vakava pyrkimys suojata omat ja kumppaneidensa tiedot.

Tietoturvasuunnitelma puolestaan on tarkempi ja konkreettisempi dokumentti, joka sisältää yksityiskohtaiset menettelytavat, kuinka määriteltyyn tietoturvallisuuden tasoon päästään. Tietoturvasuunnitelma on aina luottamuksellinen tai salainen dokumentti.

Tietoturvasuunnitelmasta muodostetaan ohjeet tietoturvallista toimintaa varten. Joskus tietoturvasuunnitelma toimii myös ohjeena. On silti huomioitava, että tietoturvasuunnitelma saattaa sisältää asioita, jotka täytyy pitää vain rajatun työntekijäjoukon tiedossa. Lisäksi tulee huomioida myös luvussa kaksi mainitut asiat, joiden vuoksi ohjeet usein jätetään noudattamatta. Näitä ovat mm. ohjeiden vaikeaselkoisuus ja ohjeiden merkityksettömyys omaan työhön. Tietoturvasuunnitelma sellaisenaan saattaa nimittäin sisältää vaikeaselkoista termistöä ja työntekijän työhön liittymättömiä merkityksettömiä asioita.

Ohjeet tietoturvalliseen toimintaan tulisi siis laatia erikseen sillä tavalla, että ne koskevat esimerkiksi yhden osaston toimiin kuuluvia tietoturvallisia toimintatapoja. Ohjeiden pitäisi olla selkeät ja niissä tulisi perustella, miksi ohjetta pitää käyttää. Lisäksi niissä tulisi ilmetä, mikä merkitys ohjeilla on työntekijöiden työhön. Tietoturvaohjeet ovat myös luottamuksellisia tai salaisia dokumentteja

Esimies

- *Tietoturvapolitiikka, -suunnitelma ja ohjeistukset muodostavat yrityksen tietoturvakulttuurin arvot.*

10.2 OHJAAMINEN, OPASTUS JA KOULUTUS VAIKUTTAVAT ARVOJEN YMMÄRTÄMISEEN

Koulutuksella, ohjaamisella ja opastuksella voidaan vaikuttaa siihen, kuinka hyvin työntekijät ymmärtävät arvot ja osaavat toimia niiden mukaisesti. Koulutus, ohjaaminen ja opastus vaikuttavat huomattavan paljon parempaan tietoturvatietoisuuteen ja sitä kautta myös asenteeseen ja motivaatioon.

Työntekijät voidaan johdattaa arvoihin koulutuksella. Näin arvot saadaan ainakin osittain jalkautettua. Pelkkä muutaman päivän koulutus ei kuitenkaan vielä välttämättä takaa arvojen ymmärtämistä konkreettisella tasolla. Koulutuksen lisäksi pitäisi olla myös ohjaamista ja opastusta arkipäivän tilanteissa.

Tietoturvallisten toimintatapojen kehittämisen alkumetreillä työntekijöiden tulisi oivaltaa kuinka laadittuja arvoja lähdetään toteuttamaan esimerkiksi osastokohtaisesti. Tämä vaatii koulutusta/kouluttautumista tai vähintään aktiivista tiedon hankintaa asian ympäriltä. Lisäksi jos työntekijät laitetaan yhdessä laatimaan tietoturvaohjeita omien toimintatapojen kehittämiseksi tietoturvallisempaan suuntaan, pitäisi työntekijöillä olla ymmärrystä myös tietojärjestelmien ja tietoteknisten laitteiden turvallisesta käyttämisestä. Usein koulutusta tarvitaan myös vielä aivan tavalliseen sovellusten ja laitteiden peruskäyttöön. Näin vältytään ainakin useimmilta vahingossa tapahtuvilta perusvirheiltä.

Monesti turvallisempien toimintatapojen kehittämiseen tarvitaan vain yksinkertaisia ja pieniä työhön liittyviä muutoksia joita voivat olla mm.:

- Käyttäjätunnuksia ja salasanoja ei kirjoiteta liimalapuille esim. näytön viereen.
- Käyttäjätunnuksia ja salasanoja ei jaeta asiakkaille tai työkavereille.
- Tehdään varmuuskopiot.
- Luottamuksellisia paperidokumentteja tai muuta luottamuksellista tietoa sisältäviä massamuistivälineitä ei jätetä työpöydille.
- Mietitään, mitä tietoa sähköpostilla voidaan lähettää.
- Millä tavoin yrityksen tietoa liikutellaan esimerkiksi kodin ja työpaikan välillä.

Usein työntekijät pystyvät kehittämään näitä turvallisia toimintatapoja ilman varsinaista johtoporrasta tai konsulttia, jos heille vain annetaan siihen aikaa. Tietoturvallisiin toimintatapoihin päästään varsin pienillä teoilla. Usein kyse on sääntöjen noudattamisen kurinalaisuudesta ja viitseliäisyydestä. Tähän voidaankin vaikuttaa jatkuvalla ohjaamisella, opastuksella ja tietoturvaan liittyvien asioiden esille nostamisella ryhmäpalavereissa ja muissa kokouksissa. Lisäksi alla käsiteltävät johtamiseen liittyvät asiat vaikuttavat opittujen toimintatapojen ja ohjeiden noudattamiseen.

Esimies

- *Laadittujen arvojen ymmärtämiseen vaikuttavat koulutus, ohjaaminen ja opastus.*
- *Varsinkin tietoturvallisten toimintatapojen kehittämisen alkumetreillä työntekijöille pitäisi saada ymmärrys, miten laadittuja arvoja lähdetään toteuttamaan.*
- *Turvallisiin toimintatapoihin päästään usein varsin pienillä teoilla.*

10.3 KOKONAISJOHTAMINEN VAIKUTTAA ARVOJEN NOUDATTAMISEEN

Johtamisella tuetaan toivottua arvojen mukaista käyttäytymistä. Tässä tulee kyseeseen luvussa seitsemän mainittuja asioita, kuten esimerkkinä oleminen, tietoturvan kehittämiseen sitoutuminen, kehittämisessä ja koulutuksessa mukana oleminen ja työntekijöiden osallistaminen tietoturvan kehittämiseen. Hyvä työntekijöiden johtaminen vaikuttaa työntekijöiden asenteeseen ja motivaatioon kehittää tietoturvallisia toimintatapoja.

Hyvä johtaminen voi olla esimerkiksi työntekijöiden mukaan ottamista tietoturvaohjeiden laatimisen yhteydessä. Tietoturvapolitiikan ja tietoturvasuunnitelmien laatimiseen ei useinkaan kuitenkaan voida käyttää koko työntekijäjoukon resursseja. Sen sijaan laadittaessa tietoturvallisia toimintaohjeita tietoturvapolitiikan ja -suunnitelman pohjalta, kannattaa työntekijöitä kuitenkin käyttää. Kunkin osaston työntekijät voivat esimerkiksi yhdessä laatia ohjeet esimiehen ja/tai ulkopuoli-

sen konsultin johdolla. Ohjeiden laatiminen saattaa työntekijät aktiiviseen ajatteluun ja yhdessä tekemiseen. Tämä johtaa väistämättä osaston työntekijöiden omien toimintatapojen kartoittamiseen ja niiden kehittämiseen tietoturvan osalta. Näin saadaan muodostumaan osastokohtainen tietoturvaohjeistus, joka koskee nimenomaan kyseisen osaston toimia.

Samalla, kun työntekijät miettivät toimintatapojaan tietoturvallisempaan suuntaan, saadaan heidän tietoturvatietoisuutensa kohentumaan aivan eri tasolle. Lisäksi, kun työntekijät ovat tehneet ohjeistuksen omista lähtökohdistaan, on myös todennäköisempää, että ohjeita noudatetaan. Näin ollen ohjeiden ymmärtämisen lisäksi saadaan aikaiseksi myös toinen ulottuvuus, joka on ohjeiden noudattaminen.

Esimies

- *Tietoturvaohjeet nostavat työntekijöiden tietoturvatietoisuutta varsinkin silloin, kun ne laaditaan yhdessä osastokohtaisesti.*
- *Työntekijät noudattavat itse laatimiaan ohjeita todennäköisemmin kuin että ne olisi laatinut osaston ulkopuolinen henkilö.*

11 YHTEENVETO

Työntekijöiden tietoturvalliset toimintatavat eivät ole itsestäänselvyys varsinkaan pk-yrityksissä. Niihin pystytään silti vaikuttamaan hyvin pienilläkin toimenpiteillä. Varsinkin pk-yritysten esimiehillä on suuri rooli ja mahdollisuudet näiden toimintatapojen parantamisen johtamisessa. Aivan ensimmäisenä yritykselle pitäisi kuitenkin luoda arvot, johon nämä tietoturvalliset toimintatavat perustuvat. Tämä tehdään laatimalla yrityksen tietoturvallista toimintaa koskeva tietoturvapolitiikka ja yksityiskohtaisempi tietoturvasuunnitelma. Nämä arvot kertovat työntekijöille, mitä pidetään toivottavana tai tavoittelemisen arvoisena käyttäytymisenä.

Näiden arvojen iskostumiseen työntekijöiden ajatuksiin esimiehet voivat vaikuttaa monin eri tavoin. Oman esimerkin näyttäminen ja omien toimintatapojen ja sanomisien tiedostaminen on ensimmäinen askel. Lisäksi ohjaamista ja opastusta tulisi olla erilaisissa arkipäivän tilanteissa kuten ryhmäpalavereissa, kehityskeskusteluissa ja työntekijöiden välisissä keskusteluissa.

Lisäksi esimiehet voivat käyttää pk-yritykselle ominaisia vahvuuksia, kuten matalaa organisaatiorakennetta, uusille ideoille avointa ympäristöä ja toiminnan kontrollia. Myös ajansaatossa muodostunut yrityskulttuuri vaikuttaa toimintatapojen kehittymiseen. Onhan selvää, että työntekijöille on vuosien aikana syntynyt erilaisia pinttyneitä toimintatapoja, jotka voivat olla tietoturvan kannalta huonoja. Näistä toimintatavoista pi-

täisi tarvittaessa poisoppia. Siksi esimiesten pitäisikin tiedostaa, millainen yrityskulttuuri yrityksessä on uuden oppimisen kannalta ja valita oma johtamistyylinsä muutokseen sen mukaisesti.

Tietoturvakoulutukseen hakeutuminen kannattaa, sillä se maksaa itsensä moninkertaisesti takaisin. Kouluttaminen ja kouluttautuminen ovatkin ehdottoman tärkeitä oikeiden tietoturvallisten toimintatapojen muokkaamiseksi ja vanhojen toimintatapojen unohtamiseksi. Koulutuksessa on kuitenkin syytä välttää kaikkea kaikille tyylistä koulutusta. Ennemminkin tulisi pyrkiä jakamaan työntekijät erilaisiin ryhmiin osaamisensa perusteella ja antaa ryhmille koulutusta kohdennetusti. Myös kouluttajalle on hyvä mainita näistä koulutuksen toiveista. Ennen kaikkea koulutuksella tulisi pyrkiä tilanteeseen, jossa työntekijät oivaltavat, mitä tietoturvaongelmia omista toimintavoista seuraa. Näin perustellaan samalla oikean turvallisen toimintatavan käyttöönotto, ja henkilöstö oppii yhä paremmin tarkkailemaan omaa toimintaansa tietoturvan kannalta.

LÄHTEET

Kyrölä, Tuija 2001. Esimies ja tietoriskien hallinta.

Puhakainen, Petri 2006. A design theory for information security awareness.

Schein, Edgar H. 2001. Yrityskulttuuri – selviytymisopas.

Siponen, Mikko & Pahnila, Seppo 2006. Tietoturvaohjeiden on oltava selkeät ja helposti saatavilla. Helsingin Sanomat 25.8.2006.

Suominen, Arto 2003. Riskienhallinta.