KARELIA-AMMATTIKORKEAKOULU

Tietojenkäsittelyn koulutusohjelma

Liisa Pappinen

PK-YRITYKSEN TIETOTURVASUUNNITELMA

Opinnäytetyö

Maaliskuu 2013

Karelia AMMATTIKORKEAKOULU	**OPINNÄYTETYÖ** **Maaliskuu 2013** **Tietojenkäsittelyn koulutusohjelma** **Karjalankatu 3** **80200 JOENSUU**

Tekijä(t)

Liisa Pappinen

Nimeke

PK-yrityksen tietoturvasuunnitelma

Toimeksiantaja itäsuomalainen PK- yritys

Tiivistelmä

Tämän opinnäytetyön aiheena oli laatia PK- yrityksen tietoturvasuunnitelma. Toimeksiantajan oli itäsuomalainen PK- yritys. Tietoturvasuunnitelman tekoa varten syvennyttiin kirjallisuuteen, jonka pohjalta laadittiin teemahaastattelukysymykset yrityksen tietoturvan kartoitusta varten. Teemahaastattelu toteutettiin keskustelemalla yrityksen henkilökunnan kanssa, haastattelun pohjalta yrityksen tietoturvasta tehtiin sekä fyysinen että tekninen kartoitus.

Yrityksessä havaittiin paljon puutteita sekä sen fyysisessä että teknisessä tietoturvassa. yrityksessä suurimmat tietoturvauhat olivat käyttöturvallisuudessa eli kulunvalvonnassa, dokumenttien säilytyksessä ja laitteistojen ja ohjelmistojen käyttöoikeuksissa sekä fyysisessä turvallisuudessa eli tuli- ja vesivahingoilta tai ilkivallalta varautumisessa. Laitteistoturvallisuuden osalta pahimmat puutteet olivat työasemien varmuuskopioinnissa. Riskianalyysin perusteella voitiin todeta, että yrityksessä todennäköisin tietoturvariski on tietovuoto.

Teemahaastattelun havaintojen ja kartoituksen sekä kirjallisuuden pohjalta laadittiin taulukko kattavan tietoturvasuunnitelman tekemisen apuvälineeksi PK- yrityksessä. PK- yrityksen tietoturvasuunnitelmaa tehtäessä taulukkoon muotoiltuja kysymyksiä voidaan hyödyntää yrityksen kannalta suurimpien tietoturvauhkien kartoituksessa ja niihin toimivia ratkaisuja ja tietoturvan osa-alueiden vastuuhenkilöitä haettaessa. Laadittua taulukkoa hyödyntäen yritykselle laadittiin tietoturvasuunnitelma; suunnitelman toteutus ei kuitenkaan enää kuulunut tämän opinnäytetyön toimeksiantoon.

Kieli suomi	Sivuja 32 Liitteet 1 Liitesivumäärä 1

Asiasanat

Tietoturvan osa-alueet, Tietoturva

Karelia UNIVERSITY OF APPLIED SCIENCES	**THESIS** **March 2013** **Degree Programme iInformation Systems** **Karjalankatu 3** **FI 80200 JOENSUU** **FINLAND**

Author(s)

Liisa Pappinen

Title: An Information Security Plan for a Small and Medium Sized Enterprise

Abstract

The aim of this study was to develop an information security plan for a small SME in eastern Finland. Based on suitable literature a theme interview questionnaire was developed for exploring information security mapping at the SME. The theme interview was carried out by talking with the staff of the company. Based on the company interview both physical and technical security mapping was done in this Case company.

In the security mapping, a number of deficiencies on both the physical and technical security were found. The biggest security threats were found in access control, storage of documents and storage of hardware and software and the use rights of the computers and software. The physical security issues like, fire and water damage or vandalism which were not taken into account at the company. The worst deficiencies on hardware safety issues were lack of back up workstations. Based on the risk analysis a security leak would be the most probable security risk in this case company.

Based on the interview findings, as well as a literature review, an information security question chart was worded as a tool for making a comprehensive information security plan for the SME. With this formulated information security question chart an information security plan for the Case - company was created next. The implementation of the security plan was no longer the mandate of this thesis.

Language	Pages 32 Appendices 1
Finnish	Pages of Appendices 1

Keywords

information security, Security aspects

Sisällys

1 Johdanto

Tietoturvan tarkoituksena on yleensä vaaran minimoiminen. Tietoturva voi olla fyysistä, teknistä tai hallinnollista. Riskien ennaltaehkäiseminen on tärkeää, koska tietoturvasta huolehtimalla voidaan välttää vahinkoja. Tietoturvallisuus on huomattavasti laajempi käsite kuin ns. atk-turvallisuus tai henkilötietoihin liittyvä tietosuoja.

Suuret kansainväliset ja kotimaiset yritykset ovat panostaneet tietoturvaan huomattavasti enemmän kuin pienet ja keskisuuret yritykset. Tämä voidaan selittää sillä, että mitä enemmän on suojeltavaa, sitä enemmän sen turvaamiseen on kiinnitettävä huomiota. Luonnollisesti suurilla yrityksillä on käytettävissä myös enemmän rahaa ja resursseja yrityksen tietoturvan kehittämiseen.

Tietoturvan tulisi olla osa yrityksen jokapäiväistä liiketoimintaa. Tietoturvassa ei ole kyse pelkästään tekniikasta vaan ihmisen toimintatavoista, jotka vaikuttavat yleiseen tietoturvallisuuteen. Yrityksen kaikkien työntekijöiden tulee tietää, miten tietoturvaa toteutetaan. Yrityksillä on usein tietoja, jotka laki velvoittaa turvaamaan. Hyvä tietoturva ei välttämättä vaadi suuria investointeja, pienikin panostus voi hyödyttää yrityksen liiketoimintaa.

Opinnäytetyöni aiheena on tietoturvasuunnitelman laatiminen eräälle metallialan pk-yritykselle. Suunnitelman tavoitteena on selvittää yrityksen tämänhetkinen tietoturvataso ja laatia mahdolliset korjausehdotukset. Toimeksianto tietoturvasuunnitelmaan tuli johdolta itseltään, mutta tässä opinnäytetyössä käsitellään tietoturvaa myös yleisellä tasolla. Näin ollen mikä tahansa pk-yritys voi soveltaa tämän työn tuloksia ja johtopäätöksiä omassa toiminnassaan.

Opinnäytetyön tieto-osuudessa luvussa 2 tarkastellaan aluksi tietoturvan osa-alueita, ja luvussa 3 selvitetään pk-yrityksen tietoturvan vaatimuksia. Luku 4 sisältää pohjamateriaalin tutkimukselle. Siinä esitellään myös tutkimuksen eri vaiheet ja osa-alueet sekä tietoturvasuunnitelman yleismalli, jota tehdessä on hyödynnetty case yrityksen suunnitelman tutkimustuloksia. Luku 5. on tiivistelmä yritykselle tehdystä tietoturvasuunnitelmasta. Loppuyhteenvedossa arvioidaan opinnäytetyön toteutusta ja saatuja tuloksia.

2 Tietoturvan osa-alueet

Tietoturvakäytänteet perustuvat CIA-menetelmään (confidenciality, integrity, availability) eli tiedon ja sisällön luottamuksellisuuteen, eheyteen sekä käytettävyyteen. Nämä kolme ovat tietoturvallisuuden peruspilarit. (Bogue. C)

Luottamuksellisuus on ensimmäinen ja tärkein tietoturvan peruspilari. Se edellyttää tietojen luokittelua koko organisaation tasolla niin, että kaikki yrityksen työntekijät tietävät luokittelusta ja sitoutuvat noudattamaan sen käytäntöjä. Yleisesti käytetty tapa luokitella tiedon luottamuksellisuutta on luottamuksellinen, salainen ja erittäin salainen tieto. Myös valtionhallinnossa käytetään tätä luokitusta. (Järvinen. P. 2002; Hakala ym. 2006.)

Luottamuksellisuus tarkoittaa sitä, että luottamukselliset tiedot ovat vain niiden henkilöiden käytössä ja saatavilla, joilla oikeus tietoihin. Jos esimerkiksi salaiseksi tai luottamukselliseksi luokiteltu tieto joutuu sellaisen henkilön käsiin, jolla siihen ei ole oikeutta, tiedon luottamuksellisuus on menetetty. (Hakala ym. 2006; Järvinen. P 2002.)

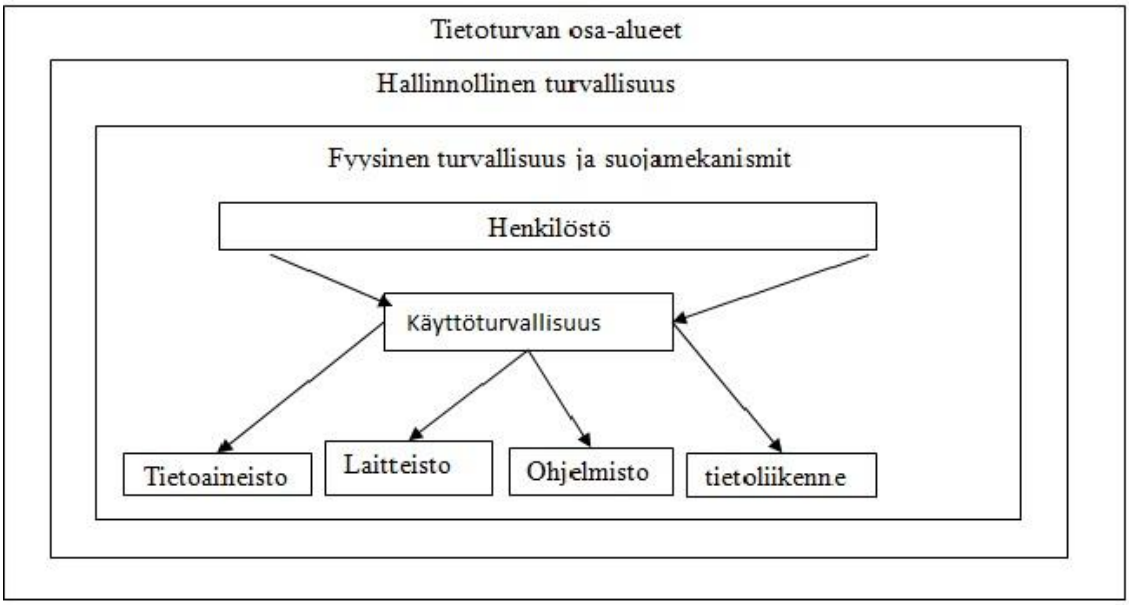
Eheydellä tarkoitetaan tiedon yhtäpitävyyttä alkuperäisen tiedon kanssa. Tieto ei saa muuttua tahattomasti tai tietoturvahyökkäyksessä. Jos näin kuitenkin käy, tiedon muuttuminen tulisi havaita. Eheys voidaan myös määritellä tietojen loogisuudeksi (sisäinen eheys) ja paikkansapitävyydeksi (ulkoinen eheys). Tietoturvan yhteydessä eheydellä tarkoitetaan tiedon oikeellisuutta siinä mielessä, että viestittyä tai talletettua tietoa ei ole muutettu jälkeenpäin muulta kuin tiedon luojan taholta. (Hakala ym. 2006.)

Käytettävyyttä kutsutaan myös tiedon saatavuudeksi. Tiedon saatavuuden tulee olla nopeaa sekä helppoa. Se on ominaisuus, joka ilmentää sitä, kuinka varmasti järjestelmä, laite, ohjelma tai palvelu on sitä tarvittaessa käyttäjien käytettävissä. Käytettävyys tarkoittaa tietoturvan yhteydessä myös sitä, että tieto on siihen oikeutettujen hyödynnettävissä haluttuna aikana. Tietoturvajärjestelyillä pyritään varmistamaan tiedon luottamuksellisuus, eheys ja käytettävyys. (ISO/IEC 17799 2000; ISO/IEC 27001 2005.)

Tietoturvakäytänteissä laaditaan selkeät ohjeet ja menettelyt oikeaoppiselle tietojenkäsittelylle, jota noudatetaan jokaisen työntekijän toimesta. Yrityksen johto vastaa viimekädessä yrityksen turvallisuudesta. Yrityksen tietoturvakäytännöistä tiedotetaan yrityk-

sen sisällä ja tehdään tarvittavat dokumentit, jotka ovat kaikkien yrityksen työntekijöiden saatavilla, sekä velvoitetaan jokainen työntekijä tutustumaan niihin.

Yrityksen tietoturvallisuuden hallintaa voidaan havainnollistaa esimerkiksi kuviossa 1 esitetyllä perinteisellä tavalla, jossa tietoturva koostuu kahdeksasta erillisestä osiosta. Ensimmäisen ja toisen osion hallinnolliset toimenpiteet ja fyysiset suojamekanismit luovat perustan muille osa-alueille. Henkilöstö on puolestaan vastuussa laitteistojen, ohjelmistojen ja tietoliikenneverkkojen turvallisesta käytöstä, joten henkilöstön osaaminen ja turvallisuus ovat olennaisia organisaation tai yrityksen tietoturvakokonaisuudessa. Yhdessä nämä kaikki kahdeksan osa-aluetta muodostavat tietoturvan perustan. Tätä perinteistä jaottelua käytetään paljon alan oppikirjoissa ja erityisesti suomenkielisissä teoksissa.



Kuva 1. Yrityksen tietoturvallisuuden jaottelu perinteisellä tavalla.

2.1 Tietoturva liiketoiminnan näkökulmasta

Perinteisen tietoturvan osatekijöiden jaottelun lisäksi käytössä on muitakin jaotteluita. Yksi lähestymistapa tietoturvan rakentamisen käytäntöihin on nähdä ne yrityksen liiketoimintaprosessien kautta. Information Security Forumin (ISF) julkaisemassa teoksessa The Standard of Good Practice for Information Security 2007 (SOGP2007) käsitellään tietoturvan parhaita käytäntöjä kuudessa liiketoiminnan kannalta tärkeässä osiossa.

ISF:n määrittelyssä yrityksen tietoverkot ja laitteistot luovat pohjan muille tietoturvan osa-alueille. Kun verkkojen ja laitteiden tietoturva on hallinnassa, voidaan keskittyä liiketoiminnan kannalta olennaisten järjestelmien turvaamiseen. Tietoaineistoturvallisuuden osa-alueen tärkeimpiä asioita ovat yleiset tietojärjestelmät sekä liiketoiminnassa tarvittavat ohjelmistot. Loput kolme osiota käsittelevät tietoturvan hallintaa sekä sovelluskehityksen ja työntekijöiden IT- käyttöympäristöjen turvallisuutta. Jotta yritysjohto saisi parhaan mahdollisen käsityksen tietoturvan laajuudesta, kannattaa heidän tutustua sekä perinteiseen että ISF:n tekemään jaotteluun (ISF 2007, 3.)

Taulukko 1. Tietoturvan hyvien käytäntöjen standardin osa-alueet kirjattuina (SOGP 2007 pohjalta).

Osa-alueet	Toimenpiteet	Seuraukset
tietoturvan johtaminen	johdon ohjeet ja järjestelyt	tietoturvalle turvallisen ympäristön luominen
liiketoimintasovellukset	vaatimukset liiketoiminta-sovellusten tietoturvalle	tietoturvaongelmien identifiointi ja ohjeet tietoturvan pitämiseksi hyväksyttävällä tasolla
laitteet ja ohjelmistot	tietokoneiden ja laitteiden konfigurointiohjeet	ylläpitotoiminnan ja sen johtamisen käytännöt
verkot	verkkojen ja laitteiden ylläpidon ohjeet	ylläpitotoiminnan ja sen johtamisen käytännöt
systeemien ja sovellusten kehittäminen	kehitystyöhön liittyvät tietoturvaohjeet	kehittämistyön ja sen johtamisen käytännöt
käyttöympäristöt	ohjeet mobiilisysteemien tietoturvalle	tietoturvan varmentamisen sovellukset ja johtaminen

2.2 Tietoaineistoturvallisuus

Tietoaineistonturvallisuudella tarkoitetaan tietojen eli tiedostojen suojaamista tietojärjestelmässä. Joskus ajatellaan, että tietoturva kostuu vain tästä. Tietoaineistoturvallisuus käsittää asiakirjojen, tiedostojen ja muiden tietoaineistojen käytettävyyden, eheyden ja luottamuksellisuuden ylläpitämisen. Keinoina voidaan käyttää tietoaineistojen luettelointia ja luokitusta sekä tietovälineiden ohjeistettua hallintaa, käsittelyä, säilytystä ja hävittämistä. Tietojen suojaaminen on tämän osa-alueen tärkein päämäärä. Tietoaineistoturvallisuus alkaa tietoaineiston synnystä ja loppuu aineiston tuhoamiseen. (valtiovarainministeriö 2009; Ruohonen 2002.)

Tietoturvallisuuteen liittyviä muita toimenpiteitä ovat käyttöoikeuksien määrittäminen, tiedostojen varmuuskopiointi, tiedostojen palautus, turvallinen säilyttäminen sekä tiedostojen tuhoaminen. Toimet liittyvät vahvasti sähköiseen materiaaliin, mutta ne pätevät myös paperisten dokumenttien käsittelyssä. (Laakso 2010.)

Tietojen tuhoutuminen tai katoaminen johtuu monesti käyttäjän omasta virheestä tai huolimattomuudesta. Käsittely-ympäristössä voi tapahtua ennalta arvaamattomia tilanteita, joihin henkilön täytyy osata varautua. Varmuuskopio on ainut keino välttää tiedostojen lopullinen tuhoutuminen. (Paavilainen, 1998.)

Tietoturvan pahin vihollinen on usko siihen, että kaikki on kunnossa, kun teknologiaa on riittävästi. Näin asia ei kuitenkaan ole. Tietoturvan suurin voimavara ja samalla heikoin lenkki on ihminen. Tietoturvaa ei saa ajatella tuotteena vaan prosessina, jota kehitetään jatkuvasti. (Rosendahl 2003.)

2.3 Ohjelmistoturvallisuus

Ohjelmistoturvallisuus kattaa tietojärjestelmissä käytettävien lisenssien ja ohjelmistojen hallinnan. Ohjelmistoturvallisuuteen lasketaan mukaan niin työpöytä- kuin palvelinkäytössäkin olevat ohjelmistot. Lisenssien hallinta ei kuulosta tärkeältä toimenpiteeltä tietoturvallisuuden kannalta, mutta hallinnan laiminlyönti voi johtaa vakaviin tietoturvaloukkauksiin. Esimerkiksi virustorjuntaohjelmiston lisenssin käyttöoikeuden loppuminen voi lopettaa samalla ohjelman toimimisen. Asianmukaisella ohjelmistohallinnalla ja -seurannalla voidaan tällaisilta ongelmilta välttyä. (Laakso 2010.)

Yrityksen ohjelmistoihin liittyvät asiat kannattaa kirjata tietoturvaperiaatteisiin ja käytäntöihin. Varmuuskopiointikäytäntöjen ja tietoturvallisten toimintatapojen ohjeistamiseen kannattaa käyttää aikaa. Henkilöstön on tiedettävä, mitä ohjelmistoja heillä on lupa käyttää työkoneillaan. Ohjelmistoturvallisuus käsittää myös ohjelmien varmuuskopioinnin ja ohjelmistojen toimittajien kanssa tehdyt riittävän kattavat tukisopimukset. (Laakso 2010.)

Ohjelmistoissa olevat virheet saattavat aiheuttaa tiedostojen katoamista tai muuttumista. Ohjelmistovirheet voivat myös mahdollistaa ulkopuolisten henkilöiden tai sovellusten pää-

syn tietoon. Tähän liittyviä riskejä voidaan vähentää tai poistaa kokonaan päivittämällä ohjelmisto säännöllisesti tai vaihtamalla ohjelmisto toiseen ohjelmistoon. (Laine 2010.)

Turvallisuuteen voidaan organisaatiossa vaikuttaa määrittelemällä ohjelmistot sallituiksi tai kielletyiksi. Voidaan lähes varmuudella sanoa, että ohjelmaa ilman turvallisuusaukkoja ei ole olemassa. Kyse on vain siitä, milloin ne löydetään. (Rosendahl 2003.)

2.4 Tietoliikenneturvallisuus

Tietoliikenneturvallisuus käsittelee yrityksen sisäisessä ja ulkoisessa verkossa tapahtuvaa liikennettä sekä verkkoliikenteen suojaamista. Tietoliikenneturvallisuutta voidaan parantaa monella tapaa. Yleisin tapa suojautua on eristää tietojärjestelmän verkko muista verkoista. Tämä voidaan tehdä esimerkiksi käyttämällä VPN-yhteyttä, joka suojaa tietojärjestelmän sen ulkopuolelta tulevalta liikenteeltä. Liikennettä voidaan suojata myös palomuurilla. Muista fyysisistä ja teknisistä suojauskeinoista löytyy paljon ohjeistusta kirjoista sekä Internetistä. (Ruohonen 2002.)

Suojaamismenetelmät kannattaa dokumentoida tietoturvaperiaatteisiin ja -käytäntöihin, varsinkin jos verkko on monimutkainen. Kokonaisvaltainen verkon ja laitteiden dokumentointi auttaa yrityksen ylläpitoa sekä helpottaa vikatilanteiden selvittelyssä. Yritysjohdossa kannattaa nimetä tietoliikenneturvallisuudesta vastaavat henkilöt ja osoittaa heille käytettävissä olevat resurssit. (Ruohonen 2002.)

Jos yrityksellä ei vielä ole kokemusta tai ohjeistusta tietoliikenteen suojaamisesta, kannattaa sitä hankkia. Nykyaikaisissa yrityksissä käytetään erityyppisiä verkkoja, joten yrityksen on hallittava niiden turvallinen käyttö. Yrityksen oman Internet-yhteyden lisäksi esimerkiksi älypuhelimet ja muut vastaavat laitteet mahdollistavat tietoliikenteen liikuttamisen. Myös näiden laitteiden tietoturva on yhtä tärkeää kuin tietokoneiden. (Laakso 2011.)

2.5 Fyysinen turvallisuus

Yrityksen laitteistojen sekä toimitilojen suojaamista kutsutaan yleisesti fyysiseksi turvallisuudeksi. Fyysinen turvallisuus on iso osa yrityksen tietoturvaa, mutta sen ei välttämättä ajatella kuuluvan tietoturvaan. Koneen suojaaminen hakkereita tai viruksilta on turhaa, jos ulkopuoliset pääsevät käyttämään yrityksen konetta tai varastamaan sen. Hakkeri, joka saa koneen haltuunsa tai pääsee fyysisesti sen luokse, pääsee ennemmin tai myöhemmin käsiksi koneella oleviin tiedostoihin, jos konetta ei ole suojattu. (Ruohonen 2002.)

Yrityksen fyysiset uhat, joihin ei voi ennalta varautua, ovat palo-, vesi- tai sähkövahingot. Nämä saattavat tuhota tietokoneita tai varmuuskopioita, joten laitteiden suojaaminen on tärkeä osa kokonaisvaltaista tietoturvan hallintaa. Yrityksen tulee ottaa huomioon myös inhimilliset vahingot, kuten ilkivalta tai laitevarkaudet. Tietoja sisältävän palvelimen eheyttä, luottamuksellisuutta ja saatavuutta ei voida varmistaa, mikäli palvelinta ei ole fyysisesti suojattu. Palvelinhuoneen turvan tasoon vaikuttaa myös ympäröivien alueiden turvallisuus. (Ruohonen 2002; Laakso 2010.)

Sen jälkeen kun työntekijöiden toimintaympäristö on saatu suojattua, voidaan keskittyä muuhun tietoturvan suunnitteluun ja kehittämiseen. Karkea arvio fyysisen tietoturvan tarpeesta yrityksessä määräytyy henkilöstön määrän ja toimitilan koon perusteella. Jos liiketoiminta vaatii useiden laitteiden hallintaa, fyysiseen turvallisuuteen on panostettava entistä enemmän. Suojaustoimet voidaan kohdentaa vain toimitilan tiettyyn alueeseen, mutta kokonaisvaltainen suojaaminen on suositeltavaa. Vastaavasti yritys, joka on vähemmän riippuvainen tietotekniikasta, keskittää suojauksen muualle. (Ruohonen 2002; Laakso 2010.)

2.6 Laitteistoturvallisuus

Laitteistoturvallisuus koostuu tietoliikenne- ja tietojenkäsittelylaitteiden kokoonpanoon, kunnossapitoon ja laadunvarmistukseen liittyvistä turvallisuusnäkökohdista. Laitteistoturvallisuudella tarkoitetaan tietojärjestelmän laitteiden suojaamista. (Paavilainen 1998)

Kaikkien yrityksen teknisten laitteiden suojaamista kutsutaan yhteisellä nimellä laitteistoturvallisuudeksi. Erityisesti tietoturvan näkökulmasta tärkeitä kohteita ovat esimerkik-

si kannettavat tietokoneet, palvelimet, tulostimet ja matkapuhelimet. Suojamekanismien käyttöönoton jälkeen kannattaa ne kirjata erilliseen asiakirjaan. Moni ei välttämättä tiedä, että esimerkiksi hajonneen tietokoneen kovalevyjen sisältö saattaa olla luettavissa, vaikka kone itsessään ei olisi toimiva. (Laakso 2010.)

Laitteistoturvallisuudella tarkoitetaan laitteistojen suojausta, asennusta, ylläpitoa ja poistoa sekä niihin liittyvää hallinnointia, jossa määritellään laitteiden omistaja ja turvaluokka sekä laitteiden valvonta ja niiden kapasiteettien suunnittelu. Ylipäätään laitteistoturvallisuudella turvataan laitteiston elinkaarta, johon kuuluvat asennuksen, takuun ja ylläpidon lisäksi erilaiset tukipalvelut ja -sopimukset sekä laitteiston turvallinen poisto elinkaaren lopussa. (Valtiovarainministeriö 2009.)

Laitteiston elinkaareen liittyvien palvelusopimuksien, palvelun tasoa määrittelevien rajojen ja vasteaikojen sopimisella voi olla merkittäviä vaikutuksia tietoturvatason ylläpidettävyyteen ja tietoturvapoikkeamiin reagointiin. Palvelusopimusten vasteaikoihin tukeutumalla voidaan vähentää varastoitavaa varalaitteistoa, mutta toisaalta riippuvuus toimittajan kyvystä toimia vasteaikojen sisällä kasvaa. Erityisen tärkeää on määritellä sopimuksilla tilanteet, joissa koko palvelu sijaitsee palvelun tarjoajalla tai osa organisaation laitteista sijaitsee siellä. Tällöin joudutaan kiinnittämään huomiota yksittäisen laitteen fyysisen turvallisuuden järjestämiseen toisen osapuolen tiloissa ja tilojen pääsynhallintaan poikkeamatilanteissa. Näissä tapauksissa palvelusopimukset ulotetaan koko järjestelmään ja vaaditaan riittävän tarkat selvitykset verkkoyhteyksistä ja fyysisestä pääsystä järjestelmään työajan ulkopuolella, mikäli palvelun täytyy olla jatkuvasti asiakkaiden käytettävissä. (Valtiovarainministeriö 2009.)

Laitteiston ylläpidossa huolehditaan, että kaikki tiedostot voidaan milloin tahansa palauttaa, kun toivutaan poikkeamasta. Tämä tarkoittaa, että laitteiston käyttöjärjestelmistä, ohjelmistoista ja niiden asetuksista on olemassa varmuuskopiot. Samaa edellytetään tietenkin niiden sisältämästä operatiivisesta tiedosta. (valtiovarainministeriö 2009)

Kaikkia järjestelmän laitteita on kyettävä jatkuvasti valvomaan ohjelmien avulla ja niiden käyttöasteiden kehittymistä seuraamaan säännöllisesti. Järjestelmien tietoturvapäivityksiä varten tarvitaan selkeät ohjeet ja ne testataan ennen tuotantojärjestelmän asennusta. Päivitysten peruminen tulee olla mahdollista, mikäli päivityksessä havaitaan ongelmia. (Valtiovarainministeriö 2009.)

2.7 Henkilöstöturvallisuus

Henkilöstöturvallisuus on henkilöstöön liittyvien tietoturvariskien hallintaa. Niitä voidaan hallita mm. toimenkuvien, käyttöoikeuksien ja koulutuksen avulla. Henkilöstöturvallisuuteen kuuluvat sekä oman henkilöstön sekä vierailijoiden tarkkailu ja valvonta. Henkilöstöturvallisuus on erittäin tärkeä osa yrityksen turvallisuutta. Yrityksen henkilöstö on voimavara, mutta se on myös yrityksen suurin tietoturvariski. (Paavilainen 1998.)

Vuonna 1995 tehdyn tutkimuksen mukaan (tiedot perustuvat Janne Huovisen ja Petri Laineen tekemään tutkimukseen 635 tietoturvatapauksesta) kaikista ihmisten aiheuttamista tietoturvatapauksista oman henkilöstön aiheuttamia oli 57,7 %. Vahingossa joko oman tai ulkopuolisen henkilöstön aiheuttamia oli 72,8 %. (Paavilainen 1998)

Pk- tietoturvatutkimuksen (2007) mukaan pk- yritykset keskittyvät suojaamaan IT- järjestelmiä pääasiassa teknisin keinoin, vaikka yritys kokee merkittävimpänä tietoturvaa uhkaavana yrityksen työntekijän. Tutkimus osoittaa, että 59 % vastaajista koki työntekijän huolimattomuuden ja tietämättömyyden tietoturvasta tietoturvariskiksi. Tutkimuksessa kävi ilmi myös, että tietoturvatasoa heikentävät merkittävästi käyttäjien tietotaso (27 %), rajallinen budjetti (14 %), IT- yksikön ajanpuute (13 %), sekä se, ettei yritysjohto ymmärrä tietoturvan tärkeyttä (9 %). (Tietotekniikan liitto Ry 2007.)

Ihmisen käyttäytyminen ja toimiminen eri prosesseissa vaikuttavat merkittävästi tietoturvallisuuden tasoon. Tämä johtaa siihen, että yrityksen työntekijöiden on tiedettävä, miten toimia eri tilanteissa, kuten esimerkiksi avatessaan epäilyttäviä tiedostoja. Henkilöstöturvallisuuteen kuuluvilla toimenpiteillä pyritään estämään työntekijöistä ja sidosryhmistä johtuvat tietoturvariskit. Esimerkiksi uuden henkilön tai yhteistyökumppanin palkkaaminen ja vanhojen työntekijöiden eroaminen ovat hetkiä, jotka mittaavat yrityksen tietoturvakäyttäytymisen tasoa. (Paavilainen 1998.)

Internetin uutispalstoilla on viikoittain luettavissa erilaisia tietoturvauutisia. Aiheet vaihtelevat haittaohjelmista tietomurtotapauksiin. Yrityksiin kohdistuvissa tietoturvahyökkäyksissä yhteistä on lähes aina ihmisen rooli. Nykyaikaiset tietokoneiden käyttöjärjestelmät ovat niin kehittyneitä, että rikollinen harvoin pääsee koneille suoraan. Yrityksen henkilöstön tietoturvattomat työskentelytavat helpottavat rikollisten toimintaa.

Parhaatkaan palomuurit tai suojaohjelmat eivät aina pysty pysäyttämään ihmisen tekemää tahallista tai tahatonta virhettä. (Paavilainen 1998.)

Inhimillisten virheiden avulla rikolliset pystyvät tuottamaan yritykselle liiketaloudellisia ongelmia. Mikäli yritysjohdon työntekijä aukaisee haittaohjelmalla varustetun sähköpostin liitetiedoston, voi rikollinen taho saada huomattavan suuret käyttöoikeudet tietojärjestelmään ja sitä kautta esimerkiksi liikesalaisuuksiin. Henkilöstöturvallisuuden tärkeyttä ei yrityksissä kannata unohtaa. Siksi on tärkeää saada henkilöstö ymmärtämään tietoturvallisuuden merkitys omalle yritykselle. (Laakso 2010.)

2.8 Käyttöturvallisuus

Käyttöturvallisuus liittyy suoraan henkilöstöturvallisuuteen, sillä järjestelmää ohjeiden vastaisesti tai huolimattomasti käyttävät käyttäjät heikentävät käyttöturvallisuutta. Käyttöturvallisuus tarkoittaa yleisesti sitä, että tietojärjestelmää käytetään turvallisesti ja hallitusti. (Ruohonen 2002.)

Yleensä käyttöturvallisuus hoidetaan paremmin suurissa yrityksissä kun pienissä. Käyttöturvallisuuden ylläpitäminen on pienissä yrityksissä vaikeaa siksi, että se tehdään työntekijävoimin. Pienissä yrityksissä yleensä ei ole resursseja tehdä kaikkia tarvittavia toimenpiteitä turvallisuuden ylläpitämiksesi. (Paavilainen 1998.)

Yrityksen päivittäisten toimintojen ja rutiinien turvaamista kutsutaan yleisesti käyttöturvallisuudeksi. Tämä osa-alue sisältää kaikki manuaalisen ja automaattisen tietojenkäsittelyn suojatoimenpiteet, kuten salasanojen hallinnoinnin ja järjestelmien valvonnan. Käyttöturvallisuuden luonteen vuoksi sitä pidetään joskus ylimääräisenä kahdeksantena tietoturvan osa-alueena. Yrityksen päätettäväksi jää, halutaanko esimerkiksi salasanakäytännöt dokumentoida useampaan kertaan. Salasanakäytännöt voidaan kirjata sekä ohjelmisto- että käyttöturvallisuuteen tai vaihtoehtoisesti vain toiseen osa-alueeseen. (Laakso 2010.)

2.9 Hallinnollinen turvallisuus

Hallinnollinen turvallisuus kostuu toimenpiteistä, joissa määritellään turvallisuutta parantavat toimenpiteet ja päätetään tietoturvatoiminnan suuntaviivat. Tämä vuoksi hallinnollinen tietoturva on koko tietoturvan lähtökohta. Ilman suunnittelua ja tietoturvan hallinnointia turvajärjestelyt voivat sisältää suuria puutteita tai ne voi olla väärin suunniteltu. Hallinnollisen tietoturvan tehtävänä on määritellä, kuka vastaa turvallisuus- toipumis- ja valmiussuunnittelusta. Näistä laaditaan ohjeet koko yrityksen henkilökunnan nähtäväksi. (Paavilainen 1998.)

Yrityksen tietoturvalliset toimintatavat tarvitsevat johtamista ja kehittämistä, kuten muutkin yleiset liiketoiminnan prosessit. Hallinnollinen tietoturva sisältää menettelytavat muiden tietoturvan osa-alueiden ohjaamiseen. Tavoitteena on varmistaa, että kaikki eri osa-alueet ovat tarpeeksi hyvällä tasolla. Hallinnollisen tietoturvan näkyvimpiä tuotoksia ovat henkilöstön organisointi, yleiset linjaukset sekä erilaiset dokumentit, kuten tietoturvapolitiikka. Esimerkiksi yritysjohdon osallistuminen ja vastuualueiden jakaminen ovat tärkeitä tietoturvan hallinnan kannalta. (Paavilainen 1998.)

Tietoturvan johtamista pidetään erittäin laajana käsitteenä. Yrityksen ei silti välttämättä tarvitse tehdä muuta kuin varmistaa, että yleiset toimintatavat ovat lainsäädännöllisesti oikein. Esimerkkinä tästä voidaan pitää henkilötietojen käsittelyä. Laajempi johtaminen on kuitenkin suotavampaa, jotta yritys pystyy varautumaan mahdollisiin riskeihin ja ongelmatapauksiin. Erilaisten suunnitelmien laatiminen auttaa selviämään esimerkiksi poikkeustilanteista. Tärkeintä on kuitenkin sisällyttää tietoturvalliset toimintatavat päivittäisiin prosesseihin. Näin varmistetaan se, että tietoturva huomioidaan joka päivä sekä työntekijöiden että yritysjohdon tasolla. (Laakso 2010.)

3 Pk-yrityksen tietoturvan vaatimukset

Tässä luvussa kerrotaan muutamista tilanteista, joita pk-yrityksen tietoturvaa suunniteltaessa tulisi ottaa huomioon. Kerron myös lainsäädännön vaikutuksista ja siitä, mitä haasteita lainsäädäntö asettaa yrityksen tietoturvansuunnittelulle. Kaksi tietoturvan osa-aluetta, joihin tässä luvussa kiinnitetään huomiota, ovat standardit ja sertifiointi. Luvus-

sa selostetaan, miten yritys voi saada sertifikaatin, mistä löytyy lisätietoa sertifioinnista sekä mitä hyötyä siitä on yritykselle. (Laakso 2010.)

3.1 Lainsäädännön vaikutukset

Yrityksen tietoturvaa suunniteltaessa, toteuttaessa ja kehittäessä on otettava huomioon laissa määriteltyjä asioita. Vaatimusten määrään vaikuttavat toimiala ja liiketoiminnan luonne, joten yrityksen on ensin selvitettävä omaa toimintaansa ohjaavat säädökset. (Jordan 2006.)

Organisaation toiminta on jaettu kolmeen eri kategoriaan, jotka liittyvät palveluihin, infrastruktuuriin ja henkilöstöön. Lakien jako kategorioihin tuo käsittelyyn selkeyttä. Selviä päällekkäisyyksiä on huomattavissa eri kategorioiden välillä. Oleellisia työntekijöiden omaan tietoturvaan vaikuttavia lakeja ovat henkilötietolaki sekä laki yksityisyyden suojasta työelämässä. Vastaavasti infrastruktuuri-osioon sisällytetty sähköisen viestinnän tietosuojalaki määrittelee, miten yrityksellä on oikeus käsitellä henkilöstön luottamuksellisia tietoja esimerkiksi IT- järjestelmissä. (Laakso 2010.)

Säädökset on jaettu useisiin lakeihin, mikä osaltaan hankaloittaa asian hallintaa yrityksen näkökulmasta. Siitä huolimatta Suomeen ei vielä ole säädetty erillistä tietoturvalakia. Uusien lakien sijasta yritykset haluavat viranomaisilta enemmän ohjeistusta tietoturvan suojamekanismien, valvonnan ja vaatimusten lainmukaiseen toteuttamiseen. (Laakso 2011.)

Lainsäädäntö asettaa omat haasteensa tietoturvallisuuden toteuttamiselle. Suomessa on lakeja, jotka on säädetty EU:n tasolla, sekä sellaisia lakeja, jotka ovat voimassa vain kansallisella tasolla. EU:ssa on säädetty myös useita välittömästi ja välillisesti tietoturvaa koskevia direktiivejä, jotka on integroitu osaksi Suomen lainsäädäntöä. (Jordan 2006.)

Suomessa ei ole varsinaisesti olemassa yhtään erillistä lakipykälää, joka koskisi pelkkää tietoturvaa. Säädökset ovat yleensä osa jotakin muuta olemassa olevaa lakipykälää, joka sisältää tietoturvasäädöksiä. Ne voivat olla esimerkiksi osana henkilötietolakia tai sähköisen liiketoiminnan tietosuojalakia. Laki kansainvälisestä tietoturvallisuudesta koskee vain murto-osaa suomalaisista yrityksistä sekä valtion toimia tietoturvallisuuden ylläpi-

tämiseksi. Yrityksiltä vaaditaan tietoista tietoturvakulttuuria, jotta lakipykälien noudattaminen onnistuu. (Jordan 2006.)

3.2 Standardit ja sertifiointi

Tietoturvallisuuden kehittämiseksi ja hallinnoinnin avuksi on kehitetty suuri joukko erilaisia standardeja, viitekehyksiä ja toimintamalleja. Tietoturvallisuuteen liittyy myös usein sertifikaatteja, jotka helpottavat tavaran kuljettamista maasta toiseen. Yleensä yhteistyöyritys joutuu sopimusten kautta hankkimaan kyseisen standardin tai ainakin noudattamaan kyseisen yrityksen standardin edellyttämää tasoa. (Jordan 2006.)

Yritys voi halutessaan hakea todistusta tietoturvallisista toimintatavoistaan. Tätä toimenpidettä kutsutaan tietoturvallisuuden hallintajärjestelmän sertifioinniksi. International Organization for Standardization (ISO) on kansainvälinen organisaatio, joka on määritellyt sertifioinnissa vaadittavat kriteerit. (Laakso 2010.)

Kyseiset vaatimukset on kuvattu ISO/IEC 27001 -standardissa. Viimeistään sertifiointivaiheessa yritykseltä vaaditaan laajaa dokumentaatiota tietoturvan hallintajärjestelmästä. Virallisten ISO-standardien hankkiminen on maksullista mutta silti kannattavaa. Internetistä on saatavilla myös hyviä ilmaisia teoksia, kuten ISF:n laatima The Standard of Good Practise for Information Security 2007. Suomen kielellä laadukasta materiaalia tarjoaa esimerkiksi Valtiohallinnon VAHTI -työryhmä. Se on julkaissut vapaasti luettavaksi lukuisia tietoturvallisuuteen liittyviä ohjeistuksia ja suosituksia. (Laakso 2010.)

Mikäli yritys haluaa kattavan tietoturvadokumentin, voidaan se luoda esimerkiksi kirjaamalla ISO:n ja ISF:n standardien pääkohdat yrityksen tietoturvaperiaatteisiin ja -käytäntöihin. Vaikka virallinen sertifikaatti ei olisikaan tavoitteena, kannattaa yrityksen silti tutustua mahdollisimman moneen aiheeseen liittyvään dokumenttiin ja ohjeistukseen. Pelkästään yhteen tietoturvadokumenttiin tutustuminen ei ole välttämättä järkevää. Tarpeeksi kattavan informaation saa vasta, kun tutustuu useampaan aiheeseen liittyvään tuotokseen. (Laakso 2010.)

Ongelmana on se, että sertifiointi on kallista ja vaatii todella tarkan seurannan sekä resursseja sen toteuttamiseen. Sertifioinnilla maalisella on tarkat kriteerit. Sertifikaatit

jaetaan yleensä seuraavasti: palvelu-, tuote-, järjestelmä- sekä henkilöstösertifikaatti. Tietoturvallisuuden sertifiointi tarkoittaa käytännössä tietoturvallisuus- järjestelmän sertifiointia. Sertifioinnin voi suorittaa vain taho, joka on saanut pätevyyden sen hoitamiseen. Tämä on kansainvälisiin kriteereihin perustuva menettelytapa. (Jordan 2006.)

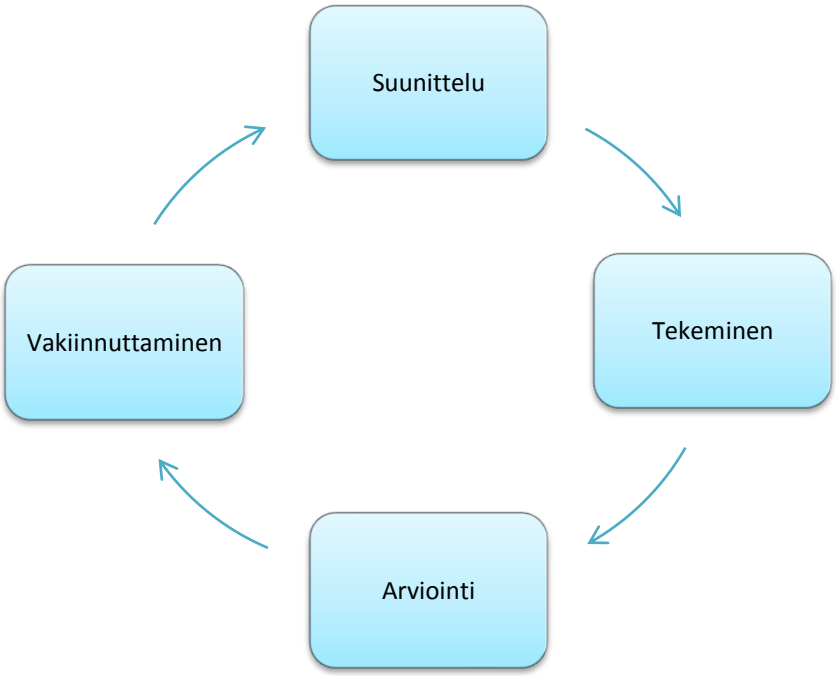
4 Pk-yrityksen tietoturvasuunnitelma

Tietoturva koostuu useasta eri osa-alueesta, ja tietoturvallisuuden tutkimiseen on kehitetty useita eri välineitä ja tapoja. Maassamme on useita eri yrityksiä, jotka tekevät tietoturvakartoituksia. Yleensä jokaisella yrityksellä on omat kyselynsä, joiden avulla kartoitus tehdään. Tietoturvakartoituksen teettäminen ulkoisella taholla tuottaa yritykselle lisäkustannuksia sekä luo vaaratekijän tietoturvallisuudelle. (Shared Assessments 2011.)

Kartoituksen avulla selvitytetään, millainen yrityksen tietoturvatilanne on sillä hetkellä. Kartoitus antaa tietoa siitä, mitä muutoksia tietoturvan parantamiseksi voidaan tehdä ja miten. Teemahaastattelu on 1 menettely tapa, jota voidaan käyttää kartoituksen apuna. Teemahaastattelu on puolistrukturoitu haastattelumenetelmä. Puolistrukturoidulle haastattelulle on ominaista, että jokin haastattelun näkökohta on lyöty lukkoon, mutta ei kuitenkaan kaikkia. Teemahaastattelussa haastattelu kohdennetaan tiettyihin aihepiireihin. (Hirsjärvi & Hurme 2010, 46-48.)

Haastattelu suunnataan siis tutkittavien henkilöiden subjektiivisiin kokemuksiin. Teemahaastattelulla voidaan tutkia yksilön ajatuksia, tuntemuksia, kokemuksia ja myös sanatonta kokemustietoa. Siinä korostuu haastateltavien oma elämysmaailma. Teemahaastattelu tuo tutkittavien äänen kuuluviin (Hirsjärvi & Hurme 2010, 46-48.)

kuva 2 on esitetty mallia PDCA- ongelmanratkaisumenetelmästä, jota käytetään yleisesti laadun parantamisen menetelmänä, mutta sitä voidaan myös soveltaa tietoturvasuunnitelman laadinnassa. PDCA- malli on pohja koko toimeksiantajan tieturvasuunnitelmaprosessille. (Laatuakatemia 2010.)



Kuva 2. PDCA- malli (ISO/IEC 27001:2005).

Suunnitteluvaiheessa kartoitetaan riskit, tehdään riskianalyysi sekä luodaan suunnitelma dokumentiksi. Toteutusvaiheessa suunnitelma laitetaan käytäntöön. Toteutusvaiheet voidaan jakaa osiin, mikä helpottaa suunnitelman tekoa. Arviointivaiheessa arvioidaan, onko yrityksen riskianalyysi ajan tasalla. Jos ei ole, se laitetaan ajan tasalle. Vakiinnuttaminen on sitä, että suunnitelmaa sekä yrityksen politiikkaa pidetään. (Laatuakatemia 2010.)

4.1 Nykytilanteen kartoitus

Hallinnollinen turvallisuus

Hallinnollisen tietoturvallisuuden kartoittamisen tavoitteena on selvittää, miten yrityksessä hoidetaan koko tietoturvan hallinnointi ja organisointi. Yrityksen koko tietoturva perustuu siihen, että vastuut ja tehtävät on organisoitu huolellisesti ja tietoturvan toteutumista valvotaan. Hallinnollisen tietoturvan näkyvimpiä tuotoksia ovat myös erilaiset dokumentit, kuten tietoturvapolitiikka. Hallinnollisen turvallisuuden yhteydessä selvitetään, ovatko yleiset toimintatavat lainsäädännön mukaisia. Tärkeintä tämän osa-alueen

kartoituksessa on selvittää, miten tietoturva huomioidaan päivittäisissä prosesseissa. (Paavilainen 1998.)

Tietoaineistoturvallisuus

Kartoitettaessa yrityksen tietoaineistoturvallisuutta selvitetään, miten yrityksen tietojärjestelmän tiedot ja tiedostot on suojattu. Suojauskeinoja ovat tietoaineistojen luettelointi ja luokitus sekä tietovälineiden ohjeistettu hallinta, käsittely, säilytys ja hävittäminen. Tietojen tuhoutuminen johtuu monesti käyttäjän omasta virheestä tai huolimattomuudesta. Tietoturva ei ole tuote vaan prosessi. Sen pahin vihollinen on usko siihen, että kaikki on kunnossa kun on riittävästi teknologiaa. (Valtiovarainministeriö 2009; Ruohonen 2002.)

Ohjelmistoturvallisuus

On tärkeää kartoittaa, miten yrityksessä otetaan huomioon ohjelmistoturvallisuus. Sillä tarkoitetaan tietojärjestelmissä käytettävien lisenssien ja ohjelmistojen hallintaa. Lisenssien hallinta ei kuulosta tärkeältä tietoturvallisuuden kannalta, mutta hallinnan laiminlyönti voi silti johtaa vakaviin tietoturvaloukkauksiin. (Laakso 2010.)

Käyttöturvallisuus

Käyttöturvallisuus liittyy suoraan henkilöstöturvallisuuteen, sillä järjestelmää ohjeiden vastaisesti tai huolimattomasti käyttävät käyttäjät heikentävät käyttöturvallisuutta. Käyttöturvallisuus tarkoittaa yleisesti sitä, että tietojärjestelmää käytetään turvallisesti ja hallitusti. Tämä osa-alue sisältää kaikki manuaalisen ja automaattisen tietojenkäsittelyn suojatoimenpiteet, kuten salasanojen hallinnoinnin ja järjestelmien valvonnan. (Laakso 2010.)

Tietoliikenneturvallisuus

Mikäli yrityksellä ei vielä ole kokemusta ja ohjeistusta tietoliikenteen suojaamisesta, kannattaa sellaista hankkia. Nykyaikaisissa yrityksissä käytetään erityyppisiä dataverkkoja, joten niiden turvallinen käyttö on hallittava. Vaikka omaa Internet-yhteyttä ei olisikaan, niin esimerkiksi älypuhelimet ja muut vastaavat laitteet mahdollistavat datan liikuttamisen. Näiden laitteiden tietoturva on yhtä tärkeää kuin esimerkiksi tietokoneiden. (Ruohonen 2002; Laakso 2010.)

Fyysinen turvallisuus

Fyysisen turvallisuuden ei välttämättä ajatella kuuluvan yrityksen tietoturvaan mutta se on merkittävä osa sitä. Tietojärjestelmän suojaaminen hakkereilta tai viruksilta ei auta, jos kuka tahansa pääsee käyttämään yrityksen tietojärjestelmiä ja varastamaan koneita. Hakkeri, joka pääsees fyysisesti koneen luokse, pääsee myös ennemmin tai myöhemmin lukemaan tietokoneella olevat tiedot, jos niitä ei suojata. (Ruohonen 2002.)

Laitteistoturvallisuus

Laitteistoturvallisuus kostuu tietoliikenne- ja tietojenkäsittelylaitteiden kokoonpanoon, kunnossapitoon ja laadunvarmistukseen liittyvistä turvallisuusnäkökohdista. Yrityksen laitteistoturvallisuudella tarkoitetaan laitteistojen suojausta, asennusta, ylläpitoa ja poistoa sekä niihin liittyvää hallinnointia, jossa määritellään laitteiden omistaja ja turvaluokka sekä laitteiden valvonta ja niiden kapasiteettien suunnittelu. Erityisesti tietoturvan näkökulmasta tärkeitä kohteita ovat esimerkiksi kannettavat tietokoneet, palvelimet, tulostimet ja matkapuhelimet. Moni ei välttämättä tiedä, että esimerkiksi hajonneen tietokoneen kovalevyjen sisältö saattaa olla luettavissa, vaikka kone itsessään ei olisi toimiva. (Valtiovarainministeriö 2009.)

Henkilöstöturvallisuus

Henkilöstöturvallisuus on erittäin tärkeä osa yrityksen tietoturvallisuutta. Henkilöstöturvallisuus on henkilöstöön liittyvien tietoturvariskien hallintaa. Niitä voidaan hallita mm. toimenkuvien, käyttöoikeuksien ja koulutuksen avulla. Henkilöstöturvallisuuteen kuuluvat sekä oman henkilöstön sekä vierailijoiden tarkkailu ja valvonta. (Paavilainen 1998.)

Taulukko 2. Yrityksen tietoturvakartoitusta varten laaditussa apukysymyslistassa on kuvattu tietoturvan eri osa-alueet. Kysymyksiin vastaamalla saadaan konkreettinen kuva tietoturvan puutteista. Myöhemmin tietoturvasuunnitelmaa tehdessä voidaan tätä samaa taulukkoa hyödyntää päätettäessä vastuuhenkilöistä ja parannusehdotuksista.

tietoturvan osa-alueet	**kysymyslista**	**nykytila**	**vastuuhenkilö ja parannusehdotukset**
hallinnollinen turvallisuus	• kuka vastaa turvallisuussuunnitelmasta? • kuka vastaa toipumissuunnitelmasta? • kuka vastaa valmiussuunnittelusta? • henkilöstön koulutus ja opastus • lainsäädännön noudattaminen • tietoturvapolitiikka • tietoturvan valvonta		
tietoaineistoturvallisuus	• kuka vastaa tietojen suojauksesta (käyttöoikeudet, varmuuskopiointi, palautus, tuhoaminen)? • missä ja miten asiakirjoja säilytään?		
ohjelmistoturvallisuus	• mistä ohjelmista on olemassa lisenssit? • onko olemassa ilmaisohjelmia tai piraattiohjelmia? • kuka vastaa lisenssien hoidosta? • miten lisenssipäivitykset hoidetaan? • miten tietoturvaohjelmien päivitys hoidetaan? • miten ohjelmistotuki toimii? • onko työntekijöillä oikeuksia asentaa ohjelmia?		
käyttöturvallisuus	• käyttääkö yritys kulunvalvontaa (vierailijat, omat työntekijät)? • missä dokumentteja säilytetään?		

tietoturvanosa-alueet	kysymyslista	nykytila	vastuuhenkilö ja parannusehdotukset
käyttöturvallisuus	• laitteistojen ja ohjelmistojen käyttöoikeudet • verkko rajoitukset • onko etäkäyttömahdollisuus (verkko ja ohjelmat)?		
tietoliikenneturvallisuus	• millainen on verkkoyhteys? • miten verkkoa on rajoitettu? • onko käytössä pilvipalveluja?		
fyysinen turvallisuus	• miten varaudutaan tuli - ja vesivahinkoihin? • onko käytössä UBS (varavirtalähde)? • onko suojauduttu ilkivaltaa vastaan? • miten varmuuskopioita hoidetaan? • miten vanhojen laiteiden tiedot tuhotaan? • onko tietojen hajautus käytössä?		
henkilöstöturvallisuus	• kuka vastaa tietoturvakoulutuksesta? • kuka vastaa henkilöstön valvonnasta? • onko työntekijöillä vaitiolovelvollisuutta?		
laitteistoturvallisuus	• miten fyysisistä laitteista huolehditaan? • kuka vastaa niiden hoidosta? • miten työasemien varmuuskopioni on hoidettu?		

4.2 Riskianalyysi

Riskianalyysi tulee tehdä huolella ja päivittää säännöllisesti. Riskianalyysissä kannattaa käyttää valmiita malleja ja soveltaa niitä oman yrityksen toimintaan. Toteutusmenetelmiä on monenlaisia, joten kannattaa tutkia, mikä eri vaihtoehdoista on paras ja sopivin kyseiselle yritykselle. (Pk-yrityksen riskinhallinta 2009)

Riskien tunnistaminen voidaan aloittaa jakamalla tietoturvariskien kokonaisuus ensin pienempiin osiin ja määrittelemällä näihin kohteisiin liittyvät uhkat. Toiminnalle on asetettava ennen analysoinnin aloittamista tavoitteet, joihin pyritään. Riskien tunnistaminen voidaan tehdä käyttäen kokemusperäistä tietoa ja käyden järjestelmällisesti läpi kohteet ja niihin liittyvät riskit. On välttämätöntä selvittää kaikki mahdolliset uhkat, vaikka ne olisivat epätodennäköisiä Jos riskianalyysissä ilmenee riskejä, joilla on vakavat seuraukset ja suuri todennäköisyys, niihin on puututtava välittömästi. Riskien arvioinnin yhteydessä ohitetaan sitten ne, jotka eivät ole todellisia. Tunnistaminen ei saa olla summittaista arvaamista ilman selkeää suunnitelmaa ja kirjallista raportointia, kuva 3. (Pk-yrityksen riskinhallinta 2009.)

Lähtötilanteessa tulee selvittää olemassa olevan järjestelmän turvallisuuden heikkoudet ja vahvuudet. Tutkitaan toimitilat ja haastatellaan avainhenkilöjä sekä tutustutaan yrityksen normaalikäyttöön ja rutiineihin. Käydään läpi yrityksen dokumentit sekä yrityksen tietoturvapolitiikka ja järjestelmän tarjoamat tietoturvaominaisuudet kuten sisään kirjautuminen ja käyttöoikeudet. Tällöin saadaan selville järjestelmässä olevat (tunnetut) riskit. (Pk-yrityksen riskinhallinta 2009.)

Kuva 3. Yleismalli riskien arviointiin (Miettinen 1999).

Seuraavassa vaiheessa selvitetään uudet riskitekijät, jotka voivat pohjautua ensimmäisessä vaiheessa tehtyyn työhön. Uudet uhkat voivat johtua teknologiasta, ihmisistä, luonnonilmiöistä tai ympäristöstä. Olennaista tietoriskien kartoituksessa on itse järjestelmän, käyttöympäristön ja rajapintojen tunteminen. Kartoituksessa tarvitaan myös ohjelmisto- ja laitteisto-osaamista. Ulkopuolisen konsultin käyttö voi olla tarpeen tuomaan kokemusta vastaavista selvityksistä. Samalla saadaan ulkopuolinen näkemys asiaan. On kuitenkin huomioitava tästä mahdollisesti aiheutuvat tietoturvaongelmat. (Jordan 2006.)

Joskus riskinotto voi olla tietoinen valinta sekä osa yrityksen strategista suunnistelua. On kuitenkin tärkeää tietää mitä tapahtuu, jos riskinotto epäonnistuu sillä, siitä voi seurata yritykselle suuria ongelmia. (Jordan 2006.)

4.3 Tietoturvasuunnitelma ja toteutus

Tietoturvasuunnitelma on kirjallinen suunnitelma, jolla kehitetään ja toteutetaan organisaation tietoturvaa**.** Tietoturvasuunnitelman voi tehdä monella tapaa ja sen tekemisessäkin voi olla tietoturvariskejä, jotka täytyy tiedostaa. Seuraavassa esitellään kolme vaihtoehtoa:

1. Yritys laatii itse tietoturvasuunnitelman ja toteutuksen, mikä vaatii ammattitaitoa ja yrityksen sisäisiä resursseja.

2. Yritys teettää suunnitelman ja toteutuksen ammattilaisella. Tällöin tieturvariskinä on tietovuotomahdollisuus.

3. Yritys teettää jommankumman ammattilaisella ja tekee loput itse. Tällöin on otettava huomioon yrityksen resurssit sekä ammattitaito.

Vahinkojen korjaamisen pitäisi tapahtua mahdollisimman nopeasti, jotta yrityksen toiminnalle koituisi mahdollisimman vähän vahinkoa sekä mahdollisia taloudellisia ongelmia. Joitakin riskejä voidaan ennalta ehkäistä, mutta kaikkiin ongelmiin ei voida varautua. Esimerkiksi vesivahinkoa tai tulipaloa ei voi ennakoida mutta niiden riskiä voidaan vähentää ja suunnitella korjausmenetelmät siten, että niistä koituisi mahdollisimman vähän vahinkoa. Tietoturvasuunnitelman toteutus on jatkuva prosessi. Suunnitelma tulee tarkistaa suunnitelmassa sovitun aikavälin mukaisesti. Tarvittaessa se pitää päivittää ajan tasalle, jotta siitä olisi jotain hyötyä. (Web-opas 2010.)

4.4 Seuranta ja arviointi

Tietoturvasuunnitelman seurantaa tulee tehdä jatkuvasti. Sen yhteydessä tulee arvioida, onko tarpeen päivittää tai uusia suunnitelmaa joidenkin riskien osalta, jota ei ollut vielä otettu huomioon. Seurannalla ja arvioinnilla pyrytään pitämään tietoturvasuunnitelma ajan tasalla.

Suunnitelmasta ei ole yritykselle paljon hyötyä, mikäli se ei ole ajan tasalla. Silloin työntekijät eivät tiedä, miten tietyissä tilanteissa pitäisi toimia. Mikäli suunnitelmaa ei pidetä ajan tasalla, sen tekeminen voidaan joutua aloittamaan alusta. (Web-opas 2010.)

5 Toimeksiantajayrityksen tietoturvakartoitus

Opinnäytetyöni tietoturvasuunnitelman pohjana käytettiin teemahaastattelua, jossa oli mukana toimitusjohtaja. Tietoturvasuunnitelman laatiminen lähti alun perin toimitusjohtajan omasta aloitteesta. Teemahaastattelun avulla saatiin tietoa kartoitettavan yrityksen tietoturvasta ja sen puutteista.

Kartoituksessa selvitimme toimeksiantajan kanssa yrityksen tämänhetkisen tietoturvatason sekä tietoturvaan liittyvät ongelmat. Kartoituksessa olisi voinut käyttää apuna luvussa 4 esitettyä kysymyslistamallia. Kartoituksessa kävi ilmi, että yrityksessä ei ollut juuri minkäänlaista tietoturvaa. Tietoturvapolitiikka oli olemassa, mutta se oli kirjoittamaton. Liikkuvia laitteita oli suojattu palomuurilla ja salasanoilla, mutta yrityksen kiinteitä laitteita oli suojattu vain palomuurilla. Yrityksen toimitiloja ei ollut suojattu millään tavalla. Fyysisiä uhkia, kuten palo-, vesi-, tai sähkövahinkoja, ei ollut edes otettu huomioon. Lapset saattoivat halutessaan käyttää yrityksen koneita ja pelata niillä ilman minkäänlaista valvontaa. Yrityksen toimitiloissa käyvät saattoivat nähdä yrityksen asiakirjat sekä koneella olevat tiedostot, jos tiesi mistä etsiä. Tietoturvariskeille ei ollut tehty minkäänlaista palautussuunnitelmaa.

Riskianalyysin perusteella voidaan olettaa, että todennäköisin tietoturvariski on tietovuoto, koska laitteita ei ollut suojattu salasanoilla. Tästä voi koitua vakavia seurauksia. Vakavimpia tietoturvariskejä ovat fyysiset uhat, mm. palo-, vesi- ja sähkövahingot. Niihin ei voida varautua mutta niiden aiheuttamia vahinkoja voidaan minimoida.

Tietoturvasuunnitelmaan on kirjattu mahdolliset riskit sekä niiden korjausehdotukset yrityksen johdolle. Suurimmat riskit, jotka tulivat ilmi kartoituksessa, olivat palo-, vesi-, ja sähkövahingot. Näiden lisäksi pitää puuttua laitteiden suojaamiseen ulkoisilta riskitekijöiltä, kuten tietovuodoilta. Laatimani tietoturvasuunnitelma käsittää ehdotukset, joilla analyysissä ilmi tulleet riskit voidaan minimoida. Tässä luvussa esitetään tiivistelmä suunnitelmasta, koska suunnitelma on luokiteltu salaiseksi. Suunnitelman toteutus ei enää kuulu toimeksiantoon. Voin toki antaa toimeksiantajalle neuvoja siitä, miten suunnitelma kannattaisi toteuttaa.

6 Yhteenveto

Oppinäytetyön tavoitteena oli laatia toimiva ja etenkin hyödyllinen tietoturvasuunnitelma yritykselle. Suunnitelman tekeminen oli mielenkiintoista, ja työtä tehdessä oppi koko ajan uusia tietoturvaan liittyviä asioita. toimeksiantoyrityksen tietoturvasuunnitelman laadintaan ei löytynyt sopivaa valmista mallia**,** joten sellainen jouduttiin laatimaan.

Työn tekemisen aikana ei ollut suuria ongelmia. Pienenä yllätyksenä tuli kuitenkin se, että tietoturvasuunnitelmat eivät todellakaan liity pelkästään teknisiin asioihin, vaan siinä otetaan huomioon hyvin paljon muutakin. Tietoturvasuunnitelmien yleinen laajuus vaikutti siihen, että työn rajauksen ja rakenteen kanssa meni aika paljon aikaa. Tutkimalla lähdekirjallisuutta sai kuitenkin hyvin paljon selvyyttä suunnitelmaan kuuluvista asioista.

Tavoitteeni työssä oli se, että työstä olisi kohdeyritykselle aidosti hyötyä, ja yritys tekisi ainakin osan ehdotetuista muutoksista tietoturvatoimintaansa. Toinen tavoite oli se, että tämän työn hyödyt eivät rajoittuisi pelkästään kohdeyritykseen, vaan suunnitelmaa olisi mahdollista käyttää pohjana myös muiden yritysten tietoturvasuunnitelmiin. Tässä työssä ei juurikaan perehdytty teknisten ratkaisujen tutkimiseen. Mielestäni edellisessä kappaleessa mainitut tavoitteet saavutettiin onnistuneesti.

Tämän opinnäytön tuloksena syntynyt tietoturvasuunnitelman yleismallin tärkein vaihe on tietoturvakartoitus ja riskianalyysi. Mikäli kartoitusta ei tehdä huolella, koko pk-yrityksen tietoturvan kehittämisprosessi jää puutteelliseksi. Tässä työssä esitetty kysymyslista-taulukko soveltui hyvin tämän toimeksiantoyrityksen tietoturvasuunnitelman tekemiseen.

LÄHTEET

Chris Bogue, University of Miami, Privacy / Data Protection Project 2006, http://privacy.med.miami.edu/glossary/xd_confidentiality_integrity_availability.htm 12.9.2011

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

Hirsjärvi, S.;& Hurme, H. 2010. Tutkimushaastattelu. Teemahaastattelun teoria ja käytäntö. Gaudeamus Kirja. Helsinki

ISO (International Organization for Standardization). ISO/IEC 17799 2000.

ISO (International Organization for Standardization). ISO/IEC 27001 2005.

Jordan, E. 2006. Strateginen IT- riskien hallinta. Edita

Järvinen, P. 2002. Tietoturva ja yksityisyys. Docendo. Jyväskylä.

Miettinen Juha.1999,Tietoturvallisuuden johtaminen. Kauppakaari Oyj 12.10.2011

Laatuakatemia. 2010, laatutyökaluja http://www.kotiposti.net/tuurala/PDCA.htm 4.10.2012

Laakso, M. 2010. PK-yrityksen tietoturvasuunnitelman laatiminen http://publications.theseus.fi/handle/10024/20793 4.10.2011.

Laine, A. 2010. Tietoturvakartoitus ja tietoturvan nostaminen. https://publications.theseus.fi/bitstream/handle/10024/28902/Laine_Antti.pdf?sequence=*1*. 22.11.2011.

Paavilainen, J. 1998. Tietoturva. Jyväskylä: Suomen Atk- Kustannus.

PK-RH. 2009 Pk-yrityksen riskin hallinta http://www.pk-rh.com/startti-riskienhallintaan.html

Rosendahl, M. 2003. Tietoturva palvelee kaikkia. http://www.helsinki.fi/atk/lehdet/103/Tietoturva%20palvelee%20kaikkia.html 28.11. 2011

Ruohonen, M. 2002. Tietoturva. Porvoo: Docendo.

Tietotekniikan liitto Ry. 2007. PK- tietoturvatutkimus. http://www.ttlry.fi/tutkimus/pk-tietoturvatutkimus. 1.9.2012.

Valtiorarainministeriö. 2009. VAHTI/ tietoaineistoturvallisuus. https://www.vahtiohje.fi/web/guest/tietoaineistoturvallisuus;jsessionid=5CE18186B5F8270404B416B45A53708BD26813267B2B590EF73B48E506506966551D21481CAAACC03176EF. 28.11.2011.

Web-opas.2010.web-opas, http://www.webopas.net/ 20.12.2012

Haastattelunrunko

1. Millaista tietoa yrityksen työntekijöillä on yrityksen tietoturvasta?
2. Millä tavalla tietoturva on otettu huomioon yrityksen toiminnassa?
3. Mitä tavalla työntekijöitä on koulutettu ja ohjattu huolehtimaan tietoturvasta?
4. Millä tavalla yritys on varautunut tietoturvariskeihin?
5. Onko yrityksessä olemassa palautus suunnitelmaa vahinkojen varalle?
6. Onko yrityksellä olemassa aikaisempaa tietoturvasuunnitelmaa?
7. Milla tavalla varmuuskopioita säilytetään jos niitä on olemassa?
8. Millä tavalla yritys on varmuuskopioinut tiedostot?
9. Millaisia standardeja ja sääntöjä yritys käyttää?