Haaga-Helia
ammattikorkeakoulu Oy

Ohje ulkoistamisen tietoturvasta pk-yritykselle

Teemu Laitinen

Opinnäytetyö
Tietojenkäsittelyn koulutusohjelma
2015

Haaga-Helia ammattikorkeakoulu Oy

Tiivistelmä

10.12.2015

Tekijä(t)
Teemu Laitinen

Koulutusohjelma
Tietojenkäsittelyn koulutusohjelma

Opinnäytetyön otsikko
Ohje ulkoistamisen tietoturvasta pk-yritykselle

Sivu- ja liitesivumäärä
25

Opinnäytetyön otsikko englanniksi
Guide for information security aspect of outsourcing for small companies

Tämän opinnäytetyön tarkoituksena on luoda opas pk-yrityksille ulkoistamisen tietoturvasta. Opinnäytetyössä on myös tietoa yleisesti tietoturvasta ja ulkoistamisesta.

Modernissa liiketoiminnassa ulkoistaminen on osa jokapäiväistä elämää. Se ei kuitenkaan tarkoita, että se tehtäisiin aina oikein. Tämän takia on tärkeä tutkia asiaa ja selvittää parhaat tavat pk-yrityksille tehdä se.

Opinnäytetyön teoriaosuudessa on tietoa tietoturvasta ja ulkoistamisesta. Tämä tieto perustaa pohjan opinnäytetyön ohje-osalle. Ohjeen jälkeen on pohdintaa ohjeen käytettävyydestä ja sen laadusta.

Opinnäytetyön tulokset olivat yllättäviä. Huolellinen suunnittelu muodostui yhdeksi pääasiaksi. Tutkimus osoittaa, että ulkoistava yritys on vastuussa ulkoistusprosessista. Ulkoistuspalveluja tarjoavalla yrityksellä on toki jotakin vastuuta, mutta loppujen lopuksi ulkoistavan yrityksen vastuulla on tarkistaa, että kaikki tehtiin niin kuin se sovittiin sopimuksessa. Vastuu osa oli todella kiinnostava, sillä olisi helppo uskoa, että ulkoistuspalveluja tarjoavalla yrityksellä olisi enemmän vastuuta.

Prosessin aika kävi ilmi, että ulkoistaminen on yleinen prosessi ja siksi siitä on myös paljon tietoa. Siksi sitä on tärkeää käyttää, eikä vain yrittää tehdä sitä itse. On tärkeää kuitenkin muistaa, että mikä toimii joillekin, ei välttämättä toimi toisille.

Loppujen lopuksi ohje on hyödyllinen, sille se käsittelee tietoturvaa ja ulkoistamista yhdessä ja antaa myös ulkoistamisprosessin perusteet. Opas ei kuitenkaan käsittele kaikkia mahdollisia näkökulmia ja sen takia sitä tulee käyttää tämä huomioon ottaen. Mutta se on hyödyllinen erityisesti niille yrityksille, jotka eivät ole ulkoistaneet paljon tai mahdollisesti ollenkaan aikaisemmin.

Asiasanat
tietoturva, ulkoistaminen, opas

Haaga-Helia
University of Applied Sciences

Abstract

Date

Author(s)
Teemu Laitinen

Degree programme
Business Information Technology

Report/thesis title	**Number of pages and appendix pages**
Guide for information security aspect of outsourcing for small companies	25

The purpose of this thesis was to make a guide for smaller companies on the information security aspect of outsourcing. The thesis describes the practices of information security and outsourcing in general.

In the modern business world outsourcing is a part of everyday life. But that does not mean that it is always done properly. Because of that it is important to recapitulate the theory and figure out the best ways for smaller companies to do it.

The theoretical part of the thesis summarizes the knowledge base for the research question. This information then forms the background for the guide part of the thesis. After the guide there is reflection upon the usefulness and quality of the guide.

The results of the study were unexpected. Careful planning became one of the main points. The study shows that the company that outsources is responsible for the outsourcing process. The company that offers the outsourcing services has of course some responsibilities, but in the end it is the commissioner's responsibility to check that everything is done the way it was agreed in the contract. The responsibility part was quite interesting, since it is easy to assume that the company that offers the services would have more responsibility.

Also during the study process it became apparent that outsourcing was a common process and therefore there was a lot of knowledge about it. Therefore it is important to use it and not just try to do it on one's own. It is important to remember though that what worked for others might not work for some.

In the end the guide is useful since it covers information security and outsourcing together and it also gives the basics of outsourcing process. However the guide does not cover all the possible aspects of the process and therefore should be used accordingly. But it is useful especially for those companies that have not done much or possibly no outsourcing before.

Keywords
information security, outsourcing, guide

Sisällys

1 Johdanto

Opinnäytetyön aiheena on tutkia ulkoistamisesta aiheutuvia tietoturvaongelmia pienten ja keskisuurten yritysten näkökulmasta. Mitä näiden yritysten tulisi ottaa huomioon ja näiden yritysten erityispiirteiden vaikutukset ulkoistamiseen. Työn tavoitteena on aikaansaada käsitys siitä, mitä ongelmia pk-yrityksien tietoturvalle voi ulkoistamisesta tulla. Samalla myös syntyy käsitys ulkoistamisen hyödyistä.

Ulkoistaminen on luontainen osa yritysten toimintaa. Niin kauan kuin yrityksiä on ollut olemassa, on yrityksillä ollut tarpeita, joita ne itse eivät ole voineet hoitaa. Nykyään edes isoimmat monikansalliset yritykset eivät pysty, eivätkä haluakaan hoitaa kaikkea itse, vaan ulkoistavat tietyt toiminnot ulkopuolisille toimijoille. Mitä pienempi yritys, sitä vähemmän sillä on resursseja tarpeittensa hoitoon. Pienessä yrityksessä esimerkiksi yhdenkin työntekijän sairastuminen voi aiheuttaa suura ongelmia. Tämän takia on tärkeää hyödyntää resurssit mahdollisimman hyvin. Mitä hoitaa itse ja mitä on parempi hoitaa ulkopuolisilla toimijoilla.

Vaikka ulkoistaminen on ollut luonnollista toimintaa yritysmaailmassa yritystoiminnan alusta asti, liittyy siihen kuitenkin ongelmia. Ehkä juuri sen luonnollisuus aiheuttaa sen, että sen seurauksia ja sen aiheuttamia ongelmia ei mietitä tarpeeksi. Resurssien vähyydestä johtuen voi myös ulkoistamisvaihtoehtojen tutkiminen olla vaikeaa ja kallista. Ulkoistamisesta voi olla monia haittoja ja hyötyjä, mutta tämän opinnäytetyön tarkoitus on keskittyä ulkoistamisen tietoturvaan liittyviin seikkoihin.

Tietoturva on myös ollut mukana yritystoiminnassa alusta asti. Ei ehkä nykyisessä merkityksessään, mutta yleispiirteissään kylläkin. Tietojen saatavuus, luetettavuus ja niiden turvaaminen ovat olleet tärkeitä kauan ennen tietokoneita. Historian saatossa uhat ovat muuttuneet, mutta tavoitteet ovat säilyneet samoina. Jos pystyisimme kysymään esimerkiksi keskiaikaiselta kauppiaalta, mitkä asiat ovat hänelle tärkeitä, olisivat tietoturvaan liittyvät vastaukset nykyajan yrittäjälle tuttuja. Varmasti hänelle olisi tärkeää, että yrityksen kirjanpito olisi varmasti turvassa, yhdenmukainen eri toimipisteiden välillä ja aina saatavilla.

Opinnäytetyössä on teoriaosuus tietoturvan ja ulkoistamisen taustoista. Sen jälkeen syntyvä ohje ulkoistamisen tietoturvasta tulee olemaan samassa dokumentissa teoriaosuuden kanssa. Ohjeen valmistuttua on vuorossa sen arviointi ja tulosten analysointi. Lopputuloksena syntyvän ohjeen on tarkoitus kertoa mitä pk-yrityksen tulee ottaa huomioon ulkoistamisessa tietoruvan näkökulmasta.

2 Ulkoistaminen

Ulkoistaminen on nykyään luontainen osa yritystoimintaa. Varsinkin parin viime vuosikymmenen aikana siitä on tullut olennainen osa yritysten toimintaa. Ulkoistamista on totta kai tehty aikaisemminkin, mutta nykyään se on aikaisempaa strategisempaa. Kustannustehokkuuden arviointi on olennainen osa ulkoistamista. Yrityksissä arvioidaan nykyään tarkkaan kannattaako jokin asia tuottaa itse, vai hoitaa se ulkopuolisella valmistajalla. Aikaisempaa enemmän arvioidaan myös onko se kannattavaa lyhyellä tai pitkällä aikavälillä. Joskus voi jokin olla kannattavaa lyhyellä aikavälillä, mutta pitkällä aikavälillä onkin parempi tuottaa se yrityksen ulkopuolella. Näin yritys voi vapauttaa pääomaa ja keskittyä yrityksen ydinliiketoimintaan. Ulkoistamisessa yksityinen sektori toimii ennen julkista sektoria. Yksityiset yritykset pystyvät nopeampiin muutoksiin, joten ne ulkoistavat julkista sektoria aiemmin. Julkisella sektorilla on myös pitkään hoidettu kaikki itse ja pitkien perinteiden muuttaminen ei ole helppoa. (Valtiovarainministeriö 2006.)

Ulkoistaminen voidaan hoitaa usealla eri tavalla. Ulkoistettavat resurssit voidaan siirtää palvelun tarjoajalle. Tässä tavassa ulkoistavasta yrityksestä siirtyy henkilökuntaa ja laitteistoa yritykseen, joka tarjoaa ulkoistamispalveluja. Ulkoistus voidaan myös tehdä niin, että resurssien siirtoa ei tapahdu. Ulkoistava organisaatio ja palvelujen tarjoaja voivat myös perustaa yhteisyrityksen joka tarjoaa varsinaiset palvelut. Yritys voi myös perustaa itse uuden yrityksen, johon se ulkoistaa halutut palvelut. Mahdollista on myös, että ulkoistaminen tapahtuu yrityksen sisällä, esimerkiksi useasta pienestä yksiköstä yhteen isoon yksikköön. (Valtiovarainministeriö 2006)

2.1 Ulkoistamisen hyödyt ja haitat

Ulkoistaminen mahdollistaa yrityksen keskittymisen sen ydinliiketoimintaan. Tämän seurauksena vapautuu pääomaa, jota yritys voi hyödyntää laadun parantamiseen, resurssien parempaan käyttöön ja niin edelleen. Kustannusten aleneminen on mahdollista, koska ulkopuolinen yritys voi tuottaa palvelun halvemmalla. Varsinkin jos se tuottaa samanlaista palvelua usealle yritykselle. Kustannusten hallinta myös helpottuu, kun tuotteen tai palvelun kokonaiskustannuksista yhä suurempi osa on suoraan sen hinnassa. Ulkopuolinen yritys voi myös pystyä seuraamaan paremmin teknistä kehitystä, koska heidän ydinliiketoimintaansa on juuri kyseinen palvelu tai tuote. Ulkoistamispalveluja tarjoava yritys on myös kiinnostava työnantaja ja ne pystyvät palkkaamaan osaavaa työvoimaa. Harvemmin kuullaan, että ulkoistaja ulkoistaa jotakin toimintaa. (Valtiovarainministeriö 2006.)

Ulkoistaminen ei kuitenkaan aiheuta pelkästään hyötyjä. Osa ulkoistamisista yksinkertaisesti vain epäonnistuu ja joistakin aiheutuu ongelmia myöhemmin. Jos ulkoistamista ei suunnitella kunnolla, on todennäköisempää, että se epäonnistuu. Tämän takia huolellinen suunnittelu on erittäin tärkeää, kun mietitään ulkoistamista. Yrityksen tarpeet voivat myös muuttua todella nopeasti, jolloin ulkoistamispalveluja tarjoava yritys voi tarjoa palvelua, joka ei vastaa enää yrityksen tarpeita. Ulkoistamisessa on myös tärkeää muistaa, että sen hyödyt saavutetaan pitkällä aikavälillä. Ulkoistaminen voi alussa olla kalliimpaa, kuin alussa suunniteltiin. Hyvä suunnittelu ja kärsivällisyys ovat tärkeitä asioita ulkoistettaessa. (Valtiovarainministeriö 2006.)

2.2 Ulkoistamisen vaiheet

Ulkoistamisessa on useita vaiheita. Ulkoistaminen alkaa päätöksellä toteuttaa ulkoistaminen. Tähän liittyy olennaisesti arviointi ulkoistamisen vaikutuksista esimerkiksi tietoturvaan. Tässä voidaan hyödyntää aikaisempia kokemuksia, tai samanlaisien yrityksien kokemuksia. Päätöksen teon jälkeen alkaa suunnittelu. Ulkoistuskohteet rajataan ja niiden riippuvuudet muihin toimintoihin määritellään. Tällöin myös tarkastetaan dokumentointi, jotta ulkoinen yritys ymmärtää asian varmasti samalla tavalla. Suunnitteluvaiheessa luodaan myös tarjouspyyntö, josta tulee ilmi halutut asiat ja yrityksen tavoitteet, sekä esimerkiksi yrityksen tietoturvavaatimukset. (Kuparinen 2006.)

Suunnittelun jälkeen alkaa kilpailuttaminen. Kilpailuttamisen aikana arvioidaan kuinka vuorovaikutus toimittajaehdokkaiden kanssa toimii. Kilpailuttamisen aikana on tärkeää tuoda esille tietoturvan rooli ja yrityksen tavoitteet sen suhteen. Samalla myös arvioidaan mahdollisia tulevia yhteistyökumppaneita. (Kuparinen 2006.)

Kilpailuttamisen loppuvaiheessa aloitetaan jäljelle jääneiden tarjousten arviointi ja sen jälkeen sopimuksen tekeminen. Tarjouspyyntövaiheessa voidaan selvittää voidaanko turvallisuusasioiden hoito liittää sopimukseen. Prosessin aikana arvioidaan myös ulkoisen yrityksen mahdollisuudet toteuttaa sopimuksessa sovittavia asioita. (Kuparinen 2006.)

Sopimuksen tekemisen jälkeen alkaa kriittinen siirtymävaihe. Tähän vaiheeseen liittyy useita riskejä esimerkiksi sopimuksen epäselvyyksien osalta tai toimintojen vaarantuminen. Jos mahdollista, niin siirto on hyvä testata ennen lopullista siirtymää. Huolellinen suunnittelu on tässä vaiheessa tärkeää molemmille osapuolille ja siitä on myös molemmille hyötyä. (Kuparinen 2006.)

Siirtovaiheen onnistumisen jälkeen alkaa tuotantovaihe. Tämän vaiheen aikana on suoritettava jatkuvaa arviointia ulkoistamisen hyödyistä ja haitoista. Näin saadaan selville pitääkö ulkoistamista esimerkiksi laajentaa tai supistaa. Yleinen toimittajan valvonta on suositeltavaa ja se voidaan myös toteuttaa esimerkiksi ulkoisen puolueettoman toimijan auditoinnilla. (Kuparinen 2006.)

Viimeisenä vaiheena on ulkoistamisen lopettaminen. Mikäli ulkoistaminen ei ole toiminut tai siitä on aiheutunut tietoturvariskejä, voidaan toiminto siirtää takaisin yritykseen. Mikäli muutoksia tai lopettamista ei tehdä hallitusti voi siitä syntyä riskejä yrityksen tietoturvalle. Ulkoistamisen lopettamisen sijaan voidaan esimerkiksi vaihtaa toimittajaa tai muuttaa palvelusisältöä. (Kuparinen 2006.)

2.3 Ulkoistamisen vaihtoehdot

Ulkoistamisen vaihtoehtoja on monia. Nykyisin yritykset keskittyvät yhä enemmän niiden ydinliiketoimintaan, joten monia yrityksen toimintoja voidaan ulkoistaa. Yritys voi halutessaan ulkoistaa tietohallinnon osittain tai kokonaan. Järjestelmien ja laitteistojen ulkoistaminen on myös yleistä. Yrityksen tietotoliikenne eli sisäverkko ja internet on myös usein ulkoistettu. Nykyisin on myös tarjolla sovellusvuokrauspalveluja. (Kaskela 2005.)

Tietohallinnon ulkoistaminen on monimutkainen päätös. Tietohallinnosta voidaan ulkoistaa osia, tai se voidaan ulkoistaa kokonaan, sen johtamista lukuun ottamatta. Mitä ulkoistetaan, kannattaa päättää yrityksen osaamisen perusteella. Se, mihin yrityksellä löytyy osaamista, kannattaa hoitaa itse. Mihin osaamista ei ole, kannattaa ulkoistaa. Yrityksille tarjotaan esimerkiksi järjestelmänhallintaa, laitteistoja, tietoliikennettä, sovellukset ja erilaiset konsultointipalvelut. (Kaskela 2005.)

Järjestelmäpalveluissa yritys ulkoistaa esimerkiksi järjestelmien ylläpidon, huollon, neuvonnan, asennuksen ja yleisen operoinnin. Näin tavallisesti yrityksen oman IT-osaston tehtävät siirtyvät ulkoisen yrityksen hoitoon. Ulkoisella yrityksellä on yleensä enemmän resursseja valvoa laitteiden toimintaa ja reagoida mahdollisissa virhetilanteissa. Laitteistoja ulkoistettaessa voidaan ulkoiselta yritykseltä saada tukipalveluita, tai laitteisto voidaan kokonaan hankkia ulkoiselta toimijalta. Tällöin yrityksen ei enää itse tarvitse huolehtia laitteiden ylläpidosta tai päivittämisestä. Palvelun tarjoaja voi esimerkiksi päivittää koneita ja uusia laitteita tietyin väliajoin tehdyn sopimuksen mukaan. Laitteistoja voidaan joko ostaa tai vuokrata tarpeiden mukaan. Yleinen toimenpide on palvelimien ulkoistaminen. (Kaskela 2005.)

Tietoliikennepalveluissa yritys voi ulkoistaa lähiverkon suunnittelun ja toteutuksen sekä internetin. Yritys voi toteuttaa nämä myös itse, mutta yleensä lähiverkon hoitaa sama palveluntarjoaja, joka hoitaa yrityksen internet-yhteyden. Yrityksen lähiverkko on helpompi hoitaa itse, mutta se yleensä hankitaan samalla ulkoisen verkon kanssa. (Kaskela 2005.)

Järjestelmien ulkoistamisessa ulkopuolinen yritys auttaa asennustöissä, vikatilanteiden hoidossa, järjestelmien käytössä ja atk-tuessa ja neuvonnassa. Laitteistopalveluissa ulkopuolinen yritys voi hoitaa laitteiston uusimisen ja ohjelmistojen asentamisen. Tällöin yrityksen ei tarvitse seurata niin paljon teknologian kehitystä, vaan ulkopuolinen yritys huolehtii siitä, että yrityksen laitteet ovat ajan tasalla, riippuen tietenkin tehdystä sopimuksesta. Tämä mahdollistaa myös esimerkiksi sen, että yrityksellä itsellään ei tarvitse olla palvelimia, vaan yritys voi ostaa palvelintilaa ulkopuoliselta yritykseltä. (Kaskela 2005.)

Sovellusten vuokraus on nykyään yleistä. Sovelluksia voidaan käyttää internetin yli ja ne voivat sijaita palveluntarjoajan palvelimilla. Tekniikan kehitys mahdollistaa nykyään sen, että yrityksen ei tarvitse enää hankkia ohjelmistolisenssejä, vaan yritys voi vuokrata sovellukset halutuksi aikaa ulkopuoliselta yritykseltä internetin välityksellä. Näin yritys säästää rahaa ohjelmistolisensseissä, eikä yrityksen tarvitse huolehtia ohjelmien asennuksesta ja päivityksistä. Yritys voi myös helpommin vaihtaa ohjelmistosta toiseen. (Kaskela 2005.)

2.4 Yleiset vaikutukset tietoturvaan

Ulkoistaminen voi vaikuttaa tietoturvaan joko positiivisesti tai negatiivisesti. Ulkoinen yritys voi tuottaa palvelun turvallisemmin tai sitten ei. Tietoturvavaikutukset riippuvat myös paljon siitä, mitä ulkoistetaan. Tärkeää on muistaa, että vastuu tietoturvasta on koko ajan ulkoistavalla yrityksellä ulkoistamisen ajan. Ulkoistuksen myötä ulkoistava yritys tulee enemmän tai vähemmän riippuvaiseksi palvelun tarjoavasta yrityksestä. Täten jos palvelun tuottaja joutuu vaikeuksiin, se heijastuu myös ulkoistavaan yritykseen. Riippuvuuden aiheuttamien ongelmien arviointi onkin yksi hankalimmista osa-alueista arvioida ulkoistamista suunnitellessa. Tätä ei voi koskaan yliarvioida. Riippuvuuden aiheuttamia vaikutuksia ei välttämättä voi kokonaan ennakoida, mutta ne kannattaa silti yrittää arvioida mahdollisimman tarkasti. (Valtiovarainministeriö 2006.)

Toimittajan vaihto voi aiheuttaa ongelmia. Vanhasta yhteistyökumppanista ollaan yleensä riippuvaisia. Muut yritykset voivat luulla, että niillä ei ole tarjouskilpailussa mahdollisuuksia, joten ne eivät tee tarjousta. Tällöin ei välttämättä synny ollenkaan kilpailevia tarjouksia. Nykyinen toimittaja voi aiheuttaa ongelmia sopimuksen loppuessa. Siirtokustannuksia voidaan liioitella, tai toimittaja voi kieltäytyä yhteistyöstä. (Valtiovarainministeriö 2006.)

Tärkeää on muistaa, että vastuu toiminnasta on lopulta ulkoistajalla. Toimittaja sitoutuu tiettyihin sääntöihin ja palvelutasoon. Sopimuksia tehdessä onkin tärkeää sopia myös vastuunjaosta, esimerkiksi ongelmatilanteita varten. Tämä on tärkeää tehdä, koska toimittaja voi luulla vastuun olevan ulkoistajalla ja ulkoistaja taas toimittajalla. Vastuunjaon merkitys korostuu, jos yrityksellä on useita toimittajia. Tämän vuoksi onkin tärkeää, että ulkoistaja valvoo toimittajien toimintaa. Varsinkin, koska Suomen lainsäädännön mukaan yritys vastaa alihankkijoidensa toiminnasta kuin omastaan. (Valtiovarainministeriö 2006.)

2.5 Ulkoistamisen tietoturva

Ulkoistaminen voi tehostaa yrityksen toimintaa. Siihen kuitenkin liittyy paljon riskejä, jotka täytyy ottaa huomioon. Osa riskeistä on kuitenkin sellaisia, että niihin on vaikea varautua. Ulkoistuspalveluja hoitavan yrityksen valinta on tärkeää tehdä huolella. Huono valinta voi johtaa palvelujen heikkenemiseen sekä niiden hidastumiseen ja myöhästymiseen. Kaikkeen ei kuitenkaan voi varautua. Luonnonmullistus tai huono taloustilanne voivat ajaa yhteistyökumppanin konkurssiin. Tällaisiin tilanteisiin on kuitenkin vaikea varautua. Aina voi kuitenkin tarkistaa, että onko yritys hyvällä taloudellisella pohjalla. (Benvenuto, Brand 2005.)

Kuten kaikessa muussakin, on suunnittelu olennainen osa prosessia. On tärkeää miettiä mitä ulkoistetaan ja miksi. Kun on päätetty mitä ulkoistetaan, pitää luoda suunnitelma yhteistyökumppanien etsimiseksi. Hyvä suunnittelu mahdollistaa kilpailukykyisen, järkevän ja toimeenpanokelpoisen sopimuksen. Samalla myös selviää mitä oikeasti halutaan saavuttaa ja mitä siitä ollaan valmiita maksamaan. Hyvän suunnittelun ansioista hyvän yhteistyökumppanin löytö on helpompaa. Neuvottelutilanteessa hyvästä suunnitelmasta on myös hyötyä. Näin jo neuvottelun alkuvaiheessa on helppo nähdä, onko neuvottelukumppani sitä mitä haetaan vai ei. Näin ei tuhlata aikaa neuvottelemalla sellaisten yritysten kanssa, joiden kanssa ei lopulta halutakaan tehdä sopimusta. (Benvenuto, Brand 2005.)

Sopimuksen teon jälkeen on vuorossa siirtymävaihe, joka on todella kriittinen. Siirtymävaiheessa on tärkeää valvoa, että sopimuksessa sovitut asiat ovat tiedossa niillä henkilöillä, jotka suorittavat varsinaisen ulkoistamisen. Sekä myös se, että sopimuksessa sovittuja asioita noudatetaan. Tämäkin vaihe on tärkeää suunnitella hyvin, jotta siirtymävaihe tapahtuisi mahdollisimman sujuvasti. Varsinkin jos yritys on itse hoitanut jotain asiaa, jonka hoito siirretään nyt ulkopuoliselle yritykselle. (Benvenuto, Brand 2005.)

Kaikesta suunnittelusta huolimatta jokin voi mennä pieleen. Mahdollisesti syntyviin ongelmiin onkin tärkeää käydä heti kiinni, jotta ne eivät pääse kasvamaan. Tämän takia on tärkeää miettiä etukäteen kuka hoitaa ongelmat, jos niitä syntyy. Näin ei pääse syntymän tilannetta, jossa kukaan ei oikein tiedä kenen ongelman oikein pitäisi ratkaista. Vaikka kaikkia ongelmia ei voi nähdä etukäteen ja kaikkeen ei voi millään varautua, on huolellinen suunnittelu erittäin tärkeää. Huolellinen suunnittelu vähentää ongelmia, nopeuttaa prosessia, sekä parantaa mahdollisuuksia onnistuneeseen ulkoistamiseen. (Benvenuto, Brand 2005.)

3 Tietoturva

Tietoturvan perustana on CIA–malli. Kyseessä ei kuitenkaan ole Yhdysvaltain keskustiedustelupalvelusta tai Amerikan kulinaarisesta instituutista. CIA muodostuu sanoista luottamuksellisuus, eheys ja saatavuus. Luottamuksellisuudella tarkoitetaan sitä, että tieto on käytettävissä vain halutuille henkilöille. Tähän käytetään käyttäjätunnuksia ja salasanoja, sekä muita tunnistusmetodeja. Luottamuksellisuus liittyy myös yleisemmällä tasolla yksityisyydensuojaan. Eheydellä tarkoitetaan tiedon luotettavuutta. Tarkoittaen, että tietoa ei ole muutettu tahallisesti tai vahingossa. Tähän liittyy myös se, että tieto on todella tullut sieltä mistä luulet sen tulleen, eikä joltain hakkerilta. Eheyteen voidaan myös liittää se, että lisätty tieto on oikeaa tietoa. Olennaisinta on kuitenkin tiedon säilyminen oikeana sen syöttämisen tai siirtämisen aikana. Saatavuudella tarkoitetaan nimensä mukaisesti tiedon saatavuutta milloin tahansa. Tietojärjestelmä joka ei ole saatavilla tarvittaessa on hyödytön. Saatavuuteen voivat vaikuttaa tekniset asiat, luonnonilmiöt sekä ihmisen vahingossa tai tahallaan aiheuttamat ongelmat. (University Of Miami.)

Tietoturvan toteuttaminen vaatii sen, että tietoturvasuunnittelu tehdään ennen kuin teknistä ratkaisua ruvetaan toteuttamaan. Tietoturva on sekä teknisiä ratkaisuja, että hallinnollisia prosesseja. Miten tiedot on salattu, ovatko laitteet ja ohjelmat ajan tasalla. Miten virusturva ja palomuuri toteutetaan. Onko yrityksen tiloissa kulunvalvontaa ja saako yrityksen tilat lukittua. Missä ja miten tietoa säilytetään ja kenellä on siihen oikeus. Yrityksen henkilökunnan tietoisuudella oikeista toimintatavoista on suuri vaikutus tietoturvaan. Tietääkö henkilöstö miten pitää toimia ja miten he voivat itse vaikuttaa tietoturvaan. Tietoturvaan kuuluu myös esimerkiksi miten toimitilat on suojattu esimerkiksi vesivaurioita, sähköjen katkeamista tai esimerkiksi rikollisia vastaan. (Valtiovarainministeriö 2012.)

Tärkeänä osana tietoturvaa on nykyään myös etätyö ja etäkäyttö. Töitä pystytään monesti nykyään tekemään kotoa käsin ja tämä vaikuttaa oleellisesti tietoturvaan. Miten työntekijä saa suojatun yhteyden yrityksen verkkoon ja miten yrityksen laitteet pysyvät suojattuna työntekijän ottaessa niitä kotiin. Tähän yrityksen pitää luoda sääntöjä, protokollia ja päättää miten etätyön suhteen toimitaan. Yrityksen tietojärjestelmiä ja palveluita voidaan myös käyttää ja huoltaa nykyisin myös yrityksen toimitilojen ulkopuolelta. Tärkeää on määrittää miten tämä toteutetaan ja mitä oikeuksia esimerkiksi laitteiden ylläpidosta huolehtivalla yrityksellä on yrityksen laitteisiin. (Valtiovarainministeriö 2012.)

Useasti yrityksellä on useita suojattavia kohteita. Tämän tärkeä on määritellä niiden tärkeysluokka, jotta voidaan selvittää kohteiden merkitys. Tärkeimmät kohteet tulee suojata ensin ja paremmin kuin kohteet, joiden tärkeys on vähäisempi. Samalla myös määritellään, kuinka paljon resursseja mihinkin osa-alueeseen käytetään. Tärkeysluokkaan ei ainoastaan vaikuta toiminnon tärkeys yritykselle, vaan myös se, mikä on tiedon suojaustaso. Tiedon suojaustaso määrittelee yleensä siihen liittyvät suojausmenetelmät. Mitä tärkeämpää tietoa, sitä paremmin se suojataan. Tiedon luottamuksellisuuteen liittyvät suojausmenetelmät, eivät yleensä ole korkeampia, kuin tiedon suojaustasoluokka. Tärkeysluokan määrittelemiseen liittyy myös varautumisen määritteleminen. Tärkeämpien kohteiden suojelemiseen varataan enemmän resursseja, sekä niiden suojaamiseen, että kriiseistä toipumiseen. Tärkeimmät palvelut luonnollisesti on tärkeää pitää toiminnassa ja saada mahdollisimman pian toiminaan niiden kaatumisen jälkeen. (Valtiovarainministeriö 2012.)

3.1 Tietoturvan osa-alueet

Tietoturva koostu kahdeksasta eri osa-alueesta. Ensimmäinen on yritys- ja henkilöstöturvallisuus, jolla tarkoitetaan miten yritys suhtautuu tietoturvaan, sekä miten yrityksen henkilökunta hoitaa ja on tietoinen tietoturvasta. Seuraavana on tietoaineistoturvallisuus, joka nimensä mukaisesti tarkoittaa tiedon turvaamista. Esimerkiksi miten tietoja säilytetään ja miten tietojen suojausluokitus on määritelty. Fyysisellä turvallisuudella tarkoitetaan esimerkiksi sitä, miten tilat on äänieristetty ja miten kulunvalvonta hoidetaan. Tietoliikenneturvallisuus tarkoittaa sitä, miten yrityksessä hoidetaan tietoliikenne. Esimerkiksi miten sähköpostit ovat salattuja ja miten yrityksessä käytetään palomuureja. Viimeiset ovat laitteistoturvallisuus ja käyttöturvallisuus. Käyttöturvallisuudella tarkoitetaan, miten yrityksessä hoidetaan esimerkiksi etätyöskentely. (Valtiovarainministeriö 2008.)

3.2 Kryptografia

Kryptografia kuuluu olennaisena osana tietoturvaan. Monelle salakirjoitus tarkoittaa nykyisiä salakirjoitusmenetelmiä mitä käytettään tietokoneiden välisessä viestinnässä. Monille tuttuja ovat esimeikiksi julkiset ja yksityiset avaimet, jotka suojataan jollakin salauksella. Salakirjoitus juontaa kuitenkin juurensa aikaan kauan ennen tietokoneita. Salakirjoitusta harrastettiin jo muinaisessa Egyptissä, missä kirjurit rupesivat käyttämään omia hieroglyfejään normaalien sijaan. Salakirjoituksilla on kautta historian pyritty pitämään haluttu tieto salassa. Sitä on käytetty esimerkiksi suojaamaan diplomaattisia viestejä tai taistelusuunnitelmia. (Kessler 2015.)

Nykyään salakirjoitukset ovat kehittyneet paljon, mutta niiden tavoitteet ovat yhä samat mitä aiemmin, niitä vain käytetään yhä useammin ja yleisemmin. Nyky-yhteiskunnassa tapahtuu paljon viestintää tietoverkkojen yli. Koska melkein kaikki näistä ovat epäluotettavia, on käytettävä salakirjoitusta. Salakirjoitusta käytetään tiedon suojaamiseen varastamiselta ja muokkaukselta ja käyttäjän tunnistamiseen. (Kessler 2015.)

Salakirjoitus alkaa salaamattoman tekstin luomisella. Tämän jälkeen teksti salataan halutulla tavalla ja viesti kuljetetaan halutulle henkilölle. Tiedon vastaanottaja saa salakirjoitetun viestin, jonka vastaanottaja sitten purkaa salakirjoitusavaimella. Lopputuloksena lähettäjä on saanut lähetettyä vastaanottajalle tietoa turvallisesti ja vastaanottaja on saanut salauksen purettua. (Kessler 2015.)

4 Suunnittelu ja arviointi

Suunnittelu on olennainen osa sekä tietoturvaa, että ulkoistamista. Hyvänä vertauskuvana suunnittelun tärkeydelle on rakennusprojektin suunnittelu. Rakennusalalla on sanonta, että suunnittelijan työpöydällä tulee selville 80 % kaikista projektin kustannuksista. Suunnittelun kustannukset ovat kuitenkin vain murto-osa kokonaiskustannuksista. Tämän takia huolellinen ja laadukas suunnittelu ovatkin elintärkeitä projektin onnistumisen kannalta. (Lommi 2009.)

Arviointi on oleellinen osa tietoturvaa. Yrityksen tietoturvan tilaa voidaan joko arvioida sisäisesti tai ulkoisesti. Itse arvioinnissa määritellään ensin vahvuudet ja kehittämiskohteet. Ulkoinen arviointi taas antaa puolueettoman kuvan yrityksen tietoturvan tasosta. Tietoturvan tuloksellisuuden arviointi on jatkuva prosessi. Jatkuvasti kehittyvä tietoturvallisuuden mittaus mahdollistaa tietoturvan parantamisen. Käytettävien arviointikriteereiden tulee olla selkeitä ja niistä pitäisi käydä ilmi tietoturvan taso. Tietoturvatoimintaa voidaan tutkia ta-

pahtuneiden tietoturvapoikkeamien läpikäynnillä, miten ne on hoidettu ja kuinka tietoturvaa on yleisellä tasolla ylläpidetty. Tietoturvan arviointi voidaan liittää annettuihin tavoitteisiin. Näin voidaan selkeästi nähdä onko suunnitellut asiat tavoitettu. Samalla voidaan myös arvioida, millä tasolla tietoturvan hallintajärjestelmä nyt on ja suunnitella miten halutulle tietoturvatasolle päästään. (Valtiovarainministeriö 6/2006.)

5 Ohje

Ulkoistaminen on nykyään yleinen toimenpide kaiken kokoisissa yrityksissä. Mutta varsinkin pienissä ja keskisuurissa yrityksissä, se on todella yleistä. Yleisyys ei kuitenkaan tarkoita sitä, että se olisi helppoa. Päinvastoin ulkoistamisessa on monta asiaa, jotka pitää ottaa huomioon. Alusta loppuun saakka.

Ulkoistaminen voi tulla eteen jo yritystä perustettaessa tai vasta myöhemmin. Nykyään yritykset joutuvat kovaan kilpailuun. Jotta kilpailussa pärjää, on tärkeää löytää yrityksen ydinliiketoiminta ja keskittyä siihen. Resurssit eivät millään riitä, jos niitä yritetään jakaa liian moneen asiaan. Ulkoistaminen mahdollistaa keskittymisen vain siihen, mikä on olennaista.

Tämän ohjeen tarkoitus on auttaa pk–yrityksiä ulkoistamisessa. pk–yrityksen määritelmä on vaihteleva, mutta yleinen määritelmä soveltuu hyvin. Yrityksellä pitää olla vähemmän kuin 250 työntekijää, liikevaihto vuodessa enintään 50 miljoonaa ja tase enintään 43 miljoonaa. (Tilastokeskus.)

Vaikka ohje onkin ensisijaisesti tarkoitettu pk-yrityksille, toimii se silti myös isommille yrityksille. Ohjeessa käsitellään ulkoistamista ja siihen liittyvää tietoturvaa siten, että se on hyödyllistä myös muillekin. Sekä niille yrityksille jotka ovat ulkoistaneet aiemminkin, että niille jotka miettivät ulkoistamista ensimmäistä kertaa. Ulkoistaminen on sen verran tärkeä toimenpide, että kokeneenkin yrityksen on välillä tärkeää palautella mieleen ulkoistamisen tärkeimpiä vaiheita ja toimenpiteitä, sekä myös se mitä ulkoistamisella halutaan saavuttaa.

Pk-yritysten resurssit ovat rajalliset. Rajalliset resurssit tarkoittavat myös sitä, että yrityksessä ei riitä osaamista ja tietotaitoa kaikkeen. Tämän takia ulkoistaminen onkin yleistä ja järkevää. Tietotekniikka kehittyy nopeasti ja pienemmän yrityksen on vaikeampi pysyä kehityksen mukana. Vähäinen tietotaito aiheuttaa myös riskejä, joten viisasta onkin kääntyä silloin ammattilaisen puoleen. Toki myös ulkoistamiseen liittyy riskejä, mutta ne ovat

pienempiä kuin itse tehdyt päätökset jos tietoa asiasta on vähän. On myös tärkeää, että yrityksessä on joku, joka ymmärtää asiasta jotain. (Kaskela 2005.)

5.1 Ulkoistaminen vaihe vaiheelta

Osalle yrityksistä ulkoistaminen on vaihtoehto ja joillekin se on ainoa vaihtoehto. Molemmissa tilanteissa tulee miettiä tarkasti, miten se tehdään. Silloinkin kun ulkoistaminen on ainoa vaihtoehto yritykselle, se tulee suunnitella huolella. Vaikka vaihtoehtoja ei olisi kuin yksi, tulee se yksikin vaihtoehto miettiä kunnolla. Kun yrityksen toiminta tulevaisuudessa riippuu siitä, että tietty toimenpide saadaan ulkoistettua, on helppo toimia hätiköiden. Tällöinkin voidaan kuitenkin päättää, mihin toiminto ulkoistetaan ja miten se hoidetaan. Pakolliset asiat täytyy hoitaa huolellisemmin, kuin vapaaehtoiset asiat. Johtuen siitä, että niillä on yleisesti ottaen suurempi vaikutus yrityksen toimintaan.

Hyvänä vertauskuvana ulkoistamiselle toimii ihmisen ruokavalio. Ihmisen on pakko syödä säilyäkseen hengissä. Voimme kuitenkin päättää mitä me syömme. Voimme valita ruokavalion, joka lyhyellä aikavälillä on nautinnollista, mutta pitemmällä aikavälillä aiheuttaa terveyshaittoja. Tämä ei ainoastaan toimi hyvänä vertauskuvana sille ulkoistetaanko vai ei, vaan miten ulkoistetaan. Ulkoistamisessa voidaan valita helpompi reitti tai vaikeampi reitti. Aina nämä eivät kuitenkaan välttämättä eroa toisistaan. Jollakin yrityksellä voi käydä tuuri ja hyvä yhteistyökumppani löytyy helposti, ja ulkoistaminen sujuu ilman ongelmia. Toisella yrityksellä taas voi olla suuria ongelmia, vaikka ulkoistaminen olisi mietitty erittäin tarkkaan ja se olisi huolellisesti suunniteltu. Ongelmista ei kuitenkaan saa lannistua, vaan on muistettava, että ne kuuluvat asiaan.

Ulkoistusta mietittäessä täytyy ensin päättää, mihin halutaan keskittyä. Kun on päätetty mitä ydinliiketoiminnaksi tulee, voidaan ruveta miettimään, mitä yrityksen toimintoja voitaisiin antaa hoidettavaksi ulkopuoliselle. Hyvä suunnittelu ja tarkka mietintä on tärkeää aloittaa heti alusta asti. Mietittäessä mahdollisia ulkoistuskohteita kannattaa ottaa huomioon osaaminen yrityksen sisällä. Jos osaamista johonkin asiaan löytyy, voi olla parempi hoitaa se yrityksen sisällä. Kannattaa keskittyä niihin asioihin ensin, joihin ei yrityksen sisältä löydy osaamista.

Sitten kun on selvillä ne kohteet, joihin yrityksessä ei löydy osaamista, on hyvä miettiä niitä joihin löytyy. Tähän mennessä on voinut olla kannattavampaa hoitaa ne itse, mutta tilanne on voinut muuttua. Maailma muuttuu koko ajan ja on tärkeää pysyä ajan tasalla. Parin viime vuosikymmenen ajan on syntynyt paljon yrityksiä, jotka tarjoavat ulkoistamispalveluja. Asiat jotka oli pakko hoitaa itse vielä parikymmentä vuotta sitten, on nyt mahdol-

lista antaa hoidettavaksi yrityksen ulkopuolelle. Koska nämä yritykset tarjoavat samaa palvelua monelle yritykselle, ne pystyvät hoitamaan sen halvemmalla, kuin yksittäinen yritys itse.

Tätäkin kuitenkin kannattaa miettiä. Ulkoistaminen on pitkäikäinen ratkaisu ja sen hyödyt tulevat esiin vasta pidemmällä aikavälillä. Siksi onkin tärkeää miettiä hyödyttääkö jonkin ulkoistaminen hetkellisesti, vai vapauttaako se yrityksen pääomaa ja resursseja pitkäaikaisesti. Mahdollistaako ulkoistaminen yrityksen keskittyminen sen ydinliiketoimintaan, vai aiheuttaako se vain lisää monimutkaisuutta. Pienemmillä yrityksillä on toki vähemmän toimipisteitä, mutta jos samaa asiaa tehdään useammassa toimipisteessä, on mahdollista tehosta toimintaa ja keksittää tietty toiminto yhteen toimipisteeseen. Näin toiminta tehostuu ja resursseja säästyy.

5.1.1 Yhteistyökumppani

Kun lopulta on päätetty mitä halutaan ulkoistaa, on aika ruveta ajattelemaan mahdollisia yhteistyökumppaneita. Kuten kaikki ulkoistamisen vaiheet, on tämäkin syytä tehdä huolella. Huonon kumppanin valinta voi johtaa moniin ongelmiin pitkäksi aikaa. Se voi johtaa paitsi ulkoistuksen epäonnistumiseen, myös yrityksen toiminnan heikkenemiseen ja asiakaspalvelun kärsimiseen. Kumppania mietittäessä kannattaa ensin miettiä haluaako etsiä ulkomailta asti, tai vain kotimaasta. Ulkomaita mietittäessä tulee esimerkiksi tärkeäksi miettiä lainsäädäntöä. Mitä yhteistyökumppani yrityksen kotimaan lainsäädäntö sanoo yrityksen vastuusta ja miten tietosuoja eroaa Suomen lainsäädännöstä.

Yhteistyökumppaneista kannattaa tarkistaa niiden taloudellinen tila ja ottaa yhteyttä sen asiakkaisiin. Näin saadaan selville ovatko asiakkaat tyytyväisiä saamaansa palveluun. Jos ulkoistamispalveluja tarjoavan yrityksen muut asiakkaat ovat tyytyväisiä, niin on todennäköisempää, että yritys on hyvä yhteistyökumppani. Jos mahdollista, olisi hyvä myös olla yhteydessä yrityksen entisiin asiakkaisiin. Näin selviää miten yritys käyttäytyy, jos haluat lopettaa yhteistyön. Jotkut yritykset voivat olla hyviä kumppaneita, mutta kun haluat lopettaa yhteistyön, ne voivat aiheuttaa ongelmia. Toimintojen siirto toiseen yritykseen voi maksaa paljon enemmän kuin arvioitu, tai ne voivat kokonaan kieltäytyä yhteistyöstä. Koska tällainen toiminta aiheuttaa suuria ongelmia yrityksen toiminnalle, onkin elintärkeää suunnitella ja tutkia yhteistyökumppani mahdollisimman hyvin ennen yhteistyön aloittamista.

5.1.2 Sopimus

Sopivan yhteistyökumppanin löydyttyä alkaa sopimusneuvottelut. Ennen neuvottelujen alkamista on tärkeää miettiä, mitä yhteistyökumppanilta halutaan ja mitä siitä ollaan valmiita maksamaan. Neuvotteleminen helpottuu paljon, kun jo ennen niiden alkua on jo tiedossa, mitä neuvotteluilla halutaan saada aikaan. Neuvottelujen aikana on tärkeää muistaa, että ulkoistava yritys on vahvempi osapuoli neuvotteluissa. Monissa tapauksissa samaa palvelua tarjoaa useampi yritys, joten neuvottelukumppani ei välttämättä ole ainoa hyvä vaihtoehto. Tämä on tärkeä pitää sekä omassa, että neuvottelukumppanin mielessä. Jos neuvottelujen edetessä tuntuu, että ehkä kyseinen yritys ei välttämättä olekaan paras vaihtoehto, voi neuvottelut lopettaa. Vaikka yritys ennen neuvottelujen alkua vaikutti parhaalta vaihtoehdolta, niin ihmiskontakti neuvottelujen aikana voi vaihtaa näkökulmaa. Ulkoistamisessa syntyy kuitenkin läheinen suhde kahden yrityksen lähelle ja loppujen lopuksi se perustuu ihmisten väliseen kommunikointiin. Jos kommunikointi ei toimi, tulee ulkoistaminen epäonnistumaan. Kun ruvetaan kirjoittamaan sopimusta, on tarkasti mietittävä mitä siihen halutaan, koska yhteistyökumppani tulee toimimaan sen mukaan. Siksi onkin tarkasti mietittävä, että sopimuksessa on kaikki mitä halutaan. Ja myös niin, että se on niin selkeästi, ettei sitä voi ymmärtää väärin.

5.1.3 Siirtymävaihe

Sopimuksen syntymisen jälkeen alkaa sovittujen asioiden siirto yhteistyökumppanille. Siirtovaiheen aikana on erittäin tärkeää valvoa, että kaikki sujuu oikein. Samalla myös tarkistetaan, että kaikki sovitut asiat tapahtuvat. Vaikka ulkoistamisprosessissa ollaan jo näin pitkällä, pitää silti muistaa huolellinen suunnittelu. Siirtovaiheessa voi jokin helposti mennä pieleen. Tämän takia on tärkeää suunnitella, mitä siirretään missäkin vaiheessa. Näin yrityksen toiminta säilyy mahdollisimman sulavana ja asiakaspalvelu heikkenee mahdollisimman vähän.

Siirtymävaiheen jälkeen sovitut asiat hoitaa nyt yhteistyökumppani. Ulkoistetut asiat eivät kuitenkaan ole ulkoistamispalveluja tarjoavan yrityksen vastuulla, vaan ulkoistavan yrityksen. Tämä pätee koko ulkoistamisprosessin ajan ja sen jälkeen. Ulkoistava yritys luulee helposti, että vastuu on ulkoistamispalveluja tarjoavalla yrityksellä ja vastaavasti toisin päin. Koko prosessin ajan on tärkeää pitää tämä mielessä. Toki ulkoisella yrityksellä on vastuuta tarjoamistaan palveluista, mutta se tarjoaa ne, kuten sopimuksessa sovittiin. Ulkoistamispalveluja tarjoava yritys on toki vastuussa, jos se ei pysty toimittamaan palvelua kuten sopimuksessa sovittiin.

5.1.4 Suhteen lopettaminen

Jossain vaiheessa tulee eteen vaihe, kun yhteistyökumppanuus halutaan katkaista. Syynä tähän voi olla esimerkiksi muuttuneet tarpeet joihin jompikumpi osapuoli ei pysty enää vastaamaan. Tällöin toivon mukaan yhteistyökumppani ei aiheuta ongelmia palvelujen siirrossa uuteen yritykseen. Ulkoistamispalveluja tarjoava yritys voi esimerkiksi pyytää liian suuria siirtomaksuja, tai vain kieltäytyä yhteistyöstä. Yhteistyön katkaisu kannattaa määritellä sopimukseen. Tällöin kumpikin osapuoli on määrittänyt kumpiakin osapuoli tyydyttävän tavan yhteistyön mahdolliseen katkaisuun. Kuten aikaisemminkin tämä prosessi tulee suunnitella huolella. Jos näin ei tehdä, voi yrityksen toiminta mennä täysin sekaisin. Entinen yhteistyökumppani on kuitenkin tehnyt asiat tietyllä tavalla, ja uudella yhteistyökumppanilla pitää olla tarkka käsitys siitä miten asiat on tehty ja tulisi tehdä. Kaikkien kolmen osapuolen välillä tuleekin olla hyvä viestintäverkko. Ennen kuin mitään aletaan tekemään, on tärkeää että kaikilla on selvää mitä tehdään ja miten se tehdään.

5.1.5 Suunnittelu

Ulkoistaminen tulee siis suunnitella hyvin alusta loppuun. Ulkoistamista ei kannata kiirehtiä, vaan se tulee suorittaa huolella. Ulkoistamisen hyödyt tulevat ilmi vasta pidemmällä aikavälillä. Alkuvaiheessa ulkoistus voi olla suunniteltua kalliimpaa, eikä se välttämättä vaikuta niin toimivalta kuin aluksi luultiin. Tässäkin tulee olla kärsivällinen, sillä ulkoistamisen tarkoituksena on juuri parantaa yrityksen toimintaa pitkäjänteisesti. Siinä on juuri yksi syistä, miksi ulkoistamista tehdään. On hyvä myös pitää mielessä, että kaikki ei välttämättä suju suunnitelman mukaan. Harvoin mikään menee täysin suunnitelman mukaan, eikä ulkoistaminen ole mikään poikkeus. Hyvän suunnitellun tarkoituksena ei olekaan poistaa kaikkia ongelmia, vaan minimoida ne. Jos jokin menee pieleen, on tärkeää pitää tämä mielessä.

Suunnittelu on kuitenkin vain osa prosessia. Suunnitelman toteuttaminen on yhtä tärkeää, sekä se miten koko prosessin ajan toimitaan. Suunnitelma on tärkeä tehdä, mutta käytäntö voi helposti olla paljon erilainen kuin luultiin. Tämän takia on tärkeää pystyä niin sanotusti unohtamaan suunnitelma ja improvisoida. Prosessin aikana tavoitteet ja mitä ulkoistetaan voi muuttua ja on tärkeää pystyä mukautumaan. Suunnitelmaa pitää aina pystyä muuttamaan ja tarvittaessa unohtamaan kokonaan. Jos suunnitelma ei näytä auttavan yhtään, voi olla parempi keskeyttää prosessi ja tehdä uusi suunnitelma uusien tietojen pohjalta. Epäonnistuneen ulkoistamisen aikana opitut asiat voivat auttaa uuden suunnitelman laatimisessa.

5.2 Riskit

Ulkoistaminen on monimutkainen prosessi. Monimutkaisuus tarkoittaa yleensä paljon ongelmia. Hyvä suunnittelu vähentää niitä, mutta ei poista niitä kokonaan. Riskejä on kuitenkin paitsi prosessin aikana myös sen jälkeen. Mitä tietoturvaan liittyviä asioita pitäisi sitten ottaa huomioon?

Tietoturva voi joko heiketä tai parantua ulkoistamisen myötä. Pienemmillä yrityksillä on vähemmän resursseja tietoturvan hoitoon, joten palvelujen siirto yritykseen, joka on keskittynyt tiettyyn asiaan, voi parantaa tietoturvaa. Näin ei kuitenkaan välttämättä ole. Hakuprosessin aikana on tärkeää tutkia tarkoin miten tietoturva hoidetaan ulkoisessa yrityksessä. On helppo vain ajatella, että se on kunnossa, mutta näin ei välttämättä ole. Tärkeää on myös miettiä, onko tietoturva riittävän kattava niille asioille, mitä sinne olisi laitettava. Yrityksen asiat voivat tarvita parempaa, kuin mitä ulkoinen yritys tarjoaa. Ulkoisen yrityksen tietoturva voi olla riittävän hyvä joillekin asioille, mutta jotkin asiat vaativat parempaa suojausta. Tämän takia onkin tärkeää löytää sellainen yhteistyökumppanin, joka tarjoaa tarvittavan suojauksen. Jos yhteistyö on aloitettu, niin silloin on oletettu, että ulkoistavan yrityksen mielestä tietoturva on riittävällä tasolla. Valittaminen jälkikäteen ei auta.

Yritystä tutkittaessa on tärkeää olla huolellinen. Onko yrityksen henkilökunta saanut millaista tietoturvakoulutusta? Miten yrityksessä on varauduttu esimerkiksi luonnonmullistuksiin? Jos esimerkiksi sähköt katkeavat, onko yrityksessä oma generaattori. Onko yrityksen palvelimet sijoitettu siten, että ne eivät esimerkiksi ole vesiputkien läheisyydessä. Ottaako yritys tiedoista varmuuskopioita ja onko yrityksellä varapalvelimia. Jos palvelimet esimerkiksi hajoavat, niin onko yrityksessä valmiit suunnitelmat joilla varmistetaan, että palvelut eivät kaadu. Monesti näitä asioita ei tule mietittyä, mutta ennen yhteistyökumppanin valintaa on tärkeää tutkia nämä asiat. Samalla tulee myös tarkistettua, onko yhteistyökumppanin valinta tehty oikein. Hyvän yrityksen tulisi ymmärtää tällaisen tarkistuksen tärkeys. Jos yritys auttaa kaikin tavoin ja selittää asiat hyvin ja huolellisesti, niin voidaan olla varmempi, että on valittu oikea yhteistyökumppani. Jos taas yritys ei suostu tähän, niin kannattaa ruveta etsimään uutta yhteistyökumppania. Ulkoistamisprosessi perustuu pohjimmiltaan luottamukseen ja jos sitä ei ole, niin ulkoistus ei tule onnistumaan. Luottamus ei kuitenkaan silti tarkoita, että ei tarkisteta että kaikki tehdään halutulla tavalla. Inhimilliset virheet ovat aina mahdollisia ja molemminpuolinen huolellinen seuraaminen ja tarkistus pitävät huolen siitä, että asiat sujuvat ilman ongelmia.

5.3 Ulkoistamisen tietoturva

Ulkoistamiseen liittyy olennaisena osana tietoturva. Mitä vain ulkoistetaankin, niin siihen liittyy oleellisena osana tietoturva vaikutusten ajattelu. Toinen vaihtoehto on se, että tietoturva on juuri se mitä ulkoistetaan. Kummin päin asia onkin, niin tietoturva on hyvä pitää aina mielessä. Tarkoitus on käydä läpi yleisimmät asiat, mitä ulkoistetaan ja mitä niistä pitää ottaa huomioon tietoturvan kannalta.

5.3.1 Laitteet

Laitteiston ulkoistaminen on yleistä. Niiden hankinta voidaan ulkoistaa, tai ne voidaan esimerkiksi vuokrata tietyksi aikaa. Tähän liittyy myös laitteiston huolto, päivitys ja ylläpito. Tietoturvaa ajatellen tässä on monta ongelmaa, mitä pitää ottaa huomioon. Jos yrityksellä on käytössä vanhoja laitteita, niin ne pitää hävittää tai kierrättää tietoturvallisesti. Laitteita voidaan käyttää uudestaan jossain muualla, mutta yrityksen tiedostot pitää ensin hävittää laitteilta. Jos yrityksen sisältä ei löydy tähän asiantuntemusta, kannattaa laitteet viedä ammattilaiselle, joilta löytyy levyn päällekirjoitusohjelmistot ja tietotaitoa asiasta.

Uusien laitteiden hankinnassa täytyy ottaa huomioon ovatko niiden ohjelmistot ajan tasalla. Tärkeää on myös miettiä niiden virusturvaa. Minkä tyyppistä ja tasoista virusturvaa halutaan. Laitteista on tärkeää tarkistaa löytyykö niistä virustorjuntaohjelmaa. On myös syytä ajatella esimerkiksi mikä käyttöjärjestelmä tietokoneisiin halutaan. Ei kannata valita niin vanhaa käyttöjärjestelmää, että sen tukiaika on jo loppunut ja on sen takia tietoturvariski. Toisaalta taas uusimman mahdollisimman käyttöjärjestelmän valinta voi taas aiheuttaa toisenlaisia ongelmia. Se ei välttämättä vielä toimi kunnolla, eikä siihen välttämättä löydy ajureita. Varsinkin jos tietokoneeseen liitetään vanhempia laitteita, voi tämä olla ongelma. Kaikki tämä sovitaan laitetoimittajan kanssa, mutta ne on silti syytä tarkistaa laitteiden käyttöönoton yhteydessä. Inhimillisiä virheitä voi sattua ja on tärkeää tarkistaa että kaikki on kunnossa, ennen kuin tietoturva on ehtinyt vaarantua.

Laitteiden huollossa on myös monia seikkoja mitä pitää ottaa huomioon. Laitteiden huoltaja pääsee käsiksi laitteiden tietoihin. Tämän takia on tärkeää valita luotettava huoltaja, jotta tiedot pysyvät suojattuna. Tietoja voi myös esimerkiksi salata ja antaa huoltajalle vain oikeudet ja salasanat niihin asioihin, joihin heidän täytyy päästä. Näin vähennetään mahdollisia riskejä ja onhan turha antaa korjaajille oikeuksia asioihin joihin ei ole tarvetta. On myös tärkeää tutkia, miten laitteita käsitellään ja säilytetään huoltavassa yrityksessä. Jos tuntuu, että yritys ei säilytä laitteita tarpeeksi turvallisesti, kannattaa miettiä toista yritystä.

5.3.2 Tietosuoja

Kaikki tämä riippuu siitä miten tärkeää tietoa koneilla säilytetään, ja miten hyvin sitä pitää suojata. On turhaa vaatia ja ylläpitää korkeampaa tietosuojaa, kuin tietojen tietosuojaluokka vaatii. Tärkeitä tietoja suojataan paremmin ja vähemmän tärkeitä tietoja ei tarvitse suojata samalla tavalla. Tärkeitä tietoja sisältävät laitteet voi esimerkiksi viedä yritykseen, jossa tietosuoja on korkea. Vähemmän tärkeää tietoa sisältävät laitteet voi viedä yritykseen, jossa tietosuoja ei välttämättä ole niin korkea. Näin voidaan säästää kustannuksissa ja nopeuttaa prosessia. Tietoturvaa ei tietenkään kannata vaarantaa, mutta ei välttämättä kannata maksaa enempää kuin on tarpeen. Hyvänä vertauskuvana toimivat esimerkiksi museot. Tärkeimmistä teoksista huolehditaan paremmin ja ne suojataan paremmin. Halvemmat teokset voidaan säilyttää eri tavalla ja niihin ei kohdistu samanlaisia uhkia kuten maailmanlaajuisesti tunnettuihin teoksiin. Samaa periaatetta kannattaa hyödyntää yleisesti oman yrityksen ja yhteistyökumppanien tietoturvaa ajatellessa.

Tärkeää on kuitenkin muistaa, että jos yrityksen sisällä käytetään monia suojaustasoja, että ne eivät vaaranna toisia. Pitää varmistaa, että suojaustasojen välinen suojaus on kunnossa. Jos esimerkiksi joku hakkeri pääsisi käsiksi vähemmän suojattuihin järjestelmiin ja niiden kautta yrityksen sisäverkkoon ja siten paremmin suojattuihin järjestelmiin. Tämän takia voi olla järkevämpää, että määritellään tarvittava suojaustaso tärkeimpien tietojen mukaan ja toteutetaan loppujen suojaus sen mukaan. Ulkoistamisessa tämä tarkoittaa sitä, että yhteistyökumppanien valinta niin, että ne täyttävät tärkeimmille tiedoille valitun suojaustason. Mitä vähemmän yhteistyökumppaneja ja mitä paremmin ne hoitavat tietoturvan, sitä pienemmät tietoturvariskit ovat. Tämä voi myös helpottaa ulkoistamista, kun ei tarvitse miettiä niin monia eri yhteistyökumppaneita. Tietoturvan muuttaminen tiedon tietosuojatarpeiden mukaan, voi kuitenkin olla yritykselle parempi ratkaisu. Siinä tapauksessa tulee vain ottaa huomioon sen aiheuttamat tietoturvariskit.

5.3.3 Palvelimet

Nykyään ulkoistetaan usein palvelimia. Joko niiden hankinta, tai ne voivat olla kokonaan jossain toisessa yrityksessä. Jos ne ulkoistetaan kokonaan, on tärkeää tutkia miten tietoturva hoidetaan palvelimet hoitavassa yrityksessä. Tavoitteena on tietenkin, että vain halutut henkilöt pääsevät vaikuttamaan palvelimien toimintaan tai pääsevät käsiksi niissä oleviin tietoihin. Koska ulkoistava yritys on siitä loppujen lopuksi vastuussa, on tärkeää olla tietoinen miten se tehdään. Toinen tärkeä osa-alue on se, miten yhteys hoidetaan ulkoisesta yrityksestä ulkoistavaan yritykseen ja asiakkaisiin. Yhteyden täytyy olla luotettava ja turvallinen. On tärkeää tietää miten palvelu on tarkoitus pitää käynnissä esimerkiksi sähkökatkon tai esimerkiksi palvelimien päivityksen, huollon tai uusimisen aikana. Kaik-

kiin mahdollisiin uhkiin on tietenkin mahdotonta varautua, mutta suurimpaan osaan pitäisi pystyä. Kummankin osapuolen pitäisi myös miettiä, miten toimitaan jos tietoturva vaarantuu. On tärkeää miettiä mitä tehdään, jos ongelmia syntyy.

5.3.4 Tietohallinto

Tietohallinto voidaan myös ulkoistaa. Sen johtaminen tulee kuitenkin pitää yrityksen sisällä. Tietotekninen osaaminen voi olla yrityksessä vähäistä ja tällöin tietohallinnon ulkoistaminen voi tulla eteen. Täytyy kuitenkin muistaa, että tietohallinnon johdon ei ole tarkoitus olla tietotekniikan asiantuntijoita. Johdon tarkoituksena on tietää asiasta sen verran, että voi päättää mitä tehdään ja tietää mitä kukin tekee. Kun tietotekniikka ulkoistetaan, voivat toimintatavat muuttua, mutta perimmäinen tarkoitus ei pitäisi. Ulkoistuspalveluja tarjoava yritys tarjoaa samoja palveluja usealle yritykselle. Sama työntekijä tekee samaa palvelua usealle yritykselle. Tämän takia tietohallinnon johtajan on tärkeää kertoa ja selvittää ulkoisille toimijoille, mikä on paras tapa toimia kyseiselle yritykselle ja miten yrityksessä toimitaan. Jos näin ei tehdä, voi ulkoinen toimija kyllä toivotut asiat, mutta ne on saatettu tehdä niin, että niitä ei ole dokumentoitu oikein. Ilman kunnollista johtamista, voi helposti käydä niin, että kumpikin osapuoli ei välttämättä tiedä, mitä toinen halua. Tai miten se pitäisi tehdä. Kun johtaminen hoidetaan oikein, asiat tehdään niin kuin ne pitäisi ja kaikki ovat ajan tasalla siitä, mitä on tehty.

5.3.5 Tietoturva

Tietoturvan ulkoistaminen onkin aivan oma lukunsa. Jos yritys ulkoistaa koko tietoturvan hoidon ulkopuoliselle, on erittäin tärkeää löytää hyvä kumppani. Jos jokin menee pieleen, voi yrityksen tietoturva vaarantua erittäin pahasti. Kuten tietohallinnon ulkoistamisessa tulee tietoturvankin johto pitää yrityksen sisällä. Kommunikointi on erittäin tärkeää. Ennen kuin tietoturva siirretään ulkopuoliseen yritykseen, täytyy olla tarkasti selvillä mitä halutaan. Tietoturvan ulkoistamiseen liittyy monia riskejä. Ulkoistuksen jälkeen voi käydä niin, että yrityksessä ei pidetä yllä tietotaitoa. Jos näin käy, ei voida enää olla varmoja, että tietoturva on riittävällä tasolla. Tietoturva muuttuu koko ajan, joten on erittäin tärkeää pysyä ajan tasalla. Ajankohtainen tieto auttaa myös ulkoisen yrityksen toiminnan tarkastelussa. Jos tietotaitoa ei ole, on mahdotonta tietää hoitaako ulkopuolinen tietoturvan hyvin vai huonosti. Tällöin ei voida myöskään tietää päivittääkö ulkopuolinen yritys tietoturvaa. On elintärkeää tietää missä mennään, jotta ei joudu luottamaan siihen mitä tietoturvan toimittaja sanoo. Kaikessa ulkoistamisessa on riskinsä, mutta tietoturvan ulkoistamisessa on, kuten voisi olettaakin todella suuret tietoturvariskit.

5.3.6 Ohjelmisto

Ohjelmistojen ulkoistaminen on erittäin yleistä, sillä harvalla yrityksellä on resursseja tehdä kaikki ohjelmistot itse. Ohjelmistojen hankintaan ei sinällään liity niin paljon riskejä, kuin muihin mahdollisiin ulkoistamisiin. Tämä ei kuitenkaan tarkoita, että niitä ei ole. Jos ohjelmistot sijaitsevat ulkoisen yrityksen palvelimilla, niin riskejä ovat esimerkiksi yhteyden katkeaminen ja palvelimien turvallisuus. Suurena riskinä on kuitenkin itse ohjelmiston tietoturva. Suurimpienkaan yrityksien tekemät sovellukset eivät välttämättä ole turvallisia. Esimerkiksi Oraclella on ollut suuria ongelmia Javan kanssa. Tämän takia onkin erittäin tärkeää tutustua ohjelmistoihin erittäin tarkasti. Yrityksen koko ei ole luotettavuuden tae. Siksi onkin aiheellista tutustua yrityksen ja ohjelmiston historiaan. Vanhaa ohjelmistoa ei kannata hankkia, koska se todennäköisemmin ei ole tietoturvallinen. Varsinkaan jos siihen ei enää tule päivityksiä. Uusimman mahdollisimman ohjelmiston valinta aiheuttaa myös ongelmia. Siinä voi olla ongelmia, joita valmistaja ei välttämättä ole huomannut. Ne voivat paitsi aiheuttaa sen, että ohjelma ei toimi kunnolla, mutta myös tietoturvariskejä.

5.3.7 Käyttöjärjestelmä

Ohjeessa puhuttiin aiemmin laitteiden ulkoistuksesta ja niiden tietoturvariskeistä. Siihen liittyy kuitenkin myös yksi toinen asia, nimittäin käyttöjärjestelmä ja sen päivittäminen. Aikaisemmin koneissa oli yksi käyttöjärjestelmä. Käyttöjärjestelmä vaihdettiin, kun koneet vaihdettiin uusiin. Nyt käyttöjärjestelmiä tulee kuitenkin uusia niin usein ja ne on mahdollista päivittää vanhaan koneeseen internetin välityksellä. Tämä aiheuttaa sen, että on vaikeampi päättää mitä käyttöjärjestelmää käytetään. Varsinkin Windowseissa tämä aiheuttaa ongelmia. Ohjeen kirjoituksen aikaan Windows 10 on ollut jo jonkin aikaa markkinoilla. Tänä aikana siinä on ollut useita ongelmia. Yksi niistä on laitteiston ajurit ja ohjelmistojen yhteensopivuus. Varsinkin vanhemmilla koneilla on käynyt niin, että kone kyllä pystyy pyörittämään käyttöjärjestelmää, mutta sen komponentteihin ei ole tullut ajureita kyseiselle käyttöjärjestelmälle. Tämän takia onkin tärkeää tutkia, löytyykö yrityksen käyttämille ohjelmille tukea uudelle käyttöjärjestelmälle. Jos laitteistoon ei löydy vielä ajureita tai ohjelmisto ei tue vielä käyttöjärjestelmää, on järkevämpää olla päivittämättä. Jos koneet päivitetään tarkistamatta, voi yrityksen toiminta hankaloitua erittäin paljon, pahimmassa tapauksessa pysähtyä kokonaan. Jos uudessa käyttöjärjestelmässä on joitakin ominaisuuksia, jotka hyödyttävät yritystä todella paljon, eikä odottaminen ole mahdollista. Tällöin voidaan ajatella uusien koneiden hankkimista uudella käyttöjärjestelmällä. Tämä ei kuitenkaan auta, jos ohjelmisto ei tue käyttöjärjestelmää.

5.3.8 Verkot

Yrityksen sisä- ja ulkoinen verkko voidaan ulkoistaa ja myös tähän liittyy riskejä. Verkot on tehtävä niin, että ne soveltuvat haluttuun tarkoitukseen. Yrityksessä pitää löytyä sen verran tietotaitoa verkoista, että tiedetään mitä halutaan. On myös erittäin tärkeää tarkistaa, että luotavasta verkosta tulee luotettava ja turvallinen. Jos verkko on tehty huonosti se voi kaatua rasituksesta, tai se voidaan murtaa. Jos näin käy yrityksen toiminta voi pysähtyä ja yrityksen tiedot voivat vaarantua. Riskinä on myös se, että verkon luontia ei dokumentoida kunnolla, jos näin käy, on vaikea tutkia miten verkko on tehty. Tämä vaikeuttaa verkon päivitystä ja sen korjausta ongelmatilanteissa. Verkkoja vaihdettaessa täyty muistaa suunnitella siirtovaihe erittäin tarkasti. Jos näin ei tehdä voi käydä niin, että vanha verkko ei ole enää käytössä ja uusi verkko ei ole vielä valmis. Verkkoa ei missään nimessä pidä ottaa käyttöön ennen kuin se on varmasti valmis. Keskeneräinen verkko ei välttämättä toimi kunnolla, eikä se luultavastikaan ole turvallinen käyttää.

5.3.9 Henkilöstö

Henkilöstöä voidaan myös ulkoistaa. Henkilöstön ulkoistaminen voi olla väliaikaista tai pitkäaikaista. Jokin työntekijä voi esimerkiksi voi sairastua ja sairauden ajaksi tarvitaan sijainen. Väliaikaiset sijaisuudet on hyvä miettiä etukäteen. Jos näin ei ole tehty, niin yrityksen toiminta hankaloituu. Jos tulee yllättävä tarve, mutta asiaa ei ole suunniteltu, voi sijaisen löytäminen olla hankalaa. Sijaisen pitää olla tietoinen yrityksen toimintatavoista ja pitää olla käytettävissä tarvittaessa. Vaikka sijainen löydettäisiinkin nopeasti, mutta sijainen ei ole tietoinen yrityksen toimintatavoista, niin moni asia voi mennä pieleen. Sijainen voi tehdä työtehtävät väärin, tai ainakin ne pitää selittää, mihin taas kuluu aikaa. Tämän takia onkin hyvä löytää hyvä yhteistyökumppani, joka pystyy tarjoamaan lisätyövoimaa tarvittaessa ja joka on tietoinen miten yritys toimii.

Tai sitten jonkin työntekijän tehtävät ulkoistetaan kokonaisuudessaan ulkoiseen yritykseen. Tässä tapauksessa pitää olla erityisen huolellinen. Lyhtyaikainen sijainen voi hankaloittaa toimintaa ja vaarantaa tietoturvaa, mutta tällöin henkilön voi helpommin vaihtaa toiseen. Pitkäaikainen ulkoistaminen on nimensä mukaisesti, ainakin toivottavasti pitkäaikainen ratkaisu. Siksi pitääkin tarkasti miettiä ulkoistetaanko maan sisällä, vai kenties ulkomaille asti. Ulkomailla työt voidaan tehdä halvemmin, mutta siitä aiheutuu myös lisää ongelmia. Kommunikointi ja valvominen hankaloituvat. Tämä voi vaatia enemmän resursseja, mitä pk-yrityksellä on varaa kuluttaa. Ulkoistaminen ulkomaille aiheuttaa myös enemmän tietoturvariskejä. Eri maissa ja eri yrityksissä on erilaiset käsitykset tietoturvasta. Jos ulkoistettu toiminto sijaitsee ulkomailla, on hankalampi valvoa miten tietoturva on siellä hoidettu ja on vaikeampi valvoa sen ylläpitoa. Toimintatapojen yhdistäminen voi

myös aiheuttaa ongelmia. Voi myös olla, että ulkomailla työ tulisi tehtyä nopeammin ja halvemmalla, mutta siinä on enemmän virheitä. Tai sitten mikään näistä riskeistä ei toteudu.

Yhteistyökumppanit tulee miettiä yrityksen toimintatapojen mukaan. Jos yritys toimii kansainvälisesti, ei ulkoistaminen ulkomaille välttämättä aiheuta suuria ongelmia ja tietoturva pysyy kunnossa. Jos taas yrityksellä ei ole ollenkaan kokemusta kansainvälisistä yhteistyökumppaneista missään muodossa, voi olla parempi miettiä ulkoistamista maan sisällä. Tai sitten voi olla parempi olla ulkoistamatta ollenkaan. Tämä täytyy miettiä yrityksen tarpeiden ja resurssien mukaan. Jos työtehtävän hoito yrityksen sisällä vaatii kaikki käytettävät resurssit, voi olla että ulkoistaminen vaatisi vielä lisää. On kuitenkin tärkeää miettiä pitkällä tähtäimellä. Voi olla, että prosessin aikana resurssit vaikuttavat loppuvan kesken ja ongelmia on enemmän kuin alun perin. Ulkoistamisen onnistumista voi ruveta miettimään vasta pitkälti prosessin loppumisen jälkeen.

5.4 Kokemuksen hyödyntäminen

Tietoturva ja ulkoistaminen ovat molemmat hankalia ja monimutkaisia asioita. Miten tahansa ne hoidetaankin voi tulla ongelmia. Ja kun ne yhdistetään, voi helposti syntyä suuria ongelmia. Siksi onkin tärkeää tietää, mitä tehdä. Kumpaankin asiaan soveltuu yksi hyvä neuvo, kysy apua. Ulkoistamista on tehty ennenkin kaikenkokoisissa yrityksissä. On erittäin todennäköistä, että yrityksellä on kontakteja muissa yrityksissä, joissa on aiemmin ulkoistettu. Näin voidaan oppia muiden tekemistä virheistä ja nähdä miten jokin on tehty onnistuneesti.

On turha yrittää selviytyä näin monimutkaisesta asiasta yksin. Pk-yrityksillä on rajallisesti resursseja ja kokemusta, mutta yhteistyön avulla näitä voidaan kasvattaa. Kenenkään ei esimerkiksi tarvitse enää keksiä pyörää uudelleen, vaan vanhaa kokemusta voidaan hyödyntää. Tämän vuoksi onkin tärkeää miettiä, onko yrityksen henkilökunnalla kontakteja joista voisi olla hyötyä. Ei kannata ainoastaan kysyä johtohenkilöiltä, vaan monipuolisesti kaikilta kontakteilta. Kukin työntekijä näkee ulkoistamisen toiminnan ja sen aiheuttamat seuraukset omalla tavallaan ja tätä kannattaa hyödyntää.

Ulkoistamisessa kannattaa ylipäätään kysyä mahdollisimman monen työntekijän mielipidettä. Tällöin voi tulla esiin asioita, joita yhdelle henkilölle ei olisi ikinä tullut mieleenkään. Täytyy kuitenkin ottaa huomioon tällöin väkisin eteen tuleva negatiivinen mielipide. Jos esimerkiksi työntekijä kokee, että häneltä lähtee työpaikka ulkoistamisen takia, on erittäin

todennäköistä, että hän on tällöin ulkoistamista vastaan. Siksi täytyykin miettiä miten ja milloin yrityksen henkilökunnan kontakteja käytetään hyödyksi.

Muiden yritysten kokemuksia tutkittaessa täytyy pitää mielessä, että ulkoistaminen on hyvin yksilöllinen prosessi. Mikä toimi jollekin yritykselle ei välttämättä toimi toiselle, tämän takia ei pidä suoraan kopioida sitä, mitä joku toinen on tehnyt, vaan pitää soveltaa. Muiden kokemuksen hyödyntäminen voi auttaa ulkoistamisprosessissa niin paljon, että sitä kannattaa ehdottomasti käyttää hyödyksi. Kunhan muistaa, että kaikki neuvot eivät välttämättä ole hyviä. Esimerkiksi pahimmalta kilpakumppanilta ei välttämättä kannata mennä kysymään neuvoja.

Kannattaa myös neuvoa muita ulkoistamisen jälkeen. Hyvä yhteistyö hyödyttää kaikkia ja koska ulkoistaminen tulee monille yrityksille eteen jossain vaiheessa, on neuvoista varmasti hyötyä ja niille on tarvetta.

6 Pohdinta

Opinnäytetyön tulokset ovat mielenkiintoisia. Osa niistä oli odotettuja, mutta osa tuloksista oli yllättäviä. Huolellinen suunnittelu ja ulkoistamisen pitkän aikavälin tavoitteet olivat odotettuja. Ulkoistajan vastuu taas tuli täytenä yllätyksenä. Suunnittelun tärkeys tuli ilmi nopeasti ja se on tärkeää koko ulkoistamisprosessin ajan. Suunnitelmia täytyy kuitenkin voida tarvittaessa muuttaa, tai kokonaan unohtaa. Suunnittelusta on hyötyä, mutta se voi myös rajoittaa, jos sen tekee väärin. Pitkän aikavälin tavoitteissa ei ollut mitään yllättävää, mutta se tulee kuitenkin aina pitää mielessä. Ulkoistajalla on enemmän vastuuta, kuin voisi luulla. Ulkoistajan täytyy valvoa, että ulkoinen yritys tekee sopimuksessa sovitut asiat, ja on myös lopulta vastuussa ulkoistamisen onnistumisesta.

Kaiken kaikkiaan opinnäytetyön tulokset osoittivat selvästi, mitä ulkoistettaessa tulee ottaa huomioon. Osa tuloksista oli ehkä hieman yllättäviä, mutta tulokset olivat selkeitä ja ne pohjautuivat selkeästi tietoperustaan. Ohjeen aiheen takia se soveltuu hyvin jatkokehitykseen. Aihealue on niin laaja, että keskittymiskohdetta vaihtamalla, voi helposti syventää tietoa johonkin toiseen osa-alueeseen, tai johonkin ohjeen osaan.

Selkeytensä vuoksi ohje soveltuu pk-yritysten käyttöön. Ohje ei kuitenkaan käsittele kaikkia mahdollisia näkökulmia ulkoistamisesta ja tietoturvasta. Tämä on hyvä ottaa huomioon ohjetta hyödynnettäessä. Tulokset olivat sen verran selkeitä, että ohje on sekä hyödynnettävä, että luotettava. Ohje on aiheeltaan erittäin ajankohtainen ja siksi myös tarpeellinen. Ulkoistamisen mahdollisuudet muuttuvat kuitenkin koko ajan, kuten myös tietoturva. Tä-

män takia ohjeella on rajallinen elinikä. Sekä ulkoistamisen, että tietoturvan perusperiaatteet tuskin kuitenkaan muuttuvat. Joten niiltä osin ohje tulee olemaan käyttökelpoinen pitkään.

Opinnäytetyön tekemisen aikana tapahtui paljon oppimista ja esille tuli uusia näkökulmia IT-alaan ja opinnäytetyön aihe-alueeseen. Opinnäytetyön tekeminen yhdessä työharjoittelun kanssa lisäsi tietoisuutta työelämän tavoitteista ja vaatimuksista. Opinnäytetyö myös anoit valmiudet mahdollisten samankaltaisten projektien tekemiseen työelämässä. Kirjoittamisprosessin aikana selvisi myös, mitä tämäntyyliseltä kirjoitelmalta vaaditaan. Kokonaisuudessaan opinnäytetyön tekeminen osoitti opintojen aikana saadut uudet kyvyt, sekä samalla lisäsi tietoisuutta omista kyvyistä ja mahdollisuuksista. Omat onnistumiset sekä virheet tuli käyttää hyödyksi ja ne tuli ymmärtää. Samalla tuli myös ymmärrystä siitä, miksi jokin asia meni pieleen ja miksi jokin onnistui.

Opinnäytetyön, työharjoittelun sekä koko opintojen aikana kävivät selväksi myös omat heikkoudet ja vahvuudet. Missä aihe-alueissa osaamista löytyy ja missä sitä on vähemmän. Opiskelu myös auttoi ymmärtämään omaa opiskeluprosessia paremmin. Opinnäytetyöprosessin aikana ja myös sitä ennen kävi myös selväksi se, että lopullinen osaaminen saavutetaan vasta työelämässä. Opiskelu voi valmentaa työelämään, mutta siinä opitaan vain perusteet. Lopullisesti ala opitaan työskentelemällä.

Opinnäytetyön tekemisen aikana suurin osa tehdyistä päätöksistä oli toimivia. Osa työskentelyn alussa kirjoitetuista kappaleista eivät kuitenkaan tukeneet lopullista työtä. Tämän takia niitä piti poistaa. Kappaleiden järjestykset myös vaikuttivat yhä huonommilta työn edetessä. Työn loppuvaiheessa pitikin muuttaa kappaleiden järjestystä ja osa kappaleista päätyi ihan toisen luvun alle. Osa kappaleista piti myös yhdistää. Työprosessin aikana työ kokonaisuutena huononi ja työn loppupuolella sitä oli pakko muokata, jotta kokonaisuus olisi yhtä hyvä kuin yksittäiset osat.

Opinnäytetyön tekemisen perusteet olivat kuitenkin toimivia. Myös aihe osoittautui hyväksi ja työskentelyprosessi oli toimiva. Kaikki valinnat eivät ehkä olleet toimivia, mutta epäonnistuneet valinnat auttoivat omassa kehityksessä. Virheet ja onnistumiset yhdessä auttoivat käsittämään kykyjä asiantuntijuuteen. Asiantuntijan tulee osata asiansa ja myös tietää se. Tarvittaessa tulee kuitenkin tunnustaa virheensä ja pystyttävä muuttamaan toimintatapojaan. Opinnäytetyöprosessi, työharjoittelu ja opinnot yhdessä auttoivat ymmärtämään mitä asiantuntijuudessa on kyse ja mitä tulee tavoitella.

Lähteet

Brand, D & Benvenuto, N. 2005. Information Systems Control Journal. Volume 5. Luettavissa: http://www.isaca.org/Journal/archives/2005/Volume-5/Pages/Outsourcing-A-Risk-Management-Perspective1.aspx. Luettu: 29.9.2015.

Crocker, S. 2015. ARPANET – The First Internet. Luettavissa: http://www.livinginternet.com/i/ii_arpanet.htm. Luettu 17.10.2015.

Global Outsourcing Agency. Advantages and Disadvantages of Outsourcing. Luettavissa: http://www.globaloutsourcingagency.com/adv.html. Luettu: 29.9.2015.

Kaskela, L. TIEKE Tietoyhteiskunnan kehittämiskeskus ry 8.8.2005. Luettavissa: http://www.tieke.fi/display/tiehan/Ulkoistamisen+vaihtoehdot. Luettu: 29:9.2015.

Kessler, G. 2015. An Overview of Cryptography. Luettavissa: http://www.garykessler.net/library/crypto.html. Luettu 17.10.2015.

Kuparinen, V-P. 2006. Ulkoistamisen hallittu prsessi. Luettavissa: http://www.huoltovarmuus.fi/static/pdf/360.pdf. Luettu: 24.11.2015.

Lommi, J. 2009. Suunnittelulla on merkittävä osa rakennusprojektissa. Luettavissa: http://www.rakennaoikein.fi/fi/artikkelit/suunnittelulla-merkitt%C3%A4v%C3%A4-osa-rakennusprojektissa. Luettu: 24.11.2015.

Tilastokeskus. PK–yritys. Luettavissa: http://www.stat.fi/meta/kas/pk_yritys.html. Luettu: 3.11.2015..

University of Miami. Confidentiality, Integrity and Availability (CIA). Luettavissa: http://it.med.miami.edu/x904.xml. Luettu: 17.10.2015.

Valtiovarainministeriö. 9/2008. Hankkeen tietoturvallisuuden osa-alueet. Valtionhallinnon tietoturvallisuuden johtoryhmä. VAHTI 9/2008. Helsinki. Luettavissa: https://www.vahtiohje.fi/web/guest/hankkeen-tietoturvallisuuden-osa-alueet. Luettu 8.12.2015

Valtiovarainministeriö. 3/2012. Teknisen ympäristön tietoturvataso-ohje. Valtionhallinnon tietoturvallisuuden johtoryhmä. VAHTI 9/2008. Suomen Yliopistopaino Oy - Juvenes Print, 2012. Luettavissa: https://www.vahtiohje.fi/web/guest/3/2012-teknisen-ymparistön-tietoturvataso-ohje. Luettu: 17.10.2015.

Valtiovarainministeriö. 6/2006. Tietoturvariskien hallinta sekä tietoturvallisuuden arviointi ja mittaaminen. Hallinnon kehittämisosasto. VAHTI 6/2006. Edita Prima Oy. Helsinki 2006. Luettavissa: https://www.vahtiohje.fi/web/guest/tietoturvariskien-hallinta-seka-tietoturvallisuuden-arviointi-ja-mittaaminen. Luettu 24.11.2015.

Valtiovarainministeriö. 7/2006. Ulkoistaminen keskeisenä muutostekijänä ja sen tietoturvavaikutuksia. Valtionhallinnon tietoturvallisuuden johtoryhmä. VAHTI 7/2006. Edita Prima Oy. Helsinki 2006. Luettavissa: https://www.vahtiohje.fi/web/guest/ulkoistaminen-keskeisena-muutostekijana-ja-sen-tietoturvavaikutuksia. Luettu: 29.9.2015.