Jussi Hartikainen

ICT-ULKOISTAMISEN HAASTEET INFORMAATIOTURVALLISUUDEN NÄKÖKULMASTA

Tietojenkäsittelytieteiden Pro Gradu

30. tammikuuta 2012

JYVÄSKYLÄN YLIOPISTO
TIETOIENKÄSITTELYTIETEIDEN LAITOS

TIIVISTELMÄ

Hartikainen, Jussi

ICT-ulkoistamisen haasteet informaatioturvallisuuden näkökulmasta
Jyväskylä: Jyväskylän yliopisto, 2012, 54 s.
Tietojenkäsittelytiede, pro gradu –tutkielma
Ohjaaja: Jari Veijalainen

ICT-ulkoistaminen on nopeasti kasvava ja kehittyvä liiketoiminnan alue. ICT-ulkoistamisen tasoja on useita, ja niihin kaikkiin liittyy informaatioturvallisuuteen kytkeytyviä haasteita.

Tutkielmassa käsitellään ICT-ulkoistamisen haasteita informaatioturvallisuuden näkökulmasta. Tutkimus on teoreettis-käsitteellinen kirjallisuuskatsaus johon sisältyy myös omia havaintoja ja pohdintoja, joita on verrattu aikaisempaan tutkimustietoon.

Tutkielmassa keskitytään ITIL-prosessikehyksen mukaiseen ulkoistamisen valmisteluun, käyttöönottoon ja kehitykseen. Erityistä huomiota saavat laitekokonaisuudet, henkilöstön käyttöoikeuksien hallinta, vikatilanteiden ideaalinen korjausprosessi ja sen kehittäminen sekä tiedotus, joita kaikkia käsitellään erityisesti informaatioturvallisuuden näkökulmasta.

Tutkielman tuloksista ilmenee, että ideaalinen ICT-ulkoistusprosessi vaatii testauksen lisäksi jatkuvaa, *ketterää* kehitystyötä asiakkaan kanssa, mutta myöskään viestinnän hyvää laatua ei tule väheksyä. ITIL-prosessikehyksestä ja sovituista aikarajoista ei saa tinkiä, ja siksi näiden aikarajojen on oltava realistisia.

Ennen kaikkea ulkoistamisen kaikissa osa-alueissa on otettava huomioon *asiakaslähtöinen* näkökulma. Ulkoistuksen palveluiden käytön sääntöjen tulee olla loppukäyttäjälle mahdollisimman yksinkertaisia, eikä loppukäyttäjän vastuulle tule jättää esimerkiksi harkintaa, missä vikatilanteissa tulee ottaa yhteyttä tiettyihin asiantuntijoihin. Vikatilanteen analysointi kuuluu aina ulkoistusyrityksen harteille, ITIL-prosessikehyksen mukaan ensisijaisesti palvelupisteeseen eli ensimmäisen asteen tukeen.

AVAINSANAT: ICT-ulkoistaminen, informaatioturvallisuus, käyttöönotto

ABSTRACT

Hartikainen, Jussi
ICT-outsourcing from the information security point of view

Jyväskylä University of Jyväskylä, 2012, 54 p.
Computer Science and Information Systems, Master's Thesis

ICT outsourcing is a rapidly growing and evolving area of ICT-business. ICT outsourcing has several levels, and they all linked to information security challenges.

This thesis deals with the challenges of ICT outsourcing, from the point of the information security view. The research is mainly a theoretical and conceptual review of the literature, bit it also includes observations and reflections of the author that have been compared to the research results in the literature.

This thesis relies on the ITIL process framework, as far as it deals with the outsourcing preparation, deployment and development. Special attention is given to information systems, especially their hardware configurations, access control of the personnel, ideal repairing process of faults and failures and its development, and the incidence notification process. These issues are handled specifically from the point of the information security.

The results show that an ideal ICT outsourcing process requires testing in addition to continuous, agile development with the customer, but good quality of communication should neither be underestimated. ITIL process framework and the agreed time limits must not be compromised, and because of this, time limits must be realistic.

Above all, the outsourcing in all areas must take into account a customer-oriented perspective. The rules of the outsourcing services use should be as simple as possible to the end user. For example, it is not end-user's responsibility to consider, when to contact which specialists in different fault situations. Responsibility for the fault analysis always remains at the company providing the outsourced services, according to the ITIL process framework. The customer should thus contact the service center or the primary support of the servicing company.

ESIPUHE

Aloittaessani Pro gradu –tutkielman tekemisen, työskentelin neljättä vuotta opintojeni ohessa yrityksessä X järjestelmäasiantuntijana. Järjestelmäasiantuntijat tekevät monimuotoisia ylläpito- ja asennustehtäviä asiakasyrityksille. Työskentelen päivittäin useiden asiakkaiden parissa ja minulla on vankka kokemus ICT-ulkoistamisesta, keskittyen erityisesti asiakasyritysten laitteiden automaattiseen valvontaan ja sen kehittämiseen. Työssäni olen havainnut, että informaatioturvallisuutta ei huomioida riittävästi käyttöönottoprojekteissa ja tästä nousi innostus tehdä tutkielma aiheesta.

SISÄLTÖ

TIIVISTELMÄ **2**

ABSTRACT **3**

ESIPUHE **4**

SISÄLTÖ **5**

LYHENNELUETTELO **7**

1 JOHDANTO **9**
1.1 Tutkimuksen taustaa 9
1.2 Tutkimusongelma ja rajaukset 10
1.3 ICT-ulkoistamisen yleinen kulku 10

2 ENNEN ICT-ULKOISTAMISEN KÄYTTÖÖNOTTOA **13**
2.1 ICT-ulkoistamisen taustaa 13
2.2 Ulkoistuksen osa-alueet 15
2.3 ICT-ulkoistuksen liiketoimintaan ja strategiaan liittyviä käsitteitä 16
2.4 Ulkoistuksen kustannukset 17
2.5 Ulkoistuspalveluja tarjoavan yrityksen toiminta eri ulkoistustilanteissa 17
2.5.1 Ensimmäisen asteen tuen prosessien tarkempi määrittely 20
2.5.2 Käytännön kriteerit ulkoistamisselvityksessä 21
2.6 Tietoturvapolitiikka 23
2.6.1 Tietoturvapolitiikka ITIL:n mukaan 24
2.7 Palvelun hallinta 25
2.8 Informaatioturvallisuuden taustaa 25
2.8.1 Salasanaturvallisuus 26
2.8.2 Tiedon muuntaminen 27
2.9 ITIL-prosessikehys 28
2.9.1 ITIL-turvallisuuden hallinta 30

3 MITÄ TOIMINTOJA ULKOISTETAAN **35**
3.1 Keskitetyt ja hajautetut järjestelmät 35
3.2 Käyttöönotto 38
3.3 Taustatietojen selvittämistä 38
3.4 Käyttöönoton aikana 40
3.5 Käyttöönoton päätyttyä 40

4 HYVÄ VIESTINTÄ ASIAKKAAN JA PALVELUA TARJOAVAN VÄLILLÄ **41**

4.1 Viestinnän eri tasot 41
4.2 Tulevaisuuden visioita 44
4.3 Muutoksiin varautuminen 44
4.4 Informaation jakaminen 45
4.4.1 Dokumentoinnin käyttöoikeuksien valvonta 45
4.4.2 Henkilöstöön kohdistuvat tekijät 46

5 KÄYTTÖÖNOTON JÄLKEEN 47
5.1 Palvelun jatkuvuus 47
5.2 Seurantapalaveri 48
5.3 Palvelun testaaminen 49

6 YHTEENVETO 50

LÄHTEET 52

LYHENNELUETTELO

AD

Active Directory on Microsoft Windows-toimialueen käyttäjätietokanta ja hakemistopalvelu joka voidaan suomentaa esimerkiksi *aktiivihakemistoksi*.

ICT

Information and Communication Technology, tieto- ja viestintäteknologia. Myös vanhaa termiä IT, information technology, käytetään usein.

IDS

Intrusion Detection System on tunkeutumisenhavaitsemisjärjestelmä Se voi olla laitteisto tai ohjelmisto tai rakentua näistä molemmista. Sen tarkoituksena on havaita tunkeutumiset tai niiden yritykset.

ITIL

Information Technology Infrastructure Library. *ITIL*® on prosessikehys, jonka avulla IT-palveluja ja niiden tuottamiseen tarvittavia prosesseja voidaan johtaa tehokkaasti.

OLA

Operational Level Agreement. Ulkoistusta tarjoavan yrityksen IT-osastojen välinen sopimus joka tukee SLA-sopimusta ja jonka noudattaminen mahdollistaa SLA:ssa sovitut palvelutasot. Tähän sisältyy esimerkiksi se, millä tavalla palvelinvastaavat päivittävät palvelimia, työasemavastaavat päivittävät työasemia ja tietokantavastaavat optimoivat tietokantoja.

PDU

Power Distribution Unit. Etähallittava virranjakelulaite. Tämän kautta sähköä saava laite voidaan sammuttaa kytkemällä PDU:sta virta pois etähallinnan kautta.

RSA

SecurID RSA Securityn valmistama laite, joka tuottaa valtuutusavaimia. Laitteen algoritmi tuottaa vaihtuvan salasanan minuutin välein. RSA on epäsymmetrinen julkisen avaimen salausalgoritmi.

sFlow

Teknologia, jolla verkkoliikennettä voidaan analysoida. Teknologia vaatii sFlow-tuen laitteelta, esimerkiksi kytkimeltä. Liikennekuormien lisäksi sFlow tuottaa raportteja siitä, millaisesta liikenteestä verkkokuorma koostuu, esimerkiksi http, ftp, sähköposti, pikaviestintä, p2p jne.

SLA

Service Level Agreement. Palvelutasosopimus. ICT-palvelusopimuksien palvelutaso ja laatukriteerit kattava sopimus, joka on ulkoistavan ja ulkoistuspalveluja tarjoavan yrityksen välinen.

SLM

Service Level Management. ICT-palvelun tason hallinta on yksi viidestä ITIL-palvelun toimittamisen prosesseista. SLM tarjoaa viitekehyksen, jonka avulla palveluita määritellään ja määrittelee, minkälaisia palvelun tasoja tarvitaan tukemaan liiketoimintaprosesseja. Siihen kuuluu myös monitorointi ja raportointijärjestelmä joka kertoo, pystyykö yritys tarjoamaan sovittua palveluntasoa. SLA ja OLA sopimukset rakentuvat SLM:n pohjalta.

SSL VPN

Secure Sockets Layer virtual private network. VPN-yhteys, joka voidaan muodostaa selaimella eikä se tarvitse varsinaista VPN-asiakasohjelmistoa.

Ulkoistusta tarjoava yritys

On tässä tutkielmassa yritys, joka tarjoaa ulkoistamispalveluita ICT-sektorilla.

Ulkoistava yritys

On tässä tutkielmassa yritys, joka ostaa ulkoistusta tarjoavalta yritykseltä palveluita ICT-sektorilta.

UPS

Uninterruptible Power Supply on järjestelmä tai laite, joka takaa tasaisen virransyötön lyhyissä sähkökatkoksissa ja tasaisen syöttöjännitteen häiriötilanteissa.

VPN

Virtual Private Network VPN verkko, avoimeen verkkoon tiettyjen käyttäjien välille muodostettu suljettu aliverkko, jonka sisäisessä liikenteessä käytetään salakirjoitusta ja käyttäjän todennusta, joten liikenne säilyy luottamuksellisena muilta avoimen verkon käyttäjiltä.

1 JOHDANTO

1.1 Tutkimuksen taustaa

Ulkoistaminen (outsourcing) on maailmanlaajuisesti yksi nopeimmin kasvavia ja kehittyviä liiketoiminnan alueita (Sloper 2004, 1). Vuonna 1996 ulkoistamisen kustannukset olivat yksin Länsi-Euroopassa 22,7 miljardia, kun vuonna 2001 kustannukset olivat 33,6 miljardia USA:n dollaria (Gonzalez, Gasco & Llopis 2005, 46). Ulkoistamisprosesseja ja tyypillisiä ulkoistetun IT-sektorin vastuualueita on olemassa useita ja olennaista onkin tässä yhteydessä määritellä, *mitä* ulkoistetaan. Tyypillisimmät ulkoistustavat on esitelty aliluvussa 2.4**.** On kuitenkin syytä huomata, että monesti ulkoistusprosessi on pikemminkin sekoitus erilaisia malleja kuin yhden ainoan IT-sektorin, esimerkiksi datan tai tietoliikennetoimintojen ulkoistamista.

Ulkoistaminen terminä on tullut käyttöön vasta 1990-luvulla, mutta itse toimintatapa on vanhempi ja on ollut yleisessä yrityskäytössä jo 1960- ja 1970-luvulla. Kuitenkin toiminnan luonne on muuttunut voimakkaasti: ennen pienet yritykset ostivat palveluja ja teknologioita jotka olivat yrityksen sisäisesti ulottumattomissa, mutta nykyään suuretkin yritykset ulkoistavat ICT-toimintojaan. Lisäksi ulkoistaminen koskee nykyään myös ICT-toimintoja, joilla on keskeinen rooli yrityksen kilpailukyvyssä (Gonzalez ym. 2005, 45).

Suurimpina syinä ulkoistamiselle voidaan nähdä esimerkiksi kasvaneet kustannukset, joiden takia yritys on kiinnostunut kustannustehokkaiden järjestelmien siirtämisestä ulkopuolisen toimitsijan konesaliin tai pilvipalvelun ostamisesta. Toisia syitä ovat kasvaneiden datamäärien käsittelyyn tarvittava laitteisto ja ammattitaito johon yrityksen oma henkilökunta ei ole välttämättä perehtynyt kovinkaan hyvin (Samarati; De Capitani di Vimercati 2010, 1). Lisäksi ulkoistaminen voi auttaa yritystä ydintoiminnan kehittämisessä, laadun paranemisessa ja riskien hallinnassa. Henkilöstön ammattitaitoon liittyen tarvitsee huolehtia myös kasvaneista verkkoturvallisuuden riskeistä. Esimerkiksi huonosti hoidetussa ja hajanaisessa verkkoympäristössä riski siitä, että tietokoneet muuttuvat roskapostittajiksi tai palvelunestohyökkäyksen toteuttajiksi on merkittävästi suurempi kuin ulkoistetussa ja hyvin hallitussa ympäristössä (Feamster, Nick 2010, 37).

ICT-ulkoistamisella (ICT-outsourcing) tarkoitetaan koko ICT-infrastruktuuriin tai sen erikseen määriteltyihin osiin liittyvien päätösten, liiketoimintaprosessien ja/tai palveluiden delegoimista tai siirtämistä ulkopuoliselle palveluntarjoajalle (Khidzir, Mohamed, Arshad 2010b, 194). Informaatioturvallisuudella voidaan tarkoittaa esimerkiksi yrityksessä menetelmiä ja käytäntöjä joilla taataan tiedon ja ICT-järjestelmien luottamuksellisuutta (confidentiality), saatavuutta (availability), eheyttä (integrity), kiistämättömyyttä (non-repudiation), vastuullisuutta (accountability), aitoutta (authenticity) ja luotettavuutta

(reliability) (Khidzir, Mohamed & Arshad 2010a, s. 235). Myös Andersonin mukaan informaatioturvallisuus pyrkii takaamaan tietojärjestelmien luotettavuuden, eheyden ja saatavuuden (Anderson, s. 308). Zwickyn Cooperin ja Chapmanin mukaan informaatioturvallisuudessa on aina kolme erillistä piirrettä joiden suojausta joudutaan erikseen miettimään (Zwicky, Cooper & Chapman, 2001, s. 28):

Tiedot: tietokoneiden sisältämä tieto

Resurssit: itse tietokoneet

Maine

Tähän listaan voidaan lisätä myös *verkon turvallisuusominaisuudet*. Esimerkiksi monissa valtion virastoissa on kielletty langattoman verkon käyttö, koska suojausominaisuuksistaan huolimatta se tarjoaa suuremmat edellytykset salakuuntelulle kuin kiinteä verkko. Langaton verkko voi olla myös väärin konfiguroitu tai salauksessa on käytetty liian alkeellista tai vanhaa tekniikkaa. Esimerkiksi WEP-salauksella toteutettu tietoliikenne on helposti salakuunneltavissa (Borisov, Goldberg & Wagner 2001).

1.2 **Tutkimusongelma ja rajaukset**

Tämän pro gradun tarkoituksena on kuvata ICT-ulkoistamisen eri vaiheita ja tarkastella niihin liittyviä haasteita informaatioturvallisuuden näkökulmasta. Tässä tutkielmassa oletetaan, että ulkoistavan asiakasyrityksen hallussa on informaatiota, jolla on rahallinen tai jokin muu arvo ja joka on salaista. Jos informaation arvo on nolla (tietoturvan, tiedon arkaluontoisuuden tai muun tärkeäksi koetun asian takia), silloin riski on myös nolla. Riski tarkoittaa tässä yhteydessä todennäköisyyttä, jolla jokin taho yrittää ohittaa turvatoimet (vastatoimet) ja saada haltuunsa informaatiota, jolla on arvoa.

Riskien painoarvo lisääntyy aina, kun uhkien määrä (esimerkiksi yrityksen tietojärjestelmiä vastaan suunnattujen hyökkäykset tietyllä aikavälillä), haavoittuvuuksien (vulnerability) määrä tai tietyn informaation arvon varastamisen tai korruptoimisen kustannukset lisääntyvät, mutta vähenee, kun vastatoimien määrä ja laatu kasvavat (Winkler 1997, s. 13).

1.3 **ICT-ulkoistamisen yleinen kulku**

Seuraavassa kuvaan yleisesti ICT-ulkoistamisen eri vaiheita yrityksessä X. Alussa ulkoistusta tarjoava yritys X tarjoaa asiakasyritykselle erilaisen paletin palveluja, niihin kuuluu yleisimmin ICT-infrastruktuurin monitorointi, helpdesk, ylläpito ja mahdollisesti koulutus. ICT-infrastruktuurin monitorointi käsittää ulkoistavan asiakkaan ympäristöön asennettavan tietokoneen, jolla monitoroidaan asiakkaan palvelimia, verkon aktiivilaitteita, tulostimia ja UPS-

laitteita. Lisäksi voidaan valvoa konesalin lämpötiloja ja kosteutta sekä havaita tulipalo tai vesivahinko. Monitorointiohjelmisto lähettää hälytyksiä yrityksen X vastuulla olevista virhetilanteista sähköpostitse ja SMS-viesteinä. Monitorointi toimii päivystäjän apuvälineenä yöaikaan, helpdeskin apuvälineenä päivän aikana sekä tarjoaa reaaliaikaista tietoa järjestelmien toiminnasta tietohallinnon erilaisiin käyttötarpeisiin.

Helpdesk-palvelussa asiakkaalle tarjotaan puhelintukea ja käyttäjätason oikeuksilla tapahtuvaa etätukea. Etätuki tarkoittaa yleensä sitä, että asiakkaan tietokoneelle muodostetaan etäyhteys puhelinsoiton aikana ja helpdesk voi käyttää asiakkaan tietokonetta verkon yli ja auttaa ongelmanselvityksessä.

Ylläpitoon kuuluvat asiantuntijapalvelut ja mahdollinen ympärivuorokautinen päivystys. Ylläpidossa on eri tasoja ja asiakas voi valita, haluaako hän reagoinnin vain päiväaikaan vai myös vuorokauden ympäri jokaisena päivänä. Ylläpitoon kuuluu myös asiakkaan ICT-infrastruktuurin kehittäminen ja yleensä nimetty järjestelmäasiantuntija, joka hoitaa enimmäkseen asiakkaalle tehtävien töiden suorittamisen.

Koulutus on yrityksen X tarjoamaa palvelua, jossa asiakasyrityksen edustajia koulutetaan esimerkiksi uuteen ohjelmistoversioon tai jonkin muun sovelluksen tai laitteen käyttöön.

Tarjouksen perusteella asiakas tilaa haluamansa palvelut. Ulkoistamisen taso vaihtelee: toisinaan asiakas haluaa tilata pelkästään ICT-infrastruktuurin monitorointipalvelun, jolloin hälytykset ohjataan asiakkaan omalle ICT-henkilöstölle. On olemassa myös asiakkaita jotka haluavat, että heidän ICT-infrastruktuurinsa ylläpito ja ongelmat siirretään kokonaan yrityksen X hoidettavaksi. Totaaliulkoistuksessa siirretään myös suurin osa asiakkaan palvelimista ulkoistusta tarjoavan yrityksen konesaliin. Yleisin tapaus on kuitenkin sellainen, jossa ICT-ulkoistaminen aloitetaan asteittain ja ulkoistamista lisätään yhteistyön edetessä.

Asiakkaan ja yrityksen X välille muodostetaan sopimus. Sopimukseen kuuluu osana salassapitosopimus sekä asiakkaasta riippuen mahdollisia sakkopykäliä. Joidenkin asiakkaiden tapauksessa salassapitosopimus tehdään asiakkaan ja yrityksen X työntekijän välille henkilökohtaisesti. Eräät asiakkaat vaativat yrityksen X työntekijöille suoritettavaksi suojelupoliisin henkilöselvityksen. Lisäksi asiakas saattaa vaatia, että yrityksen X työntekijä on suorittanut työturvallisuuskortin tai jonkin muun asiakkaan oman koulutuksen. Sopimuksen osana on räätälöity hinnasto tehtävistä töistä, vaste-aika, jolla työ aloitetaan sekä irtisanomisaika, tätä kutsutaan palvelutasosopimukseksi (SLA, Service Level Agreement).

Kun sopimus on allekirjoitettu ja ylläpidon taso on selvillä, voidaan siirtyä käyttöönottovaiheeseen. Tähän kuuluu yrityksen X tekemä kartoitus asiakkaan ICT-infrastruktuurista. Kartoitusvaiheessa selvitetään kaikki asiakkaan palvelimet, työasemat, kytkimet, palomuurit ja UPS:t. Palvelimista tarkastetaan

niiden ns. *care-packit*, eli millainen takuu palvelimilla on. Lisäksi käydään läpi palvelinten levyosiot, tuotantoon liittyvät erikoisohjelmistot, varmistuskäytännöt ja aktiivihakemisto (Active Directory). Käyttöönottovaiheessa asiakkaalla on tärkeä osa, koska asiakkaalla (tai asiakkaan edellisellä ICT-kumppanilla) on tässä vaiheessa paras tieto ICT-ympäristöstä. Käyttöönottovaiheessa asiakkaan ja yrityksen X välille muodostetaan perinteisesti lähiverkosta lähiverkkoon VPN-yhteys, jotta työtä voitaisiin tehdä mahdollisimman paljon etätyönä. Asiakkaan toimipisteet voivat sijaita ympäri maailmaa ja asiakkaat voivat itse tehdä töitä hotelleista tai muista erikseen määrittelemättömistä pisteistä, joten tietoliikenneyhteyksien hyvällä valvonnalla on tärkeä osa ulkoistamisprojektissa.

Käyttöönottovaiheen jälkeen yrityksellä X tulisi olla kattava dokumentaatio asiakkaan ICT-infrastruktuurista ja riittävän paljon tietoa, jotta yritys X kykenee hoitamaan ongelmatilanteita itsenäisesti ja huomauttamaan asiakkaalle investointitarpeista sekä kehittämiskohteista.

Käyttöönoton päätyttyä alkaa varsinainen ylläpito. Asiakkaan kanssa sovitaan seurantapalavereista, joissa yhteisiä pelisääntöjä tarkennetaan ja tarkastellaan käyttäjätyytyväisyyttä. ICT-infrastruktuurin monitorointi tuottaa raportteja, joista voidaan tarkastella millaisia hälytyksiä ympäristöön on liittynyt, miten hälytyksiin liittyviä raja-arvoja on muokattu ja minkälaisia kohteita valvontaan on lisätty.

Luvussa kaksi käsitellään ICT-ulkoistamisen käyttöönotossa huomioon otettavia seikkoja, joista tärkeimmät ovat tietoturvapolitiikka, käytännön kriteerejä ja ITIL-prosessikehyksen huomioimista. Kolmannessa luvussa käsitellään ulkoistettavia tietojärjestelmiä erityisesti laitetasolla. Luvussa neljä paneudutaan viestinnän ja infomaation jakamisen eri tasoihin ja muotoihin sekä näihin liittyviin käyttöoikeuksiin ja riskeihin. Viidennessä luvussa seurataan käyttöönoton jälkeistä kehitystä, salasana- ja verkkoturvallisuutta sekä näiden valvontaa.

2 ENNEN ICT-ULKOISTAMISEN KÄYTTÖÖNOTTOA

Tässä luvussa käsitellään tekijöitä, jotka tulee huomioida ennen ICT-ulkoistuksen aloittamista. Tärkeimmät hyödyt, joita ulkoistava yritys yrittää tällä muutoksella saada aikaan ovat palvelun parantaminen, ketterät resurssit, strateginen muutos ja mahdollisuus, kilpailuhyöty sekä parempi riskien hallinta (Sloper 2004, s. 35).

Erityisesti tarkastelun aiheena ovat kustannuskysymykset, eri ulkoistamisen tasot ja niiden tarkempi analysointi ja prosessikuvaus. Myös lakisääteisiä asioita analysoidaan sekä Suomen sisäisellä että kansainvälisellä tasolla. Tämä kaikki pyritään sulauttamaan ITIL-prosessikehykseen.

2.1 **ICT-ulkoistamisen taustaa**

Monissa yrityksissä on huomattu, että taloudellisesti voi olla järkevää ulkoistaa osittain tai kokonaan joitakin ICT-toimintoja. Varsinkin pienemmissä yrityksissä voidaan pyrkiä kaikkien ICT-toimintojen ulkoistamiseen, jolloin asiakkaan vastuulle jää vain toiminnan laadun valvominen. ICT-ulkoistaminen on ennen kaikkea asiakaslähtöistä liiketoimintaa, sillä ilman asiakkaan voimavaroja ei ole perustaa arvioida palvelun arvoa (Taylor, Case & Spalding, 2007e, s. 65). Näiden voimavarojen voidaan katsoa koostuvan esimerkiksi seuraavista elementeistä (Taylor, Case & Spalding, 2007f, s. 23):

Johto

Organisaatio

Prosessit

Tietotaito

Työvoima

Informaatio

Sovellukset

Infrastruktuuri

Pääoma

Näistä neljä ensimmäistä voidaan lukea yrityksen kykyihin, neljä jälkimmäistä resursseihin. Työvoiman voidaan katsoa kuuluvan molempiin sektoreihin (Taylor, Case & Spalding, 2007e, s. 38).

On tärkeää huomata, että kummankin sektorin tehokas toiminta on välttämätöntä yrityksen liiketoiminnalle. Vaikka sovellukset, infrastruktuuri ja

pääoma olisivat kunnossa, niitä ei pystytä kunnolla kohdentamaan ilman toimivaa johtoa, organisaatiota tai tietotaitoa.

Vaikka itse kustannukset ovat asiakkaan hyväksyttävissä, on ulkoistusta tarjoavan yrityksen suunniteltava näiden kustannusten minimointi asiakkaan kanssa, sillä etenkin pienemmissä yrityksissä ei yleensä ole kokemusta arvioida, kuinka paljon ICT-ulkoistukseen täytyy sijoittaa. Kustannustehokkuudeltaan alhaisella järjestelmällä on riskinsä sekä ulkoistusta tarjoavan yrityksen maineen että kilpailijoiden ratkaisuiden taholta.
ICT-ulkoistusta tarjoavien yritysten haasteet ovat melko samanlaiset kuin ydinliiketoimintaan keskittyvillä asiakasyrityksillä, sillä niiden täytyy analysoida ja koota palvelumallinsa aivan kuten muussa liiketoiminnassa. Niillä on yhteinen tarve hallita tekijöitä, jotka vaikuttavat kysyntään ja tarjontaan ja myydä toimintansa kustannustehokkaasti ja tehdä kulujen rakenne mahdollisimman läpinäkyväksi (Taylor, Case & Spalding, 2007e, s. 98), koska ainoastaan läpinäkyvyys takaa sen, että asiakasyrityksen johdolla on tarpeeksi tietoja ICT-palveluita koskeviin päätöksiin.

Kustannusten leikkausten lisäksi ICT-ulkoistamisella on kolme pääpiirrettä, jotka vaikuttavat asiakasyrityksen päätöksiin. Nämä ovat:

Palvelun saatavuus

Palvelun luotettavuus

Palvelun tehokkuus

(Taylor, Case & Spalding, 2007a, s. 66)

Näihin saatavuus- luotettavuus- ja tehokkuuspyrkimyksiin sekä kustannusleikkausten kysyntään tarjoavat ratkaisuja alalle erikoistuneet yritykset. Jyväskylän seudulla tällaisia isoja yrityksiä ovat esimerkiksi Enfo, Atea, Fujitsu ja Inmics Oy. Alalla on kova kilpailu myös Keski-Suomessa ja parhaan toimittajan valinta ei ole helppoa.

Toimittajan valinta perustuu ensinnäkin kilpailuttamiseen ja siihen liittyviin kustannuksiin. Kunnallisissa ja valtiollisissa organisaatioissa kilpailuttaminen on tarkasti lakisääteistä, mutta myös yksityiset yritykset kilpailuttavat palveluita järjestelmällisesti. Taloudellinen hyöty ei kuitenkaan ole ainoa syy toimittajan valintaan, vaan yrityksen täytyy luottaa siihen, että ulkoistettava palvelu toimii asianmukaisesti. Mikäli ICT-ulkoistamisesta ei ole aiempaa kokemusta, ulkoistusyrityksen maine ja pitkä kokemus alalla toimimisesta ovat tärkeitä tekijöitä valinnassa.

2.2 **Ulkoistuksen osa-alueet**

ICT-ulkoistaminen voidaan määritellä toiminnaksi, jossa ulkoinen toimija tarjoaa laitteisto- ja/tai henkilöstöresursseja, jotka liittyvät joko kaikkiin ICT-infrastruktuurin osiin tai sen tiettyyn osa-alueeseen (Gonzalez ym. 2005, s. 45).

ICT-ulkoistuksen osa-alueet voidaan jaotella esimerkiksi seuraavasti (Khidzir ym. 2010a, s. 194):

ISP (Internet Service Provider) eli yritys, joka tarjoaa asiakkailleen internet-yhteyden (Hunt, 2002, s. 89)

Webhotelli (web hosting) on palvelu, jossa asiakas vuokraa palveluntarjoajan www-palvelimelta kiintolevytilaa omia verkkosivujaan ja muita verkkopalveluja varten

ICT-sovellusten hallinta ja tuki

ICT-infrastruktuuri

Ohjelmointi

Elektroninen liiketoimintaratkaisu

Sovellusanalyysi, jossa ulkopuolinen konsultti määrittelee ohjelmiston hyödyt, kustannukset ja kehittämistarpeet

Sovellusten ylläpito

Loppukäyttäjän tuki, esimerkiksi helpdesk

Henkilöstön koulutus

ICT-turvallisuuden auditointi eli arviointipalvelu, tietoturvapolitiikka ja standardisointi

Eri ulkoistustapoja voidaan määritellä myös seuraavasti (Gonzalez ym. 2005, s. 45):

Liiketoimintaprosessien ulkoistaminen: tämä tarkoittaa ICT-ulkoistuksen tuen ja konsultoinnin yhdistämisen liiketoiminnalliseen ulkoistukseen

ASP (Application Service Provider)-ulkoistaminen jossa kolmas osapuoli jakelee, hallinnoi ja tarjoaa ohjelmistoja keskitetystä sijainnista pitkäaikaisella vuokrasopimuksella. Tämä voidaan toteuttaa myös pilvipalveluna software-as-a-service (SaaS), eli ohjelmisto hankitaan palveluna perinteisen lisenssipohjaisen tavan sijasta (Li ym., 2009, s. 1).

Sähköisen liiketoiminnan ulkoistamisessa jossa tarjotaan web-perustaisia sovelluksia, jotka mahdollistavat asiakasyrityksen siirtymisen sähköisen liiketoiminnan varaan.

Globaali ulkoistaminen. jolla tarkoitetaan tuotannon ja työpaikkojen siirtämistä ulkomaille (esimerkiksi Intiaan) joissa on käytettävissä hyvin koulutettua ja halpaa työvoimaa.

Tässä työssä käytetään Khidzirin luokittelua.

2.3 **ICT-ulkoistuksen liiketoimintaan ja strategiaan liittyviä käsitteitä**

Palvelun parantamisella tarkoitetaan laadun parantamista, vaste-aikojen normalisointia ja jatkuvuutta. Voidaan ottaa käyttöön uusia ominaisuuksia, kuten esimerkiksi ympärivuorokautisia valvontoja. Yrityksellä X on esimerkiksi tarjottavana huoltosopimus, jossa yritystä velvoitetaan reagoimaan virhetilanteiden sattuessa elintärkeiden palvelimien huoltamiseen neljän tunnin vasteajalla. Mikäli tätä vaatimusta ei pystytä ulkopuolisista toimitsijoista riippumatta sopimusaikana täyttämään, voidaan sopimuksessa yritys X velvoittaa rahallisiin hyvityksiin.

Palvelun ketteryys tarkoittaa resurssien ja palveluiden joustavuutta: poikkeustilanteiden varalla yrityksellä X on tarjottavana erillinen asiantuntija, joka ei kenties normaalitilanteessa työskentele ulkoistavan asiakasyrityksen ICT-infrastruktuurin kanssa. Tällä menetelmällä pystytään säästämään aikaa, koska sitä ei erikseen tarvitse varata normaalin ylläpitäjän ongelmanselvitykseen ja tarvittavan lisäkoulutuksen hankintaan. Tätä ketterää palveluntarjontaa voidaan soveltaa myös koulutukseen ja helpdesk-palveluihin.

Yrityksessä X on muun muassa helpdeskissä tarjolla korkealaatuista Office-osaamista, jota ei todennäköisesti ole yrityksen X järjestelmäasiantuntijoiden keskuudessa. Näin rikotaan perinteinen delegointikaavio, jossa haastavat ongelmat delegoidaan aina eteenpäin korkeamman tason ylläpitäjille. Joskus korkeamman tason järjestelmäasiantuntijat saavat delegoida osan selvitystyöstä helpdeskille.

Strateginen muutos ja tämän luomat mahdollisuudet tarkoittavat voimavarojen uudelleenorganisointia silmälläpitäen suurinta mahdollista tehokkuutta. Tässä strategiassa on huomioitava ensisijaisesti asiakaslähtöisyys: ulkoistava yritys ei ota kantaa yrityksen X resurssien joutoaikaan, vaan on kiinnostunut ainoastaan omien ongelmiensa vasteajoista ja palvelun laadusta niin sosiaalisessa kuin teknisessäkin mielessä. Käytännössä muutos näkyy tietohallinnon ydinosaamisen korostumisena helpdesk- ja ylläpitotoimien siirtyessä oman talon sisältä ulkopuolisille toimitsijoille.

Kilpailuhyötyä ulkoistava yritys saa kun ICT-järjestelmien käytettävyys paranee ja ongelmat ratkaistaan nopeammin. On huomattava, että investointivaiheessa yritys ei ole välttämättä kiinnostunut välittömistä rahallisista eduista vaan se voi pyrkiä pääsemään kilpailijoidensa edelle jopa rahallisin uhrauksin, koska tämän toivotaan tuottavan voittoa pitkällä aikavälillä.

Parempi riskienhallinta saavutetaan ennalta sovituilla vasteajoilla. Keskitetyllä konesalipalvelulla saavutetaan todennäköisemmin sovitut vasteajat, koska palvelimet ovat yhdessä sijainnissa ja ylläpitotiimillä on riittävä määrä sertifikaatteja ja osaamista yhdessä sijainnissa, jolloin asiantuntijoiden voimavarat saadaan keskitetymmin käyttöön ongelmatilanteissa.

2.4 **Ulkoistuksen kustannukset**

Usein ulkoistuksen aloituksen yhtenä perusteena on kustannusten leikkaaminen. Toisaalta, vaikka ulkoistuksen motiivina olisikin esimerkiksi palvelutason parantaminen, on siitä päättävien ihmisten tärkeää tietää kokonaiskustannusten ennuste. Kustannuksia ulkoistusta tarjoavalle yritykselle aiheuttavat seuraavat tekijät:

> *Työvoimakustannukset*: ulkoistuksen toteuttajien työvoimakustannukset sekä ulkoistuksesta huolehtivien sekä sitä johtavien työntekijöiden palkkakustannukset.
>
> *Työkaluihin liittyvät kustannukset*: ohjelmistojen ja laitteistojen hankinta, lisensiointi, asennus ja konfigurointi. Työkalujen räätälöinti ei kuulu tähän kuluerään. Työkalut voivat olla kustannuserä ulkoistusyritykselle, joka puolestaan laskuttaa eteenpäin ulkoistavaa yritystä.
>
> *Koulutuskustannukset*: kustannukset, jotka aiheutuvat yrityksen henkilöstön koulutuksesta, joka keskittyy teknisiin toimenpiteisiin, työkaluihin ja toimintatapoihin.
>
> *Erityisosaajien kustannukset*: kustannukset, jotka aiheutuvat asiantuntijoiden ja konsultaatioyrityksen suunnittelusta, toteutuksesta ja ylläpidosta.
>
> (Taylor, Case & Spalding, 2007a, s. 95)

Esimerkiksi ulkoistusta tarjoava yritys voi joutua pyytämään konsultointiapua Lotus Domino-sähköpostipalvelimen konfiguroinnissa siihen erikoistuneelta yritykseltä. Se voi joutua myös ostamaan palvelua liittyen VMware-virtualisointiin liittyvissä vaikeissa ongelmatilanteissa. Asiakasyrityksellä saattaa olla toive IBM Cognos-koulutuksesta ja tällöin ulkoistusta tarjoava yritys saattaa joutua ostamaan koulutuksen IBM-kumppanilta.

2.5 **Ulkoistuspalveluja tarjoavan yrityksen toiminta eri ulkoistustilanteissa**

ISP-palveluntarjoajan täytyy huolehtia ennen kaikkea riittävän selkeästä ja toimivasta automaattisesta hälytysjärjestelmästä ja palvelun vikaraporttipalvelusta, sillä monesti kaikissa ICT-toiminnoissa Internet-

yhteyden toimivuus on kriittinen osa-alue. Myös ulkoistusta tarjoavan yrityksen kannalta tiedotuksen pelisääntöjen on oltava selviä, koska verkkohteyden katkeamisen jälkeen helpdesk-palvelut voivat ruuhkautua. Voidaan esimerkiksi sopia, että yrityksen toimipisteiden sovittuja avainhenkilöitä tiedotetaan ensimmäiseksi, ja he levittävät tietoa eteenpäin. On pyrittävä välttämään esimerkiksi tilanteita, joissa verkkoyhteyden katkeamisesta ilmoitetaan ainoastaan tietyllä verkkosivulla, joka on toki välttämätön, mutta yksinään toteutettuna myös riittämätön toimenpide.

Web-hotellipalvelun tarjoajan täytyy huolehtia asiakkaan sivustojen toimivuudesta, koska WWW-sivut ovat tärkeä osa yrityksen julkista imagoa. Suurempien yritysten tapauksessa ne voivat sisältää joitakin palvelun kannalta kriittisiä toimintoja, kuten avainasiakkaiden verkkokaupan tai esimerkiksi SharePoint-tyylisiä raportointijärjestelmiä. Lisäksi on hyvä resurssien ja budjetin rajoissa tarkistaa, että eri domainpäätteet (.com, .org, .net) ovat myös yrityksen hallinnassa, ettei kolmas osapuoli pääse kyseenalaistamaan yrityksen mainetta, pakottamaan yrityksen ostamaan nämä domainit huomattavan kalliilla tai jopa asettamaan näille sivuille tiedon kalastelusovelluksia (phishing), joiden avulla avainasiakkaiden salasanat pyritään selvittämään.

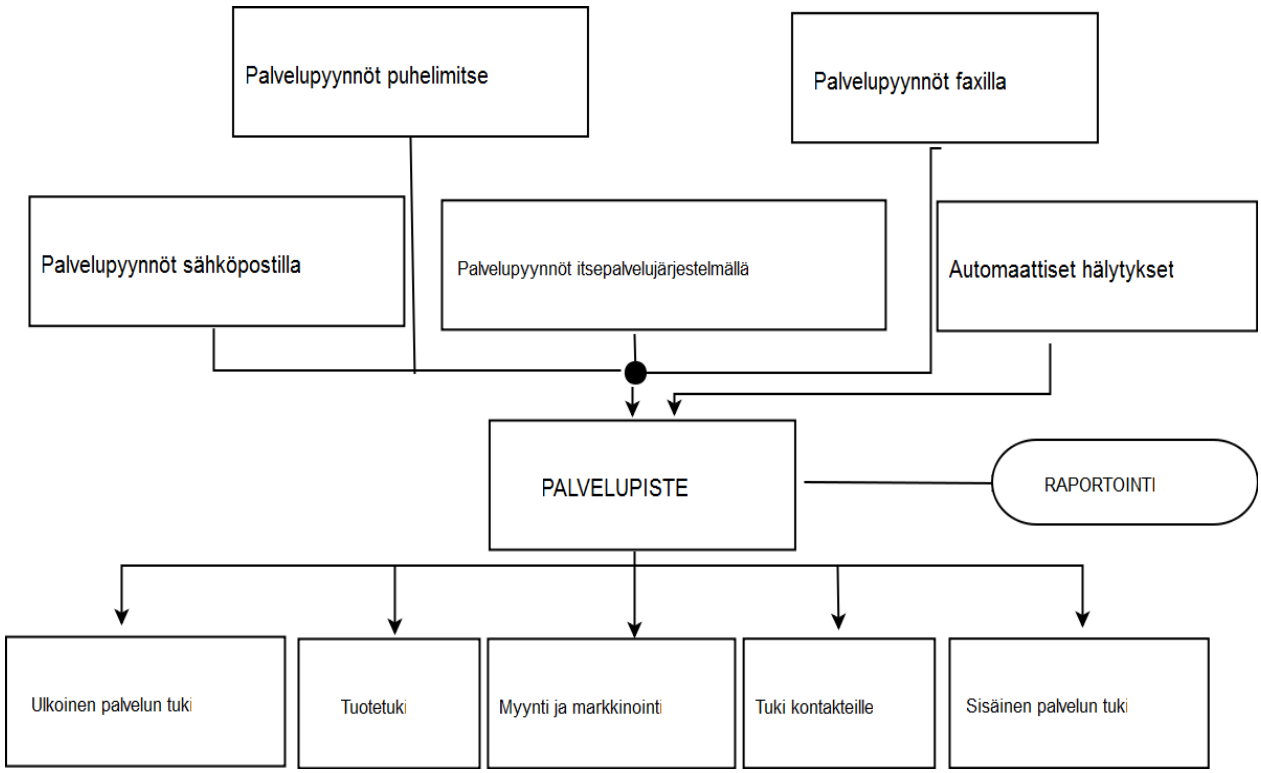
ICT-infrastruktuuripalvelu käsittää palvelimien ylläpitoa ja toiminnan valvomista sekä verkon topologian suunnittelua ja toteutusta. *ICT-sovellusten hallinta ja tuki* käsittelee yksityiskohtaisemmin palvelimilla olevien sovellusten, kuten sähköpostijärjestelmän ylläpitoa ja päivittämistä.

Ohjelmointipalvelu tarkoittaa sovellusten luontia ja muokkausta tilanteessa, jossa soveltuvaa sovellusta ei löydy valmiina sovelluskaupasta tai se halutaan jostain muusta syystä toteuttaa tai muokata itse. Esimerkiksi usein pelkkä SharePoint-alusta sellaisenaan ei ole riittävä yrityksen toimintaa ajatellen, vaan siihen täytyy erikseen kehittää yrityksen toimintaa palveleva kokonaisuus, kuten verkkokauppa tai toiminnanohjausjärjestelmä. Pidemmälle vietynä tästä voidaan käyttää myös termiä *elektroninen liiketoimintaratkaisu*. Pelkkä sovelluksen toteuttaminen ei riitä, vaan siihen täytyy tehdä myös päivityksiä ja muutoksia, jolloin puhutaan *sovelluksen ylläpidosta*. Tosin on huomattava, että sovellusta voidaan ylläpitää myös siinä tapauksessa, että se ei ole omaa tuotantoa. Laajempien ohjelmistokokonaisuuksien tapauksessa tulee tarpeelliseksi myös *sovellusanalyysi*, jossa pyritään käyttäjäkokemuksiin, teknisiin tietoihin, tietoturvapoikkeamiin ja vikatilanneraportteihin nojautuen ottamaan selville, mitkä sovelluksen ominaisuudet kaipaavat päivittämistä tai muutoksia.

Helpdesk-palvelu on tärkeää, jos yrityksen oman henkilökunnan taitotaso koneen arkikäytössä ei ole tyydyttävällä tasolla. Monesti helpdesk käsitetään toiminnoksi, jolla pystytään auttamaan käyttäjiä ainoastaan käyttäjän oikeuksien viitekehyksessä, jolloin helpdeskin tärkeimmäksi toiminnoksi tulee sovellusten käytön opastaminen, Windowsin vikatilojen esitutkinta ja reitittimien uudelleenkäynnistyksen neuvominen, mutta helpdesk voidaan

laajentaa myös *palvelupisteeksi*, jolloin ensimmäisen asteen tuen merkitys korostuu ja se pystyy ratkaisemaan myös korkeamman tason ongelmia, kuten ajurien päivitys, ohjelmien asennus tai koko käyttöjärjestelmän uudelleenasentaminen (Macfarlane & Rudd, 2005, s. 11)

Seuraavassa kuviossa on esitetty laajennetun helpdesk-palvelun eli palvelupisteen toiminta tapahtumien prosessinkäsittelyssä:



Kuvio 1. Tapahtumien rekisteröinnin syötteet (Macfarlane & Rudd, 2005, s. 12)

Henkilöstön koulutus tarkoittaa henkilöstön taitotason ylläpitämistä ja kehittämistä. Usein suorittavan työn tekijöillä tämä tarkoittaa esimerkiksi MS Officen hyötykäyttöä, tietoturvapolitiikan periaatteiden kertaamista (sähköpostin liitetiedostot, verkon käyttöperiaatteet jne), mutta varsinkin laajemmalla yrityksellä on myös erilaisten sovellusten pääkäyttäjiä, joiden osalta täytyy varmistaa, että heidän tekemänsä toimenpiteet, esimerkiksi käyttäjien lisääminen järjestelmään tai salasanojen vaihto, on ulkoistavan yrityksen periaatteiden mukaista. Usein myös tiedostojen varmistuksen manuaalinen työ, esimerkiksi varmistusnauhojen vaihto sovitun kierron mukaisesti, on ulkoistavan yrityksen työntekijän vastuulla. *ICT-turvallisuuden auditointi* on hyvä pyrkiä liittämään mukaan koulutukseen, jotta saataisiin tarkemmin selvyyttä ongelmakohdista, joihin käyttäjät usein kompastuvat. Tätä hyväksikäyttäen voidaan myös käyttäjien oikeuksia säätää siten, että tietoturvapoikkeamia ei päästä tekemään vahingossa, mutta on myös

muistettava, että järjestelmien käytettävyys poikkeustilanteissa on myös varmistettava.

2.5.1 Ensimmäisen asteen tuen prosessien tarkempi määrittely

Helpdeskin (helpdesk = opastuspuhelin) toiminnan mahdollisimman suuren tehokkuuden takaamiseksi asianmukaiset työvälineet ja teknologiat ovat avainasemassa. ITIL:in (alikulu 2.9.1) mukaan nämä teknologiat ovat seuraavia:

Puhelinjärjestelmä on elintärkeä osa ensimmäisen asteen tuen toimintaa. Toimivaa puhelinjärjestelmää edesauttavat seuraavat asiat:

> Automaattinen soitonohjaus eteenpäin, esimerkiksi asiakkaan syöttämien numeroiden tai äänenohjauksen avulla (Taylor, Case & Spalding, 2007d, s. 160). Tällä tavalla saadaan esimerkiksi laiteviat, Office-ongelmat ja sähköpostiongelmat eteenpäin ongelmiin perehtyneelle asiantuntijalle. Valikkojen riittävän suureen yksinkertaisuuteen on kiinnitettävä huomiota. Asiakasta ei saa päästää valinnan jälkeen ylemmän tason valikkoon, koska tämä tuottaa hämmennystä. Esimerkiksi yleiseen ensimmäisen asteen tukeen liittyvä valikon rakennevaihtoehto on esitetty kuviossa 8.
>
> Tietokonejärjestelmä, joka hakee esimerkiksi soittajien puhelinnumeron perusteella soittajan perustiedot ensimmäisen asteen tuelle
>
> VoIP-teknologia, joka voi merkittävästi vähentää puhelinkuluja
>
> Tilastollinen ohjelma, jonka avulla puhelinliikennettä voidaan tarkkailla ja tilastoida, esimerkiksi puheluiden lukumäärän, vastausaikojen, ohimenneiden puheluiden lukumäärän tai puheluiden keskimääräisen keston perusteella
>
> Hands-Free-laitteet, joiden avulla useammat työntekijät voivat kuunnella samaa puhelua, esimerkiksi uuden työntekijän perehdytystilanteessa.

Vikailmoitusten hallintajärjestelmän avulla ensimmäisen asteen tuki pystyy hallitsemaan vikatilanteitaan huomattavasti tehokkaammin ja etsimään asiakkaan edellisiä ratkaistuja palvelupyyntöjä (Taylor ym, 2007d, s. 160). Hallintajärjestelmä voi olla yrityksen itse rakentama ohjelmisto tai valmis tuote. Jälkimmäiset voivat olla joko ilmaisia tai kaupallisia sovelluksia.

Hallintajärjestelmässä on hyvä olla ratkaisuehdotusten tietokanta, joka toimii avainsanojen syötöllä. Tästä syystä myös ratkaistut ongelmat on syytä dokumentoida kunnolla ja vakiintunutta terminologiaa käyttäen.

Oma apu web-sivusto, josta käyttäjät voivat etsiä apua yleisiin ongelmatilanteisiin. Sivusto tulee olla saatavilla jatkuvasti ja voi sisältää esimerkiksi seuraavia asioita:

Usein kysytyt kysymykset

Ohjeita erilaisiin perustoimintoihin

Ilmoitustaulu jossa on tietoa ajankohtaisista asioista, esimerkiksi järjestelmiin liittyvistä suunnitelluista käyttökatkoista

Salasanan vaihtamisen mahdollistava palvelu, esimerkiksi sähköpostin salasanan vaihtaminen

Ohjelmistoihin liittyviä päivityksiä

Ohjelmistoihin liityviä automaattisia korjaustoimenpiteitä

Ohjelmistojen poisto- tai asennuspyyntöjä

Etähallinta on helpdeskin työväline jolla se saa etäyhteyden käyttäjän työasemalle (Taylor ym, 2007d, s. 161). Esimerkkejä tällaisista ohjelmistoista ovat Remoteus, Teamviewer ja VNC.

2.5.2 Käytännön kriteerit ulkoistamisselvityksessä

Asiakasyrityksen tulisi selvittää mahdollisimman paljon taustatietoja yrityksestä X: millaisia asiakkaita yrityksellä X on ennestään, noudattaako yritys X ITIL-prosessikehystä (aliluku 2.9) toiminnassaan ja kuinka kauan yritys X on toiminut alalla, kuinka iso yritys X on ja onko yritys osa suurempaa konsernia.

Oma kokemus on osoittanut, että kun ICT-ratkaisujen kokonaistoimittaja fuusioidaan, muutokset asiantuntijapalveluissa voivat olla negatiivisia ainakin lyhyellä aikavälillä. Esimerkiksi teleoperaattorin ostaessa ICT-ratkaisujen toimittajan, ICT-ratkaisujen toimittajan entiset asiakkaat saattavat harkita sopimuksensa irtisanomista. Tämä voi johtua siitä, että kun palveluiden kirjo lisääntyy, sen hallinta muuttuu yhä vaativammaksi (Taylor ym, 2007f, s. 205).

Vaikka sertifikaattien ja työkokemuksen perusteella uudella ICT-ratkaisujen toimittajalla voisi olla enemmän resursseja ongelmatilanteiden ratkaisemiseen, aikaisemmin toimineessa ylläpitoyrityksessä on kuitenkin ollut paljon *hiljaista tietoa (tacit knowledge)*, joka yksinkertaisuudestaan huolimatta saattaa olla hyvinkin kriittistä, kuten esimerkiksi vähän käytettyjen järjestelmien ylläpitäjien henkilöllisyys, palvelimien ja palomuurien fyysinen sijainti, yrityksen sisäiset toimintatavat joista ei ole tehty dokumentaatiota tai vaikka opitut sosiaaliset taidot asiakkaan yrityksen ICT-hallinnon kautta.

Tärkeitä muita selvityksiä ovat yrityksen X muut kumppanit, kumppanuustasot laite- ja ohjelmistovalmistajien kanssa sekä muut referenssit. Esimerkiksi metallialan ulkoistaja voi kiinnittää huomiota siihen, onko yrityksellä X ylläpidossaan jo muita saman alan yrityksiä. Tällöin yrityksestä X saa sellaisen kuvan, että sillä on myös kenttäkokemusta alan yritysten toimitavoista, tiloista

ja kriittisistä ICT-ongelmista jotka voivat vaikuttaa yrityksen tuotantoprosesseihin.

Laite- ja ohjelmistovalmistajilla on tapana järjestää koulutuksia koskien tuotteitaan. Näitä koulutuksia käymällä yrityksen työntekijät voivat saada sertifikaatteja ja nämä vaikuttavat siihen millainen kumppanuustaso yrityksellä X on esimerkiksi Microsoftin tai VMwaren kanssa. Tämä kumppanuustaso on jonkinlainen indikaattori siitä millaista teknistä osaamista yrityksessä on.

Lisäksi asiakkaan tulisi selvittää yrityksen X kilpailijat ja selvittää samat asiat niistä. Asiakasyrityksen on hyvä tarkastaa oma tietoturvapolitiikkansa ennen ICT-ulkoistamista, näin asiakkaalle muodostuu paremmin käsitys siitä kuinka yritys X:n tarjous tukee nykyistä tietoturvapolitiikkaa. Tietoturvapolitiikaksi määritellään esimerkiksi johdon kannanotto, joka määrittelee tietojen turvaamisen tavoitteet, vastuut ja toteutuskeinot (aliluku 2.6.1). Tietoturvapolitiikka määräytyy ensisijaisesti sen ympäristön mukaan, missä informaatiota käsitellään. Lisäksi informaation luottamuksellisuus, eheys ja saatavuus vaikuttavat tietoturvapolitiikkaan. Jatkuva uusien teknologioiden kehittyminen, yhteiskunnalliset muutokset ja käyttäjien muuttuvat vaatimukset edellyttävät tietoturvapolitiikan jatkuvaa kehittämistä (Klaic & Hadjina 2011, s. 1532).

Jun Lin ym. mukaan tiedon varmuus taataan seuraavilla vaatimuksilla (Li ym. s. 3-4):

> Yksityisyyden vaatimukset: esimerkiksi maantieteellinen sijainti (EU, IVY-maat, Kiina) ja siihen liittyvät oletusarvoiset lait, jotka liittyvät tietoturvaan, yrityksien hyväksymät standardit ja yritysten ilmoitusvelvollisuus datavuodon tapahtuessa vaikuttavat oleellisesti näihin vaatimuksiin.
>
> Datan siirtymisen vaatimukset: ennen siirtoa täytyy selvittää vaatimukset jotka liittyvät datan siirron turvalliseen välittämiseen. Myös sen varmistaminen, että ainoastaan valtuutetut henkilöt pääsevät dataan käsiksi, on olennaista. Lisäksi on kontrolloitava datan siirtymiseen liittyvien kolmansien osapuolien saama tieto siitä. Myös eri osapuolten on saatava tieto toimintatavoista joilla dataa siirretään.
>
> Datan säilyttäminen: datalla on tietty elinikä, täytyy tietää milloin data tuhotaan kun sitä ei enää tarvita ja että siitä saadaan ilmoitus.
>
> Datan luottamuksellisuus: data täytyy salakirjoittaa säilytettäessä ja siirrettäessä.
>
> Datan saatavuus: data täytyy olla saatavilla niille osapuolille jotka ovat siihen oikeutettuja ja saatavuutta täytyy voida valvoa.
>
> Datan eheys: eheyden takaamiseksi täytyy suorittaa testejä jotta eheys voidaan taata.

Tarkoituksenmukainen käyttö: kaikkien osapuolten ajankohtaisissa tiedoissa on varmennettava, että data on päivitettyä ja validia.

2.6 **Tietoturvapolitiikka**

Tietoturvapolitiikka sisältää käytäntöjä ja sääntöjä joilla informaatioturvallisuutta pyritään hallitsemaan. Säännösten noudattamisella ja sertifioinnilla on tärkeä merkitys tietoturvapolitiikan onnistumiselle. Esimerkiksi turvallisuusstandardi ISO 27001-2 suosittelee parhaita käytäntöjä menestyksekkääseen tietoturvan hallintaan (Onwubiko & Lenaghan 2009, s. 381). Myös ITIL-prosessikehyksen turvallisuuden hallinta perustuu ISO 27001-standardiin ja sitä voidaan hyödyntää laadittaessa tai tarkasteltaessa tietoturvapolitiikkaa (aliluku 2.9.1). Esittelen seuraavassa hyvän luokituksen kriteereitä joita voidaan käyttää tietoturvapolitiikan laatimisessa.

Tavoitteet voivat olla joko intentionaalisia tai ekstensionaalisia. Intensionaaliset käsitteet luonnehtivat niitä ominaisuuksia, jotka vaaditaan kaikille tietoturvapolitiikan vastuualueelle kuuluviin olioihin (Järvinen & Järvinen 2004, s. 21), kuten käyttäjiin, työasemiin tai mobiililaitteisiin. Esimerkiksi työasemilta voidaan vaatia hyvää salasanojen keskitettyä hallintaa, tai kaikilta olioilta voidaan vaatia tietyn laatujärjestelmän mukaista toimintaa.

Käsitteen ekstensio eli ala on niiden olioiden joukko, johon käsitettä (tietoturvapolitiikka) voidaan soveltaa (Järvinen & Järvinen 2004, s. 21), esimerkiksi WWW-selaimen käyttö, salassapitovelvollisuussopimus tai reititin.

Intentionaalisten ja ekstensionaalisten tietoturvapoliittisten tavoitteisiin kuuluvat mm. kattavuus, pysyvyys ja yhteispisteettömyys (Järvinen & Järvinen 2004, s. 21). Taksonomisessa tarkastelussa kattavuus ja pysyvyys ovat tietoturva-alalla ongelmallisia alan nopeasti muuttuvan ja kehittyvän teknologian takia, joten on syytä panostaa *yhteispisteettömyyteen*. Yhteispisteettömyydellä tarkoitetaan sitä, että yhteen olioon, johon sovelletaan tiettyä intensiota (esimerkiksi tietoturvaton WWW-selain) ei ole olemassa kahta erilaista ohjesääntöä, jonka mukaan ongelma täytyy ratkaista. Esimerkiksi tietoturvattoman WWW-selaimen tapauksessa ongelmanratkaisuna voivat olla mm. selaimen päivitys uudempaan versioon tai palomuurin konfigurointi. Yhteispisteetön tietoturvapolitiikka antaa yksikäsitteiset toimintaohjeet vikatilanteisiin, on ristiriidaton ja säästää aikaa sekä kustannuksia.

Yhteispisteettömyyden vaatimus edellyttää tietoturvapolitiikan laatijalta jatkuvaa uudelleenkouluttautumista olemassa oleviin tietojärjestelmiin sekä myös käsitteellistä hahmotuskykyä. Suuremmassa organisaatiossa on tarpeellista kehittää tietoturvaprosessit oman prosessikehyksen, esimerkiksi ITIL:in mukaiseksi (aliluku 2.9).

2.6.1 Tietoturvapolitiikka ITIL:n mukaan

Informaatioturvallisuuden hallinta tulisi olla rakentunut tietoturvapolitiikkaan ja erityisiin turvallisuusjärjestelyihin. Parhaassa tapauksessa tietoturvapolitiikalla ja turvallisuusjärjestelyillä on täysi tuki tietohallinnon johdolta ja sillä tulisi olla myös ylimmän yritysjohdon tuki. Tietoturvapolitiikan tulisi kattaa kaikki informaatioturvallisuuden osa-alueet ja sen tulisi sisältää seuraavat kohdat (Taylor, Case & Spalding, 2007c, s. 142):

- Yleinen tietoturvapolitiikka
- Tietoturvapolitiikan oikea käyttö
- Pääsynhallinnan politiikka
- Salasanapolitiikka
- Politiikka sähköpostin käytöstä ja käsittelystä
- Internetin käyttöpolitiikka
- Antiviruspolitiikka
- Informaation luokittelu (esimerkiksi julkinen, sisäinen, sisäisesti rajattu, erittäin salainen)
- Dokumentin luokittelu (esimerkiksi julkinen, sisäinen, sisäisesti rajattu, erittäin salainen)
- Etäkäytön säännöt
- Kolmannen osapuolen pääsynhallinta järjestelemiin
- Tietoaineiston käytöstä poisto ja hävittäminen

Näiden säännöstöjen tulee olla saatavilla asiakkaille ja käyttäjille. Säännöstöjen tulee olla johdon hyväksymiä ja niitä on tarkastettava tarvittaessa, mutta vähintään kerran vuodessa.

On huomattava, että liian tiukka politiikka voi haitata käytettävyyttä. Tyypillisesti kolmannen osapuolen pääsynhallinta toteutetaan VPN-yhteydellä. Toteutuksesta riippuen käytettävyys vaihtelee hyvin paljon. Esimerkiksi SonicWALL:n Aventail SSL VPN-toteutus (Sonicwall kotisivu 2011) voi vaatia käyttäjältä tietyn antivirusohjelmiston ajantasaisilla virustunnisteilla, tietyn käyttöjärjestelmän ja sen ajantasaiset päivitykset, PIN koodin, RSA SecurID token-salasanan ja monivaiheisen kirjautumisen.

Sähköpostiin liittyvää käyttöä hankaloittava seikka on liitetiedostojen suodatus sähköposteista. Suodatusta voidaan tehdä esimerkiksi tiedostopäätteiden perusteella. Suodatus voi pureutua myös pakattujen liitetiedostojen sisälle sekä analysoida tiedoston päätteestä huolimatta, onko se vaarallisten listalla. Tämä saattaa hankaloittaa joissain tapauksissa materiaalin toimittamista kumppaneiden välillä.

2.7 **Palvelun hallinta**

Palvelulla tarkoitetaan niitä asiakkaalle toteutettuja keinoja, joiden avulla asiakas saa haluamansa lisäarvon, mutta välttää samalla tiettyjä riskejä joita liittyy palvelun toteuttamisessa tarvittaviin laitteisiin ja henkilökuntaan (Taylor ym, 2007d, s. 11). Erityisen tärkeää palvelun toteuttamisessa on operationaalisen ja strategisen hallinnan yhteistyö, jonka yksityiskohtia kuvaillaan seuraavassa kuviossa:

Kuvio 2. Operationaalisen ja strategisen hallinnan yhteistyössä esiin nousevia kysymyksiä ja vastauksia niihin (Taylor ym, 2007d, s. 12).

2.8 **Informaatioturvallisuuden taustaa**

Tässä tutkielmassa määritellään informaatioturvallisuus Yhdysvaltojen lakia mukaillen: informaatioturvallisuus on informaation ja tietojärjestelmien turvaamista luvattomalta pääsyltä, käytöltä, häirinnältä, muuntamiselta tai tuhoamiselta (Andress 2011, s. 2).

Yksinkertaisin esimerkki luvattomasta pääsystä ja käytöstä on toisen ihmisen käyttäjätunnuksen käyttäminen tai tämän käyttöoikeuksien saaminen itselleen luvattomin keinoin (salasanan brute force-murtaminen, olan yli salasanan vakoileminen, lukitsemattomalle tietokoneelle istuminen tai sellaisten dokumenttien lukeminen, johon omilla käyttövaltuuksilla ei ole lupaa). Tietojen muuntaminen ja tuhoaminen on erilaisin keinoin tapahtuvaa tiedostojen,

lokitietojen tai asiakirjojen muuttamista tai tuhoamista. Tietojärjestelmien häirintää ovat esimerkiksi hajautetut palvelunestohyökkäykset (DDOS, Distributed Denial Of Service), jossa pyritään useista koneista yhtäaikaisesti lähettämään palvelimelle yhteyspyyntöjä, jolloin palvelimen kuormittuessa myös oikeiden henkilöiden yhteyspyynnöt palvelulle viivästyvät tai lakkaavat toimimasta kokonaan (Andress 2011, s. 115).

Baldwin A (Baldwin ym. 2006, s. 53) mainitsee, että huolimatta laajasta levinneisyydestään, ISO27000-2-standardin sisältö, joka perustuu Iso-Britannialaiseen standardiin BS7799, on jäänyt suureksi osaksi huomioimatta niiden henkilöiden parissa, jotka vastaavat organisaationsa informaatioturvallisuudesta. Vain yksi ihminen kymmenestä on tietoinen standardin sisällöstä (Baldwin ym. 2006, s. 53). Vaikka oma tarkasteluni perustuu ITILin tarkoista prosessikohtaisista ohjeista kootulle standardille BS15000 (Mscfarlane & Rudd 2005, s. 5), voidaan tästä tutkimuksesta kuitenkin päätellä joitakin suuntaviivoja: IT-standardit eivät yleensäkään ole kovin tunnettuja informaatioturvallisuuden päättäjien keskuudessa.

Huonosti toteutettu ICT-ulkoistus voi johtaa katastrofiin erityisesti, jos informaatioturvallisuutta ei huomioida riittävästi. Esimerkiksi, jos ulkoistetussa ICT-infrastruktuurissa on laiminlyöty palomuuri, tunkeutumisen mahdollisuus tietoverkkoon kasvaa (Zwicky ym., s. 33). Ongelmat voivat johtua monesta muustakin seikasta, kuten esimerkiksi puutteellisesta käyttöönotosta tai ICT-ulkoistusta tarjoavan yrityksen ammattitaidon puutteesta.

Kokemus on osoittanut, että pienet ja jopa keskisuuret yritykset vaihtavat herkästi ICT-ratkaisujen toimittajaa, jos ne eivät ole tarpeeksi tyytyväisiä palvelun tasoon tai teknisiin toteutuksiin. Kokemuspohjaisena esimerkkinä mainittakoon sähköpostin tai verkkoyhteyksien toiminta; usean päivän katkokset verkkoyhteyksissä tai sähköpostissa hermostuttavat yrityksen henkilökuntaa hyvin voimakkaasti. Myös tiedon muuntamiseen liittyvät asiat voivat vaikuttaa (aliluku 2.8.2). Palvelun hinta ei ole yleensä ensimmäinen kriteeri palveluntarjoajan vaihtamiselle. Vaihtaminen on kuitenkin asiakasyritykselle haasteellista ja myös kallista, koska yleensä käyttöönotto laskutetaan asiakkaalta. Alalla on paljon eritasoisia toimijoita ja valinta voi olla vaikea, varsinkin jos asiakkaan sisäinen ICT-tietotaito on alhaisella tasolla.

2.8.1 Salasanaturvallisuus

Jokainen salasana on tietynmittainen joukko merkkejä. Esimerkiksi kaikkien kuuden merkin mittaisten a-z-aakkosiin rajoittuneiden salasanojen mahdollinen määrä on 26^6=308 915 776. Mikäli kirjainkoko ratkaisee, eli otetaan käyttöön isot ja pienet kirjaimet, on salasanojen mahdollinen määrä 52^6=1 9770 609 664. Näiden lukujen välillä on 64-kertainen ero, mikä merkitsee 64 kertaa pidempää keskimääräistä aikaa brute-force-hyökkäyksessä. Ottamalla huomioon erikoismerkit, mahdollisten salasanojen joukko lisääntyy entisestään.

On kuitenkin huomattava, että pelkästään tekninen salasanojen monimutkaisuus ei riitä, vaan käyttäjiä on koulutettava siihen, ettei salasana ole esimerkiksi selvä suomenkielinen tai englanninkielinen sana: monet brute-force-ohjelmat kokeilevat läpi erilaisia sanastoja, joten jollakin kielellä jotain tarkoittava pitkäkin sana on hyvin tietoturvaton vaihtoehto salasanaksi. Tällaisen hyökkäyksen onnistumisen todennäköisyys on yrityksestä riippuen 20-50% (Winkler 1997, s. 129). On huolehdittava ohjelmatasolla, ettei salasana voi olla myöskään sama kuin käyttäjätunnus tai samankaltainen viimeksi käytettyjen salasanojen kanssa.

Esimerkkinä voidaan mainita yrityksen Active Directory-salasanapolitiikka: Active Directoryssa on mahdollisuuksia laatia tiukkoja salasanan vaihtamiskriteereitä, jotka liittyvät erikoismerkkeihin, salasanan pituuksiin ja samankaltaisuuksiin edellisten salasanojen kanssa. On kuitenkin huolehdittava myös siitä, että salasanapolitiikka ei saa olla liian tiukka: jos järjestelmä vaatii salasanaan useamman erikoismerkin kokonaisuuden, voi käyttäjälle tulla houkutus kirjoittaa salasanoja muistilapuille, matkapuhelimeen tai sähköpostiin, mikä taas on ehdottomasti tietoturvaa heikentävä tekijä.

On tärkeää pyrkiä pois sovelluksiin sisäänrakennetuista kovakoodatuista (hard-coded) salasanoista joita ei voi vaihtaa (Andress, 2011, s. 151).

2.8.2 Tiedon muuntaminen

Muuntamishyökkäykset pyrkivät järkyttämään tietojärjestelmien eheyttä muuttamalla kriittisiä teknisiä yksityiskohtia (Andress 2011, s. 9). Toisenlaisena esimerkkinä tästä voidaan mainita tahaton informaation muuntaminen. Tällaisessa tapauksessa ICT-ulkoistusta tarjoava sekoittaa henkilöiden yhteystietoja, laitteiden IP- tai MAC-osoitteita aiheuttaen kommunikointivirheitä eri laitteiden tai ihmisten välillä tai kokonaan järjestelmän osittaista toimimattomuutta.

Tiedon muuntuminen voi olla myös tahatonta, jolloin tiedon konteksti voi muuttua kielteiseen suuntaan. Esimerkiksi automaattisissa sähköposti- tai tekstiviestihälytysjärjestelmissä ei haluta vastaanottajan tietoon ICT-ulkoistuksen toteuttajan tietoja, koska useimmiten yritysjohto haluaa säilyttää vaikutelman oman ICT-infrastruktuurin itsenäisyydestä. Samasta syystä esimerkiksi sähköpostiviestien halutaan lähtevän asiakasyrityksen omasta, eikä ICT-ulkoistajan domainista. Domainien ja muiden lisätietojen vaikutuksista johtuva tiedon kontekstin muuntuminen voi johtaa asiakkaiden yritystä koskevan ammattitaidon kyseenalaistamiseen. Esimerkiksi helpdeskin lähettämän tiedotteen toivotaan yleensä tulevan osoitteesta, joka on muotoa helpdesk@ulkoistava_yritys.fi eikä osoitteesta helpdesk@ulkoistusta_tarjoava_yritys.fi.

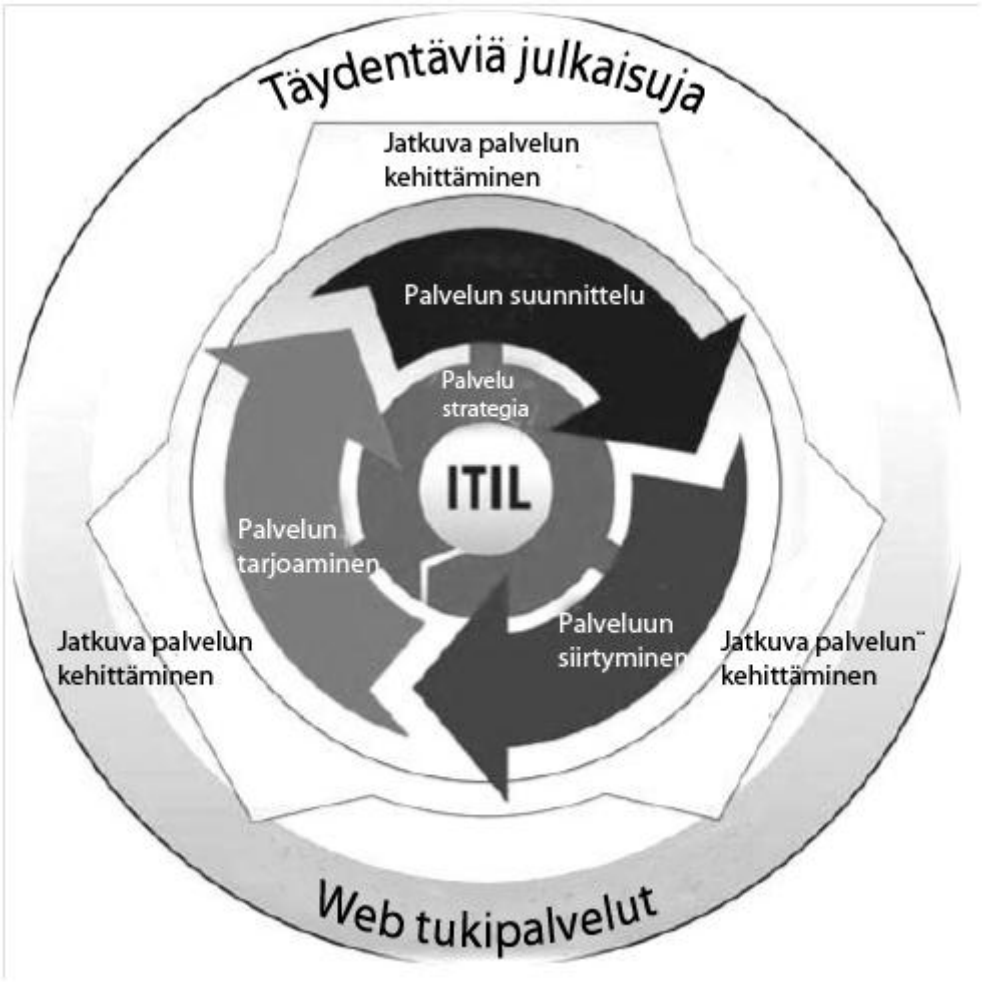
Myös helpdesk-toiminnassa on hyvä ottaa nämä psykologiset tekijät huomioon. On useimmiten suotavaa, että helpdesk esiintyy nimenomaan yrityksen X omana helpdeskinä, eikä suuren ulkoistamisyrityksen ongelmatapauksia kirjaavana osastona. Tällöin myös yrityksen oma henkilökunta voi suhtautua luottavaisemmin helpdeskin toimintaan. Yleensä puhelinjärjestelmä on rakennettu siten, että eri asiakkaille on oma numero johon he soittavat, näin saadaan helposti tunnistettua minkä asiakasyrityksen työntekijä milloinkin soittaa.

2.9 **ITIL-prosessikehys**

ITIL-prosessikehys on käytännöllinen lähestymistapa palvelunhallintaan: ”tee se, mikä toimii”. Tämä sisältää yleisten toimintatapojen viitekehyksen, joka yhdistää kaikki ICT-palvelut yhtä päämäärää kohti, joka on arvon tuottaminen liiketoiminnalle (Taylor, Case & Spalding, 2007b, s. 3).

ITIL on jaettu useaan eri osa-alueeseen, tässä tutkielmassa keskitytään pääosin informaatioturvallisuuden hallinnan prosessiin.

Koska ICT-ulkoistaminen kasvaa jatkuvasti, on välttämätöntä että sitä hallitaan. Näin pyritään takaamaan, että ulkoistamisesta saadaan hyötyä ja riskejä voidaan hallita ja minimoida (Mobarhan, Rahman, Majidi, 2011, s. 5).



Kuvio 3. ITIL V3 viitekehys (Mobarhan, Rahman, Majidi, 2011, s. 3).

Kuviossa 3 nähdään ITIL-prosessikehyksen jatkuva iterointiprosessi. Palvelun suunnittelusta siirrytään palveluun siirtymiseen ja tarjoamiseen, ja tästä huolehtivat Web-tukipalvelut, ensisijaisesti ensimmäisen asteen tukipalvelut. Palvelun tasosta saadaan jatkuvaa palautetta, jonka perusteella siirrytään takaisin palvelun suunnitteluun, josta tehdään täydentävää dokumentaatiota jonka avulla uusia palvelumuotojen variaatiota otetaan jälleen käyttöön. Näin palvelun taso ja prosessin aukottomuus paranee ajan kuluessa.

Tätä viitekehystä voidaan soveltaa myös palveluiden elinkaaren arvioinnissa, jolloin yksittäisiä palveluita voidaan suunnitella, niihin siirrytään ja niitä kehitetään (Taylor ym, 2007a, s. 19). On huomioitava, että ITIL-viitekehyksessä palveluita pyritään *iteroimaan*. Tämä tarkoittaa sitä, että palvelun lakkauttaminen kokonaan ja siirtyminen uuteen järjestelmään tulee tehdä kehittäen palvelun osa-alueita jatkuvasti. Usein ohjelmistojen kokonaan vaihtuessa tulee vakavia yhteensopivuusongelmia, jotka voidaan minimoida sopeuttaen ja kehittäen palvelua jatkuvasti ja portaittain. Palvelutason hallinta (SLM, Service Level Management) on välttämätön jatkuvan palvelun parantamisen takaamiseksi (Taylor ym., 2007a, s. 28)

2.9.1 ITIL-turvallisuuden hallinta

ITIL-turvallisuuden hallinnan prosessi kuvaa kuinka informaatioturvallisuus sovitetaan osaksi organisaation hallintaa. ITIL-turvallisuuden hallinta perustuu ISO 27001-standardiin. ISO.ORG:n mukaan: "ISO / IEC 27001:2005 kattaa kaikentyyppiset organisaatiot (esim. kaupalliset yritykset, valtion virastot, ei-voittoa tavoittelevat järjestöt). ISO / IEC 27001:2005 jaottelee dokumentoidun turvallisuuden hallinnan vaatimukset perustamiseen, toteuttamiseen, käyttämiseen, valvomiseen, arvioimiseen, huoltamiseen ja parantamiseen. Se määrittelee vaatimukset turvakäytäntöjen täytäntöönpanoon ja sitä voidaan räätälöidä tarpeiden mukaan. ISO / IEC 27001:2005 on suunniteltu takaamaan adekvaatti valinta turvakontrolleihin ja turvatarkastuksiin suojaamaan informaatiota ja takaamaan sidosryhmien luottamuksen." (Wikipedia 2011a)

Informaatioturvallisuuden hallinnan tavoite on yhdistää ICT-turvallisuus ja liiketoiminnan turvallisuus ja varmistaa sen hallinnan kaikilla palvelunhallinnan osa-alueilla (Taylor ym, 2007c, s. 141).

Osa turvallisuuden hallintaa on siis informaatioturvallisuuden hallinta. ITIL:n mukaan ensisijainen päämäärä on suojella informaatioon liittyvää arvoa ja taata informaation luottamuksellisuus, eheys ja saatavuus. ITIL-turvallisuuden hallinta on jaettu kahteen osaan:

- Palvelutasosopimuksessa (SLA) ja muissa ulkoisissa tai sisäisissä vaatimuksissa määritellyt vaatimustasot
- Turvallisuuden perustaso jolla taataan palvelun jatkuvuus ja toisaalta saavutetaan palvelutasosopimuksen ensimmäinen taso informaatioturvallisuudessa

Koska organisaatiot ja niiden tietojärjestelmät muuttuvat jatkuvasti, turvallisuuden hallinta on jatkuva prosessi ja sitä voidaan verrata PDCA-sykliin (Plan, Do, Check, Act). William Edwards Demingin tunnetuksi tekemä PDCA perustuu ympyrään, jota kierretään: ensin suunnitellaan (plan), sitten tehdään (do). Tekemisen jälkeen tarkistetaan (check) ja tehdään tarvittaessa korjaukset (act). Korjausten jälkeen ympyrässä palataan alkuun, eli suunnitteluun (Wikipedia 2011b).

Kuvio 4. Informaatioturvallisuuden hallinnan viitekehys (Taylor ym, 2007c, s. 143)

Kuvion viitekehys on laajasti käytetty ja se perustuu ISO 27001-standardin suosituksiin. Tässä kuviossa nähdään myös kuviossa 3 käsitelty iterointiprosessi ja siitä voi tunnistaa PDCA-syklin.. Kuvion viisi elementtiä on esitelty seuraavassa (Taylor ym, 2007c, s. 143):

Kontrolli

Hallinnointipuitteet tietoturvan hallintaan organisaatiossa

Organisaatio joka vastaa tietoturvapolitiikan toteuttamisesta

Vastuualueiden jako

Dokumentaation luominen ja kontrollointi

Organisaatiossa on siis yleensä jokin osasto, mahdollisesti osana tietohallintoa, joka organisoi tietoturvapolitiikkaan liittyviä asioita. Eri vastuualueet on tarkasti määritelty ja dokumentaatio on olemassa ja sitä kontrolloidaan.

Suunnittelu

Suunnittelun tavoitteena on laatia ja suositella asianmukaisia turvatoimia jotka soveltuvat organisaation vaatimuksiin. Vaatimukset muodostuvat liiketoimintaan ja palveluihin liittyvistä riskeistä, suunnitelmista ja strategioista, SLA- (Service Level Agreement) ja OLA- (Operational Level Agreement) sopimuksista sekä informaatioturvallisuuden moraalisista ja eettisistä vastuista. Käytettävissä oleva rahoitus ja organisaation asenteet informaatioturvallisuutta

kohtaan on otettava huomioon. Tietoturvapolitiikka määrittelee organisaation asenteen informaatioturvallisuuteen ja vastuu kuuluu yleensä tietoturvapäällikölle.

Toteutus

Toteutuksen on varmistettava asianmukaiset menettelyt joilla tietoturvapolitiikka pannaan täytäntöön. Konfiguraation- ja sisällönhallinta ovat tärkeässä roolissa. Informaation luokittelusta täytyy myös huolehtia. Onnistunut toteutus riippuu seuraavista osatekijöistä:

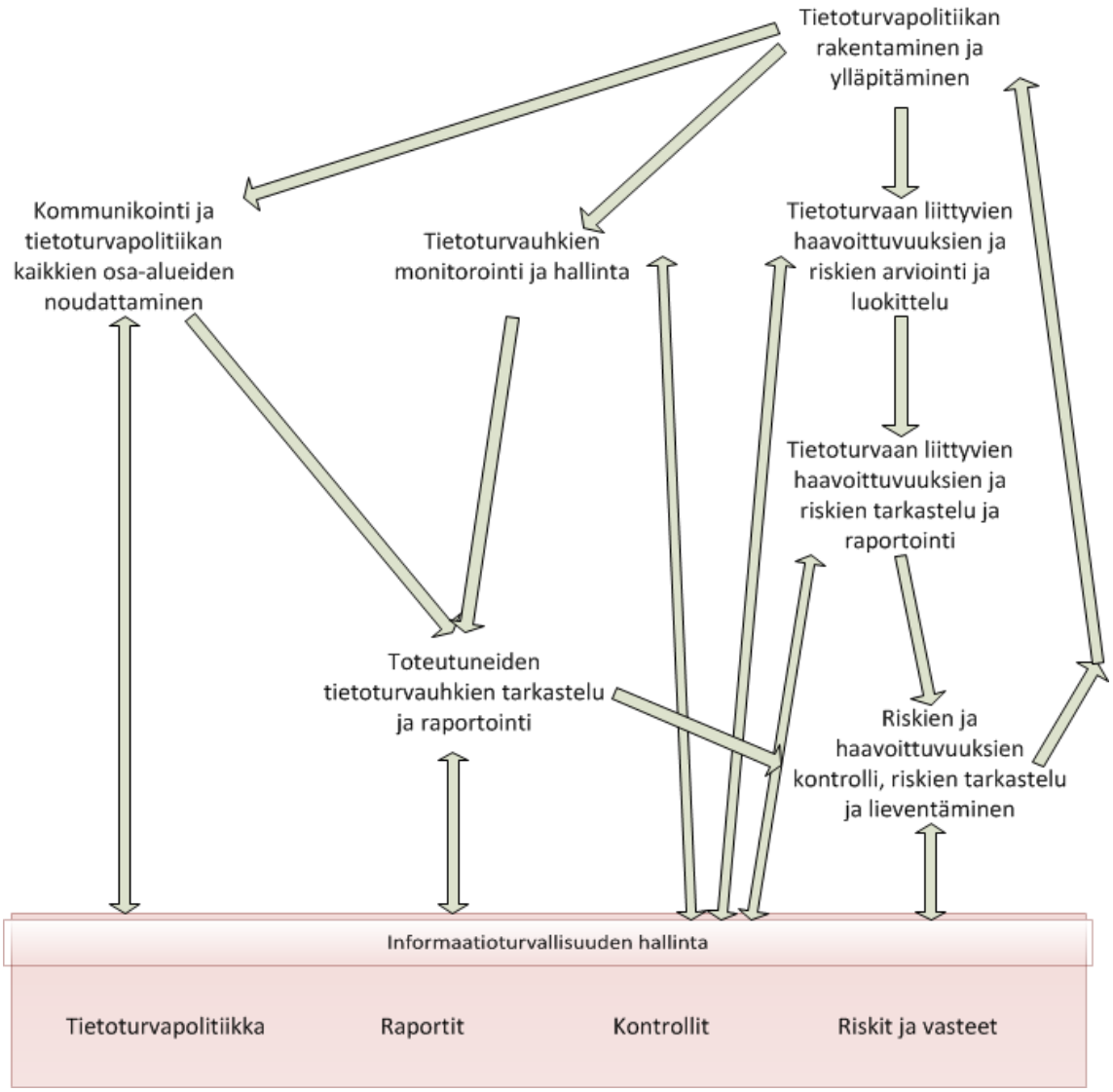
- Selvän (hyvin määritellyn) ja hyväksytyn politiikan määrittely, joka voidaan integroida osaksi liiketoiminnan tarpeita
- Menettelyt ovat asianmukaisia ja perusteltuja sekä niillä on johdon tuki
- Tietoturvapolitiikka markkinoidaan tehokkaasti ja henkilöstö koulutetaan noudattamaan sitä
- Mekanismi parannusehdotuksia varten

Arviointi

- SLA:ssa ja OLA:ssa määritellyn tietoturvapolitiikan ja siihen liittyvien turvallisuusvaatimusten varmistamista ja valvontaa
- Tietojärjestelmien informaatioturvallisuuden säännöllinen auditoini
- Tarvittaessa informaation toimittaminen ulkopuolista auditointia varten

Ylläpito

- SLA:ssa ja OLA:ssa esiintyvien tietoturvasopimusten parantaminen
- Tietoturvakäytäntöjen ja kontrollien parantaminen



Kuvio 5. Informaatioturvallisuuden hallinnan prosessi (Taylor ym, 2007c, s. 145)

Kuviossa 5 esitellään informaatioturvallisuuden hallinnan prosessi. Informaatioturvallisuuden hallintajärjestelmä koostuu neljästä elementistä: *tietoturvapolitiikasta*, *informaatioturvallisuuteen liittyvistä raporteista*, *tietoturvakontrolleista* ja *informaatioturvallisuusriskeistä/vasteista*.

Ylimpänä kuviossa on *tietoturvapolitiikan luominen ja ylläpitäminen*. Riskeihin ja vasteisiin liittyy ensin *haavoittuvuuksien ja riskien arviointi ja luokittelu*. Näiden *tarkastelu ja raportointi* sekä *kontrollointi ja keinot*, joilla riskejä voidaan lieventää. Kontrollointi on läheisessä vuorovaikutussuhteessa tietoturvauhkien monitorointiin ja hallintaan sekä niiden arviointiin ja raportointiin. Esimerkiksi verkonvalvontaohjelmisto voi monitoroida haavoittuvuuksia ja näin ollen toimia osana tietoturvauhkien kontrollointia. Monitorointiohjelmisto tuottaa yleensä myös raportteja, joita tulisi hyödyntää edelleen kontrollien kehittämisessä ja riskien lieventämisessä. Tietoturvapolitiikka muodostuu

toisaalta itse dokumenteista mutta myös siitä, että sisäinen viestintä toimii ja tietoturvapolitiikan kaikkia osa-alueita noudatetaan.

3 MITÄ TOIMINTOJA ULKOISTETAAN

Tarjousten perusteella ja ICT-kumppanin kanssa keskustellen selvitetään, mitkä toiminnot aiotaan ulkoistaa. Ulkoistavan asiakkaan täytyy perehtyä tarkasti palveluihin joita hänelle tarjotaan. Esimerkiksi helpdesk-palvelusta täytyy tietää aukiolon lisäksi myös muuta, kuten kuinka nopeasti ongelma otetaan työn alle (tämä määritellään yleensä palvelutaso sopimuksessa) ja kuinka kauan tietynlaisen ongelman ratkaiseminen kestää (vaikeampi määritellä ennen ulkoistamista). Monitorointipalvelusta täytyy myös selvittää lukuisia asioita. Raja-arvot joilla hälytyksiä generoidaan, täytyy asettaa räätälöidysti asiakkaan todellisten tarpeiden mukaan eikä siten, että ICT-kumppani saa sen avulla generoitua laskutettavaa työtä.

Esimerkiksi Microsoft Windows-palvelimen C:-osion täyttyminen ei ole vielä hälytysrajalla jos siitä on 50%:a täynnä. Yleisesti käytetyt raja-arvot Windows-palvelimen järjestelmälevyn vapaan levytilan hälytysrajoille ovat kahdesta Gigatavusta vapaata tilaa annettu varoitus ja yhdestä Gigatavusta vapaata tilaa annettu kriittinen varoitus. Nämä rajat ovat suurempia esimerkiksi tietokantapalvelimen dataosiolla. Palvelin ei välttämättä kaipaa toimenpiteitä, jos sen keskusmuistin käyttö on vain hetkellisesti korkea. Tämä riippuu voimakkaasti palvelimen roolista. Monitorointipalvelusta täytyy vaatia tarkka kuvaus, jotta siitä voidaan saada paras hyöty irti. Yritysjohdolle voi olla tärkeää saada raportti, josta käy ilmi kriittisen järjestelmän toiminta esimerkiksi 5 vuoden ajalta. On selvitettävä, pystyykö asiakkaalle tarjottu monitorointipalvelu tähän. Lisäksi tulee huomata, että tarvittaessa monitorointipalvelusta voi saada raportteja myös informaatioturvallisuuteen liittyvistä haavoittuvuuksista (Kuvio 5). Esimerkiksi Nagios IT-infrastruktuurin monitorointiohjelmisto (Nagios kotisivu, 2012) voidaan räätälöidä siten, että se raportoi verkkoliikenteen kuormia verkkolaitteista, tarkkailee palvelinten viruskuvausten ja päivitysten ajantasaisuutta sekä varmuuskopioinnin onnistumista. Yksi monitorointiohjelmisto ei silti voi olla kattava, yleensä verkkoliikenteen tarkempaan analysointiin ja haittaliikenteen seulontaan on käytössä sFlow (sFlow kotisivu, 2012) analysaattori, kaupallinen laite/ohjelmisto tai ilmainen ohjelmisto.

3.1 **Keskitetyt ja hajautetut järjestelmät**

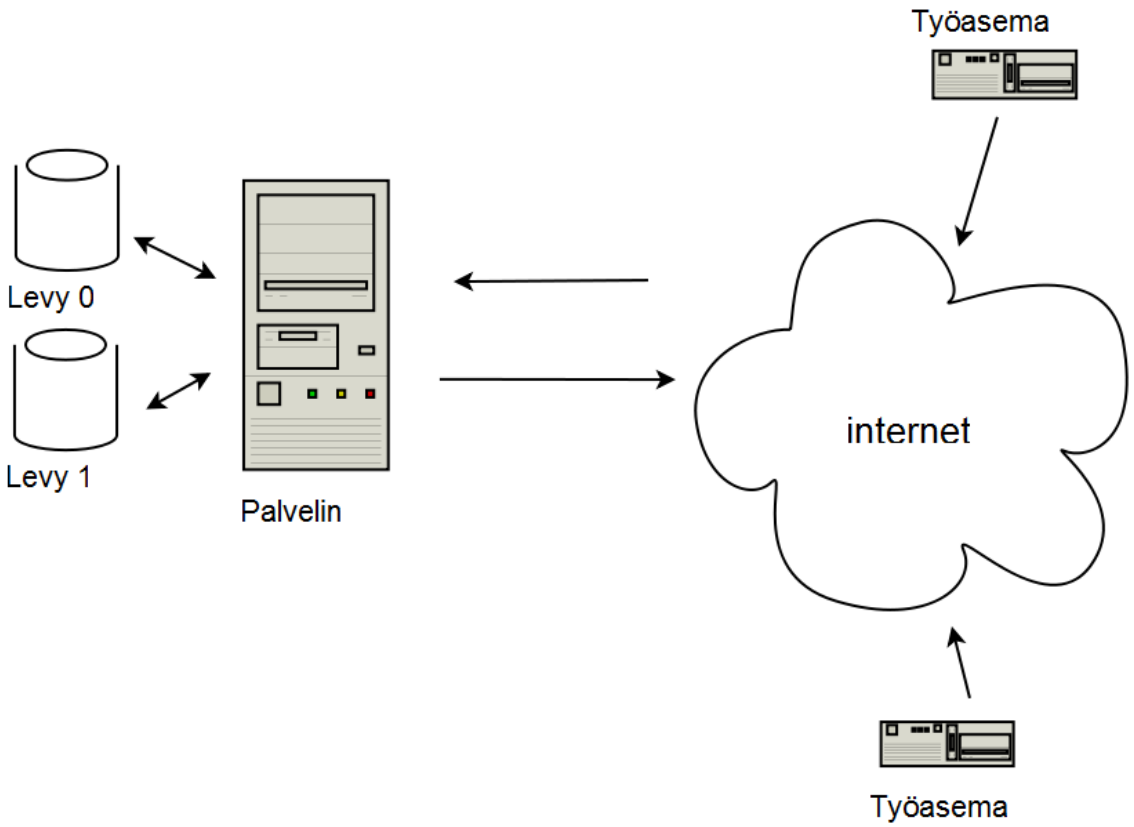
Keskitetyt ja hajautetut järjestelmät voidaan mieltää monella tavalla. Esimerkiksi yksittäisasennettuja ohjelmistoja eri työasemilla voidaan sanoa hajautettuiksi, kun taas salasanojen hallintaa AD-palvelimella voidaan sanoa keskitetyksi järjestelmäksi. Kuitenkin myös keskitetty järjestelmä voi olla hajautettu, jos palvelimien toiminnallisuus on varmennettu palvelinklusterilla,

jota ympäröi yhtenäinen pilvipalvelu. Loogisesti keskitetty mutta fyysisesti hajautettu, eli palvelimet ovat eri sijainneissa ja kommunikoivat keskenään verkon yli.

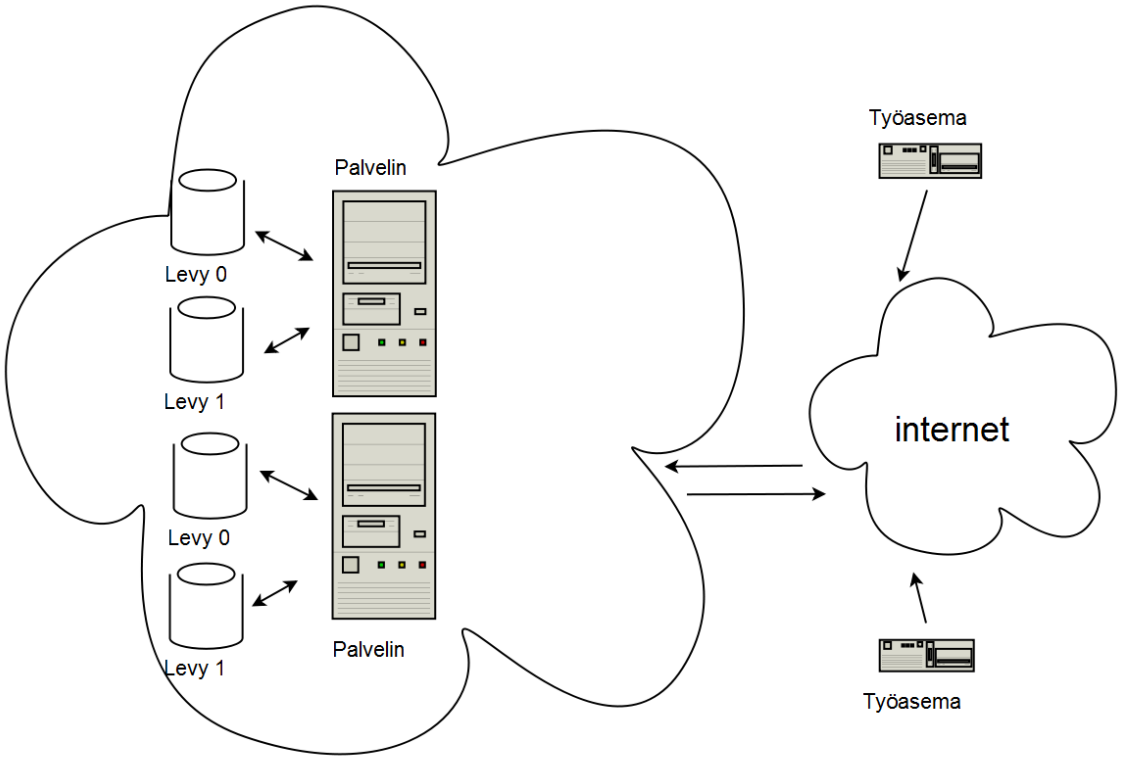
Yksittäisasennettujen ohjelmistojen haitat ovat ilmeiset, kun ohjelmistoja käytetään suuremmassa mittakaavassa. Esimerkiksi tuotannon työasemissa voi olla sovellus joka käyttää SQL-tietokantaa, tällöin olisi järkevää käyttää yhtä sql-klusteria eikä joka työasemaan asennettua omaa SQL-palvelinta. Myös laitteistoviat voivat aiheuttaa yksittäisasennettujen ohjelmistojen tapauksessa huomattavaa haittaa ja tuotannon viivästymistä. Huolimatta näistä haitoista kokemukseni mukaan yksittäisasennettuja ohjelmistoja käytetään yhä suuremmissakin yrityksissä, kun kustannussyistä tai yhteensopivuusongelmien takia ei ole koettu tarvetta siirtyä keskitettyihin järjestelmiin. Myös keskitettyjä palvelinjärjestelmiä on olemassa jopa tuotantokäytössä.

Keskitetyissä järjestelmissä, missä toiminnallisuus on ohjattu pääosin yhden palvelimen varaan, on omat riskinsä, koska kaikki toiminnallisuus on yhden palvelimen varassa (single point of failure). Tästä syystä nykyisin yleisimmin käytetty ratkaisu on hajautettu palvelinjärjestelmä, jossa työkuorma on jaettu useille palvelimille useissa eri fyysisissä paikoissa. Hyvässä toteutuksessa yhden palvelimen vikatilanne ei aiheuta käyttäjälle näkyvää ohjelmiston toimintavirhettä. Vikatilanteen ilmettyä voidaan tämä korjata aiheuttamatta merkittävää vahinkoa tuotantoketjulle. On kuitenkin huomioitava hajautetun palvelinjärjestelmän resurssit; yhden palvelimen vikatilanne voi kuormittaa järjestelmää niin, että ohjelmiston käyttö hidastuu tai jopa katkeaa kokonaan.

Monet tutkimukset osoittavat, että hajautettu palvelinjärjestelmä vähentää merkittävästi tiedonsiirron määrää järjestelmien välillä taaten samalla paremman vikasietoisuuden järjestelmän toimivuudelle (esim. Moss 2007, s. 765). Seuraavissa kuvioissa on esitetty keskitettyjen ja hajautettujen palvelinjärjestelmien skemaattinen periaate:



Kuvio 6. Keskitetty järjestelmä



Kuvio 7. Hajautettu järjestelmä

3.2 **Käyttöönotto**

Tässä tutkielmassa käyttöönotto tarkoittaa niitä toimia, joita liittyy ICT-ulkoistamisen alkuvaiheeseen. ICT-järjestelmissä ja toiminnoissa on niin paljon vaihtelua yrityksittäin, että palvelua tarjoava yritys tarvitsee aikaa kartoittaa ja dokumentoida asiakkaan ICT-ympäristöä. Esimerkiksi jos asiakas haluaa ulkoistaa loppukäyttäjien tuen, täytyy tätä varten mahdollisesti perehtyä asiakkaan käyttämiin sovelluksiin, saada toimialueen käyttäjätili, jolla helpdesk voi vaihtaa unohtuneen toimialueen salasanan. Yritysten välillä täytyy myös rakentaa etäyhteys ylläpitoa varten. Etäyhteyden laatimiseen voi olla tietoturvapolitiikassa tarkka politiikka (aliluku 2.6.1). Jokaiseen ICT-ulkoistamisen tyyppiin liittyy käyttöönotto.

3.3 **Taustatietojen selvittämistä**

On sovittava tarkasti mitä käyttöönotossa oikeastaan tapahtuu, minkä tason tunnuksia yritys X tarvitsee asiakkaan järjestelmiin suorittaakseen kartoituksen ja mitä voi mennä pieleen jo käyttöönottovaiheessa. Asiakkaan olisi hyvä saada selvyys kartoitusvaiheen eri menetelmistä. Millaisia ohjelmistoja yritys X

käyttää kartoittaessaan ICT-infrastruktuuria, kuka kartoituksen tekee ja millaisia dokumentteja kartoituksesta muodostetaan. On tärkeää, että muodostettavat dokumentit tallennetaan järjestelmään jonne ei ole pääsyä kuin tietyillä ennalta nimetyillä henkilöillä. Voi olla myös merkittävää, että tieto ICT-ulkoistuksesta ei leviä, ennen kuin käyttöönotto on kokonaisuudessaan tehty.

Entä millaiset etäyhteydet tarvitaan, tuleeko yrityksen X päästä suoraan kaikkiin asiakkaan verkkoihin vai riittäisikö pääsy hallintaverkkoon tai kenties vain yhdelle ylläpitoa varten perustetulle palvelimelle? Jos asiakkaan verkossa ei ole erikseen hallintaverkkoa, käyttöönotossa saattaa olla järkevää rakentaa sellainen. On syytä huomioida myös identiteetin hallinta. On tärkeää, että yrityksen X jokainen käyttäjä voidaan identifioida omalla tunnuksellaan. Näin asiakkaalle tehtävä työ on henkilökohtaisempaa, ja mahdolliset ongelmatilanteet selviävät nopeammin. Jos yrityksellä X olisi vain yksi tunnus asiakkaan järjestelmään, asiakas ei voisi mitenkään tietää kuka sitä milloinkin käyttää.

Asiakasyrityksen tulisi kohdistaa huomiota yrityksen X henkilöstöön. Ira Winklerin mukaan suurin uhka Yhdysvaltojen informaatioturvallisuudelle on inhimillinen erehdys (Winkler, 1997, s. 39). On selvää, että tämä pätee myös globaalissa mittakaavassa. Henkilöstön puutteellinen koulutus ja puutteelliset toimintaohjeet, jotka voivat johtaa salasanojen vuotoon, ovat informaatioturvallisuutta heikentäviä osatekijöitä.

Voisi olla järkevää vaatia salassapitosopimuksen solmimista jokaisen osallisen työntekijän kanssa henkilökohtaisesti. Yrityksen X sisäisestä tietoturvapolitiikasta ei välttämättä saa todenmukaista kuvaa, joten on ehkä syytä vahvistaa informaation turvallisuutta ja salassapitoa tällä tavalla. Sopimuksen sakkopykälät kannattaa tarkastaa erityisellä huolella, ei saa jäädä epäselväksi kuka on vastuussa jos tietojärjestelmiin tulee ongelmia. Selvää täytyy olla myös vaitiolovelvollisuus puolin ja toisin. Ennen kaikkea ylläpitosopimuksesta pitää käydä tarkasti ilmi, millä vasteajalla reagointi tapahtuu (SLA-sopimuksessa on määritelty vasteajat, tämä on yleensä aina osa ylläpitosopimusta). Reagoinnin täytyy tapahtua tietyssä vasteajassa myös ICT-infrastruktuurin ja tietoturvapolitiikan aihealueella, vaikka tämä reagointiaika olisikin merkittävästi pidempi kuin vasteaika yksittäisiä työasemia tai verkkolaitteita koskeviin ongelmiin. Mikäli tämä vasteaika ylitetään, on palvelupyyntö otettava erityistarkasteluun ja varmistettava säännöt, joita tulee vastaavien palvelupyyntöjen tapauksessa noudattaa.

Tämä ei kuitenkaan koske pelkästään ongelmia vaan myös kehittämiskohteita. Kehittämiskohteita voivat olla esimerkiksi vanhentuneet verkon aktiivilaitteet, työasemat sekä ohjelmistot ja tietoturvapolitiikan luonteva käytäntöönpano henkilökunnan keskuudessa.

Jos asiakas tarvitsee jonkin järjestelmän tai minkä tahansa ICT-hankinnan, tulee ICT-kumppanin kyetä toimittamaan se järkevässä tai ennalta sovitussa ajassa.

Kirjallisena sopimus on edes jollain tavalla sitova. Järkevä aika uuden työaseman hankinnalle voi olla yhdestä kolmeen vuorokautta, uuden palvelimen toimittaminen kolmesta viiteen vuorokautta.

3.4 **Käyttöönoton aikana**

On hyvä tehdä käyttöönottosuunnitelma josta käy ilmi aikataulu asioiden etenemiselle. Asiakkaan on syytä seurata kuinka yritys X suorittaa käyttöönottoa ja olla siinä mukana mahdollisimman tiiviisti. Hyvä viestintä osapuolien välillä edistää ICT-ulkoistamista (luku 4). Aikataulussa pysyminen on yksi mittari käyttöönoton onnistumiselle. Käyttöönotto tulisi järjestää siten, että siitä ei aiheudu asiakkaalle turhia katkoksia tietojärjestelmien toimintaan tai mitään muutakaan näkyvää haittaa. Mahdolliset katkokset järjestelmien käytössä tulisi ajoittaa siten, että niistä aiheutuu mahdollisimman vähän haittaa asiakkaan liiketoiminnalle. Esimerkiksi asiakkaan palomuuri voidaan joutua vaihtamaan ennen kuin käyttöönotto voi edetä pidemmälle. Tästä aiheutuu luonnollisesti lyhyt katkos tietoliikenteeseen. Voi myös olla, että jotain muuta asiakkaan laitteistoa tai ohjelmistoja täytyy uusia, jotta käyttöönotto voi edetä hallitusti.

3.5 **Käyttöönoton päätyttyä**

Kun käyttöönotto on saatu päätökseen ja yrityksen X tarjoamat palvelut käynnistetään, asiakkaan tulisi voida luottaa palveluiden toimivuuteen. Joitain kysymyksiä saattaa silti nousta vielä mieleen. Onko asiakkaan järjestelmistä laadittu dokumentaatio varmasti riittävällä tasolla ja tallessa luotettavassa järjestelmässä?

4 HYVÄ VIESTINTÄ ASIAKKAAN JA PALVELUA TARJOAVAN VÄLILLÄ

Viestinnän järkevä toteuttaminen riippuu usein yrityksen toiminnan laajuudesta, mikä vakiintuneessa ympäristössä on useimmiten korrelaatiossa palvelupyyntöjen määrään. Hyvä viestintäsuunnitelma vähentää muutosvastarintaa ulkoistavassa yrityksessä. Tämä muutosvastarinta tulee siis huomioida kun laaditaan viestintäsuunnitelmaa. Tehokkaasti toimiva viestintä vaatii oman suunnitelman, jossa määritellään roolit, aikataulu, menetelmät, tavoitteet, kohderyhmät ja riskit viestinnälle (Palmila 2008, s. 56). Joidenkin tutkimusten mukaan työntekijät eivät pidä tietokonevälitteistä viestintää niin tärkeänä kuin perinteistä kasvokkain viestimistä (Jones 2011, s. 247).

Jos viestintä tapahtuu sähköpostitse, on huomioitava sähköpostiin liittyvä informaatioturvallisuuden riski. Salaamaton sähköposti voi olla riski jos se sisältää arvokasta informaatiota. Jos tietoturvapolitiikka noudattaa ITIL-periaatteita (aliluku 2.6.1), sähköpostin käyttöön on laadittu säännöt joilla informaatioturvallisuuden riski siltä osin pienenee. Lisäksi identiteetin varmistaminen on tärkeää ja se voi olla vaikeaa (Andress 2011, s. 18). Sosiaalinen hakkerointi (Social Engineering) on tapa yrittää taivuttaa ihmisiä luovuttamaan salassapitosopimuksen alaista informaatiota vakuuttamalla heitä kertomalla valheellista tietoa (Winkler 1997, s. 94).

Dokumentointitaito ja hyvä kirjallinen viestintä ovat tärkeässä asemassa kun puhutaan ICT-ulkoistamisprojekteista (Jones 2011, s. 268). Tämä tulisi huomioida kun palkataan esimerkiksi uutta järjestelmäasiantuntijaa, sillä dokumentointitaito tukee teknistä osaamista.

4.1 Viestinnän eri tasot

Suppeassa ympäristössä riittää pelkkä sähköpostiviestintä yksityishenkilöiden välillä. Tällaisen viestinnän raja tulee vastaan siinä vaiheessa, kun sähköpostin määrä ylittää tietyn reagoimiskynnyksen. Tällä työskentelytavalla on myös muita esteitä: esimerkiksi työntekijän sairasloman tai muun poissaolon takia työt voivat viivästyä.

Ensimmäisen asteen parannus tähän toimintamalliin on sähköpostiryhmien perustaminen: yhdessä Saapuneet-kansiossa on käyttöoikeudet useammalle työntekijälle. Mikäli palvelupyynnöt delegoidaan eteenpäin näille ryhmille, ei yhden henkilön poissaolo keskeytä työntekoa kokonaan.

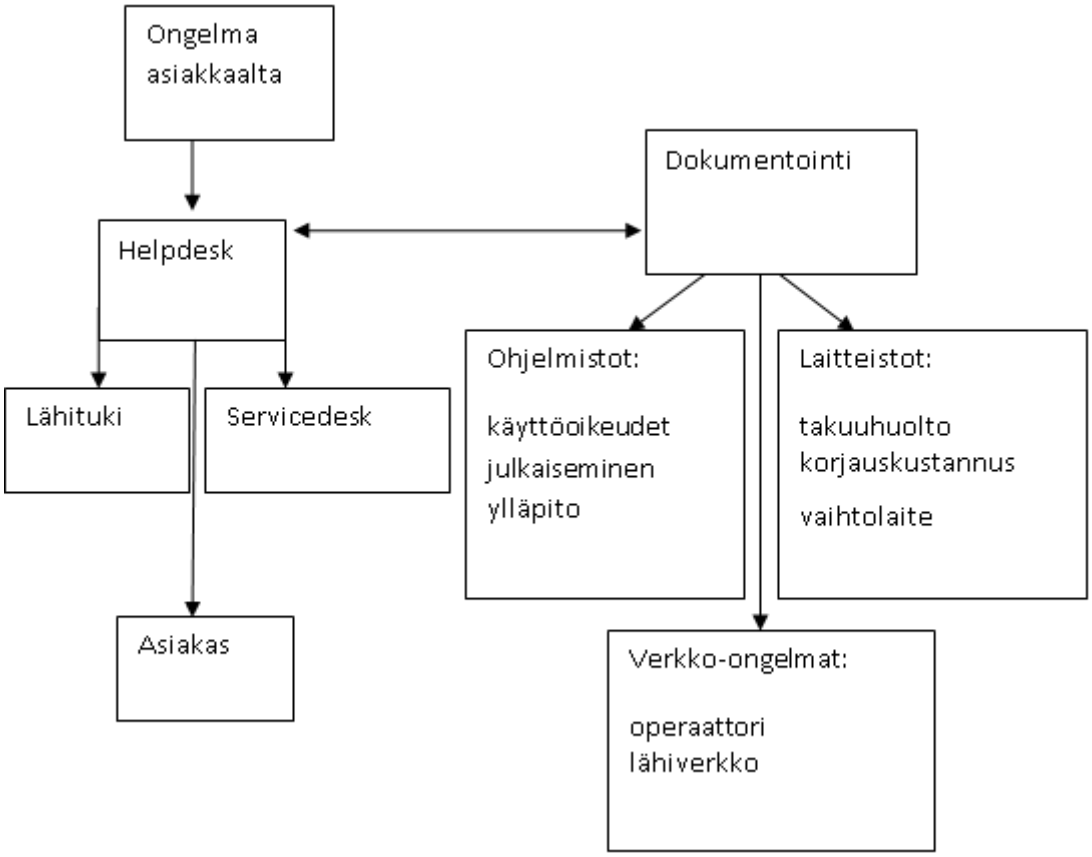
Sähköpostiryhmien toteutus vaatii tarkkaa suunnittelua, sillä jos ryhmäsähköposti on esimerkiksi vain uudelleenlähetysosoite, josta palvelupyynnöt lähetetään eteenpäin tiettyihin yksityishenkilöiden postilaatikkoihin, voi tämä järjestely jopa vaikeuttaa työntekoa: henkilöt voivat

luottaa perusteettomasti siihen, että toinen ihminen huolehtii tästä palvelupyynnöstä, tai voi esiintyä päällekkäistä työtä.

Toisen asteen parannus saavutetaan, kun pyritään saavuttamaan riippumattomuus sähköpostilaatikoista kokonaan: tällöin ratkaisuna ovat toiminnanohjausjärjestelmän sisältämät työlistat, joihin asiakas voi suoraan syöttää palvelupyyntöjä ja ulkoistusyritys voi syöttää suoraan ratkaisuvaihtoehtoja. Hyvässä toiminnanohjausjärjestelmässä myös varmistetaan, että päällekkäistä työtä ei ole mahdollista suorittaa, ja jokaiselle palvelupyynnölle on nimetty ensisijaiset vastuuhenkilöt. Hyvän toiminnanohjausjärjestelmän ominaisuuksiin kuuluu myös palvelupyyntöjen delegointimahdollisuus, hyvät etsintätoiminnot ja varoitustoiminnot, jotka varoittavat esimerkiksi kauan listalla olleista tekemättömistä töistä tai kriittisten asiakkaiden palvelupyynnöistä, jotka on ratkaistava erityisen kiireellisesti.

Valvontamonitorista tulevat sähköpostiviestit voidaan myös ohjata siten, että ne kirjautuvat suoraan toiminnanohjausjärjestelmään ja niistä voidaan lähettää myös tekstiviestejä ylläpitäjien toivomiin kännykkäliittymiin. Asiakas voi haluta toiminnanohjausjärjestelmään myös ominaisuutta, jonka avulla kuka tahansa työntekijä voi kirjata WWW-lomakkeen avulla palvelupyyntöä soittamatta Helpdeskiin. Toiminnanohjausjärjestelmän ja sähköpostin välinen vuorovaikutus pitäisi myös olla säädettävissä: esimerkiksi voidaan havaita, että tietyistä valvontatoiminnoista tulee tarpeettomia hälytysposteja, joita koskeviin vikoihin reagoidaan joka tapauksessa prosessin aikana: tällöin nämä hälytyspostit voidaan kytkeä pois päältä.

Muita viestintätekniikoita kuin sähköposti ovat muun muassa videoneuvotteluteknologiat. Tällaisia ratkaisuja ovat esimerkiksi Microsoftin Lync (Microsoft Lync kotisivu, 2012) ja Cisco Webex (Cisco Webex kotisivu, 2012). Tämän lisäksi tai kokonaan itsenäisenä ratkaisuna käytetään yrityskäyttöön tarkoitettuja pikaviestimiä, joilla voidaan reaaliaikaisesti tarkkailla työntekijöiden saatavuusstatusta ja lähettää heille pikaviestejä.



Kuvio 8. Työn kulku

Asiakkaan ongelma suunnataan aluksi helpdeskiin, joka ITIL-termistössä on palvelupiste (aliluku 2.5.1). Helpdesk pyrkii käyttäjän oikeuksin ratkaisemaan asiakkaan ongelmaa. Usein ongelma liittyykin sähköpostin, MS Office-ohjelmien tai Windowsin käyttöön, jolloin ongelmanratkaisuun päästään välittömästi.

Joskus kuitenkin ongelma liittyy esimerkiksi ajuriversioihin tai ohjelma-asennuksiin, jonka ratkaisemiseen helpdeskillä ei ole oikeuksia. Tällöin ongelma siirtyy lähitukeen, lähituki voi olla joko asiakkaan yrityksessä tai ulkoistusta tarjoavassa yrityksessa.

Helpdeskin vastuulla on myös dokumentointi: on tärkeää pitää yllä sääntöjä, kenelle ohjelmia asennetaan ja millä reunaehdoilla, ja mitkä kustannus- ja lisensiointiasiat tähän liittyvät. Esimerkiksi voi olla sovittu, että tietyn ohjelman lisenssiin vaaditaan työpisteen esimiehen lupa. Helpdeskillä on myös velvollisuus olla yhteydessä operaattoreihin, jos ongelma johtuu ulkoistuspalveluyrityksestä riippumattomista verkko-ongelmista tai työaseman laitteistosta koskevista ongelmista, jolloin palvelu kuuluu työasemia välittävän yrityksen takuukorjauksen piiriin (ellei tämä yritys ole itse ulkoistava yritys). Yhteyskanavien, mm. avainhenkilöiden puhelinnumeroiden ajan tasalla oleva dokumentointi on ehdottomasti työn nopeuden kannalta elintärkeä toimenpide.

Jos ongelma liittyy palvelinympäristöön, esimerkiksi sähköpostin tai verkkolevyjen tilaongelmiin, siirtyy ongelma servicedeskiin.

Joskus ongelma siirretään takaisin asiakasyrityksen avainhenkilölle, jos asiasta on erikseen sovittu. Näin toimitaan usein mm. sähköpostitunnusten tai verkkotunnusten luomisen yhteydessä tai asiakasyrityksen erityisohjelmien käyttöoikeuksien muuttamisen yhteydessä.

4.2 **Tulevaisuuden visioita**

Koska tekniikka muuttuu ja kehittyy, myös viestintätekniikoiden täytyy kehittyä. Blogit, Wikipedian tekniikkaan pohjautuvat dokumentointijärjestelmät ja pikaviestimet ovat vain muutamia esimerkkejä yritysten viestintäteknologioista jotka vielä jonkin aikaa sitten nähtiin lähinnä vain viihdekäyttöön sopivina, mutta nykyään nämä ovat suurtenkin yritysten päivittäisessä käytössä. Uutena lupaavana tekniikkana voidaan nähdä esimerkiksi Second Life-tyyliset virtuaalimaailmat (Jennings 2010, s. 456). Näissä virtuaalimaailmoissa käyttäjä luo oman avatarin, joka on virtuaalinen kopio omasta henkilöhahmosta. Tällainen ympäristö voisi toimia osana helpdeskiä ja sitä voitaisiin soveltaa myös koulutusten järjestämiseen.

4.3 **Muutoksiin varautuminen**

On myös syytä varautua aikataulun muutoksiin. Jos aikaa ei ole varattu riittävästi, käyttöönottovaiheen jälkeiset dokumentit jäävät puutteellisiksi. Järjestelmiin liittyvä dokumentointi tulee olla kuitenkin jatkuvaa ja siihen tulee kiinnittää myös huomiota. Tosielämässä näkee esimerkkejä tapauksista, joissa päivystäjä herää keskellä yötä kriittiseen hälytykseen ja etsittyään ensin turhaan dokumentaatiosta tunnuksia tai muuta tiedonjyvää, joutuukin lopulta soittamaan kollegalle tai asiakkaan edustajalle kysyäkseen neuvoa. Myös vanhentuneet toimintaohjeet aiheuttavat monenlaisia ongelmia, päivystäjä saattaa käynnistää uudelleen vääriä palvelimia tai soittaa väärille yhteyshenkilöille. Asiakkaan on hyvä muistaa, että dokumentaatio kannattaa saattaa mahdollisimman hyväksi jo käyttöönoton aikana, asioilla on tapana unohtua jos sovitaan dokumentaatiota täydennettäväksi sitten joskus myöhemmin. Asiakkaan ja ICT-kumppanin välillä saattaa olla erimielisyyksiä siitä, kauanko käyttöönottoon tulisi varata aikaa. Asiakas ei haluaisi maksaa liian perusteellisesta kartoituksesta ja hyvä ICT-kumppani ei haluaisi tehdä asioita kiireellä koska se kostautuu myöhemmin.

4.4 Informaation jakaminen

Asiakkaalla on usein tarve jakaa dokumenttejaan kolmansien osapuolien kanssa, tietoturvapolitiikka ottaa tähänkin kantaa jos se on ITIL:n mukainen (aliluku 2.6.1). Tässä yhteydessä on ensiarvoisen tärkeää, että dokumentit ovat saatavilla vain niille henkilöille joille se on tarkoituksenmukaista. Yksi mahdollisuus on, että asiakas ostaa ohjelmiston tähän käyttötarkoitukseen (Xiong 2007, s. 1). Esimerkkejä tämänkaltaisen tiedon jakamiseen ovat Microsoft SharePoint, Lotus Quickr sekä Wiki-pohjaiset ratkaisut. Erityisesti valitussa ohjelmistossa kannattaa huomioida, että pääsynhallinnan tasot ovat tarpeeksi monipuolisia ja tarkoituksenmukaisia. Useinkaan ei riitä pelkästään se että käyttäjällä on pääsy tiettyyn kohteeseen joko luku- tai muokkausoikeuksin. Tarvitaan eriasteisia muokkausoikeuksia. Esimerkiksi IBM Lotus Notes-tietokannoissa voidaan muokata koko tietokannan arkkitehtuuria ja luoda tai poistaa kokonaisia tietokantoja tai sitten vain siinä esiintyviä yksittäisiä asiakirjoja (IBM Lotus Notes kotisivu, 2012). Kaikkia näitä toimintoja varten voidaan luoda eriasteisia muokkausoikeuksia siten, että yksittäisellä toimijalla ei ole liian vahvoja oikeuksia omaan toimenkuvaansa nähden.

4.4.1 Dokumentoinnin käyttöoikeuksien valvonta

Hyvällä dokumentoinnilla on esimerkiksi ennalta tiedetty kohdeyleisö (Cooke & Oldfield, 1987, s. 3). Käytännön tasolla tämä tarkoittaa käyttöoikeuksien säätämistä siten, että tietyt henkilöt pääsevät katsomaan vain heille tarkoitettuja dokumentteja. Ylimmällä tasolla tämä tarkoittaa sitä, että asiakasyritykset erotetaan toisistaan. Yksityiskohtaisemmalla tasolla erotetaan toisistaan julkinen tieto, yrityksen sisäinen tieto, sisäisesti rajoitettu tieto, erityisen suojattu tieto. Julkinen tieto on muun muassa tieto joka voidaan julkistaa yrityksen www sivuilla tai toimintakertomuksissa, sisäinen tieto on yrityksen henkilöstön saatavilla, sisäisesti rajoitettu tieto on tarkoitettu ainoastaan tietyille henkilöstöryhmille ja erityisen suojattu tieto on tarkoitettu henkilöille joiden pääsy järjestelmään on identiteetin hallinnan piirissä. Sama jaottelu on käytössä valtion virastoissa ja puolustusvoimissa.

Pääseekö dokumentointijärjestelmään käsiksi kaikkialta, ja jos pääsee, niin millainen autentikointi järjestelmään on? Jos sovelluksella on web-käyttöliittymä, täytyy kyseenalaistaa onko tarpeen sallia pääsy kaikkialta. Lisäksi asiakkaan on syytä tietää, onko dokumentointijärjestelmä oma järjestelmänsä vai kuuluuko se osana yrityksen toiminnanohjausjärjestelmään. Onko käytössä oleva dokumentointijärjestelmä avoin vai suljettu, onko se kaupallinen, vapaa ohjelmisto vai kenties yrityksen itse kehittämä tuote? Avoimen lähdekoodin tuotteissa voi olla monia tietoturvariskejä, koska mahdolliset murtautujat pystyvät saamaan yksityiskohtaisempaa tietoa järjestelmästä.

4.4.2 Henkilöstöön kohdistuvat tekijät

Informaatioturvallisuuden nimissä asiakkaan tulee tehdä muutamia testejä jotka kohdistuvat yrityksen X henkilöstöön. Ira Winklerin mukaan useimmat ihmiset ovat erittäin halukkaita auttamaan työtovereitaan. Avuliaat henkilöt ovat monesti hyvin innokkaita tarjoamaan tiedon jota he tarvitsevat vaikka kysyvän henkilön henkilöllisyydestä ei ole suurempia takeita (Winkler 1997, s. 148). Näitä testejä on syytä tehdä toistuvin väliajoin sillä yrityksessä X luultavasti palkataan uusia työntekijöitä ja vanhat työntekijät saattavat lopettaa.

Yksi tyypillinen testi on soittaa helpdeskiin ja tekeytyä henkilöksi joka on unohtanut salasanan – kuinka helposti helpdesk vaihtaa unohdetun salasanan, millä tavoin soittajan identiteetti varmennetaan. Käytännössä tällainen testi voisi olla puhelinnumeron omistajan selvittäminen. Jos puhelin on varastettu ja soittaja tekeytyy puhelimen oikeaksi omistajaksi, lisäkysymyksenä voitaisiin esittää asiakkaaseen liittyviä kysymyksiä, kuten toimipaikka ja lähin esimies. Jos on syytä epäillä identiteettivarkautta, lupa salasanan vaihtamiseen voidaan kysyä esimieheltä. Tällöin vastuu siirtyy asiakasyrityksen esimiehelle.

5 KÄYTTÖÖNOTON JÄLKEEN

ICT-ulkoistaminen ei ole projekti jolla on selvä alkamis- ja päättymiskohta (kts. kuvio 3). Siihen kuuluu jatkuva palvelun kehittäminen ja yhteistyö osapuolien välillä. Yleensä sovitaan käyttöönoton jälkeen seurantapalavereja joissa käydään läpi kehittämiskohteita ja yleisten ongelmien ratkaisuprosentteja sekä niihin kulunutta aikaa.

Yleisesti asiakasyritystä kiinnostaa ongelmien ratkaisuprosentit tietyssä ajassa: voidaan esimerkiksi laatia taulukko, jossa on lueteltu ratkaistut ongelmat tiettyjen aikarajojen sisällä (heti, 30 minuutin sisällä, 4 tunnin sisällä, seuraavan työpäivän aikana tai kauemmin). On tärkeää, että yrityksen X käyttämä toiminnanohjausjärjestelmä tukee tällaisen raportin helppoa laadintaa.

On kuitenkin huomattava, että pelkkien ongelmanratkaisuprosenttien painottaminen ei anna kuvaa yrityksen X toiminnasta: esimerkiksi vastuutehtävien lisääntyessä tai asiakasyrityksen ottaessa käyttöön uutta järjestelmää, on väistämätöntä että ongelmanratkaisuprosentti tilapäisesti alenee, koska yrityksen X henkilöstö joutuu käyttämään aikaansa uuden järjestelmän yksityiskohtien opiskeluun.

Lisäksi on huomattava kausittaiset vaihtelut: esimerkiksi tilinpäätöskausien aikana voi yritykselle tulla hyvinkin haastavia taulukkolaskentaan liittyviä ongelmatilanteita sekä epäonnistuneemman ohjelmistopäivityksen aikana paljon aikaa vieviä virhetilanteita, joissa joudutaan yksityiskohtaisesti kokeilemaan esimerkiksi eri tulostinajuriversioiden toimivuutta. Nämä ongelmakohdat hahmottuvat yksityiskohtaisesti vasta pitkän, vuosia kestäneen yhteistyön tuloksena.

Erityisen tärkeänä pidetään nykyään ns. *ketterää (agile)* järjestelmäkehitystä. Erilaiset ohjelmisto- ja strategiapäivitykset vaativat tiukkaa riippuvuuksien hallinnointia, koska ohjelmistojen vähän tunnetut moduulit ja järjestelmien vaatimukset saattavat aiheuttaa ei-toivottuja sivuvaikutuksia yllättävissä tietojärjestelmien osissa. Tällöin puhutaan järjestelmän *mätänemisestä (software rot),* joka aiheuttaa yllättäviä lisäkuluja etenkin järjestelmän ylläpidon piirissä (Martin 2000, s. 4).

5.1 **Palvelun jatkuvuus**

Palvelun jatkuvalla parantamisella tarkoitetaan ICT-kumppanin kykyä mukautua liiketoiminnan muuttuviin haasteisiin ja toteuttamaan parannuksia liiketoimintaprosesseja tukeviin palveluihin.

Kolme pääperiaatetta ovat:

Yleinen palvelunhallinnan tarkkailu

> Jatkuva ICT-palveluiden mukauttaminen ja luominen
>
> ICT-prosessien toteuttaminen siten, että ne noudattavat jatkuvaa palvelun elinkaaren mallia
>
> (Taylor ym, 2007b, s. 3)

Esimerkiksi ICT-ulkoistajalta voi puuttua SharePoint-osaamista ja se joutuu sitä hankkimaan asiakkaiden vaatimusten muuttuessa. Tämä on yksi palveluiden jatkuvuuden edellytys. SharePointin tapauksessa nämä pääperiaatteet voidaan huomioida esimerkiksi seuraavasti:

> Pitää tarkkailla, missä mitassa Sharepoint-palvelut on syytä implementoida asiakkaan nykyiseen tietojärjestelmään ja tarkkailla, minkälaisissa tapauksissa palvelu tuo lisäarvoa järjestelmään.
>
> SharePoint-palveluita tulee luoda asiakkaan tarpeiden mukaisesti: esimerkiksi jollekin yrityksille riittää dokumentointijärjestelmän pohjaksi tiedostojen ja dokumenttien tietokanta, jossa on tehokas etsintätoiminto. Laajemmissa tapauksissa voidaan harkita kokonaisen Intranet-palvelun tai Wiki-sivuston luomista tällaisten tietokantojen ympärille. Useinkaan pelkkä hakusanatoiminto ei riitä, koska käyttäjät eivät aina osaa havainnoida, millä hakusanoilla tietoa on syytä etsiä. Tämänkaltaista toimintoa on syytä harkita etenkin, jos yrityksellä ei ole käytössä yhtenäistä terminologiaa tai dokumentteja on luotu useammalla kielellä.
>
> Jatkuvan elinkaaren mallissa (aliluku 2.9) on huomioitava jatkuva ja asteittainen palveluiden eri osa-alueiden kehittäminen. SharePointin ja siihen mahdollisesti kytkeytyvän Intranetin vuorovaikutuksessa on huomioitava esimerkiksi eri HTML-standardien yhteensopivuus ja tietokannoissa olevien Office-dokumenttien ongelmaton aukeaminen. Usein jälkimmäisessä tapauksessa esiintyvien ongelmien syynä on tiedostoformaattien muuttaminen, esimerkiksi *.doc-tiedostojen muuntaminen *.docx-formaattiin, johon ICT-ohjeistuksessa ei ole otettu tarpeeksi selkeää kantaa.

5.2 **Seurantapalaveri**

Käyttöönoton jälkeen on sovittu yksi tai useampia seurantapalavereja. Seurantapalaveri voidaan järjestää asiakkaan tai yrityksen X tiloissa. Nykyään yleistyneet videoneuvottelut ovat myös suosittuja, kuten Tandbergin (Tandberg kotisivu, 2012), Ciscon (Cisco Webex kotisivu, 2012) tai Microsoftin (Microsoft Lync kotisivu, 2012) kehittämät ratkaisut. On selvää, että asiakasta kiinnostaa ratkaistujen palvelupyyntöjen määrä ja vaste-ajat. Huomioita tulisi kiinnittää myös yrityksen informaatioturvallisuuden kehittämiseen. Tässä apuna voivat toimia sFlow-analysaattorin ja IDS-järjestelmän raportit. Autentikointia vastaan

kohdennettuja hyökkäyksiä voidaan tehokkaasti estää hyvällä salasanapolitiikalla (Andress, 2011, s. 151). Jos yrityksessä eivät ole käytössä vähintään 8 merkin salasanat joissa vaaditaan erikoismerkkejä, isoja ja pieniä kirjaimia sekä numeroita, se altistuu brute-force (raaka voima, väsytysmenetelmä) -hyökkäyksille.

5.3 **Palvelun testaaminen**

Hyvä keino seurata ICT-kumppanin toimintaa on seurantapalaverien lisäksi palveluiden testaaminen. Mikäli käyttöön otettiin monitorointipalvelu, hälytysviestit voidaan vaatia sähköpostilla myös asiakkaalle. Näin asiakas voi seurata, millaisia hälytyksiä järjestelmistä tulee ja kuinka nopeasti niihin on reagoitu. Näistä viesteistä voidaan myös havainnoida, ovatko raja-arvot säädetty, kuten on sovittu.

Lisäksi varmistusjärjestelmän toimivuutta voi testata kopioimalla testitiedoston muistitikulle ja sen jälkeen poistamalla sen verkkolevyltä. Tämän jälkeen suoritetaan soitto helpdeskiin ja tehdään palautuspyyntö. Lisäksi voidaan tarkastella, millä tavalla laitehankinnat sujuvat, pitääkö ICT-kumppani rekisteriä laitteista ja muuttuvatko oletussalasanat. Mikäli nämä eivät muutu, on syytä olettaa että ICT-kumppanin salasanapolitiikka ei ole asianmukainen.

Jos kytkimien, palomuurien tai UPS:ien oletussalasanoja ei vaihdeta, tästä voi seurata merkittäviä tietoturvaongelmia. Esimerkiksi ilkeämielinen työntekijä saattaa yrittää kirjautua laitteisiin oletussalasanoilla, tehdä omia asetuksia, tai sammuttaa koko järjestelmän. Ilkeämielinen henkilö voi laatia myös Telnet-skriptin, joka yrittää kirjautua kaikkiin UPS:eihin ja PDU:hin oletussalasanalla ja sammuttaa ne.

6 YHTEENVETO

ICT-ulkoistaminen on yksi nopeimmin kasvavia liiketoiminnan alueita. Tässä tutkielmassa esiteltiin ICT-ulkoistamisen eri tasoja ja analysoitiin niitä. Lisäksi käsiteltiin ITIL-viitekehystä ja erityisesti siihen liittyvää turvallisuuden hallinnan prosessia. Myöhemmin käytiin läpi yleisesti millaisia vaiheita ICT-ulkoistamiseen liittyy ja mitä huomioitavaa vaiheissa on informaatioturvallisuuden kannalta.

ICT-ulkoistamisessa on monenlaisia haasteita informaatioturvallisuuden kannalta. Näistä tärkeimpiä ovat mm. kasvaneet verkkoturvallisuuden riskit, jotka tulevat esille huonosti hoidetussa ja hajanaisessa verkkoympäristössä, esimerkiksi huonosti konfiguroidun palomuurin tapauksessa. Ulkoistusta tehdessä tulee varmistaa, että ulkoistuspalveluja tarjoavan yrityksen ammattitaito ja resurssit ovat ajan tasalla ja palvelulle tulee lisäarvoa, joka huolehtii näistä riskeistä. Myös palvelun luotettavuus on tärkeää, sillä pitkään helpdeskin työjonossa viipyvät esimerkiksi verkkoturvallisuuteen liittyvät palvelupyynnöt voivat olla riskitekijöitä myös informaatioturvallisuuden kannalta. Näitä riskejä voidaan pienentää esimerkiksi ITIL:in mukaisella palvelutaso-sopimuksella, jonka yhteydessä on määritelty sovitut vasteajat. Vasteajan ylittävät palvelupyynnöt voidaan tämän perusteella ottaa eskaloinnin kohteeksi, jolloin palvelupyyntö ohjataan seuraavan tason tukiportaaseen ja tarvittaessa tarkistetaan säännöt, joita vastaavien palvelupyyntöjen tapauksessa tulee noudattaa.

On tärkeää mieltää, että ulkoistamisprosessi ei ole projekti, jolla on selkeä alkamis- ja päättymisajankohta, vaan se on jatkuvaa prosessia, jossa tikettijärjestelmän raporttien, seurantapalaverien ja muiden sovittujen tapojen mukaan seurataan tilanteiden kehittymistä. Myös palvelun tietoturvan testaaminen sekä sosiaalisilla että teknisillä testeillä voi olla oleellinen osa tietoturvapolitiikkaa.

Salasanaturvallisuus on oleellinen osa tietoturvaa. On huolehdittava siitä, että salasanapolitiikka ja käyttäjien osaaminen on sillä tasolla, että esimerkiksi brute-force-hyökkäykset hankaloituvat oleellisesti. Salasanoja on vaihdettava riittävän usein. Tiedon eheydesta on huolehdittava ja varmistettava, että sitä ei päästä tahallisesti tai tahattomasti muuntamaan. Oleellisesti tässä auttaa hyvä identiteetin hallinta ja yhteisillä pelisäännöillä ja laadullisilla kriteereillä toimiva dokumentointi. Dokumentointitaito ja hyvä kirjallinen viestintä ovat tärkeässä asemassa.

Inhimillisiä erehdyksiä on pyrittävä välttämään esimerkiksi asianmukaisella käyttöoikeuspolitiikalla. Myös sosiaalinen hakkerointi on tehtävä mahdollisimman vaikeaksi, kumminkaan yrityksen tuottavuuden siitä kärsimättä.

Erilaiset hälytystoiminnot ovat elintärkeitä ulkoistavan yrityksen toiminnalle. Yksittäisten hälytysten kirjaaminen ei kuitenkaan riitä, vaan tikettijärjestelmästä on voitava ajaa tilastollisia raportteja, joiden avulla voidaan tarkastella systemaattisia ongelmakohtia yrityksen tietoturvassa.

Useille palvelimille jaettu työkuorma, pilvipalvelut ja muutenkin hajautetut järjestelmät ovat vikasietoisempia kuin keskitetyt tai yksittäisillä työasemilla toimivat sovellukset. Ulkoistamisessa on suunniteltava prosesseja, jotka turvaavat tuotannon myös vikatilanteiden, esimerkiksi palvelinrikon tapahtuessa. On huomattava, että palvelun tilapäinen toimivuus ei riitä, vaan palvelun on oltava mahdollisimman yhtäjaksoisesti myös vikasietoinen.

Haasteet ovat uusiutuvia ja niiden hallintaan vaaditaan asiakkaan aktiivista osallistumista ja yhteistyötä ICT-ulkoistajan kanssa. Asiakkaan vastuulla on huolehtia, että hän tilaa sellaista palvelua joka soveltuu asiakkaan omiin tietoturvakäytäntöihin. Toisaalta nämä tietoturvakäytännöt on syytä tarkastaa ITIL-viitekehyksen mukaisiksi. ICT-ulkoistajan vastuulla on ymmärtää informaatioturvallisuuden merkitys ja arvo asiakkaan näkökulmasta, sillä tulee myös olla valmiudet tehdä tietoturvakartoitus asiakkaalle tarpeen vaatiessa kuten ITIL-turvallisuudenhallinnan prosessissa kuvataan (aliluku 2.9.1). Yksi merkittävä informaatioturvallisuuden vaarantaja ICT-ulkoistamisprojekteissa on riittämätön huomio inhimilliseen tekijään, kuten esimerkiksi jos käyttöönoton aikana käyttöönottoa tekevät työntekijät ovat stressaantuneita tai joutuvat työskentelemän kuluttavissa olosuhteissa (Khidzir ym. 2010b, s. 199). Tiukalle vedetyt resurssit johtavat työmäärän jatkuvaan kasaantumiseen ja aiheuttavat stressiä. Tätä ei nopeaa voittoa tavoitteleva yritysjohto aina ota huomioon.

LÄHTEET

Anderson, James M. (2003). Why we need a new definition of information security.*Computers and Security, vol 22, issue 4,* 308-313.

Andress, J. (2011). *The Basics of Information Security - Understanding the Fundamentals of InfoSec in Theory and Practice*. (1. painos). Waltham: Syngress Press.

Baldwin A., Beres Y., Shiu S. & Kearney P. (2006). A model-based approach to trust, security and assurance. *BT Technology Journal*, 24(4), 53-68.

Borisov, N., Goldberg I. & Wagner, D (2010). Security of the WEB algorithm. [Viitattu 13.12.2011]. Saatavilla www-muodossa: <http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html>

Cisco Webex kotisivu (2012). [Viitattu 28.1.2012]. Haettu 28.1.2012 osoitteesta <http://www.webex.com>

Cooke, C. & Oldfield, R. (toim.) (1987). *IEEE Standard for Software User Documentation*. New York: The Institute of Electrical and Electronic Engineers.

Feamster, N. (2010). Outsourcing Home Network Security. Teoksessa C. Gkantsidis, K. Papagiannaki & T. Salonidis (toim.), *Proceedings of the ACM SIGCOMM workshop on Home networks* (s. 37-42). New Delhi, September 3, 2010.

Gonzales, R., Gasco J. & Llopis J. (2005). Information systems outsourcing risks: a study of large firms. *Industrial Management & Data Systems*, 105(1), 45-62.

Hunt, C. (2002). *TCP/IP network administration.* (3. painos). Sebastopol: O'Reilly Media, Inc.

IBM Lotus Notes kotisivu (2012). [Viitattu 28.1.2012]. Haettu 28.1.2012 osoitteesta <http://www.ibm.com/software/lotus/products/notes/>

Jennings, S. E. (2010). Virtually endless possibilities for business communication. *Business Communication Quarterly*, 73(4), 456-459.

Jones, C. G. (2011). Written and computer-mediated accounting communication skills: An employer perspective. *Business Communication Quarterly*, 74(3), 247-271.

Järvinen, P. & Järvinen, A. (2004). *Tutkimustyön metodeista*. Tampere: Opinpaja Oy.

Khidzir, N. Z., Mohamed, A. & Arshad N. H. Hj. (2010a). Information Security Risk Factors- Critical Threats and Vulnerabilities in ICT Outsourcing. Teoksessa Z. A. Bakar, T. M. T. Sembok, H. B. Zaman, P. Bruza, F. Crestani, S. T. Urs & Z. Awang (toim.), *Second International Conference on*

Information Retrieval & Knowledge Management (CAMP) (s. 194-199). Sham Alam Convention Centre, Malaysia. March 17-18, 2010.

Khidzir, N. Z., Mohamed, A. & Arshad N. H. Hj. (2010b). Information Security Risk Management- An Empirical Study on the Difficulties and Practices in ICT outsourcing. Teoksessa B. Werner (toim.), *Second International Conference on Network Applications, Protocols and Services (NETAPPS)* (s. 234-259). Alor Setar, Kedah, Malaysia. IEEE Computer Society. September 22-23, 2010.

Klaic, A. & Hadjina, N. (2011). Methods and Tools for the Development of Information Security Policy – A Comparative Literature Review. Teoksessa P. Biljanovic (toim.), *Proceedings of the 34th International Convention* (s. 1532-1537). Opatija, Croatia, May 23-27, 2011.

Li J., Stephenson B., Motahari-Nezhad H. R. & Singhal S. (2009). A Data Assurance Policy Specification and Enforcement Framework for Outsourced Services. *HP Laboratories* HPL-2009-357. Haettu 20.1.2012 osoitteesta http://www.hpl.hp.com/techreports/2009/HPL-2009-357.pdf

Macfarlane I., Rudd C. (2005). *IT Palvelunhallinta, ITIL Käsikirja* (5. uud. painos). United Kingdom: itSMF ltd.

Martin, R. (2000). Design Principles and Design Patterns. Haettu 5.10.2011 osoitteesta http://www.objectmentor.com/resources/articles/Principles_and_Patterns.pdf

Microsoft Lync kotisivu (2012). [Viitattu 28.1.2012]. Haettu 28.1.2012 osoitteesta <http://office.microsoft.com/lync/>

Mobarhan, R., Rahman A. A. & Majidi M. (2011). Outsourcing Management Framework Based on ITIL v3 Framework. Teoksessa A. W. Yeo, C. W. Shiang, J. Labadin & K. Zen (toim.),*7th International Conference on Information Technology in Asia (CITA*) (s. 1-5). Kuching, Sarawak, Malaysia. July 12-14, 2011.

Moss, M. B. (2007). Comparing Centralized and Distributed Approaches for Operational Impact Analysis in Enterprise Systems. Teoksessa L. O'Conner (toim.), *IEEE International Conference on Granular Computing* (s. 765-769). November 2-4, 2007. Los Alamitos: IEEE Computer Society.

Nagios kotisivu (2012). [Viitattu 28.1.2012]. Haettu 28.1.2012 osoitteesta <www.nagios.org>

Onwubiko, C. & Lenaghan A. P. (2009). Challenges and complexities of managing information security. *Electronic Security and Digital Forensics*, 2(3), 306–321.

Palmila, P. (2008). *Muutoshallinnan kehitys IT-palveluyrityksessä*. Diplomityö. Helsingin teknillinen korkeakoulu, tietotekniikan osasto.

Samariti, P. & De Capitani di Vimercati, S. (2010). Data Protection in Outsourcing Scenarios: Issues and Directions. Teoksessa D. Feng, D. Basin & P. Liu (toim.), *Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security* (ASIACCS '10), *April 13-16* (s. 1-14). Beijing, China.

Sloper, A. (2004). Meeting the Challenge of Outsourcing. *IEEEngineering Management*, *14(3),* 34-37.

sFlow kotisivu (2012). [Viitattu 28.1.2012]. Haettu 28.1.2012 osoitteesta <www.sflow.org>

Sonicwall kotisivu (2012). [Viitattu 28.1.2012]. Haettu 28.1.2012 osoitteesta < http://www.sonicwall.com/us/support/3891.html>

Tandberg kotisivu (2012). [Viitattu 28.1.2012]. Haettu 28.1.2012 osoitteesta <https://www.tangberg.com>

Taylor, S., Case, G., Spalding, G (toim.). (2007a). *ITIL3 Continual Service Improvement* (1. painos). United Kingdom: Blackwell.

Taylor, S., Case, G., Spalding, G. (toim.). (2007b). *ITIL3 Official Introduction* (1. painos). United Kingdom: Blackwell.

Taylor, S., Case, G., Spalding, G. (toim.). (2007c). *ITIL3 Service Design* (1. painos). United Kingdom: Blackwell.

Taylor, S., Case, G., Spalding, G. (toim.). (2007d). *ITIL3 Service Operation* (1. painos). United Kingdom: Blackwell.

Taylor, S., Case, G., Spalding, G. (toim.). (2007e). *ITIL3 Service Strategy* (1. painos). United Kingdom: Blackwell.

Taylor, S., Case, G., Spalding, G. (toim.). (2007f). *ITIL3 Service Transition* (1. painos). United Kingdom: Blackwell.

Winkler, I. (1997). *Corporate Espionage: what it is, why it is happening in your company, what you must do about it.* United States: Prima Publishing.

Xiong, L. (2007). Preserving Data Privacy in Outsourcing Data Aggregation Services. *Transactions on Internet Technology (TOIT)*, 7(3), 1-28.

Zwicky, E. D., Cooper, S. & Chapman D. B. (2001). *Internet-Palomuurien rakentaminen.* Helsinki: Talentum Media Oy.

Wikipedia (2011a). [Viitattu 8.12.2011]. Haettu 8.12.2011 osoitteesta <http://en.wikipedia.org/wiki/ITIL_security_management>

Wikipedia (2011b). [Viitattu 8.12.2011]. Haettu 8.12.2011 osoitteesta <http://fi.wikipedia.org/wiki/PDCA>