764

Markku Aapakari

Pienten ja keskisuurten yritysten tietojenkäsittelyn tietoturvan hallinta sekä tietojenkäsittelyn ulkoistamisen vaikutukset tietoturvallisuuteen.

Tietojärjestelmätieteen
Pro gradu -tutkielma
18.3.1998

Jyväskylän yliopisto
Tietojenkäsittelytieteiden laitos
Jyväskylä

TIIVISTELMÄ

Aapakari, Markku, Mikael
Pienten ja keskisuurten yritysten tietojenkäsittelyn tietoturvan hallinta sekä tietojenkäsittelyn ulkoistamisen vaikutukset tietoturvallisuuteen.
Jyväskylä, Jyväskylän yliopisto, 1998.
134 s.
Pro gradu –tutkielma.

Tässä tutkielmassa tarkastellaan pienten ja keskisuurten yritysten tietoturvan muodostumista , kartoitetaan tietoturvauhkia sekä pyritään selvittämään tietoturvariskien hallintaa. Tietojenkäsittelyn ulkoistamista tietohallintomenetelmänä on käsitelty laajasti ja sen vaikutuksia tietoturvaan on analysoitu.

Tutkielma on yhdistelmä kirjallisuuskatsauksesta sekä pienille ja keskisuurille yrityksille suunnatusta tietoturvakyselystä. Näin on varmistettu lähdemateriaalin sopivuus juuri pienten ja keskisuurten yritysten tarpeita ajatellen.

Tietojärjestelmien ja -ohjelmistojen yhä monimutkaistuessa yritysten kohtaamat tietoturvauhat monipuolistuvat ja kasvavat. Tutkielmassa todetaan kuitenkin, että vaikka esim. teollisuusvakoilu on voimakkaassa kasvussa, yritysten suurin tietoturvariski on edelleen oma henkilökunta.

Tutkielmassa todetaan edelleen, että pienillä ja keskisuurilla yrityksillä on mahdollisuus riskienhallinnan ja erilaisten tietoturvallisuusmenetelmien avulla hallita vallitsevia tietoturvauhkia. Tutkielmassa esitellään myös näitä keinoja.

Tietojärjestelmän ulkoistamisen todetaan olevan monessa suhteessa varteenotettava vaihtoehto pk-yrityksille tietohallintomenetelmänä. Tietoturvallisuutta se ei kuitenkaan välttämättä automaattisesti lisää. Tutkielmassa todetaan, että yrityksellä, joka ulkoistaa tietojenkäsittelynsä täytyy itsellänsä olla hyvä tietoturvaosaaminen; tietojärjestelmäänsä ei missään tapauksessa saa ulkoistaa huonon tietoturvatietämyksen vuoksi.

Tutkielmassa todetaan lisäksi, että osa yrityksistä ei ole sisäistänyt tietoturvan oleellisuutta yhtenä yrityksen kantavista komponenteista, vaikka kaikilla yrityksillä on tietoja, joita ne eivät haluaisi ulkopuolisten saavan.

Avainsanat: Tietoturva
Johtaminen
Ulkoistaminen

SISÄLLYSLUETTELO

1 Johdanto 5
1.1 Tutkimuksen taustaa 5
1.2 Tutkimuksen tavoitteet ja rajaukset 6
1.3 Tutkimusmenetelmät ja tutkimuksen rakenne 7

2 Tietoturva 10
2.1 Tietoturvan peruskäsitteet ja osa-alueiden määritys 11
2.2 Tietoturvallisuuden uhkat ja muodostuvien riskien hallinta 15
2.2.1 SBA eli haavoittuvuusanalyysi 17
2.2.2 Courtney'n menetelmä 20
2.3 Tietoturvaohjeistus 22
2.4 Tietoturvaohjeistuksen luominen yrityksessä 24
2.5 Tietoturvaohjeiden käyttäminen yrityksessä 26
2.6 Tietoturvapolitiikka 26

3 Ulkoistaminen ja tietoturva 29
3.1 Tietojenkäsittelyn ulkoistamisen määritys 30
3.2 Tietojenkäsittelyn ulkoistamisen etuja ja haittoja 33
3.3 Tietoturvaohjeistukset ulkoistamisessa 39
3.4 Tietoturvavaatimuksia tietojärjestelmän ulkoistamisessa 40
3.5 Tietoturvapolitiikka ulkoistamisessa 43
3.6 Yhteenveto 46

4 Yrityskysely 47
4.1 Yritysten tietojenkäsittely-ympäristö 48
4.2 Yritysten kokemia tietoturvallisuusuhkia 50
4.3 Tietoturvan ylläpito yrityksissä 51
4.4 Tietoturvan hallinta yrityksissä 52
4.5 Tietojenkäsittelyn ulkoistamisen valmiudet yrityksissä 54
4.6 Yhteenveto 57

5 Yrityksen tietoturvaan kohdistuvia uhkia 59
5.1 Yrityksen sisäiset tietoturvallisuusuhat 59
5.1.1 Henkilöstöturvallisuus 60
5.1.2 Laitteistoturvallisuus 62
5.1.3 Ohjelmisto- ja järjestelmäturvallisuus 63
5.1.4 Tietoaineisto ja –käyttöturvallisuus 65
5.2 Yrityksen verkkokäytön tietoturvallisuusuhkia 67
5.2.1 Verkkokäytön tietoturvauhkia 67
5.2.2 Verkosta löydetyn tiedon vahingollisuus 70
5.2.3 Elektronisen postin tietoturvauhkia 72
5.2.4 Internetin muodostamia tietoturvauhkia 75
5.3 Tietojärjestelmien ulkoistamisen tietoturvauhkia 77

5.4 Tietokonerikokset 82
5.5 Yhteenveto 85

6 Tietoturvan hallinta yrityksessä 87
6.1 Johtaminen ja tietoturva, riskien hallinta 87
6.1.1 Riskien hallinta 89
6.1.2 Henkilöstö ja tietoturva 89
6.1.3 Tekniset kysymykset 91
6.1.4 Ulkopuolinen apu 92
6.2 Tietoturvan hallinta tietojärjestelmän ulkoistamisessa 93
6.3 Erillisiä tietoturvaratkaisuja 99
6.3.1 Fyysinen suojaus 98
6.3.2 Käytännön komponentteja tietoturvan parantamiseksi 101
6.4 Yhteenveto 108

7 Johtopäätökset 110
7.1 Yhteenveto 110
7.2 Jatkotutkimuskohteet 115

Lähdeluettelo 117

Liitteet: Liite 1: Lyhenteitä ja sanastoa
Liite 2: Yrityskysely
Liite 3: PGP

1 JOHDANTO

1.1 Tutkimuksen taustaa

Tietoturvallisuudella tarkoitetaan tietojen, järjestelmien ja palveluiden asianmukaista suojaamista sekä normaali että poikkeusoloissa lainsäädännön ja muiden toimenpiteiden avulla. Tietojen luottamuksellisuutta, eheyttä ja käytettävyyttä suojataan laitteisto- ja ohjelmavikojen, luonnontapahtumien tai tahallisen, tuottamuksellisten ja tapaturmaisten inhimillisten tekojen aiheuttamilta uhkilta ja vahingoilta. (Hetky 1997)

Tietoturvallisuutta vaarantavat erilaiset uhkatekijät. Uhkasta muodostuu organisaatiolle riski, jos sen todennäköisyys on suurempi kuin nolla (uhkan toteutuminen on mahdollinen), ja jos siitä aiheutuu toteutuessaan huomattavaa välitöntä tai välillistä vahinkoa (vahinkokustannus on merkittävä).

Usein pienten ja keskisuurten yritysten (myöh. pk-yritykset) toiminta perustuu innovatiiviseen ajatteluun, jonka tuloksena on tieto, joka kantaa yritystä. Tämä tieto on elintärkeää yhtiölle ja sen katoaminen tai vuotaminen esim. kilpailijoille vaikeuttaisi olennaisesti yhtiön toimintaa. Näiden yhtiöiden tietoturvasta, sen hallinnasta on hyvin vähän, jos lainkaan, tutkimustietoa Suomessa. Tämän vuoksi on perusteltua selvittää tietoturvan käsittelyä ja hallintaa juuri pienissä ja keskisuurissa yhtiöissä.

Tietojenkäsittelyn ulkoistaminen on noussut uudeksi tietohallintomenetelmäksi. Suuryritykset ovat maailmalla ja Suomessakin yhä kasvavassa määrin ulkoistamassa tietohallintoaan. On arvioitu, että ulkoistaminen lisääntyy 26 prosentin vuosikasvulla (IDC 1997) tulevina vuosina. Vaikka Suomessa tietoturvaa ja tietojärjestelmien ulkoistamista ovat tutkineet ainakin Heikkinen ja Jurvelin (1996) ja

esimerkiksi Douglas (1993), Gates (1992), Oltman (1990), Gupta ja Gupta (1992), Altinkemer, Chaturverdi ja Gulati (1994) sekä Voltti (1994) ovat tutkineet tietojärjestelmien ulkoistamista, tietojenkäsittelyn ulkoistamisen soveltuvuutta pk-yrityksille ja etenkään tietojenkäsittelyn tietoturvan muodostumista ulkoistamistapauksissa ei kuitenkaan ole juurikaan kartoitettu. Kuitenkin ulkoistamispalveluita tarjotaan nykyään hyvinkin aggressiivisesti myös pk-sektorille.

Tietoturvallisuus on tavoitteellista toimintaa. Todennäköisyys sille, että asiat sujuisivat omalla painollaan, on järjestelmien monimutkaistuessa pieni. Tietoturvallisuutta toteutetaan käytännössä vahingontorjunnalla. Vahingontorjunta perustuu tietoturvariskin hallintaan.

Tietoturvallisuuden tavoitteiden tulee lähteä tarpeesta eikä järjestelmän ominaisuuksista. Kun tiedetään, miten hyvin jotakin tietoa halutaan suojata, voidaan valita sille asianmukainen säilytystapa ja riittävät suojaustoimenpiteet.

1.2 Tutkimuksen tavoitteet ja rajaukset

Tämä tutkimus pyrkii vastaamaan kysymyksiin:

- Mitkä ovat tietoturvan painopistealueet pk-yrityksissä?
- Kuinka tietoturvaa käytännössä hallitaan pk-yrityksissä?
- Kuinka tietoturvaa tulisi hallita pk-yrityksissä?
- Mitkä ovat tietojenkäsittelyn ulkoistamisen vaikutukset pk-yrityksen tietoturvaan ja sen hallitsemiseen.

Tutkimuksessa pyritään toisin sanoen analysoimaan pienten ja keskisuurten yhtiöiden tietoturvan hallintaa. Siinä pyritään määrittämään olemassa olevia tietoturvariskejä ja esittämään ratkaisumalleja niiden hallitsemiseksi. Tämä tutkimus pyrkii myös selvittämään suomalaisten pienten ja keskisuurten yhtiöiden

suhtautumista tietoturvaan ja sen hallitsemiseen. Erityisesti, varsin uutena asiana, käsitellään tietojärjestelmän ulkoistamisen vaikutuksia tietoturvaan ja sen hallintaan.

Monet kysymykset, erityisesti tietojen eheyteen liittyvät, saattavat tulla käsiteltyä aivan eri yhteyksissä. Tämä on sinänsä täysin oikein, ne saattavat varsin hyvin kuulua turvallisuuden sijasta hyvään järjestelmäsuunnitteluun. Turvallisuutta suunniteltaessa on kuitenkin varmistauduttava, että keskeiset asiat löytyvät jostakin. Tämä tutkimus painottuu siis tietoturvan osa-alueista tiedon luottamuksellisuuteen ja saatavuuteen, joskin muitakin osa-alueita käsitellään, koska ne eivät ole suinkaan irrallisia.

Tutkimuksen luonteen vuoksi yhtiöiden tietoturvasuojaa ei ole voitu loukata. Tämä seikka rajaa tutkimuksesta pois eräiden asioiden, lähinnä järjestelmien ja ohjelmistojen, yksilöidyn ja yksityiskohtaisen tarkastelun. Sen sijaan tutkimuksessa pyritään keskittymään yhtiöiden tietoturvasuojaan yleisellä tasolla. Tutkimuksessa pyritään selvittämään myös mahdollisia rakenteellisia ja asenteellisia kysymyksiä.

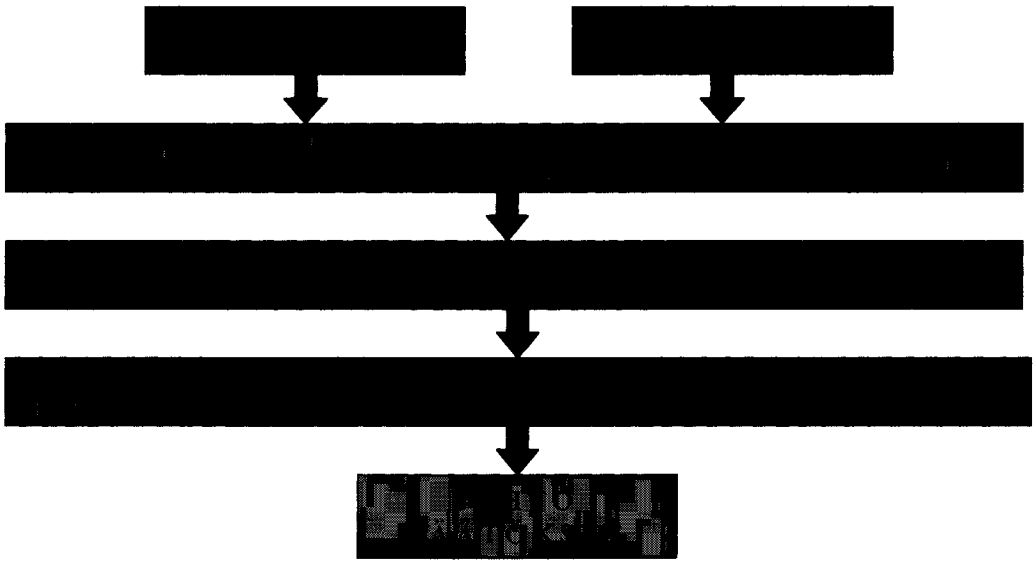
1.3 Tutkimusmenetelmät ja tutkimuksen rakenne

Tutkimus pyrkii kartoittamaan kentän, jolla pelataan, selvittämällä aluksi kirjallisuushakuun perustuen tietoturvallisuuden rakenteen sekä tietojenkäsittelyn ulkoistamisen olemuksen ja sen vaikutuksia tietoturvaan. Näiden perusteella tutkimuksen empiirisen osan muodostaa yrityksille suunnattu kyselytutkimus, jolla selvitettiin pk-yritysten tietojenkäsittely-ympäristöä, niiden kokemia tietoturvauhkia ja niiden tietohallintokäytäntöjä tietoturvan suhteen sekä niiden lähtökohtia tietojenkäsittelyn ulkoistamiseen. Tältä pohjalta tutkimuksessa tuodaan esille tietoturvallisuuteen kohdistuvia ongelmia ja keinoja niiden vähentä-

miseen. Lopulta edellä esitetyn pohjalta ja kirjallisuuteen perustuen voidaan esittää keinoja muodostuneiden tietoturvariskien hallintaan sekä kuvata tietojenkäsittelyn ulkoistamisen vaikutuksia tietoturvallisuuteen ja sen hallintaan.

Tutkimuksen pohjana on kirjallisuuskatsaus tietoturvasta ja tietojenkäsittelyn ulkoistamisesta. Tietoturva käsitteenä ja yrityksen yhtenä peruskivenä käsitellään luvussa 2. Tietojärjestelmien ulkoistamista on pyritty selvittämään varsin uutena asiana perusteellisesti ja laajasti luvussa 3. Kyselytutkimus, jolla pyrittiin selvittämään yritysten yleistä tietojenkäsittely-ympäristöä suhteessa tietoturvaan, suhtautumista tietoturvaan ja tietohallintokäytäntöjä puretaan luvussa 4. Kirjallisuuden ja mainitun kyselyn perusteella voidaan määrittää todelliset tietoturvauhat ja kyetään esittämään niihin ratkaisumalleja ongelmatasolla luvussa 5.

Luvussa 6, kyselyn sekä edellä esitetyn pohjalta ja kirjallisuuteen perustuen, määritellään ja muodostetaan kuva yritysten keinoista tietoturvan hallintaan ja selvitetään yritysten valmiutta ja lähtökohtia tietohallinnon ulkoistamiseen ja tämän vaikutuksia tietoturvaan. Luvussa 7 esitetään johtopäätökset.(Kuvio 1)



Kuvio 1: Tutkimuksen rakenne

Kyselytutkimuksessa on pk-yritykset rajattu siten, että kysely suunnattiin yrityksille, joiden vuotuinen liikevaihto on 10 - 25 miljoonaa markkaa ja toisaalta yrityksille joiden vuotuinen liikevaihto on 100 ja 150 miljoonan markan välillä (Yritys - Suomi CD 2/97, 1997). Näin saadaan hahmotettua yrityskoon mahdolliset vaikutukset kyselyssä esitettyihin asioihin. Näitä kahta ryhmää käsitellään tutkimuksessa erikseen, mikäli yritysryhmien välillä on merkittäviä eroja, muuten yrityksiä käytetään yhtenäisenä ryhmänä. Rajaus on tutkijan itsensä valitsema, ja kuvaa hyvin suomalaista yritysrakennetta; yritykset ovat toiminnaltaan varsin paikallisia. Sanottakoon, että rajaaminen on hyvin vaikeaa, koska tapoja määrittää yrityksen koko on lukuisia.

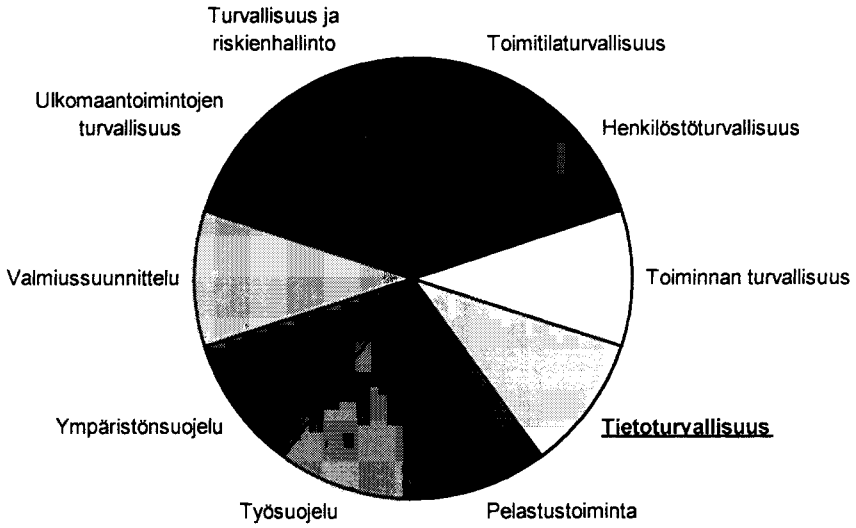
Kysely (liite 2) lähetettiin 120 yritykselle, joiden liikevaihto on 10-25 miljoonaa markkaa. Näitä yrityksiä oli mainitussa lähteessä 870 kpl. Ja toisaalta kysely lähetettiin 120 yritykselle, joiden liikevaihto on 100 - 150 miljoonaa markkaa. Vastaavasti näitä yrityksiä oli lähteessä 411 kpl. Kyselyyn vastasi ensimmäisestä ryhmästä 52 ja toisesta ryhmästä 46. Kysely osoitettiin yritysten johdolle.

Edellä mainittu käsittelytapa on mielestäni oivallinen pohja ja maasto käsitellä tietoturva-aihetta pk-yritysten tarpeita vastaavasti ja niitä kartoittaen.

2 TIETOTURVA

Tietoturva on osa yrityksen turvallisuustoimenpiteitä. Yritysturvallisuus voidaan (Miettinen & Kajava 1991) jaotella seuraavasti (Kuvio 2):

- Toimitilaturvallisuus
- Henkilöstöturvallisuus
- Toiminnan turvallisuus
- Tietoturvallisuus
- Pelastustoiminta
- Työsuojelu
- Ympäristönsuojelu
- Valmiussuunnittelu
- Ulkomaantoimintojen turvallisuus
- Turvallisuus ja riskienhallinto



Kuvio 2: Yritysturvallisuuden jaottelu

On hyvin vaikea kuvitella yritystä, jossa ei olisi mitään tietoa, jota ei jollakin tavoin pitäisi suojella. Tiedon luokittelu onkin ensimmäisiä toimenpiteitä, kun tietoturvaa aletaan soveltaa yrityksen toiminnoissa. On tärkeää, että tietoturvaa parantavat toimet kohdistuvat tasapuolisesti yrityksen kaikille osa-alueille. On huomattava antaa kaikille resursseille riittävä suoja ja panostaa enemmän niiden resurssien suojaamiseen, jotka sitä eniten tarvitsevat. Täydellinen tietoturva merkitsee äärettömiä kustannuksia ja olematon tietoturva merkitsee kestämättömiä menetyksiä (Murray 95). Usein riittää, että yrityksen toiminnalle tärkeät tiedot on suojattu ja varmistettu riittävän hyvin. Näin varmistetaan toiminta myös mahdollisen kriisitilanteen jälkeen.

Tietoturvan peruskäsitteet, saatavuus, eheys ja luottamuksellisuus ja tarkastettavuus muodostavat perinteisen mallin tietoturvan perustasta (Parker 1995). Tässä luvussa perehdytään tietoturvan ominaisuuksiin, käsitteisiin ja hallintaan yleisellä tasolla.

2.1 Tietoturvan peruskäsitteet ja osa-alueiden määritys

Tietoturvan perustekijät ja tavoitteet voidaan (Mm. Miettinen & Kajava 1994a, Parker 1995) jakaa neljään osaan (Kuvio 3).

- Tiedon luottamuksellisuus (confidentiality)
- Tiedon saatavuus (availibility)
- Tiedon eheys (integrity)
- Tiedon tarkastettavuus (audit)

Tiedon luottamuksellisuudella tarkoitetaan, että tiedot ovat vain niihin oikeutettujen käytettävissä. Tietojen ja dokumenttien turvaluokitus määrittelee, kenellä on oikeus tietoihin sekä niiden säilytykseen ja tuhoamiseen. Yksilön tietosuoja (privacy) määrittelee yksityistä ihmistä koskevien tietojen käsittelystä.

Tiedon saatavuudella tarkoitetaan, että tiedot, laitteet ja palvelut saadaan käyttöön niitä tarvittaessa. Saatavuus on pyrittävä takaamaan kaikissa olosuhteissa. Saatavuuteen kuuluu myös varaosien, tarvikkeiden, varalaitteistojen ja ohjelmistopäivitysten saatavuuden varmistaminen. Tietojärjestelmän kriittiset osat ja tiedot määritellään ja niiden saatavuus varmistetaan myös katastrofitilanteissa.

Tiedon eheys eli oikeellisuus tarkoittaa tiedon muuttumattomuutta syötön, varastoinnin, käsittelyn ja tiedonsiirron aikana. Lisäksi vaaditaan etteivät tiedot muutu eivätkä häviä laitteisto-, ohjelmisto- ja tiedonsiirtovirheiden eikä minkään luvattoman toimenpiteen seurauksena.

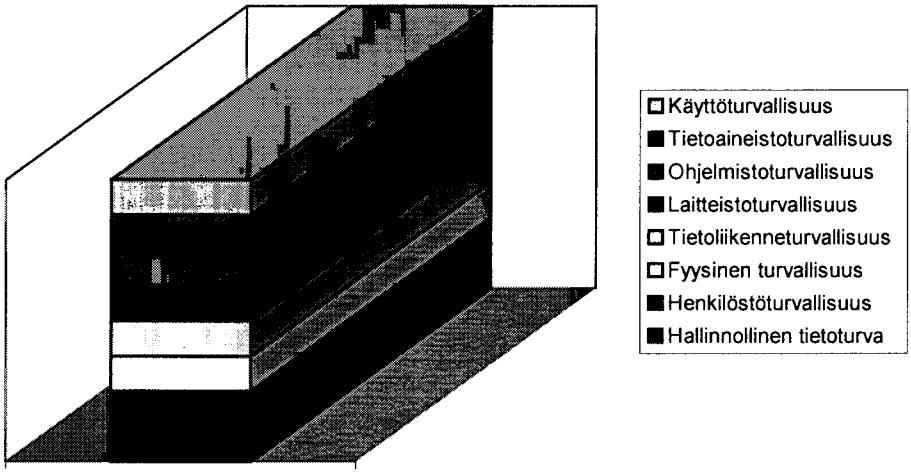
Tiedon tarkastettavuus taas voidaan selittää seuraavasti: Tietojenkäsittely ja sen tuloksena saatu tieto on kyettävä tarkastamaan ja osoittamaan sen oikeellisuus. Tiedon tarkastettavuus on olennaista, jotta edellä olevat kolme periaatetta voivat toteutua ja ne voidaan todeta olevan kunnossa. Tietoturvaongelman ilmettyä pitää olla mahdollista tarkistaa ja jäljittää syy ja aiheutuneet vahingot. Tarkastaminen on tehtävä mahdolliseksi tietojärjestelmän tekijän ja atk-asiantuntijoiden lisäksi myös toiminnan tarkastajille, jotka eivät ole atk-asiantuntijoita.

Kuvio 3: Tietoturvan perustekijät

Tietoturvan hallinta jakaantuu vastaavasti eri osa-alueisiin, joista jokainen on huomioon otettava. Tietoturvan eri osa-alueiden määrityksessä on käytetty Valtiovarainministeriön (1992) ja Liikenneministeriön Valmiusohjeen (1995) mukaista jaottelua. Tietoturvallisuudella pyritään varmistamaan tietojen loukkaamattomuus tietojen ollessa tietojärjestelmässä sähköisessä, optisessa tai jossakin vastaavassa muodossa.(Kuvio 4)

- *Hallinnollinen tietoturva* tarkoittaa niitä toimenpiteitä, joilla määrätään noudatettavista periaatteista ja toimintalinjoista yleensä. Hallinnollinen tietoturva on muiden tietoturvan osa-alueiden strateginen lähtökohta. Hallinnollinen tietoturvallisuus muodostaa perustan tietoturvallisuustoiminnalle. Hallinnollisella turvallisuudella varmistetaan organisaation johdon ja henkilöstön sitoutuminen tietoturva-asioiden järjestelmälliseen kehittämiseen ja hoitamiseen.
- *Henkilöstöturvallisuus* tarkoittaa henkilöstöön liittyvien luotettavuusriskien hallintaa toimenkuvien, käyttöoikeuksien määrittelyiden sekä turvallisuuskoulutuksen ja valvonnan avulla. Henkilöstöturvallisuus ulottuu organisaation vakinaiseen ja tilapäiseen henkilöstöön sekä organisaatiolle palveluja tarjoaviin toimittajiin ja heidän henkilöstöönsä.
- *Fyysinen turvallisuus* tarkoittaa laitteisto-, käyttö- ja varastointitilojen, arkistojen sekä laitteiden ja materiaalien fyysistä turvaamista. Fyysinen turvallisuus muodostuu erilaisista fyysisistä suojauksista ja pääsykontrolleista järjestelmässä.
- *Tietoliikenneturvallisuus* tarkoittaa niitä televiestintään liittyviä toimenpiteitä, joilla pyritään varmistamaan tietoverkossa välitettävien tietojen luottamuksellisuus, eheys ja käytettävyys.
- *Laitteistoturvallisuus* tarkoittaa tietojenkäsittely ja tietoliikennelaitteiden kokoonpanoon, kunnossapitoon ja laadunvarmistukseen liittyviä turvaominaisuuksia. Jokainen tietoverkossa käytettävä fyysinen laite sisältää joukon turvallisuusominaisuuksia, jotka vaikuttavat laitteistoturvallisuuteen.

- *Ohjelmistoturvallisuus* tarkoittaa tietojenkäsittelylaitteistojen käyttöjärjestelmien ja sovellusohjelmien samoin kuin tietoliikennejärjestelmien ohjelmien turvaominaisuuksia. Ohjelmistoturvallisuus käsittää myös edellä mainittujen ohjelmien käyttömahdollisuudet.
- *Tietoaineistoturvallisuus* tarkoittaa asiakirjojen, tietueiden ja tiedostojen tunnistamista ja turvaluokitusta sekä tietovälineiden hallintaa ja säilytystä niiden kaikissa eri käsittelyvaiheissa luomisesta hävittämiseen. Tietoaineistoturvallisuus käsittää kaikki eri talletusmuodossa olevien tietojen suojauksen.
- *Käyttöturvallisuus* tarkoittaa henkilöstön turvallisia käyttöperiaatteita, käyttöympäristöön ja varsinaisen tietojenkäsittelyn turvallisuuteen vaikuttavien tapahtumien sekä toiminnan jatkuvuuden turvaamiseen vaikuttavien tapahtumien valvontaa sekä toiminnan jatkuvuuden turvaamiseen liittyvien menettelytapojen käyttöä. Edellä mainittujen menettelytapojen käyttö edistää tietojärjestelmän turvallisuutta tietojärjestelmän käyttötapoihin vaikuttamalla.



Kuvio 4: tietoturvan osa-alueet

2.2 Tietoturvallisuuden uhat ja muodostuvien riskien hallinta

Tietoturvallisuusuhkia kohdistuu monelta taholta. Analysoitaessa uhkatekijöitä tulee huomioida seuraavat tekijät: mistä uhka tulee, millaisia seurauksia se voi aiheuttaa, kuinka vakava on aiheutettu vahinko ja kuinka se korjataan sekä miten uhka aiheuttaa vahingon.

Turvallisuusuhkien aiheuttajia voivat olla oma henkilökunta, teollisuusvakoilu, tulipalot, vesivahingot, tekniset viat, ulkopuoliset tunkeutuja ja tietokonevirukset. Suurimman uhan aiheuttaja määräytyy sovelluksen ja ympäristön mukaan. Perinteisesti oma henkilökunta on muodostanut suurimman uhan, mutta Internetin käyttäjäkunnan laajentuminen lisää ulkoisen uhan asemaa.

Aiheutuneet tietoturvavahingot voivat olla turvallisuutta heikentäviä, tietoihin kohdistuvia tai laitteistoihin kohdistuvia.(Caelli 1991)

- *Turvallisuutta heikentävät* vahingot eivät itsessään ole haitallisia, vaan altistavat systeemin muille uhille. Tällaisia ovat mm. varmuuskopiointivirheet, virheelliset ohjelmat, ulkopuolisten tunkeutuminen järjestelmään ja järjestelmän turvatasojen murtaminen. Virheellisten ohjelmien aiheuttamat tietoturvavahingot ovat lisääntyneet ohjelmien tuotantonopeuden ja kilpailun lisääntyessä, jolloin uusia ohjelmia ei ole kunnolla testattu.
- *Tietoihin kohdistuvia* vahinkoja ovat tietojen vuoto ja varastaminen, tietojen tuhoutuminen tai korruptoituminen sekä väärän tiedon luonti ja levitys.
- *Laitteistoihin kohdistuvia* tietoturvavahinkoja ovat laitteiston turmeleminen tai varastaminen sekä virheiden aiheuttaminen laitteiston toimintaan. Laitteistojen varastaminen on viime aikoina lisääntynyt yhä enemmän. Varkaustapauksissa on kiusallista arvokkaan datan katoaminen varkaalle, joka on kiinnostunut vain laitteistosta.

Vahingoilta suojautumisessa on olennaisen tärkeää ennakkosuunnittelu. Riskit on analysoitava ennakolta, todennäköiset uhat sekä turvallisuusjärjestelmän kyvyt on tiedostettava ja on suunniteltava ja luotava oikeantasoiset suojatoimenpiteet.

Tietoriskien tunnistaminen on edellytyksenä suojautumiselle niitä vastaan. Siinä etsitään järjestelmällisesti tietosysteemiä uhkaavat vaaratekijät. Riskien tunnistamisessa voidaan käyttää esim. Parkerin uhkamallia(ks. taulukko 1), jossa uhkapolkujen avulla ja niitä tutkimalla kyetään löytämään uhkat. (Miettinen 1994)

Lähteet	Motiivit	Teot	Seuraukset	Vahingot
Ihmiset	Taloudelliset	Tahattomat	Muuntuminen	Taloudelliset
Luonnonvoimat	Kateus	Tahalliset	Tuhoutuminen	Fyysiset
	Poliittiset		Häviäminen	Imago
	Sosiaaliset			

Taulukko 1: Parkerin uhkamalli

Riskien etsiminen voidaan aloittaa jakamalla järjestelmä ensin pienempiin osiin ja määrittelemällä näihin kohteisiin liittyvät uhat. Toiminnalle on asetettava ennen sen aloittamista tavoitteet, joihin pyritään. Riskien tunnistaminen voidaan tehdä käyttäen kokemusperäistä tietoa käyden järjestelmällisesti läpi kohteet ja niihin liittyvät riskit. On välttämätöntä selvittää kaikki mahdolliset uhkat, vaikka ne olisivat epätodennäköisiä. Riskien arvioinnin yhteydessä ohitetaan uhkat, jotka eivät ole todellisia. Tunnistaminen ei saa olla summittaista arvaamista ilman selkeää suunnitelmaa ja kirjallista raportointia. (Tässä tutkimuksessa kartoitetaan pk-yritysten tietoturvauhkia yrityskyselyn ja kirjallisuuden avulla. Havaittuja uhkia käsitellään perusteellisemmin luvussa 5.)

Lähtötilanteessa tulee selvittää olemassa olevan järjestelmän turvallisuuden heikkoudet ja vahvuudet. Tutkitaan toimitilat ja haastatellaan avainhenkilöjä sekä tutustutaan järjestelmän normaalikäyttöön ja rutiineihin. Käydään läpi jär-

jestelmän dokumentit sekä yrityksen tietoturvapolitiikka(ks. 2.6) ja järjestelmän tarjoamat tietoturvaominaisuudet kuten sisäänkirjautuminen ja käyttöoikeudet. Tällöin saadaan selville järjestelmässä olevat (tunnetut) riskit. Seuraavassa vaiheessa selvitetään uudet riskitekijät, jotka voivat pohjautua ensimmäisessä vaiheessa tehtyyn työhön. Uudet uhkat voivat johtua teknologiasta, ihmisistä tai ympäristöstä.

Uhkasta voi muodostua yritykselle tietoinen riski, jos uhka voi aiheuttaa vahinkoa ja jos uhkaa ei saada kokonaan eliminoitua tai sen poistaminen on hyvin kallista tai mahdotonta. Tämä edellyttää kuitenkin riskien määrittämistä. Kuten aikaisemminkin tässä tutkimuksessa on todettu, tietoturvan hallitseminen on riskien hallintaa. Yrityksen tietoturvariskien hallinnassa voidaan soveltaa useita menetelmiä. Seuraavaksi esitellään kaksi käytössä olevaa menetelmää. Kvalitatiivisena menetelmänä SBA eli haavoittuvuusanalyysi ja kvantitatiivisena mallina Courtney'n menetelmä.

2.2.1 SBA eli haavoittuvuusanalyysi

SBA eli haavoittuvuusanalyysi(sårbarhetsanalys) on Ruotsissa "Dataföreningen i Sverige" –yhdistyksen sekä liike-elämän ja julkisen sektorin yhteistyössä kehittämä menetelmä. Se koostuu 7 osasta, joita voidaan käyttää myös erikseen. Menetelmä perustuu käyttäjien määrittelemien uhkatilanteiden ja niiden vaikutusten arviointiin.

Menetelmän kehitystyölle asetettiin seuraavia vaatimuksia:
Organisaation tulee itse kyetä arvioimaan menetelmän avulla tietojärjestelmänsä haavoittuvuus ja sen riippuvuus ulkopuolisista järjestelmistä. Analyysin tulee olla selkeä ja helposti ymmärrettävä sekä vähän koulutusta vaativa. Menetelmä

soveltuu yksittäisen tietojärjestelmän sekä koko organisaation systeemin analysointiin.

Menetelmä perustuu kolmen avaintietoriskin analysointiin:

1. Tiedon laatu (Virheettömyys, ajantasalla olo, kattavuus)
2. Tietojärjestelmien keskeytykset
3. Tietojen valtuuttamaton käyttö (Paljastuminen, muuttaminen)

Menetelmällä pystytään käsittelemään sekä tahallisia että tahattomia uhkia.

Menetelmään kuuluvat seuraavat osat:

Käynnistys (Introduction): Organisaation johdon karkea arvio haavoittuvuudesta. Arviointi suoritetaan kyselylomakkeen avulla, johon vastaavat kunkin osa-alueen johtajat. Kunkin valitun tehtävän tai toiminnon osalta arvioidaan edellä mainitut kolme avainriskiä. (ks. Kuvio 5)

Esim. Tarkastellaan tietojen valtuuttamatonta käyttöä.

Kysymys: Mitä seurauksia on yritykselle, jos tietojärjestelmän sisältämä tieto joutuu väärien henkilöiden tietoon.

SEURAUKSET	VAIKUTUKSET			
	EI	**VÄHÄN**	**PALJON**	**TUHOISA**
KUSTANNUKSET				
TULOT				
MARKKINAOSUUS				
SOPIMUKSET				
LAIT				
IMAGO				
MUUTA(määrittele)				

Kuvio 5: Avainriskien arviointi

Organisaation ylin johto analysoi vastaukset ja tuloksena saadaan haavoittuvimmat toiminnot. Tämän vaiheen tulosten pohjalta päätetään, käynnistetäänkö Alustava tutkimus -vaihe.

Alustava tutkimus: Tutkitaan yksityiskohtaisemmin kuin Käynnistys -vaiheessa toimia, jotka on todettu kaikkein haavoittuvimmiksi. Ensin tutkitaan organisaation osat, joihin toiminto liittyy ja jotka ovat siitä riippuvia. Seuraavaksi tutkitaan toimintoon liittyvää tietojenkäsittelyä sekä sovellutusten vaativuutta. Lopuksi asetetaan osastot ja sovellukset tärkeysjärjestykseen.

Pidetään kokous, jossa päätetään, kuinka menetellään ja mihin tietoturvatoimenpiteisiin ryhdytään valittujen toimintojen osalta.

Skenaario-osa: Skenaario-osa on tärkein SBA:n analysointimenetelmä. Kuviteltujen tapausten avulla kuvataan uhkia ja niiden aiheuttamia vaikutuksia eri kohteille. Selvitetään uhkien syntymiseen vaikuttavat tekijät, vahinkojen suuruus ja todennäköisyys. Nämä ns. uhkaskenaariot analysoidaan ja tehdään alustavat toimenpide-ehdotukset. Skenaarioiden tekemiseen osallistuvat kaikki tietojärjestelmän käyttöön liittyvät työntekijäryhmät. Skenaarioiden laatiminen vaatii useita päiviä aikaa sekä monia henkilöryhmiä, joten se on useimmiten paras toteuttaa seminaarina.(Miettinen & Kajava 1994b)

Uusi järjestelmä: Uuden järjestelmän hankintaa valmisteltaessa analysoidaan, kasvaako organisaation haavoittuvuus sen myötä. Vaiheen toteutus on samanlainen kuin Alustava tutkimus -vaihe, mutta tutkitaan ainoastaan hankittavaa järjestelmää.

Projekti – osa: Projektityön riskien arviointi: vaikutukset laatuun, projektin etenemiseen, valmistuminen, kustannukset. Projektista tutkitaan seuraavia osa-alueita:

- Projektin koko
- Toimiala
- Tekniikka ja välineet
- Projektiorganisaatio
- Projektin sidosryhmät

Tuloksena saadaan kultakin osa-alueelta sekä koko projektista riskiluokitus (korkea, keski, matala).

Systeemin kehitystyö: Määrittelee toimenpiteet systeemin suunnittelun eri vaiheissa, jotta tarvittava tietoturva saavutetaan suunnittelun eri vaiheissa.

Auditointi –osa: Määrittelee, kuinka atk-tarkastajat voivat käyttää menetelmiä työssään.

2.2.2 Courtney'n menetelmä

Yrityksen tietoturvariskejä voidaan arvioida myös *matemaattisin menetelmin. Robert Courtney* (IBM) kehitti 70-luvun lopulla kvantitatiivisen riskianalysointimenetelmän. Menetelmä on otettu USA:n valtion virastojen riskianalyysistandardiksi ja sen pohjalta on toteutettu monia analysointiohjelmia.

Menetelmä perustuu arvioihin kunkin uhan esiintymislaajuudesta p sekä toteutuneen uhkan aiheuttamista menetyksistä v.

Uhkien esiintymistaajuus P saadaan kaavasta:

P=10^ (p-4), missä p saa arvon
0 - ei koskaan

1 - kerran 1000 vuodessa

2 - kerran sadassa vuodessa

3 - kerran kymmenessä vuodessa

4 - kerran vuodessa

5 - kerran kuukaudessa (10 kertaa/v)

6 - kaksi kertaa viikossa (100 kertaa/v)

7 - kolmesti päivässä (1000 kertaa/v)

Uhkan aiheuttama menetys V saadaan kaavasta:

V=10^v, jossa v saa arvon (kertavahinko, mk):

0 - 5

1 - 50

2 - 500

3 - 5000

4 - 50000

5 - 500000

6 - 5000000

. . .

Menetysten vuotuisten kustannusten odotusarvo E saadaan kaavalla:

E=V*P=10^(v+p-4)

Saadun arvon E perusteella voidaan riskit ja suojaukset asettaa tärkeysjärjestykseen. Vuotuisen menetysten ja suojausten vaatimien kustannusten vertailu tuo esille suojausten kannattavuuden. Menetelmän käytön ongelmana on tilastollisen tiedon puute, jolloin lähtötiedot ovat arvioita. Edellisestä johtuen ovat kaavoissa esiintyvät v ja p määritelty varsin karkeasti.(Miettinen & Kajava.1994b)

2.3 Tietoturvaohjeistus

Yrityksen on muodostettava selkeä kuva suhteestaan tietoturvallisuuteen. Tietoturvaohjeistus määrittelee käytettävät linjaukset ja toimintamallit poikkeustilanteita varten. Tietoturvaohjeistuksessa voidaan mennä hyvinkin yksilölliselle tasolle (ks. loppukäyttäjän ohjeistukset 2.3), jos yrityksen työntekijäin työnkuvat poikkeavat suuresti toisistaan.

Tietoturvaohjeistuksen aluksi organisaation on selvitettävä olemassa olevat resurssit: talous, henkilöstö, laitteistot ja ohjelmistot. Jos resurssit eivät riitä tietoturvapolitiikan toteuttamiseen, määritellään lisäresurssien määrä ja laatu. Tietoturvan toteuttamiseen varataan ja valitaan tarvittavat henkilöresurssit. Tietoturvasta vastaavat henkilöt voivat toimia organisaation koosta ja toiminnan laadusta johtuen joko oman toimensa ohella tai pelkästään tietoturvaan keskittyen. Yrityksen sisällä tulee määritellä tietoturvahenkilöstön paikka ja toiminta-edellytykset organisaatiossa. Vaikka yrityksellä on tietoturvaorganisaatio, on koko henkilöstölle tehtävä selväksi vastuu tietoturvasta.

Nykyajan organisaatiossa tiedot eri muodoissaan ovat kriittinen tekijä. Vaikka tietojenkäsittely ei olisikaan organisaation päätoimiala, vaatii toiminta aina pohjakseen tietoja eri asioista. Tietojen kriittisyys heijastuu myös niitä käsitteleviin ja säilyttäviin järjestelmiin.

Yrityksen tiedot voivat olla monessa olomuodossa. Asiakirjat ovat paperilla, tietokannat tietokoneella. Lisäksi organisaatiossa on aina tietoa, joka ei ole varastoituna mihinkään yksittäiseen paikkaan, se on organisaatiossa itsessään ja siinä toimivissa henkilöissä. Oma lukunsa ovat vielä avainhenkilöt ja heidän päässään olevat tiedot.

Eri tyyppiset tiedot ovat eri tavalla tärkeitä yritykselle. On tietoja, joiden tulee olla ehdottoman luottamuksellisia: sopimuksia, suunnitelmia, tutkimuksia ja niin edelleen. Toisaalta on tietoja, joiden tulee olla aina käytettävissä: varastotilanne, kirjanpito, tilaukset. Kaikista näistä on kuitenkin asiaankuuluvalla tavalla pidettävä huoli, jotta yritys pystyisi toimimaan.

Koska tiedot ovat tärkeitä yrityksen toiminnalle, on luonnollista, että niihin suhtaudutaan asiaankuuluvan huolellisesti. Huolellisuus tarkoittaa mm. sitä, että keskeiset tietovarastot ja merkitys organisaatiolle tunnetaan. Vasta uhkien tuntemisen jälkeen voidaan kunnolla päättää, mitä riskejä halutaan ottaa.

Tietovarastojen ja niihin liittyvien riskien selvittäminen on jo lähellä tietojen luokittelua. Tunnistamalla varastot ja niiden yritykselle aiheuttamat uhat voidaan tietoaineisto luokitella. Kun lisäksi tunnetaan tietovarastoa uhkaavat tekijät, voidaan valita suojautumistoimenpiteet. (Holbrook & Reynolds 1991)

Organisaation ylimmän johdon tai turvallisuusyksikön tehtävänä on hyväksyä kunnolliset tietoturvaohjeistukset organisaatiolle. Organisaation tietoturvaohjeistuksien lähtökohtana ovat tunnistetut tietoturvauhkat ja -riskit. Tietoturvan perusvaatimusten mukaan voidaan muodostaa organisaation tietoturvaohjeistukset.

Organisaatiossa tietoturvan käytännön toteuttaminen jää lopulta tietojärjestelmän loppukäyttäjien vastuulle. Jos organisaation käytössä on tietoturvaohjeistuksia, mutta niiden käytännön toteuttamista ei valvota, ei tietoturvaohjeistuksien linjauksia välttämättä noudateta. Yksityiskohtaiset *loppukäyttäjien ohjeistukset* on laadittava tapauskohtaisesti, koska konkreettiset tietoturvatarpeet voivat olla erilaiset organisaation eri toimipisteissä ja eri yksiköitä ulkoistettaessa. Tietojärjestelmän ulkoistaminen voidaan toteuttaa hyvin usealla tavalla ja nämä eri toteutustavat aiheuttavat erilaisia vaatimuksia tietoturvalle.

Tietojärjestelmän loppukäyttäjien ohjeistuksissa voidaan määrittää esimerkiksi kuinka monta isoa ja pientä kirjainta käyttäjien salasanoissa tulee vähintään olla, montako erikoismerkkiä salasanassa tulee olla ja montako samaa merkkiä voi olla peräkkäin. Loppukäyttäjien ohjeistuksissa voidaan kieltää työpaikalla sijaitsevien laitteiden, tiedostojen ja dokumenttien vienti työpaikan ulkopuolelle.

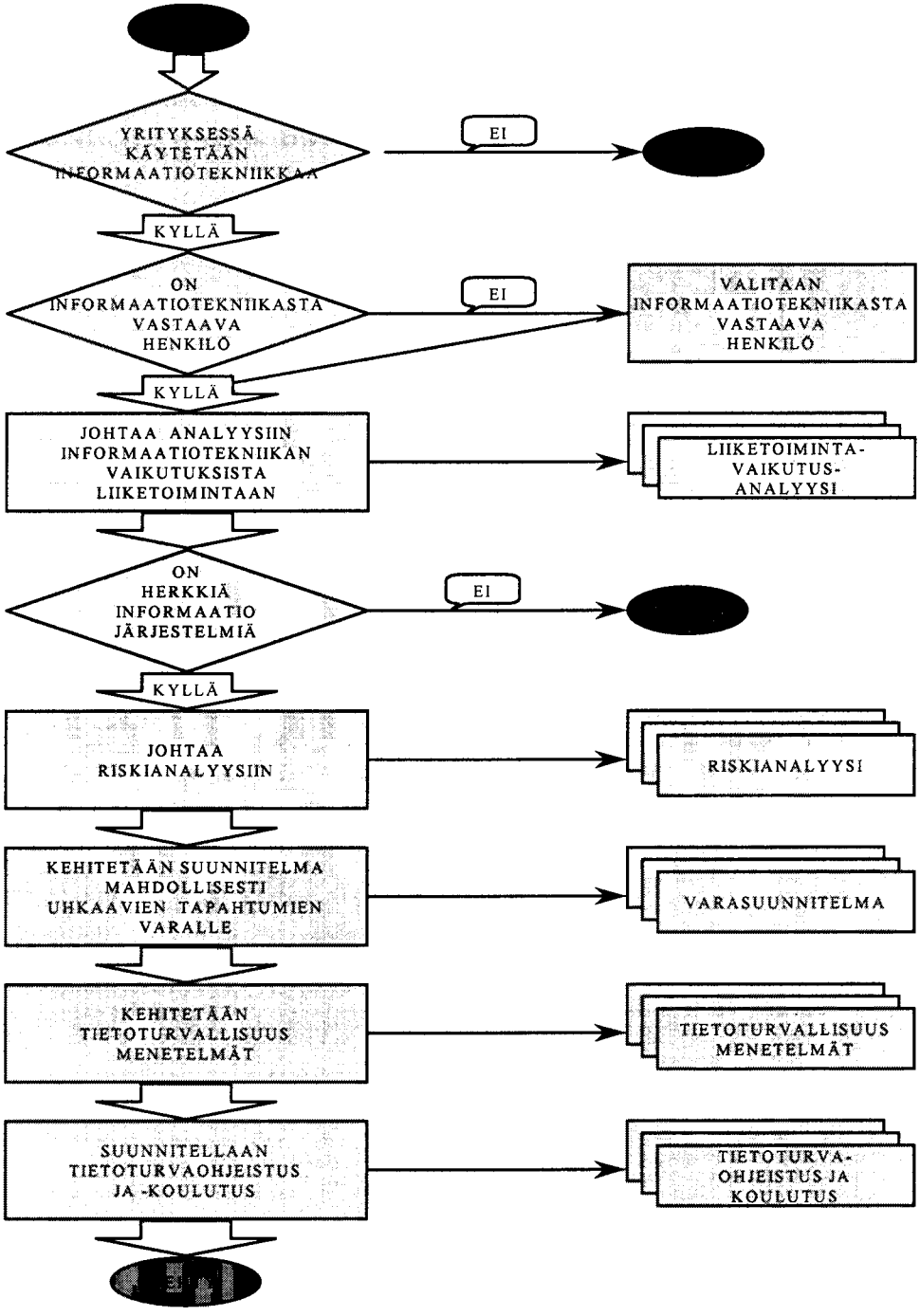
2.4 Tietoturvaohjeistuksen luominen yrityksessä

Viimekädessä yrityksen johto vastaa yrityksen tietoturvallisuudesta. Sen vuoksi yrityksen johdon on vähintäänkin luotava yritykseen *tietoturvallisuusohjelma* (ks. kuvio 6) ja asetettava vastuuhenkilö(t) sille. Tietoturvallisuusohjelmassa yritykseen muodostetaan tietoturvallisuusnormit ja -ohjeisto sekä suunnitellaan niitä vastaava koulutus.

Tietoturvan suunnittelussa työ ei voi alkaa ellei yrityksestä löydy asiantuntemusta ko. alalta. Ulkopuolisen avun käyttäminenkään ei välttämättä tuo ratkaisua, sillä yrityksen tulee voida hallita myös jatkossa tietojenkäsittelyään. Sen vuoksi ensimmäinen toimi tietoturvasuunnitelmaa tehtäessä on tietoturvasta vastaavan henkilön palkkaaminen tai koulutuksen hankkiminen jo yrityksessä toimivalle henkilölle. Vaihtoehtoisena toimenpiteenä on tietenkin tietojenkäsittelyn ulkoistaminen.

Yrityksen tietoturvasuunnitelma voidaan tehdä esimerkiksi seuraavalla tavalla: Tietoturvasta vastaava henkilö luo yrityksestä kuvan, jossa kartoitetaan yrityksen tietotekniikasta riippuvaiset toiminnot sekä määritellään niiden haavoittuvuus ja suhde liiketoimintaan. Tämän jälkeen suoritetaan riskianalyysi, jossa lasketaan tietosuojan kustanne suhteessa liiketoiminnan mahdollisiin menetyk-

siin. Seuraavaksi tehdään suunnitelmat mahdollisesti uhkaavien, äkkinäisten tilanteiden hallitsemiseksi. Kun yrityksen suhde tietoturvaan on selvitetty ja riskit sekä yrityksen voimavarat tiedetään, voidaan yrityksessä sopia tietoturvallisuusmenetelmistä. Lopuksi tietoturva on ohjeistettava ja huolehdittava henkilökunnan koulutuksesta. (ks. kuvio 6).



Kuvio 6: Tietoturvallisuusohjelma vaiheittain (Lähde: Commonwealth of Virginia, Council on Information Management.1995.)

Kun organisaation tietoturvaohjeistuksia muodostetaan tulee huomioida ainakin se kenellä on oikeus käyttää atk-resursseja sekä millainen on atk-resurssien oikea käyttötapa. Lisäksi tietoturvaohjeistuksia muodostettaessa on huomioitava vaatimukset tietojärjestelmän ylläpitohenkilöstölle sekä mitä oikeuksia ja vastuita tietojärjestelmän käyttö- ja ylläpitohenkilökunnalla on ja kuinka arkaluonteista tietoa tulee käsitellä. (Holbrook & Reynolds 1991)

2.5 Tietoturvaohjeiden käyttäminen yrityksessä

Kun organisaatio on muodostanut ohjeistukset tietojärjestelmän loppukäyttäjiä varten, niin tietojärjestelmän vastuuhenkilöiden tulee valvoa tietojärjestelmän loppukäyttäjien toimintaa. Jos tietojärjestelmän loppukäyttäjät työskentelevät organisaation omissa tiloissa, on heidän luotettava valvonta suhteellisen helppoa. Organisaation omien tilojen ulkopuolella tapahtuvan tietojärjestelmän käyttötoiminnan valvonta on monimutkaisempaa, mutta välttämätöntä. Ihmisten kunnollinen kouluttaminen on yksi tärkeä tietoturvamenetelmä (Holbrook & Reynolds 1991).

2.6 Tietoturvapolitiikka

Tietoturvapolitiikka on organisaation johdon hyväksymä ja vahvistama perusperiaate, joka määrittelee tietoturvan toteutuksen ja painotukset. Sen perusteella ryhdytään toteuttamaan tietoturvan toimintoja, rutiineja ja ohjeita. Organisaation johdon ja henkilöstön tulee sitoutua määriteltyyn politiikkaan. Jotta tietoturvapolitiikan noudattamista voidaan vaatia henkilöstöltä, on se julkistettava ja tuotava esiin sen tärkeys yrityksen toiminnalle ja sen jatkuvuudelle.

Tietoturvapolitiikalla tarkoitetaan myös organisaation valitsemaa tietoturvaperiaatteiden soveltamistapaa. Politiikkaa tarkastettaessa tulisi ottaa huomioon esim. seuraavia asioita:

- onko yrityksessä määritetty tietoturvapolitiikka tai tietoturvaperiaatteet, joiden mukaan toimitaan
- onko tietoturvapolitiikka ajan tasalla
- onko tietoturvapolitiikka ylimmän johdon vahvistama
- onko tietoturvapolitiikasta ja sen muutoksista tiedotettu ja onko se riittävän hyvin tunnettu
- vastaako käytännön toiminta politiikkaa
- miten politiikan toteutusta valvotaan
- onko muita erityiskysymyksiä käsitteleviä tietoturvapolitiikkoja
- arvioidaan niiden ominaisuudet vastaavasti

Jatkuvalla koulutuksella henkilöstö saadaan sisäistämään ja sitoutumaan yrityksen tietoturvapolitiikkaan. Koulutuksen toteutus voi vaihdella, mutta olennaista on koulutuksen tärkeyden ymmärtäminen ja että se on jatkuvaa. Koko henkilökunnalle annetaan peruskoulutus tietoturvasta, joka voidaan liittää muun koulutuksen osaksi. Eri kohderyhmille annetaan lisäksi suunnattua jatkokoulutusta ryhmän tarpeiden ja vaatimusten mukaisesti. (Yrityksen Tietoturva 1991)

Tietoturvallisuuden oikea hoitaminen muodostaa merkittävän tekijän hyvään tulokseen pyrittäessä. Mikäli tulosvastuulliset yksiköt joutuvat kilpailemaan asiakkaista keskenään tai kaupallisten yritysten kanssa, saattaa tietoturvallisuudesta tulla merkittävä kilpailutekijä. Toimittaja, joka asettaa turvallisuustason liian korkealle on kilpailukyvytön muihin nähden. Liian matala turvallisuustaso aiheuttaa lisäkuluja toiminnassa tai asiakkaiden luottamuksen menettämisen. (Holbrook & Reynolds 1991) Tarjottaessa palveluita muille yrityksille on peruslähtökohtana se, että ostaja määrää haluamansa turvallisuustason. Vaikka myyjä voikin tarjota myös jotain muuta pyydetyn lisäksi, on lähtökohtana neu-

votteluille aina pyydetty turvallisuus. Tällaisissa tapauksissa ostajan tehtävä on määrätä turvallisuustaso ja palvelun toteuttajan on arvioitava, millä hinnalla se kykenee vaaditun tason täyttämään. Myyjä voi tietysti katsoa myös, että sillä ei ole edellytyksiä tarjota vaadittua tasoa kilpailukykyisesti.

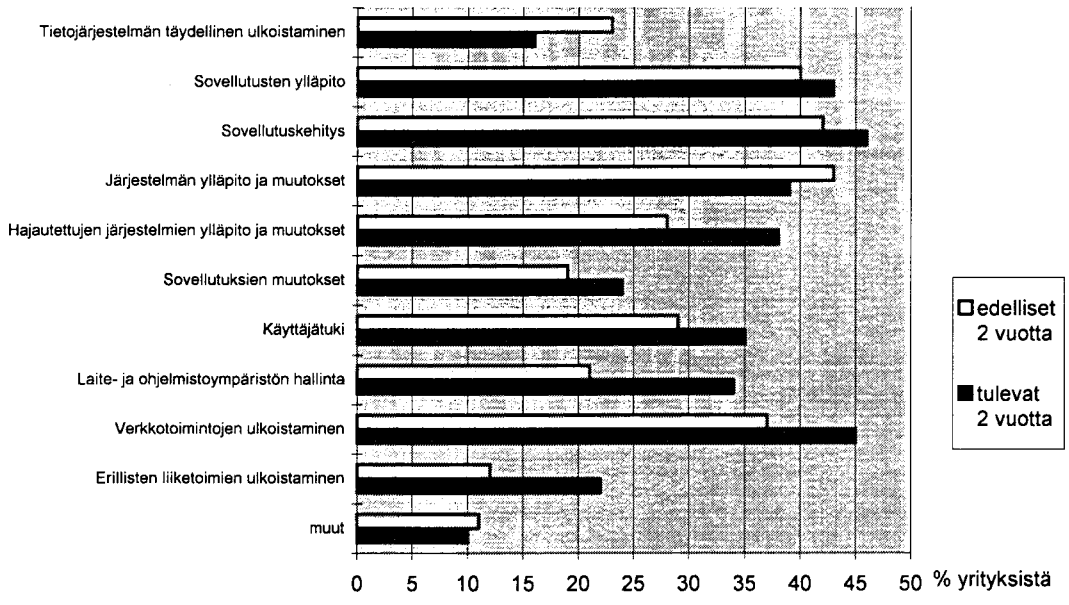
Palveluita tuottavan yksikön kannattaa jo aikaisessa vaiheessa miettiä omaa toimintastrategiaansa turvallisuuskysymyksissä. On asiakkaita, jotka vaativat korkeaa turvallisuustasoa, ja sellaisia, joille turvallisuudella ei ole erityistä merkitystä. Näiden kahden ryhmän yhdistäminen samaan palvelutaloon ei välttämättä onnistu, koska monet järjestelyt on tehtävä vaativimman ryhmän mukaan ja silloin palveluiden hinta saattaa nousta korkeammaksi kuin mitä alhaiseen tasoon tyytyvä on valmis maksamaan.

Imagokysymykset saattavat myös olla merkittävä tekijä palveluiden tuottajaa valittaessa. Yksikön, joka profiloituu turvallisten palveluiden tuottajaksi, ei välttämättä kannata ottaa asiakkaakseen sellaista tahoa, joka itse ei välitä turvallisuuskysymyksistä, koska tällöin palvelun tuottaja saa helposti ulkopuolisten silmissä syyn asiakkaan piittaamattomuudesta.

3 ULKOISTAMINEN

Tässä luvussa määritellään tietojenkäsittelyn ulkoistaminen. Aihetta käsitellään laajasti varsin uutena tietojenkäsittelyn hallintamuotona. Tietojenkäsittelyn ulkoistamisen suhdetta tietoturvaan kartoitetaan perusteellisesti tutkielman aiheen mukaisesti.

Vielä vuonna 1994 Voltin (1994) mukaan, tietojärjestelmien ulkoistaminen suoritettiin yleensä koko tietojärjestelmän ulkoistamisena. Nyttemmin suuntaus on tietohallinnon erillisten osien tarveharkintaisessa ulkoistamisessa (ks. kuvio 7). Tietojärjestelmän ulkoistamisella tavoitellaan edelleenkin taloudellisia etuja mutta yhä enenevässä määrin haetaan puuttuvaa tietotaitoa organisaation käyttöön (vrt. Lacity & Hirschheim 1993).



Kuvio 7: Eurooppalaisten yritysten ulkoistamispalveluiden kysynnän muutos 1997. (lähde: IDC 1997)

3.1 Tietojenkäsittelyn ulkoistamisen määritys

Tietojenkäsittelyn ulkoistamisella tarkoitetaan organisaation sisäisen tietojenkäsittely-yksikön tehtävien osittaista tai täydellistä siirtoa ulkopuolisen yrityksen hoidettavaksi (Lacity & Hirschheim 1993). Ulkoistaminen ei ole alihankintaa, vaikka selviä yhteneväisyyksiä onkin havaittavissa. Tietojenkäsittelyn ulkoistamisessa siirretään organisaation sisäistä tietojenkäsittelyä ulkopuolisen organisaation hoitoon. Alihankinnassa hankittujen palvelujen saavuttamiseksi käytetään hyväksi ulkopuolisen tarjoamia resursseja, esimerkiksi tietokonelaitteistoja ja atk-henkilöstöä. Alihankinnassa organisaation sisäisiä tietojenkäsittelyresursseja ei käytetä tai siirretä organisaation ulkopuolelle. Oltmanin (1990) mukaan ulkoistamisella tarkoitetaan tietojenkäsittelytoiminnan vastuun osittaista tai totaalista siirtoa yrityksen ulkopuolelle.

Ulkoistamisessa toimittajalla on *päävastuu palvelujen tuottamisesta*, kun taas alihankinnassa palvelujen tarjoajan vastuulla on hankkia määritellyt palvelut yrityksen ulkopuolelta (Voltti 1994). Ulkoistamisen merkitys on myöhemmin laajentunut koskemaan myös tietojärjestelmän komponenttien ulkoistamista (sovellusten ulkoistaminen, outsourcing applications). *Alihankinta* on sopimukseen perustuvaa asiakasyrityksen ja alihankkijan välistä *tuotannollista yhteistyötä*, jossa alihankkija tekee päähankkijan tuotteeseen osia tai työvaiheita asiakkaan määrittelemien tuotevaatimusten mukaan (Tanskanen 1987).

Sääksjärven (1991) mukaan tietojärjestelmän lyhytaikainen ulkoistaminen voidaan kuitenkin määritellä alihankinnaksi, koska siinä ulkoistamisen toimintojen päävastuu kuuluu asiakkaalle. Tietojärjestelmän lyhytaikainen ulkoistaminen sisältää osittain erikois- ja kapasiteettialihankinnan käsitteitä (Voltti 1994), mutta Lacity & Hirschheim (1993) ovat laajentaneet ulkoistamisen käsitteen koskemaan myös alihankinnan omaista toimintaa. Lacityn & Hirschheimin (1993) mukaista ulkoistamisen määritelmää noudatetaan tässä tutkielmassa.

Tietojärjestelmän ulkoistaminen voidaan määrittää organisaation sisäisten atk-toimintojen siirtämisenä organisaation ulkopuolelle. Tähän määrittelyyn voidaan lisätä Oltmanin (1990) vastuuasiat atk-järjestelmän toiminnoista. Ulkoistamisen määrittely on laajentunut myöhemmin koskemaan myös tietojärjestelmän komponenttien (laitteiden ja ohjelmien) ulkoistamista. Tietojärjestelmän ulkoistaminen käsittää siten ulkoistettuun tietojärjestelmään liittyvät tiedot, toiminnot, laitteistot, ohjelmat sekä vastuuasiat tietojärjestelmän toiminnoista. Tulee myös huomata, että tietojärjestelmän ulkoistamisessa siirretään tietojärjestelmän ulkoistajaorganisaation ulkopuolelle mahdollisesti ulkoistettavaan tietojärjestelmän osaan liittyvä tietotaito. Esimerkiksi tietojärjestelmän ulkoistamisessa siirretään yleensä tietojärjestelmän hoitohenkilöstö organisaation ulkopuolelle ja siten hoitohenkilöstön mukana tietotaito tietojärjestelmän ylläpidosta.

Tietoturvan kannalta tietojärjestelmän ulkoistaminen käsittää siten ainakin atk toimintojen, henkilöstön sekä atk-laitteistojen turvaamisen. Nykyisin organisaatiot ulkoistavat yleensä koko tietojärjestelmänsä ja tällöin on huolehdittava koko tietojärjestelmän tietoturvasta. Organisaation kaikkien toimintojen turvaamisen kannalta organisaation käytössä tulee olla sopivia tietoturvaohjeistuksia(ks. 2.2.). Tietojärjestelmän ulkoistamisessa organisaation toiminnan jatkumisen kannalta on tärkeää, että organisaation sisällä säilyvät atk-järjestelmän strategiset toiminnot, esimerkiksi atk-toimintojen johtaminen ja suunnittelu (Keen & Cummings 1994). Organisaation strategisiin toimintoihin kuuluvat myös tietoturvaan liittyvä suunnittelu, kehitys ja ylläpitotyö. Käytännössä organisaatiot toteuttavat liiketoimintastrategioidensa mukaista tietoturvan hallintaa tietoturvapoliitikoiden ja tietoturvaohjeistuksien avulla.

Tietojärjestelmän *lyhytaikainen ulkoistaminen* (Body Shop) on kestoajaltaan lyhyt, esimerkiksi vain muutama kuukausi. Tällöin organisaation käyttöön hanki-

taan ulkopuolista apua selvästi määritellyn tehtävän toteuttamiseksi. Tehtävän suorittaminen johdetaan ulkoistajaorganisaatiosta käsin. Projekteja ulkoistaessa (Project Management) organisaatio voi ulkoistaa kokonaisia tai osaprojekteja. Kokonaan ulkoistetut projektit toimitetaan yleensä "avaimet käteen" -periaatteella. Ulkoistettuja projekteja voivat olla esimerkiksi määrittely, suunnittelu ja toteutusprojektit. Palvelujen toimittaja yleensä vastaa projektin johtamisesta.

Täydellisessä ulkoistamisessa (Total Outsourcing) palvelujen toimittajalla on kokonaisvastuu joistakin tietojärjestelmän toiminnoista tai koko tietojärjestelmän toiminnasta. Palveluilla tarkoitetaan tässä yhteydessä tietojärjestelmän toimintoihin liittyviä asioita sekä toimittajalla tarkoitetaan organisaation ulkopuolista tahoa. (Lacity & Hirschheim 1993)

Organisaatio voi aluksi ulkoistaa vain atk-tehtäviään ja ulkoistamisen tämä vaihe kestää yleensä lyhyen ajanjakson. Seuraavassa vaiheessa organisaatio voi ulkoistaa projekteja, mikäli kokemukset ulkoistajan tarjoamista palveluista ovat olleet myönteisiä. Ulkoistettuihin projekteihin organisaatio voi käyttää omaa ja/tai tietojärjestelmän ulkoisen hoitajan tarjoamaa henkilökuntaa. Lopuksi organisaatio voi ulkoistaa koko tietojärjestelmänsä havaittuaan tämän mahdolliseksi.

Ulkoistamissuhteen kesto täydellisessä ulkoistamisessa voi olla kolmesta viiteen vuoteen. Pelkkä atk-tehtävien tai projektien ulkoistaminen voi kestää myös useita vuosia. Toiminta, jossa käytetään hyväksi tietojärjestelmän ulkoisen hoitajan tietojärjestelmää eikä organisaation omia resursseja siirretä organisaation ulkopuolelle, on edellä esitetyn määritelmän mukaan alihankintaa.

Ei ulkoistetun tietojärjestelmän ylläpito ja käyttötoiminta tapahtuu yleensä organisaation sisällä. Tietoturvauhkat ja -riskit kohdistuvat sisäiseen tietojärjes-

telmään liittyviin tietoihin. Ulkoistetun tietojärjestelmän ylläpitotoiminta sijoittuu yleensä yrityksen omien tilojen ulkopuolelle. Tietoturvauhkat ja -riskit liittyvät lisäksi tietojärjestelmän ulkoisen hoitajan suorittamiin toimintoihin, tietojärjestelmän ulkoisen hoitajan laitteisiin sekä tietojärjestelmän ulkoistamisen osapuolten välillä siirrettyihin tietoihin. Tietojärjestelmän ulkoistamiseen liittyvät toiminnot, laitteet ja vastuut määritetään tietojärjestelmän ulkoistamissopimuksessa.

Ulkoistetun tietojärjestelmän tietoturvan hallintaan kaikissa ulkoistamisen eri muodoissa voidaan käyttää tietoturvamenetelmiä, tietojärjestelmän ulkoistamissopimuksessa asetettuja tietoturvavaatimuksia, vastuuasioiden ja henkilöiden tehtävämäärityksiä sekä erityisiä tietoturvaohjeistuksia. Tietoturvan hallinnan kannalta on tärkeää, että tietoturva-asioista sovitaan sitä tarkemmin mitä suurempi osa tietojärjestelmää ulkoistetaan. Esimerkiksi ulkoistaessa koko tietojärjestelmä tietoturvavaatimukset ulkoistettua tietojärjestelmään kohtaan ovat hyvin yksityiskohtaiset.

3.2 Tietojärjestelmän ulkoistamisen etuja ja haittoja

Kansainvälisen kilpailun kiristyminen, rahamarkkinoiden vapautuminen, tietojenkäsittelypalvelujen myynnin kasvaminen ja tietotekniikan asiantuntijoiden puute puoltavat tietojärjestelmän ulkoistamista (Ketler & Walström 1993). Uma G. Gupta ja Ashok Gupta (1992) luokittelevat ulkoistamissyyt seuraaviin neljään luokkaan:

1. Strateginen keskittyminen.
2. Taloudelliset säästöt.
3. Markkinavoimien painostus
4. Tekniikkaan liittyvät näkökohdat

Huomattavaa on, ettei tuolloin vielä osattu ajatella henkilöresurssien vajeesta johtuvaa tietotekniikan ulkoistamistarvetta. Nykyisin tietojärjestelmän ulkoistaminen on merkittävä tapa saada organisaation käyttöön erikoistietämystä, koska teknisen kehityksen nopeus ja ammattitaidon vaatimukset ovat kasvaneet niin, että on yksinkertaisempaa ja halvempaa hankkia puuttuva tietotaito organisaation ulkopuolelta (ks. kuvio 8).

Tietojärjestelmän ulkoistamista ei tehdä nykyisin pelkästään, jotta alennettaisiin liiketoiminnan kustannuksia, vaan myös strategisena toimenpiteenä tuottamaan lisäarvoa organisaation liiketoiminnalle. Tietojärjestelmän ulkoistaminen on yksi tapa välttää tai siirtää taloudellisia investointeja. Tästä syystä organisaatio voi saada tarvittavan lisäajan ratkaisevien liiketoiminnallisten päätösten tekemiseksi (Douglas 1993).

Kuvio 8: Henkilöresurssien vaje tietojenkäsittelyssä aiheuttaa yrityksille tarvetta hakea tietotaitoa yhä enenevissä määrin ulkoistamispalvelujen kautta seuraavan kahden vuoden kuluessa. (lähde: IDC 1997)

Tietojärjestelmän ulkoistamisen aloittamisen suurin syy on yleensä kuitenkin kustannussäästöjen hankinta. Ammattitaidon ja tietojen saanti organisaation käyttöön on myös yhä merkittävämpi syy aloittaa tietojärjestelmän ulkoistaminen (ks. kuvio 8). Ongelmia tulee, jos organisaation omien resurssien kehittämisestä ei ole huolehdittu tietojärjestelmän ulkoistamissuhteen loppuessa, esi-

merkiksi tietojärjestelmän ylläpitoon liittyvistä asioista. Organisaation tulee huolehtia myös oman atk-henkilökunnan jatkuvasta koulutuksesta. Tietojärjestelmän ylläpidon kannalta merkittävä etu tietojärjestelmän ulkoistamisessa on toimintojen tehostuminen sekä organisaation kyky keskittyä olennaisiin liiketoimintoihin. Tietojärjestelmän ylläpidon kannalta merkittävä haittatekijä on tietojärjestelmän suoran ohjauksen menetys sekä mahdolliset ristiriidat tavoitteiden asettelussa tietojärjestelmän toimintojen ohjaukseen liittyvistä asioista. Sääksjärvi (1991) on tutkinut tietojärjestelmän ulkoistamisen taloudellisia vaikutuksia organisaation toimintoihin. Tietojärjestelmän ulkoistamisessa etuna on tietojärjestelmän käyttötoiminnan tehostuminen ja atk-toimintojen kustannusten alentuminen. Organisaation taloudellinen joustavuus myös kasvaa, koska kiinteät kustannukset vähenevät ja pääomaa voidaan keskittää organisaation kilpailukyvyn kannalta tärkeisiin liiketoimintoihin. Organisaatio saa käyttöönsä myös tarvitsemaansa erikoisasiantuntemusta ja tietojenkäsittelyhenkilökunta voi keskittyä organisaation toimintojen kannalta strategisesti tärkeisiin atk-toimintoihin. Yrityksen taloudelliset ongelmat yleensä vähenevät, mutta ongelmia voi esiintyä myöhemmin, mikäli tietojärjestelmän ulkoistamista ei ole suunniteltu huolella. Tietojärjestelmän ulkoistamisen onnistumisesta riippuu, miten ulkoistamisella haetut taloudelliset edut saavutetaan.

Tietojärjestelmän ulkoistamisessa etuna on tietojärjestelmän ylläpitoasioihin liittyvien ongelmien vähentyminen, koska puuttuvaa tietotaitoa voidaan hankkia organisaation ulkopuolelta. Haittatekijänä tietojärjestelmän ulkoistamisessa on tietojenkäsittelypalvelujen laadun, vahingoista toipumisen ja tietojärjestelmän tietoturvan suoran ylläpitotoiminnan ohjauksen menetys. Tietojärjestelmässä käsiteltäviin tietoihin liittyvät ominaispiirteet vaikuttavat tietojärjestelmän ulkoistamisen suoritustapaan ja asetettaviin tietoturvavaatimuksiin. Etuna tietojärjestelmän ulkoistamisessa on organisaation mahdollisuus siirtää ei-strategiset liiketoiminnot organisaation ulkopuolelle ja siten organisaatiolla on mahdollisuus keskittyä vain strategisesti tärkeisiin liiketoimintoihin. Haittatekijä tieto-

järjestelmän ulkoistamisessa on kuitenkin strategisten ja ei-strategisten liiketoimintojen määrittämisen vaikeus. (Ketler & Walström 1993)

Tietojärjestelmän ulkoistamisprosessiin vaikuttaa käytettävissä olevaan henkilökuntaan liittyvät asiat. Tietojärjestelmän ulkoistamisessa etuna on, että siirretyn henkilökunnan mukana saadaan tietoa ja asiantuntemusta tietojärjestelmän ylläpitoon liittyvistä asioista. Tietojärjestelmän ulkoistamisessa on mahdollista siirtää henkilökuntaa myös lyhytaikaisiin projekteihin.

Haittatekijänä tietojenkäsittelyn ulkoistamisessa on myös organisaation oman atk-asiantuntijahenkilökunnan katoaminen sekä tietojenkäsittelyhenkilökunnan erottamisesta johtuvat lisäkustannukset. Taloudelliset syyt vaikuttavat hyvin suuresti päätökseen ulkoistaa organisaation sisäinen tietojärjestelmä. Etuna tietojärjestelmän ulkoistamisessa on kustannusten alentuminen sekä organisaation rutiinitoimintaan sitoutuneen pääoman vapautuminen muuhun liiketoimintaan. Haittatekijänä ulkoistamisessa on odotettua suuremmat kustannukset tietojärjestelmän ulkoisen hoitajaorganisaation kykyjen yliarvioimisesta tai sopimusväärinkäsityksistä johtuen ja siksi liiketoiminnallinen voitto on pienempi. (Ketler & Walström 1993)

Yrityksen ominaispiirteet, esimerkiksi liiketoimiala, vaikuttavat erityisesti tietojärjestelmän ulkoistajan hallintaan ja valvontaan. Etuna tietojärjestelmän ulkoistamisessa on mahdollisuus poistaa yrityksen tietojärjestelmän ylläpitotoimintaan liittyvien tietojen puute. Tietojärjestelmän ulkoistaminen soveltuu erityisen hyvin palveluorganisaatioille, koska palveluorganisaatiot yleensä käyttävät tietojärjestelmiään lähinnä rutiininomaisten toimintojensa hoitamiseen. Haittatekijänä tietojärjestelmän ulkoistamisessa on liiketoimintojen suoran ohjauksen menettäminen byrokraattisissa ja johtajakeskeisissä organisaatioissa. Myöskään dynaamisille organisaatioille ei ole helppo määrittää sopivaa tietojärjestelmän ulkoistamistapaa. (Ketler & Walström 1993)

Tietojärjestelmän ulkoistamisesta aiheutuva joustavuuden kasvu asettaa suurempia vaatimuksia organisaation tietoturvatoiminnalle. Organisaatio voi keskittyä kehittämään oman liiketoimintansa kannalta tärkeitä alueita tai aloittaa kokonaan uusia liiketoimintoja, mutta haittatekijänä on tietojärjestelmän palvelujen laadun suoran ohjauksen menetys. Tietojärjestelmän ulkoistamisen purkaminen (insourcing) sekä oman liiketoimintastrategian ja strategisesti tärkeiden resurssien kehittäminen jatkossa voi olla vaikeaa. Ulkopuolisen palveluorganisaation henkilöstön taidot voidaan helposti yliarvioida ja tietojärjestelmän ulkoistajalla ja ulkoisella hoitajalla voi esiintyä ristiriitoja liiketoimintatavoitteiden asettamisessa. Organisaatio tarvitsee kuitenkin sisäistä tietotekniikan asiantuntemusta ulkopuolisen toimittajan valvontaan ja organisaation omien liiketoimintayksiköiden tarpeiden ymmärtämiseen (mm. Sääksjärvi 1991). Kuviossa 9 on tiivistetty ulkoistamisen etuja ja haittoja.

ETUJA

- Kustannussäästöt.
- Tietojärjestelmän ylläpito helpottuu.
- Tietohallinnon ammattitaidon ja tietojen saanti organisaation käyttöön.
- Liiketoiminnan lisäarvo strategisena toimenpiteenä.

ULKOISTAMINEN

HAITTATEKIJÖITÄ

- Suoran ohjauksen menetys tietojärjestelmään.
- Atk tietämyksen väheneminen yrityksen sisällä.
- Atk henkilökunnan menetys.
- Liiketoiminnallisten muutosten mahd. ristiriidat tietojärjestelmän ohjauksessa.
- Sopimuksen valvontavaikeudet ja sopimusväärinkäsitykset.

TIETOJÄRJESTELMÄN ULKOINEN HOITAJAORGANISAATIO

Kuvio 9: Tietojärjestelmän ulkoistamisen etuja ja haittoja

Tietoturvan kannalta ulkoistetun tietojärjestelmän käyttöhenkilöstön oikeudet ja vastuut tietojen sekä tietojärjestelmän käyttöön tulee määrittää huolellisesti. Tietojärjestelmän ulkoistamisen haittatekijät ovat tietoturvan kannalta myös ongelmallisia. Ulkoistamissopimusneuvotteluissa tulee tietojärjestelmän ulkoistamisen osapuolten pystyä sopimaan kaikki ongelmia aiheuttavat asiakohdat.

Tietojärjestelmän ulkoistamisen suunnitteluvaiheessa on punnittava tietojärjestelmän ulkoistamisen etu- ja haittatekijät tarkasti. Vaikka rahalliset säästöt olisivat huomattavia, kannattaa huomio kiinnittää aina hyväksyttävän tietoturvan saavuttamiseen.

Tietojärjestelmän ulkoistajaan ja ulkoistamissopimukseen liittyvät asiat, esimerkiksi aikaisemmin hankittu kokemus tietojärjestelmän ulkoistamisesta, vaikuttavat suuresti tietojärjestelmän ulkoistamisen onnistumiseen. Tietojärjestelmän ulkoiselle hoitajalle on eduksi aikaisemmin hankittu kokemus ja onnistuminen tietojärjestelmän ulkoistamisessa sekä kokemus pitkäaikaisesta suunnittelusta. Tietojärjestelmän ulkoiselle hoitajalle on eduksi myös, jos käytettävä teknologia on tehokasta ja nykyaikaista sekä teknologian kehittämistä varten on olemassa suunnitelmia ja tietojärjestelmän ulkoinen hoitaja on halukas neuvottelemaan hinnoista, palveluista ja omistusoikeuksista tietojärjestelmän toiminnoissa. Tietojärjestelmän ulkoistamissuhteen tulee perustua avoimuuteen. Tietojärjestelmän ulkoisen hoitajaorganisaation taloudellisen tilan tulee olla vakaa tietojärjestelmän ulkoistamisen aloitusvaiheessa niin, että tietojärjestelmän ulkoistamissuhteen aloitus ei perustu nopeaan pääoman tavoitteluun ja tietoturvan hyväksyttävä taso voi jäädä saavuttamatta. (Ketler & Walström 1993)

3.3 Tietoturvaohjeistukset ulkoistamisessa

Tietojärjestelmän ulkoistamisessa tarvitaan tietoturvaohjeistuksia, jotka ovat molempien tietojärjestelmän ulkoistamisen osapuolten hyväksyttävissä ja toteutettavissa. Tietojärjestelmän ulkoistamisen toteutustavasta riippuen organisaation sisällä voi olla aihetta muodostaa yksityiskohtaisempia ja tilannekohtaisempia tietoturvalinjauksia sekä -ohjeistuksia tietojärjestelmän loppukäyttäjiä varten.(ks. 2.3)

Tietoturvaohjeet ovat tietoturvayksikön/henkilön tiedossa ja organisaation muut yksiköt/henkilöt huolehtivat tietoturvan perustasosta itsenäisesti. Tietojärjestelmän ulkoiselle hoitajalle asettavat vastuut ja oikeudet on sovittava ulkoistamissopimusneuvotteluissa. Esimerkiksi se kuka voi hoitaa viestinnän organisaation ulkopuolelle ja millaista tietoa organisaatiosta voidaan julkaista (Holbrook & Reynolds 1991).

Tietoturvaohjeistuksia tarvitaan sekä tietojärjestelmän ulkoisen hoitajaorganisaation johtoa että tietojärjestelmän loppukäyttäjiä varten. Näkökulma tietoturvaan on hieman erilainen tietojärjestelmän ulkoisen hoitajaorganisaation johdolla ja tietojärjestelmän loppukäyttäjillä, mutta tehokas tietoturvan käytännön toteuttaminen vaatii tiivistä yhteistyötä eri sidosryhmiltä.

Organisaation tietojärjestelmän loppukäyttäjiä varten tulee muodostaa tietoturvaohjeistukset. Tietoturvan käytännön toteuttaminen jää lopulta tietojärjestelmän loppukäyttäjien vastuulle ja tietojärjestelmän loppukäyttäjät ovat loppujen lopulta suurin tietoturvaa uhkaava tekijä (Kajava & Leiwo 1995). Ilman kunnollisia ohjeistuksia tietojärjestelmän loppukäyttäjät ja ylläpitohenkilöstö muodostavat liian suuren uhkatekijän ulkoistetun tietojärjestelmän tietoturvalle. Tietoturvaohjeistuksien ja henkilöstön koulutuksen avulla voidaan varmistaa

tietojärjestelmän käyttöhenkilöstön ammatillista pätevyyttä, mikä lisää myös tietojärjestelmän ulkoisen hoitajan luotettavuutta.

Organisaatio tarvitsee erityisen tietoturvaohjeistuksen, mutta tämän lisäksi organisaatiossa tulee olla käytössä useita yksityiskohtaisia tietoturvapolitiikkoja eri ulkoistamistapauksia varten. Työntekijöiden työskentelyprosessia ei tule kuitenkaan sitoa liiaksi kaikenlaisiin ohjeisiin ja rajoituksiin (Kajava 1996).

Tietoturvaohjeistukset ja tietoturvapolitiikat muodostavat perustan organisaation tietoturvatoiminnalle. Tietoturvapolitiikan pohjalta muodostetaan tietojärjestelmän loppukäyttäjien ohjeistukset, joissa esitetään miten tietoturvavaatimukset käytännössä toteutetaan tietoturvamenetelmillä.

3.4 Tietoturvavaatimuksia tietojärjestelmän ulkoistamisessa

Kun tietojärjestelmien ulkoistamista harkitaan organisaation ylimmän johdon tulee määrittää se mitkä toiminnot säilytetään organisaation sisällä, mitä toimintoja ulkoistetaan tai mitä ohjeita tulee noudattaa kun muodostetaan tietojärjestelmän ulkoistamissopimusta tietojärjestelmän ulkoisen hoitajan kanssa (Alpar & Saharia 1995).

Tietojärjestelmän ulkoistajan tulee kartoittaa ulkoistettuun tietojärjestelmään kohdistuvat tietoturvauhkat ja -riskit ennen tietojärjestelmän ulkoistamisen aloittamista sekä tietoturvauhkien ja -riskien muuttumista tulee seurata säännöllisesti. Tietojärjestelmän ulkoisen hoitajan toiminnan valvontamenetelmät sekä korvaus ja korjausmenettelyt tulisi määrittää tarkasti tietojärjestelmän ulkoistamissopimuksessa.

Tietojärjestelmän ulkoistamisessa huomionarvoisia tietoturvamenetelmiä ovat tietojärjestelmän ulkoisen hoitajan valvontamenetelmät. Tietojärjestelmän ulkoisen hoitajan valvontaan voidaan käyttää yhteisiä tietoturvan katselmointitilaisuuksia, tarkastus käyntejä sekä tietojärjestelmän käyttölokitiedostojen tarkastamista.

Taloudelliset syyt sekä ulkoistajan ja sopimuksen erityispiirteisiin liittyvät tekijät jäävät tässä tutkimuksessa käytettävän tietoturvajaottelun (ks. 2.1.) ulkopuolelle. Tietojärjestelmän ulkoisen hoitajan taloudellista tilaa voidaan tarkkailla esimerkiksi säännöllisten raporttien avulla. Tietojärjestelmän ulkoistamissopimuksessa tulee määrittää menetelmät tietojärjestelmän ulkoisen hoitajan taloudellisen tilan raportoinnista ja tarkkailusta. Seuraavissa kappaleissa koskien tietoturvavaatimuksia, on käytetty Valtiovarainministeriön (1992) ja Liikenneministeriön Valmiusohjeen (1995) mukaista jaottelua.

Hallinnolliseen turvallisuuteen liittyen organisaatiolla tulee olla tietoturvasuunnitelma, atk-valmiussuunnitelma sekä toipumissuunnitelma, jotka ovat tietojärjestelmän ulkoistamisen osapuolten hyväksyttävissä. Organisaation ylin johto on aina kokonaisvastuussa tietoturvan toteuttamisessa ja tietoturvan toteuttamisesta tulee huolehtia nimetyn vastuuhenkilön. Tietoturvan ylläpito ja kehittäminen edellyttää säännöllisiä organisatoristen vastuiden ja tietojärjestelmän ulkoisen hoitajan toimintojen tarkastamista sekä tietojärjestelmän käyttöhenkilöstö tarvitsee säännöllistä koulutusta. Ulkoistamisen tietoturvapolitiikka tulee olla määriteltynä ennen tietojärjestelmän ulkoistamista ja mahdollisesti esiintyvät tietoturvauhat tulee selvittää esimerkiksi tietoturvan tarkistuslistojen ja/tai riskianalyysien avulla.

Henkilöstöturvallisuuteen liittyen organisaation tulee tarkastaa tietojärjestelmän hoito- ja käyttöhenkilöstön tausta-asiat ja sopivuus työtehtävien hoitamiseen viimeistään työhönottovaiheessa sekä ulkoistetun tietojärjestelmän käyttöhen-

kilöstö tulee motivoida ja kouluttaa noudattamaan tietoturvallisia tietojärjestelmän käyttötapoja..

Fyysiseen turvallisuuteen liittyen tietojärjestelmän ulkoisen hoitajan tulee sijoittaa atk-tilat mahdollisimman suojattuun ja huomiota herättämättömään ympäristöön. Kiinteistöjen sekä atk-laitteiden ja käyttötilojen turvaamisesta tulee tietojärjestelmän ulkoisen hoitajan huolehtia tilojen kunnollisella lukituksella sekä tehokkaalla kulunvalvonnalla. Tietojärjestelmän ulkoisen hoitajan tulee varautua palo-, vesi-, sähkö- ja ilmastointivahinkojen torjuntaan.

Tietoliikenneturvallisuuteen liittyen tietojärjestelmän ulkoisen hoitajan tulee huolehtia tiedonsiirtolaitteiden ja kytkentätilojen lukituksesta. Tietojärjestelmän ulkoisen hoitajan tulee huolehtia tietoliikenteen ja elektroniikan turvallisuudesta eristämällä organisaation sisäiset tietoverkot yleisistä tietoverkoista palomuurilla.

Laitteistoturvallisuuteen liittyen tietojärjestelmän ulkoisen hoitajan ja ulkoistajan tulee kahdentaa koko atk-laitteisto tai ainakin atk-laitteiston tärkeimmät osat mahdollisuuksien mukaan. Tietojärjestelmän ulkoistamisen osapuolten tulee hankkia vikasietoisia ja yhteensopivia laitteita ja estää ihmistä johtuvat vahingot, tietojärjestelmän laitteistokapasiteetti tulee mitoittaa käyttötarpeen mukaan.

Ohjelmistoturvallisuuteen liittyen tietojärjestelmän ulkoisen hoitajan tulee huolehtia tietojärjestelmän käyttöhenkilöstön luotettavasta tunnistuksesta, tietojärjestelmän pääsynvalvonnasta ja käyttöoikeuksien määrittelyistä sekä tietojärjestelmän ulkoisen hoitajan tulee kirjata kaikki tietojärjestelmän käyttötapahtumat ja käyttäjät lokitiedostoon. Tietojärjestelmän ulkoistajan ja ulkoisen hoitajan tulee hankkia ohjelmistot vain luotettavilta toimittajilta, virustentorjuntaohjeita tulee noudattaa sekä virustentorjuntaohjelmia tulee käyttää säännöllisesti. Räätälöityjen ohjelmistojen omistusoikeuksien tulee siirtyä ostajalle

ja ohjelmistojen tulee olla hyvin dokumentoituja, ohjelmistojen toimittajan tulee huolehtia ohjelmistojen ylläpidosta ja siitä tulee tehdä kirjallinen sopimus.

Tietojärjestelmän ulkoistajan ja tietojärjestelmän ulkoisen hoitajan tulee kartoittaa *tietoaineisto* sekä luokitella tietoaineiston turvaamisen tarve. Tietojärjestelmän ulkoisen hoitajan ja ulkoistajan tulee huolehtia sähköisessä, optisessa tai muussa muodossa olevan tiedon käyttämisestä, säilyttämisestä, kuljetuksesta, kopioinnista, jakelusta, varmuuskopioinnista, hävittämisestä sekä käyttämisestä katastrofitilanteessa. Käytettävät ohjelmistot tulee aina rekisteröidä ja tietojärjestelmän ulkoisen hoitajan tulee säilyttää tietoaineiston varmuuskopiot murto-, palo-, sähkö- ja vesivahinkojen varalta suojatuissa tiloissa esimerkiksi paloturvallisessa kassakaapissa.

Tietojärjestelmän *käyttöturvallisuuteen* liittyen tietojärjestelmän ulkoistajan ja ulkoisen hoitajan tulee kohdentaa tarkasti henkilöiden työtehtävät, oikeudet ja vastuut. Tietojärjestelmän käyttäjät ja tapahtumat tulee kirjata lokitiedostoon ja tietojärjestelmän ulkoistajan tulee estää vaarallisten työtehtäväyhdistelmien muodostuminen työtehtäviä eriyttämällä.

Tietojärjestelmän ulkoisen hoitajan vaatimukset voivat tuntua kohtuuttoman kovilta. Kun ulkoistamisessa kyseessä on kuitenkin usein yrityksen kriittisen tiedon jakaminen ulkopuolisten kanssa ja yrityksen koko toiminnallinen tietotaito saattaa olla ulkopuolisten hallussa, on luontevaa, että ulkoistamisprosessi ja -sopimus tehdään niin aukottomaksi kuin pystytään.

3.5 tietoturvapolitiikka ulkoistamisessa

Tietoturvapolitiikka perustuu organisaation johdon tai turvallisuusyksikön päätöksiin tietoturvan suuntaviivoista ja vaatimuksista(ks. 2.5). Ulkoistamisen tie-

toturvapolitiikka voidaan määritellä myös ennen tietojärjestelmän ulkoistamista. Lähtökohta tietoturvallisuuden suunnittelussa on organisaation tietoturvapolitiikka, joka määrittelee vastuut tietojen suojaamisesta riippumatta siitä, miten informaatio on esitetty tai välitetty (Rautiainen 1989). Jos yrityksessä on useita tasoja, organisaation alayksiköiden esimiesten on oltava vastuussa toimintojensa tietoturvasta ja yksityiskohtaiset tietoturvapolitiikat ovat pohjana tietojärjestelmän loppukäyttäjien ohjeistuksille.

Tietojärjestelmän ulkoistamisen tietoturvapolitiikka on organisaation tietoturvatoiminnan perusta. Tietoturvaohjeistukset muodostetaan ennen tietojärjestelmän ulkoistamista tai tietojärjestelmän ulkoistamisen valmisteluvaiheen aikana, joka voi kestää 1-3 vuotta. Ulkoistamisen tietoturvapolitiikan ja tietojärjestelmän loppukäyttäjien ohjeistuksien merkitys korostuu erityisesti tietojärjestelmän ulkoistamisen aikana ja tietojärjestelmän ulkoistamisen lopettamisvaiheessa. Tietojärjestelmän ulkoistamisen tietoturvaohjeistuksien merkitys korostuu tietojärjestelmän ulkoistamisen suunnittelu ja valmisteluvaiheessa.

Tietoturvaohjeistuksen laatiminen voi olla esimerkiksi seuraavan kaltainen. Aluksi selvitetään kyselyiden avulla tietojärjestelmän ulkoistamisessa esiintyviä tietoturvaongelmia. Kyselyt analysoidaan ja haastatteluiden avulla selvitetään perusteellisemmin merkittävimpiä tietoturvaongelmia. Seuraavaksi muodostetaan alustava tietoturvaohjeistus ulkoistamista varten. Tietoturvaohjeistus testataan pilotti - projektissa ja kokemukset tietoturvaohjeistuksesta kerätään. Kokemukset tietoturvaohjeistuksesta analysoidaan ja tämän pohjalta tietoturvaohjeistusta kehitetään. (Holbrook & Reynolds 1991)

Tietojärjestelmän ulkoistamissopimusneuvotteluissa muodostetaan pohja organisaation tietojärjestelmän ulkoistamiselle. Sopimusneuvotteluissa tulee käsitellä ainakin tietoturvan perusvaatimukset. Ulkoistamisen tietoturvapolitiikassa tulee esittää tietoturvajohdon riskien kartoitus, tietojen turvaamisen tärkeysjär-

jestys sekä tietoturvan ja riskien katselmointi, organisaatiossa käytettävät tietoturvaohjeistukset, perusvaatimukset ja toimintatavat.

Tietoturvapolitiikan tulee määrittää käytettävät tietoturvamenetelmät, tietoturvamenetelmien tehokkuuden määrittäminen, tietoturvamenetelmien käytön valvonta ja tehokkuuden tarkastus sekä tapahtuneista vahingoista toipuminen. Tietojärjestelmän loppukäyttäjien valvontamenetelmät ovat tietojärjestelmän ulkoistamisessa tietoturvapolitiikan erityisen huomion kohteena. Organisaation tietoturvakoulutuksen ja tietoturvatietämyksen ylläpito sekä tietoturvapolitiikan uudelleen katselmointiin johtavat tekijät tulee esittää myös tietoturvapolitiikassa. Tietoturvapolitiikan tehokkuuden kannalta tietoturvapolitiikan tulee esittää tietoturvapolitiikkaan tehtävät muutokset, muutosten tekemisen suoritus sekä muutosten tekemisen hallinta. (International Organization for Standardization 1994)

Tietoturvan perustan on aina lähdettävä organisaation johtotasolta, joka hyväksyy käytettävän tietoturvapolitiikan (Saari 1988). Tietojärjestelmän ulkoisella hoitajalla voi olla määriteltynä myös oma tietoturvapolitiikka, joka on tietojärjestelmän ulkoistajaorganisaation katselmoitavissa ja hyväksyttävissä. Tietojärjestelmän ulkoisen hoitajan ohjaaminen on mahdotonta ilman selkeitä tietoturvavaatimuksia. Organisaation tietoturvapolitiikan tulee määrittää tietojärjestelmän ulkoisen hoitajan tietoturvaraporttien muoto, sisältö, raportointitapaukset sekä hyväksyttävät raportointitavat. Tietoturvaraporttien oikeellisuus tulee varmistaa tietojärjestelmän ulkoisen hoitajan toiminnan valvonnalla ja siksi organisaation tietoturvapolitiikan tulee määrittää myös tietojärjestelmän ulkoisen hoitajan toiminnan valvontamenetelmät.

3.6 Yhteenveto

Tietoturva voidaan jakaa erityisiin osa-alueisiin. Näitä osa-alueita ovat hallinnollinen-, henkilöstö-, fyysinen-, tietoliikenne-, käyttö-, ohjelmisto- , tietoaineisto- sekä laitteistoturvallisuus. Yrityksen turvallisuuden perustana ovat tietoturvapolitiikat ja tietoturvaohjeistukset myös ulkoistettaessa tietojenkäsittely.

Hallinnollinen tietoturva on esillä tietojärjestelmän ulkoistamisen suunnittelussa ja tietojärjestelmän ulkoistamisen aikana. Hallinnollinen tietoturva on pohjana organisaatiossa käytettäville tietoturvaohjeistuksille sekä on koko tietoturvatoiminnan perusta. Esimerkiksi tietojärjestelmän ulkoistamissopimus ja tietoturvapolitiikat kuuluvat hallinnolliseen turvallisuuteen. Henkilöstö-, käyttö- ja tietoliikenneturvallisuus ovat yhtä tärkeitä tietojärjestelmän ulkoiselle hoitajalle ja tietojärjestelmän ulkoistajalle, koska esitettyihin tietoturvan osa-alueisiin ulkoistamisen molemmat osapuolet voivat vaikuttaa omilla toimillaan jatkuvasti. Esimerkiksi henkilöstöturvallisuuteen voi vaikuttaa sopivien henkilöiden valinnalla ja etenkin henkilöiden riittävällä koulutuksella.

Jos tietojärjestelmä sijaitsee ulkoistajaorganisaation ulkopuolella, niin fyysiseen turvallisuuteen tietojärjestelmän ulkoistaja voi vaikuttaa vain tietojärjestelmän ulkoisen hoitajan kautta ja tietojärjestelmän ulkoisen hoitajan toiminnat vaikuttavat suoranaisesti fyysiseen turvallisuuteen. Ainakin fyysistä-, ohjelmisto-, henkilöstö-, käyttö-, tietoliikenne- ja laitteistoturvallisuutta varten tulee tietojärjestelmän ulkoistajan muodostaa ohjeisto tietojärjestelmän loppukäyttäjiä varten. Kaikki tietoturvan osa-alueet ovat yhtä tärkeitä tietojärjestelmän ulkoistamisessa, mutta eri tietoturvaohjeistuksissa painotetaan eri tietoturvan osa-alueita. Tietoturvaohjeistuksissa tulee ottaa huomioon kaikki tietoturvan osa-alueet ja tietoturvan käytännön toteuttajien erilaiset näkökulmat ja vaatimukset tietoturvaa kohtaan.

4 Yrityskysely

Kyselytutkimuksen tarkoituksena oli selvittää, minkälaisessa tietojenkäsittely-ympäristössä tietoturvan kannalta suomalaiset pk-yritykset toimivat. Muutamalla peruskysymyksellä tarkennettiin myös tietoturvan konkreettista ylläpitoa. Toisaalta yritettiin selvittää yritysten tietohallintokäytäntöä ja asennetta tietoturvan ylläpitämiseksi. Tutkimuksen luonteeseen liittyen ja siihen olennaisesti kuuluen, selvitettiin myös pk-yritysten valmiutta ja lähtökohtia tietojenkäsittelyn ulkoistamiseen.

Kyselytutkimuksen kohteeksi valittiin kaksi liikevaihtonsa perusteella erikokoista pk-yritysten ryhmää, jotta saatiin kuva myös yrityskoon mahdollisesta vaikutuksesta tietoturvan hallintaan. Tutkimuksessa on käsitelty tuloksia näiden kahden ryhmän välillä, mikäli ne poikkeavat merkitsevästi toisistaan, muuten tuloksia käsitellään yhtenäisesti.

Kysely (liite 2) lähetettiin 120 yritykselle, joiden liikevaihto on 10-25 miljoonaa markkaa(myöh. pienemmät). Näitä yrityksiä oli lähteessä 870 kpl. Ja toisaalta kysely lähetettiin 120 yritykselle, joiden liikevaihto on 100 - 150 miljoonaa markkaa(myöh. suuremmat). Vastaavasti näitä yrityksiä oli lähteessä 411 kpl (Yritys - Suomi CD 2/97, 1997). Kyselyyn vastasi ensimmäisestä ryhmästä 52 ja toisesta ryhmästä 46. Kyselyn vastaukset käsiteltiin Microsoft Excel taulukkolaskentaohjelmalla. Yrityskyselyn tulokset (=tämä tutkimus) luvattiin kyselyyn osallistuneiden yritysten käyttöön.

Tässä luvussa puretaan kyselytutkimuksen tulokset. Niiden perusteella ja pohjalta on seuraavassa luvussa tarkoitus tuoda esiin yritysten tietoturvaan kohdis-

tuvia ongelmia. Yritysten tietoturvan hallintaa eli muodostuneitten riskien hallintaa ja käytännön mahdollisuuksia tietoturvan toteuttamiseen pohditaan tämän kyselytutkimuksen ja esitettyjen lukujen pohjalta luvussa 6. Tutkimuksen luonteen mukaisesti tietojenkäsittelyn ulkoistamisen vaikutuksia tietoturvaan käsitellään tutkimuksessa omana linjanaan. Kyselyn tulokset taulukkomuodossa esitetään liitteessä 2.

4.1 Yritysten tietojenkäsittely-ympäristö

Tässä tutkimuksessa, kuten aikaisemminkin on todettu, painotetaan tietoturvan osa-alueista tiedon luottamuksellisuutta. Luvaton tai asiaton tietojärjestelmään tunkeutuminen tai sen käyttö liittyy kuitenkin tiedon saatavuuteen ja tiedon eheyteen kiinteästi. Kyselyssä haluttiin selvittää yritysten tietojenkäsittely-ympäristöä. Tutkimuksessa selvisi, että kaikilla yrityksillä on tietoja, joita ne eivät haluaisi ulkopuolisten(esim. kilpailijan) saavan. Näitä tietoja säilytti sähköisessä muodossa 93% vastanneista. Voidaankin perustellusti sanoa tietojenkäsittelyn luottamuksellisuuden olevan yrityksille tärkeä asia.(Kuvio 10)

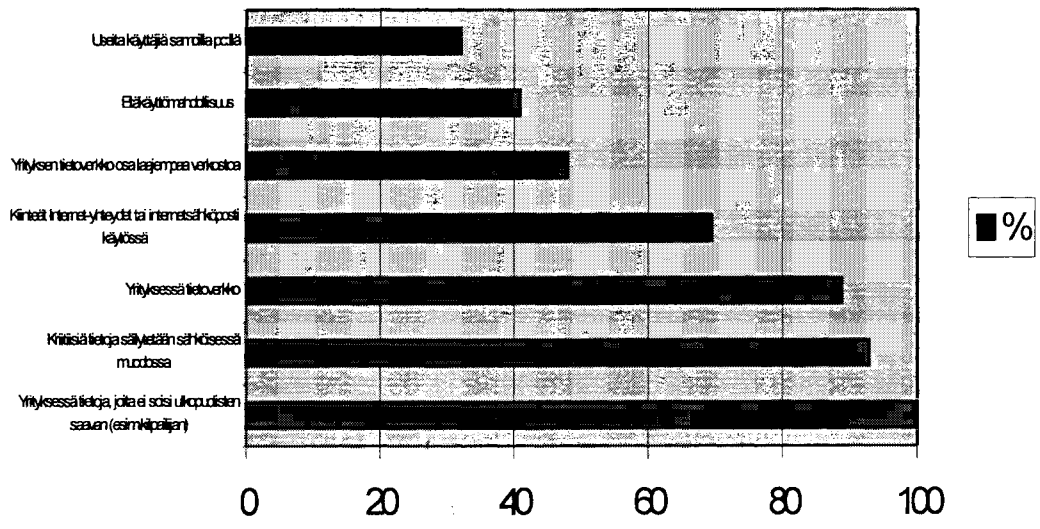
Kuvio 10: Kriittinen tieto yrityksissä. Kysyttäessä yrityksiltä onko niillä tietoa, jota eivät haluaisi vieraisiin käsiin, Ilmoittivat kaikki yritykset omistavansa tällaista tietoa. Sähköisessä muodossa tätä tietoa säilytti 93% yrityksistä.

Kysyttäessä onko yrityksissä tietoverkkoa saatiin yllättäen tulokseksi, että peräti 89% yrityksistä käyttää tietojenkäsittelyssään verkkoympäristöä ja puolet näistä on verkottunut laajemmaltikin. Tutkimuksessa on syytäkin käsitellä tietoverkkojen uhkatekijöitä ja muodostuvien riskien hallintaa perusteellisesti.

Internet on kasvava tiedon valtaväylä, mutta sen luonteesta ja kehityksestä johtuen käyttö sisältää runsaastikin uhkatekijöitä. Näistä voi hallitsemattomina muodostua tietoturvallisuusongelmia. Yrityksistä 2/3 ilmoitti käyttävänsä Internet-palveluja, joten "Netti" on ilmeisesti tullut jäädäkseen myös yritysmaailmaan.

Tietojenkäsittely-ympäristöä kartoitettaessa todetaan joissakin yrityksissä henkilökunnan käyttävän yhteisiä tietokoneita, joskin valtaosassa yrityksiä käyttää kukin henkilökohtaista tietokonetta. Etäkäyttömahdollisuus yrityksen tietojärjestelmään näyttää lisääntyvän yrityskoon kasvaessa (27%<<57%).

Nykyään on vaikea kuvitella yritystä, jolla ei olisi jonkinlaista suhdetta tietojenkäsittelyyn (ks. kuvio 11). Lähtökohtana voidaankin pitää, että yritykset ottavat yhä enemmän tietojenkäsittelyn mahdollisuuksia käyttöönsä ja toisaalta tulevat yhä riippuvaisemmiksi niistä. Tietojenkäsittelyn tietoturvalla on myös yhä enemmän merkitystä: Yrityksen kriittisten tietojen joutuminen vääriin käsiin tai vahingoittuminen voi aiheuttaa kohtalokkaita seurauksia.



Kuvio 11: Tietojenkäsittely-ympäristö yrityksissä

4.2 Yritysten kokemia tietoturvallisuusuhkia

Kysyttäessä yrityksiltä niiden suurinta tietoturvariskiä saatiin vastaukseksi monitahoinen joukko uhkakuvia, jotka tässä sensuroimatta ja mitenkään järjestelemättä esitetään.

- Virus e-mailin liitetiedostossa
- Työntekijöiden tietovuodot
- Henkilökunnan rikollinen toiminta
- Huhut
- Henkilökunta yleensä
- Suulaat työntekijät johtotasolla
- Kilpailevat yhtiöt samassa talossa
- Kesäharjoittelijoiden tiedostojen imurointi
- Henkilökunnan vaihtuminen
- Murto
- Entinen henkilökunta
- Vieraan pääsy asiakaskantaamme
- Järjestelmän kaatuminen
- Tulipalo
- Tietovuodot oman henkilökunnan kautta
- Vanha järjestelmä
- Työpaikkaa vaihtava henkilökunta
- Toimistotiloihin murtautuminen
- Avain henkilön lähteminen yrityksestä
- Fyysiset viat
- Markkinointiohjelma
- Vuosi 2000

Yritysten kokemat uhkat ovat moninaisia, ja liittyvät tietoturvallisuuden eri sektoreille. Merkille pantavaa on kuitenkin se, että yritysten kokemista uhista

enin joukko kosketti tavalla tai toisella yrityksen työntekijöitä.

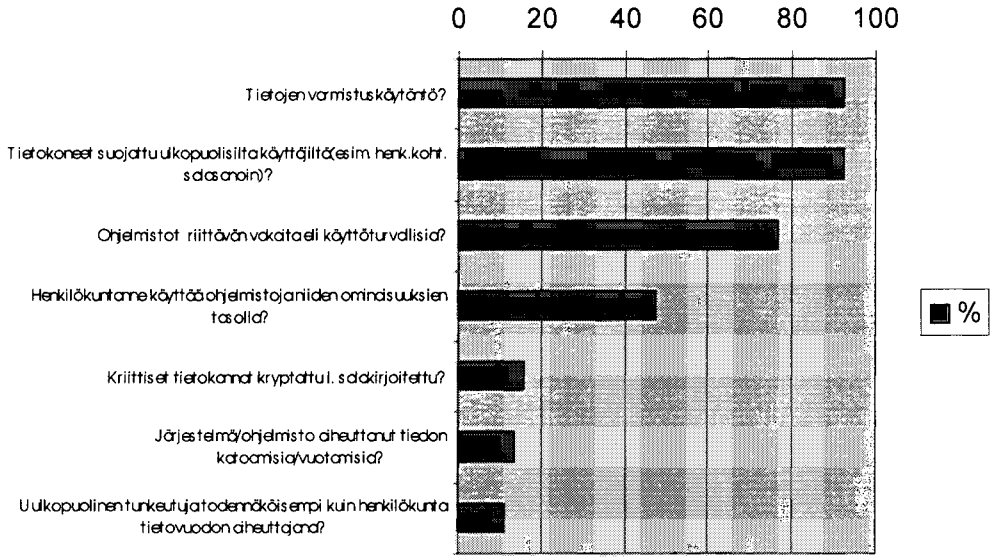
4.3 Tietoturvan ylläpito yrityksissä

Tietoturvan ylläpitoa yrityksissä kartoitettiin muutamalla valitulla kysymyksellä. Näin saatiin kuva todellisista ja jo tehdyistä tietoturvatoimenpiteistä.

Tietojen varmistuskäytäntö on omaksuttu yrityksissä hyvin. Yli 90% vastanneista yrityksistä suojasi tietonsa katoamisilta. Tietokoneet suojataan salasanoin yrityksissä yleensä myös hyvin. Sensijaan kriittiset tiedot oli kryptannut eli salakirjoittanut vain 15 prosenttia yrityksistä. Kun vain joka kymmenes yritys piti ulkopuolista tunkeutujaa todennäköisempänä kuin omaa henkilökuntaansa tietovuodon aiheuttajana ja vain joka viides yritys piti yleensä mahdollisena ulkopuolista tunkeutujaa, yritysten kannattaisi tietojen saatavuuden lisäksi kiinnittää huomiota niiden luottamuksellisuuteen.

Yrityksistä ¾ ilmoittaa ohjelmistojensa olevan vakaita eli käyttöturvallisia. Samaan aikaan vain alle puolet yrityksistä katsoo, että yrityksen henkilökunta osaa käyttää ohjelmistoja niiden ominaisuuksien tasolla. Ja joka kymmeneltä yritykseltä oli kadonnut/vuotanut tietoja. Henkilökunnan merkitystä tietoturvallisuuteen selvitetään lähemmin luvuissa 5 ja 6, mutta tässäkin yhteydessä voidaan todeta sen olevan suuri resurssi tietoturvan toteuttamiselle mutta myös suuri uhka tietoturvalle. (Kuvio 12)

Internetin mahdollisuuksia hyödynnetään yrityksissä laajalti, varsinkin Internet-sähköposti on tullut yhä suositummaksi. Palomuurikoneita käytetään kuitenkin vain joka toisessa niistä yrityksessä, jotka ilmoittavat hyödyntävänsä Internetiä. Samaten vain joka kolmas yritys niistä, jotka sallivat työntekijöilleen etäkäyttömahdollisuuden, on varmistanut etäkäytön takaisinsoitolla.



Kuvio 12: Ohjelmisto- ja järjestelmäturvallisuus yrityksissä

Tietoturvatoimenpiteet yrityksissä ovat usein fyysisiä; on helpompi ostaa kone tai ohjelma kuin kouluttaa henkilökunta osaavaksi ja vastuuntuntoiseksi. Seuraavassa luvussa hieman enemmän aiheesta.

4.4 Tietoturvan hallinta yrityksissä

Kyselyllä pyrittiin saamaan kuva siitä, kuinka yritysten tietoturvan hallinta on järjestetty eli kuka vastaa ja mistä. Yleisesti mielenkiinnon kohteena oli myös tietoturvan asema yrityskulttuurissamme: Mikä on asenne tietoturvaa kohtaan?

Kyselyssä kävi ilmi, että 4/5 yrityksestä oli yleisellä tasolla pohtinut tietoturvakysymyksiä. Tämä ei ole kuitenkaan olennaista vaan se, että joka viides yritys ei ollut edes yleisellä tasolla avannut yrityksen tietoturvakeskustelua. Kun taas kysyttiin johdon ja henkilökunnan perehtyneisyyttä tietoturvaan, havaittiin, että joka toinen yritys oli perehdyttänyt johtonsa. Sensijaan henkilökuntansa oli tietoturvan hallintaan perehdyttänyt vain joka kolmas yritys.

Tietoturvan hallintaan olennaisesti kuuluu, että joku yrityksessä vastaa siitä. Yrityskoon kasvaessa yhä useampi yritys on sisällyttänyt tietoturva-asiat erikseen mainitulle henkilölle. Kuitenkin luvun ollessa pienemmillä yrityksillä 42% ja suuremmillakin vain 65%, voidaan vielä todeta olevan lukuisia yrityksiä, joissa tietoturvasta ei vastaa kukaan.

Tietoturvan toteuttamisessa sen ohjeistaminen (ks. 2.2) yrityksen sisällä on liki välttämätöntä. Jos yrityksen henkilökunta ei tiedä, kuinka tietoturvaa käytännössä toteutetaan, ei voida puhuakaan hallitusta tietoturvallisuudesta. Yrityksille lähetetyn kyselyn perusteella vain joka neljäs yritys on normittanut tietojenkäsittelynsä tietoturvan kattavaksi.

Tehdyn kyselyn perusteella voidaan sanoa, että Suomessa on lukuisa joukko yrityksiä joiden tietoturvallisuustaso on pelkästään uskomusten ja hyvän tuurin varassa. Tätä kuvastaa sekin, että vain puolet yritysjohdosta ilmoittaa omaavansa riittävän kuvan tietoturvariskeistä. Myös se, että vain puolet yrityksistä ilmoittaa olevansa omavaraisia tietoturvan tietotaidon suhteen peilaa tilannetta.

Kyselyssä käy lisäksi ilmi, että ulkopuolista apua on käytetty tietoturva-asioiden hallintaan enemmän suuremmissa yrityksissä(29% << 46%). Toimia tietoturvan kehittämiseksi on suunnitellut pienemmissä yrityksissä 63% vastanneista ja suuremmissa 80%. Tämä kuvastaa luonnollisesti jonkinasteista tietoturvaherää-mistä. Seuraavaa tietoturvatoimenpidettä kysyttäessä sai yrityksiltä seuraavanlaisia vastauksia, jotka tässä esitetään luettelonomaisesti:

- Varmistusten toimivuus, palautustoiminnon varmuus
- Takaisinsoittovarmistus
- Tietoturvaprojektin käynnistys
- Salakirjoituksen käyttöönotto
- Organisaatio ja koulutus
- Käyttöoikeuksien tarkistus

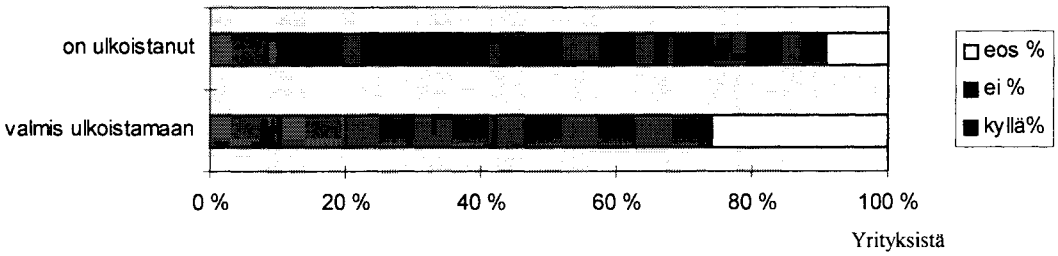
- Palomuurin hankinta
- Tietoturvaohjeiden laatiminen
- Virustorjunta
- Kulunvalvonta
- Laitekannan uusinta
- Internet-yhteyksien tietoturvan varmistus
- Sähköpostinvarmistus
- Salasanojen muuttaminen
- Järjestelmän uusiminen
- Kartoitus riskeistä

Suurin osa yritysten tietoturvatoimenpiteistä näyttää hyvin rajoittuneilta. Tietoturvan kokonaisvaltaiseen hallitsemiseen tarvitaan kuitenkin suunnitelmallisuutta. Sitä tullaankin käsittelemään myöhemmin luvussa 6.

4.5 Tietojenkäsittelyn ulkoistamisen valmiudet yrityksissä

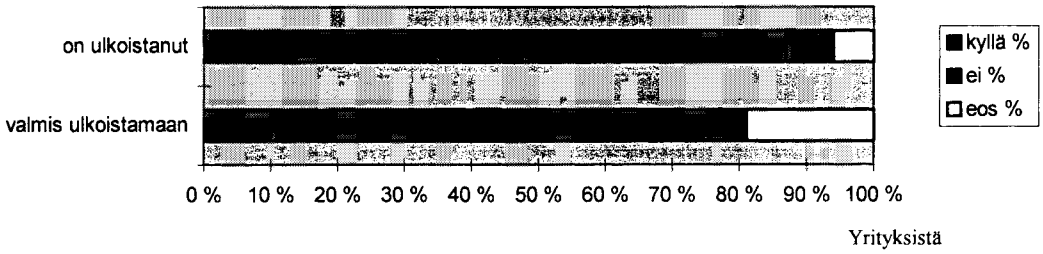
Kun yritysjohto päättää tietohallinnon järjestelyistä, tietohallinnon ulkoistaminen on tietojenkäsittelyn edelleen monimutkaistuessa yhä varteenotettavampi vaihtoehto. Tietohallinnon ulkoistamisella ikään kuin siirretään vastuu pois omalta reviiriltä "alan ammattilaisten" asiaksi. Lisäksi yrityksessä, joka ulkoistaa tietohallinnon, vapautuu pääomia varsinaista liiketoimintaa varten. Ulkoistaminen tuntuu varsin helpolta vaihtoehdolta.

7/10 yrityksestä tiesi mitä tietojenkäsittelyn ulkoistaminen merkitsee. Varsin uutena asiana kuitenkin vain kyselyn suuremmilta yrityksiltä on löytynyt rohkeutta ulkoistaa tietojenkäsittelynsä. Näistä 15% luotti tietohallintonsa ulkopuolisiin käsiin. Suuremmista yrityksistä lähes kaikki, jotka ovat valmiit ulkoistamaan tietojenkäsittelynsä ovat sen tehneet.(Kuvio 13)



Kuvio 13: Ulkoistaminen; yritykset, joissa 100 - 150 milj. liikevaihto

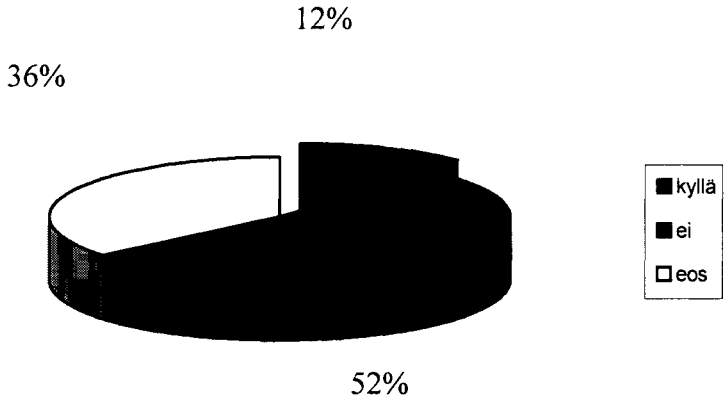
Pienemmistä yrityksistä ainutkaan ei ollut ulkoistanut tietojenkäsittelyään. Sen sijaan valmius ulkoistamiseen oli 12% vastanneista(Kuvio 14). Yritysjohdon tietohallintotietämystä kuvastanee se, että molemmissa ryhmissä oli joukko vastanneita, jotka eivät osanneet sanoa oliko yritys ulkoistanut tietohallintonsa vai ei.



Kuvio 14: Ulkoistaminen; yritykset, joissa 10 - 25 milj. liikevaihto

Yritysten valmiutta tietohallinnon ulkoistamiseen, selvitettiin myös kysymällä minkälaisen datan he ovat valmiit luovuttamaan ulkopuolisen yhteistyökumppanin käsiin. Yrityksen kriittiset tiedot oli valmis luovuttamaan 12% vastanneista. Vain rutiininomaisen datan oli valmis luovuttamaan 41% yrityksistä. Tietojärjestelmän ulkoistamisessa on yleensä kyseessä totalitäärinen tietohallinnon siirto ulkoistamispalvelut tarjoavaan yritykseen. Tämä organisaatio tuskin voi pk-yritysten tapauksessa olla osa ulkoistavaa organisaatiota tai konsernia, kuten usein on tapana suuryritysten ollessa kyseessä.

Ulkoistamisen etuja ja haittoja oli yrityksistä pohtinut neljännes pienemmistä yrityksistä ja puolet suuremmista yrityksistä. Ulkoistamisen pääomia vapauttavasta vaikutuksesta oli tietoinen hieman useampi. Tietojenkäsittelyn ulkoistaminen on varsin tuore asia pk-sektorilla, minkä tämäkin kysely osoittaa. Tietoturvanäkökulmasta katsottuna yritykset ovat varsin skeptisiä: Vain 12% yrityksistä uskoo tietoturvan kasvavan tietojenkäsittelyn ulkoistamisessa. (Kuvio 15).



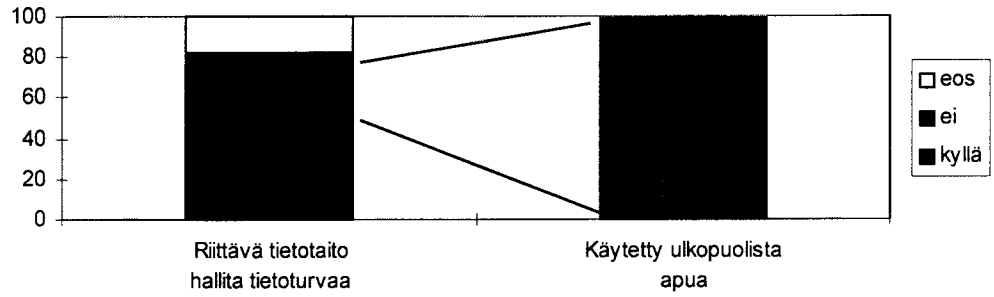
Kuvio 15: yritysten mielipide siitä, kasvaako tietoturva ulkoistettaessa

Ulkoistaminen on varsin heikosti tunnettu tietohallinnon organisointimenetelmä pk-yritysten piirissä. Tietojenkäsittelyn perusluonteeseen on kuitenkin kuulunut alan syntyhetkistä lähtien tietty luoksepääsemättömyys; toisinsanoen: "Joko hallitset kaiken tai et yhtään mitään". On aivan odotettavaa, että ulkoistaminen tulee houkuttelevana vaihtoehtona lisääntymään yritysten tietohallintokäytäntönä. Varsinkin silloin, jos niin sanotut verkkotietokoneet (nc, net pc) lyövät itsensä läpi kivenkovien pc- ja ohjelmistomarkkinoiden.

4.6 Yhteenveto

Yrityksen tietoturvaan kohdistuu useanlaisia uhkia (ks. Luku 4.2). Yritykset pitävät ulkopuolista tunkeutujaa vain yhdessä tapauksessa kymmenestä mahdollisena tietovuodon aiheuttajana; suurimpana uhkana pidetään omaa henkilökuntaa. Yrityksen keinona hallita tietoturvallisuutta on tunnistaa uhat ja määrittää aiheutuvat riskit. Tämän jälkeen voidaan riskejä hallita erikseen toteutettavan tietoturvallisuusohjelman avulla. Siinä määritellään tietototuryaohjeistus (ks. 2.4). Henkilökunnan ja yrityksen johdon perehtyneisyys tietoturvaseikkoihin on myös tärkeää. Yrityskyselyn perusteella yrityksiä joissa sekä johto että henkilökunta ovat perehtyneitä tietoturvaseikkoihin ja tietoturva on ohjeistettu on vain 13 prosenttia.

Yrityksille on tarjolla keinoja ja menetelmiä tietoturvan hallintaan. Kyse lienee usein vain tietämyksen ja tahdon puutteesta, jos tietoturva-asiat jäävät takaalalle yrityssuunnittelussa. Yrityskyselyn perusteella niistä yrityksistä, joissa ei ole riittävää tietoturvatietämystä, 2/3 ei ollut käyttänyt ulkopuolista apuakaan (Kuvio 16) ja joka kolmas ei ole edes suunnitellut toimia tietoturvan kehittämiseksi.



Kuvio 16: Tietoturvan hallinta yrityksissä. Tietoturva-asennetta kuvaavaa on se, että niissä yrityksissä joissa ei ole riittävää tietotaitoa hallita tietoturvaa ei myöskään kahdessa tapauksessa kolmesta ollut käytetty ulkopuolista apua.

Tietojärjestelmän ulkoistamisprosessi on vaikea ja vaativa toimenpide. Tieto-

järjestelmän ulkoistamisen kesto on yleensä useita vuosia, joten ulkoistamista on suunniteltava huolella. Jos yrityksessä ei ole riittävää tietotaitoa hallita tietoturvaa, on mahdotonta tehdä kattavaa ulkoistamissopimusta ja valvoa sitä. Yrityksiä, jotka ilmoittivat ettei riittävää tietohallinnon tietotaitoa ole, oli kyselyn perusteella 30 %. Näistä viidennes olisi kuitenkin valmis ulkoistamaan tietojenkäsittelynsä. Tämänkaltaiset yritykset saattavat jäädä täysin ulkoistamispalvelun tarjoavan organisaation armoille - ainakin tietoturva-asioissa.

5 YRITYKSEN TIETOTURVAAN KOHDISTUVIA UHKIA

Tässä luvussa käydään läpi vallitsevia tietoturvauhkia. Edellisen luvun, siis yrityskyselyn pohjalta, on kartoitettu yritysten kohtaamia uhkia ja ongelmia tietoturvan suhteen ja verrattu niitä kirjallisuuden esittämiin näkökohtiin. pyritty tuomaan esille toimivia tietoturvaratkaisuja ongelmakohtaisesti

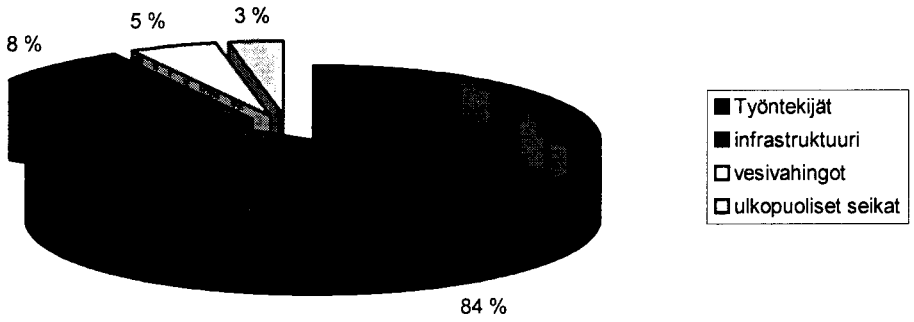
Kaikki kyselyyn osallistuneet yritykset ilmoittivat, että niillä on tietoja, joita eivät soisi ulkopuolisten saavan. Sähköisessä muodossa näitä tietoja säilytettiin 93 % yrityksistä. On siis varsin tärkeää tietää yrityksen kriittisiin tietoihin kohdistuvista uhkatekijöistä.

5.1 Yrityksen sisäiset tietoturvallisuusuhat

Johdannoksi yritysten tietoturvallisuusuhkien käsittelyyn, tietojenkäsittelyn ongelmista johtuvien taloudellisten menetysten voidaan ajatella jakautuvan seuraavasti (Computer System Security and Privacy Advisory Board. 1992), (Kuvio 17):

- 65% virheistä ja laiminlyönneistä
- 13% epärehellisistä työntekijöistä
- 6% tyytymättömistä työntekijöistä
- 8% infrastruktuurin pettämisistä; mukaanlukien sähkön, telekommunukaation, tulipalot, tulvat, laitteiden tahattomat rikkoontumiset, kuljetuksen ja liikenteen sekä levottomuudet jne.
- 5% aiheutui vedestä; poislukien tulipalot ja tulvat
- 3% ulkopuolisista; mukaanlukien mm. virukset, vakoilun, toisinajattelijat ja entiset, yli 6 viikkoa poissaolleet työntekijät.

(Vesivahinkojen osuus on tässä kyseisessä yhdysvaltalaisessa tutkimuksessa tavattoman suuri; sopii vain toivoa, että Suomessa vesi- ja viemärityöt on tehty paremmin.)



Kuvio 17: Työntekijöiden osuus tietojenkäsittelyvahingoista suhteessa yrityksen taloudellisiin menetyksiin. (Computer System Security and Privacy Advisory Board 1992)

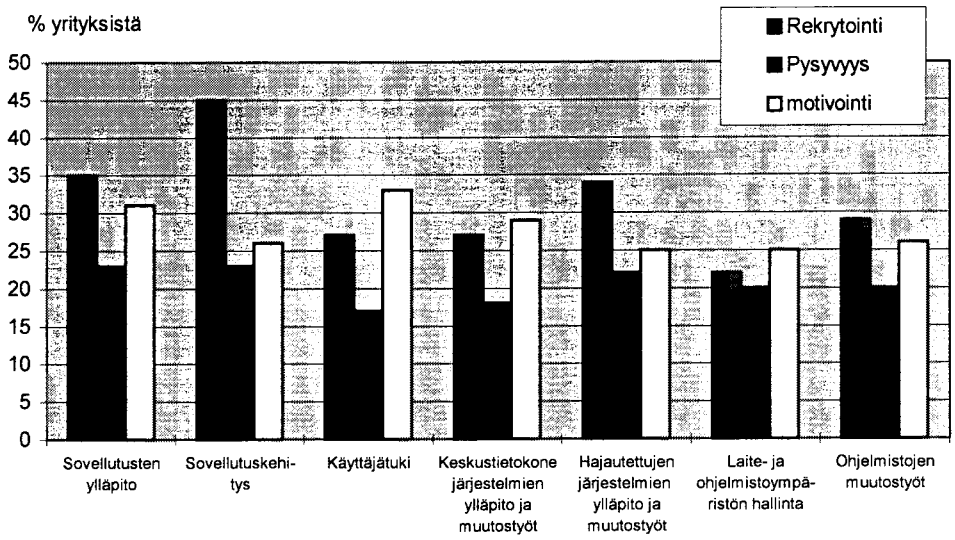
5.1.1 Henkilöstöturvallisuus

Yrityksille suunnatun kyselyn perusteella yrityksistä vain 11 % piti ulkopuolista tunkeutujaa henkilökuntaa todennäköisempänä riskinä mahdollisen tietovuodon aiheuttajana. Toisaalta vain 22 % yrityksistä katsoi yleensä olevan mahdollista, että ulkopuoliset pääsisivät tunkeutumaan yritysten kriittisiin tietoihin.

Henkilöstö on suuri resurssi tietoturvan toteuttamiselle, mutta samalla se on myös mahdollinen uhka tietoturvalle. Henkilökunnan toimenpiteet perustuvat vastuiden, velvollisuuksien ja ohjeiden noudattamiseen tietoturvaan liittyvissä toimissa. Henkilöstön huomioonottaminen tietoturvaa suunniteltaessa on on-

nistumisen kannalta erittäin merkittävä tekijä. Noin 5 % järjestelmien käyttäjistä katsotaan olevan potentiaalinen uhka tietoturvalle. Toisaalta n. 80 % tietoturvaloukkauksista (tahattomista tai tahallisista) tapahtuu suomalaisen tutkimuksen mukaan yrityksen sisältä.(Mäntylä & Kajava 1997)

Työntekijöiden taitamattomuus ja osaamattomuus on nousemassa varsin suureksi ongelmaksi koko tietohallinnolle. On selvä, että myös yritysten tietoturvaan kohdistuu suuri uhka juuri henkilöstön taitamattomuudesta. Enin osa yrityksistä kokee, että niillä on puutteita IT -henkilöstön osaamistasossa (ks. kuvio 18). Henkilökunnan jatkuva koulutus näyttääkin olevan pakollinen toimenpide nykyaikaisessa yrityksessä.



Kuvio 18: Yritysten kokemia ongelmia pätevän IT-henkilöstön suhteen.(IDC 1997)

Erään tutkimuksen mukaan päällikkötason IT-henkilöt pitivät 90 % työntekijöistä uhkana tietoturvallisuudelle, näillä ei siis katsottu olevan tarvetta päästä käsiksi yritysten kriittisiin tietoihin. (Ks. Violino & Panettieri 1993). On kuitenkin selvää, että yrityksen sisäpiiri aiheuttaa suurimman riskin tietoturvallisuudelle. Sisäpiiriin voidaan lukea sekä virkailijat, että tekninen henkilöstö.

Myös yrityksen aiemmat työntekijät muodostavat varteenotettavan uhan, koska he tuntevat kohteena olevan tietojärjestelmän (mm. Charney 1993).

Kuriositeettina voidaan mainita, että esim. vuonna 1992 Yhdysvalloissa pidätettiin kaksi tusinaa liittovaltion tai osavaltion työntekijää, kun he olivat myyneet henkilötietoja sosiaaliturvahallinnon tietokannoista. (House Committee on Ways and Means 1992)

Henkilöriskeistä johtuen mikään tietoturvaratkaisu ei voi olla täysin varma!

5.1.2 Laitteistoturvallisuus ja fyysinen turvallisuus

Laitteistoturvallisuudella pyritään varmistamaan tietokonelaitteiston häiriötön ja luotettava toiminta. Ongelmia voivat aiheuttaa laitteistovirheet, väärät käyttöolosuhteet tai virheellinen käyttö. Fyysinen ympäristö kuten sähkövirran laatu, pöly, ilmankosteus ja lämpötila voivat aiheuttaa laitteisto-ongelmia.

Turvallisuuteen liittyy laitteiden säännöllinen huolto. Virhe- ja ongelmatilanteessa nopeasti saatavissa oleva huolto tai varalaitteisto pelastaa tilanteen. Varaosien ja tarvikkeiden saatavuus on varmistettava ja kannattaa myös pitää riittävää omaa varastoa. Laitteistojen kunnon selvittämisessä ja huollon tarpeen arvioinnissa voidaan käyttää erilaisia testausohjelmia.

Laitteistohäiriöitä aiheuttavat tyypillisesti:

- virheelliset ohjelmistot
- piirikorttien vikaantuminen
- näyttölaitteen kuluminen
- levymuistin vioittuminen
- laitteiston kuluminen ja likaantuminen

- näppäimistön kuluminen ja vaurioituminen
- laitteiston kuljetukset
- asennus- ja huoltotoimenpiteet
- sähköiset häiriöt (jännitepiikit)

Laitteistojen luvaton käyttö voidaan estää fyysisillä turvamenetelmillä sekä salasanoilla ja laitteiston lukituksilla. 93 % yrityskyselyyn osallistuneista yrityksistä olikin suojannut tietokonekantansa ainakin salasanoin, mutta esim. etäkäytön oli varmistanut takaisinsoitolla vain kolmannes etäkäyttöä käyttävistä yrityksistä. On Lisäksi todettava, että esimerkiksi Microsoft -ohjelmistoissa käytettävät salasanat ovat helposti purettavissa. Salasanan avausohjelmia saa ostaa näihin tuotteisiin vapaasti n. tuhannen markan hintaan(ks. esim. http://www.crak.com). Ainoa luotettava salausmenetelmä lienee salasanalla varmistettu kryptaus.

Etäkäyttömahdollisuus, tai etätyö, vaatii etäkäyttöpisteessä samojen tietoturvallisuusnormien noudattamista kuin yrityksessä itsessäänkin. Lisäksi erityistä huomiota on kiinnitettävä tietoliikenteen turvaamiseen. Tietoliikenneyhteyksien varmistaminen takaisinsoitolla estää hyvinkin asiattomilta tunkeutujilta. (Ks. Hetky 1997)

5.1.3 Ohjelmisto- ja järjestelmäturvallisuus

Yrityskyselyn perusteella 76 % vastaajista ilmoitti ohjelmistojensa olevan riittävän vakaita eli käyttöturvallisia. Yrityksistä 72 % ilmoitti, etteivät järjestelmä/ohjelmistot ole aiheuttaneet tiedon katoamisia tai vuotamisia. Huomioitavaa on, että joka kymmenes vastanneista ei osannut määritellä käyttöturvallisuustasoa saati sitä, onko mahdollisten tietovuotojen taustalla ohjelmistot/järjestelmä.

Ohjelmistoturvallisuus voidaan jakaa sovellusohjelma- ja käyttöjärjestelmäturvallisuuteen. Suurimpina riskeinä ovat virheellisesti toimivan sovellusohjelman ajaminen käyttöjärjestelmässä, joka ei sisällä tietoturvaominaisuuksia.

Ohjelmien ja järjestelmien virheet (bugs) ovat laskeneet tasolle, joka vastaa yhtä virhettä koodissa per tuhat kirjoitettua riviä (NIST 1996). Ohjelmien ja järjestelmien koon kasvaessa on kuitenkin havaittavissa "täydellisten" ohjelmien totaalinen puuttuminen. Ohjelmistovirheet saattavat aiheuttaa hyvinkin traagisia menetyksiä, taloudellisia - ja jopa ihmishenkiä.

Itse tehdyt tai räätälöidyt sovellusohjelmat ovat suuri tietoturvariski. Ongelmia aiheuttavat usein tekijöiden riittämätön osaaminen, laadunvalvonta sekä puutteelliset tai olematon dokumentointi ja käyttöohjeet. Monesti ohjelman tekee yksi ihminen, jolloin neuvonta ja ohjelmiston korjaus ja päivitys voi olla ongelmallista.

Järjestelmän suunnittelussa tulisi huomioida seuraavat seikat:

- Suunnittelumenetelmä on standardisoitu ja hyväksytty (tilaaja)
- Modulaarisuus, jolloin jokainen moduuli tekee tarkoin määritellyn pienen tehtävän
- Rakenteinen ylhäältä - alas -lähestyminen
- Ohjelmien suunnitteluun ja kuvaamiseen osallistuu ainakin kaksi henkilöä

Ohjelmoitaessa puolestaan tulisi huomioida seuraavaa:

- Ohjelmointiympäristö on vakio (hakemistot)
- Ohjelma jaetaan moduuleihin
- Moduulin alussa on sen esittely
- Moduulit kommentoidaan
- Moduulissa on yksi aloituskohta ja korkeintaan kaksi lopetuskohtaa
- Käytetään korkean tason ohjelmointikieliä

- Ohjelmiin lisätään tarkistuksia (tarkistussummia), jolloin voidaan havaita ohjelman laiton muuttaminen
- Kriittiset muutokset varmistetaan toisen henkilön toimesta
- Ohjelmaan tehtävät muutokset tulee dokumentoida sekä ohjelmakoodiin että muihin dokumentteihin

Ohjelmien testaus on tietoturvan kannalta tärkein osa tietosysteemin rakentamista. Testaukseksi ei riitä ohjelman tekijän suorittama moduulitestaus vaan lopullisen systeemin hyväksymistestauksen suorittavat tilaaja ja systeemin käyttäjät.

Testaussuunnitelma tehdään ennen testauksen aloittamista. Siinä selvitetään mitä testataan, testiaineisto, odotettavissa olevat tulokset, hyväksymiskriteerit, testaaja ja käytettävä menetelmä. Testauksen tulisi simuloida systeemin todellista käyttöä. Tuloksista toimitetaan kirjallinen testausraportti, josta ilmenevät testauksen tulokset. Ohjelman tekijän ei itse pitäisi koskaan suorittaa varsinaista testausta. Testauksessa ja muutenkin ohjelman kehitystyössä ohjelman käyttäjät tulisi ottaa mukaan työhön mahdollisimman aikaisessa vaiheessa. Näin järjestelmästä saadaan vakaampi ja käyttöhenkilöstö on motivoituneempaa ja osaavampia ohjelman käytössä. Yrityksille suunnatun kyselyn perusteella osasi henkilökunta käyttää ohjelmistoja niiden ominaisuuksien tasolla vain 46 %:ssa yrityksistä. Suuremmissa yrityksissä osaamistaso näyttää heikkenevän (58 % >> 33%). Osaamiseen investoiminen saattaa maksaa sijoituksen korkojen kanssa takaisin.

5.1.4 Tietoaineisto- ja käyttöturvallisuus

Tietoaineiston turvaamisessa pyritään estämään tiedon tuhoutuminen tai muuttuminen sekä sen joutuminen asiattomiin käsiin. Siihen liittyy olennaisena osana

tiedon varmistaminen, säilytyksen asiallisuus ja tiedon hävittäminen. Tietoaineiston luokittelu määrittelee oikeat menettelytavat. Tietojen tuhoutuminen johtuu yleensä käyttäjän virheellisestä toiminnasta, ympäristövahingosta, tietovälineiden väärästä käsittelystä, ohjelmisto- tai laitteistovirheistä.

Asianmukaisella varmuuskopioinnilla voidaan vahingot minimoida. Varmistusväli ja kopioiden säilytyksen asiallisuus ovat olennaisia. Tietoaineisto on varmistettava vähintään kahtena säännöllisesti päivitettävinä kopioina. Kopiot tulee säilyttää eri paikoissa mieluiten eri rakennuksessa. Toinen kopio säilytetään varmuusarkistossa, joka on suojattu tuli- ja vesivahingoilta. Paperituloste voi toimia varmuuskopiona, jos magneettinen kopio on tuhoutunut (ohjelmalistaukset). Ohjelmien dokumentaatio tulee myös suojata. Yrityskyselyn perusteella 93 % yrityksistä suorittaa tietojen varmistamisen, loput luultavasti luottavat muistinsa.

Käyttäjien tahatonta tietojen tuhoamista voidaan estää oikein määritellyillä käyttöoikeuksilla. Organisaation käyttämä tiedostojen nimeämisstandardi selventää yhteisten tiedostojen käsittelyä.

Tietoturvan loukkaukset johtuvat varsin usein inhimillisistä tietojärjestelmän käyttöön liittyvistä asioista. Tiedon häviäminen ja muuttuminen johtuvat useimmiten käyttäjän tahattomista teoista, vahingoista, tietämättömyydestä tai osaamattomuudesta.

Käyttöturvallisuutta voidaan edistää koulutusta lisäämällä. Käyttäjien tunnistaminen ja käyttöoikeudet estävät tahallisia ja tahattomia tietoturvaloukkauksia. Lokitiedostoja ylläpitämällä ja niitä tutkimalla voidaan selvittää ongelmien syitä ja tietoturvauhkia.

Testi- ja ohjelmistoympäristö tulisi eristää käyttöympäristöstä, jolloin ne eivät pääsisi häiritsemään toisiaan. Tuotannon- ja prosessinohjausjärjestelmissä ei tulisi sallia normaalia tietokoneen käyttötoimintaa.

5.2 Yrityksen verkkokäytön tietoturvallisuus

Verkkoon tunkeutujan käyttämät murtautumismenetelmät voidaan jakaa sosiaalisiin ja teknisiin menetelmiin. Sosiaalisissa menetelmissä tunkeutuja käyttää väärin omia oikeuksiaan tai huijaa toisia käyttäjiä. Tämä on hyvin usein helpompaa kuin teknisten ratkaisujen käyttö. Myös laitteistojen heikkouksia voi käyttää hyväksi, esimerkiksi suojaamaton muistijärjestelmä on tehokas keino salasanojen selvitykseen.

5.2.1 Verkkokäytön tietoturvauhkia

Yrityskyselyn (ks. luku 4) perusteella yhdeksällä kymmenestä yrityksistä oli tietoverkko ja puolet näistä kuului laajempaan tietoverkostoon. Verkkokäytön lisääntyminen onkin ajan ilmiö mutta se tuo tullessaan myös joukon ongelmia. Seuraavana on lueteltu eräitä verkkoturvallisuuden kannalta harmillisia menetelmiä:

Virukset ovat useimmiten harmittomia ohjelmanpätkiä, mutta voivat olla äkäisiäkin; pahimmillaan ne aiheuttavat koko tartunnan saaneen laitteiston tai jopa verkon lamaantumisen. Virustorjuntaohjelmien käyttäminen onkin jokseenkin välttämätön suojautumiskeino kaikissa tietojärjestelmissä. Viruksia havaitaan Yhdysvalloissa liike-elämän tietokoneissa 1 / 1000 pc / neljännesvuosi. Todellisten infektioiden määrä lienee kuitenkin paljon suurempi, 3 - 4 kertainen, koska suuri osa yritysmaailmankin tietokoneista on huonosti viruksilta

suojattuja (ks. Kephart & White 1993). Vaikka tunnettujen viruksien määrä lisääntyy jyrkästi, virus infektioiden määrä kasvaa vain tasaisesti. Viruksista on tulossa yhä tavanomaisempia vierailijoita.

Salakuuntelu on tehokas murtautumistapa ja se on päätteiden ja lähiverkkojen tapauksessa melko helppoa.

Troijan-hevoset ovat ohjelmanpätkiä joita pyritään huomaamattomasti ujuttamaan suojattuun järjestelmään. Päästyään järjestelmään ohjelman tekee suojamuuriin aukon josta murtautuja pääsee halutessaan sisään systeemiin.

Suojausaukot ovat virheellisiä suojausmäärittelyjä, jotka altistavat systeemin turvallisuusuhalle. Tyypillinen tapaus on Unix-tiedosto jonka käyttöoikeudet on väärin määritelty.

Salasanojen arvailu on yleinen tapa päästä systeemiin. On tutkittu, että jopa joka neljännellä käyttäjällä on huono salasana. Jos päästään käsiksi suureen määrään salasanatietoja on yhden salasanan arvaaminen mahdollista melko nopeastikin.

Ohjelmistovirheet ovat myös tapa päästä järjestelmään. Jokainen ohjelma sisältää virheitä, joista monia ei edes koskaan havaita. Käytännössä ohjelmistovirheiden täydellinen poistaminen esimerkiksi suuresta käyttöjärjestelmästä on käytännössä mahdotonta.

Tiedonsiirto erilaisissa tietoverkoissa, oli ne sitten yksityisiä eli suljettuja tai avoimia, on lisääntynyt räjähdyksenomaisesti viime vuosina. Erityisesti avoimen Internet-tietoverkon käyttö on tuonut julkiseen keskusteluun myös tietoverkkojen turvallisuuden eli tietoturvan. Yleisesti aikaisemmin tästä asiasta olivat huolestuneet vain suuret yritykset, rahalaitokset ja puolustushallinnon verkon käyttäjät.

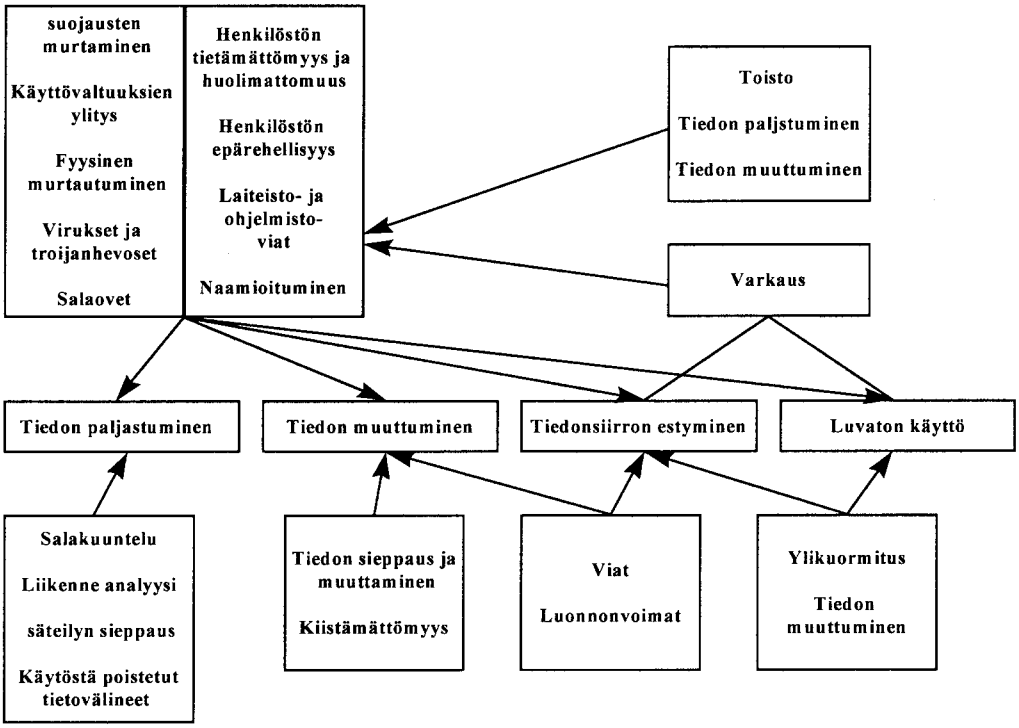
Tietoverkkojen, erityisesti TCP/IP-verkkojen reititystekniikka, perustuu siihen, että yhteyksittäin muodostuu aina silloiseen tilanteeseen teknisesti paras yhteys. Täten ko. yhteyden muodostumisreittiä ei voida aina ennakoida. Tällöin yhteys

voi kulkea sellaisen reitittimen kautta, jonka läpikulkevaa liikennettä seurataan asiattomasti.

Kotimaan yhteyksillä yhteydenmuodostusreitit ovat suurimmalta osalta tunnettuja verkkojen luonteesta johtuen, mutta mitä kauemmaksi yhteydenmuodostusreitti kasvaa, sitä suurempi on mahdollisuus, että joku asiaton seuraa läpikulkuliikennettä.

Läpikulkuliikenteen vakoilumahdollisuudelta ei voi aukottomasti suojautua, jos liikennöidään useammassa kuin yhdessä tietoliikenneverkossa. Mikäli tieto on sen tyyppistä, että se halutaan suojata ulkopuoliselta vakoilijalta, on syytä käyttää tehokkaita salausmenetelmiä mekaanisine salaamislaitteineen ja hallittuine avaintunnuksineen. Kuviossa 19 on kuvattu tietoverkkojen mahdollisia uhkia.

Verkkoturvallisuuteen liittyy luonnollisesti kaikki yrityksen sisäiset tietoturvallisuusuhat. Onhan jokainen verkkoon liittynyt henkilö, laite, järjestelmä ja ohjelmisto oma uhkatekijänsä. Suuren uhkan, joka korostuu tietoturvatietämättömyydestä, muodostaa verkossa mahdollisesti oleva epäkurantti tietoaineisto, josta enemmän seuraavassa luvussa.



Kuvio 19: Verkkokäytön tietoturvallisuusuhkia (Lähde: Airaksinen 1995)

5.2.2 Verkosta löydetyn tiedon vahingollisuus

Koska verkko on täynnä mitä erilaisinta tietoa, verkosta löydettävä tiedosto voi sisältää yrityksen järjestelmiä vahingoittavia ohjelmanosia. Varsinkin pakatut tiedostot saattavat sisältää jotain sellaista, jota ei tiedoston nimestä olekaan pääteltävissä. Verkosta haetut tiedostot on varminta hakea sitä varten erikseen varatulla koneella, jolla puretulle tiedostolle voidaan tehdä virustarkastukset mahdollisimman uudella ohjelmalla.

Sähköpostiohjelmistot mahdollistavat useimmiten postin lähettämisen väärällä lähettäjätunnuksella. Tarkemmin viestiä tutkittaessa lähettäjätietojen virheelli-

syys on useimmiten varsin helposti havaittavissa. Tämä ei poista sitä tosiasiaa, että väärennetty lähettäjätunnus voi jäädä siitä huolimatta huomaamatta.

Sähköpostiviestinnässä on otettava huomioon mahdollisuus, että viesti on joltakin muulta kuin lähettäjätiedoissa näkyvältä käyttäjätunnukselta. Mikäli on pystyttävä täysin varmentamaan lähettäjä, on syytä käyttää sähköistä allekirjoitusta. Myös viestin salaaminen parantaa tietoturvaa, mikäli käytetään luotettavaa salausmenetelmää.

Tietojärjestelmään murtautumisessa joku verkon tai yksittäisen koneen käyttäjä pyrkii tietoisesti murtautumaan sellaisen verkon tai koneen sisään, jolle hänellä ei ole oikeutta. Mikäli hän kykenee murtautumaan järjestelmään sisään, hän voi joko vakoilla tietoja tai vahingoittaa systeemiä.

Internetiin kiinteästi liitetty asiakasjärjestelmä on syytä suojata vähintään reitittimissä tehtävillä suodatuksilla tai yhdessä suodatuksilla, osoitteistuksella sekä palomuurikoneilla (ks. 6.3).

Edellä mainitut kauttakulkuliikenteen analysointi (ks. 5.2.1), verkosta löydetyn tiedon vahingollisuus ja osoitteiden väärentäminen ovat enemmänkin ominaisuuksia, joita ei voida täysin poistaa mutta, jotka voi ottaa huomioon Internetiä käytettäessä. Ne koskevat niin valinnaista kuin kiinteää yhteyttä käyttävää käyttäjää.

Sitä vastoin tietoturvajärjestelmään murtautuminen koskee lähinnä kiinteän yhteyden Internet-käyttäjiä. Kiinteä Internet-liittymä voidaan suojata usealla eri tavalla. Minkälainen suojaus valitaan, riippuu osittain siitä, mitä palveluita aiotaan tarjota Internetiin päin ja minkälainen on lähiverkon omien sovellutusten tietoturva. Jos verkosta liikennöidään vain ulospäin, voidaan valita kevyemmät

ratkaisut mutta mitä enemmän tarjotaan sovellutuksia Internetiin päin, sitä kattavampi tietoturvaratkaisu on syytä valita

5.2.3 Elektronisen postin tietoturvauhkia

73 % yrityksistä ilmoitti käyttävänsä sähköpostipalvelua. Kun yritykset suurenevat luku näyttää kasvavan. Internet-sähköpostia ilmoittaa käyttävänsä 63 % vastanneista.(liite 2) Sähköpostista näyttää muodostuvan perinteisten informaatioväylien rinnalle uusi kanava. Sähköpostin käytössä on kuitenkin vielä omat riskinsä.

Internet-järjestelmistä tulleen sähköpostiviestin lähettäjätietoihin ei periaatteessa voida luottaa. Epäilyttävissä tapauksissa on tutkittava sanoman reititystietoja ja pyydettävä lähettäjältä asia kirjallisesti. Tilanne korjautuu tältä osin sitten, kun lähettäjän luotettavan tunnistamisen mahdollistavat menetelmät (sähköinen allekirjoitus ja "luotettu kolmas osapuoli" -palvelu) tulevat yleiseen käyttöön.

Sähköpostin tietoturvariskit ovat tai ainakin tulisi olla tiedossa kaikille sähköpostin käyttäjille. Tosin useimmiten suurin riski on tässäkin tapauksessa käyttäjä itse tai hänen työtoverinsa. Sähköpostin turvallisuus ja turvattomuus ovat pitkälti kiinni Internetin turvallisuudesta. Sähköpostin kuljettamiseen Internetissä käytetään SMTP-protokollaa.

Sähköpostiin liittyvät tietoturvaongelmat:

- Viestin lähettäjän luotettava tunnistaminen
- Salakuuntelu ja lukeminen
- Väärään osoitteeseen tai liian laajalle ryhmälle menevät viestit
- Viestin muuttumattomuus

- Viestien väärentäminen
- Sähköposti-hyökkäys

Osoite ja lähettäjä voidaan väärentää, jolloin kuka tahansa voi lähettää viestin nimissäsi. Saadessasi viestin et voi olla varma sen lähettäjästä. Lähes jokainen on lähettänyt vahingossa viestin jonkin toisen sähköpostiosoitteella (postiohjelman konfigurointi unohtunut) - jos sellainen voi tapahtua vahingossa voi sen tehdä myös tarkoituksella.

Internetin luonteesta johtuen lähetetyn viestin reittiä vastaanottajalle on vaikeaa määrätä ennakolta. Koska viesti liikkuu selväkielisenä voidaan se siepata, lukea, muuttaa ja lähettää edelleen vastaanottajalle. Saatuasi postin ei se ole vieläkään turvassa. Käyttäjän omassa postilaatikossa olevat viestit ovat yleensä tekstitiedostossa, joka on luettavissa tavallisella tekstieditorilla. Postipalvelimella voidaan tarvita salasanaa niiden lukemiseen, mutta jos postit siirretään omalle mikrolle ovat ne luettavissa ilman salasanoja. Lähetetystä postista jää yleensä kopio ja vaikka viestit poistetaan ei käyttäjä voi olla varmaa onko posteista olemassa kopiot esimerkiksi organisaation postipalvelimella.

Tietoturvaongelman voi synnyttää väärään osoitteeseen menevä viesti. Se voi johtua käyttäjän huolimattomuudesta, kirjoitusvirheestä tai väärennetystä viestistä, jolloin lähettäjä uskoo viestin menevän toiselle henkilölle. Toinen vieläkin ongelmallisempi tilanne tapahtuu, jos vastaanottajaksi valitaan yhden vastaanottajan sijasta suurempi joukko. Tämä voi tapahtua käytettäessä alias-nimiä, joiden taakse kätkeytyy suuri joukko vastaanottajia. Yleensä tilanne on lähinnä kiusallinen, mutta viestin luonteesta riippuen se voi olla myös vakavampaa.

Yrityksen kannattaa huomioida sähköpostihyökkäyksen mahdollisuus. Siinä yrityksen sähköpostijärjestelmä tukitaan lähettämällä suuri määrää sähköpostia. Tämä voi olla seurausta yritykseen pettyneistä asiakkaista tai tarkoituksellisesta

sabotaasista, jonka suojassa voidaan myös yrittää hakkerointia. Hyökkäystä vastaan voidaan suojautua käyttämällä erillistä postipalvelinta sekä oikein konfiguroitua palomuuria.

Sähköpostin suojaus riippuu lähetettävän postin luonteesta. Jos posti on julkista ei se välttämättä vaadi erityisiä suojauksia. Jos taas postissa lähetetään luottamuksellista tai salaista tietoa täytyy suojaustoimiin ryhtyä. Tulee myös harkita voitaisiinko salainen tieto siirtää jotakin turvallisempaa kanavaa pitkin.

Lähes kaikki edellä mainitut tietoturvaongelmat voidaan ratkaista salakirjoittamalla viestit ja käyttämällä digitaalista allekirjoitusta ja sinetöintiä. Eniten käytetty ja turvallinen salakirjoitusmenetelmä on PGP(ks. liite 3), jota jaetaan ilmaiseksi Internetin välityksellä.

Turvallinen sähköpostiviesti voidaan tehdä PGP:llä seuraavasti:

1. Kirjoita viesti selväkielisenä
2. Allekirjoita viesti PGP:llä
3. Salakirjoita viesti ja allekirjoitus

Jos käyttäjä haluaa lähettää viestejä tai käydä keskusteluja nimettömänä esimerkiksi uutisryhmissä, voi hän käyttää anonyymipalvelimia, jotka korvaavat lähettäjän sähköpostiosoitteen satunnaistunnuksella. Sanoma lähetetään edelleen verkkoon, eikä vastaanottaja voi selvittää lähettäjän henkilöllisyyttä. Anonyymipalvelimet ovat joutuneet vaikeuksiin virkavallan kanssa, koska niiden oikeudellinen asema on epäselvä ja niitä on käytetty myös rikollisiin tai muuten epäilyttäviin tarkoituksiin.

Uutisryhmiä on käytetty virusten levittämiseen. Viruksia on piilotettu uutisryhmien välityksellä levitettävien ohjelmien ja kuvatiedostojen mukana. Uutisryh-

mien käyttöä voidaan valvoa ja estää käyttämästä tietoturvan kannalta epäilyttäviä. Samoin sähköpostiohjelmien liitetiedostojen välityksellä voi levittää viruksia. Esimerkiksi sähköisiä asiakirjoja siirrettäessä voi niiden mukana kulkea ns. makroviruksia. Nämä käyttävät hyväkseen Microsoft Word for Windows - tekstinkäsittelyohjelmiston makrokieltä. Vastaavia makroviruksia on kehitetty myös eräisiin muihin ohjelmistoihin. Näitä ja muita viruksia vastaan suojaudutaan parhaiten asentamalla työasemiin pysyvästi muistissa oleva virustentorjuntaohjelmisto, joka tarkkailee tilannetta koko ajan.

Sähköpostin varajärjestelmänä voidaan käyttää kiireellisissä tapauksissa telekopiota ja muuten normaalia postia. On kuitenkin huolehdittava, että varajärjestelmästä ei muodostu säännöllistä varmistustapaa, jolloin sähköpostin tehokkuusetu menetetään. Sähköpostilla vastaanotetun asiakirjan oikeellisuus ja aitous todennetaan tarvittaessa pyytämällä lähettäjältä oikeaksi todistettu jäljennös alkuperäisestä asiakirjasta.

Kaikesta pelottelusta huolimatta sähköposti ei ole sen turvattomampi kuin perinteisin keinoin lähetty kirje. Samat ongelmat liittyvät kirje- ja faksi - lähetyksiin.

5.2.4 Internetin muodostamia tietoturvauhkia

Yrityskyselyn perusteella yrityksistä 53 prosentilla on kiinteät Internet - yhteydet. Näistä 2/3 suojasi Internet-liikennettä palomuurin (ks. 6.3) avulla.

Käsiteltäessä Internetin tietoturvallisuutta riskit hajaantuvat useampaan kohtaan. Yhteydessä tulee huomioida verkon tietokonejärjestelmien, verkon solmujen, verkon hallintamekanismien sekä tietoliikenneprotokollien suojaus. Yk-

sittäinen liittymä ei voi vaikuttaa koko verkon turvallisuuteen, vaan sen tulee keskittyä oman järjestelmänsä ja sen liitännän turvallisuuteen.

Internet lähti alunperin avoimuuden pohjalta, joten turvakysymyksiä ei ole ajateltu alusta alkaen, joten esimerkiksi Unix-systeemissä riittävän turvan saavuttaminen voi vaatia melkoista konfigurointia. Käyttäjämäärän nopea kasvu ja monien uusien liittymien heikkotasoinen turva vaikuttavat myös osaltaan koko verkon turvallisuuteen. Maailmanlaajuisuus vaikeuttaa salausmenetelmiä, sillä tietyissä maissa, kuten esimerkiksi Ranskassa ja USA:ssa salausmenetelmien käyttöoikeuksia on rajoitettu.

TCP/IP-protokollaperheessä on useita turvallisuusheikkouksia, joita ovat otollisia hyökkäyskohteita. näistä yleisimpiä ovat:

- *Verkon salakuuntelu*, joka onnistuu helposti, mikäli saadaan fyysinen yhteys siirtomediaan. Päästyään käsiksi kaapeliin liitettyyn koneeseen murtautuja voi kuunnella liikennettä vaikkapa diagnostiikkaohjelmaa käyttäen ja poimia liikenteestä käyttäjien salasanoja.
- *IP-osoitteiden väärennys* tapahtuu lähettämällä UDP paketteja joiden IP-osoite on väärä. Tällöin vastaanottajan paluupaketit eivät tietenkään tule perille. Tätä voidaan käyttää mm. hyökkäyksessä Nfs:ää vastaan sekä IP-osoitteeseen perustuvan tunnistuksen kiertoon.
- *ICMP-hyökkäyksessä* tunkeutuja uskottelee olevansa reititin käyttäen ICMP:tä. Hyökkääjä uskottelee laitteelle lyhyimmän tien tiettyyn osoitteeseen kulkevan itsensä kautta ja saa näin siepattua lähtevät paketit. Mikäli hyökkääjällä on myös väärennetty IP-osoite saa tämä haltuunsa myös paluupaketit.
- *ARP-kysely* soveltuu myös tietoturvahyökkäyksiin. ARP , "Addres Resolution Protocol" -protokollalla voidaan selvittää samassa verkossa olevan laitteen Ethernet -osoite. ARP-kyselypaketissa kysytään mikä on tiettyä IP -osoitetta vastaava Ethernet-osoite. Normaalisti IP-osoitteen omakseen tun-

nistava laite vastaa Ethernet-osoitteellaan, mutta mikäli hyökkääjällä on laite samassa verkossa voi tämä vastata ennen oikeaa konetta ja uskotella olevansa tämä.

- *IP-lähdereititystä* voidaan käyttää reitityksen muuttamiseen. Sitä on tarkoitus käyttää reititystaulujen mennessä sekaisin. Lähdereitityksen avulla murtautuja voi laittaa oman IP-osoitteensa tilalle reitin, jossa hänen osoitteensa on. Vastaanottaja näkee lähettäjänä reitin viimeisen osoitteen, vaikka käytännössä paketit pysähtyvät jo murtautujan osoitteen kohdalla.
- *Käänteisnimipalvelun* avulla voi muuttaa oman IP-osoitteensa. Nimipalvelu DNS muuttaa domain nimen vastaavaksi IP-osoitteeksi ja käänteisnimipalvelu tekee vastakkaisen toiminnon. Itse nimipalvelu on varsin varmatoiminen, mutta käänteisnimipalvelua voidaan huijata liittämällä IP-osoitteeseen haluamansa nimi. Useissa palvelimissa tämä on estetty nimikysely avulla, jolloin käänteisnimipalvelussa saatu nimi tarkistetaan suorittamalla sille nimipalvelukysely.

Internet on kehittyvä valtaväylä, sen kehitys on niin nopeaa, että ohjelmistot, joista julkaistaan turvallinen ja testattu versio, ovat jo ilmestyessään vanhan aikaisia. Internetin kaikkia tietoturvaongelmia ei ole toistaiseksi pystytty ratkomaan.

5.3 Tietojärjestelmän ulkoistamisen tietoturvauhkia

Yrityskyselyyn perustuen 69 % yrityksistä tiesi mitä tietojenkäsittelyn ulkoistaminen merkitsee. Rutiininomaisen tietojenkäsittelyn olisi valmis luovuttamaan ulkopuolisille 41 % yrityksistä. Sensijaan vain 12 % yrityksistä olisi valmis luovuttamaan kriittiset tietonsa ulkopuolisen hallittavaksi. 7 % yrityksistä oli ulkoistanut tietojenkäsittelynsä, huomattavaa on, että tutkituista aineistosta ei ai-

nutkaan alle 25 milj. markan liikevaihdon omaava yritys ollut ulkoistanut tietojenkäsittelyään. (ks. Liite 2)

Yrityksessä on hyvä tiedostaa tietojenkäsittelyn hajauttamiseen liittyviä uhkia, joihin on syytä varautua myös tietojärjestelmiä ulkoistettaessa ja joihin voidaan puuttua esimerkiksi tietoturvavaatimusten avulla. Uhkia ovat mm. naamioituminen, järjestelmän resurssien luvaton käyttö, tiedon luovuttaminen ulkopuolisille, järjestelmän ja tietojen muuttaminen, tehtyjen toimenpiteiden aitouden kiistäminen ja palvelun kieltäminen siihen oikeutetuilta käyttäjiltä. (Varadharajan 1995)

Tietojärjestelmän ulkoistamisessa tietojen turvaaminen on ongelma, koska organisaatio menettää käytännössä tietojärjestelmän suoran hallinnan ja siksi organisaatio ei voi suoraan jatkuvasti vaikuttaa tietojärjestelmän toiminnan turvallisuuteen (Wong 1993). Tietojärjestelmän tietoturvasta huolehtii pääosin tietojärjestelmän ulkoinen hoitaja. Vastaantulleissa ulkoistamissopimuksissa esim. Fazerin (Tietoviikko 1996) ja viimeisimpänä Tamron (Aamulehti 1997) tapauksissa ko. yritysten tietotekniikasta vastaava henkilöstö on siirtynyt työntekijöiksi ulkoistamispalvelun tarjoavaan yhtiöön. Näin voi olettaa käyvän myös pienempien yritysten ulkoistaessa laajasti tietojenkäsittelyään.

Tietoturvan hyväksyttävän tason on selvittävä tietojärjestelmän ulkoistamissopimuksesta. Tietojärjestelmän ulkoistamissopimuksessa on määriteltävä yksiselitteiset vaatimukset tietojärjestelmän tietoturvalle (Wong 1993). Tietojärjestelmän ulkoistamissopimuksen vaatimusten pohjalta tietojärjestelmän ulkoistajaorganisaatio pystyy valvomaan tietoturvan nykytasoa. Tietojärjestelmän ulkoistamissopimuksen vaatimusten puitteissa tapahtuvat sopimusrikkomukset tai laiminlyönnit velvoittavat tietojärjestelmän ulkoisen hoitajan korjaamaan puutteet. Tietojärjestelmän ulkoistajaorganisaatio on myös oikeutettu esittämään rahallisia korvauksia aiheutuneista vahingoista.

Tietojärjestelmän ulkoistamisessa on uhkana arkaluonteisten tietojen vuotaminen tietojärjestelmän ulkoisen hoitajan tietojärjestelmästä. Tietojärjestelmän ulkoinen hoitaja joutuu välittämään raportteja tietojärjestelmän tilasta ja muista tietoturvaan liittyvistä asioista. Välitetyt raportit voivat joutua ulkopuolisen käsiin. Tietojärjestelmän ulkoinen hoitaja tai ulkopuolinen raportin sieppaaja voi lähettää myös väärennettyjä raportteja tietojärjestelmän nykytilasta. Tietojärjestelmän ulkoisen hoitajan ja tietojärjestelmän ulkoistajan ristiriitaiset tavoitteet tietojärjestelmän tietoturvasta on koko tietojärjestelmän ulkoistamisprosessia uhkaava tekijä ja siksi tietojärjestelmän ulkoistamissopimus on solmittava huolella.

Tietojärjestelmän ulkoistamisen aloittaminen ja lopettaminen ovat tietojärjestelmän ulkoistamisessa erityisiä uhkatekijöitä, koska arkaluonteisia tietoja ja laitteita voidaan joutua siirtämään organisaatioiden välillä ja siirrettävät tiedot ja laitteet voivat joutua ulkopuolisen käsiin. Tietojärjestelmän ulkoistamisessa uhkatekijän muodostavat myös puutteelliset tietojärjestelmän ulkoisen hoitajan seuraus, valvonta ja ohjausmenetelmät. Tietoturvauhka on myös arkaluonteisten tietojen hävitys ja tietojärjestelmän käyttöhenkilöstön mahdolliset väärinkäytökset. Tietoturvauhkat kohdistuvat lähinnä tietojärjestelmän ylläpitotoimintaan sekä tietojärjestelmän ulkoistajaan ja ulkoistamissopimukseen liittyviin asioihin ja siksi tietojärjestelmän käyttötoiminnan ja tietojärjestelmän ulkoisen hoitajan valvonta on tärkeää.

Tietojärjestelmän ulkoinen hoitaja ei yleensä tavoittele voittoa samoilla tavoilla kuin tietojärjestelmän ulkoistanut organisaatio (Lacity & Hirschheim 1993) ja tämä muodostaa siksi erään uhkatekijän tietojärjestelmän ulkoistamisessa. Tietojärjestelmän ulkoistamisessa tietoturvauhkana on tietojen myös teollisuusvakoilu. Tietojärjestelmän ulkoista hoitajaa vastaan tapahtuvat kavallukset ja

sabotaasit muodostavat vaikeasti hallittavan tietoturvauhan, jonka aiheuttajana voi olla joko organisaation oma henkilökunta tai jokin ulkopuolinen taho.

Huomattavan tietoturvauhan muodostavat tietojärjestelmän ulkoisen hoitajan vahingoista atk-järjestelmissä johtuva atk-toimintojen keskeytyminen, puutteelliset sopimukset sekä epäpätevä tai tyytymätön henkilökunta. Tietojärjestelmän ulkoisen hoitajan konkurssi sekä tappiot liiketoiminnassa voivat aiheuttaa tietoturvan tason hallitsemattoman alentumisen. Tietojärjestelmän ulkoistamisessa tulee huomata, että riippuvuus tietopalvelujen toimittajasta voi olla hyvin suuri, mikä voi olla vahinkojen sattuessa hyvinkin kohtalokasta tietojärjestelmän ulkoistamisen osapuolille. Tietojärjestelmän käyttäjien luotettava todentaminen sekä käyttäjien toiminnan seuraaminen muodostavat erityisen tietoturvauhan. Esimerkiksi tietojärjestelmän käyttäjien toiminnan seurantaan käytettyä lokitiedostoa voidaan yrittää muuttaa jälkeenpäin.

Tietojärjestelmän ulkoistaminen on tietojenkäsittelypalvelujen hankkimista organisaation ulkopuolelta. Hankittaessa palveluita organisaation ulkopuolelta tulee aina määrittää kriteerit, jotka palvelujen tarjoajan tulee pystyä täyttämään. Organisaatiot määrittelevät palvelujen kriteerien täyttämisen laatuna, joten yrityksessä tulee olla käytössä kirjallinen laatupolitiikka. Tarjotun palvelun laatuun kuuluu osana myös tietojärjestelmän tietoturvan käytännön toteuttaminen ja ylläpito. Tietojärjestelmän ulkoistamisessa tietojärjestelmän ulkoistaneen organisaation pitää voida luottaa tietojärjestelmän ulkoisen hoitajan palvelujen tason säilymiseen halutun minimitason yläpuolella.

Huomioon otettavana tietoturvauhkana on epäselvistä vastuista aiheutuvat puutteet turvallisuudessa ja tästä johtuen ongelmien vaikea havaitseminen vastuuhenkilöiden puuttuessa. Tietoturvauhkana on lisäksi toimittajan hitaus toimituksissa, heikko valvonta ja tästä johtuen huono palvelutaso (Harmanen 1993). Mahdollisesti esiintyvät tietoturvauhkat, -riskit ja -ongelmat tulee tieto-

järjestelmän ulkoistamisen osapuolten selvittää systemaattisella tavalla esimerkiksi riskianalyysien, haastattelujen, tarkistuslistojen tai kyselyiden avulla. Selvinneiden tietoturvauhkien asettamien vaatimusten pohjalta voidaan muodostaa organisaatiossa käytettävät tietoturvaohjeistukset.

Asiakkaan tarpeiden muuttuminen, tietojärjestelmän ylläpidon tehostaminen tai tyytymättömyys toimittajaan ovat asiakkaan syitä ulkoistamisen lopettamiseen. Asiakkaan toiminta voi muuttua esimerkiksi siten, että ulkoistettu tietojärjestelmä tulee tarpeettomaksi, tietojärjestelmän ylläpito ei vaadi ulkopuolista yritystä tai tietojärjestelmän käyttötarve on muuten muuttunut tavalla, joka tekee toimittajan käytön tietojärjestelmän ylläpidossa kannattamattomaksi. Myös toimittajan kykenemättömyys ylläpitää tietojärjestelmää esimerkiksi taloudellisen tilansa heikentymisen vuoksi voi johtaa ulkoistamisen päättämiseen. Toimittajan tarjoama palvelu saattaa pitkän ulkoistamisen jälkeen olla tehottomampaa kuin jonkin toisen toimittajan tai sisäisen yksikön tarjoama palvelu, mikä saa asiakkaan vaihtamaan toimittajaa tai palauttamaan tietojärjestelmän ylläpidon sisäiselle yksikölle (Sharp 1993).

Ulkoistamisen etuja ja haittoja oli pohtinut 38 % yrityksistä, suuremmat yritykset lähes puolet suuremmalla joukolla (27 % << 50 %). Yrityksistä olisi valmis ulkoistamaan tietojenkäsittelynsä 15 %. Yrityksen koon kasvaessa halukkuus näyttäisi suurenevan (12 % << 20 %). Halukkuus tietojärjestelmän tai sen osien ulkoistamiseen näyttää lisääntyvän yritysten kokeman ammattitaitoisen atk-henkilökunnan vajeen kasvaessa.(ks. kuvio 8, s. 33). Tietoturvan arvelee ulkoistamistapauksessa, tehdyn kyselytutkimuksen mukaan, kuitenkin lisääntyvän vain 15 % yrityksistä, ja tässä suhteessa suuremmat yritykset ovat kielteisempiä (9 %). (Liite 2)

5.4 Tietokonerikokset

Tietotekniikka on luonut perinteisille rikoksille uuden tekoympäristön, jossa sitä ei ole otettu huomioon eikä yksiselitteisesti kriminalisoitu. Lainmuutoksia tietokonerikoksiin liittyvään lainsäädäntöön on Suomessa tehty vuosina 1991 ja 1995 ja 1997. Tietokonerikoksen rangaistavuuden rajaksi on asetettu suojauksen murtaminen eli välttämättä ei tarvitse tehdä varsinaista vahinkoa. Tietokonerikoslakien yhdenmukaisuus eri maissa on olennaista, koska rikokset jotka tapahtuvat tietoverkkojen välityksellä eivät pysähdy maan rajoille. Suomen lainsäädäntö vastaa pitkälti Euroopan Neuvoston antamia suosituksia. (EU:n neuvoston suositus yleisistä tietotekniikan turvallisuuden arviointiperusteista 1995)

Vuoden 1991 alussa voimaan tulleen rikoslain kokonaisuudistuksen 1. vaiheessa atk-rikossäännökset koskevat tietoon (data) kohdistuvia rikoksia. Tällaisia rikoksia ovat:

- Luvaton käyttö - etäkäyttö
- Tietoväärennös
- Tietovahingonteko
- Yritysvakoilu
- Virukset
- Tietokonepetos
- Tulosteiden väärennös esim. väärien tietojen syöttämisellä
- Toiselle kuuluvan käyttäjätunnuksen käyttö

Uudistuksen toinen vaihe astui voimaan 1.9.95 ja siinä laajennettiin säännökset koskemaan myös tietoon viestintänä. Säädökset tuntevat mm. seuraavat rikostyypit:

- Yksityisen salassapitorikkomus
- Viestintäsalaisuuden loukkaus
- Sähköpostiin tunkeutuminen
- Tietoliikenteen häirintä
- Tietomurto
- Tietojärjestelmiin tunkeutuminen
- Tunkeutumisen yritys
- Tietojen hankkiminen heijastuvan hajasäteilyn avulla

Tietoverkoissa tapahtuvaan maksuliikenteeseen soveltuvan tallenteen tai ohjelman valmistaminen, maahantuonti, hankkiminen, vastaanottaminen ja hallussapito maksuvälinepetostarkoituksessa on kriminalisoitu 1997.

Uusi lainsäädäntö ei kriminalisoi virusten kirjoittamista eikä niiden jakamista. Ainostaan niiden käyttäminen on rangaistava teko. Oikeusministeri Kari Häkämiehen mukaan oikeusministeriö valmistelee lakia, jossa myös virusten kirjoittaminen tulee rangaistavaksi teoksi. Suomesta tulee viides maa Euroopassa, jossa virusten ohjelmointi on rikollista toimintaa (Belgia, Hollanti, Italia, Sveitsi). Ankarin rangaistus tulisi olemaan 2 vuotta ehdotonta vankeutta. (Suomen säädöskokoelma. 1997.) Turvallisuuteen tuudittautuneiden suomalaisyritysten on hyvä muistaa, että 1985 - 1992 välisenä aikana teollisuusvakoilu oli lisääntynyt Yhdysvalloissa 260 % (Heffernan, Swartwood 1993), joten luvut lienevät samansuuntaisia Suomessakin.

Atk-rikos (computer crime) tarkoittaa rikosta, jonka tekotapa edellyttää tietotekniikan tuntemusta. Atk-rikoksen tunnusmerkkinä on suojauksen murtaminen (Pajala 1995). Atk-rikos voidaan salata tietojärjestelmän ulkoistajaorganisaatiolta, koska tietojärjestelmän ulkoisen hoitajaorganisaation maine saattaa kärsiä atk-rikosten tapahtuessa ja siten tietojärjestelmän ulkoinen hoitaja voi menettää asiakkaita. Suuret atk-rikokset vaikuttavat heikentävästi myös yrityskuvaan,

jolloin ulkopuoliset yrityksen palveluja käyttävät organisaatiot tuntevat myös omia toimintojaan uhattavan. Tietojärjestelmään kohdistuvia atk-rikoksia ei aina huomata, koska tietojärjestelmän käyttäjät eivät tiedä riittävästi tietotekniikasta (Autio 1991).

Tietojärjestelmän ulkoisen hoitajan ammattitaidon tulee riittää kaikkien atk-rikosten havaitsemiseen. Jos peittely-yrityksiä havaitaan, niin tämä johtaa toimenpiteisiin ja pahimmillaan suuriin korvausvaatimuksiin sekä tietojärjestelmän ulkoistamisen purkautumiseen. Atk-rikos voi kohdistua joko tietojärjestelmän ulkoistamiseen tai tietojärjestelmän ulkoisen hoitajan tarjoamiin palveluihin tai molempiin edellä mainittuihin tekijöihin samanaikaisesti. Esimerkiksi väärien tietojen antamisena tietojärjestelmän ulkoistamissopimuksessa tai tietojen vuotamisena ulkoistetusta tietojärjestelmästä. Atk-rikokset kohdistuvat joko organisaation henkilökuntaan tai heidän käyttämiään suojauskeinoja vastaan.

Yrityksen tietoturvaa vaarantaa varkaus, jolloin varastettavalla tavaralla on vaihtoarvoa tai käyttöä rikoksen tekijälle itselleen. Tietovarkaus on ulkoistetussa tietojärjestelmässä vakavasti otettava riskitekijä, koska tiedostot tai asiakirjat sisältävät arvokasta, käyttökelpoista ja edelleen myytävää tietoa. Teollisuusvakoilun riski kasvaa tietojärjestelmän ulkoistamisessa, etenkin jos yrityksessä on kehitteillä uusi tuote, joka tulee olemaan merkittävä.

Sabotaasin uhka voi kasvaa tietojärjestelmän ulkoistamisessa ja tällöin tavoite on aiheuttaa organisaatiolle vahinkoa eikä saavuttaa suoranaista hyötyä vahingoista. Sabotaasin uhka voi kasvaa erityisesti samalla liiketoimialalla kilpailevien organisaatioiden taholta.

Tietojärjestelmän käyttöhenkilöiden kiristämisen uhka voi kasvaa tietojärjestelmän ulkoistamisessa. Silloin ulkopuolinen haluaa hyötyä merkityksellistä tietoa omaavan henkilön hallussa olevien tietojen käyttökelpoisuudesta. Tieto-

järjestelmän ulkoisen hoitajan hallussa on runsaasti tietoteknistä asiantuntemusta sekä rahanarvoista tietoa eri organisaatioista ja siksi tietojärjestelmän ulkoistamisessa tulee kiinnittää huomio erityisesti tietoturvaan.

Suomen lainsäädännön mukaan rikollista on tietojärjestelmän resurssien, ohjelmien tai tietojen väärinkäyttö tai muuttaminen. Ainakin sellainen tietojen käyttötapa tai -tarkoitus, mistä ei ole sovittu tietojärjestelmän ulkoistamissopimuksessa. Myöskin edellä mainittujen resurssien väärinkäytön yritys on rangaistavaa (Pajala 1995).

5.5 Yhteenveto

Yrityksen henkilökunta on tärkeä resurssi yritykselle, mutta valitettavasti myös suurin uhka tietoturvallisuudelle. Erilaiset käyttäjävirheet (tahattomat tai tahalliset) aiheuttavat suurimman osan yrityksen tietojärjestelmästä johtuvista taloudellisista menetyksistä. Yrityksen ulkopuolisten uhkatekijöiden taloudellinen merkityksellisyys verrattuna yrityksen sisäisiin uhkiin on vähäinen, niiden moninaisuudesta huolimatta. Verkkokäytön muodostuminen käytännöksi, etätyöskentelyn lisääntyminen ja Internetin yleistyminen asettavat kuitenkin omat vaatimuksensa tietoturvallisuudelle.

Vaikka taloudellisesti ajateltuna nykyiset menetykset ovatkin pieniä, on ulkopuolisiin uhkiin suhtauduttava riittävällä vakavuudella. Niiden aiheuttamat tuhot voivat äärimmäisen vakavia. Toisaalta näitä uhkia on mahdollisuus pienentää teknisin menetelmin hyvinkin pitkälle, jolloin niistä muodostuvat riskit ovat vähäisiä.

Tietojärjestelmän ulkoistaminen ei poista yrityksen henkilökunnan taitamattomuudesta ja osaamattomuudesta johtuvia tietoturvaongelmia. Sen sijaan ohjel-

mistoturvallisuus sekä laitteistoturvallisuus voivat hyvinkin parantua saataessa käyttöön "ison talon" resurssit ja hyvin suunniteltu infrastruktuuri. Toisaalta ulkoistaminen lisää tiedonkulun tarvetta ulkoistajaorganisaation ja tietojärjestelmän ulkoisen hoitajan välillä, mikä muodostaa luonnollisesti uuden uhkan tietoturvallisuudelle.

Tietokonerikosten yksi tunnusmerkki on tietojärjestelmän suojauksen murtaminen. Tietokonerikokset ovatkin yhä enenevissä määrin ammattilaisten työtä. Esimerkiksi teollisuusvakoilu on lisääntymässä jyrkästi; Yhdysvalloissa 260 % vuosina 1985 - 1993 (ks. Heffernan, Swartwood 1993). Tämä asettaa tietoturvallisuudelle luonnollisesti uusia tasovaatimuksia. Tietojärjestelmän ulkoinen hoitaja ei puolestaan välttämättä halua tuoda julkisuuteen siihen kohdistuneita tietoturvaloukkauksia liiketaloudellisista ja imagosyistä johtuen, mikä pitää huomioida ehkäpä tietoturvauhkanakin.

6 TIETOTURVAN HALLINTA

Tässä tutkimuksessa on jo perehdytty tietoturvan olemukseen sekä ulkoistamiseen tietohallinnan menetelmänä. Lisäksi yrityksille suunnatun kyselyn pohjalta edellisessä luvussa on kyetty määrittämään yrityksen tietoturvallisuutta kohtaavia uhkia. Tässä luvussa on kysymys muodostuvien riskien hallinnasta ja kuvan luomisesta siitä, kuinka yrityksissä voidaan tietoturvaa hallita ja mitkä ovat mahdollisia keinoja sen toteuttamiseen. Luvussa selvitetään myös tietojenkäsittelyn ulkoistamisen vaikutusta tietoturvallisuuden hallintaan.

6.1 Johtaminen ja tietoturva

Yrityskyselyn perusteella vain 49 % yrityksistä oli perehdyttänyt johtonsa tietoturvan hallintaan. Samanaikaisesti vain 48 % yrityksistä ilmoitti johdollansa olevan riittävän kuvan tietoturvariskeistä. Vaikka tietoturvallisuudesta vastaavatkin kaikki organisaation jäsenet, jää johtajille ja esimiehille silti joitakin tehtäviä.

Johtajan on vastattava siitä, että alaisilla on mahdollisuus toimia turvallisesti. Turvallinen työskentely saattaa vaatia tiettyjä menettelytapoja tai resursseja ja näistä huolehtiminen on johtajan asia. Johtajan vaatimukset tehdä työ tietyllä, hänen mieleisellään, tavalla sitoo alaisten kädet hyvin tehokkaasti. Jos johtajan edellyttämä tapa ei ole turvallinen, ei tällaisen yksikön toimintakaan sitä ole.

Resurssikysymykset ovat toinen johtajan tehtävä. Turvallisuuden vaatimista lisäresursseista voidaan olla monta mieltä. Kokonaiskustannuksia turvallinen toiminta ei välttämättä juuri nosta, se saattaa kuitenkin siirtää kuluja tietystä

toiminnosta toiseen. Tulosvastuu merkitsee yhä selvemmin sitä, että kukin yritys on itse vastuussa toiminnastaan ja myös itse vastuussa toimintatavoistaan. Yrityksen on itse osattava järjestää toimintansa niin turvalliseksi kuin se itse haluaa ja osattava haluta oikeita asioita. Vastuun vieminen yksittäisiin käyttäjiin asti on keskeinen tietoturvallisuuden periaate. Jokainen tietoa käsittelevä joutuu tällöin ottamaan kantaa tietoturvallisuusasioihin ja myös toteuttamaan vaaditut toimenpiteet omalta osaltaan. Tätä auttaa, jos koko organisaatiossa on vallalla positiivinen suhtautuminen turvallisuusasioihin. Turvallisuus ei ole mikään yksittäinen ohje tai määräys vaan tapa toimia.

Oma esimerkki ja sitoutuminen turvalliseen työtapaan on täysin välttämätöntä tällaisten asioiden läpi saamiseen organisaatiossa. Aivan kuten laatukysymyksien ja johtamistapaan liittyvien uusien oppienkin kohdalla noudatetaan turvallisuuteenkin liittyviä ohjeita suureksi osaksi esimerkin voimalla. Johtaja, joka itse laiminlyö omia tai yläpuoleltaan tulevia ohjeitaan, nähdään helposti joko pellenä tai kapinallisena eikä kumpikaan tulkinta kannusta muitakaan noudattamaan ohjeita.

Johtajan on annettava tai välitettävä yhteiset turvallisuusperiaatteet. Näiden valmistelu on luonnollisesti asiantuntijan työtä, mutta organisaatiolle ohjeet antaa johtaja, kuten muutkin koko organisaatiota koskevat ohjeet. Tällaisia ohjeita ovat yleisperiaatteet ja tavoitteet sekä tietojen luokittelu- ja käsittelyohjeet. Hierarkkisessa organisaatiossa kukin porras saattaa tarkentaa ylempää tulevia ohjeita paremmin vastaamaan omaa alaa, kuitenkaan tarkentavat ohjeet eivät saa olla ristiriidassa yleisten periaatteiden kanssa.

6.1.1 Riskien hallinta

Tässä tutkimuksessa on sekä kirjallisuuden että yrityskyselyn perusteella kartoitettu yrityksen tietoturvaan kohdistuvia uhkia. Uhkasta voi muodostua yritykselle tietoinen riski, jos uhka voi aiheuttaa vahinkoa ja jos uhkaa ei saada kokonaan eliminoitua tai sen poistaminen on hyvin kallista tai mahdotonta. Tämä edellyttää kuitenkin uhkien tuntemista ja riskien määrittämistä. Luvussa 2.2 on esitetty esimerkiksi kaksi erilaista riskien arviointimenetelmää. Olennaista on kuitenkin tietoturvariskien keskinäisen suhteellisuuden ymmärtäminen ja varsinkin pk-yrityksen kyseessä ollessa voimavarojen oikea kohdentaminen.

6.1.2 Henkilöstö ja tietoturva

Henkilöstöpolitiikalla, työnsuunnittelulla ja henkisellä työilmapiirillä on suuri vaikutus turvallisuuden toteutumisessa sekä henkilöstön sitoutumisessa organisaation tietoturvapolitiikkaan. Henkilöstöturvallisuuden avainalueita ovat henkilöstön luotettavuuden ja ammattitaidon tarkistaminen, henkilöstön intimiteettisuojan säilymisen varmistaminen, henkilöstön suojaaminen joutumasta tahallisen tai tahattoman hyökkäyksen kohteeksi sekä avainhenkilöriskien estäminen (Liikenneministeriö 1995). Yrityskyselyn perusteella voidaan sanoa, että henkilöstön tietoturvaperehtyneisyys on yleensä ottaen huono. Vain 38 % yrityksistä oli perehdyttänyt henkilökuntansa tietoturvan hallintaan.

Tietoturvaan liittyvät toimet alkavat jo ennen henkilön palkkaamista organisaation palvelukseen. Henkilön taustojen selvittäminen kuluu asiaan ainakin, jos hänellä on tulevassa tehtävässä pääsy tietoturvan kannalta kriittisiin tietoihin tai hän tulee suorittamaan korkeata tietoturvaa vaativia työtehtäviä. Selvitystyö voi ja useimmiten sen pitää olla avointa ja siihen on hyvä pyytää lupa tutkinnan

kohteena olevalta henkilöltä. Näin vältetään mahdollinen vastareaktio, kun henkilö saa selville taustansa tutkimuksen.

Uuden työntekijän valinnan jälkeen häneltä vaaditaan allekirjoitus salassapitolupaukseen, sekä määritellään sanktiot sopimuksen rikkomisesta. Työntekijän työhön perehdyttämisen ja koulutuksen yhteydessä selvitetään organisaation tietoturvapolitiikka ja tietoturvaan liittyvät säännöt ja määräykset.

Työtehtävien koulutus on tärkeää, sillä henkilöstön osaamattomuus ja virheellinen toiminta vaarantaa muuten huolella suunnitellun ja toteutetun tietoturvan. Tietoturvaan liittyvää koulutusta tulee antaa säännöllisesti myös vanhoille työntekijöille.

Toimivalla varahenkilöjärjestelmällä sekä työnkierrolla pystytään välttämään vaikeudet tietoturvan kannalta kriittisten henkilöiden lopettaessa tai ollessa pois työstä. Toimenpiteillä vältetään korvaamattomien henkilöiden syntyminen ja estetään tahalliset väärinkäytökset sekä tahattomat virheelliset toiminnot. Avainhenkilöriskejä voidaan myös vakuuttaa, jolloin pystytään minimoimaan taloudellisia vahinkoja. Avainhenkilöiden palkkauksen tulisi vastata työn vaativuutta ja olla kannustavaa (tulospalkkiot). Kun työ koetaan tärkeäksi ja arvostetuksi, vältetään tyytymättömyydestä johtuva välinpitämättömyys ja tahalliset haitanteot.

Työntekijän työsuhteen loppuessa huolehditaan, että työntekijä noudattaa salassapitovelvollisuutta myös työsuhteen loppumisen jälkeen. Työntekijän tulee palauttaa avaimet, organisaatiolle kuuluvat tiedot (levykkeet, dokumentit). Käyttäjätunnukset ja käyttöoikeudet peruutetaan välittömästi. Avainhenkilön lopettaessa voi olla perusteltua siirtää hänet irtisanomis-/irtisanoutumisajaksi toisiin tehtäviin tai vapauttaa hänet kokonaan työstä. Tyytymättömät ja omasta mielestään väärin perustein erotetut työntekijät ovat suorittaneet monia atk -

rikoksia ja ilkivaltaisia toimenpiteitä. (Computer System Security and Privacy Advisory Board 1992)

Yrityksissä tulisikin kartoittaa ja tiedostaa henkilökunnan aiheuttamat riskit. Organisaation johto voi toteuttaa tämän esimerkiksi tekemällä nelikenttäanalyysin (SWOT, vahvuudet, heikkoudet, mahdollisuudet, uhkat) yrityksen henkilöstöturvallisuudesta.

6.1.3 Tekniset kysymykset

Kaikilla ei voi olla turvalliseen toimintaan vaadittavia tietoja ja taitoja, eikä se ole tarpeellistakaan. Valitettavasti tekninen kehitys on muuttanut työvälineet sellaisiksi, että keskimääräinen työntekijä ei todellisuudessa lainkaan tiedä, miten hänen käyttämänsä laite toimii.

Tietoa käsittelevien järjestelmien suunnittelijoille ja ylläpitäjille tämä asettaa suuren haasteen, koska heidän on pystyttävä saamaan aikaan sellaisia järjestelmiä, joita käyttäjät osaavat käyttää turvallisesti ja toisaalta tehokkaasti. Toisaalta järjestelmien hyväksikäyttäjillä tulee olla tieto siitä, mihin he voivat arkaluontoiset tietonsa laittaa ja mitä järjestelmiä niiden käsittelyyn käyttää.

Tekniikkaa turvallisuuden parantamiseksi on olemassa riittävästi. Sen arviointi ja valinta on syytä jättää tekniikan ammattilaisten murheeksi. Johtajalla on kuitenkin oltava näkemys siitä, millaisia ongelmia tekniikalla on mahdollista ratkaista ja mihin tekniikan antamat mahdollisuudet yltävät.

6.1.4 Ulkopuolinen apu

Ulkopuolisten asiantuntijoiden käyttö turvallisuuskysymyksissä aiheuttaa helposti vaikeuksia. Ulkopuoliset edustavat usein suurempaa asiantuntemusta kuin oma henkilökunta, mutta toisaalta tällä tavoin hankittu asiantuntemus katoaa yleensä konsultin mukana. Koska tietoturvallisuustyö on luonteeltaan pikemminkin jatkuvaa kuin kertaluonteista, osaamisen jääminen taloon tulisi varmistaa. Kuitenkin 47 % yrityksistä ilmoitti, ettei heillä ole määritelty tietoturvasta vastaavaa henkilöä. 37 % tutkituista yrityksistä oli käyttänyt ulkopuolista apua tietoturvan hallitsemiseksi. Luku näyttää suurenevan yrityskoon kasvaessa (29 % << 46 %), mikä onkin luonnollista järjestelmien monimutkaistuessa.

Hyviä kohteita ulkopuolisen asiantuntemuksen käytölle ovat erilaiset selvitys- ja hankintaprojektit. Omien asiantuntijoiden on usein päivittäisiltä tehtäviltään mahdotonta seurata eri alojen kehitystä ja tämänkaltaisissa projekteissa saatu tietämys on yleensä helppo esittää raportin muodossa. Hankinnan onnistuminen on luonnollisesti tärkein tulos hankintaprojektista ja konsultti pystyy vielä siinä vaiheessa olemaan työssä täysipainoisesti tukena.

Yrityksen tietoturvallisuuspolitiikkaa luotaessa ovat ulkopuoliset mallit ja esimerkit erittäin hyödyllisiä. Mallien etsimisessä ja arvioimisessa on täysin mahdollista käyttää myös ulkopuolista asiantuntemusta. Mallin sovittaminen oman yrityksen toimintaan ja loppusilauksen antaminen on kuitenkin syytä tehdä omin voimin, koska tässä vaiheessa tarvitaan ennen kaikkea yrityksen toiminnan tuntemusta. Toisaalta tätä mallia joudutaan jatkossa käyttämään ja soveltamaan jatkuvasti; ei ole mielekästä antaa sen tekemistä henkilölle, joka poistuu paikalta ja vie asiaan liittyvän osaamisen mennessään.

Oma lukunsa ovat erilaiset säännöllisesti hankittavat palvelut, joihin voi luonnollisesti kuulua myös tietoturvallisuus. Tällöin yllämainitut ongelmat eivät tietysti ole akuutteja, koska sama ulkopuolinen taho suunnittelun lisäksi hoitaa asiaa myös käytännössä. Tällöin arvioinnin kohteena on enemmänkin ulkopuolisen tahon luotettavuus.

6.2 Tietoturvan hallinta tietojärjestelmän ulkoistamisessa

Tärkein ja yleisin ulkoistamisen peruste on kustannustehokkuuden parantaminen, joka merkitsee kustannussäästöjen aikaansaamista. Yritykset tavoittelevat yhä enemmän myös toiminnallista tehokkuutta. Uusissa client server -ympäristöissä katkokset ja häiriöt ovat yleisempiä kuin perinteisissä keskuskoneympäristöissä. Ja jokainen katkoshan tuntuu heti tehokkuuden heikkenemisenä. Nykyisenlaisissa kilpailuoloissa yrityksellä ei ole varaa tehon menetyksiin, joten toimintavarmuus nousee ulkoistamisprosessissa keskeiseksi perusteeksi . Kirjavien laitteistojen ja järjestelmien yhteensovittaminen on ongelmallista ja vaikeaa, varsinkin kun kokemukset client server -arkkitehtuurista ovat vielä aika niukkoja. Organisaatioissa vallitsee huomattava epästandardius. Eri standardien yhteensovittaminen ja järjestelmien ja laitteistojen integroiminen on yllättävän kallista ja vaikeaa.

Ulkoistamisessa tietojärjestelmään kohdistuvat tietoturvauhat ja -riskit pitää tunnistaa sekä tietoturvauhkien ja -riskien muuttumista ja vaikutuksia tietojärjestelmään tulee seurata jatkuvasti. Lisäksi on huolehdittava siitä, että tietojärjestelmän ulkoisen hoitajan tarkkailua, seurantaa ja ohjausta varten on olemassa mekanismit ja menettelytavat. Kun yritysten johdosta vain puolet on tehdyn tutkimuksen mukaan(ks. Liite 2) perehtynyt tietoturvan hallintaan, ja tästä joukosta 2/3 ilmoittaa omaavansa riittävän kuvan tietoturva- riskeistä, ei yrityksillä

yleensä, ilman lisäkoulutusta voi katsoa olevan valmiuksia tietojärjestelmän ulkoisen hoitajan seurantaan ja valvomiseen.

Tietojärjestelmän ulkoistamisessa tulee tietojärjestelmän ulkoisen hoitajan täyttää tiettyjä tietoturvan perusvaatimuksia. Tietoturvan perusvaatimukset ovat perusta organisaation tietoturvaohjeistuksille. Organisaatiolla tulee olla ajantasalla oleva tietoturvapolitiikka, organisaation kirjalliset vastuut pitää olla määritelty sekä vastuuhenkilöt on oltava nimetty. Tietojärjestelmän toipumissuunnitelma on oltava muodostettu ja toipumissuunnitelma pitää olla testattu ennen käyttöönottoa sekä tietojärjestelmän ja ulkoisen hoitajan toiminnasta ja tietojärjestelmän tietoturvan tasosta on raportoitava säännöllisesti.(ks. 3.5)

On syytä selvittää, että palvelun tarjoajan tietojärjestelmän laitteille ja -tiloille sekä tietoverkolle on olemassa varalaitteet, -tilat ja -liikennereitit. Ilmoitusmenettely, toiminta ja korvausmenettelyt poikkeustilanteissa on sovittava tietojärjestelmän ulkoistamissopimuksessa, tietojärjestelmän hoitohenkilöstön taustaasiat pitää selvittää ennen työhönottoa sekä kirjalliset henkilökohtaiset vaitiolosopimukset tulee tehdä. Lisäksi on huolehdittava, että henkilöstöä koulutetaan jatkuvasti tietoturvaan ja atk-järjestelmän käyttöasioihin, että tietojärjestelmän hoitohenkilöstöllä on varahenkilöt, ja että henkilöstölle on annettu riittävät tietoturvamenetelmät sekä tietojärjestelmän käyttöoikeuksien myöntämis- ja aktivoimiskäytännöt on selvitetty.

Tietojärjestelmän ulkoisen hoitajan tulee huolehtia, että tietojärjestelmään kytkeytymisiä ja kytkeytymisyrityksiä seurataan päivittäin, tietojärjestelmän salasanat vaihdetaan säännöllisesti ja salasanojen jakelua valvotaan sekä salasanojen hyvyyttä myös testataan. Ulkopuolisten pääsyä tietokonetiloihin valvotaan ja seurataan käyttämällä esimerkiksi avaimia ja kulkukortteja, tietokonelaitteet ovat lukituissa murto-, vesivahinko- ja palosuojatuissa tiloissa. Tietoverkon käyttöä pitää valvoa lokikirjauksella ja tietoverkossa siirrettävä arkaluonteinen

tieto tulee salakirjoittaa kunnollisella salakirjoitusmenetelmällä. Kaikelle tietoaineistolle määritellään yksikäsitteiset käsittely- ja hävittämissäännöt, tietoaineisto turvaluokitellaan sekä tietoaineistolla on vastuuhenkilöt.

Tietojärjestelmän ulkoistamisessa tärkeä tietoturvan hallintamenetelmä on tietojärjestelmän ulkoistamissopimus. Tietojärjestelmän ulkoistamissopimus muodostaa perustan tietojärjestelmän ulkoistamiselle. Tietojärjestelmän ulkoistamissopimuksen pohjalta tietojärjestelmän ulkoistanut organisaatio pystyy valvomaan tietojärjestelmän ulkoista hoitajaa sekä esittämään vaatimuksia tietojärjestelmän ulkoiselle hoitajalle. Tietojärjestelmän ulkoistanut organisaatio pystyy siten hallitsemaan tietojärjestelmän ulkoistamista tietojärjestelmän ulkoistamissopimuksen avulla.

Tietojärjestelmän ulkoistamisessa sopimusasioihin tulee kiinnittää erityishuomiota, mutta tietojärjestelmän ulkoistamissopimuksessa ei tule kuitenkaan esittää kohtuuttomia vaatimuksia, sillä tällöin houkutus petkutukseen kasvaa. Vaatimusten tulee olla riittävät turvaamaan tiedot ja samalla tietojärjestelmän ulkoisen hoitajan mahdollisia täyttää. Tietoturvakoulutuksen tulee olla jatkuvaa organisaatiossa sekä tietojärjestelmän loppukäyttäjien ohjeistuksien tulee olla tietojärjestelmän käyttöhenkilöstön saatavilla. Tietojärjestelmän ulkoistamisen osapuolten tulee noudattaa tietojärjestelmän ulkoistamisen aikana erityisiä tietoturvaohjeistuksia. Tietoturvavaatimukset tulee tarvittaessa asettaa muuttuneiden olosuhteiden vaatimusten mukaisiksi.

Tietojärjestelmän ulkoistamissopimuksen sisällön tulisi olla mahdollisimman selkeä ja yhtenäinen asetettujen vaatimusten osalta. Tietojärjestelmän ulkoistaminen voidaan sopia vaiheittain ja jokaisessa vaiheessa voidaan muodostaa omat sopimukset. Näiden vaiheiden aikana tulisi käsitellä eri tietojen merkitys ulkoistamisen eri osapuolille. Tietojärjestelmien ja ohjelmistojen kehittämisen monivaiheisuus olisi myös hyvä selvittää ennen tietojärjestelmän ulkoistamista.

Tietojärjestelmän ja ohjelmistojen kehittämisessä tarvittavien tietojen yhdenmukaisuus tietojärjestelmän ulkoistamisen eri osapuolille tulisi myös määrittää. (ks. Richmond & Seidman 1993)

Ulkoistamissopimus tulee laatia siten, että siinä määritellään tarkasti tuotettava palvelu ja sille asetetut vaatimukset sekä hinta. Riitatilanteiden varalta sopimuksessa on määriteltävä vakuutukset, vastuut ja korvaukset sekä muut sopimukset, patentit ja tavaramerkit (esim. Wildish 1993).

Koska tietojärjestelmän ulkoistamisessa vaadittavat tietoturvamenetelmät eivät kata kaikkia tietojärjestelmän ulkoistamiseen vaikuttavia tekijöitä, niin tietojärjestelmän ulkoistamissopimus täytyy ottaa uudeksi tietoturvamenetelmäksi. Tietojärjestelmän tietoturvan tehokkaan ja hallitun toteuttamisen kannalta tarvitaan tietojärjestelmän ulkoistamisessa tietoturvaohjeistuksia. Koska tietojärjestelmän ulkoistamisessa tietojärjestelmän ulkoistamisen osapuolten tavoite tietoturvan kannalta tulee olla sama, niin yhtenäisten tietoturvaohjeistuksien tulee olla käytössä tietojärjestelmän ulkoistamisen eri osapuolilla.(ks.2.2 & 3.3)

Tietojärjestelmän ulkoistamissopimusneuvotteluissa on käsiteltävä atk -toiminnan varmistaminen varajärjestelmin ja -laittein sekä atk -keskusten fyysinen turvallisuus. Ulkoistamissopimusneuvotteluissa on käsiteltävä erityisesti se, miten hankitaan luotettavaa henkilöstöä hoitamaan ulkoistettua tietojärjestelmää sekä miten valitaan henkilöstöä, joka kykenee täyttämään asetetut tietoturvavaatimukset. Atk -tietoturvavaatimusten hinnoittelusta ja tietojärjestelmän toiminnan turvallisuuden testaamisesta on sovittava sopimusneuvotteluissa, jotta lisäkustannukset sekä turvallisuuden testauksen puute eivät yllättäisi myöhemmin. (ks. Harmanen 1993)

Henkilöstöturvallisuuden kannalta on sovittava henkilöstön vaihdoista ja henkilöstövaihdosten ilmoittamisesta etukäteen sekä tietojärjestelmän hoitohenki-

löstön vaitiolosopimuksista. Vaitiolosopimukset tulee allekirjoittaa ennen henkilöstön työtehtävien aloittamista. Tietojärjestelmän toiminnan seurannasta ja raportoinnista tulee sopia, jotta myöhemmin ei muodostuisi epäselvyyksiä ja epäluottamusta tietojärjestelmän ulkoistamissuhteessa. Tietoturvatoiminnan tarkistamisesta ja tietojärjestelmän toiminnan jatkuvuuden varmistamisesta tulee sopia, jotta tietojärjestelmän ulkoistamissuhde kestäisi koko sopimuskauden. (Harmanen 1993)

Kunnollisen ulkoistamissopimuksen teossa on otettava huomioon, että tietojärjestelmän ulkoistaminen ei tarkoita kontrollin luovuttamista ulkopuoliselle. Tietojärjestelmän ulkoistajan on huomioitava, että sopimuksen pituus on yleensä 3-5 vuotta ja siksi yrityksen roolin muuttuminen liiketoiminnan uusien suunnitelmien johdosta on otettava huomioon tietojärjestelmän ulkoistamissopimusta muodostettaessa. Tietojärjestelmän ulkoistamissopimuksessa tulee määrittää myös toimenpiteet tietojärjestelmän ulkoisen hoitajan taloudellisten vaikeuksien varalta ja se millä tavoin annetaan atk - laitteiden käyttöasioihin neuvontaa ja muuta koulutusta (mm. Gates 1992).

Kunnollisen tietojärjestelmän ulkoistamissopimuksen tekeminen edellyttää, että tietojärjestelmän ulkoistamisen lisäkustannukset on otettu huomioon. Tietojärjestelmän ulkoiseen hoitajaan tulee pitää jatkuvasti yhteyttä ja tietojärjestelmän ulkoisen hoitajan tulee mahdollistaa säännölliset katselmoinnit, valmennus ja koulutus tietojärjestelmän käyttöhenkilökunnalle. Sopimusneuvotteluissa tulee tarkistaa tietojärjestelmän ulkoisen hoitajan mahdollisuus tarjota haluttuja atk - palveluita ja tukea sekä tietojärjestelmän ulkoisen hoitajan tulee avustaa käytettävän tietojärjestelmän valinnassa. Tietojärjestelmän muutostilanteet tulee tarkistaa ja muutokset tietojärjestelmään tulee katselmoida huolella. Tietojärjestelmän ulkoisen hoitajan tulee tehdä välitön ilmoitus havaituista tietoturvarikkomuksista tietojärjestelmän ulkoistajaorganisaatiolle sekä tietojärjestelmän

ulkoisen hoitajan tietämys tulee kuulua osana tietojärjestelmän ulkoistamissopimusta. (Gates 1992)

Tietoturvan kannalta tietojärjestelmän ulkoistamissopimusneuvotteluissa on huomioitava organisaation tietoturvapolitiikka, sallitut pääsykeinot tietoverkkoon, käyttäjätunnusten ja salasanojen hallinta sekä tietoverkon käyttäjien käyttöoikeudet. Sopimusneuvotteluissa on oltava esillä myös kuvaus kaikista tietojärjestelmän palveluista, jotka ovat käyttäjien saatavilla sekä lista kaikista tietojärjestelmän käyttöön oikeutetuista henkilöistä. Tietojärjestelmän palvelujen saantiajankohdat sekä ulkoistamissopimuksen solmijaosapuolten luotettavuus ulkoistamissopimusta tehtäessä tulee varmistaa sopimusneuvotteluissa. Tietoturvan perusvaatimukset, käytettävät tietoturvamenetelmät sekä vastuut lakiasioissa tulee sopia sopimusneuvotteluissa, jotta vältyttäisiin ristiriidoilta myöhemmin.

Sopimusneuvotteluissa tulee sopia oikeudesta estää käyttäjien toimintaa tietoverkossa sekä vastuista laitteistojen ja ohjelmistojen asentamisesta ja ylläpidosta, jotta vältettäisiin ylimääräisiä ristiriitoja ja kustannuksia myöhemmin. Sopimusneuvotteluissa tulee sopia sopimusvastuuasioista sekä tietojen kopioinnin ja julkituomisen rajoituksista, jotta tahattomia tietovuotoja ei pääsisi syntymään. Sopimusneuvotteluissa tulee sopia tietojen palautusajoista tai tuhoutumisesta sekä takarajoista ulkoistamissopimuksen kestossa, jotta epäselvyydet ja sopimuksen purkautumiseen liittyvät asiat olisivat kunnossa. Sopimusneuvotteluissa tulee sopia tietojärjestelmän käyttöhenkilöstön koulutuksesta, käyttöturvasta, tietojärjestelmän käyttäjien pääsyoikeuksista tietoverkkoon sekä tietoturvauhkien ja -riskien vaikutusten raportoinnista, tutkinnasta ja torjumisesta. (A Code of Practice 1993)

Erityisen huomion kohteena tietojärjestelmän ulkoistamisessa tulee olla vastuukysymykset sekä erilaisten raporttien sisällöistä, raportointitavoista ja -ajoista

tulee sopia asianmukaisesti. Tietojärjestelmän ulkoistamisessa tulee huolehtia ulkoistamissopimuksen kattavuudesta ja joustavuudesta, sillä jälkeenpäin tehtävät muutokset ulkoistamissopimukseen voivat tulla kalliiksi ja ulkoistamisella haetut säästöt voivat muuttua turhiksi lisäkuluiksi. Tietojärjestelmän ulkoistajan tulisi voida käyttää vain vähän resursseja tietojärjestelmän ulkoisen hoitajan valvontaan, koska tietojärjestelmän ulkoistamissuhteen tulee perustua hyvään yhteistyöhön ja luottamukseen. Tietojärjestelmän ulkoistamissopimusneuvotteluissa tulee kiinnittää erityishuomio siihen milloin on aihetta lopettaa tietojärjestelmän ulkoistaminen sekä miten tarpeelliset tiedot palautetaan takaisin tietojärjestelmän ulkoistajaorganisatioon. (ks. 5.3)

6.3 Erillisiä tietoturvaratkaisuja

Tässä luvussa on tarkoitus esitellä lyhyesti käytettävissä olevia tietoturvaa lisääviä toimenpiteitä ja komponentteja, joita tietoturvan hallinnassa voidaan käyttää. Tietoturvan hallinnassa on oleellista tuntea vaihtoehtoisia suojautumismenetelmiä.

6.3.1 Fyysinen suojaus

Fyysinen suojaus on hyvinkin tärkeää, sillä kaikista tietojenkäsittelyn keskeytymisen aiheuttavista häiriöistä, joilla on taloudellista merkitystä katsotaan aiheutuvan yli 10 % infrastruktuurin pettämisestä. (Computer System Security and Privacy Advisory Board 1992)

Fyysinen suojaus täydentää loogisia tietoturvamenetelmiä. Suojauksessa tulee huomioida myös ulkopuoliset kohteet, joista atk:n toiminta on riippuvainen

(sähkö, lämmitys, vesi, puhelin). Fyysinen turvallisuus keskittyy atk - laitteiden ja tilojen suojaamiseen.

Organisaation tilat tulisi luokitella turvavyöhykkeisiin (vrt. dokumenttien turvaluokitus), jolloin kulunvalvonnalla ja kiinteistönvalvonnalla kyetään rajoittamaan sekä ulkopuolisten että oman henkilökunnan liikkumista kriittisissä osissa rakennusta. Tilojen oikealla sijoittelulla voidaan helpottaa ja edistää turvallisuutta. Julkiset tilat tulisi sijoittaa mahdollisimman selkeästi erilleen suojatuista tiloista.

Siirtyminen turvavyöhykkeeltä toiselle tulee tapahtua valvotusti ja se tulisi kirjata ylös. Työntekijällä on pääsy ainoastaan tiloihin, joita hän tarvitsee työtehtävien suorittamisessa. Vierailijoita ja alihankkijoita ei saa päästää liikkumaan organisaation tiloissa ilman isäntää. Tietoturvan kannalta kriittisiin tiloihin ei ulkopuolisia viedä kuin erittäin painavista syistä, eikä koskaan suurina ryhminä. Tilojen maantieteellinen sijoittelu tulisi myös huomioida. Tilojen siivous ja siisteyskin on olennainen osa tietoturvaa. Siivouksen järjestämisessä tulee huomioida tietoturvanäkökohdat.

Rakennuksen ja tilojen suunnittelussa tulisi huomioida tietoturvan vaatimukset:

- Ikkunat - tarve, sijoittelu
- Lattiaviemärit
- Palo - ovet
- Mihin kerrokseen tilat sijoitetaan?
- Mitä toimintaa on viereisissä huoneissa?
- Sähkön ja veden saanti
- Kaapeloinnin toteutus
- Automaattiset hälyttimet ja sammuttimet - palo, vesi, kosteus, pöly, lämpö

Itse atk - tilojen suojaamisen lisäksi tulee suojata myös tietoliikennekaapelointi ja teleliittymät, jotka ovat atk - tilojen ulkopuolella. Arkistojen turvallisuus taataan sopivilla kassakaapeilla (paloturvallisuus, sijoittelu, paino).

6.3.2 Käytännön komponentteja tietoturvan parantamiseksi

PATU - Pankkiaineistojen turvaratkaisu
Yrityksille tarjottava yhtenäinen tietoturvaratkaisu konekieliseen tiedonsiirtoon. PATU on pankkien yhteisesti kehittämän menetelmä yritysten käyttämien pankkiliikenneohjelmien tiedonsiirron suojaamiseen ja varmistamiseen.

PATU tunnistaa siirron osapuolet sekä varmistaa lähetettävän aineiston aitouden. Järjestelmään liittyy kaksi siirtoavainta, jotka toimitetaan asiakkaille postitse kahdessa eri kirjeessä eri päivinä. Siirtoavaimet on syötettävä pankkiyhteysohjelmaan 30 päivän sisällä niiden voimaantulopäivästä.

Siirtoavaimen avulla ohjelmisto salakirjoittaa käyttöavaimen ja turva-avaimen, joiden avulla PATU tunnistaa lähettäjän ja vastaanottajan ja tarkistaa lähetyksen muuttumattomuuden. Menetelmä perustuu ISO-standardien mukaisiin tarkistekenttiin, jotka lasketaan turva-avaimilla. Pankkiaineiston ympärille määritellään turvakehys, jonka ansiosta sisällön muuttaminen tai muuttuminen vastaanottajan huomaamatta on mahdotonta.(Suomen Pankkiyhdistys , Tietotekninen turvallisuusjaosto. 1995.)

Seuraavat tietoturvakomponentit on poimittu Instrumentointi Oy:n ja Setec Oy:n esitemateriaaleista.

Toimikortit

Toimikortit ovat käyttäjän henkilökohtaisesti mukana kuljetettava turvakomponentti. Käyttäjän toimikorttia käytetään mm. seuraaviin tarkoituksiin:

- Käyttäjälle myönnetyt työasemien käynnistysoikeudet talletetaan toimikortille.
- Käyttäjälle myönnetyt salausavaimet tallennetaan toimikortille, näitä salausavaimia käytetään työasemien ja palvelimien levyille talletettavien tietojen salaamiseen.
- Käyttäjien yksilöintitiedot on tallennettu toimikortille: Kortilla on mm. henkilönumero, turvaluokka sekä yksikäsitteinen hakemistonimi.
- Käyttäjän salakirjoitusavain (RSA, DES) ja siihen liittyvät tiedot tallennetaan toimikortille, näiden avulla voidaan toteuttaa mm seuraavaa.
- käyttäjä voi digitaalisesti allekirjoittaa tiedostoja,
- käyttäjä voi turvallisesti kirjautua kohdejärjestelmiin,
- käyttäjä voi turvallisesti salata ja siirtää tiedostoja toisille.
- valinnainen toiminto: toimikortille voidaan tallentaa käyttäjätunnus ja salasana, jotka luetaan kortilta kirjauduttaessa levypalvelimelle.

Näiden tietojen lisäksi toimikortilla on yksikäsitteinen sarjanumero sekä PIN-tunnusluku, joka käyttäjän tulee antaa voidakseen käyttää korttia.

Toimikortin pinnalle voidaan myös tulostaa käyttäjäkohtaisia tietoja. Useimmiten kortin pinnalla on ainoastaan kortin sarjanumero ja mahdollinen palautusosoite. Käyttäjän lisäksi toimikortteja yksilöidään laitteiden ja ohjelmien käyttöön. Esimerkiksi jokaisella turvasillalla voi olla oma toimikortti, joka sisältää turvasillan salausavaimia ym. tietoja. Kaupalliset toimikortit maksavat 100-200 mk/kpl (Instrumentointi oy)

Toimikortin lukijat

Kaupallisesti on saatavilla useita toimikortin lukijoita. Toimikortin lukijoiden keskeiset toiminnot ovat:

- Toimikortin luku- ja kirjoitustoiminnot. Nämä ovat keskeisimmät kaikista toimikortinlukijan toiminnoista.
- Toimikortin ja kortinlukijan välinen tunnistus.
- Erilaisten turvaluokkien salauspalvelut. Tässä toimikortin lukija sisältää erillisen haluttua algoritmia suorittavan salauspiirin.
- Satunnaisluvun generointi: Toimikortin lukijan turvamoduuli sisältää satunnaislukugeneraattorin.
- Työasemien käynnistyksen valvonta (optiona joissain lukijatyypeissä).

Toimikortin lukijoita käytetään myös toimikorttien ja avainhallinnon järjestelmissä. Tällöin kyseiset lukijat sisältävät hallinnollisen turvamoduulin. Toimikortin lukijoita on saatavissa kaikkiin tavallisimpiin liitäntäportteihin, kuten sarjaportteihin, ISA-väylään sekä SCSI-väylään.

Käytönvalvontaohjelmat

Käytönvalvontaohjelmat ovat eri käyttöjärjestelmiin suunniteltuja ohjelmia, jotka sisältävät mm. seuraavat osakokonaisuudet:

- Käyttäjää pyydetään laittamaan toimikortti lukijaan.
- Käyttäjän tulee esittää kortin PIN-tunnus.
- Lukijan turvamoduuli ja toimikortti kättelevät eli tunnistavat toisensa
- Lukija tarkistaa, että kortilla on haluttuun työasemaan käyttöoikeus
- Käynnistystapahtumien loki.

Windows-käyttöliittymän läsnäolon valvonta on tarkoitettu käyttäjän läsnäolon valvontaan Windows-käyttöliittymässä. Ohjelma valvoo, että käyttäjän toimikortti on lukijassa. Mikäli kortti poistetaan lukijasta tai työasemaa ei käytetä

lainkaan asetettuna ajanjaksona (esim. 10 min), ohjelma lukitsee Windows-käyttöliittymän. Tällöin näppäimistö ja hiiri ovat ohjelman hallussa, myös näyttö voidaan pimentää. Lukitus voidaan poistaa asettamalla lukijaan työaseman käyttöön tarkoitettu toimikortti sekä esittämällä tämän kortin PIN-tunnus.

Tiedostojen salausohjelmat

Eri käyttöjärjestelmiin on saatavissa tiedostojen salausohjelmia. Yleensä ne on tarkoitettu:

1. Paikallisten eli ns. levytiedostojen salaukseen. Tässä tapauksessa tiedostot on tallennettu tyypillisesti työaseman paikalliselle kiintolevylle tai jollekin levypalvelimelle. Tiedostojenkäyttö voi olla sallittua yhdelle tai useammalle käyttäjälle. Salaukseen ja salauksen purkuun käytettävät salausavaimet talletetaan toimikortille.
2. Siirtotiedostojen salaukseen. Tässä tapauksessa tiedosto salataan siirron ajaksi siten, että salauksen purun voi suorittaa ainoastaan tiedoston lailliset vastaanottajat. Itse salattu tiedosto voidaan siirtää esim. sähköpostilla, levykkeellä, ftp-ohjelmalla. Tiedoston salausta varten generoidaan ainoastaan siirron suojauksen aikana käytettävä kertakäyttöinen salausavain.

Toimikorttipohjaiset login-ohjelmat unix-koneisiin

Esimerkkinä Windows Secure Login on Windows-ympäristöön toteutettu toimikorttipohjainen login-ohjelma Unix-hosteihin. Varsinainen sisäänkirjoittautuminen ja päätetyöskentely tapahtuu jollakin PC-työasemassa olevalla kaupallisella x-emulaattorilla, jonka kanssa Secure Login kommunikoi Windows-ympäristössä. Secure Loginissa pyritään vahvaan todennukseen. Se perustuu RSA-algoritmin käyttöön.

Unixin käytönvalvontaohjelmat

Unixin käytönvalvontaohjelmat ovat Unix-ympäristöön toteutettuja ohjelmia, jotka toiminnallisesti ovat vastaavien PC-käytönvalvontasovellutusten kaltaisia. Tällä hetkellä niitä on saatavissa mm Sun Solarikseen ja ne sisältävät ainakin seuraavat osakokonaisuudet:

1. Secure Start: Unix-työaseman käynnistyksen valvonta.
Käynnistyksessä Unix-työasemassa suoritetaan seuraava sekvenssi

- Käyttäjää pyydetään laittamaan toimikortti lukijaan.
- Käyttäjän tulee esittää kortin PIN-tunnus, jolloin tarkistetaan, kortinhaltijan laillisuus.
- Lukijan turvamoduuli ja toimikortti kättelevät toisiaan eli tunnistavat toisensa.
- Lukija tarkistaa, että kortilla on ko. Unix-työaseman käyttöoikeus

2. Secure Login: Unixin sisäänkirjautuminen ja käyttöliittymän läsnäolon valvonta

Secure Login on ohjelma, joka sisältää toiminnot Unix-laitteen konsolilla tapahtuvaan toimikorttipohjaiseen sisäänkirjautumiseen sekä käyttäjän läsnäolon valvontaan. Secure Loginin sisäänkirjautuminen toteuttaa vahvan todennuksen, joka perustuu RSA-algoritmin käyttöön. Secure Login korvaa Unix-laitteen oman login-prosessin. Lisäksi Secure Login on tarkoitettu käyttäjän läsnäolon valvontaan Unix-työasemassa. Ohjelma valvoo, että käyttäjän toimikortti on lukijassa. Mikäli kortti poistetaan lukijasta tai työasemaa ei käytetä lainkaan asetetun (esim. 10 min) ajanjakson aikana, ohjelma lukitsee työaseman. Tällöin näppäimistö ja hiiri ovat ohjelman hallussa, sekä tarvittaessa myös näyttö voidaan pimentää. Lukituksen voi purkaa asettamalla lukijan työaseman käyttöön oikeuttavan toimikortin sekä esittämällä tämän kortin PIN-tunnuksen.

Tiedostojen salausohjelmat Unixiin

Unix Crypt on Unix-ympäristöön toteutettu tiedoston salausohjelma. Tällä hetkellä se on saatavissa ainakin Sun Solarikseen. Unix Crypt on tarkoitettu:

1. Paikallisten eli ns. levytiedostojen salaukseen. Tässä tapauksessa tiedostot on tallennettu Unix-työaseman paikalliselle kiintolevylle tai jollekin levypalvelimelle. Tiedostojen käyttö voi olla sallittua yhdelle tai useammalle käyttäjälle. Salaukseen ja salauksen purkuun käytettävät salausavaimet tallennetaan toimikortille.
2. Siirtotiedostojen salaukseen. Tässä tapauksessa tiedosto salataan siirron ajaksi, siten että salauksen purun voi suorittaa vain tiedoston lailliset vastaanottajat. Itse salattu tiedosto voidaan siirtää esim. sähköpostilla, levykkeellä, ftp-ohjelmalla, internetissä jne. Tiedoston salausta varten generoidaan ainoastaan siirron suojauksen aikana käytettävä kertakäyttöinen salasana-avain.

Turvasilta

Turvasilta on tarkoitettu tietoliikenteen salaamiseen. Turvasiltoja voidaan käyttää kaukoverkossa siirrettävän tiedon salaamiseen, jolloin kaukoverkkoon liitetyissä lähiverkoissa on kullakin omat turvasiltansa. Turvasiltaa voidaan käyttää myös paikallisverkon liikenteen salaamiseen, esim. turvasilloilla voidaan suojata erillisiä segmenttejä paikallisverkossa.

Turvasillan salaus on täysin läpinäkyvää verkkoon liitetyille turvasillan takana oleville laitteille ja sovelluksille. Turvasilta voidaan konfiguroida myös siten, että osa liikenteestä päästetään läpi selväkielisenä. Turvasilta tukee TCP/IP-liikenteen salausta. Salausalgoritmina turvasilta käyttää turvasilta 2 algoritmia. Lisäksi turvasilta toteuttaa staattisen reitityksen. Turvasilta on käytännössä PC-laite, joka sisältää turvasiltaohjelmiston. Lisäksi tarvitaan fyysiseen liitäntään tarvittavat verkkokortit sekä toimikorttilukijan.

Firewall -ratkaisut

Firewall, eli suomeksi palomuuri, on suodatin joka yleensä toimii portinvartijana lähiverkon ja Internetin (tai muun WAN:in) välillä. Firewallin tarkoitus on useimmiten toimia suojana ulkopuolisia tunkeutujia vastaan ja se voi myös rajoittaa tai valvoa lähiverkosta ulospäin siirtyvää dataa. Melko usein jälkimmäistä ei katsota kovinkaan suureksi uhkaksi, mutta joissakin yrityksissä se voi olla erittäin tärkeätä.

Firewall ei saa ainoastaan toimia esteenä, vaan sen pitää myös koko ajan valvoa verkkoliikennettä ja tapahtumia. Pahin mahdollinen tapahtuma voisi olla jos joku kaikista suojauksista huolimatta pääsee firewallin läpi ja muuttaa tietoa ilman että siitä jää jälkeäkään. Firewallin tehtävänä on myös rajoittaa turvallisuusriskit yhteen pieneen helposti hallittavaan paikkaan.

Heijastava reititin (screening router) on useimpien firewallien peruskomponentti. Heijastavat reitittimet yleensä estävät verkkoliikenteen verkkojen ja tiettyjen tietokoneiden välillä, IP-portti tasolla. Jotkut firewallit koostuvat pelkästään heijastavasta reitittimestä.

Linnoituspalvelin (bastion host) on keskipiste tietoverkon turvallisuudessa ja sillä on yleensä varsin kehittyneitä valvonta- ja seurantaohjelmistoja. Ohjelmistot ovat yleensä hieman muokattuja, eli luodaan hieman lisäturvallisuutta "security through obscurity"-periaatteella.

Yhteenvetona edellisiin: On ennustettu että mikään yritys ei pärjää enää vuoden 2001 jälkeen ilman OVT:tä ja sähköisiä palveluita. Näin ollen, suurin osa yrityksistä joutuu liittymään Internetiin ja/tai muihin tietoverkkoihin turvallisuusriskeistä huolimatta. Tästä syystä jokaisen yrityksen on luotava mahdollisimman hyvä tietoturvasuunnitelma ja -politiikka, jotta se voisi mahdollisimman kitkattomasti vastata uusiin haasteisiin.

WWW:ssä on erittäin paljon etuja ja CGI-lomakkeiden avulla voidaan rakentaa erittäin käyttäjäystävällinen ja kansainvälinen palvelujärjestelmä. Interaktiivisia palveluita voidaan myös yhdistää WWW:n ja toisen järjestelmän kanssa. Voisi esimerkiksi ajatella että teleoperaattorilla on CGI-lomakkeita uusien puhelinpalveluiden tilaamiseksi tai että tilausvideo-operaattoreilla tulee olemaan monipuolisempia palvelulomakkeita WWW:ssä.

PGP (ks. liite 3) tarjoaa jo tällä hetkellä erittäin monipuolista tietoturvaa ja tulevaisuudessa on ehkä myös mahdollista lisätä henkilökohtaisia turvallisuusmenetelmiä muihin telepalveluihin, esimerkiksi koodata GSM-puheluita henkilökohtaisilla PGP-koodeilla, jolloin eivät edes teleoperaattorit tai viranomaiset voisi salakuunnella puheluita. Toinen vastapuoli ei voisi myöskään väittää olevansa joku muu.

6.4 Yhteenveto

Yrityksen tietoturvaan kohdistuu useanlaisia uhkia. Suurimmat niistä tulevat yrityksen sisältä (ks. 4.1). Yrityksen keinona hallita tietoturvallisuutta on tunnistaa uhat ja määrittää aiheutuvat riskit. Tämän jälkeen voidaan riskejä hallita erikseen toteutettavan tietoturvallisuusohjelman, jossa määritellään tietototurvaohjeistus (ks. 6.1), avulla. Henkilökunnan ja yrityksen johdon perehtyneisyys tietoturvaseikkoihin on myös tärkeää. Yrityksille on tarjolla keinoja ja menetelmiä tietoturvan hallintaan. Kyse lienee usein vain tietämyksen ja tahdon puutteesta, jos tietoturva-asiat jäävät taka-alalle yrityssuunnittelussa.

Ulkoistamisprosessissa yrityksen sisäistä toimintoa siirretään ulkopuolisen yrityksen tuotettavaksi, jolloin on mahdollista saavuttaa taloudellisia säästöjä. Ulkoistamalla yritys voi keskittyä paremmin olennaiseen liiketoimintaansa hankkimalla ulkoistettavan toiminnan tietotaidon munalta. Keskeiset tietoturvaan

liittyvät ongelmat ovat ulkopuoliselle yritykselle asetettavat tietoturvavaatimukset sekä ulkoistamissopimuksessa, ulkoistamisprosessissa ja ulkoistamisen päättymisestä huomioitavat tietoturvaseikat.

Ulkoistamisesta aiheutuvia tietoriskejä voidaan pienentää, kun ulkoistamissopimuksessa määritetään yksikäsitteisesti tietoturvaan liittyvät vaatimukset. Ne voidaan esittää tarkkana vaatimuslistana ja vaatimuksien täyttämiselle voidaan tarvittaessa sopia tietty aikaväli. Ulkoistamisprosessiin liittyviä tietoturvaongelmia voidaan hallita valvonnan ja tarkastuksien avulla. Ulkoistamisen päättäminen tulee huomioida jo ulkoistamissopimusta tehtäessä. Tällöin voidaan vaikuttaa tietojärjestelmän takaisinsiirrosta aiheutuviin tietoturvakysymyksiin. Ulkoistamisprosessi on vaikeasti hallittavissa, jos yrityksessä ei ole riittävää tietotaitoa hallita tietoturvaa ja asettaa vaatimustasoa kattavaksi.

7 JOHTOPÄÄTÖKSET

7.1 Yhteenveto

Tietokonelaitteiden, tietoliikenteen ja niihin liittyvän teknologian sekä ohjelmistojen kehittyessä nopeasti, ovat tietoturvan uhkat muuttuneet ja kasvaneet entisestään. Samoin on uhkatekijöiden selvittäminen ja niiden hallinta vaikeutuneet tietojärjestelmien kehittyessä nopeammin kuin niihin liittyvät turvaratkaisut. Tämä näkyy varsinkin pk-yrityksissä, joiden henkilöstömäärä on varsin rajallinen ja sen seurauksena voimavarat ovat heikommat kuin suuryrityksissä.

Laitteistojen ja ohjelmistojen uudet versiot ja päivitykset ja niihin usein liittyvät dokumentoimattomat ominaisuudet sekä suoranaiset virhetoiminnot tekevät tietoturvan toteuttamisen todella vaikeaksi. Uhkatekijät eivät enää ole pelkästään fyysisillä menetelmillä estettävissä, vaan tarvitaan yhä enemmän loogisia suojausmenetelmiä.

Suurimpia uhkia ovat käyttäjien tekemät virheet sekä ohjelmistovirheet. Ohjelmistovirheet aiheutuvat järjestelmien monimutkaisuudesta, tekijöiden osaamattomuudesta sekä huonosta testauksesta. Myös itse teknologian monimutkaisuus aiheuttaa uusia uhkia. Käyttäjästä ja tietojenkäsittelytoiminnasta aiheutuvat uhat johtuvat puutteellisesta koulutuksesta sekä eri järjestelmien yhteensopimattomuudesta.

Jotta uhkiin voidaan varautua, on ne tunnettava. Yrityksen toiminta tulee arvioida järjestelmällisesti ja kaikki uhat on käytävä läpi. Tähän tarkoitukseen on olemassa erityisiä menetelmiä, jotka pyrkivät varmistamaan kaikkien uhkien mukaantulon kartoitukseen. Monissa tapauksissa kuitenkin riittää aivan tavalli-

nen terve järki. Kun uhat tunnetaan, voidaan arvioida myös niiden mahdollisesti aiheuttamat menetykset, taloudelliset tai muut.

Lait, määräykset ja sopimukset rajoittavat kunkin organisaation mahdollisuuksia vapaasti päättää omasta riskitasostaan, mihin se on varautunut ja mihin ei. Niiden antamissa puitteissa organisaation on kuitenkin päätettävä, mihin se varautuu ja miten. Loppujen uhkien kohdalla otetaan harkittu riski.

Kaikkiin uhkiin ei ole järkevää varautua. Joidenkin asioiden kohdalla saattaa olla mahdotonta edes arvioida todennäköisyyksiä ja vahinkojen suuruutta. Erityisesti todennäköisyyden ollessa hyvin pieni on suureenkin uhkaan varautuminen vaikeaa. Vahingot, jotka aiheuttavat suuria kustannuksia ja ovat helppoja torjua, on ilman muuta järkevää torjua. Erittäin harvoin sattuvat vaikeasti torjuttavat uhkat jäävät todennäköisesti torjumatta niiden aiheuttamasta tuhosta riippumatta. Näiden ääripäiden välillä kunkin organisaation on löydettävä oma optimaalinen riskitasonsa, joka vaihtelee luonnollisesti organisaation laadun ja toimialan mukaan. Riskitasoa voidaan arvioida myös matemaattisesti esim. Courtney :n menetelmällä.

Jotta tietoturvallisuus tulisi asianmukaiseen kuntoon, jonkun on vastattava siitä. Harvassa pk-yrityksessä on tarvetta päätoimiselle tietoturvallisuuspäällikölle, tehtävän on kuitenkin kuuluttava jonkun tehtäväkenttään. Jokaisella tiedolla ja järjestelmällä on oltava omistaja. Omistaja on vastuussa tietojen luokittelusta, käyttöperiaatteista sekä laillisuudesta. Tietojen omistajien ja käyttäjien on pystyttävä määrittelemään vaatimuksensa. Organisaatioiden välillä tämä tapahtuu sopimuksin, mutta myös niiden sisällä on kyettävä luokittelemaan tieto. Turvallisuutta vaativan käyttäjän on myös tavalla tai toisella vastattava syntyvistä kustannuksista.

Monissa pk-yrityksissä tietoturvallisuustilanne on huono. Tilanteen asianmukaiseksi saattaminen on vaikeaa ja saattaa maksaa paljon, koska tietoturvallisuudesta on tullut menestyvä liiketoimiala. Omaan henkilökuntaan panostamalla yritys voi tietoturvallisuusnäkökohdasta katsottuna saavuttaa paljon.

Turvallisuusvaatimusten lisääminen järjestelmiin näkyy tietysti myös silloin, kun tällaisia järjestelmiä hankitaan oman talon ulkopuolelta. Nämä näkyvät silloin hankintasuunnitelmissa ja tarjouspyynnöissä vaatimuksina ja lopulta sopimuksissa. Joillakin toimittajilla on taipumusta laiskuuteen tällaisten vaatimusten kohdalla ja halu tarjota mieluummin tavanomaista tavaraa. Toimittajien edessä kannattaa kuitenkin olla tiukkana. Tilaaja määrää, mitä haluaa, eikä toimittaja.

Usein tietoturvallisuustoimissa painotetaan järjestelmien ja ohjelmistojen turvallisuutta sekä suojaudutaan ulkopuolisilta tunkeutujilta unohtaen kokonaan, että taloudellisista vastoinkäymisistä on infrastruktuurin pettämisen lisäksi pääasiassa vastuussa yrityksen oma henkilökunta; näiden osuus voi nousta jopa 90 prosenttiin. Yrityksen johdon ja henkilökunnan tietoisuus tietoturvaa vaarantavista tekijöistä ja niiden hallitseminen riskienhallinnan avulla on ehdoton perusta tietoturvallisuudelle.

Toiminnan luovuttaminen ulkopuolisen asiantuntijaorganisaation hoidettavaksi eli ulkoistaminen koskee yhä useammin myös tietotekniikkaa. Joskus atk:n aamuhämärässä tietojenkäsittely kuului vielä joidenkin yritysten jopa strategisiin kilpailuetuihin. Nyt lähes kaikissa organisaatioissa tarvitaan tietotekniikkaa. Se on ydintoiminnan kannalta välttämätön, mutta se itse ei ole useinkaan ydintoimintaa.

Tässä tutkimuksessa on aiheena ollut tietoturvan hallitseminen sekä erityisesti tietoturvan mahdollinen ulkoistaminen. Tutkimuksessa on käynyt ilmi, että tie-

tojenkäsittelyn ulkoistaminen on monelle yritykselle varsin vieras asia. 3/10 yrityksestä ei edes tiedä mitä tietojenkäsittelyn ulkoistaminen merkitsee.

Jokainen ulkoistamistapaus on oma yksilönsä. Ulkoistamissopimus on lähes aina suuri, paljon suurempi kuin yleensä muut tietotekniikkasopimukset, siksi ulkoistamissopimus tulee kilpailuttaa huolellisesti. Ennen sopimuksen tekoa tulee varautua useitten kuukausien tiiviiseen neuvotteluvaiheeseen. Mitä harkitumpi ja konkreettisempi sopimus, sitä paremmin se myös toimii - ja päinvastoin. Tämän tutkimuksen mukaan ulkoistamissopimuksen hallinta on lähes ainoa tietoturvamenetelmä ulkoistamistapauksessa. Yrityksen tulisikin välttää sellaisen tietotekniikan kokonaisuuden kilpailuttamista, jonka tarjontapuolella ei ole kilpailua. Sitä parempi sopimus, mitä paremmassa kunnossa ovat yrityksen omat asiat. Ulkoistaminen ei saa olla tapa ratkaista oman yrityksen henkilöstön, palvelun ja/tai tekniikan sekavia ongelmia.

Tietotekniikan ulkoistaminen seuraa tietotekniikan kehitystä - tosin aika paljon eri tavalla kuin joskus arveltiin. Vielä 90-luvun alussa ulkoistaminen koski vain suurtietokoneiden käyttötoimintoja sekä niihin liittyviä ohjelmistojen ylläpito- ja kunnossapitotoimintoja. Ulkoistaminen oli ja on niissä tapauksissa suoraviivaista. Nykyiset hajautuneet tietotekniikkaympäristöt muuttuvat yhä monimutkaisemmiksi ja vaikeammin hallittaviksi. Tätä kuvastaa sekin, että tämän tutkimuksen mukaan vain joka kolmannella pk-yrityksellä on tietoturva-asioista perillä oleva johto.

Odotuksien vastainen kehitys merkitsee ulkoistamisen kannalta lähinnä kahta asiaa:

1. Kustannusvertailut yrityksen olemassa olevan tietotekniikkavaihtoehdon ja ulkoistusvaihtoehdon välillä monimutkaistuvat; asiantuntemuksen ja ammattitaidon vaatimukset kasvavat.

2. Yritysten itsensä on yhä vaikeampi pitää omassa piirissään yllä sellaista osaamista, joka takaa, että järjestelmät pysyvät hallinnassa ja että ne myös kehittyvät yrityksen kilpailukyvyn edellyttämällä tavalla ja tahdilla.

Tietotekniikan asiantuntijat ovat jokseenkin yhtä mieltä siitä, että jokaisen talon on räätälöitävä oma ulkoistamisratkaisunsa. Ei ole olemassa yleistä mallia, kaavaa tai perustetta, joiden nojalla ulkoistamispäätökset voidaan tehdä. Yläjohto vastaa siitä, että ratkaisut mitoittuvat yrityksen tarpeiden ja tavoitteiden mukaan.

Joiltakin osin tietotekniikan ulkoistaminen on yhtä luontevaa kuin minkä tahansa perusrutiinien siirtäminen ulkopuolisiin käsiin. Yritykselle on yksinkertaisesti tärkeää, että kone toimii. Esimerkiksi taloushallinnon ja palkanlaskennan rutiinit ovat liukuhihnatoimintaa, jota kannattaa parhaiten tehdä siellä, missä saavutetaan samanaikaisesti volyymietuja, kustannussäästöjä ja toiminnallista varmuutta. Atk-ihmiset usein kavahtavat, kun sanotaan, että näiltä osin tietotekniikan ulkoistaminen on samanlaista kuin siivouksen tai kuljetusten ulkoistaminen. Tämän tutkimuksen mukaan tällaisen, vain rutiininomaisten tietojen käsittelyn on valmis ulkoistamaan 4/10 yrityksestä.

Yrityksen on oltava kustannustehokas. Mitä suuremman osan kokonaiskustannuksista ja liikevaihdosta atk-kustannukset muodostavat, sitä tärkeämpää yritykselle on kustannushyötyjen etsiminen ja aikaansaaminen tietotekniikan alueella. Vanhan ja perinteisen osaamisen vaaliminen pelkän tradition vuoksi ei todellakaan ole yrityksen edun mukaista. Kun yrityksen järjestelmät ja koneet eivät enää kestä ajan paineita, ne on ohjattava "saattohoitoon". Sellaisessa tapauksessa vanha atk-alusrakenne käyttötoimintoineen ja sovellusten ylläpitoineen yleensä ulkoistetaan. Silloin yrityksen omat tietotekniikkahenkilöt pystyvät keskittymään ja panostamaan siihen, miten tietotekniikkaa voidaan kehittää ja hyödyntää yrityksen omassa bisneksessä. Ongelmana on kuitenkin, varsinkin tieto-

turvan kannalta, että useimmissa ulkoistamistapauksissa tietotekniikkahenkilökunta siirtyy palveluntarjoajan palkkalistoille, jolloin tietotekniikan kehittymistä työvälineenä yrityksessä ei ohjatakaan enää tarvelähtöisesti vaan myyjän argumentein.

Omatuotantoisessa tietotekniikassa kustannustehokkuus toteutuu yleensä huonommin kuin palvelusopimussuhteessa. Kun yritys ostaa palveluja ulkoa, toiminta on markkinaehtoista. Sen sijaan sisäinen toiminta on periaatteessa tehottomampaa. Ostajan ja myyjän välinen jännite ja kilpailu toimivat puutteellisesti yrityksen sisällä. Ulkoistamisessa aito kilpailutilanne sekä kahden osapuolen neuvotteluasetelma ja asiakassuhde painavat hintoja alaspäin sekä nostavat laatua ja palvelua ylöspäin. Toisaalta tämä saattaa aiheuttaa myös tiettyjen toimintojen laadun alasajoa; esimerkiksi tietoturvan Tässä tutkimuksessa on todettu myös, että on mahdotonta neuvotella kattava ulkoistamissopimus, jos yrityksessä ei ole tietojenkäsittelyn tietotaitoa. Palvelun tarjoajaa on myös mahdotonta valvoa, jos yritys ei tiedä mitä pitäisi seurata.

Lopuksi voisi vielä kaiken yhdistäen todeta, että jos yrityksen johto ei hallitse henkilökuntaansa tietoturvallisuusriskinä, ovat kaikki muut toimenpiteet marginaalisia, oli kyse sitten tietojenkäsittelyn ulkoistamisesta tai muusta tietoturvallisuustoimenpiteestä. Tämän tutkimuksen mukaan pk-yritykset itsekin pitävät suurimpana tietoturvauhkana henkilökuntaansa, mutta on usein helpompi ostaa valmis tietoturvapaketti kuin kouluttaa henkilökuntaa ja varsinkin yrityksenjohtoa.

7.2 Jatkotutkimuskohteet

Pk-yritysten tietoturvaratkaisuja ei juurikaan ole kirjallisuudessa käsitelty. Tarjottavat mallit ovat varsin raskaita toteutettavaksi pienin ja puutteellisin resurs-

sein. Kuitenkin pienet ja keskisuuret yritykset muodostavat valtaosan yritysrakenteesta. Yksittäisiä tietoturvakomponentteja, kuten virustorjuntaohjelmia, tarjotaan kyllä, mutta kokonaisuuksia ei ole tarjolla. Kokonaisvaltaisen tietoturvaohjelman suunnittelu ja kartoitus avaa lukuisia aiheita jatkotutkimukselle

Tietojärjestelmän ulkoistamisessa jatkotutkimuskohteita löytyy useita. Esimerkiksi teknologian muutosten vaikutukset yrityksen ulkoistetun tietojärjestelmän tietoturvaan. Riskianalyysin, tietoturvamallin tai tietoturvaohjelmien kehittäminen tietojärjestelmän ulkoistamista varten on myös mielenkiintoinen jatkotutkimuskohde.

Lähdeluettelo

Aamulehti 1997. Tamro ulkoistaa tietotekniikkansa IBM:lle Suomessa ja Ruotsissa, AL 30.12.1997 s.16.

A Code of Practice for Information Security Management. Department of Trade and Industry. GBIS. PD 0003, London, England, September 1993.

Airaksinen I., Kajava J. 1994. Lähiverkot turvallisemmiksi. In: Seminaari tietoliikenteen tietoturvallisuudesta.Telecom Finland & International Baseline Security, Helsinki 1994.

Alpar, P. & Saharia, A. N., 1995: Outsourcing Information System Functions: An Organization Economics Perspective. Journal of Organizational Computing, 5(3), 197-217.

Altinkemer, K. & Chaturverdi, A. & Gulati, R. 1994. Information Systems Outsosurcing: Issues and Evidence. International Journal of Information Management, Vol. 14, No. 4, 252-286.

Autio, J. 1991. ATK-ammattilaisen oikeusoppi. Valtion Painatuskeskus, Helsinki.

Caelli, W. 1991. Caelli William, Dennis Longley, and Michael Shain. *Information Security Handbook.* New York, NY: Stockton Press, 1991.

Charney, S. 1993. Letter from Scott Charney, Chief, Computer Crime Unit, U.S. Department of Justice, to Barbara Guttman, NIST. July 29, 1993.

Commonwealth of Virginia, Council on Information Management.1995. Information Technology Resource Management Standard. Information Technology Security COV ITRM Standard 95-1.

Computer System Security and Privacy Advisory Board. 1992. Gaithersburg, MD, 1991 Annual Report, March 1992.

Douglas, D. P., 1993, New Wrinkles in Outsourcing, I/S Analyzer, September 1993, Vol. 31. No. 9, 1-17.

EU:n neuvoston suositus yleisistä tietotekniikan turvallisuuden arviointiperusteista 1995, VM 9/73/95, 7.9.1995.

Gates, J. 1992. Successful Outsourcing Depends on a Successful Contract. Corporate Controller, Faulkner & Gray Inc. May/Jun, 17-19.

Gupta, U. G. & Gupta, A. 1992. Outsourcing the IS function. Information systems management. Vol. 9, Iss. 3, 44-50.

Harmanen, P. 1993. Tietojenkäsittelyn turvallisuus kunnallishallinnossa. Katko, Kunnallishallinnon tietotekniikkaneuvottelukunta, Puolustustaloudellinen suunnittelukunta. Julkaisu. Helsinki. 1993.

Heffernan R. J. & Swartwood D. T.1993. "Trends in Competitive Intelligence," Security Management 37, no. 1 ,January 1993, pp. 70-73.

Heikkinen, S. J. P. & Jurvelin, P. 1996. Tietoturva tietojärjestelmien ulkoistamisen yhteydessä, Oulun Yliopisto tietojenkäsittelyopin laitos, Oulu.

Hetky. 1997. Tietoturvallisuus etätyössä (toim. H. Salminen), Suomen Atk-kustannus Oy. Espoo. Sivut 27 - 55.

Holbrook, P. & Reynolds, J. Site Security Handbook. Site Security Policy Handbook Working Group. RFC 1244, FYI 8, CICnet, ISI, July 1991.

House Committee on Ways and Means, Subcommittee on Social Security, Illegal Disclosure of Social Security Earnings Information by Employees of the Social Security Administration and the Department of Health and Human Services' Office of Inspector General: Hearing, 102nd Cong., 2nd sess., 24 September 1992, Serial 102-131.

IDC 1997, European Software and Services Market Forecast 1996 - 2001. IDC June 1997.

International Organization for Standardization 1994. Guidelines for the Management of IT Security (GMITS): Part 3 Concepts and Models for IT Security. ISO/IEC JTC 1/SC 27 N. 962.

Instrumentointi Oy.1997. SecGo(tm), Tietoturvallisuuden tietopaketti SecGo Tutor, Instrumentointi Oy Erikoisjärjestelmät, Tampere 1997.

Jaakonhuhta, H.1995. Suuri tietotekniikan käsitteistö ja sanasto. Suomen ATK-kustannus Oy 1995.

Kajava, J. 1996. Organisaatioiden tietoturvaohjeistus. Turvapäivät Otaniemessä 13.-14.2.1996 (toim.) Maila Virkkala, Teknillinen Korkeakoulu, Espoo.

Kajava, J. & Leiwo, J. 1995. Information security for workstations Implications for end- users, IFIP TC11 Eleventh International Conference on Information

Security, IFIP/Sec 1995 WG 11.1, Information Security Management The Next Decade. 8 May 1995, Cape Town, South Africa.

Keen, P. G. & Cummings, M. J. 1994. Networks in Action: Business Choices and Telecommunications Decisions. Wadsworth Publishing Company, Belmont, California.

Kephart, Jeffrey O. and White, Steve R. 1993. "Measuring and Modeling Computer Virus Prevalence," Proceedings, 1993 IEEE Computer Society Symposium on Research in Security and Privacy (May 1993): 14.

Ketler, K. & Walström, J. 1993. The Outsourcing Decision. International Journal of Information Management. No 13, Butterworth-Heinemann LTD, 449-459.

Lacity, M. C. & Hirschheim, R. 1993. Information Systems Outsourcing. John Wiley & Sons, Guilford, Surrey. 1993.

Liikenneministeriö, 1995. Valmiusohje 4/95. Tietoturvallisuus televerkoissa. Valtion Painatuskeskus Oy, Helsinki. 1995.

Miettinen, J & Kajava, J. 1991. Tetoturvan hallinta nykyaikaisessa yrityksessä. Oulun Yliopisto, Tietojenkäsittelyopin laitos, B22.

Miettinen, J & Kajava, J. 1994a. Tietojenkäsittelyn varmistaminen yrityksen turvallisuusjärjestelyjen osana. Oulun Yliopisto, Tietojenkäsittelyopin laitos, julkaisusarja B31.

Miettinen, J & Kajava, J. 1994b. Tietoriskien arviointi. Oulun Yliopisto, Tietojenkäsittelyopin laitos, julkaisusarja B31.

Murray,William Hugh. 1995. Security should pay. It should not cost. In: Eloff Jan, von Solms Sebastiaan: Information Security - The Next decade. Proceedings Of the IFIP TC11 eleventh international conference and Information security. IFIP Sec '95, Chapman & Hall, London 1995.

Mäntylä, V. & Kajava, J. 1997. Information security in Systems Management. Univercity of Oulu, Department of information processing science. Working papers series B46. 1997.

NIST, 1996. The National Institute of Standards and Technology. Handbook, chap 4, Errors and Omissions.

Oltman, J. R. 1990. 21st Century Outsourcing. Computerworld, April 16.

Pajala, M. 1995. Tieto ja viestintärikoksista. Luento tietoturvan perusteet-kurssilta. Oulun Yliopisto. 1.12. 1995. Oulu.

Parker, D. B. 1995. A New Framework for Information Security to Avoid Information Anarchy. In Eloff J. H. P. & von Solms S. H. (eds.) Information Security - the Next Decade. London: Chapman & Hall, 155 - 164.

Puolustustaloudellinen suunnittelukunta Valtionvarainministeriön järjestely-osasto 1989. Tietojenkäsittelyn turvaaminen ja valmiussuunnittelu. Valtion painatuskeskus, Helsinki.

Rautiainen, L. 1989. Tietojenkäsittelyn turvaaminen, Oulun yliopisto tietojenkäsittelyopin laitos, Oulu.

Richmond, W. B., Seidman, A. 1993: Software Development Outsourcing Contract: Structure and Business Value. Journal of Management Information Systems, Summer 1993, Vol.10,No.1,57-72.

Saari, J. 1988. Tietoturvallisuuden käsikirja. Otava, Keuruu. ss. 205-212.

Sharp, B. 1993. Is it time to insource your financial apps? Datamation. Vol. 39, Iss. 18, 75-77.

Suomen Pankkiyhdistys , Tietotekninen turvallisuusjaosto. 1995. PATU, Pankkien asiakasyhteyksien tietoturva, Tiedostosiirron suojaaminen. Osat 1,2 ja 3. 15.2.1995.

Suomen säädöskokoelma. 1997. Suomen lakimiesliiton kustannus.1997. Ri 37, 38L.

Sääksjärvi, M. 1991. Outsourcing, Tietohallinnon tehokkuus ja palvelevuus palvelujen ulkoistamisen valossa, Helsingin Kauppakorkeakoulun julkaisuja, D-147, Helsinki.

Tanskanen, K. 1987. Osahankintayhteistyö yritysesimerkkejä, Suomen Metalliteollisuuden Keskusliitto, Tekninen tiedotus 3/87, Helsinki.

Tietoviikko 1996. Responsor vei Fazerin tietotekniikan. Tietoviikko. 12.1.1996. Nro 1. Helsinki, 4.

Valtiohallinnon Tietoturvallisuuspäätös. Valtionvarainministeriö. 6/1992, 26.6.1992, Helsinki.

Varadharajan V. 1995. Distributed Object Systems Security. In Eloff J. H. P. & von Solms S. H. (eds.) Information Security - the Next Decade. London: Chapman & Hall, 305 - 321.

Violino B. and Panettieri J. C. 1993. "Tempting Fate," InformationWeek, October 4, 1993: p. 42.

Voltti, P. 1994. Tietojenkäsittelypalvelujen ulkoistamisen onnistumiseen vaikuttavista tekijöistä ja palvelustrategia mallin käytettävyydestä ulkoistamisessa, Oulun yliopisto tietojenkäsittelyopin laitos, Oulu.

Wildish, N. 1993. Outsourcing IT - Safeguarding Your Legal Interests, Purchasing & Supply Management, December 1993, 30 - 33.

Wong, K. 1993. How to implement an end-to-end Security Framework. Computer Fraud & Security Bulletin, Elsevier Science Publishers Ltd. July, 11-13.

Zimmerman, P.1996. The Pretty Good Privacy Manual Page, 1996.

Yrityksen Tietoturva. Lujanen P. 1991. (toim.). Suomen Atk-Kustannus. Myllykoski.

Yritys-suomi CD 2/97.1997. Helsinki Media Blue Book. Helsinki Media 1997.

LIITE 1

Lyhenteitä ja sanastoa

ARPANET, Advanced Research Projects Agency Computer Network
Yhdysvaltain puolustusministeriön sisäinen pakettivälitysverkko, joka toimi vuodesta 1969 vuoteen 1990 kunnes se poistettiin käytöstä.

ARP ,address resolution protocol
TCP/IP-verkoissa osoitteenselvittämisprotokolla, jolla kytketään verkkoprotokollan verkko-osoite (yleensä IP-osoite) lähiverkon MAC-osoitteeseen (RFC 826). Katso LAN.

ARQ, automatic repeat request
Mikä tahansa käytäntö (protokolla), joka käyttää positiivista ja negatiivista kuittausta tai vastaavaa mekanismia saadakseen aikaan hävinneen tai viallisen sanoman uudelleenlähetyksen.

Atk, automaattinen tietojenkäsittely
Yleisesti tietokoneella tapahtuva tietojen käsittely, kuten esimerkiksi tekstinkäsittely, kirjanpito, laskutus, taulukkolaskenta jne. Atk-lyhenteen tilalla suositellaan käytettäväksi sanaa tietotekniikka.

ATM, asynchronous transfer mode
ITU-T:n (ent. CCITT) standardoima nopea (satoja megabittejä sekunnissa) pakettivälitystekniikka, joka perustuu määrämittaisten (48 tavua dataa + 5 tavun otsake) solujen (pakettien) dynaamiseen varaukseen. ATM-tekniikan avulla voidaan siirtää kaiken tyyppistä liikennettä dataa, kuvaa ja ääntä. ATM soveltuu televerkkoihin, LAN- sekä WAN-verkkoympäristöihin.

CGI, Computer Graphics Interface
Laiteohjaimen ISO:n mukainen standardi, joka pyrkii tukemaan mahdollisimman monia graafisen tietojenkäsittelyn syöttö- ja tulostuslaitteita. CGI määrittelee laitetason liitännän. Liitäntä toteutetaan lähitulevaisuudessa suoraan laitteistoissa.

DES, Data Encryption Standard
Yhdysvalloissa IBM:n kehittämä, vuonna 1977 standardisoitu salakirjoitusmenetelmä, joka muuttaa koodattavan merkkijonon 64 bitin mittaisiksi paloiksi. Paloissa olevia bittejä sekoitetaan ja niistä lasketaan monivaiheisilla kaavoilla uusi bittijono. Menetelmä ei ole Suomessa saatavilla. Menetelmästä on olemassa myös kehittyneempi versio DES II.

EDI, Electronic Data Interchange for Administration
Organisaatioiden välinen tiedonsiirto. EDI:n tavoite on rationalisoida hallinnon elektroninen tiedonsiirto yhtenäisillä suosituksilla.

FTP, file transfer protocol
1. Yleisnimi tiedonsiirtokäytännöille erityisesti unix- ja Internet-verkoissa.
2. Tiedonsiirtokäytäntö, joka käyttää alemman tasoista TCP/IP-käytäntöä tiedostojen siirtämiseen tietokoneelta toiselle (RFC 959). FTP on monikerroksinen järjestelmä, jossa ylempi taso olettaa alemman tietoliikennetason suorittavan tehtävänsä ja toimivan oikein. Alimman tason muodostaa fyysinen siirtotie, jonka tehtävänä on siirtää tieto oikeassa muodossa siirtotietä pitkin.

GSM, Group Special Mobile
Pohjoismaiden ja Hollannin aloitteesta käynnistetty Euroopan telehallintojen yhteistyöelimen CEPT:in erityistyöryhmä, jonka tehtävänä on kehittää yhteinen eurooppalainen digitaaliseen ISDN-siirtotekniikkaan perustuva matkapuhelinjärjestelmä.

HTML, hypertext markup language
WWW-järjestelmässä hypertekstien kuvauskieli, jolla luodaan WWW-sivujen muoto ja sisältö. WWW-sivujen HTML-kieli perustuu SGML:ään. Kieli on yleistynyt erityisesti Internetin käytön myötä.

HTTP, hypertext transfer protocol
WWW-järjestelmässä käytetty dokumenttien siirtokäytäntö. Katso HTML ja URL.

IP-osoite. IP-verkossa verkon osoite, joka esitetään neliosaisena pisteellä erotettuna lukuna, esimerkiksi 126.36.27.1. Jokaisen luvun tulee olla välillä 0,1,..,255. IP-osoite ei saa esiintyä kahta kertaa samassa verkossa.

ICMP. Internet control message protocol, (tl)
Tietoliikenneverkoissa IP:n verkkotason apuprotokolla, jonka tehtävänä on viestittää tietosähkeen lähettäneelle asemalle siirrossa havaituista virheistä ja olla apuna verkkoa testattaessa.

ISA, Industry Standard Architecture
IBM:n julkaistessa PC:nsä vuonna 1981 oli siinä lisäkorttipaikkoja varten oma väylänsä. Tätä väylää on alettu kutsumaan ISA-väyläksi. Toisinaan käytetään nimitystä AT-väylä ja silloin tarkoitetaan ISA-väylän 16 bittistä korttipaikkaa. Väylän nopeus on 5 Mbps.

ISDN, Integrated Services Digital Network, (tl)

ITU-T:n (ent. CCITT) monipalveluverkkoa kuvaava suositus. Digitaalinen monipalveluverkko on tarkoitettu täydentämään jo olemassa olevia telepalveluja. Samassa verkossa on silloin yhdistettynä esimerkiksi telex, kuvapuhelin, radio- ja tv-ohjelmien siirto, datasiirto sekä telemaattisia palveluita kuten telekopio, teletex, videotex jne.

ISO, International Standard Organization
Kansainvälinen vuonna 1947 perustettu standardisointijärjestö. Siihen kuuluu noin 90 maata. ISO:n standardisointityö tapahtuu eri alojen pysyväisissä teknisissä komiteoissa (160 kappaletta), alakomiteoissa (590 kappaletta) ja työryhmissä (1300 kappaletta).

IT, information technology, informaatiotekniikka

ITU-T, ITU Telecommunication Standardization Sector
Kansainvälisen telelaitosten liiton (ITU) telestandardeja käsittelevä jaosto, joka julkaisee telealan erilaisia suosituksia ja joilla käytännössä on lähes standardin asema. Järjestö tunnettiin vuoteen 1993 nimellä CCITT.

LAN, local area network
Tietoliikenteessä paikallisverkko, lähiverkko. Maantieteellisesti rajatun pienehkön alueen sisäistä tietoliikennettä hoitava suuren siirtokapasiteetin omaava verkko, jonka tavallisesti omistaa yksi yritys tai laitos. Verkko koostuu työasemista ja palvelimista.

NFS. Network File System
Tietoliikenteessä lähiverkon tasolla hajautettu tiedostojärjestelmä, joka on kehitetty Sun Microsystemsin kehittämän idean pohjalta. NFS-käytännöllä voidaan tiedostoja käyttää verkon kautta ilman, että se näkyy käyttäjälle. NFS tukeutuu TCP:hen ja UDP:hen ja sen avulla työasemille voidaan tarjota mm. virtuaalilevy- ja kirjoittimenjakopalveluita. NFS on erityisen tunnettu unix- ja Internet-ympäristöissä

OVT, organisaatioiden välinen tiedonsiirto
Käsite, joka Suomessa vastaa EDI:ä. OVT sisältää mallin, jonka mukaan kehitetään OVT:n suosituksia. Ne noudattavat ja täydentävät kansainvälisiä EDI-suosituksia sekä täyttävät samalla kotimaiset tarpeet. Käytännössä tämä tarkoittaa yritysten ja yhteisöjen välistä konekielistä tiedonsiirtoa. Esimerkiksi yritys ja pankki voivat siirtää maksuvälitystietojaan konekielisessä muodossa.

PC, personal computer
Henkilökohtainen tietokone. Käytetään usein myös merkityksessä, joka tarkoittaa Intel 8088-suoritinpohjaista mikrotietokonetta. Nykyisin lyhenteellä tarkoitetaan yleensä PC/MS-DOS -käyttöjärjestelmäpohjaisia mikrotietokoneita.

PIN, personal identification number
Henkilökohtainen tunnistenumero. Käytetään esimerkiksi pankkikorteissa, kulunvalvontajärjestelmissä, puheposteissa ja useissa tietopankeissa.

RSA, Rivesti-Shamir-Aldeman
Rivestin, Shamirin ja Aldemanin kehittämä julkisen avaimen salakirjoitusmenetelmä. Menetelmä on julkaistu Yhdysvalloissa 1970-luvun lopulla.

SCSI, Small Computer System Interface
Mikrotietokoneissa käytetty laiteriippumaton oheislaitteiden liitäntästandardi (ANSI X3.131-1986) ulkoista kiintolevyasemaa, nauhuria tai optista levyasemaa varten. Se on kehitetty Shugart Associatesin 1970- ja 1980-lukujen vaihteessa valmistetusta SASI (Shugart Associates System Interface)-standardista. SCSI on rinnakkaisväylä, johon voi olla liitettynä 8 laitetta eli mikrotietokone ja 7 oheislaitetta. Tiedon siirtonopeus on noin 4 - 5 MBps eli 32 Mbps (SCSI 2:ssa 16 - 20 Mbps). Standardi määrittelee ainoastaan levyohjaimen ja levyn välisen jonotuksen sekä ohjauksen. SCSI:n merkitys on jatkuvasti kasvamassa.

SGML, Standard Generalized Markup Language
ISO 8879:ssä määritelty asiakirjastandardi. Merkintätapa, jolla kuvataan tekstien rakennetta standardiesitysmuotona. SGML:ssä teksteihin mukaan koodataan täsmällisesti tieto esimerkiksi otsikoista, lauseista, sivuista, kappalejaosta ja mahdollisesti tekstin luonteesta. Tuloksena syntyy standardinomainen tiedosto, jossa jokainen oleellinen tekstien rakenteen elementti on merkitty täsmällisesti.

TCP/IP, Transmission Control Protocol/Internet Protocol
Tietoliikenteessä tiedonsiirtokäytäntö, joka on mm. Pentagonin ainoa unix-järjestelmissä käytettävä tiedonsiirtokäytäntö ja kehitettiin alunperin Yhdysvaltain puolustusministeriön (DoD) toimesta ARPANET:in yhteydessä. Sen kehitystyö aloitettiin 1960-luvulla, jota kehitystyötä kesti 1980-luvun alkuun jolloin TCI/IP vakiinnutti asemansa. Yhdysvalloissa TCP/IP:stä käytettiin aikaisemmin nimitystä DoD/IP. TCP/IP on yleisesti käytössä lähiverkoissa.

UDP, user datagram protocol (unreliable datagram protocol), (tl)
TCP/IP-protokolliin liittyvä tietosähkepohjainen protokolla.

URL, uniform resource locator
Internet-verkoissa käytettävän WWW-palvelussa oleva linkki, jonka osoitteen perusteella asiakasohjelma ottaa yhteyttä WWW-palvelimeen. Katso HTML ja HTTP.

WAN, wide area network

Tietoliikenneverkko, jolle on tyypillistä maantieteellinen ulottuvuus paikkakunnalta toiselle tai maan rajojen ulkopuolelle aina maanosien väliseksi verkoksi.

WWW, World Wide Web
CERN-tukimuskeskuksessa englantilaisen Tim Berners-Leen vuonna 1989 kehittämä palvelu, joka tähtää maailmanlaajuiseen multimedia- ja hypertekstitiedon välittämiseen HTTP-protokollan avulla Internet-verkossa. WWW:stä käytetään myös nimeä W3.

(Jaakonhuhta 1995)

Liite 2

Yrityskysely (esitetyt kysymykset ja vastaukset)

- Kysymyslomake
- Vastaukset, kaikki yritykset
- Vastaukset , alle 25 milj. liikevaihto(= pienet)
- Vastaukset, 100 -150 milj. liikevaihto(=suuret)
- Ristikysymykset ja data (levyke)

Aineiston käsittelyssä on käytetty Microsoft Excel taulukkolaskentaohjelmaa, jossa muodossa myös yksityiskohtainen vastausaineisto (=data) levykkeellä esitetään.

KYSYMYKSET	KYLLÄ	EI	EOS
Onko yrityksessänne yli 10 työntekijää?			
Onko yrityksessänne tietoja, joita ette soisi ulkopuolisten saavan(esim. kilpailijan)?			
Säilytetäänkö näitä tietoja sähköisessä muodossa?			
Onko yrityksessänne pohdittu tietoturvakysymyksiä yleisellä tasolla?			
Onko yrityksenne johto perehdytetty tietoturvan hallintaan?			
Onko yrityksenne henkilökunta perehdytetty tietoturvan hallintaan?			
Onko yrityksessänne tietoturvasta ja -järjestelmistä erikseen vastaava henkilö/henkilöitä?			
Onko yrityksessänne ohjeistettu tietoturva? Ts. onko tietojenkäsittely normitettu tietoturvallisuuden kattavaksi?			
Onko yrityksessänne tietoverkko?			
Onko yrityksenne tietoverkko osa laajempaa verkostoa?			
Onko yrityksessänne kiinteät Internetyhteydet?			
Onko yrityksessänne sähköposti käytössä?			
Käytetäänkö yrityksessänne Internetsähköpostia?			
Käytetäänkö yrityksessänne palomuuria suojaamaan Internetliikennettä?			
Käyttääkö yrityksessänne jokainen henkilökohtaista tietokonetta? vai käyttääkö samoja koneita useat henkilöt(=ei)?			
Onko henkilökunnallanne mahdollisuus etäkäyttää yrityksen tietokoneita?			
Onko etäkäyttö varmistettu takaisinsoitolla?			
Oletteko valmiit luovuttamaan yrityksenne kriittiset tiedot ulkopuolisen yhteistyökumppanin hallittavaksi?			
Oletteko valmis luovuttamaan vain rutiiniluontoisen datan käsittelyn yrityksenne ulkopuolelle?			
Tiedättekö mitä merkitsee tietojenkäsittelyn ulkoistaminen?			
Oletteko ulkoistaneet tietojenkäsittelynne?			
Oletteko valmis ulkoistamaan tietojenkäsittelyn?			
Oletteko pohtineet ulkoistamisen etuja ja haittoja?			
Oletteko tietoisia tietojärjestelmän ulkoistamisen pääomaa vapauttavista vaikutuksista?			
Tiedättekö lähipiirissänne yrityksiä, jotka olisivat ulkoistaneet tietojenkäsittelynsä?			
Lisääntyykö tietoturva mielestänne tietohallinnan ulkoistamisessa ?			
Ovatko käyttämänne ohjelmistot mielestänne riittävän vakaita eli käyttöturvallisia?			
Onko järjestelmänne/ohjelmistonne aiheuttanut tiedon katoamisia/vuotamisia?			
Osaako henkilökuntanne käyttää ohjelmistoja niiden ominaisuuksien tasolla?			
Onko yrityksessänne tietojen varmistuskäytäntö?			
Onko yrityksenne tietokoneet suojattu ulkopuolisilta käyttäjiltä(esim. henk.koht. salasanoin)?			
Onko yrityksenne tietokoneiden kriittiset tietokannat kryptattu l. salakirjoitettu?			
Onko ulkopuolisella mahdollisuus tunkeutua mielestänne yrityksenne kriittisiin tietoihin?			
Pidättekö ulkopuolista tunkeutujaa todennäköisempänä riskinä kuin henkilökuntaa mahdollisen tietovuodon aiheuttajana?			
Onko yrityksenne käyttänyt ulkopuolista apua tietoturvan hallitsemiseksi?			
Onko Yrityksen johdolla riittävä kuva tietoturvariskeistä?			
Onko yrityksellä itsellänsä riittävä tietotaito hallita tietoturvaa?			
Onko yrityksenne suunnitellut toimia tietoturvan kehittämiseksi?			
Mielestänne suurin tietoturvariski yhtiössänne?			
Seuraava tietoturvaan liittyvä toimenpide johon ryhdytte yhtiössänne?			

	kysymykset	kyllä %	ei %	eos %
		kaikki vastanneet		
1	Onko yrityksessänne yli 10 työntekijää?	91	9	0
2	Onko yrityksessänne tietoja, joita ette soisi ulkopuolisten saavan(esim.kilpailijan)?	100	0	0
3	Säilytetäänkö näitä tietoja sähköisessä muodossa?	93	6	1
4	Onko yrityksessänne pohdittu tietoturvakysymyksiä yleisellä tasolla?	80	20	0
5	Onko yrityksenne johto perehdytetty tietoturvan hallintaan?	49	47	4
6	Onko yrityksenne henkilökunta perehdytetty tietoturvan hallintaan?	38	56	6
7	Onko yrityksessänne tietoturvasta ja -järjestelmistä erikseen vastaava henkilö/henkilöitä?	53	47	0
8	Onko yrityksessänne ohjeistettu tietoturva? Ts. onko tietojenkäsittely normitettu tietoturvallisuuden kattavak	24	63	12
9	Onko yrityksessänne tietoverkko?	89	11	0
10	Onko yrityksenne tietoverkko osa laajempaa verkostoa?	48	50	2
11	Onko yrityksessänne kiinteät Internetyhteydet?	53	46	1
12	Onko yrityksessänne sähköposti käytössä?	73	27	0
13	Käytetäänkö yrityksessänne Internetsähköpostia?	63	36	1
14	Käytetäänkö yrityksessänne palomuuria suojaamaan Internetliikennettä?	34	58	8
15	Käyttääkö yrityksessänne jokainen henkilökohtaista tietokonetta, vai käyttääkö samoja koneita useat henkilö	68	32	0
16	Onko henkilökunnallanne mahdollisuus etäkäyttää yrityksen tietokoneita?	41	59	0
17	Onko etäkäyttö varmistettu takaisinsoitolla?	15	62	22
18	Oletteko valmiit luovuttamaan yrityksenne kriittiset tiedot ulkopuolisen yhteistyökumppanin hallittavaksi?	12	76	12
19	Oletteko valmis luovuttamaan vain rutiiniluontoisen datan käsittelyn yrityksenne ulkopuolelle?	41	47	12
20	Tiedättekö mitä merkitsee tietojenkäsitelyn ulkoistaminen?	69	23	7
21	Oletteko ulkoistaneet tietojenkäsittelynne?	7	86	7
22	Oletteko valmis ulkoistamaan tietojenkäsittelyn?	15	62	22
23	Oletteko pohtineet ulkoistamisen etuja ja haittoja?	38	51	11
24	Oletteko tietoisia tietojärjestelmän ulkoistamisen pääomaa vapauttavista vaikutuksista?	48	39	13
25	Tiedättekö lähipiirissänne yrityksiä, jotka olisivat ulkoistaneet tietojenkäsittelynsä?	37	51	12
26	Lisääntyykö tietoturva mielestänne tietohallinnan ulkoistamisessa ?	12	52	36
27	Ovatko käyttämänne ohjelmistot mielestänne riittävän vakaita eli käyttöturvallisia?	76	14	10
28	Onko järjestelmänne/ohjelmistonne aiheuttanut tiedon katoamisia/vuotamisia?	16	72	11
29	Osaako henkilökuntanne käyttää ohjelmistoja niiden ominaisuuksien tasolla?	46	41	13
30	Onko yrityksessänne tietojen varmistuskäytäntö?	93	5	2
31	Onko yrityksenne tietokoneet suojattu ulkopuolisilta käyttäjiltä(esim. henk.koht. salasanoin)?	93	6	1
32	Onko yrityksenne tietokoneiden kriittiset tietokannat kryptattu l. salakirjoitettu?	15	64	20
33	Onko ulkopuolisella mahdollisuus tunkeutua mielestänne yrityksenne kriittisiin tietoihin?	22	59	18
34	Pidättekö ulkopuolista tunkeutujaa todennäköisempänä riskinä kuin henkilökuntaa mahdollisen tietovuodon	11	74	14
35	Onko yrityksenne käyttänyt ulkopuolista apua tietoturvan hallitsemiseksi?	37	60	3
36	Onko Yrityksen johdolla riittävä kuva tietoturvariskeistä?	48	31	21
37	Onko yrityksellä itsellänsä riittävä tietotaito hallita tietoturvaa?	52	30	18
38	Onko yrityksenne suunitellut toimia tietoturvan kehittämiseksi?	71	23	5

	kysymykset	kyllä %	ei %	eos %
	pienet			
1	Onko yrityksessänne yli 10 työntekijää?	88	12	0
2	Onko yrityksessänne tietoja, joita ette soisi ulkopuolisten saavan(esim.kilpailijan)?	100	0	0
3	Säilytetäänkö näitä tietoja sähköisessä muodossa?	90	8	2
4	Onko yrityksessänne pohdittu tietoturvakysymyksiä yleisellä tasolla?	69	31	0
5	Onko yrityksenne johto perehdytetty tietoturvan hallintaan?	50	48	2
6	Onko yrityksenne henkilökunta perehdytetty tietoturvan hallintaan?	38	58	4
7	Onko yrityksessänne tietoturvasta ja -järjestelmistä erikseen vastaava henkilö/henkilöitä?	42	58	0
8	Onko yrityksessänne ohjeistettu tietoturva? Ts. onko tietojenkäsittely normitettu tietoturvallisuuden kattavak	21	65	13
9	Onko yrityksessänne tietoverkko?	85	15	0
10	Onko yrityksenne tietoverkko osa laajempaa verkostoa?	40	60	0
11	Onko yrityksessänne kiinteät Internetyhteydet?	44	56	0
12	Onko yrityksessänne sähköposti käytössä?	62	38	0
13	Käytetäänkö yrityksessänne Internetsähköpostia?	56	42	2
14	Käytetäänkö yrityksessänne palomuuria suojaamaan Internetliikennettä?	33	60	8
15	Käyttääkö yrityksessänne jokainen henkilökohtaista tietokonetta, vai käyttääkö samoja koneita useat henkilö	63	37	0
16	Onko henkilökunnallanne mahdollisuus etäkäyttää yrityksen tietokoneita?	27	73	0
17	Onko etäkäyttö varmistettu takaisinsoitolla?	19	62	19
18	Oletteko valmiit luovuttamaan yrityksenne kriittiset tiedot ulkopuolisen yhteistyökumppanin hallittavaksi?	10	85	6
19	Oletteko valmis luovuttamaan vain rutiiniluontoisen datan käsittelyn yrityksenne ulkopuolelle?	38	50	12
20	Tiedättekö mitä merkitsee tietojenkäsitelyn ulkoistaminen?	65	29	6
21	Oletteko ulkoistaneet tietojenkäsittelynne?	0	94	6
22	Oletteko valmis ulkoistamaan tietojenkäsittelyn?	12	69	19
23	Oletteko pohtineet ulkoistamisen etuja ja haittoja?	27	62	12
24	Oletteko tietoisia tietojärjestelmän ulkoistamisen pääomaa vapauttavista vaikutuksista?	44	44	12
25	Tiedättekö lähipiirissänne yrityksiä, jotka olisivat ulkoistaneet tietojenkäsittelynsä?	33	56	12
26	Lisääntyykö tietoturva mielestänne tietohallinnan ulkoistamisessa ?	15	46	38
27	Ovatko käyttämänne ohjelmistot mielestänne riittävän vakaita eli käyttöturvallisia?	79	13	8
28	Onko järjestelmänne/ohjelmistonne aiheuttanut tiedon katoamisia/vuotamisia?	12	75	13
29	Osaako henkilökuntanne käyttää ohjelmistoja niiden ominaisuuksien tasolla?	58	33	10
30	Onko yrityksessänne tietojen varmistuskäytäntö?	90	6	4
31	Onko yrityksenne tietokoneet suojattu ulkopuolisilta käyttäjiltä(esim. henk.koht. salasanoin)?	94	6	0
32	Onko yrityksenne tietokoneiden kriittiset tietokannat kryptattu l. salakirjoitettu?	15	63	21
33	Onko ulkopuolisella mahdollisuus tunkeutua mielestänne yrityksenne kriittisiin tietoihin?	25	62	13
34	Pidättekö ulkopuolista tunkeutujaa todennäköisempänä riskinä kuin henkilökuntaa mahdollisen tietovuodon	10	67	23
35	Onko yrityksenne käyttänyt ulkopuolista apua tietoturvan hallitsemiseksi?	29	67	4
36	Onko Yrityksen johdolla riittävä kuva tietoturvariskeistä?	50	31	19
37	Onko yrityksellä itsellänsä riittävä tietotaito hallita tietoturvaa?	56	25	19
38	Onko yrityksenne suunitellut toimia tietoturvan kehittämiseksi?	63	33	4

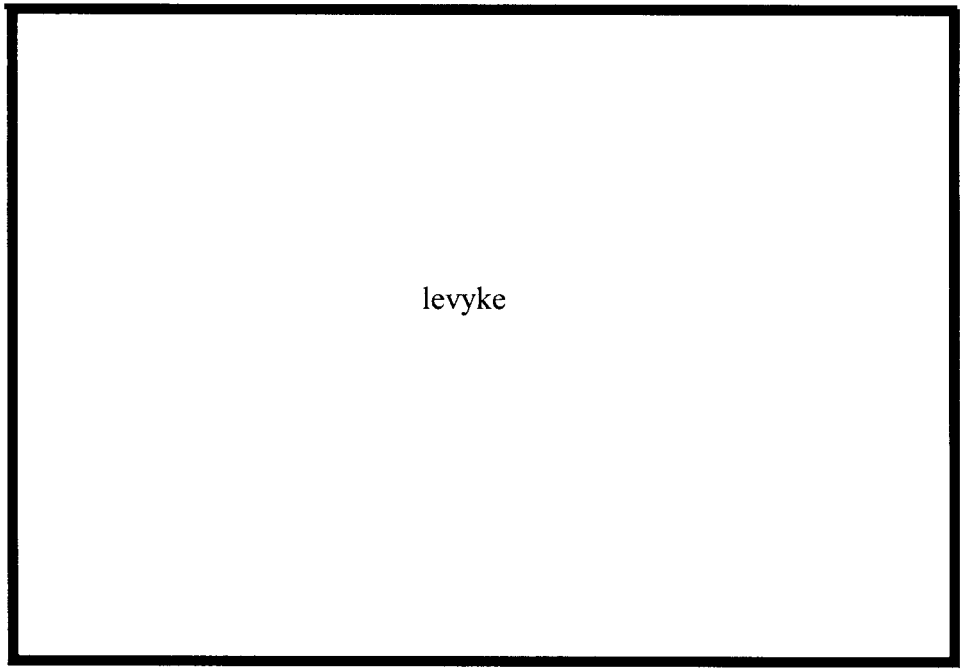
	kysymykset	kyllä % suuret	ei %	eos %
1	Onko yrityksessänne yli 10 työntekijää?	93	7	0
2	Onko yrityksessänne tietoja, joita ette soisi ulkopuolisten saavan(esim.kilpailijan)?	100	0	0
3	Säilytetäänkö näitä tietoja sähköisessä muodossa?	96	4	0
4	Onko yrityksessänne pohdittu tietoturvakysymyksiä yleisellä tasolla?	91	9	0
5	Onko yrityksenne johto perehdytetty tietoturvan hallintaan?	48	46	7
6	Onko yrityksenne henkilökunta perehdytetty tietoturvan hallintaan?	37	54	9
7	Onko yrityksessänne tietoturvasta ja -järjestelmistä erikseen vastaava henkilö/henkilöitä?	65	35	0
8	Onko yrityksessänne ohjeistettu tietoturva? Ts. onko tietojenkäsittely normitettu tietoturvallisuuden kattavak	28	61	11
9	Onko yrityksessänne tietoverkko?	93	7	0
10	Onko yrityksenne tietoverkko osa laajempaa verkostoa?	57	39	4
11	Onko yrityksessänne kiinteät Internetyhteydet?	63	35	2
12	Onko yrityksessänne sähköposti käytössä?	87	13	0
13	Käytetäänkö yrityksessänne Internetsähköpostia?	72	28	0
14	Käytetäänkö yrityksessänne palomuuria suojaamaan Internetliikennettä?	35	57	9
15	Käyttääkö yrityksessänne jokainen henkilökohtaista tietokonetta, vai käyttääkö samoja koneita useat henkilö	74	26	0
16	Onko henkilökunnallanne mahdollisuus etäkäyttää yrityksen tietokoneita?	57	43	0
17	Onko etäkäyttö varmistettu takaisinsoitolla?	11	63	26
18	Oletteko valmiit luovuttamaan yrityksenne kriittiset tiedot ulkopuolisen yhteistyökumppanin hallittavaksi?	15	65	20
19	Oletteko valmis luovuttamaan vain rutiiniluontoisen datan käsittelyn yrityksenne ulkopuolelle?	43	43	13
20	Tiedättekö mitä merkitsee tietojenkäsitelyn ulkoistaminen?	74	17	9
21	Oletteko ulkoistaneet tietojenkäsittelynne?	15	76	9
22	Oletteko valmis ulkoistamaan tietojenkäsittelyn?	20	54	26
23	Oletteko pohtineet ulkoistamisen etuja ja haittoja?	50	39	11
24	Oletteko tietoisia tietojärjestelmän ulkoistamisen pääomaa vapauttavista vaikutuksista?	52	33	15
25	Tiedättekö lähipiirissänne yrityksiä, jotka olisivat ulkoistaneet tietojenkäsittelynsä?	41	46	13
26	Lisääntyykö tietoturva mielestänne tietohallinnan ulkoistamisessa ?	9	59	33
27	Ovatko käyttämänne ohjelmistot mielestänne riittävän vakaita eli käyttöturvallisia?	72	15	13
28	Onko järjestelmänne/ohjelmistonne aiheuttanut tiedon katoamisia/vuotamisia?	22	70	9
29	Osaako henkilökuntanne käyttää ohjelmistoja niiden ominaisuuksien tasolla?	33	50	17
30	Onko yrityksessänne tietojen varmistuskäytäntö?	96	4	0
31	Onko yrityksenne tietokoneet suojattu ulkopuolisilta käyttäjiltä(esim. henk.koht. salasanoin)?	91	7	2
32	Onko yrityksenne tietokoneiden kriittiset tietokannat kryptattu l. salakirjoitettu?	15	65	20
33	Onko ulkopuolisella mahdollisuus tunkeutua mielestänne yrityksenne kriittisiin tietoihin?	20	57	24
34	Pidättekö ulkopuolista tunkeutujaa todennäköisempänä riskinä kuin henkilökuntaa mahdollisen tietovuodon	13	83	4
35	Onko yrityksenne käyttänyt ulkopuolista apua tietoturvan hallitsemiseksi?	46	52	2
36	Onko Yrityksen johdolla riittävä kuva tietoturvariskeistä?	46	30	24
37	Onko yrityksellä itsellänsä riittävä tietotaito hallita tietoturvaa?	48	35	17
38	Onko yrityksenne suunitellut toimia tietoturvan kehittämiseksi?	80	13	7

ALKUPERÄISESTÄ DATA - AINEISTOSTA TEHTYJÄ YHDISTELMÄKYSYMYKSIÄ

Laskettu koko aineistosta.

Numerot viittaavat edellisten sivujen kysymysnumeroihin.

2 = kyllä	3 = kyllä	37 = kyllä	**48%**
5 = kyllä	6 = kyllä	8 = kyllä	**13%**
37 = ei	38 = kyllä		**19%**
35 = kyllä	37 = ei		**9%**
22 = kyllä	37 = ei		**6%**
22 = kyllä	37 = kyllä		**6%**
22 = kyllä	24 = kyllä		**11%**
16 = kyllä	17 = kyllä		**12%**
21 = kyllä	22 = ei		**1%**
35 = ei	37 = ei		**20%**



data

LIITE 3

PGP

Pretty Good Privacy eli PGP on erittäin laajassa käytössä oleva RSA-kryptausmenetelmään ja julkisiin avaimiin perustuva kryptaus- ja integriteetti-varmistusmenetelmä. PGP-ohjelman avulla voit luoda itsellesi salaisia ja julkisia koodiavaimia oman salasanan avulla. Kun kirjoitat esimerkiksi sähköposti-viestejä tai luot uusia WWW-sivuja, voit "allekirjoittaa" näitä PGP-ohjelman avulla. PGP laskee ko. viestiin ja sinun salaiseen avaimeen perustuvan avaimen, joka lisätään, yleensä selväkielisenä, viestin loppuun. Tämän jälkeen vastaan-ottaja voi tarkistaa onko viestin lähettäjä todellakin sinä ja onko se saapunut muuttumattomana.

Huomaa siis että viesti allekirjoitetaan sinun salaisella avaimellasi ja avataan ja tarkistetaan viestin avaimella ja sinun julkisella avaimellasi.

On myös mahdollista kryptata viestejä omalla salaisella avaimella sekä vastaan-ottajan julkisella avaimella, jolloin vain vastaanottaja pystyy lukemaan viestin sinun julkisen avaimen avulla.

PGP on siis erittäin varma ja turvallinen järjestelmä. Sen ainoa heikko kohta on oikeastaan julkisen avaimen saaminen. Eli, mistä voit tietää että henkilö joka ilmoittaa olevansa Bill Gates ja joka lähettää sähköpostilla oman julkisen avaimensa, on todellakin Bill Gates. Ja jos henkilö nimeltään Andreas Holm-berg ilmoittaa että julkisen avaimen löydät komennolla `finger pan-dy@hila.hut.fi' jonka jälkeen kirjoitat tämän komennon; miten tiedät että tämä on juuri se oikea pandy@hila.hut.fi eikä joku toinen kone esim. pirate.sea.edu,

joka hetkellisesti esiintyy peitenimellä hila.jyu.fi. Yksi ratkaisu on esimerkiksi jos henkilö B on antanut julkisen avaimensa sinulle luotettavalla tavalla, esimerkiksi jossain konferenssilla, kun hän todisti henkilöllisyytensä. Jos voit luottaa B:hen ja B on saanut C:n PGP-avaimen luotettavalla tavalla; B voi tietenkin lähettää C:n avaimen sinulle PGP-allekirjoitettuna sähköpostiviestinä. (Zimmerman 1996)