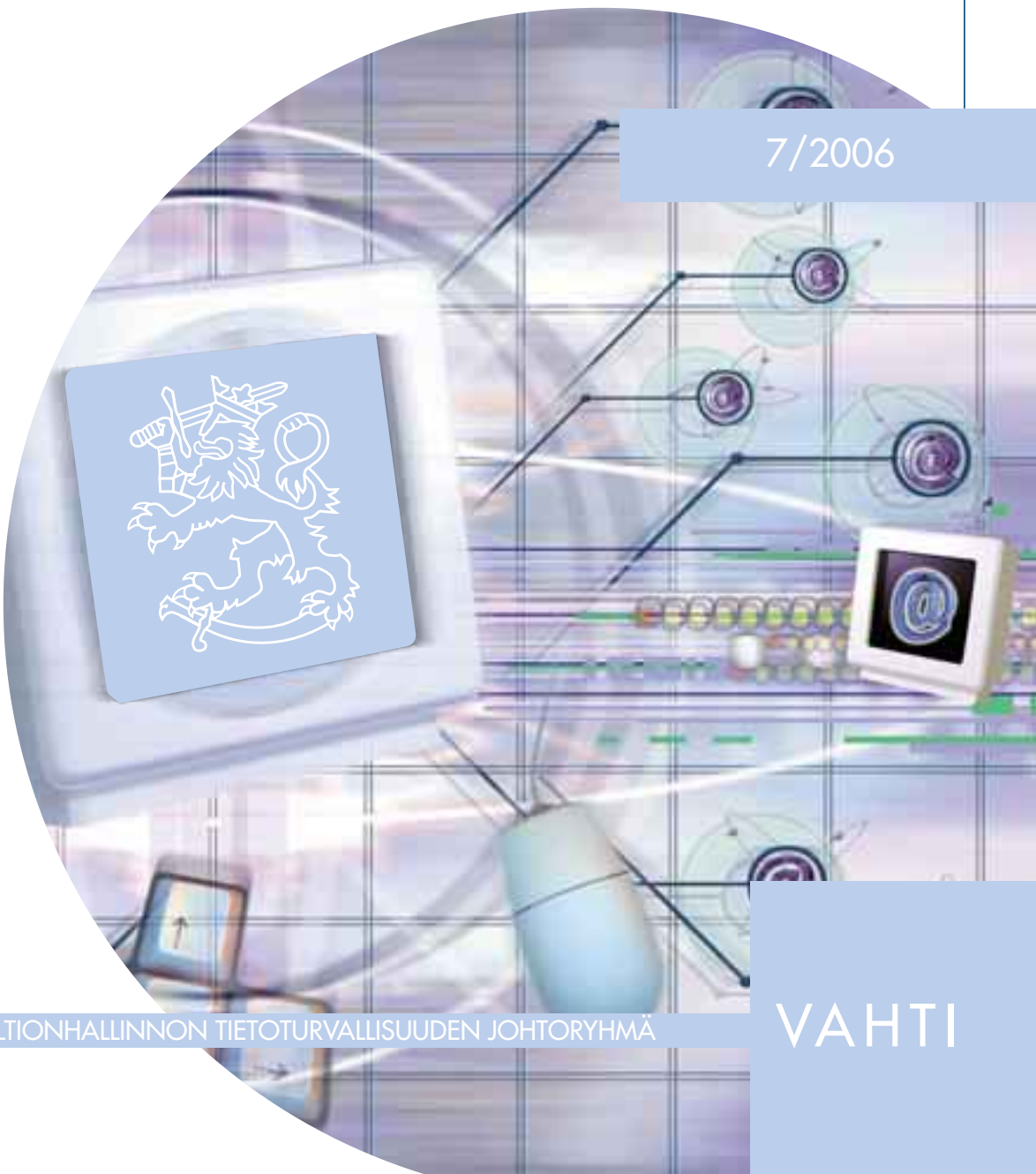
VALTIOVARAINMINISTERIÖ

MUUTOS JA TIETOTURVALLISUUS, ALUEELLISTAMISESTA ULKOISTAMISEEN – HALLITTU PROSESSI



7/2006

VALTIONHALLINNON TIETOTURVALLISUUDEN JOHTORYHMÄ

VAHTI

MUUTOS JA TIETOTURVALLISUUS, ALUEELLISTAMISESTA ULKOISTAMISEEN – HALLITTU PROSESSI

7/2006

VALTIOVARAINMINISTERIÖ
HALLINNON KEHITTÄMISOSASTO

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28
00023 VALTIONEUVOSTO

Puhelin
(09) 160 01

Telefaksi
(09) 160 33235
Internet
www.vm.fi

Julkaisun tilaukset
Puh. (09) 160 33287
ISSN 1455-2566
ISBN 951-804-624-7 (nid.)
ISBN 951-804-625-5-X (pdf)

Edita Prima Oy
HELSINKI 2006

VALTIOVARAINMINISTERIÖ

Hallinnon kehittämisosasto

VM 19/01/2006

OHJE
21.6.2006

Ministeriöille, virastoille ja laitoksille

MUUTOS JA TIETOTURVALLISUUS

Valtiovarainministeriön ohessa antaman tietoturvaohjeen (jäljempänä ohje) tavoitteena on tukea tietoturvallisuuden hallintaa valtionhallinnon erilaisissa muutostilanteissa. Ohje on tarkoitettu ministeriöiden ja virastojen johdolle, talous- ja henkilöstöhallinnon esimiehille ja tietohallinto-, kehitys- ja tietoturvajohdolle sekä riskienhallinnan koordinaattoreille ja kaikille tietoturvallisuuden kehittämiseen osallistuville.

Ohje on laadittu Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI ohjauksessa ja alaisuudessa osana valtionhallinnon tietoturvallisuuden kehitysohjelmaa (VAHTI-julkaisu 1/2004). Ohje korvaa suosituksen ulkoistamisen tietoturvallisuudesta (VAHTI 2/1999).

Valtion organisaatioiden tulee panostaa jatkuvaan ja laaja-alaiseen tietoturvallisuuden kehittämiseen, koska muutoksen lähtötilanteen hyvä tietoturvallisuus luo parhaat edellytykset muutoksen tietoturvalliselle toteutukselle. Tietoturvallisuus tulee ottaa huomioon prosessien kehittämisen alkuvaiheesta asti prosessin koko elinkaaren ajan.

Työtekijöiden ja muiden muutokseen osallistuvien motivointi, mahdollisen muutosvastarinnan käsittely ja hyvä tiedottaminen ehkäisevät tietoturvariskien toteutumista muutoksessa. Muutoksen tietoturvavaikutukset ja –riskit tulee arvioida ennen muutoksen käynnistämistä ja toteuttamista.

Ulkoistus ja sen tietoturvallisuus on suunniteltava erityisellä huolellisuudella. Ulkoistajan on selvitettävä ja arvioitava, mitkä ovat ulkoistettavan toiminnon tietoturvallisuuden erityispiirteet ja otettava ne huomioon ulkoistamistamisen suunnittelussa ja toteuttamisessa.

Asiakirja tulee VAHTIn Internet-sivuille (www.vm.fi/vahti). Ohjetta kehitetään tarvittaessa mm. saatavan palautteen pohjalta. Palautteen voi toimittaa valtiovarainministeriön hallinnon kehittämisosastolle (hko@vm.fi). Lisätietoja antavat tietoturvallisuusasiantuntija Juhani Sillanpää ja neuvotteleva virkamies Mikael Kiviniemi (etunimi.sukunimi@vm.fi)

Toinen valtiovarainministeri — Ulla-Maj Wideroos

Neuvotteleva virkamies — Mikael Kiviniemi
VAHTIn puheenjohtaja

Liite *Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen- hallittu prosessi (VAHTI 7/2006)*

ESIPUHE

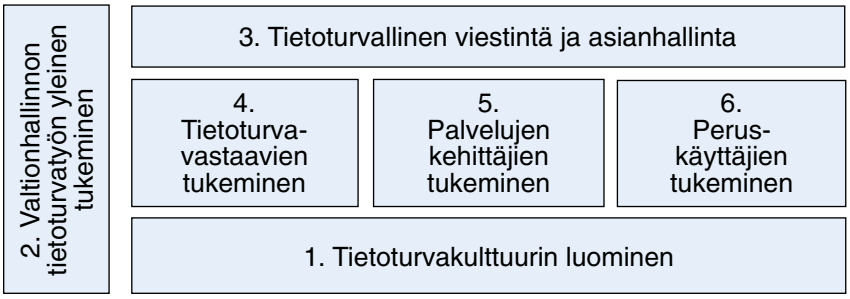
Valtiovarainministeriö (VM) vastaa valtion tietoturvallisuuden ohjauksesta ja kehit-tämisestä. Ministeriö on asettanut Valtionhallinnon tietoturvallisuuden johtoryhmän (VAHTI) hallinnon tietoturvallisuuden yhteistyön, ohjauksen ja kehittämisen elimeksi. VAHTIssa ovat edustettuina eri hallinnonalat ja -tasot.

VAHTIn tavoitteena on tietoturvallisuutta kehittämällä parantaa valtionhallinnon toimintojen luotettavuutta ja jatkuvuutta sekä edistää tietoturvallisuuden saattamista kiinteäksi osaksi valtionhallinnon kaikkea toimintaa. VAHTI käsittelee valtionhallinnon tietoturvallisuutta koskevat määräykset, ohjeet, suositukset ja tavoitteet sekä muut tietoturvallisuuden linjaukset ja toimenpiteet. Valtionhallinnon lisäksi VAHTIn toiminnan tuloksia hyödynnetään laajasti myös kunnallishallinnossa, yksityisellä sek-torilla, kansalaistoiminnassa ja kansainvälisessä yhteistyössä. VAHTI on tunnettu muun muassa tietoturvajulkaisuista ja –ohjeista sekä tietoturvahankkeistaan (www.vm.fi/vahti).

Valtion tietoturvallisuuden kehitysohjelma on julkaistu VAHTI-julkaisusarjassa nimellä Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004–2006, VAHTI 1/2004. Kehitysohjelmalla kehitetään tietoturvallisuutta laajasti osana kaikkea toimintaa. Kehitysohjelmaan sisältyy kaikkiaan 29 laajaa kehittämiskohdetta, joista osaa toimeenpannaan työryhmien tai jaostojen valmistelussa ja osaa muilla toimenpiteillä.

Kehitysohjelmaan osallistuvat laajasti kaikki hallinnonalat ja lisäksi osassa hankkeita on mukana kuntien ja elinkeinoelämän edustajia sekä ulkopuolisia asiantuntijoita. Hankkeissa on vuonna 2005 ollut mukana valtionhallintotasolla nimettyinä noin 300 osallistujaa. Osa kehitysohjelman kehitystyöstä toteutetaan hanketyöllä ja osa muulla ohjaus-, kehitys- ja yhteistyöllä. Virallisesti asetetut hankkeet löytyvät valtioneuvoston hankerekisteristä (http://www.hare.vn.fi/) VAHTIn (VM166:00/2003) alahankkeina. Seuraavassa kuvassa on esitettyinä kehitysohjelman osa-alueet.

Kaavio kehitysohjelmasta ja sen hankealueista



Tämä asiakirjan on laatinut VAHTIn alainen tietoturvallisuuden tulosohjaus ja mittaustyöryhmä. Työryhmän työ on osa kehitysohjelman tietoturvakulttuurin luominen-hankealuetta.

VAHTIn toiminnan kokonaisuutta vuodelta 2005 sekä hankkeiden tavoitteita on kuvattuna VAHTIn toimintakertomuksessa (VAHTI 1/2006).

Sisällysluettelo

1 JOHDANTO

1.1 Hankkeen tausta

Valtionhallinnon tietoturvallisuuden johtoryhmä VAHTI julkaisi vuonna 1999 ulkoistuksen tietoturvallisuutta käsittelevän ohjeen[1] , jonka nyt käsillä oleva ohje korvaa. Kyseisen ohjeen kehittäminen ja uudistaminen on tullut ajankohtaiseksi mm. seuraavista syistä:

– Tarve erilaisten muutostilanteiden hallintaan keskittyvään tietoturvaohjeistukseen on ilmeinen. Ulkoistamisen ohella ja siihen liittyen tiedon hallinnan kenttään kohdistuu lukuisia turvauhkia, jotka tulee muutostilanteissa olevissa organisaatioissa huomioida muutoksen eri vaiheissa.
– Ulkoistamiseen keskittynyt VAHTI-ohje 2/1999 käsitteli aihetta jossain määrin rajatusti keskittyen lähinnä tietojärjestelmien käyttöpalveluiden hankintaan. Ulkoistus on valtionhallinnossa muutostekijänä laajentunut kattamaan muitakin toimintoja. Lisäksi tarkasteltavaksi on tullut muita merkittäviä muutostekijöitä, kuten sähköinen asiointi.
– Valmistuessaan ohje oli ensimmäisiä VAHTI-ohjeita. Siinä ei siten ollut mahdollista viitata muihin ohjeisiin, vaan lukijalle oli esiteltävä tietoturvallisuuden perusasioita. Ohjekokonaisuuden ollessa nykyisellään laaja ja kattava sekä lukijakunnan tietojen ja kokemusten niin tietoturvallisuudesta kuin ulkoistamisesta olennaisesti paremmat kuin aikaisemmin, uudistettavan ohjeen laadinnassa on voitu keskittyä ydinasioihin ja mm. viitata hankintojen, tietoturvallisuuden hallintajärjestelmän arvioinnin ja muiden asioiden kohdalla niistä laadittuihin VAHTI-ohjeisiin.
– Valtion- ja yleensä julkishallinnon kehittyvät palvelukeskukset ovat tuoneet muutos- ja ulkoistustekijänä (sisäinen ulkoistaminen) uuden ulottuvuuden tarkasteluun.
– Ohjeen uusiminen liittyy myös keskeisesti Valtionhallinnon tietoturvallisuuden johtoryhmän VAHTI:n asettaman työryhmän valmistelemaan valtionhallinnon tietotur-

[1] http://www.vm.fi/tiedostot/pdf/fi/3405.pdf

vallisuuden kehittämisohjelmaan vuosille 2004-2006[2] . Ohje toteuttaa kehittämisohjelman seuraavia kohtia:
5.1.2 Tietoturvallisuuden sitominen virastojen palveluihin ja prosesseihin
5.2.2 Tietoturvaohjeistuksen kehittäminen
ja osin myös
Ohjelman korin neljä tietoturva- ja tietojärjestelmävastaavien työn tukemiseen liittyvän luvun 5.4 kehityskohteita (alalukuja).

Uusi ohje on siis sisällöltään entistä kattavampi. Muutos ymmärretään tässä yhteydessä laajasti ja sen katsotaan sisältävän kaikki toiminnalliset, lainsäädännölliset, tekniset kuin muutkin organisaatioiden toimintaympäristöissä tapahtuvat muutokset. Ulkoistusta tarkastellaan toiminnan kehittämisen yhtenä muutostekijänä eikä erillisenä ilmiönä. Laajuus teki työstä haastavan koska sen perustaksi tuli arvioida, mitkä valtionhallintoa koskettelevista muutoksista ovat tietoturvallisuuden kannalta tärkeimpiä. Työn haastetta lisäsivät myös tunnistettujen muutostekijöiden heterogeenisyys ja niiden väliset kytkökset ja riippuvuudet.

1.2 Suosituksen laatiminen

Suosituksen laadinta on käynnistetty osana valtionhallinnon tietoturvallisuuden kehitysohjelman 2004 – 2006 (VAHTI 1/2004) toteuttamista. Suosituksen uusiminen on ollut kehitysohjelmaan liittyen asetetun Tietoturvallisuus valtion prosesseissa -jaoston keskeisin työ. Tämän VAHTIn alaisen jaoston toiminnan tavoitteeksi asetettiin tehostaa ja monipuolistaa tietoturvallisuuden sitomista osaksi ministeriöiden, virastojen ja laitosten toimintoja, prosesseja, hankintoja ja järjestelmien kehitystä. Jaoston ja samalla ohjetyöryhmän kokoonpano on ollut seuraava:

Puheenjohtaja:
tietohallintojohtaja **Ari Uusikartano**, ulkoasiainministeriö
Jäsenet:
neuvotteleva virkamies **Marjukka Ala-Harja**, valtiovarainministeriö
tietoturvapäällikkö **Hellevi Huhanantti**, Väestörekisterikeskus
yli-insinööri **Olli Jokinen**, Maanmittauslaitos
toimistopäällikkö **Maija Kleemola**, Tietosuojavaltuutetun toimisto
johtaja **Kaarina Koskinen**, Ulkomaalaisvirasto
tietohallintojohtaja **Markku Kuula**, Helsingin kauppakorkeakoulu
atk-erikoistutkija **Timo Larmela**, Teknillinen korkeakoulu
tietohallintojohtaja **Asta Partti**, Kaakkois-Suomen verovirasto

[2] http://www.vm.fi/tiedostot/pdf/fi/70508.pdf ja
http://www.vm.fi/vm/liston/page.lsp?r=70507&l=fi&menu=70511

tietoturvapäällikkö **Kaisu Rahko**, Oulun yliopisto
tietohallintopäällikkö **Erja Saraste**, Huoltovarmuuskeskus
tietoturvapäällikkö **Seppo Sundberg**, Valtiokonttori.

Työryhmän konsultteina ovat toimineet Olli-Pekka Soini, Pekka Ruuskanen ja Seppo Salminen WM-data Oy:stä sekä hankesihteerinä avustaja Rauni Vuorensola kauppa- ja teollisuusministeriöstä.

Jaosto on pyrkinyt työssään hyödyntämään mahdollisimman paljon jo olemassa olevaa ja uudistuksen alla kehitettävää VAHTI-ohjeistusta. Läheisimmät kytkökset ohjeella on kehitysohjelman tulosohjaukseen ja arviointiin liittyviin ohjeistushankkeisiin.

VAHTI päätti suosituksen julkaisemisesta kokouksessaan 27.4.2006.

1.3 Suosituksen tarkoitus ja rajaus

Organisaation kokemat muutokset vaihtelevat suurista strategisista pieniin operatiivisiin muutoksiin. Osassa tapauksista organisaatio itse hakee muutosta osallistuen aktiivisesti sen läpivientiin. Osassa taas organisaatio koettaa sopeutua parhaan kykynsä mukaan ympäristön muutokseen.

> Muutoksella ymmärretään tilannetta, jossa organisaatio tai sen toimintaympäristö muuttuu enemmän kuin vähäiseksi katsottavissa määrin.

Eräs tällainen muutos on ulkoistus, jonka työryhmä valitsi muita muutostekijöitä lähemmän tarkastelun kohteeksi.

Ulkoistuksen ja palveluhankinnan käsite riippuu tarkastelunäkökulmasta, koska toisen hankinta on toisen ulkoistus. Ohjetta tulisi lukea hankintojen tietoturvallisuudesta annetun VAHTI-ohjeen (6/2001) rinnalla ja päinvastoin. Myös tietoturvallisuuden hallintajärjestelmän arvioinnista annettu suositus (3/2003) liittyy kiinteästi aihealueeseen. Muutoksen taustalla on yleensä pyrkimys organisaation tuloksellisuuden ja tuottavuuden parantamiseen, johon löytyy kytkentä ohjeeseen 2/2004.

Pääsääntöisesti ulkoistettavasta toiminnosta (toiminnon tuottamasta palvelusta) on vastannut organisaatio itse, mutta ulkoistetusta toiminnosta voidaan puhua myös tilanteessa, jossa toiminto on organisaatiota perustettaessa päätetty hankkia ulkoisena palveluna. Lopputulos on sama, mutta tulokset eroavat tietoturvallisuuden kannalta toisistaan: ensimmäisessä tapauksessa ulkoistukseen liittyy muutos, jälkimmäisessä ei.

Työryhmä määritteli ulkoistuksen käsitteen seuraavasti:

> Ulkoistaminen on organisaation jonkin toiminnon tai toiminnon itsenäisten osien siirtämistä palvelutoimittajan hoidettavaksi.

Ohjeen tarkoituksena on auttaa toimintojansa ulkoistaneita tai tätä suunnittelevia organisaatioita takaamaan asiaan liittyvä tietoturvallinen toimintamalli. Toinen tärkeä kohderyhmä ovat organisaatiot, jotka haluavat varmistaa tietoturvallisuutensa säilymisen muunkinlaisissa muutostilanteissa.

Tietoturvallisuus (VAHTI 4/2003 mukaan) on
1) tavoitetila, jossa tiedot, tietojärjestelmät ja palvelut saavat asianmukaista suojaa siten, että niiden luottamuksellisuuteen, eheyteen ja käytettävyyteen kohdistuvat uhat eivät aiheuta merkittävää vahinkoa yhteiskunnalle ja sen jäsenille
2) lainsäädäntö ja muut normit sekä toimenpiteet, joiden avulla pyritään varmistamaan tietoturvallisuus (1) niin normaali- kuin poikkeusoloissakin.

Ulkoistusta ja muutosta tarkastellaan enemmän toiminnallisena kuin teknisenä asiana. Ohje on pyritty kirjoittamaan siten, että sen lukeminen ei edellytä tietotekniikan syvällistä osaamista. Se sopii niin tietohallintopäättäjille ja kehitysjohdolle kuin talous- ja henkilöstöhallinnon toiminnoista vastaaville esimiehille. Organisaation ylimmän johdon on myös syytä perehtyä muutosten tietoturvavaikutuksiin ennen muutostilannetta. Tällöin muutoksiin voidaan vielä vaikuttaa ja hallita niitä.

1.4 Suosituksen rakenne

Ohjeen monipuolisen aiheen vuoksi toimivan rakenteen aikaan saaminen oli haasteellista pyrittäessä aiheen kannalta loogiseen jaotteluun.

Lukuun kaksi on koottu johdon yhteenveto, joka sisältää suosituksen ydinkohdat.

Luvussa kolme on arvioitu, mitkä muutostekijät ovat valtionhallinnon kannalta keskeisimpiä ja käsitelty lyhyesti niiden tietoturvavaikutuksia. Luvun neljä aiheena on muutoksen johtaminen. Luku viisi keskittyy puolestaan ulkoistuksen tietoturvallisuuden analysointiin.

Prosessien kehittämisen ja tietoturvallisuuden yhteydestä kerrotaan luvussa kuusi.

Ulkoistuksen ja muiden muutostekijöiden kannalta keskeisiä säädöksiä ja juridiikkaa on käsitelty luvussa seitsemän.

Luvussa viisi esiteltyjä asioita käsitellään tarkemmin luvussa kahdeksan. Tarkastelu tapahtuu ulkoistamisen elinkaaren eri vaiheiden avulla.

Lukuun yhdeksän sisältyvät henkilötietojen käsittelyä ja poikkeusoloihin varautumista käsittelevät jaksot.

Ulkoistuksen kohteet ovat laajentumassa perinteisen tietohallinnon toimintojen ja ICT-infrastruktuurin ulkoistuksesta myös muihin toimintoihin. Tästä syystä ohjeessa on pyritty aiheen yleiseen käsittelyyn. Arvioinnin avuksi kehitetty yksityiskohtainen kysymyslista on esitetty raportin liitteenä.

Ohjeen sovellettavuutta on lisätty sisällyttämällä tekstiin esimerkkejä. Ne kaikki ku-

vaavat todellisia tapauksia, joskin nimet ja muut tunnistustiedot on jätetty pois. Suurin osa esimerkeistä on suomalaisia työryhmän jäsenten omia kokemuksia ja osa uutisista poimittuja toteumia muutostilanteiden vaikutuksista.

2 JOHDON YHTEENVETO

Erilaisten organisaation toimintaan liittyvien muutostilanteiden tulee olla hallittavissa. Riskit kasvavat kun tutut toimintamallit ovat muutoksen kohteena. Tässä ohjeessa keskitytään tietoturvallisuuden huomiointiin suhteessa muuttuvaan toimintaan.

Monista muutoksen, ulkoistuksen ja prosessien kehittämisen tietoturvallisuuteen liittyvistä linjauksista keskeisimmät ovat:

Muutos

- **Muutoksen johtaminen ja muutokseen valmistautuminen** vaikuttavat tietoturvallisuutta edistävästi.
- Ihmisten motivointi, **muutosvastarinnan käsittely ja hyvä tiedottaminen** ehkäisevät tietoturvariskien toteutumista muutoksessa. Muutoksen syyt ja seuraukset tulee selvittää henkilöstölle.
- **Lähtötilanteen hyvä tietoturvallisuus** luo parhaat edellytykset muutoksen tietoturvalliselle toteutukselle.

Prosessit

- Tietoturvallisuus tulee ottaa huomioon prosessien kehittämisen **alkuvaiheessa**, ei lopussa.
- **Ihminen toteuttaa prosessit.** Paperilla tietoturvallisin prosessi ei toimi, jos prosessin inhimillinen puoli ei toimi.
- Tietoturvallisuus on mukana **jokaisessa prosessissa,** jossa käsitellään tietoa. Oleellista on **tunnistaa** tietoturvallisuuden kannalta kriittiset prosessit ja niiden vaiheet.

Ulkoistus

- **Toiminnot voi ulkoistaa, mutta vastuuta ei.**
- Ydintoimintoja ei ulkoisteta, mutta tukitoimintojen ulkoistaminen lisääntyy.

- Ulkoistajan on tiedettävä, mitkä ovat ulkoistettavan toiminnon tietoturvallisuuden erityispiirteet ja tuotava ne selkeästi esille.
- Ulkoistettavan toiminnon tietoturvallisuuden korkea taso luo edellytykset onnistuneelle ulkoistukselle.
- Ulkoistuksessa **sitoudutaan** toimittajaan. Ulkoistajan tulee arvioida palvelun toimittajan kykyä vastata tietoturvallisuudesta myös pitkällä aikavälillä.
- Ulkoistus on **suunniteltava** huolella. Erityisesti ulkoistuksen lainmukaisuus on selvitettävä.
- **Ulkoistussopimukset on laadittava huolella.** Niissä on huomioitava tietoturvallisuus ja yksityisyyden suoja.
- Ulkoistetun toiminnon **valmiussuunnittelusta ja jatkuvuussuunnitelmista** on huolehdittava.

3 VALTIONHALLINNON KESKEISIÄ MUUTOSTEKIJÖITÄ JA TRENDEJÄ

Luvun perustana esitetään ohjeen laatineen työryhmän arvio valtionhallinnon toimintaan vaikuttavista merkittävimmistä muutostekijöistä sekä näiden vaikutuksista tietoturvallisuuteen.

3.1 Työryhmän arvio valtionhallinnon suurimmista muutostekijöistä

Ohjetta valmistellut työryhmä laati arvion julkishallintoa – etenkin valtionhallintoa – koskettavista muutoksista ja niiden vaikutuksista tietoturvallisuuteen.

Arviointi tehtiin koostamalla laaja muutostrendilista, jota työn edetessä karsittiin. Näin saatiin lopullinen lista, jossa on lueteltuna 15 merkittävää muutostekijää. Tarkastelussa on huomioitava, että tekijät ovat osittain päällekkäisiä ja myös osin riippuvaisia toisistaan. Ensimmäisessä sarakkeessa on kirjattuna myöhemmissä kuvissa esiintyvä muutostrendin tunnistetieto (M-kirjain ja numero).

Taulukko 1. Työryhmän kokoamat keskeisimmät muutostrendit[3] .

M1	alueellistaminen
M2	ulkoistaminen
M3	liikelaitostaminen ja yhtiöittäminen
M4	kiinteämpi organisaatioiden välinen yhteisyö
M5	yhteiskäyttöiset tietokannat ja -järjestelmät
M6	sähköinen asionti
M7	eläköityminen
M8	palvelukeskukset
M9	tehokkuusvaatimukset
M10	PPP-yhteistö
M11	Kunta- ja aluehallinnon organisaatiomuutokset
M12	Valtiohallinnon organisaatiomuutokset
M13	Ministeriöiden ohjauksen jämäköityminen
M14	Kansainvälistyminen
M15	valtion tietohallinnon yhteinen johto (ValtIT)

[3] PPP = Public Private Partnership eli yksityisen ja julkisen sektorin välinen yhteistyö

Kutakin lopulliselle listalle päässyttä muutosta arvioitiin jatkossa kahden tekijän suhteen:

1) Kuinka merkittävä muutos on julkishallinnon kannalta (taulukko 2)?
2) Kuinka paljon muutos vaikuttaa tietoturvallisuuteen (taulukko 3)?

Työryhmän jäsenten analyysin pohjalta muodostettiin taulukossa esitetty näkemys. Esitetyt muutostekijät kuvattiin myös graafisesti (kuva 1).

Taulukko 2. Muutoksen merkittävyys julkishallinnon kannalta (skaala: 1 = vähäinen vaikuttavuus – 5 = erittäin merkittävä tai äärimmäisen tärkeä vaikuttavuus).

M6	sähköinen asionti	4,5
M2	ulkoistaminen	3,8
M4	kiinteämpi organisaatioiden välinen yhteisyö	3,8
M5	yhteiskäyttöiset tietokannat ja -järjestelmät	3,4
M8	palvelukeskukset	3,4
M9	tehokkuusvaatimukset	3,3
M13	Ministeriöiden ohjauksen jämäköityminen	3,3
M15	valtion tietohallinnon yhteinen johto (ValtIT)	3,2
M3	liikelaitostaminen ja yhtiöittäminen	3,2
M14	Kansainvälistyminen	3,1
M7	eläköityminen	3,0
M12	Valtiohallinnon organisaatiomuutokset	2,8
M1	alueellistaminen	2,7
M10	PPP-yhteistö	2,6
M11	Kunta- ja aluehallinnon organisaatiomuutokset	2,6

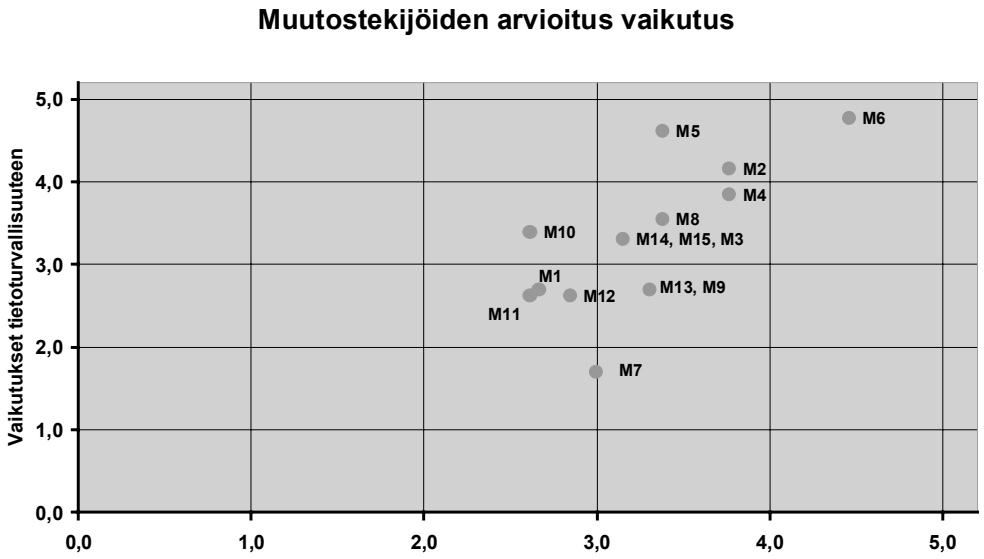
Taulukko 3. Muutoksen vaikuttavuus suhteessa tietoturvallisuuteen (skaala kuten edellä).

M6	sähköinen asionti	4,8
M5	yhteiskäyttöiset tietokannat ja -järjestelmät	4,6
M2	ulkoistaminen	4,2
M4	kiinteämpi organisaatioiden välinen yhteisyö	3,8
M8	palvelukeskukset	3,5
M10	PPP-yhteistö	3,4
M3	liikelaitostaminen ja yhtiöittäminen	3,3
M14	Kansainvälistyminen	3,3
M15	valtion tietohallinnon yhteinen johto (ValtIT)	3,3
M9	tehokkuusvaatimukset	2,8
M1	alueellistaminen	2,7
M13	Ministeriöiden ohjauksen jämäköityminen	2,7
M11	Kunta- ja aluehallinnon organisaatiomuutokset	2,6
M12	Valtiohallinnon organisaatiomuutokset	2,6
M7	eläköityminen	1,7

Kokonaiskuva kahden tekijän yhteisvaikutuksesta saadaan parhaiten esille sijoittamalla muutokset sirontadiagrammiin[4] kuvassa 1.

[4] Esitysteknisistä seikoista johtuen joitain lähekkäin olevia datapisteitä on yhdistetty

Kuva 1. Muutoksen merkittävyyden korrelaatio tietoturvavaikutukseen.



Selkeästi tärkeimmäksi valtionhallinnon tietoturvallisuuteen vaikuttavaksi tekijäksi työryhmä arvioi sähköisen asioinnin (M6). Sen vaikutus niin tietoturvallisuuteen kuin valtionhallinnon toimintaan arvioitiin suuremmaksi kuin minkään muun tekijän. Toiminnallisen muutoksen kannalta ero seuraaviin on suuri, tietoturvallisuuden osalta yhteiskäyttöiset tietojärjestelmät ja tietokannat (M5) on vaikutukseltaan lähes samansuuruinen. Viimeksi mainittu tekijä yhdessä ulkoistamisen (M2) ja valtionhallinnon organisaatioiden välisen yhteistyön lisääntymisen (M4) kanssa muodostavat seuraavaksi tärkeimmän ryhmän. Valtionhallinnon yhteisten ja tietyn hallinnonalan sisäisten palvelukeskusten perustaminen erottuu muutostekijöiden ”pääjoukon” kärjestä. Pääjoukosta poikkeaa vain eläköityminen, jonka tietoturvavaikutusten arvioitiin olevan pieni – vain hieman positiivinen.

Muutostekijät ovat usein riippuvuussuhteessa toisiinsa eri tavoin; toinen muutos voi olla toisen seurausvaikutusta. Joillakin muutostekijöillä on yhteinen syy tai ne ovat pohjimmiltaan asioita, jotka ovat hyvin lähellä toisiaan. Alueellistaminen, ulkoistaminen ja liikelaitostaminen sisältävät kaikki saman peruselementin: palvelun tuottamisen siirtämisen jonnekin joko fyysisesti tai toiminnallisesti. Nämä kaikki kolme ovat osa julkishallinnon organisaatiomuutoksia. Yhteistyön tiivistymisen (M4) ja yhteiskäyttöisten järjestelmien (M5) välinen yhteys on ilmeinen. Monia vastaavia yhteyksiä muutostekijöiden välillä on olemassa, mikä vaikeuttaa yksittäisten muutostekijöiden arviointia ja niiden erottamista toisistaan.

Työryhmä totesi, että muutostekijät ovat jaettavissa neljään pääryhmään:

1) sähköinen asiointi ja sähköinen hallinto

2) ulkoistus
3) verkottuminen
4) kansainvälistyminen.

Sähköinen asiointi kokonaisuutena merkitsee erittäin laajaa muutosta tapaan toimia ja tuottaa julkishallinnon palveluita. Ulkoistustoimet ja niihin monesti liittyvät organisaatioiden verkottumisen ja jopa palvelutoiminnan kansainvälistymisen aspektit ovat toki muutoksia tapaan tuottaa palveluja, mutta ne ovat kuitenkin usein vain taustatekijöitä sähköisten palvelujen toteuttamisen ja tuottamisen kokonaiskentässä.

3.2 Sähköinen asiointi ja sähköiset palvelut

3.2.1 Suuri sähköinen muutos

Sähköisellä asioinnilla tarkoitetaan hallintoasian sähköistä vireillepanoa, käsittelyä ja päätöksen tiedoksiantoa[5]. Sähköiseksi palveluksi ymmärretään sähköinen asiointi sekä muut julkisyhteisön yleisölle tai toisille julkishallinnon tarjoamat palvelut ja niihin liittyvät prosessit silloin, kun palvelun käyttö tapahtuu sähköisellä tiedonsiirtomenetelmällä[6].

Sähköisen asioinnin merkitys on suuri – ehkä historiallisesti suurempi kuin kykenemme arvioimaan. Muutos on parhaimmillaan syvällinen, sillä se ei rajoitu vain asiakasrajapinnassa oleviin verkkopalveluihin, vaan kattaa palveluita tarjoavan yksikön tietojärjestelmät, prosessit ja organisaatiokulttuurin. Sähköisen palvelun tietoturvauhissa on paljon sellaisia, joita perinteisissä palveluissa ei ole. Tämän lisäksi tulevat itse muutoksen aiheuttamat tietoturvavaikutukset. Prosessien ja asenteiden muuttuessa on tietoturvallisuuden vaarantuminen paljon todennäköisempää kuin entisessä stabiilissa tilanteessa.

3.2.2 Sähköisten palvelujen tietoturvallisuus

Sähköisten palveluiden tietoturvauhkia ja niiltä suojautumisen keinoja on esitelty VAHTI-ohjeessa Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje (4/2001)[7]. Varsinkin ohjeen luvussa viisi on kuvattu näitä asioita. Tässä esityksessä käydään vain yleisluontoisesti läpi sähköisen palvelun aiheuttamia tietoturvavaatimuksia silloin kun kyseessä on muutos, eli perinteisten palveluiden tilalle tai näiden rinnalle tullessa sähköinen palvelu.

[5] Laki sähköisestä asioinnista viranomaistoiminnassa 24.1.2003/13

[6] Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje (VAHTI 4/2001) pohjalta.

[7] http://www.vm.fi/tiedostot/pdf/fi/3372.pdf

- velu on tuotantokäytössä. Perinteisten palvelujen tietoturvauhat on hyvin tiedostettuja ja niitä vastaan on olemassa asianmukaisia vastakeinoja, mutta sähköisellä puolella näin ei välttämättä ole. Uusi tekniikka ja uudet toimintatavat tuovat mukanaan uusia uhkia, joita ei niitä käyttöönotettaessa ole ymmärretty. Keinoja hallita ongelmaa on lukuisia. Sähköisen palvelun kehittämisprojektin alkuvaiheessa tehty ja prosessin aikana jatkuvasti ylläpidetty riskianalyysi auttavat hallinnassa. Ulkopuolisen arvioijan käyttäminen näkökulman laajentamiseksi on suositeltavaa. Pitäytyminen tutuissa teknisissä ratkaisuissa parantaa tietoturvallisuuden hallintaa. Asianmukaiset suunnitelmat tietoturvariskien toteutumisen varalle ovat viimeinen keino, jos kaikki muu valmistelu pettää.
- Sähköisen palvelun yhteydessä kehitetään yleensä prosesseja, jolloin esiin tulevat prosessien muutoksiin liittyvät tietoturva-asiat. Siirtyminen uusiin toimintatapoihin vaatii aikaa, eikä se useinkaan tapahdu kitkatta. Uusi toimintatapa on yleensä sekoitus vanhaa ja uutta, jolloin esimerkiksi järjestelmän käyttöoikeudet saattavat olla liian pienet tai suuret, kun taas oikeellisuuden ja käytettävyyden valvonta voivat osaltaan jäädä katveeseen. Tärkein keino tämän kaltaisten ongelmien hallintaan on prosessien järjestelmällinen kehittäminen ja prosessin käynnistäminen hyvissä ajoin ennen suunniteltua muutosta. Hyvin hoidettu muutoshallinta sekä tietoturvakulttuurin hyvä perustaso auttavat muutosta oikeaan suuntaan. Asiaa on käsitelty laajemmin jäljempänä luvussa viisi.
- Sähköisten palvelujen myötä tietoturvallisuus muuntautuu ulos perinteisestä linnaajattelusta, jossa uhat voitiin sulkea muurien ulkopuolelle. Sähköisten palveluiden monimuotoisessa teknisessä ja toiminnallisessa ympäristössä uhkia hallitaan, mutta niitä ei kategorisesti suljeta pois. Tämä edellyttää uutta ajattelua: on tarvelähtöisesti tunnistettava, mitkä tietojärjestelmät ja tiedot ovat kriittisiä ja missä suojauksen taso voi olla vähemmän korkea.

3.2.3 Uusia vaatimuksia

Sähköisen asioinnin ja palvelujen on katsottu edellyttävän myös uutta lainsäädäntöä.

Henkilötietojen käsittelyä säädeltiin vuoden 1988 alusta lähtien henkilörekisterilailla (471/1987). Se korvattiin 1.6.1999 lähtien henkilötietolailla (523/1999). Henkilörekisterilain ja henkilötietolain tarkoituksena oli ja on luoda pelisäännöt sähköisesti (automaattisen tietojenkäsittelyn avulla) tapahtuvalle henkilötietojen käsittelylle sekä näin ehkäistä ennakolta tällaiseen käsittelyyn liittyviä tietosuoja- ja tietoturvariskejä. Viranomaisen asiakirjoja koskevat seuraavat lait: 1.12.1999 voimaan tullut laki viranomaisten toiminnan julkisuudesta (621/1999, jäljempänä Julkisuuslaki) ja asetus (1030/1999; uudistettavana). Lakiin sisällytettiin myös hyvää tiedonhallintaa koskevat säännökset.

Asiakirjojen ja tietojen käsittelyn lainmukaisuuden varmistaminen sähköisessä käsittelyssä ja käytössä edellyttää uudenlaisia menettelytapoja ja osaamista. Toimivien ja

lainmukaisten teknisten ratkaisujen aikaansaaminen ja kehittäminen tietoturvallisuuden ja suojaamisvelvoitteiden, tietojen eheys-, virheettömyys- ja tarpeellisuusvaatimusten sekä salassapidon huomioon ottamiseksi asettavat suuria vaatimuksia erityisesti etukäteissuunnittelulle.

Tietojärjestelmien kehittäminen on kallista ja kehiteltävien ratkaisujen tulisi toimia yleensä pidemmän aikaa ja mahdollistaa myös organisatoriset muutokset ja uudelleenjärjestelyt sekä palvelujen hankkimisen ulkopuolisilta palvelujen tuottajilta. Suunnittelu- ja analysointityö on sen vuoksi tarpeen tehdä varsin yksityiskohtaisesti viranomaisten eri tehtävien, henkilötietojen eri käsittelytarkoitusten (eri henkilörekisterien) ja niiden prosessien ja työnkulkujen osalta.

Tietojärjestelmien ja sähköisten palveluiden toteuttaminen ovat kokonaisuuksia, joiden käyttöönotto edellyttää tiivistä ja toimivaa yhteistyötä eri osaajien ja ammattiryhmien sekä hankkeen muiden mahdollisten osapuolten välillä. Tietotekninen perusosaaminen ja omien oikeuksien tuntemus ovat tietoyhteiskunnassa keskeisiä kansalais- ja yhteiskuntataitoja. Niitä edellytetään jokaiselta henkilötietojen käsittelyn kohteena olevilta henkilöiltä (rekisteröidyiltä) heidän omien henkilötietojensa käsittelyyn liittyvien oikeuksiensa turvaamiseksi. Henkilötietoja käsittelevien (rekisterinpitäjien) palveluksessa olevilta vaaditaan tekniikan ja lainsäädännön hyvää osaamista, jotta nämä kykenevät toteuttamaan henkilötietojen käsittelyn laissa säädetyllä tavalla.

Asiakirjojen ja tietojen ylläpidossa käytettävät tietojärjestelmät ja niiden toimivuus nousevat aikaisempaan verrattuna yhä keskeisemmiksi tekijöiksi viranomaisten tehtävien hoidossa.

Sähköisessä käsittelyssä myös rekisteröityjen henkilöiden tiedonsaantitarve lisääntyy ja muuttuu. Olennaisena osana tietojärjestelmien toteutusta tulee varmistua siitä, että asiakkaat tietävät, mitä ja miten heidän tietojaan järjestelmässä käsitellään. Tietoisuus käsittelytavasta lisää myös luottamusta organisaation ja kansalaisen välillä. Avoimuuden toteuttamista sääntelevät eri tavoin sekä julkisuuslaki että henkilötietolaki. Tietojenkäsittelyn avoimuutta tulee toteuttaa hyvän tietojenhallintotavan edellyttämän palvelun tasotavoitteiden mukaisesti.

Verkkopalvelussa on huolehdittava, että henkilötietolain 24§ edellyttämät tiedot käsittelystä ovat kansalaisten saatavilla verkossa.

3.3 Ulkoistus

Ulkoistus muutosprosessina on vaikuttavuudeltaan merkittävä. Tässä ohjeessa ulkoistuksen tietoturvallisuutta käsitellään luvuissa viisi ja kahdeksan.

3.4 Verkottuminen

Verkottumisessa yritys, virasto ja muu toimija joutuvat läheisesti tekemisiin toisten yritysten ja virastojen kanssa. Syitä verkottumiseen on useita[8]. Erikoistuminen on pilkkonut yrityksiä ja on syntynyt tilanteita, joissa aiempi yksi yritys on jakautunut useampaan yksikköön ilman, että toiminta on juurikaan muuttunut. Kommunikaatiokustannukset ovat alentuneet ja ihmisten halu kommunikoida keskenään on kasvanut.

Verkottumisessa useat organisaatiot joutuvat tekemisiin toistensa tietoturvallisuuden kanssa. Organisaatioiden välinen raja voi tällöin olla matala, jolloin kokonaisuuden tietoturvallisuus muodostuu heikoimman lenkin periaatteen mukaan.

Verkottuminen liittyy usein nopeaan muutokseen, jossa tapauksessa tietoturvallisuus joutuu koetukselle. Tulee helposti tilanteita, joissa – ainakin näennäisesti – joudutaan tekemään valintoja käytettävyyden ja luottamuksellisuuden välillä.

Verkottuminen johtaa siis suurempaan riippuvuuteen verkottuvien yksiköiden kesken. Esimerkkinä sähköisen palvelun käytettävyys voi laskea, kun tunnistamispalvelun toimittajan alihankkijan tekemä ohjelman osa ei toimikaan tarkoitetulla tavalla tai jokin muu verkottuneen palveluntuotantoketjun osa ei vastaa asetettuja tavoitteita.

Verkottuneen maailman tietoturvallisuuden hallinta on valtava haaste. Se on suurempi kuin mitä sähköisten palveluiden tulo on ollut, sillä niissä merkittävä osa ongelmista oli tekniikasta johtuvia ja teknisin keinoin hallittavissa. Verkottumisessa on pitkälti kyse tietoturvallisuuden ”pehmopuolesta”, mutta hallinnollisilla ja teknisillä ratkaisuilla on oma sijansa kokonaisuudessa.

Vahva tietoturvakulttuuri sekä kumppaniverkon hallinta edistävät verkottuneen toimintaympäristön tietoturvallisuutta. On myös tärkeää huomata, että verkottuminen ei poista tai useinkaan edes siirrä vastuuta. Verkottuvan organisaation johdon vastuu pikemminkin kasvaa kuin pienenee, koska verkostokumppanien toimien puutteet saattavat vaikuttaa huomattavasti kyseisen organisaation toimintaedellytyksiin. Vastuunjaon selkeys, asioiden esille ottaminen ja hyvä käsitys omasta tietoturvatilanteesta edistävät verkottumisen tietoturvallisuuden hallintaa.

Tietojen ja toimitilojen luokittelu ja näitä tukevien ratkaisujen helppokäyttöisyys pienentävät riskiä luottamuksellisuuden rikkoontumiselle. Kumppanit voivat ilmentää tietoturvallisuutensa tasoa erilaisilla sertifikaateilla, keskinäisillä auditoinneilla ja arvioinneilla tai esittämällä ulkopuolisten auditointien tuloksia. Erilliset turvallisuussopimukset ovat erinomainen keino, jolla saavutetaan kaksi tietoturvallisuuden kannalta tärkeää tavoitetta: turvallisuusasioista sovitaan, mikä helpottaa monia käytännön asioita ja lisäksi turvallisuussopimuksen tekeminen ja erityisesti sen vaatiminen viestittää osapuolten halusta edistää tietoturvallisuutta.

[8] Hyvä yleisesitys verkottumisesta on esitetty julkaisussa Unbundling the Corporation, Harvard Business Review, Maaliskuu 1999. Verkottumisen uhkia on esitetty Puolustustaloudellisen suunnittelukunnan julkaisussa Internet, toiminnan verkottuminen ja sen haavoittuvuus (2/2001), http://www.huoltovarmuus.fi/documents/3/Internetohje_ver2.pdf

Esimerkki: *Yrityksellä X on monia asiakkaita, joiden turvallisuustarpeet ovat erittäin suuret. Palvelut X tuottaa kumppanien kanssa, joten palvelun toimittaa yritysverkosto. X solmii turvallisuussopimuksia toimittajakumppaniensa ja alihankkijoidensa kanssa. Sopimuksen teko viestii sopimuskumppaneille turvallisuuden merkityksestä ja pakottaa nämä arvioimaan omaa tietoturvatasoaan.*

Verkottuneessa maailmassa joudutaan aiempaa enemmän luottamaan palveluntuottajasta syntyneeseen mielikuvaan – brändiin. Asiakkaan on usein mahdotonta saada selville, ketkä kaikki osallistuvat palvelun tuotantoon. Hänen on siis luotettava siihen, että palvelun tarjoaja on pitänyt huolta kokonaisuuden turvallisuudesta. Mikäli ulkoistajalle on tärkeää tietää, mitkä yritykset osallistuvat palveluntuotantoon on sopimukseen sisällytettävä kohta, joka velvoittaa päätoimittajan informoimaan ulkoistajaa, mikäli joku ennalta määrätyistä alihankkijoista vaihtuu. Kriittisimmissä tapauksissa voidaan edellyttää ulkoistajan hyväksyntää toimittajavaihdoksille tai toiminnan edelleen ulkoistamiselle.

3.5 Kansainvälistyminen ja ulkomaille ulkoistaminen

Kansainvälistyminen, globalisaatio ja eurooppalaistuminen ovat kaikki saman asian ilmentymiä: elämme maailmassa, jossa kansallisten rajojen merkitys on vähäisempi kuin ennen. *Off-shoring, near-shoring* ja Kiina-ilmiö kuuluvat myös kansainvälistymiseen. Kansainvälistyminen saattaa muuttaa toimintatapoja ja -paikkaa ja tuo suomalaiset kosketuksiin muiden maiden lainsäädännön kanssa.

Henkilötietojen siirtämisen edellytykset EU:n ulkopuolelle on säädetty henkilötietolaissa (luku 5 ja 36-37§)[9]. Kohdemaan lainsäädäntö ja oikeuskäytäntö saattavat osoittautua suuresti suomalaisesta poikkeavaksi[10].

Maantieteellinen ja kulttuurinen etäisyys lisäävät joitain riskejä, mutta myös vähentävät toisia. Maariski pienenee, mutta tietoturvallisuus saattaa vaarantua yllättävistä tekijöistä - kuten kulttuurieroista tai luonnonmullistuksista - johtuen. Aikaero ja ero paikallisessa lainsäädännössä saattavat aiheuttaa yllätyksiä.

Esimerkki: *Kansainvälinen yritys Z oli ulkoistanut IT-toimintonsa suurelle kansainväliselle toimijalle, joka puolestaan oli siirtänyt help-desk -toimintoja Aasiaan. Tietojärjestelmien käytettävyys alkoi kärsiä, kun kieli- ja kulttuurieroista johtuen virhetilanteiden selvittäminen kesti pitkään. Tilannetta korjattiin vaihtamalla aasialaisen*

[9] ks. http://www.tietosuoja.fi/1582.htm ja Asiaa tietosuojasta 1/2005.

[10] Ohjeen laatimisen aikana Intian uudistettu tietoturvalainsäädäntö on synnyttänyt keskuste-lua. Laki on parannus edelliseen verrattuna, mutta ei vieläkään vastaa länsimaiden tasoa.

maan help-desk:in esimiehiksi Eurooppaa tuntevia ja paremmin englantia osaavia henkilöitä. Lisäksi lähitukeen lisättiin resursseja.

Yksittäinen organisaatio voi kohdata kansainvälistymisen monella tavalla. Tietoturvamielessä merkittävimmät ovat:

1) *Suorat kansainväliset suhteet.* Tässä tapauksessa kansainvälinen kanssakäyminen tapahtuu selkeällä toimintamallilla. Henkilötietojen siirtoa koskevien tai muihin kansainvälisyyteen liittyvien säädösten noudattaminen on sikäli helppoa, ettei asian kansainvälisyys jää huomaamatta. Osallistuminen kansainvälisiin työryhmiin, yhteistyöelimiin tai muunlainen maan rajat ylittävä toiminta ovat esimerkkejä suorasta kansainvälistymisestä.
2) *Kansainvälistyminen ulkoistamalla ulkomaille.* Tätä ei julkishallinnossa toistaiseksi ole tapahtunut, mutta asia yleistynee tulevaisuudessa. Ulkomaille ulkoistamisen asioita käsitellään myöhemmin tässä ohjeessa.
3) *Välillinen kansainvälistyminen.* Suoran, selkeästi havaittavan kansainvälistymisen lisäksi tätä tapahtuu välillisesti, kun toimittajat ja kumppanit ulkoistavat toimintojaan ulkomaille. Toistaiseksi suomalaiset IT-yhtiöt ovat siirtäneet toimintojaan ulkomaille vain vähäisessä määrin (lähinnä ohjelmointia), mutta asia tulee suurella todennäköisyydellä lisääntymään ja muut toimialat seuraavat kehityksessä perässä.

Esimerkki: *Yrityksen Y eräs asiakas edellytti, että tiettyyn osaan yrityksen tiloihin pääsevistä henkilöistä on tehty turvallisuusselvitys. Kilpailutuksen tuloksena Y vaihtoi kiinteistöpalvelujen tarjoajaa. Merkittävä osa uuden kiinteistöpalveluyrityksen Z työntekijöistä tuli maista, joiden kansalaisista ei turvallisuusselvitystä ollut mahdollista saada, joten Y joutui neuvottelemaan Z:n kanssa asiasta. Sovittiin, että vain sellaisia työntekijöitä käytetään, joiden taustaselvitykset on tehty. On kuitenkin huomattava, että taustaselvitysten teko on tarkasti säädelty laissa yksityisyyden suojassa työelämässä (759/2004). Tietojen hankkiminen tulee tapahtua pääsääntöisesti työntekijän suostumuksella.*

3.6 Muita muutostekijöitä

Tuottavuus- ja tehokkuusvaatimusten kasvu lisää julkisen sektorin paineita. Tehokas, joustava ja asiakaslähtöinen julkishallinto on kaikkien etu. Tietoturvallisuuden kannalta kehityssuunnalla on useita seurauksia. Kaiken rahankäytön on oltava hyvin perusteltua, mikä edellyttää usein laskelmia ja mitattavaa hyötyä. Tietoturvallisuuden nähdään kilpailevan resursseista muiden investointi- ja käyttökohteiden kanssa. Päätöksentekotilanteessa tietoturvallisuudesta on helppo tinkiä, mikäli se koetaan vain kustannuseränä ja pahimmillaan asiakaspalvelua tai muuta toimintaa haittaavana asiana.

Tuottavuuden kasvua haetaan erilaisilla keinoilla. Ulkoistaminen, julkishallinnon palvelukeskukset ja organisaatiomuutokset ovat esimerkkejä tämän kaltaisista pyrkimyksistä. Kussakin tapauksessa on omat tietoturvallisuuteen liittyvät erityispiirteensä, jotka tulee huomioida. Esimerkiksi valtionhallinnon tietohallinnon ja kokonaisuuteen liittyen myös tietoturvallisuuden ohjaamisen tiivistäminen (ValtIT-hanke) on muutos, joka täysimittaisesti toimintamallina toteutuessaan vaikuttaa merkittävästi nykyiseen tilanteeseen. Vahvana vaikuttavana tekijänä on usko keskitetyn päätöksenteon ja palvelutuotannon tuottavuutta lisäävään vaikutukseen. Keskitetty rakenne tuo uusia tietoturvallisuuteen liittyviä haasteita liittyen esimerkiksi palvelukeskuksiin.

Asiakasnäkökulman korostuminen julkishallinnossa on muutostekijä, jolla on myös seurannaisvaikutuksia. Se korostaa tietoturvallisuuden osa-alueista käytettävyyttä, sillä tämän puutteen asiakas havaitsee nopeasti. Asiakasnäkökulman korostaminen ei saa kuitenkaan vaarantaa muita tietoturvallisuuden osa-alueita, eli luottamuksellisuutta ja eheyttä. Esimerkiksi sähköisten koostepalvelujen tuottamisessa, jossa palvelun sisällön tuottaa useampi organisaatio, tietoturvallisuuden vastuujako tulee olla selkeästi määritelty sopimuksin.

Muutostekijöinä on ollut esillä myös erilaisia hallintomallin muutoksia (liikelaitostaminen ja yhtiöittäminen, keskushallinnon tiiviimpi ohjaus), globalisoitumisen vaikutuksia (kansainvälistyminen, off-shoring) sekä viraston fyysiseen toimintaympäristöön vaikuttavia hankkeita (toiminnan hajauttaminen, alueellistaminen). Voidaan todeta, että muutostekijöiden yhteisvaikutuksena asioiden hoidon aika-, paikka- ja tapasidonnaisuus vähenee tekniikan kehityksen myötä ja tämä nostaa luonnollisesti tietoturvahaasteiden tasoa. Tietoturvallisuuden kannalta ongelmallisia ovat esimerkiksi etätyötavat, joissa etätyön tekijälle odotetaan luotavan organisaation normaalien toimitilojen ulkopuolella olevaan työpisteeseensä aivan vastaavat tietoyhteydet kuin normaalissa toimipisteessä olevat. Langattoman laajakaistaisuuden mahdollistama mobiilityö on vieläkin haastavampi kokonaisuus turvattavaksi.

Eläköityminen vaikuttaa tietoturvallisuuteen; osin sitä heikentävästi, mutta osin vaikutukset ovat myös positiivisia. Ns. hiljainen tieto ei siirry itsestään ja huomattava osa tietoturvakulttuurista pohjautuu tälle olettamukselle. Suurten ulkoistumispäätösten yhdistäminen merkittävään henkilöstön poistumaan on väistämättä riskin moninkertaistamista.

4 MUUTOKSEN JOHTAMINEN JA TIETOTURVALLISUUS

Muutos ei ole vain passiivista sopeutumista. Aktiivisella ja asiantuntevalla johtamisella on saavutettavissa huomattavia hyötyjä. Muutosjohtaminen on laaja, monipuolinen aihe ja sitä käsitellään tässä yhteydessä vain lyhyesti.

Muutosjohtamisella ymmärretään niitä järjestelmällisiä toimia, joilla organisaatio varautuu muutokseen ja muuttaa hallitusti omaa toimintaansa.

4.1 Muutostilanteet

Organisaation toimintaympäristö muuttuu jatkuvasti. Johdon on kyettävä hallitsemaan muutostilanne ja hyödyntämään se. Asiayhteydessä on tapana käyttää termiä muutosjohtaminen (Change Management).

Tietoturva-asiantuntijoilla on monta roolia muutoksen hallinnassa: he voivat toimia mahdollistavassa roolissa, jolloin toimintaa kehitettäessä uudet tietoturvaratkaisut takaavat turvallisuuden tason säilymisen. Tietoturvallisuudesta vastaavat voivat myös esitellä uusia ratkaisuja ja näin aikaansaada muutosta. Verkkopalveluiden yleistyminen on hyvä esimerkki näistä kahdesta roolista. Kenties tärkein tehtävä on kuitenkin muutosten tietoturvavaikutusten arviointi. Virastojen ja laitosten johdolle on kyettävä antamaan perusteltu arvio muutoksen vaikutuksista tietoturvallisuuteen ja keinoista, joilla mahdollisesti heikkenevää turvallisuuden tasoa voidaan korjata.

4.2 Muutoksen johtaminen

Muutoksen hallinta on kaikkien organisaatioiden tavoitteena. Voiko muutosta kuitenkaan aina hallita ja onko se siten aina edes tavoitteena realistinen? Muutoksen hallinnan sijasta pyritään hallittuun reagointiin muutostilanteissa ja ennakoimaan suunnitellusti tulevia tilanteita ja muutoksen vaikutuksia. Tavoitteena on tällöin muutoksen hallinnan sijasta sen vaikutusten hallinta.

Muutoksen johtamisessa pyritään hyödyntämään jatkuva muutos reagointiherkkyytenä ja jatkuvana muuttumisena: tasaisen harmonian (tai staattisen tasapainon) tavoittelu johtaa usein vallitsevan tilanteen säilymiseen ja siten vanhojen jäykkyyksien ja organisaation jännitteiden aiheuttamaan alentuneeseen tehokkuuteen.

Muutoksen johtamisessa on lopulta kyse ihmisten johtamisesta. Julkisten organisaatioiden ohjaamiseen on tulossa yhä teknistyvämpi ihmiskuva ja johtamisote – ihminen persoonana unohtuu, jos henkilöstö käsitellään puhtaasti välineenä ja kustannustekijänä. Henkilöstön motivaatio ja sitoutuminen organisaatioon, sen tuloksiin ja myös muutokseen heikkenevät. Tällä on suoria vaikutuksia myös tietoturvallisuuden toteuttamiseen ja ylläpitämiseen niin muutostilanteissa kuin muulloinkin. Tyytymätön, petetyksi itsensä kokeva työntekijä saattaa ääritapauksissa ryhtyä tieto- tai muun turvallisuuden sabotointiin. Vastaavasti muutoksen hyväksyvä henkilöstö omaksuu uusia tietoturvallisia toimintatapoja.

Muutos voi vaatia syntyäkseen kovia otteita. Pelko uudesta, tuntemattomasta ja hallitsemattomasta hillitsee muutoshalukkuutta tehokkaasti – syntyy muutosvastarintaa.

Muutoksen johtamiseen voidaan soveltaa seuraavaa toimintamallia:

1. Henkilöstö ja muut sidosryhmät sitoutetaan muutokseen. Johdon avoimuus, selkeä ja suora tiedottaminen (myös ikävistä asioista), sekä muutosvastarinnan olemassa olon myöntäminen edistävät sitoutumista. Muutos on usein myös mahdollisuus niin yksilö- kuin organisaatiotasolla. Tätä seikkaa on syytä korostaa prosessin aikana.
2. Yhteisen vision luominen; kuva siitä, minkälainen malli tarvitaan muutoksen toteuttamiseen ja mitä muutos tuo tullessaan. Henkilöstöllä on usein hyviä näkemyksiä, joita tulee hyödyntää, jotta visiosta tulee realistinen.
3. Tulevan mallin ymmärtäminen ja ymmärryksen levittäminen: visiosta kertominen ja ”menestystarinan” luominen.
4. Riskianalyysin ja riskienhallintasuunnitelman laatiminen sekä riskeihin varautuminen hälventävät ennakkoluuloja sekä auttavat muutoksen läpiviennissä.
5. Lyhyen aikavälin onnistumisten suunnittelu (ns. ”quick wins”) tekee kokonaisuudesta helpommin hallittavan ja motivoi jatkamaan.
6. Lopullisten tavoitteiden saavuttamisen vaiheittainen suunnittelu.
7. Muutoksen läpivienti (muutosprojektin toteutus) ilman viivytyksiä vähentää syntyvää epävarmuutta.
8. Muutoksen vakiinnuttaminen; prosessien mukauttaminen osaksi arjen toimintaa.

Muutosprosessissa on oleellisista tunnistaa muutoksen vaikutukset ja sen aikaansaamat toimenpiteet. Muutoksen johtaminen kokonaisvaltaisesti varmistaa myös tietoturvatavoitteiden toteutumisen.

Muutokseen liittyvän epävarmuuden hallinnassa asiallisen, avoimen ja hyvin ajoitetun viestinnän tärkeyttä on syytä korostaa. Tiedotus hälventää muutokseen väistämättä liittyvää epätietoisuutta ja välinpitämättömyyttä, joka saattaa vaarantaa tietoturvallisuuden. Tiedotusvastuu suurista muutoksista kuuluu organisaation johdolle.

5 ULKOISTAMINEN KESKEISENÄ MUUTOSTEKIJÄNÄ JA SEN TIETOTURVAVAIKUTUKSIA

Tämä luku käsittelee ulkoistusta ja siihen liittyviä tietoturvallisuuden perusteita. Ulkoistuksen lyhyt historia antaa lukijalle ”syvyyttä” asian käsittelyyn ja akateemisessa tutkimuksessa esitettyjen asioiden ymmärtäminen puolestaan ”leveyttä”. Luvun loppupuolella esitellään konkreettisia tietoturva- ja muita hyötyjä ja haittoja, joita ulkoistamisesta saattaa seurata.

5.1 Yleistä ulkoistuksesta

5.1.1 Ulkoistuksen lyhyt historia

Ulkoistus (engl. *outsourcing*) on noussut liike-elämässä esille viimeisen parinkymmenen vuoden aikana. Tosiasiallista ulkoistamista on tehty tätä ennenkin, mutta ratkaisevaan muutokseen vaikutti kaksi seikkaa. Ensiksi yrityksissä alettiin entistä useammin arvioida, kannattaako jokin tuote tai palvelu valmistaa itse. Muutosajurina oli kustannustehokkuus *(make-or-buy* –analyysit), mutta myöhemmin kuvaan astuivat strategiset asiat. Vaikka oma valmistus saattoi olla kannattavaa lyhyellä aikavälillä, se ei ollut sitä pitkällä tähtäimellä. Pääomien vapauttaminen ja yleinen halu keskittyä ydinliiketoimintaan ajoivat organisaatioita yhä suurempiin ulkoistuksiin.

Toiseksi palvelua tai tuotetta ei ollut välttämätöntä tuottaa itse. Oli syntynyt yrityksiä, jotka kykenivät tekemään tämän. Näiden yritysten ydinliiketoiminta koostui juuri niistä toiminnoista, mitä asiakasyrityksissä ulkoistettiin.

Logistiikan ulkoistus on ehkä ensimmäinen laajasti ulkoistettu toiminto yksityisellä sektorilla. Tietotekniikka on seurannut samanlaista kehitystä kuin logistiikka aikoinaan. Aluksi yrityksillä oli omat osastonsa ja kalustonsa tätä varten, seuraavaksi ryhdyttiin

hankkimaan entistä enemmän ulkoisia palveluja ja lopuksi omasta palvelutuotannosta on luovuttu kokonaan. Vain suunnittelu, hankintaosaaminen ja johtaminen on jätetty itselle.

Julkishallinto on seurannut toiminnassa yksityistä sektoria. Perinteet omasta palvelutuotannosta ovat olleet vahvoja, eikä julkisella sektorilla ole mahdollista tehdä vastaavia nopeita järjestelyjä kuin yksityisissä yrityksissä. 1980-luvulla Iso-Britanniassa julkissektoria ryhdyttiin voimakkaasti yksityistämään ja ulkoistamaan. Syyt olivat etupäässä ideologiset, mutta myös käytännölliset. Suomessa kuntien palvelutuotannossa ostopalvelujen (siis palvelujen tuotannon osittainen ulkoistaminen) on ollut esillä jo 1970-luvulta saakka ja aiheuttanut ajoittain kiivasta keskustelua.

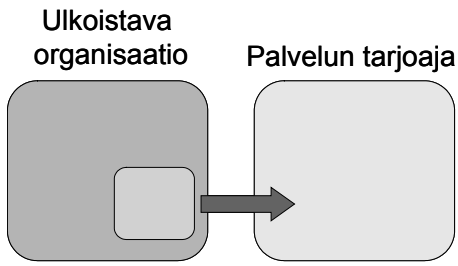
Insourcing tarkoittaa palvelun tuotannon keskittämistä konsernin sisällä palveluntuotantoon erikoistuneeseen yksikköön. Termiä käytetään toisinaan outsourcing termin vastakohtana eli palvelutuotannon ottamisella takaisin omaan organisaatioon.

5.1.2 Erilaisia ulkoistuksia

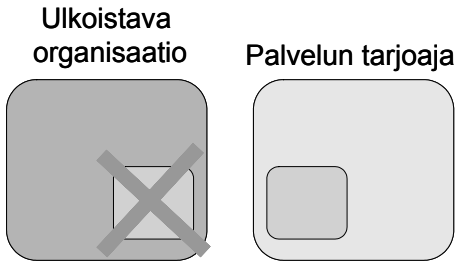
Tässä raportissa käytetään termiä *ulkoistaja* toimeksiantajasta ja *(ulkoistus)palvelun tarjoaja* siitä, joka ulkoistajan lukuun tuottaa palvelua. Perinteistä teollisuudessa yleistä käsitettä *alihankkija* on vältetty, sillä ulkoistukset ovat usein laajoja, pitkäaikaisia suhteita.

Ulkoistuksista on olemassa erilaisia variaatioita, jotka voidaan luokitella esimerkiksi seuraavalla tavalla:

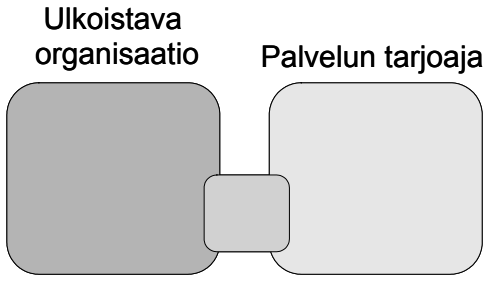
1) Ulkoistus, jossa resursseja (omaisuus ja ihmiset) siirtyy ulkoistajalta ulkoistuspalveluja tuottavalle yritykselle



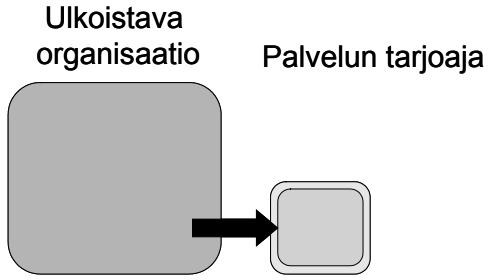
2) Ulkoistus, jossa resurssien siirtoa ei tapahdu



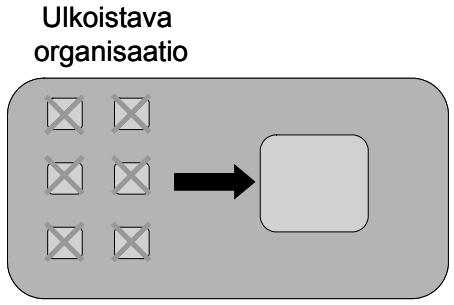
3) Ulkoistus yhteisyritykselle



4) Ulkoistus perustettavaan uuteen yritykseen (spin-off -tyyppinen)



5) Ulkoistus konsernin sisällä (Group outsourcing tai insourcing).



5.1.3 Ulkoistuksen hyödyistä ja haitoista

Oikein tehdyllä ulkoistuksella on saavutettavissa merkittäviä hyötyjä. Tällaisia ovat:

1. Keskittyminen omaan ydinliiketoimintaan vapauttaa pääomia sen kehittämiseen joka puolestaan mahdollistaa palvelun laadun parantamisen, resurssien paremman allokoinnin ja muita tavoiteltavia asioita.
2. Kustannusten aleneminen. Ulkoistuspalveluja tarjoavat yritykset voivat saavuttaa mittakaavaetuja tarjoamalla samanlaisia palveluita useille yrityksille.
3. Kustannukset ovat paremmin hallittavissa, kun aiempaa suurempi osa tuotteen tai palvelun kokonaiskustannuksista on sisällytetty tuotteen hintaan. Tällöin tuotannon vaatimia yleiskustannuksia ei ole tarpeen jakaa tuotteille jyvittämällä, *management-fee:* nä tai muuten.
4. Ulkoistuspalveluja tarjoava yritys kykenee paremmin seuraamaan teknistä kehitystä ja osallistumaan toimialajärjestelyihin.
5. Ulkoistuspalveluja tarjoava yritys on usein houkuttelevampi työnantaja ja kykenee rekrytoimaan ammattitaitoista työvoimaa. Tämä pätee erityisesti osaamisintensiivisiin tuotannonaloihin, kuten IT-palveluihin.

Ulkoistus on ”arkipäiväistynyt”, eikä sitä enää koeta yhtä pelottavaksi kuin vielä joitain vuosia sitten.

Off-shoring on tuotannon siirtämistä ulkomaille, *near-shoring* lähialueille.

Ulkoistuksen yhteydessä puhutaan usein tuotannon siirtämisestä halvemman työvoiman maihin eli *off-shoring*:sta. Mikäli kohdemaat sijaitsevat maantieteellisesti lähellä, puhutaan *near-shoring*:sta. Amerikkalaisessa liike-elämän lehdissä ulkoistusta *(outsourcing*) ja *off-shoring*:a käsitellään tavallisesti samassa yhteydessä; ellei aivan synonyymeinä niin ainakin saman asian kääntöpuolina.

Yritysten verkottuminen on lisääntynyt myös ulkoistuksen avulla: palvelun tuottaja saattaa ulkoistaa edelleen osia ulkoistetuista palveluista. Tällä seikalla on tietoturvallisuuden kannalta merkitystä, joten asiaa käsitellään myöhemmin tässä ohjeessa.

Kokemukset ulkoistuksesta eivät ole aina pelkästään hyviä. Erään arvovaltaisen arvion mukaan noin puolet suurista ulkoistuksista ovat menestyksekkäitä, viidennes osittaisia onnistumisia ja jopa 30 % on eriasteisia epäonnistumisia[11]

Suomessa tilanne lienee edellä kuvattua parempi. Tutkimuksen mukaan[12] IT-ulkoistuksissa suurin osa odotettavista hyödyistä toteutuu. Vain kustannussäästöt näyttävät te-

[11] McKinsey Quarterly, February 2005: Outsoursing Grows Up. Tutkimuksen kohteena olivat erittäin suuret ulkoistukset (sopimuksen arvo yli 20 mrd USD) Yhdysvalloissa vuosina 2001-2005. On luultavaa, että epäonnistumisen riskit tällaisissa erittäin suurissa sopimuksissa ovat oleellisesti suuremmat kuin pienissä.

[12] Market-Visio: IT-ulkoistamisen hyödyt ja haasteet, 12/2003.

kevän poikkeuksen. Kustannusten parempi hallittavuus ei myös usein toteudu odotetulla tavalla, joten esimerkiksi kilpailukyvyn odotetussa parantumisessa joudutaan toisinaan pettymään.

Ulkoistuksesta saatavien hyötyjen määrä on sidoksissa asiakkaiden ja toimintaympäristön muutokseen. Toimittajat pyrkivät vakioimaan palveluitaan (konseptointi), jotta palveluista saadaan tehokkaita ja tasalaatuisia. Mikäli asiakkaiden tarpeet muuttuvat nopeasti on helposti edessä tilanne, jossa tuotetaan tehokkaasti asiakkaiden uudistuneita tarpeita vastaamatonta palvelua.

Ulkoistuksen hyödyt toteutuvat vuosien kuluessa, sillä kyseessä on strateginen päätös. Etenkin ensimmäistä kertaa ulkoistettaessa saattaa ulkoistusprosessin alku (yleensä projektina toteutettava osuus) olla kivulias ja oletettua kalliimpi.

Ulkoistuksen potentiaaliset hyödyt jäävät toisinaan saavuttamatta, kun työntekijöiden siirtoa ulkoistuspalveluita tarjoavan yrityksen palvelukseen ja muita henkilöstömuutoksia ei kunnolla suunnitella. Mikäli ulkoistuksen seurauksena ”vapautuville” henkilöstöresursseille ei ole vaihtoehtoista, tuottavaa käyttöä tai ulkoistuksen hallinnasta tehdään liian raskas on mahdollista, että seurauksena on uusi ”välikerros” organisaation ja toimittajan välissä.

5.2 Ulkoistuksen yleisiä tietoturvavaikutuksia

Tietoturvallisuuden kannalta ulkoistus merkitsee muutosta. Muutos voi olla kohti parempaa tai huonompaa; vaikutukset ovat tapauskohtaisia. On olemassa eräitä yleisiä tietoturvallisuuteen vaikuttavia seikkoja, jotka vaikuttavat useimmissa ulkoistuksissa.

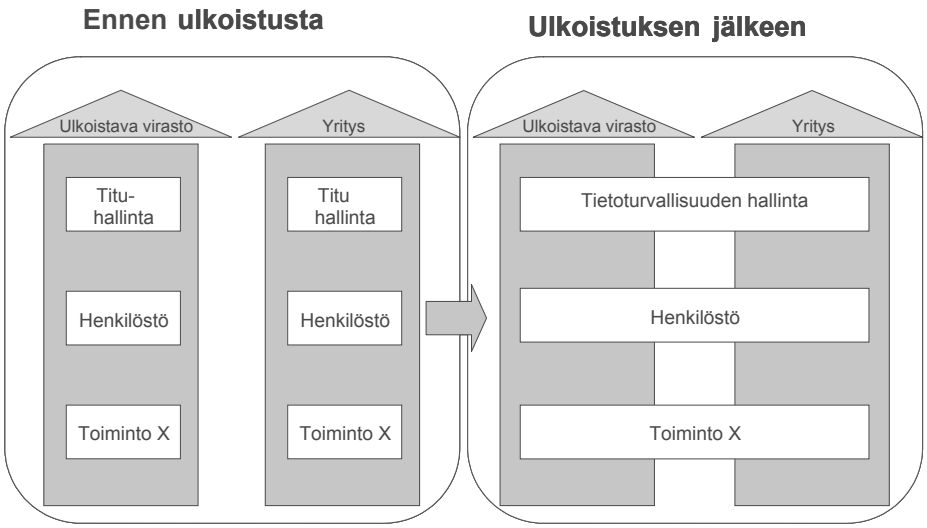
Ulkoistuksen tietoturvavaikutukset riippuvat ratkaisevasti siitä, minkä tyyppistä hankittava palvelu on. Työpaikkaruokalan ulkoistus tai tietohallinnon tärkeimpien toimintojen hankkiminen palveluna ovat niin erilaisia tapahtumia, että niiden käsittely samassa yhteydessä on luonnollisesti vaikeaa. Kussakin tapauksessa on kohteesta riippuvia erityispiirteitä, jotka tulee hallita. Tässä apuna voi käyttää VAHTI-ohjeita, Internetistä saatavia tarkistuslistoja tai alan ammattikirjallisuutta.

Vastuuta ei voi ulkoistaa. Vastuu tietoturvallisuudesta jää ulkoistavan organisaation johdolle. Sen on kyettävä varmistamaan vaadittava tietoturvataso koko ulkoistusprosessin ajan, eli tarjouspyynnöistä ulkoistuksen tuotantovaiheeseen asti.

5.2.1 Riippuvuuden lisääntyminen

Ulkoistaja tulee riippuvaiseksi palvelun toimittajasta ainakin suoranaisen ulkoistetun palvelun osalta, mutta mahdollisesti myös laajemmin (kuva 2). Palveluntarjoajan mahdolliset taloudelliset, toiminnalliset tai muut vaikeudet heijastuvat tarjottavaan palveluun ja tätä kautta suoraan ulkoistajan toimintaan.

Kuva 2. Ulkoistuksen yleisiä vaikutuksia.



Riippuvuuden lisääntymisen aiheuttamien riskien hallinta on vaikeaa, ehkä vaikeampaa kuin muiden ulkoistukseen liittyvien tietoturva-asioiden. Ulkoistuksessa pyritään yleensä suurten selkeiden kokonaisuuksien ulkoistamiseen, joten yleensä ulkoistetaan koko toiminto[13] tai ainakin mahdollisimman suuri osa siitä. Kahden rinnakkaisen toimittajan kanssa tehtävät sopimukset eivät tällöin yleensä tule kyseeseen, vaan toimittajien määrä supistuu yhteen.

Tarjouskilpailuvaiheessa riippuvuuden lisääntymisen hallintakeinot painottuvat toimittajan arviointiin. On parempi tulla riippuvaiseksi vakavaraisesta, voitollisesta yrityksestä kuin huonossa taloudellisessa tilanteessa olevasta. Tämän seikan tarkastamiseen velvoittaa myös hankintoihin liittyvä lainsäädäntö. Yleisten taloudellisten arviointikohteiden (vakavaraisuusaste, liiketoiminnallinen tulos ja omistus) lisäksi toimittajan kyky aitoon yhteistyöhön määrittelee pitkälti, onko kyseessä riippuvuussuhde vai kumppanuus. Mikäli ulkoistuspalveluita tarjoava yritys on kannattava, sen tase vahva ja omistajat sitoutuneita pitkäaikaiseen sijoitukseen, on arvioitavissa yrityksen olevan toiminnassa vielä vuosienkin jälkeen. Globaalissa taloudessa maayhtiön hyvä tilanne ei kuitenkaan välttämättä ole tae koko konsernin vakaasta taloudellisesta tilanteesta, eikä konsernin hyvä taloudellinen tilanne vastaavasti takaa maayhtiön tulevaisuutta.

[13] Kokonaisen toiminnon tai prosessin ulkoistuksesta käytetään lyhennettä BPO (*Business Process Outsourcing*). Maailmanlaajuisesti yleisimpiä ulkoistettuja toimintoja ovat logistiikka, asiakaspalvelu ja eräillä toimialoilla valmistava tuotanto.

Esimerkki: *Organisaatio Y on ulkoistanut toimintaansa liittyvän palvelun ASP-toimijalle, joka tarjoaa samaa palvelua myös muille asiakkailleen. Y oli aikanaan mukana kyseisen palvelun kehittämisessä. Palvelu on muuttumassa organisaation kannalta entistä tärkeämmäksi. Palvelun jatkuvuuden varmistamiseksi ja oman toimintansa turvaamiseksi organisaatio ja ASP-toimija kehittävät palvelua yhteistyössä entistä käyttövarmemmaksi ja tietoturvallisemmaksi. Organisaatio on hyötynyt edelläkävijän asemastaan.*

Esimerkki: *Maayhtiö toteutti asiakkaalle sovellusmäärittelyn. Emoyhtiön joutuessa taloudellisiin vaikeuksiin se pumppasi maayhtiön varoja omaan toimintaansa, jolloin maayhtiö joutui kustannussyistä erottamaan palveluksestaan keskeisiä asiantuntijoita. Toiminnan loppuvaiheessa maayhtiö ei kyennyt vastaamaan taloudellisista ja muista velvoitteistaan konsernin toiminnan lakatessa. Sovelluksen toteutus keskeytyi ja toimittajan vastuiden ja velvoitteiden selvittäminen sekä vahingonkorvausten saaminen sopimussuhteen kariutuessa osoittautui erittäin haastavaksi.*

IT-toimintojen ulkoistuksen uudessa kilpailutuksessa on usein ongelmana, että nykyisestä toimittajasta ollaan liian riippuvaisia. Tarjouskilpailussa muilla tarjokkailla ei katsota olevan käytännön mahdollisuuksia. Tämä puolestaan johtaa toisinaan tilanteisiin, joissa varteenotettavia kilpailevia tarjouksia ei saada. Lisäksi ulkoistajan kannalta huolena on nykyisen toimittajan toiminta sopimuskauden loppuvaiheessa, mikäli ulkoistussopimusta ei jatketa. Entisen palveluntuottajan tekemä siirtokustannusten liioittelu tai haluttomuus yhteistyöhön palvelun siirtyessä uudelle toimittajalle voivat hankaloittaa toimintaa.

Ulkoistettavan toiminnon tai palvelun tarkka määrittely ulkoistuksen alussa ja määrittelyn ylläpito ulkoistussopimuksen aikana ovat tärkeitä. Mitä paremmin toiminto – erityisesti sen liittymät – on kuvattu ja dokumentoitu, sitä paremmin sen siirto toiselle palveluntoimittajalle onnistuu.

Esimerkki: *Yritys Y oli ulkoistanut erään keskeisen tietojärjestelmänsä kokonaisuudessaan ASP-toimijalle. ASP-toimija puolestaan hankki käyttöpalveluja, tietoliikenne- ja muita tärkeitä alihankkijoiltaan ja nämä taas kriittisiä palveluita omiltaan. Vaikka kaikki toimivat tietoturvallisesti – osa jopa erinomaisen hyvin – oli kokonaisuuden kannalta ongelmana vastuiden määrittely ja yhteistyö mahdollisissa kriisitilanteissa. Vastuista sopiminen, yhteystietojen jako ja eräät menettelytapoihin liittyvät sopimukset paransivat tilannetta olennaisesti.*

Liiallista riippuvuutta voidaan vähentää myös prosessien kehittämisellä vakioiduiksi. Selkeisiin, hyvin toimiviin ja kuvattuihin prosesseihin perustuva toiminta on helpompi siirtää toiselle toimittajalle ja mahdollistaa myös osaltaan hyvän tarjouspyynnön laatimisen.

Liiallista riippuvuutta voidaan alusta alkaen pienentää arvioimalla tarjouspyynnössä toimittajan kykyä siirtää ulkoistus toiselle toimittajalle. Tarjouspyynnön referenssit-koh-

dassa voidaan pyytää toimittajaa luettelemaan menestyksellisesti hoidetut ulkoistuksen siirrot sekä toimittajalle että toimittajalta pois. Mikäli jälkimmäiseen kohtaan ei löydy yhtään tapausta on arvioitava, eikö toimittajalla ole yhtään päättynyttä ulkoistussopimusta vai eikö ulkoistussopimuksia ole osattu siirtää uudelle toimittajalle.

Vaikka ulkoistuksessa toimintoja ja näihin liittyvää osaamista siirtyy muualle, on ulkoistettujen toimintojen johtamisen ja niiden hankkimisen kannalta välttämätön osaaminen säilytettävä organisaation sisällä.

Osaamisen liiallinen siirtyminen pois ulkoistusta hankkivasta organisaatiosta on riski, johon on varauduttava ulkoistusprosessin alussa. Vuosien aikana karttuneen asiantuntemuksen menettäminen on paljon helpompaa kuin sen hankkiminen, joten keskeisten henkilöiden nimeäminen on suositeltavaa tehdä ulkoistusprosessin alussa. Näille henkilöille voidaan antaa koulutusta, joka lisää organisaation valmiuksia ulkoistukseen liittyvän riippuvuuden lisääntymisen hallinnassa.

5.2.2 Vastuunjaon selkeyden merkitys

Lopullinen vastuu toiminnasta säilyy aina ulkoistavalla organisaatiolla. Tämä on seikka, joka on syytä pitää mielessä, vaikka vastuita voidaan ja niitä tulee jakaa ulkoistuksen yhteydessä uudelleen. Ulkoistuspalveluita tarjoava yritys sitoutuu tiettyyn palvelutasoon, joka vaikuttaa olennaisesti palvelun käytettävyyteen. Ulkoistajan on kuitenkin määriteltävä nämä tasot ja valvottava niiden toteutumista.

Sovittaessa palvelutasosta, hinnoista ja muista seikoista on syytä sopia myös vastuunjaon yksityiskohdista. Käytännössä esiintyy tilanteita, joissa vastuiden harmaat alueet aiheuttavat ongelmia. Ulkoistuspalvelun asiakas olettaa vastuun jostain kokonaisuudesta olevan toimittajalla, koska asiasta ei ole erikseen sovittu. Toimittaja puolestaan olettaa samasta syystä vastuun olevan asiakkaalla.

Siirtyminen yksittäisten asioiden ulkoistuksista suurempiin kokonaisuuksiin helpottaa vastuunjakoon liittyvää problematiikkaa. Sopimusten auditointi, selkeät määrittelyt vastuista ja osapuolten välinen jatkuva kommunikaatio auttavat. Laajoja asioita mittaavien palvelutasomittarien kehittäminen on myös kannatettavaa.

Vastuunjaon merkitys tulee korostumaan monitoimittajaympäristöissä ja erilaisissa verkostoissa. On syytä määritellä mahdollisimman yksiselitteisesti mikä on toimittajan vastuu, kun kolmannen osapuolen tarjoama palvelu häiriintyy. Suomen lainsäädännön mukaan toimittaja vastaa yleensä alihankkijoidensa toiminnasta kuin omastaan[14].

Monitoimittajaympäristöt yleistyvät. Tietoturvallisuuden kannalta vastuun jaon selkeyden merkitys korostuu. Toimittajien väliset vastuut – rajapinnat – on kirjattava sopimuksiin tai niistä on muuten sovittava yksiselitteisesti ja selkeästi. Yhteiset työryhmät tai

[14] Lisää ulkoistussuhteen vaikutuksista vastuukysymyksiin Jarkko Kiihan teoksessa Yritystoi-minnan ulkoist14aminen ja sopimusvastuu, Kauppakaari 2002.

palvelun seurantapalaverit ovat tilaisuuksia, joihin kannattaa kutsua edustajia useammalta kuin yhdeltä toimittajalta.

Monitoimittajaympäristössä turvallisuussopimusten ja kolmansien osapuolten tekemien auditointien merkitys on suurempi kuin perinteisissä toimittajamalleissa. Ensikäden auditointien tekoon ei yleensä ole resursseja eikä aina edes osaamista, joten joudutaan turvautumaan ulkopuolisten tekemiin auditointehin ja turvallisuussopimuksiin. Turvallisuussopimuksessa toimittajaosapuoli sitoutuu normaaliin sopimusvastuuseen tilaajan esittämistä vaatimuksista. Vaatimusten tulee olla selkeitä ja mahdollisia toteuttaa. Vakiomuotoinen menettely edesauttaa sopimusten solmimista.

5.2.3 Henkilöstöön liittyvät asiat

Ulkoistuksessa tapahtuu usein henkilöiden siirtymistä toisen organisaation palvelukseen vaikka tehtävät pysyvätkin. Aikaa myöden on tavallista, että henkilöt vaihtuvat ja ulkoistuspalveluita tarjoava yritys tuo tilalle uusia. Vaihtuvuus saattaa olla joskus tiheääkin. Ulkoistavan organisaation on varattava itselleen oikeus taustatarkistuksiin, henkilöiden haastatteluun ja henkilökohtaisten turvasopimusten solmimiseen. Ulkoistuspalveluita tarjoavan yrityksen vakuutus henkilökunnan luotettavuudesta on normaali rutiininomainen menettely, jonka paikkaansa pitävyyttä tulee tarkistaa pistokokein.

> ***Esimerkki:*** *Pienehkö yksikkö X päätti osittain ulkoistaa lähituen ja palvelinten ylläpidon. Palvelimia ei siirretty pois toimipisteestä, vaan paikallinen palveluntarjoaja sitoutui tekemään ylläpitoa paikan päällä. Pääsy yksikön tiloihin oli tarkasti valvottua, mutta (ulkopuolisen yrityksen) ylläpitohenkilökunta tarvitsi pääsyn tiloihin. Jatkuva valvonta ei ollut käytännössä mahdollista, sillä palveluntarjoajan henkilövaihtuvuus oli kohtuullisen suuri (paljon opiskelijatyövoimaa). Sovittiin, että pääsy toimipisteeseen on vain kahdella toimittajan edustajalla, jotka tunnettiin henkilökohtaisesti. Näiden kanssa laadittiin henkilökohtaiset sopimukset ja lisäksi sovittiin, että muita toimittajan henkilöitä saa käyttää vain, mikäli asiasta erikseen sovitaan. Ulkoistaja tiedosti, että menettely saattoi johtaa lievään palvelutason heikentymiseen.*

Usein toistetun lausuman mukaan suurin osa tietoturvallisuuden uhista tulee organisaation sisältä. Ulkoistuksen yhteydessä sisäisen uhan lähteet muuttuvat: ulkoistuspalveluita tarjoavan yrityksen henkilöistä tulee ainakin osittain ”talon omaa väkeä”. Mahdollinen tyytymättömyys työnantajaorganisaatioon, puutteellinen tietotaso tai heikko tietoturva-asenne saattavat vaarantaa ulkoistuspalveluiden asiakkaan tietoturvallisuuden. Ulkoistetun toiminnon henkilöstö on otettava huomioon organisaation tietoturvakoulutusta suunniteltaessa.

5.2.4 Tietoturvallisuuden erityisosaaminen ja työkalut

Tietoturvallisuuteen liittyvät tekniset asiat vaativat erityisosaamista, jota on ylläpidettävä jatkuvasti. Tietoteknisten laitteiden ja ohjelmien toimittajilla on omia osaamissertifikaatteja, joita myönnetään kyseisten ohjelmien ja laitteiden käytön hyvin hallitseville osaajille. Sertifioitujen henkilöiden ja muiden osaajien rekrytointi on ulkoistuspalveluiden tarjoajalle helpompaa kuin muille yrityksille.

Tietoturvallisuuden toteuttamisessa käytettävien laitteiden, ohjelmien ja muiden välineiden hallinta saattaa olla hankalaa ja niiden asentaminen ja lisensiointi kallista. Ulkoistuspalveluiden tarjoajat voivat jakaa nämä kustannukset asiakasyritystensä kesken ja hyödyntää siten välineitä tehokkaalla tavalla.

5.2.5 Kansainvälistymiskehityksen vaikutukset

Tietoturvallisuus on kansainvälistä ja nopeasti muuttuvaa. Uhat tulevat entistä nopeammin ja vastakeinojen on oltava käytössä nopeasti. Ulkoistuspalveluita tarjoavat yritykset kykenevät seuraamaan yleistä tilannetta asiakkaitaan paremmin, mutta toimialakohtaisten erityisvaatimusten osalta näin ei aina ole.

5.3 Ulkoistamisen tietoturvariskit ja -mahdollisuudet

Ulkoistus ei tietoturvallisuuden kannalta sinänsä merkitse heikennystä tai parannusta, mutta eräät riskit ja mahdollisuudet toistuvat.

Tietoturvallisuutta parantavat yleensä seuraavat tekijät:

- Toimittajalla on yleensä hyvä erityisosaaminen tietoturvallisuuden teknisistä asioista, mikäli nämä eivät ole harvinaisia tai vain ulkoistuksen kohteeseen liittyviä. Käyttöpalveluita tarjoava yrityksellä voidaan hyvällä syyllä olettaa olevan kykyä hallita palomuurit, virustorjunta, varmistukset ja muut vastaavat tekniset asiat. Taloushallinnon ulkoistuspalveluyritys on todennäköisesti kehittänyt järjestelmät, joilla vaarallisia työyhdistelmiä vältetään ja joilla tarkistetaan työntekijöiden luotettavuus.
- Mittakaavaedut tuovat etua myös tietoturvallisuuden kannalta. Toimittajan henkilöstö oppii ja rutinoituu ja toimittajalle on järkevää kouluttaa henkilökuntaa tietoturva- ja muissa asioissa. Mittakaavaetujen ansiosta eräät kalliit tietoturvaratkaisut tulevat halvemmiksi toteuttaa, kun toimintoja on keskitetty yhdelle toimittajalle.
- Osaaminen on kriittinen menestystekijä tietoyhteiskunnassa ja osaavien henkilöiden rekrytointi on entistä tärkeämpää. Ulkoistuspalveluja tarjoavat yritykset ovat tietoturva- ja IT-ammattilaisille houkuttelevia työpaikkoja; ne tarjoavat kiinnostavia uramahdollisuuksia.

Ulkoistukseen liittyvistä riskeistä monet kytkeytyvät siihen, että ulkoistaja menettää osan kontrollistaan. Palvelua ei enää kyetä valvomaan tutuilla tavoilla, vaan siihen tarvitaan kolmatta osapuolta.

Ulkoistuspalvelujen toimittaja ei yleensä ole selvillä ulkoistuksen kohteen tietoturvallisuuden erityiskysymyksistä, vaan ulkoistajan on kerrottava ne erikseen. Dokumentoimattomat asiat eivät välity, sillä tietoturvallisuutta ei ulkoistuksen yhteydessä useinkaan käsitellä erillisenä kysymyksenä.

> ***Esimerkki:*** *Yritys oli ulkoistanut osan taloushallinnostaan ASP-palveluksi. Huomattiin, että eräällä varmuuskopiolla oli sinne kuulumatonta aiheistoa, joka oli suojaamatonta ja helposti palautettavissa luettavaan muotoon. Aineisto kuuluu eräälle toiselle yritykselle, joka oli myös ulkoistanut toimintojaan samalle ASP-palvelujen tarjoajalle. Varmuuskopiointiin käytettyjä tietovälineitä ei käsitelty oikein, vaan luottamuksellisuus vaarantui.*

5.4 Edellytykset ulkoistamisen tietoturvariskien käsittelylle

Ulkoistuksen tietoturvallisuuden hallinnan kannalta keskeisessä asemassa ovat:

1. ulkoistavan organisaation tietoturvallisuuden hallinta
2. ulkoistettavan kohteen tietoturvallisuuden erityisasiat
3. ulkoistuspalveluita tarjoavan yrityksen tietoturvallisuuden hallinta
4. kummankin organisaation kyky muutoshallintaan
5. toimittajan ja ulkoistajan kyky yhteistoimintaan eli kohtien 1 ja 3 välinen kommunikaatio.

Kohtien 1 ja 3 arvioinnissa voidaan hyödyntää vastaavaa laadittua VAHTI-ohjetta Tietoturvallisuuden hallintajärjestelmän arviointisuositus (VAHTI 3/2003).

Ulkoistavalle yksikölle ulkoistus saattaa olla ensimmäinen laatuaan, mutta ulkoistuspalveluita tarjoavalle ei. Tilannetta voidaan helpottaa käyttämällä ulkopuolista konsulttia, jolla on tietoturvaosaamista. Ulkoistavan organisaation tietoturvallisuuden kokonaistila vaikuttaa onnistumiseen, mutta kaikkein keskeisintä on kyetä määrittelemään ulkoistettava kohde etenkin tietoturvallisuuden erityistekijöiden osalta. Lisäksi tulee hahmottaa asiakkaan kyky kyetä yhteistoimintaan ulkoistuspalvelujen tarjoajan kanssa. Tietoturvallisuudessa iso osa asioista on dynaamisia, nopeasti muuttuvia tai entuudestaan tuntemattomia, jolloin on kyettävä nopeaan hyvin koordinoituun toimintaan.

Mikäli kohta 2 sisältää tietojärjestelmiin tai tietohallintoon liittyviä toimintoja, tietoturvallisuuden arviointi on tehtävä viimeistään ulkoistusta suunniteltaessa. On kohtuutonta olettaa, että toimittaja olisi entuudestaan selvillä ulkoistettavan kohteen tietoturvallisuuden erityiskysymyksistä - etenkin mikäli kohde ei ole täysin vakioitu, yleisessä käytössä oleva ja yksinkertainen.

6 PROSESSIEN KEHITTÄMINEN JA MUUTOKSET

Tässä luvussa käydään lävitse lyhyt esittely prosessiajatteluun sekä kuvaus eräistä tavanomaisista tietoturvaongelmista, joita prosessiajattelun soveltamisella voidaan ratkaista. Lisäksi tarkastellaan esimerkin avulla kuinka prosessien kehittämisessä usein käytettyä työvälinettä voidaan hyödyntää tietoturvallisuuteen liittyen. Prosessien kehittämisessä lähdetään liikkeelle nykyisistä prosesseista, kuvataan millaisia ne ovat tavoitetilassa ja lopuksi suunnitellaan, miten tavoitetilaan siirtymisen edellyttämä muutos toteutetaan.

Prosessilla tarkoitetaan toimintoketjuja, jotka tähtäävät sisäisen tai ulkoisen asiakkaan tarpeen tyydyttämiseen, ja jotka ovat säännöllisesti toistuvia ja yleensä vakioituja.

6.1 Yleistä prosesseista

Prosessien kehittämisellä tarkoitetaan organisaation toiminnoista muodostuvien toimintoketjujen kokonaisvaltaista kehittämistä. Tavoitteena on prosessien tuoman hyödyn maksimointi sekä niiden kustannusten ja suorituskyvyn optimointi. Tässä yhteydessä muutos tarkoittaa prosessien kehittämistä, jolloin siihen osallistuvien henkilöiden ja tietojärjestelmien työnkulut, roolit ja tehtävät saattavat muuttua.

Prosessi alkaa asiakkaan tarpeesta ja päättyy sen tyydyttämiseen. Osapuolia ja tehtäviä voi olla useita tai vain yksi. Perinteisesti prosessien kuvaamisessa on pitäydytty oman organisaation sisäisissä työnkuluissa, mutta viime vuosina on pyritty kehittämään organisaatiorajat ylittäviä prosesseja. Verkottumisen yleisiä vaikutuksia on käsitelty toisaalla tässä ohjeessa.

Tietojärjestelmien tarjoaman tuen huomiointi on keskeistä prosessien kehittämisessä. Tämä korostuu organisaatiorajat ylittävissä prosesseissa, joissa myös tietoturvanäkökulma tulee korostetusti esiin. Lisäksi prosessin toimivuuden ja kustannustehokkuuden kannalta tietotekninen lähestymistapa on keskeinen. Tulee kuitenkin pitää mielessä, et-

tä prosesseja kehitetään ensisijaisesti lähtien liikkeelle muuttuvien toimintojen tarpeista – ei tietojärjestelmien.

> ***Esimerkki:*** *Vanginvartijan tehtävänä on huolehtia siitä, että vanki suorittaa rangaistuksensa siten kuin lainlaatija on tarkoittanut ja tuomioistuin määrännyt. Tavoitetta edesauttaa se, että vartija saa käsiinsä olennaisen tiedon vangin tuomiosta ja rikoshistoriasta. Nämä tiedot tallennetaan muualla kuin vankienhoitolaitoksessa (poliisi ja tuomioistuinlaitos), joten tukiprosessin kehittäminen vaatii organisaatiorajat ylittävää viranomaisyhteistyötä. Vankia koskevat tiedot ovat arkaluonteisia, joten niiden tietosuojaan on kiinnitettävä erityistä huomiota. Tietojen siirto on sallittu vain lain sallimissa tapauksissa, joten edellä kuvatun organisaatiorajat ylittävän prosessin toteutus on vaatinut sen laillisuuden selvittämistä.*

Lähtötilanne prosessien kehittämisessä vaihtelee voimakkaasti, mikä luonnollisesti vaikuttaa prosessien kehittämishankkeen läpivientiin ja tuloksiin. Myös tietoturvallisuuden kannalta erot kehitysasteissa ovat suuria. Seuraavassa on kuvattu jaottelu, jota voidaan hyödyntää lähtötilanteen arvioinnissa:

1) **Prosessiajattelu on organisaatiolle tuntematon.** Prosesseja ei ole lainkaan määritelty eikä dokumentoitu ja prosessiajattelu on tuttua vain johdolle. Tietoturvallisuuden kannalta kriittisiä toimintoja ei ole kuvattu, eikä aina edes tunnistettu. Tällaisessa vaiheessa olevan palvelun tai toiminnon ulkoistaminen on iso riski niin ulkoistajalle kuin ulkoistuspalveluita tarjoavalle yritykselleKin.
2) Toiminnan **ohjaaminen perustuu prosessiin osallistuvien toimintojen tavoitteisiin,** jotka voivat olla prosessin kriittisten menestystekijöiden toteutumisen kannalta ristiriitaisia. Toiminnoittain tapahtuva johtaminen aiheuttaa informaatiokatkoksia toimintojen välillä ja estää prosessin tehokkaan toteuttamisen.
3) **Prosessit on määritelty ja kuvattu,** mutta toiminta ei ole käytännössä prosessien mukaista. Se on joko muuttunut kuvaamisen jälkeen tai on kuvattu tavoitetilaiset prosessit, mutta näiden implementointi on jäänyt kesken. Muutoksen tietoturvallisuuden kannalta tämä saattaa olla jopa huonompi tilanne kuin prosessien kuvaamattomuus mikäli ero todellisten ja kuvattujen prosessien välillä on suuri. Prosessikuvausten saattaminen ajan tasalle ennen ulkoistusta tai muuta muutosta on välttämätöntä.
4) **Prosesseissa ei kyetä hyödyntämään** käytössä olevan tietojärjestelmän tarjoamia mahdollisuuksia. Tällöin prosessien kehittämisessä kannattaa ehdottomasti kartoittaa tietojärjestelmän täysimittaisen hyödyntämisen mahdollisuus. Tietoturvan kannalta tilanne ei ole yhtä huono kuin edellä kuvatut vaiheet; käyttämättömät ominaisuudet saattavat sisältää tosiasiallisen ”takaoven” ja niiden käyttöönotossa on syytä tehdä vastaavanlainen tietoturva-arviointi kuin uuden järjestelmän käyttöönotossa.
5) Tietojärjestelmien tarjoama tekninen ja toiminnallinen **tuki prosesseille on puutteellinen.** Tämä on tavallinen tilanne prosessien kehittämisessä ja seuraavana vaiheena on tietojärjestelmäkehityksen aloittaminen.

6.2 Prosessinkehittämisessä esiintyviä tietoturvaongelmia

Toimintaprosessien kehitysprojekteissa esiintyy monenlaisia ongelmia. Niistä osa liittyy tekniikkaan ja osa puolestaan ihmisiin.

Tulokset toimintatavan muutoksesta eivät näy heti, koska henkilöstö ei ole oppinut toimimaan tehokkaasti uudessa tilanteessa. Saatetaan toistaa vanhoja toimintatapoja tai käyttää ”oikopolkuja”. Tämä vaihe aiheuttaa monenlaisia tietoturvariskejä: henkilöillä ei ole riittäviä oikeuksia tai niitä on liikaa edellisten tehtävien peruna.

Uuden teknologian käyttöönotossa ilmenee usein vaikeuksia. Tietoa voi hukkua, sitä voi päätyä väärille henkilöille tai tieto ei saavuta oikeita henkilöitä. Luottamuksellisuus, käytettävyys ja eheys ovat kaikki vaarassa, mikäli käyttöönoton tietoturvallisuutta ei ole asianmukaisesti hoidettu.

Työntekijöillä voi toisaalta olla heikko motivaatio, esiintyy muutosvastarintaa tai suoranaista muutoksen torpedointia. Näillä seikoilla on prosessien kehittämisessä kenties suurempi vaikutus kuin muilla tekijöillä. Henkilöstön asenteiden merkityksen tärkeyttä on korostettu lukuisissa VAHTI-ohjeissa. Asenteet altistavat muille tietoturvallisuutta heikentäville uhille. Vastakeinoja on monia. Muutoksen tuomaa epävarmuutta voidaan hälventää viestinnällä ja koulutuksella. Etenkin ns. mielipidevaikuttajiin on oltava yhteydessä ja kyettävä löytämään muutosagentteja organisaation sisältä.

Aina ei ole löydettävissä halukkuutta toimia systemaattisesti, toimintoja ei ole harmonisoitu tai ei ole olemassa yhtenäistä tapaa syöttää informaatiota tietojärjestelmiin. Tämä aiheuttaa laaturiskin hallittavaan tietoon, etenkin sen eheyteen ja hyödynnettävyyteen.

Tietojärjestelmien heikko käytettävyys johtaa usein rinnakkaisten vaihtoehtoisten prosessien syntymiseen.

Vastuut ovat usein epäselviä. Väärät henkilöt saattavat käsitellä hyvässä uskossa asioita, jotka eivät heille kuulu. Tällöin luottamuksellisuus saattaa vaarantua.

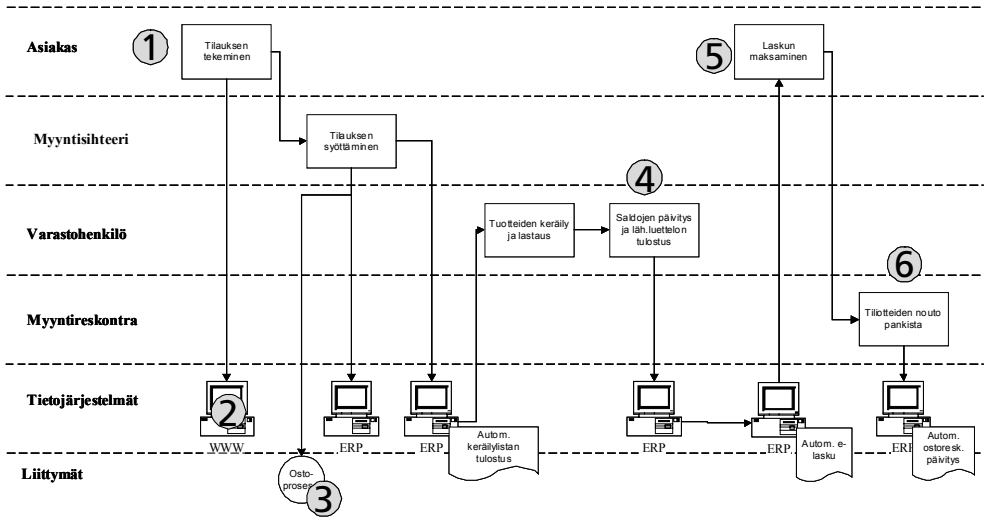
Prosessit ovat olemassa riippumatta siitä, onko ne tunnistettu ja kuvattu. Prosessien kehittämisen kannalta niiden kuvaaminen on hyvä keino. Se helpottaa kehittämistä erityisesti silloin, kun kehittämiseen osallistuu ulkopuolisia asiantuntijoita tai prosessien kehittämistä seuraa tietojärjestelmäkehityshanke.

6.3 Prosessien kuvaus

Prosessien kehittämisen yhteydessä ne myös kuvataan. Joskus voidaan tukeutua muussa yhteydessä tehtyihin prosessikuviin, mutta toisinaan taas kehitysprojektin luonteen vuoksi ei ole tarvetta erilliselle kuvaamiselle.

Tietojärjestelmähankkeen alkuun kuuluu siten usein toimintaprosessien kuvaaminen ns. uimaratakuviksi (ks. kuva 3). Tässä yhteydessä on syytä ottaa tietoturvanäkökohdat

Kuva 3. Prosessin (yleiskuva eräästä tilaus-toimitusprosessista tavoitetilassa) kuvaamisen yhteydessä on analysoitu prosessin kriittiset tietoturvakohdat (numerot). Kussakin kohdassa on arvioitu riskin todennäköisyys ja vaikutukset toteutuessaan, sekä arvioitu keinoja tärkeimpien riskien hallintaan. Numerot ovat tunnisteita ja numerointi etenee prosessin myötä. Koko tunnistenumero sisältää prosessin nimen (esim. TITO2) ja riskin tunnistenumeron (esim. TITO2-5).



huomioon. Tällöin analysoidaan, mitkä prosessin vaiheet ovat turvallisuuden kannalta tärkeimmät, miten niiden turvallisuus riippuu prosessin muista vaiheista ja miten ne itse vaikuttavat prosessin muihin vaiheisiin.

> ***Esimerkki:*** *Tietoturvanäkökohdat voidaan ottaa huomioon prosessien kuvaamisen yhteydessä joko heti kuvaamisen aikana tai arvioimalla asiaa jälkikäteen, kun kaikki on kuvattu.*

6.4 Muutoksen suunnittelun tulokset

Muutoksen huolellinen suunnittelu ja hyvin johdettu toteutus ehkäisevät tietoturvariskien konkretisoitumista. Suuret muutokset toteutetaan erillisenä projektina, pienemmät taas hoituvat muun toiminnan ohessa. Kenties kaikkein tärkein ohje muutoshallinnassa on suunnitella muutos hyvin ja tunnistaa tietoturvallisuuden riskitekijät ennakolta; mielellään erillisenä kohtana läpivientisuunnitelmassa.

Esimerkki: Suuri teollisuusyritys oli uudistamassa taloushallinnon keskeisintä tietojärjestelmää. Uusittu järjestelmä oli tarkoitus ottaa käyttöön yhdellä kertaa. Projektista tehtiin riskianalyysi, jossa tunnistettiin tärkeimmät riskit sekä suunniteltiin niiden hallinta. Tässä yhteydessä todettiin kokonaisuuden olevan niin mutkikas, ettei tehtyyn riskianalyysiin voi täysin luottaa. Tästä syystä ennen muutosprojektin alkua testattiin vanhan järjestelmän palautustoimet. Mikäli uusitussa järjestelmässä esiintyisi liikaa ongelmia, tultaisiin hätätapauksessa palaamaan vanhaan. Uusittu järjestelmä toimi eikä ongelmia esiintynyt. Toipumissuunnitelmien testaus antoi varmuuden, että toiminta voi jatkua, vaikka ennalta arvaamaton suuri riski toteutuisikin.

Organisaation strategian mukaiset kriittiset menestystekijät sekä mittarit on oltava dokumentoituna, jotta tietoturvakriittiset kohdat on mahdollista tunnistaa. Näin voidaan helpommin kohdentaa tietoturvatoimet oleellisten uhkien torjuntaan eikä tyytyä ”vakiouhkienvakiotorjuntaan”. Myös johdon todellinen sitoutuminen niin muutoksen läpivientiin kuin tietoturvallisuuteen on parempaa, kun molempien tekijöiden yhteys strategiaan on selkeä.

Tavoitetilan prosessit tulee olla hyvin kuvattuna ja ne tulee kuvata sillä tasolla, että kehittämishankkeen seuraava vaihe saa riittävät lähtötiedot. Tämä vaikuttaa etenkin järjestelmän sisältämien tietojen käytettävyyteen. Henkilö- ja muut luottamukselliset tiedot voidaan prosessikuvauksissa merkitä erikseen, sillä näitä käsittelevät vaiheet ovat tietoturvan toteutumisen kannalta tärkeitä.

Tavoitetilan mukainen organisaatio on oltava selvillä. Muutostilanne on aina otollinen hetki valmentaa henkilöitä tietoturva-ajatteluun. Kun tietoturvakriittiset kohdat on sisäistetty prosessikaaviotasolla, on kuvauksen pohjalta laadittavissa hyvin kohdennettu tietoturvan koulutusohjelma[15]. Koulutuksessa läpikäydään tietoturva-asiat nimenomaan prosessien näkökulmasta siten, että osallistujat sisäistävät oman roolinsa kokonaisuudessa.

Uutta toimintatapaa ja prosesseja tukeva integroitu järjestelmä saattaa olla uuden toimintatavan käyttöönoton edellytys. Tämä pätee etenkin organisaatiorajat ylittävissä, kokonaan tietotekniikan varaan rakennetuissa prosesseissa. Monet uudet palvelut eivät olisi lainkaan mahdollisia toteuttaa ilman tietotekniikkaa. Koska tietoa käsitellään yhä laajemmissa piireissä ja monipuolisemmin, on tietoturvanäkökulman oltava aina mukana[16].

Dokumentoidut nyky- ja tavoitetilan prosessikuvaukset on oltava käytettävissä, jotta henkilöstö sisäistää tehtävissä tapahtuneet keskeiset muutokset. Organisaation omat asiantuntijat laativat nykytilan prosessikuvaukset käyttäen mahdollisesti apunaan ulkopuolisia prosessien hallinnan asiantuntijoita. Vertailemalla tilannetta ennen muutosta ja muutoksen jälkeen on mahdollista alustavasti nimetä tietoturvakriittiset kohdat muuttuneessa tilanteessa.

---

[15] Lisätietoja koulutusasioista on ohjeesta Opas julkishallinnon tietoturvakoulutuksen järjestä-misestä (VAHTI 6/2003)

[16] IT-kehitystyön tietoturvallisuudesta katso Valtionhallinnon tietojärjestelmäkehityksen tieto-turvallisuussuositus (VAHTI 3/2000), etenkin luvut 5-7.

Tavallisesti valmistellaan dokumentoitu ja priorisoitu kehityssuunnitelma, joka perustuu nykytila-analyysiin ja kehitystavoitteisiin. Tietoturvan puutteet voivat toisinaan olla myös kaavailtua kehitystä estävänä tekijänä. Uuden toimintamallin käyttöönotto ei etene, jos johto pelkää luottamukselliseksi nimetyn tiedon joutuvan hallitsemattomasti kumppanin tai ulkopuolisen käsiin.

Yleensä laaditaan priorisoidut toimenpidesuositukset tavoitetilan toteuttamiseksi. Tämä kokonaisuus saattaa sisältää tietoturvasuunnitelman ja riskienhallintasuunnitelman. Prosessien kuvaamisen päätteeksi tehdään yleensä ehdotus hankkeen seuraavasta vaiheesta. Suunnitelmiin tulee sisällyttää jokaiseen vaiheeseen tietoturvasuunnitelma, jotta tietoturva-ajattelu etenee johdonmukaisesti työkulkuihin, sovelluksiin ja IT-infrastruktuuriin saakka.

7 SÄÄDÖKSET

Sähköisen asiankäsittelyn tietoturva- ja tietosuojauhkien ehkäisemiseksi on säädetty erikseen lainsäädäntöä, jota tulee ottaa huomioon aina kun sähköisesti tapahtuvaa asiakirjojen ja tietojen käsittelyä suunnitellaan ja toteutetaan. Ulkoistus ja muutoksen läpivienti ovat merkittävästi helpompia, mikäli lakiin pohjautuvat velvoitteet on hoidettu ja tieto näistä voidaan välittää ulkoistuspalveluita tarjoavalle yritykselle.

Ei ole syytä olettaa, että yksityinen yritys tuntee julkista sektoria koskevaa lainsäädäntöä tai toimialakohtaisia säädöksiä, joten tarjouksissa, sopimuksissa ja muussa yhteydenpidossa on syytä selvittää, mitkä lait, asetukset ja muut normit ovat tapauksen yhteydessä relevantteja.

Vaikka lainsäädännön määrittelemät vaatimukset tietoturvallisuuden ja tietosuojan varmistamiseksi koskevat sekä manuaalista että sähköistä asiakirjojen käsittelyä, lakien velvoitteiden huomioiminen on erityisen tärkeää sähköisessä käsittelyssä. Tärkeimmät tietojärjestelmien suunnittelussa ja toteutuksessa huomiotavat lait ovat laki viranomaisten toiminnan julkisuudesta, henkilötietolaki sekä arkistolaki, mutta järjestelmien suunnitteluun vaikuttavat myös kunkin hallinnonalan mahdolliset asiaa koskevat erityissäännökset, sekä sähköistä allekirjoitusta, asiointia ja sähköistä viestintää koskevat lait. Lisäksi huomioon tulee ottaa useita muita lakeja kuten poikkeustilaa koskevat säännökset.

Henkilötietolain, julkisuuslain ja arkistolain hyvän tiedonhallinnan edellyttämät analysointi-, suunnittelu- ja selvittämistoimet sekä vaatimukset tietoturvallisuuden toteuttamiseksi on tarkoituksenmukaista toteuttaa samanaikaisesti.

7.1 Ulkoistamisen lainsäädännölliset edellytykset

Ulkoistamisen yhtenä perusasiana tulee olla tieto siitä, mitä lainsäädäntö edellyttää kyseessä olevalta prosessilta ja tehtäviin liittyvältä tietojen käsittelyltä.

Lainsäädännön asettamat edellytykset ulkoistamiselle selvitetään erikseen. Viranomaisten tehtävien hoidon ulkoistamiselle voi olla säännöksiä kyseistä viranomaista ja sen tehtäviä koskevassa lainsäädännössä.

Laista viranomaisten toiminnan julkisuudesta (Julkisuuslaki 621/1999; 5§2) ilmenee välillisesti, että viranomainen voi hoitaa tehtäviään myös toimeksiantona. Toisin sanoen tehtävä voidaan ulkoistaa siten, että ulkopuolinen palvelujen tuottaja toimii viranomaisen lukuun. Tämä merkitsee, että viranomaisen vastuut eivät muutu. Säännöksen mukaan viranomaisen toimeksiantona hankkiman palvelun asiakirjat ovat viranomaisen asiakirjoja. Henkilötietojen käsittelyä edellyttävien tehtävien ulkoistamisen näkökulmasta tämä merkitsee, että rekisterinpitäjän vastuut eivät muutu.

Myös henkilötietolaista (523/1999) ilmenee välillisesti, että viranomainen voi antaa toimeksiantona esimerkiksi tietojenkäsittelytehtäviä ulkopuolisen yrityksen hoidettavaksi (8§1 kohta 7). Henkilötietolaki ei rajoita henkilötietojen käsittelyä koskevien palvelujen hankkimista ulkopuolisilta, jos se tapahtuu kyseisen viranomaisen omaan lukuun. Viranomainen toimii tällöin edelleen henkilötietolain tarkoittamana rekisterinpitäjänä joka viime kädessä vastaa siitä, että käsittely tapahtuu henkilötietolain mukaisesti. Palveluntuottajan vastuu määräytyy sopimusvastuuna. Siksi on tärkeää, että asiaa koskevassa toimeksiantosopimuksessa on riittävän yksiselitteiset sopimusmääräykset siitä, mitä tehtäviä, vastuita ja velvollisuuksia palveluntuottajalle henkilötietojen käsittelyssä kuuluu, mukaan lukien tietoturvan varmistaminen. Palveluntuottajaa sitovat suoraan lain nojalla myös henkilötietolain suojaamis- ja huolellisuusvelvoitteet samoin kuin yleensä viranomaista koskevat salassapitovelvoitteet. Asia on kuitenkin aina arvioitava kutakin viranomaista velvoittavan salassapitosääntelyn perusteella.

Henkilötietojen käsittelyä tekevät yritykset ovat velvollisia tekemään tietosuojavaltuutetulle henkilötietolaissa tarkoitetun toimintailmoituksen. Vastaavasti tietojenkäsittelypalveluja toimeksiantona hankkivien viranomaisten tulee tehdä tietosuojavaltuutetulle rekisteri-ilmoitus (henkilötietolaki 36 ja 37 §, tietosuojavaltuutetun asiaa koskevat ohjeet, www.tietosuoja.fi).

Silloin kun palvelujen tuottajana ja järjestäjänä on valtion toinen viranomainen, vaatimukset sopimuksenteolle eivät muutu, ellei erikseen kyseisestä tehtävästä ja niihin liittyvistä vastuista ole toisin lailla säädetty. Ellei siis kysymys ole lainsäädännöllä järjestetystä uudelleenorganisoinnista, asiasta on tehtävä asianmukaiset toimeksiantosopimukset. Esimerkiksi palvelukeskusten on tehtävä sopimukset niiden viranomaisten kanssa, joiden tehtäviä se ryhtyy hoitamaan. Henkilötietojen käsittelyn kannalta palvelukeskus toimii kunkin rekisterinpitäjän lukuun, ellei palvelukeskuksen tehtävistä ja vastuista olisi toisin säädetty lailla.

Myös viranomaisten suunnittelemien yhteisten tietojärjestelmien vastuut tietojärjestelmien ylläpidosta, muun muassa tietoturvakysymyksistä on määriteltävä sopimuksin. Tietojärjestelmässä toteutettava henkilötietojen käsittely ja vastuu tietojen suojaamisesta ja tietoturvallisuudesta tapahtuu kutakin viranomaista koskevan lainsäädännön ja tehtävien mukana. Käsittelystä ja vastuista on tätä osin tehtävä toimeksiantosopimus, ellei jollekin viranomaiselle ole säädetty erikseen asiaan liittyviä tehtäviä ja vastuita. Esimerkiksi väestörekisterikeskukselle on säädetty lailla vastuu koko väestötietojärjestelmän toimivuudesta.

Henkilötietojen siirroista ulkomaille, tarkastusoikeudesta, tietojen korjaamisesta ja muista ajankohtaisista asioista on löydettävissä ohjeita ja malleja Tietosuojavaltuutetun toimiston verkkosivuilla.

7.2 Julkisuuslaki ja -asetus

Laki viranomaisten toiminnan julkisuudesta (621/1999) säätää viranomaisten asiakirjojen julkisuudesta ja salassapidosta. Lakiin sisältyvät lisäksi erityisesti sähköisten asiakirjojen ja tietojen käsittelyn kannalta tärkeät hyvää tiedonhallintaa koskevat säännökset (18 §). Nämä säännökset edellyttävät muuan muassa tietojärjestelmien käyttöönottoa valmisteltaessa toimenpiteiden vaikutusten selvittämistä julkisuuteen, salassapitoon ja tietojen laatuun sekä toimenpiteitä tietojärjestelmien ja niihin liittyvien tietoturvauhkien selvittämiseksi ja tietojen suojauksen järjestämiseksi. Laki edellyttää suunnitelmallisuutta hyvän tiedonhallinnan tavoitteiden saavuttamiseksi sekä tietojen suojaamiseksi ja tietoturvallisuuden varmistamiseksi.

Julkisuuslain säännöksistä asiakirjojen ja tietojen käsittelyn suunnitteluun ja luokitteluun vaikuttavat myös säännökset asianosaisen tiedonsaantioikeudesta (11 §) ja oikeudesta saada tieto itseään koskevasta asiakirjasta (12 §), henkilötietojen henkilörekisteristä luovuttamista koskeva säännös (16.3 §), lupamenettelyä koskeva säännös salassa pidettävien tietojen luovuttamisesta tieteellistä tutkimusta ja tilastointitarkoitusta varten (28 §) sekä salassapidon lakkaamista koskeva säännös (31 §). Samoin sovelletaan julkisuuslain 23 §:n säännöstä, jonka mukaan salassapitovelvollisuus koskee myös lain nojalla salassa pidettäviä tietoja saaneita henkilöitä, joita ovat asianosaisena tietoja saaneet, julkisen toimintayksikön lukuun toimivat palvelun tuottajat (ml. ulkoistus) ja niiden henkilöstö sekä em. 28 §:n nojalla salassa pidettäviä tietoja saaneet. Julkisuuslain 25 §:ssä säädetään salassa pidettävään asiakirjaan tehtävistä luokitusmerkinnöistä.

Asetuksessa viranomaisten toiminnan julkisuudesta ja hyvästä tiedonhallintatavasta (1030/1999; uudistettavana) säädetään tarkemmin eräiden julkisuuslain säännösten soveltamisesta. Sähköisen asiakasasiakirjojen ja -tietojen käsittelyn kannalta tärkeitä ovat erityisesti hyvän tiedonhallinnan toteuttamista koskevat säännökset, mukaan lukien asetuksen säännökset erityissuojattavan tietoaineiston luokituksesta sekä erityissuojattavan aineiston yleisistä tietoturvatoimenpiteistä.

7.3 Henkilötietolaki

Viranomaistoiminnassa tapahtuvassa henkilötietojen käsittelyssä tärkein ja ensimmäisenä huomioon otettava laki on henkilötietolaki (523/1999). Se säätää hyvän tietojenkäsittelytavan aikaansaamiseksi henkilötietojen käsittelyn yleisistä edellytyksistä, henkilötietojen käsittelyssä noudatettavista yleisistä periaatteista, kuten suunnitelmallisuuden vaatimuk-

sesta sekä rekisteröityjen henkilötietojen käsittelyn liittyvistä oikeuksista. Henkilötietolaki säätää siten niistä keinoista, joiden avulla lain tavoitteet voidaan saavuttaa. Täydentävästi suunnittelussa tulee ottaa huomioon julkisuuslaki, arkistolaki (831/1994) ja muut edellä ja jäljempänä mainitut lait.

Henkilötietolaki koskee kaikkea henkilötietojen käsittelyä. Lainmukaisuuden varmistamisvelvollisuus koskee kaikkia käsittelyvaiheita, myös sähköisesti tapahtuvien käsittelyjen osalta. Sähköisen käsittelyn osalta korostuvat tietojen suojaamisen ja tietoturvallisuuden vaatimukset. Käsittelyllä tarkoitetaan henkilötietojen keräämistä, tallettamista, järjestämistä, käyttöä, siirtämistä, luovuttamista, säilyttämistä, muuttamista, yhdistämistä, suojaamista, poistamista, tuhoamista sekä muita henkilötietoihin kohdistuvia toimenpiteitä.

Seuraavassa on kuvattu etukäteisen suunnittelutyön kannalta keskeisimmät vaatimukset.

1) Ensimmäinen vaatimus hyvän tietojenkäsittelytavan ja tiedonhallinnan toteuttamiseksi on henkilötietojen käsittelyn tarkoituksen määrittely (henkilörekisterin käyttötarkoituksen määrittely). Tätä koskeva velvollisuus sisältyy henkilötietolain 6 §:ään. Säännöksen mukaan henkilötietojen käsittelyn tarkoitus tulee määritellä siten, että siitä ilmenee, minkälaisten rekisterinpitäjän tehtävien hoitamiseksi henkilötietoja käsitellään.

   Henkilörekisterin määritelmä on lain 3.1 kohdassa 3. Henkilörekisteri on se looginen tietokokonaisuus, joka muodostuu sanotussa käyttötarkoituksissa talletettavista tiedoista; esimerkiksi henkilöstöhallinnon rekisteri muodostuu kaikista niistä tiedoista, joita rekisterinpitäjä tallettaa palvelussuhteen hoitamisessa (looginen rekisterikäsite). Tähän loogiseen kokonaisuuteen kuuluvat mm. nimitysasiakirjat, palkanmaksutiedot, koulutustiedot, poissaolotiedot, kulunvalvontatiedot, kehityskeskustelun tiedot, olivatpa tiedot talletettu manuaalisesti tai sähköisesti. Loogiseen henkilörekisteriin kuuluvat myös rekisterinpitäjän lukuun ulkopuolisen yrityksen toimesta tapahtuva henkilötietojen käsittely.

   Myös julkisuuslain soveltamisessa on välttämätöntä tietää siitä, mitä eri käyttötarkoituksia varten perustettuja henkilörekistereitä organisaatiossa on tai tietojärjestelmässä ylläpidetään, koska tällä on merkitystä tietojen käytön (käyttötarkoitussidonnaisuuden vaatimus) ja luovuttamisen oikeutusta selvitettäessä. Tämän vuoksi myös tietojärjestelmäselosteessa tulisi muun ohella olla tieto siitä, mitkä henkilötiedot kuuluvat johonkin viranomaisen pitämään henkilörekisteriin.
2) Toinen keskeinen vaatimus hyvän tietojenkäsittelytavan ja hyvän tiedonhallinnan toteuttamiseksi on suunnitella henkilötietojen käsittely edellä mainitun loogisen rekisterikäsitteen pohjalta. Ellei tietojen käsittelyjen analysointia ja prosessien kuvausta tehdä kyseisessä tehtävässä muodostuvan toiminnallisen kokonaisuuden ja tietojen perusteella, sähköisen tietojen käsittelyn etuja ei voida kaikilta osin hyödyntää, eikä esimerkiksi tarpeettomia ja päällekkäisiä käsittelyjä välttää. Looginen rekisterikäsite merkitsee myös vaatimusta arvioida ja suunnitella osana rekisterinpitoa myös ne tie-

tojen ja asiakirjojen käsittelyt, jotka teetetään organisaation lukuun (toimeksiannosta). Palvelut tilaava valtion viranomainen on vastuussa siitä, että toiminta ja asiakirjojen käsittely tapahtuu lainmukaisesti. Tällaisen toimeksiantosopimuksen perusteella tuotettuihin palveluihin sovelletaan myös viranomaisten toiminnan julkisuudesta annettua lakia, sen 5 §:n 2 momentin perusteella.

3) Kolmas vaatimus on huomioida ja kuvata paitsi toimintayksikön sisäisen toiminnan edellyttämät tietotarpeet ja toiminnot myös tietojenkäsittely-ympäristöön liittyvät toiminnot. Tietojärjestelmien suunnittelun pohjana on välttämätöntä olla tieto kaikista toiminnan edellyttämistä käsittely- ja tietotarpeista mukaan lukien erityisesti tiedot siitä, mistä henkilötietoja säännönmukaisesti hankitaan sekä mihin niitä säännönmukaisesti luovutetaan, mikä on tietojen julkisuus, miten kauan tietoja tulee ja voidaan säilyttää. Säännönmukaisten tietolähteiden ja tietojenluovutusten määrittelyvelvollisuudesta on säädetty nimenomaisesti henkilötietolain 6 §:ssä. Muun käsittelytoiminnan kuvaus- ja suunnitteluvelvollisuus perustuu paitsi henkilötietolain 5 §:n huolellisuusvelvoitteeseen myös siihen, ettei lain vaatimuksista voida muutoin varmistua

   Alueellisten tai muuten verkottuvien tietojärjestelmien kehittämishankkeet, joissa on mukana useita eri organisaatioita ja osapuolia, toteutus edellyttää, että vastuut on yksiselitteisesti todettu ja määritelty, sopimukset yhteistyöstä ja sen periaatteista ja toteuttamistavoista on tehty, työn koordinaatio toimii ja hankkeen toteutukselle on luotu tehokas ja ajantasainen seurantajärjestelmä, jossa on selkeät vastuut. Perusedellytyksenä on kuitenkin, että hankkeiden kehittäjillä on käytettävissään riittävän kattava kokonaiskuva hankkeesta ja sen osapuolista ja toimijoista (ml. suunnitelma ulkopuolisista palvelujen tuottajista ja näiden tehtävistä) ja kuvaukset eri osapuolten toiminnoista, asiakirjoista ja prosesseista sekä valmiuksista, henkilötietojen käsittelyn osalta kuvaukset eri henkilörekistereistä. Alueellisten hankkeiden osana joudutaan yleensä hankkimaan tietojenkäsittely- ja muita palveluja ulkopuolisilta palvelujen tuottajilta. Tällaisten palvelujen hankkimisen suunnittelu ja toteutus ja asiaan liittyvät sopimukset ovat osa koko hankkeen suunnittelua.

4) Neljäs keskeinen vaatimus on arvioida järjestelmää ja siinä toteutettavaa tietojen käsittelyä rekisteröidyn henkilön kannalta. Toiminnallisesti tavoitteena on saada aikaan tietojärjestelmät, joiden avulla tehtävät voidaan toteuttaa organisaation ja sen työntekijöiden työn kannalta mahdollisimman tehokkaasti ja viivytyksettä ja tekemättä tarpeetonta ja päällekkäistä työtä. Asiakkaan luottamuksen turvaamiseksi on kuitenkin yhtä tärkeää varmistaa, että rekisteröidyn (esimerkiksi asiakkaan) tietojensaantioikeudet ja hänen muut tietojenkäsittelyyn liittyvät oikeutensa ja niiden toteutuminen huomioidaan tietojärjestelmien suunnittelussa ja että yksityisyyttä edistäviä tekniikoita ja ominaisuuksia (mm. oikeuksista muistuttaminen) kehitetään osana järjestelmien kehittämistyötä

Malli henkilötietojen käsittelyn suunnittelusta on tämän ohjeen luvussa 9 (kuvat 9 ja 10).

7.4 Eräitä muita säädöksiä

Arkistolakiin (831/1994 myöhempine muutoksineen) sisältyvät säännökset laissa määriteltyjen *julkisen sektorin viranomaisten ja laitosten* arkistotoimen järjestämisestä sekä siihen liittyen muun muassa tieto- ja asiakirjahallinnon järjestämisestä, asiakirjojen säilyttämisaikojen määrittelystä sekä säilyttämisessä ja hävittämisessä noudatettavista vaatimuksista ja periaatteista. Myös arkistolaki edellyttää suunnitelmallisuutta, johon sisältyvät käytännön tehtävien järjestämistä koskevat suunnitelmat. Henkilötietolain näkökulmasta arkistotoimen vaatimukset tulee huomioida erikseen kaikissa käsittelyvaiheissa. Arkistolain säännökset edellyttävät nimenomaisesti myös tietoturvan ja suojan huomioimista arkistotoimen hoitamisessa ja järjestämisessä.

Sähköisistä allekirjoituksista annetun lain (14/2003**)** tarkoituksena on edistää sähköisten allekirjoitusten käyttöä ja niihin liittyvien tuotteiden ja palveluiden tarjontaa sekä sähköisen kaupankäynnin ja sähköisen asioinnin tietosuojaa ja tietoturvaa. Lailla säädetään sähköisestä allekirjoituksesta ja sen oikeusvaikutuksista, varmentamistoiminnan edellytyksistä, kuten sähköisiin allekirjoituksiin liittyvien varmenteiden tarjonnasta, niiden tarjoajien velvollisuuksista ja vastuista sekä henkilötietojen suojasta.

Laissa sähköisestä asioinnista viranomaistoiminnassa (13/2003) säädetään viranomaisten ja näiden asiakkaiden oikeuksista, velvollisuuksista ja vastuista sähköisessä asioinnissa.

Lakia sovelletaan hallintoasiain, tuomioistuinasian, syyteasiain ja ulosottoasiain sähköiseen vireillepanoon, käsittelyyn ja päätöksen tiedoksiantoon, sekä soveltuvin osin myös muussa viranomaistoiminnassa. Laissa säädetään muun muassa kirjallisen muodon ja allekirjoitusvaatimuksen täyttymisestä, sähköisen asiakirjan kirjaamisesta tai muusta rekisteröinnistä, päätöksen sähköisestä tiedoksi antamisesta, sekä sähköisen asiakirjan arkistoinnista. Lakia voitaisiin soveltaa sen perustelujen (HE 17/2002) mukaan myös viranomaisten väliseen tiedonsiirtoon.

Lain tarkoittamaa sähköistä asiointia olisi esimerkiksi telefaksin ja sähköpostin käyttö sekä varmennettu sähköinen asiointi. Jos käsiteltävät asiakirjat ovat salassa pidettäviä tai arkaluonteisia tietoja ja/tai kysymys on vireille panijan tai vastaanottajan oikeusturvaan vaikuttavista asioista, sähköisen asioinnin luotettavuudella, osapuolten tunnistamisella ja tietojen virheettömyydellä ja tietojen suojaamisella on tärkeä merkitys. Sen vuoksi asioinnissa tulisi edellyttää luotettavaa tunnistamista.

Laki on yleislaki, jossa säädetään lähinnä sähköisen asioinnin menettelyistä ja teknisestä toteutuksesta. Lain 3 §:n mukaan viranomaisasiointiin sovelletaan muutoin, mitä esimerkiksi viranomaisten toiminnan julkisuudesta tai henkilötietojen käsittelystä säädetään. Jos muussa laissa on sähköiseen asiointiin vaikuttavia erityissäännöksiä, niitä sovelletaan yleislain sijasta.

Lakiesityksen perusteluissa todetaan, että sähköisen viranomaisasioinnin onnistunut toteuttaminen edellyttää viranomaisten toimintaprosessien tarkkaa analysointia ja suunnit-

telua. Viranomaisten toiminnassa esimerkiksi erilaiset hakemukset kuuluvat usein myös johonkin henkilötietolain tarkoittamaan henkilörekisteriin ja ovat julkisuuslain tarkoittamia asiakirjoja. Sen vuoksi henkilötietolain ja julkisuuslain edellyttämässä suunnittelutyössä on käsittelyn lainmukaisuutta arvioitava eri käsittelyvaiheiden osalta myös sähköistä asiointia viranomaistoiminnassa koskevien säännösten valossa.

Lakia sähköisen viestinnän tietosuojasta (516/2004) sovelletaan yleisissä viestintäverkoissa tarjottaviin verkkopalveluihin, viestintäpalveluihin, lisäarvopalveluihin ja palveluihin, joissa käsitellään palvelun käyttöä kuvaavia tietoja. Lain tarkoituksena on turvata sähköisen viestinnän luottamuksellisuus ja yksityisyyden suojan toteutuminen sekä edistää sähköisen viestinnän tietoturvaa ja monipuolistaa sähköisten viestinnän palvelujen tasapainoista kehitystä. Tietojärjestelmähankkeissa ensimmäisenä tulee huomioida julkisuuslain ja henkilötietolain ja arkistolain vaatimukset suunnittelussa ja toteutuksessa. Erikseen arvioidaan, millä tavoin sähköisen viestinnän tietosuojalain säännökset tulee mahdollisesti ottaa huomioon esimerkiksi organisaatioiden välillä muutoin lähettävien viestien suojaamisessa. Sähköpostien lähettämisessä noudatetaan sähköisen viestinnän tietosuojalain säännöksiä. Tietojärjestelmien käyttöoikeudet ja katseluoikeudet ja niiden lainmukaisuus suunnitellaan ja arvioidaan siten henkilötietolain ja julkisuuslain perusteella ja mukaisesti. Viranomaisorganisaatioita voivat koskea esimerkiksi sähköisen viestinnän tietosuojalain yhteisötilaajia koskevat säännökset.

Eri hallinnonalojen tehtäviä koskevaan lainsäädäntöön sisältyy muun muassa tietojen, etenkin henkilötietojen luovuttamista ja salassapitoa sekä tiedonsaantioikeuksia ja suostumuksen muotoa koskevia säännöksiä ja määräyksiä. Rekisterinpidon vastuut ja eri rekisterien pidon lainsäädännölliset perusteet määräytyvät pääosin asiaa koskevan lainsäädännön perusteella.

Laki yksityisyyden suojasta työelämässä (759/2004) koskee organisaatioiden henkilöstöä koskevien tietojen käsittelyä. Lakia sovelletaan ensisijaisena henkilötietolakiin nähden siinä säädettyjen asioiden osalta. Lain rinnalla sovelletaan kuitenkin kaikkia niitä henkilötietolain yleissäännöksiä, joista työelämälakiin ei sisälly säännöksiä, kuten henkilötietolain yleisvelvoitteet ja pääosin rekisteröityjen oikeuksia koskevat säännökset. Tietojärjestelmien lokitietojen tallettamisessa ja käytössä voi olla kysymys myös työelämän tietosuojalain tarkoittamasta työntekijöiden teknisestä valvonnasta, jotka tulee käsitellä yhteistoimintalain mukaisessa järjestyksessä.

Laki julkisista hankinnoista (1505/1992, uudistettavana) määrittää lukuisia tekijöitä, jotka on huomioitava julkisissa hankinnoissa. Ulkoistava organisaatio voi asettaa tietoturvallisuutta koskevat valintakriteerit haluamalleen tarkkuustasolle, kunhan ne ovat suhteessa siihen mitä hankitaan, eivät syrji tai suosi ketään tarjoajista ja ovat välttämättömiä hankinnan sisällön suhteen. Hyvänä keinona laajoissa ulkoistuksissa on sopia ulkoistetun palvelun tarkastuksesta ja arvioinnista jo hankinnan yhteydessä (ks. liite 1a ja 1b, turvallisuussopimus). Turvallisuussopimus on kytkettävissä Valtion tietotekniikkahankintojen yleisiin sopimusehtoihin (VYSE 1998).

Kaksivaiheisissa hankinnoissa tietoturvakriteerejä voidaan käyttää joko osana ensimmäisen vaiheen kelpoisuusehtoja tai toisessa vaiheessa ehdokkaita arvioitaessa (ks. 8.2.3 jäljempänä).

8 TIETOTURVALLISUUS ULKOISTETUN TOIMINNON ELINKAAREN ERI VAIHEISSA

8.1 Ulkoistuksen elinkaaresta

Tässä luvussa ulkoistusta käsitellään sen elinkaaren mukaisesti vaiheittain. Elinkaaren elementit on jaoteltu kolmeen pääjaksoon.

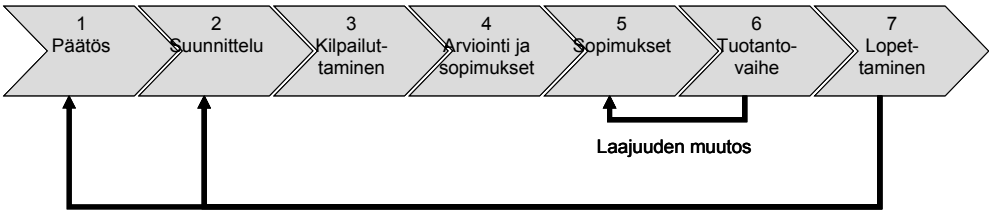
Jaottelu on yleinen ja vaiheet toistuvat niin yksityisissä yrityksissä kuin julkishallinnossakin, vaikka jaottelun taustalla on julkishallinnon hankintaprosessi.

8.2 Toiminnon tai palvelun ulkoistaminen

8.2.1 Päätös ulkoistamisesta

Päätös ulkoistuksesta voidaan tehdä joko vapaasta tahdosta tai kyseessä voi olla tilanne, jossa tosiasiallisia vaihtoehtoja ulkoistamiselle ei ole. Jälkimmäinen esimerkki on tavallisesti heikko lähtökohta onnistumiselle, joten ulkoistuksen suomia mahdollisuuksia ja omaa kykyä hoitaa toimintoa tai palvelua on seurattava jatkuvasti.

Kuva 4. Ulkoistamisen elinkaari.



Ulkoistuspäätöksen lähtökohtien on oltava toiminnallisia ja perustelujen on noudatettava organisaation palvelujen tuottamisen strategiaa. Yleensä pyritään ulkoistamaan tukipalveluja ja -toimintoja ja keskittymään ydintoimintaan. Jaossa on pitkälti kyse määrittelystä eli siitä, mitkä toiminnot organisaatio on määritellyt ydintoiminnoikseen.

Yritysmaailmassa ydinprosesseina pidetään yleensä sellaisia prosesseja, jotka ovat ainutkertaisia, luovat yritykselle kilpailuetua ja joiden siirto muiden tehtäviksi olisi joko mahdotonta tai heikentäisi ratkaisevasti yrityksen toimintaedellytyksiä. Yrityksissä tyypillisiä ydinprosesseja ovat myynti, tuotekehitys ja johtaminen. Aiemmin ydinprosessina usein ollut tuotanto on nykyisin hankittavissa ulkoistettuna.

Vaikka ydinprosesseja ei ulkoisteta kokonaan, voidaan osittaista ulkoistusta hyödyntää. Tuotekehityksestä tai myynnistä saatetaan ulkoistaa sellaisia osia, jotka eivät ole toiminnan kannalta merkittäviä. Ulkoistus etenee tällöin vähitellen ja kehityksen tuloksena aiempi ydinprosessi saattaa olla jossain vaiheessa lähes kokonaan ulkoistettu.

Julkishallinnossa kehitys etenee hitaammin. Tilaaja-tuottaja -mallissa on kyse strategisen tason ulkoistuksesta. Virastot ja laitokset ovat ulkoistaneet tukitoimintojaan, kuten siivous ja vartiointi. Niistä on helpompaa tehdä päätös kuin henkilöstö- ja taloushallinnosta, jotka ovat lähempänä ydintoimintaa.

Ulkoistuksen ja sen tietoturvallisuuden kannalta on merkityksellistä, onko organisaatiolla aiempaa kokemusta ulkoistusprosessista. Jos sitä ei ole tai aiemmat kerrat ovat epäonnistuneet, on harkittava ulkopuolisen asiantuntijan käyttöä. Konsultilla tulee tällöin olla kokemusta myös valtionhallinnon tietoturvallisuuden tarvetasosta ja tavoitteista.

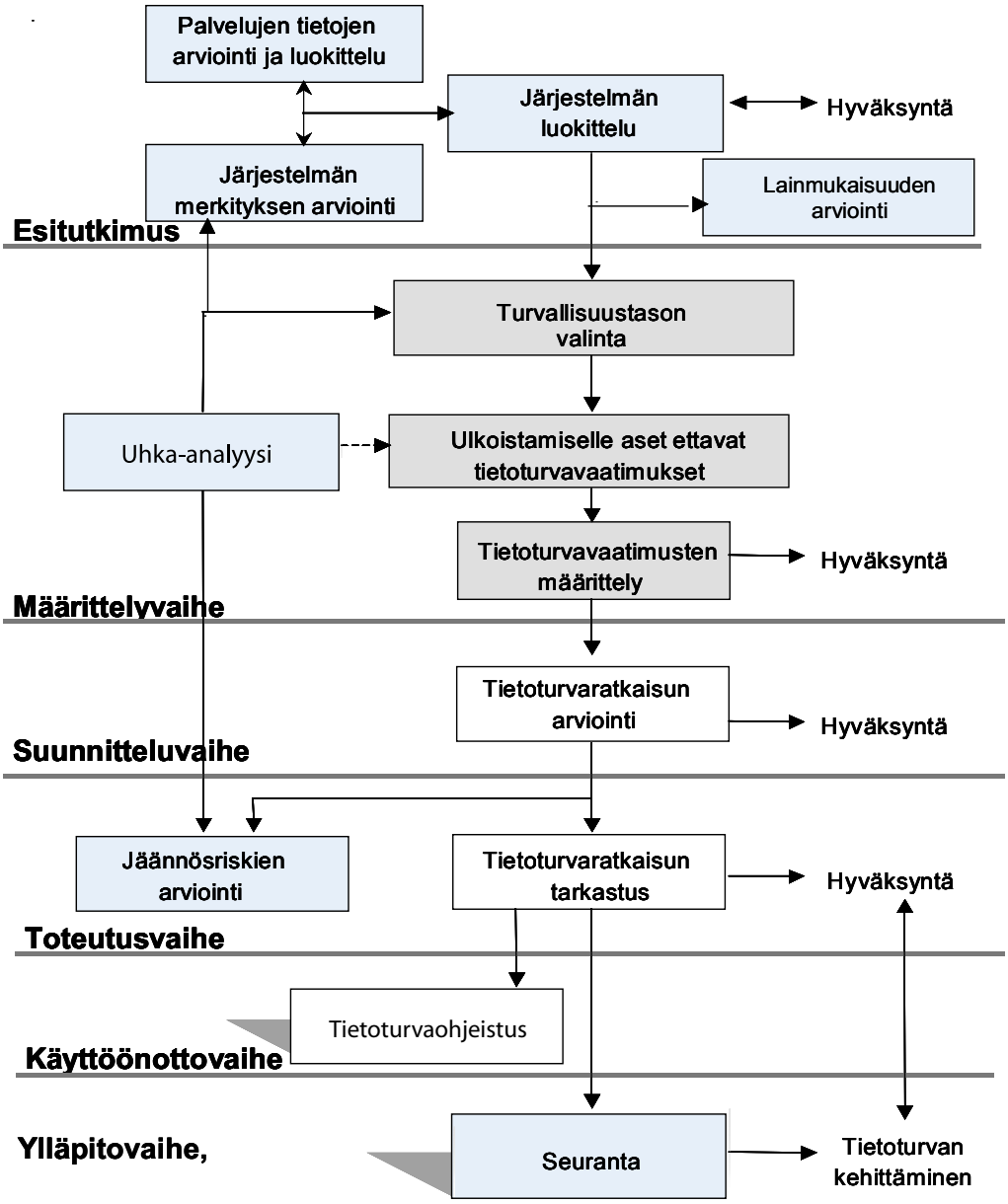
Mitä paremmin ulkoistaja tuntee ulkoistuksen kohteen ja pystyy kuvaamaan (ja tarvittaessa erityttämään) sen, sitä paremmat edellytykset ulkoistukselle on. Ongelmallinen ulkoistus on usein seurausta yrityksestä ulkoistaa ongelmat.

Ulkoistettavan tietojärjestelmän tietoturvallisuutta voidaan tarkastella kuvan 5 mukaisena vaiheittain etenevänä prosessina. Kuvan vaiheet poikkeavat hieman tässä esityksessä käytetystä jaottelusta, koska kyseinen kuva perustuu tietojärjestelmän elinkaaren vaiheisiin.

Henkilöstö on tietoturvallisuuden kannalta keskeisessä asemassa, kuten aiemmissa luvuissa on todettu. Ulkoistuksen osalta tämä on korostetun tärkeää monesta syystä. Henkilöstö kokee ulkoistuksen osalta epävarmuutta omasta asemastaan ja saattaa pahimmassa tapauksessa ryhtyä aktiiviseen muutosvastarintaan.

Organisaation johto vastaa asiakirjojen ja henkilötietojen käsittelyjen lainmukaisuudesta. Johdon tulee kyetä vaatimaan lainmukaisia ja toimivia ratkaisuja myös toimintoja ulkoistettaessa (ks. luku 9). Siten myös johdolta edellytetään tietoa toiminnallisia, teknisiä ja oikeudellisia edellytyksiä koskevista vaatimuksista ja niiden merkityksestä. Näihin kuuluvat sopimus- ja hankintakysymykset. Tietojärjestelmiä koskevia hankintoja ja sopimuksia ei voida tehdä ilman asianmukaisia selvityksiä ja suunnitelmia, joihin osana liittyvät henkilötietojen käsittelyyn liittyvät analysoinnit ja kuvaukset. Johdon tehtävänä on myös huolehtia siitä, että henkilöstöllä (omalla ja tarvittaessa myös ulkoistetun toimin-

Kuva 5. Ulkoistettavan tietojärjestelmän tietoturvallisuuden arviointimalli.



non henkilöillä) on tarvittava ja lainmukainen osaaminen tietojärjestelmien suunnittelussa, toteutuksessa ja käytössä. Suunnitteluun hankitaan tarvittava osaaminen, jos henkilöstöllä ei sitä ole.

Tilaajalla on toimintaansa tarvittavaa osaamista, mutta sen sijaan riittävää lainsäädännön ja teknistä osaamista ei välttämättä ole kattavasti varsinkaan pienemmillä valtionhallinnon organisaatioilla. On myös otettava huomioon, että yrityksille julkishallintoa koskevat säädökset saattavat olla vieraita.

Ulkoistamispäätöstä tehdessä on tuotava selkeästi esille, että vaikka tietty toiminto ulkoistetaan, vastuu sen toimivuudesta jää ulkoistavaan organisaatioon.

8.2.2 Ulkoistuksen suunnittelu

Tietoturvallisuuden kannalta ehkä kriittisin vaihe on aika välittömästi ulkoistuspäätöksen jälkeen. Ulkoistuksen kohde on rajattava, sen riippuvuus muihin järjestelmiin ja palveluihin on kuvattava ja ulkoistuksen kohteeseen liittyvät vastuut on määriteltävä. Kaikki tämä on kyettävä tekemään tavalla, jonka ulkoistetusta toiminnosta vastaava kykenee ymmärtämään. Osa tietoturvallisuuden kannalta keskeisistä asioista tulee käsiteltyä ulkoistusprosessissa, mutta eräät kohdat on syytä käydä läpi yksityiskohtaisesti, kuten:

- Mitä organisaation tietoturvapolitiikka edellyttää ulkoistukselta?
- Käsitelläänkö ulkoistettavassa toiminnossa henkilötietoja? Onko asiasta tehty lain vaatimat ilmoitukset Tietosuojavaltuutetun toimistolle?
- Käsitelläänkö ulkoistettavassa toiminnossa turvaluokiteltuja tietoaineistoja?
- Onko tietoteknisissä järjestelmissä joitain vain tälle tietojärjestelmälle ominaista?
- Mikä on ulkoistettavan toiminnon merkitys? Onko sille asetettu erityisiä kriittisyysvaatimuksia?
- Onko syytä olettaa, että ulkoistettu toiminto kiinnostaa tietomurtautujia?

Ulkoistusprosessin huolellinen suunnittelu pienentää riskejä. Organisaation tietoturvapäällikön tai vastaavan on oltava mukana ulkoistuksen suunnittelu- ja toteuttamisprosessissa.

Ulkoistuksen suunnittelun tärkein vaihe on tarjouspyynnön teko. On suositeltavaa, että tarjouspyyntöön sisältyy oma erillinen lukunsa ulkoistuksen kohteen tietoturvavaatimuksista. Ulkoistuksen kohteeseen liittyvät julkishallinnon erityisvaatimukset tulee esittää mahdollisimman selkeästi, mielellään erillisenä kohtanaan. Tietoturvallisuuden taso tulee määritellä selkeästi ja yksiselitteisesti mitattavasti. Toimittajalta ei saa olettaa liikaa, vaan kaikki tietoturvavaatimukset on tuotava esiin. Viittaukset asiaa sääteleviin lakeihin ei yleensä riitä vaan tilaajan on esitettävä menettelyt, joilla laissa säädetyt velvoitteet voidaan täyttää.

On suositeltavaa, että toimittajan tietoturvaosaamisesta annetaan pisteitä. Kriteerien on oltava sellaisia, jotka tuovat julki tarjoajien väliset todelliset tietoturvatasoerot. Esimerkiksi johdon sitoutumista tietoturvallisuuteen ei kannata kysyä, koska yksikään tarjoa-

ja ei yleensä vastaa tähän kieltävästi. Toimittajan tietoturvallisuuden arvioinnissa voidaan hyödyntää vastaavaa VAHTI-ohjetta[17]. Sen soveltamisessa on otettava huomioon, että se on laadittu auditointiin, jossa toimittajan vastaukset voidaan tarvittaessa verifioida. Tarjouskilpailussa mahdollisuudet tähän ovat vähäiset.

Tietoturvallisuuden osuus kokonaispistemäärästä tulisi olla 5-15 % välillä. Maksimipisteiden lisäksi merkitystä on pisteiden hajonnalla. Ovatko kysymykset todella sellaisia, että ne erottelevat toimittajat tietoturvallisuuden suhteen? Tietoturva-asiat voivat sisältyä arvioinnin muihin kohtiin, mutta on suositeltavaa eriyttää tietoturva-asiat omaksi kohdakseen.

Toimittajan tietoturvallisuuden kokonaisuuden arvioinnin pääkohdat ovat:

1. toimittajan tietoturvallisuuden hallintajärjestelmän arviointi (ks. ed. VAHTI-ohje)
2. toimittajan erityisosaaminen ulkoistuksen kohteen tietoturvallisuudesta
3. toimittajan henkilöstön tietoturvaosaaminen.

Tietoturvallisuuden hallintajärjestelmän arvioinnissa voidaan hyödyntää esimerkiksi seuraava tasojaottelua:

1. toimittajan tietoturvan johtamisjärjestelmä on sertifioitu (esim. BS7799:n mukainen ja se on toiminut vähintään 3 vuotta (toiminta vakiintunutta)
2. toimittajalla on sertifioitu tietoturvallisuuden johtamisjärjestelmä, joka on toiminut vähemmän kuin 3 vuotta
3. toimittajalla on suunnitelmat tietoturvallisuuden johtamisjärjestelmän sertifioinnista ja sillä on toimiva laatujärjestelmä
4. toimittaja tekee tietoturvallisuuden johtamista järjestelmällisesti, mutta sillä ei ole sitovia päätöksiä tietoturvajärjestelmän sertifioinnista. Yrityksellä on:

a. nimetty tietoturvapäällikkö tai -johtaja, jolla on alan tutkinto kuten CISSP, CISA tai CISM)
   b. tietoturvallisuuden johtoryhmä tai vastaava elin
   c. toimittajalla on selkeä toimintasuunnitelma tietoturvarikkeiden varalle: CIRT-ryhmä, tiedotussuunnitelma ja muut vastaavat dokumentit[18]
   d. tietoturvakoulutus on osa henkilöstön koulutusohjelmaa (tätä voidaan arvioida esimerkiksi selvittämällä kuinka paljon tietoturvakoulutusta toimittaja on vuoden aikana järjestänyt)

5. toimittaja pitää tietoturvallisuutta tärkeänä, mutta ei kehitä sitä järjestelmällisesti (yrityksellä on tietoturvapolitiikka ja sitä tukevat muuta ohjeet)
6. toimittajalla ei ole tietoturvapolitiikkaa, joka voidaan antaa nähtäväksi ulkoistuksen tarjouksien kanssa; toimittaja vakuuttaa kuitenkin asioiden olevan kunnossa
7. muut kuin edellä luetellut tapaukset.

[17] Tietoturvallisuuden hallintajärjestelmän arviointisuositus (VAHTI 3/2003; http://www.vm.fi/tiedostot/pdf/fi/53805.pdf

[18] Tässä voidaan hyödyntää ohjetta Tietoturvapoikkeamatilanteiden hallinta (VAHTI 3/2005; http://www.vm.fi/tiedostot/pdf/fi/95673.pdf)

Toimittajan prosessien ja erityisesti tietoturvallisuusprosessien yksityiskohtainen arviointi on yleensä mahdotonta, koska sen toteuttaminen vaatisi runsaasti aikaa ja rahaa. Tarjouspyynnöissä voidaan pyytää kuvaukset erikseen valittavista, tärkeimmistä prosesseista ja arvioida näiden soveltuvuutta. Toinen lähestymistapa on kysyä, noudattavatko yrityksen tietoturvallisuuden kannalta keskeiset prosessit jotain alan standardia tai ohjeita (ITIL, CoBIT ja ISF[19]).

Mikä paino toimittajan tietoturvallisuudelle tulisi antaa? Eikö tietoturvallisuus toteudu - tai toisaalta murru - yksityiskohdissa? Ulkoistus on pitkä, usein laaja yhteistyösuhde, jossa kaksi organisaatiota tulee riippuvaisiksi toistensa tietoturvallisuudesta. Yksityiskohtia on erittäin paljon ja ne muuttuvat ajan myötä. Yksittäisten asioiden arvioinnin sijaan tulee keskittyä sellaisiin asioihin, joiden voidaan olettaa indikoivan hyvää tietoturvallisuutta vuosien päästäkin. Teot, kuten tietoturvasertifikaatti ja henkilöstön koulutus, ovat merkki tällaisesta tietoturvallisuuden pitkäjänteisestä kehittämisestä.

Toimittajan erityisosaamisen arvioinnin perusteina voidaan käyttää tietoturvallisuudeltaan vastaavien toimintojen ja palveluiden ulkoistuksia (referenssit). Kysymykset voivat olla seuraavan kaltaisia:

– Huolehditteko sellaisen järjestelmän ulkoistuksesta, jossa käsitellään turvaluokiteltua materiaalia tai henkilötietoja? Kuinka hallinnoidaan järjestelmää, jonka arvioidaan olevan tietomurtojen kannalta yhtä houkutteleva?
– Vastaatteko jonkin sellaisen järjestelmän toiminnosta, jossa tekniset turvaratkaisut ovat arvioitavaa tapausta vastaavia?

Ulkoistettavan toiminnon tietoturvallisuuden lisäksi tulee pyrkiä arvioimaan toimittajan kykyä hoitaa siirtymävaiheen tietoturvallisuutta. Asiaa voidaan selvittää pyytämällä toimittajaa kuvaamaan, miten vastaavissa hankkeissa tietoturvallisuus on hallittu.

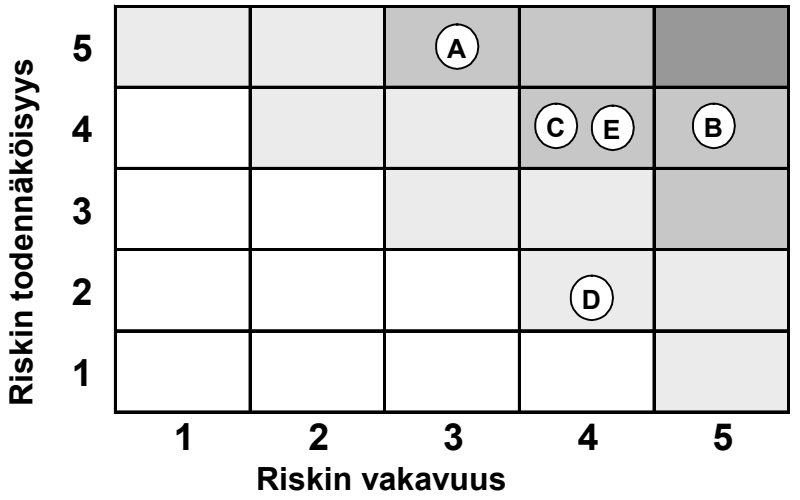
Tarjouspyynnössä on syytä viitata VAHTI-ohjeisiin, mutta yleisluontoista ”tietoturvallisuus VAHTI:n mukainen” määrittelyä ei tule käyttää. Sen sijaan on osoitettava tärkeimmät ohjeet ja niistä kohdat, jotka tulevat kyseeseen. Kohta voi olla seuraavanlainen (esimerkki):

– ”Haittaohjelmien suojautumisessa noudatamme pääosin VAHTI ohjetta 3/2004. Edellytämme, että toimittaja noudattaa ohjeen luvussa 4.3 esitettyä toimintamallia haittaohjelmien havainnosta torjuntaan tai esittää oman, vastaavan mallinsa. Käytössämme olevan MS Internet Explorer sovelluksen asetuksissa noudatamme ohjeen liitteessä 2 olevaa esimerkkiä seuraavin poikkeuksin… ”

Ulkoistuksen ja muiden muutosten riskien arvioinnissa käyttökelpoinen työväline on riskienhallinnassa yleisesti käytetty jako kahteen komponenttiin: riskin todennäköisyys ja toteutuneen riskin vakavuus (kuva 6).

[19] http://www.itil.org/ (ITIL), http://www.securityforum.org (ISF) ja http://www.isaca.org (CoBIT)

Kuva 6. Esimerkki erään ulkomaille tapahtuneen ulkoistuksen riskien arvioinnista (kaavio perustuu todelliseen tapaukseen).



A Työntekijöiden sitoutuminen muutokseen
B Avainhenkilöt jättävät yrityksen
C Tietämys ei siirry
D Toiminnan fyysinen siirto ei onnistu
E Henkilöiden rekrytointi uudessa paikassa

8.2.3 Kilpailuttaminen

Ulkoistuskilpailutuksessa noudatetaan julkisista hankinnoista annettua lakia (1505/1992, uudistettavana). Tämä tarkoittaa usein sitä, että hankinnassa noudatetaan ns. avointa menettelyä.

Mikäli ulkoistuksen kohde on sellainen, että tarjouksia voidaan olettaa tulevan runsaasti, vaarana on, että tietoturvallisuuden arviointi ”hukkuu” tarjousten paljouteen. Tällöin tulee käyttää apuna kaksivaiheisen menettelyn suomaa mahdollisuutta arvioida ensimmäisessä vaiheessa kelpoisuusehdot täyttävät tarjoajat. On muistettava, että mikäli yritystason tietoturvavaatimukset sijoitetaan ensimmäisen vaiheen kelpoisuusehtoihin (joiden täyttäminen on edellytys pääsystä varsinaiseen tarjousvertailuun) ei tietoturvallisuudesta yleisenä tekijänä saa enää antaa lisäpisteitä toisessa vaiheessa. Tietoturvallisuudesta voi saada pisteitä henkilöstön osaamisesta, teknisistä ratkaisuista ja muista arviointikohdista, mutta ei ensimmäisen vaiheen arviointikriteerin ylityksen asteesta. Kuinka asiassa halutaan toimia, tulee arvioida tapauskohtaisesti.

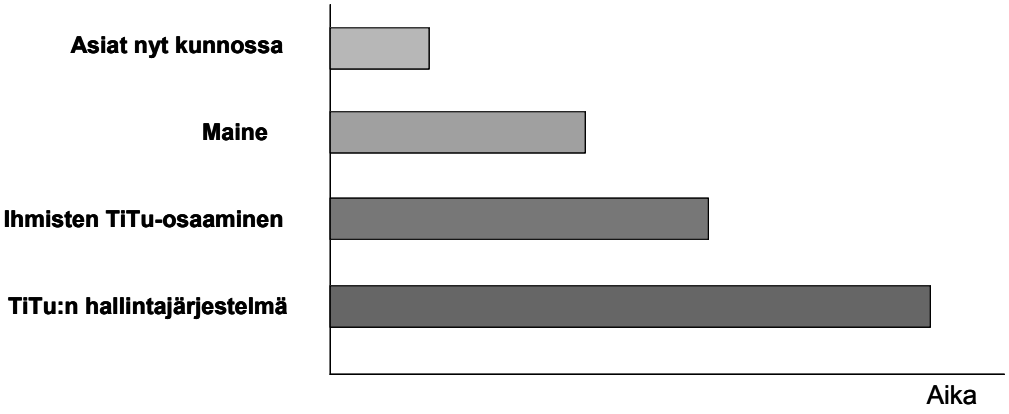
Mikäli toimittajille pidetään tiedotustilaisuuksia, on tietoturvallisuus syytä ottaa omaksi kohdakseen asialistalla. Tietoturvallisuuden erillinen käsittely korostaa sen tärkeyttä. Tilaisuudessa voidaan käsitellä seuraavia asioita:

- Ulkoistuksen kohteen kannalta tärkeiden VAHTI-ohjeiden ja muiden dokumenttien tai linkkilistan jako. Vain tärkeimmät ohjeet tulee jakaa.
- Tietoturvapäällikön esittäytyminen.
- Tietoturvavaatimusten lyhyt läpikäynti sekä ulkoistuksen kohteen että siirtymävaiheen projektin osalta.

Mikäli ulkoistettava toiminto on tietojärjestelmien käyttöpalvelua, voidaan toimittajan laiteteknisten tilojen arvioinnissa käyttää VAHTI-ohjetta Tietoteknisten laitetilojen turvallisuussuositus, (1/2002), jossa erityisesti luvun 1.5 taulukko ja luku 3 sisältävät selkeitä vaatimuksia[20].

Vaikka toimittajan tilanne olisi arviointihetkellä erittäin hyvä, voi vakava haittaohjelmatartunta tai muu tietoturvallisuuden korruptoituminen muuttaa tilanteen. Mikäli yrityksellä on sertifioitu tietoturvallisuuden hallintajärjestelmä, on perusteltua olettaa, että yritys kykenee selviytymään myös vakavista tietoturvaongelmista. Oheinen kaavio esittää arvion eräiden tekijöiden merkityksestä sen suhteen, kuinka pitkälle tulevaisuuteen niiden vaikutus kestää.

Kuva 7. Eräiden tietoturvatekijöiden vaikutuksen kesto: kuinka pitkälle tulevaisuuteen kyseisen tekijän voidaan katsoa ennakoivan hyvän tietoturvatason säilymistä.



[20] Tietoteknisten laitetilojen turvallisuussuositus (VAHTI 1/2002; http://www.vm.fi/tiedostot/pdf/fi/15209.pdf)

8.2.4 Tarjousten arviointi ja sopimukset

Tarjousten vertailussa vaikeutena on arvioida, mitä toimittajan vastaukset kertovat syvemmin tietoturvallisuustasosta. Eräänä ratkaisuna on edellä esitetty periaate, että suositaan selkeitä asteikkoja, joihin toimittajien tietoturvallisuustasot sijoitetaan (ks. kuva 7). Suurten tarjousten arviointi on ylipäätään vaikeaa, eivätkä ulkoistustarjoukset ole tässä poikkeuksia.

Tietoturvallisuuden osalta pisteytyksessä on suositeltavaa käyttää tietoturvapäällikön asiantuntemusta. On selvitettävä jo hankinnan alkuvaiheessa toimittajan kyky ja halu saattaa turvallisuusasioiden hoito sopimuspohjaiseksi. Tämä edellyttää myös kilpailuttavan organisaation taholta kykyä ja asiantuntemusta hyödyntää luotavaa järjestelyä asianmukaisesti.

8.2.5 Siirtymävaihe

Ulkoistuksen siirtymävaihe on ulkoistuksen tietoturvallisuuden ensimmäinen kriittinen vaihe. Potentiaalisia riskejä on paljon. Ulkoistusratkaisusta tyytymättömän henkilöstön tai siirron aiheuttamien käyttökatkosten riski on suurimmillaan juuri tässä vaiheessa.

Mikäli ulkoistukseen liittyy henkilöjärjestelyjä, on tehtävien siirrosta sovittava yksityiskohtaisesti. Siirtoon on varattava riittävästi aikaa ja sitä voidaan edistää yhteisillä työpajoilla, yhteystietoluetteloilla sekä redundanssilla (varakapasiteetti). Vaikka vastuu siis siirtyy tiettynä päivänä, on asiasta ennen vastanneen hyvä olla mahdollisuuksien mukaan valmiina auttamaan prosessissa.

Siirtoa tulee testata, mikäli se ulkoistuksen kohteen laajuuden, vaikeuden tai siinä käytettävien järjestelmien tietoliikenteen tai muiden seikkojen johdosta on mahdollista. Testaus pienentää varsinaisen tuotantokäytön käytettävyysongelmien riskiä, mutta on huolehdittava, ettei siinä käytetyn aineiston eheyden puute muodostu ongelmaksi. Testauksen tietoturvallisuutta on käsitelty VAHTI-ohjeessa Valtionhallinnon tietojärjestelmäkehityksen tietoturvasuositus[21] erityisesti luvussa 6.10.

Mikäli siirtymävaiheessa tarvitaan poikkeuksellisia tietoliikenneyhteyksiä, tulee näiden muodostamisessa hyödyntää VAHTI-ohjetta Turvallinen etäkäyttö turvattomista verkoista[22].

Siirtovaiheen huolellinen suunnittelu on molempien ulkoistusprosessin toimijoiden etujen mukaista.

Siirtymävaiheessa on mahdollista laatia vastaavuustaulukoita, joissa toimittaja ja ulkoistaja käyvät yhdessä läpi tietoaineiston, tietojärjestelmien ja muiden asioiden luokituksia ja sopivat vastaavuuksista.

---

[21] Valtionhallinnon tietojärjestelmäkehityksen tietoturvasuositus (VAHTI 3/2000; http://www.vm.fi/tiedostot/pdf/fi/3391.pdf)

[22] Turvallinen etäkäyttö turvattomista verkoista (VAHTI 2/2003; http://www.vm.fi/tiedostot/pdf/fi/44978.pdf)

8.3 Ulkoistettu palvelu

Ulkoistetun palvelun tietoturvallisuuden valvonta riippuu ratkaisevasti palvelun tyypistä. Palvelukohtaisesti on saatavilla erilaisia tietoturvallisuuden tarkistuslistoja ja suosituksia, joita tulee soveltaa. Kohteesta riippumatta turvallisuutta voidaan edistää seuraavilla tavoilla:

1. Ulkoistuspalvelun tarjoajan hallinnollisen tietoturvallisuuden valvonta. Tämä valvonta toimii, mikäli tarjoajan hallinnollinen tietoturvallisuus on hyvin hoidettu. Ulkoistuspalvelun asiakas voi pyytää arvion palveluntarjoajan tietoturvallisuuden yleistilanteesta, turvallisuuden kehittämisen suuntaviivoista tai muista vastaavista asioista. Raporttien tulee olla yleisluontoisia, eivätkä ne voi olla liian yksityiskohtaisia, jotta ne eivät vaarantaisi palveluntarjoajan tietoturvallisuutta.
2. Ulkoistuspalvelun asiakkaan on syytä pitää huolta, että tietoturvallisuus on mukana ulkoistuspalvelun laatuarvioinnissa ja yhteistyöpalaverien vakioasioiden listalla.
3. Auditoinnit ovat oikein käytettynä hyvä keino myös ulkoistettujen toimintojen valvontaan. Niitä tulee käyttää ja tarpeen mukaan hyödyntää ulkopuolista, mahdollisimman asiantuntevaa ja puolueetonta asiantuntijaa.
4. Ulkoistetun palvelun hyötyjä ja mahdollisia ongelmia tulee jatkuvasti arvioida peilaten palvelua organisaation toiminnalle asetettuihin tulostavoitteisiin erilaisten mittarien avulla (ks. VAHTI 2/2004[23]). Tällöin on mahdollista muodostaa kokonaiskuva ulkoistustoimintaan mahdollisesti kohdennettavista muutoksista, kuten laajentaminen ja supistaminen.

8.4 Muutoksia ulkoistuksessa

Ulkoistetun toimintokokonaisuuden suhteen tapahtuvien muutosten tulee olla muun prosessin tapaan hallittuja. Kaikissa muutosvaiheissa on korostettava selkeiden ja yksityiskohtaisten sopimusmääräysten tärkeyttä.

8.4.1 Laajentaminen ja supistaminen

Toiminnon tai palvelun sisällön muuttaminen kuuluu sen elinkaareen. Ulkoiset muutokset, sisäinen kehittäminen tai teknologinen kehitys voivat muuttaa ulkoistetun palvelun sisältöä tai sen laajuutta. Toiminnallisessa laajennuksessa (kuten uusia palveluja käyttöön otettaessa) on pyrittävä laajentamaan hyväksi havaittuja tietoturvamenettelyjä uuteen osaan ja otettava huomioon uuden toiminnallisuuden asettamat uudet vaatimukset

[23] Tietoturvallisuus ja tulosohjaus (VAHTI 2/2004; http://www.vm.fi/tiedostot/pdf/fi/86049.pdf)

tietoturvallisuudelle. Lähtökohtana voidaan käyttää uuden palveluosan tietoturvakuvauksia tai muuta vastaavaa dokumentaatiota.

Palvelun laajentamisen vastakohta – sen supistaminen – edellyttää myös suunnittelua. Käytettävyyteen liittyvät asiat korostuvat ja lopetettavan palvelun tietoaineiston turvallisuus on huomioitava. Toimittajalle on tähdennettävä, että esimerkiksi vaitiolositoumukset ovat edelleen voimassa.

Palveluiden supistaminen suunnitelmallisesti ja ennakoidusti on tietoturvallisuuden kannalta suositeltavaa.

8.4.2 Toimittajan vaihtaminen

Ulkoistetussa palvelussa toimittajan ja asiakkaan välinen suhde on tiiviimpi kuin tavallisessa ostaja-myyjä -suhteessa. Syvemmälle viety kumppanuus palvelujen kehittämisessä tuottaa ainakin hetkellistä tehokkuutta, mutta ei lainsäädännön rajoitteista johtuen voi muodostua kovin syvälliseksi. Kynnys toimittajan vaihtoon on kuitenkin yleensä korkea. Tilanteeseen on syytä kuitenkin varautua monesta syystä. Liika riippuvuus yhdestä toimittajasta on kuitenkin riski eikä nopeasti muuttuvassa toimintaympäristössä ole takeita siitä, että toimittaja tai toimittajan tarjoama ratkaisu on jatkuvasti paras mahdollinen. Jo hankintalainsäädäntö edellyttää säännöllistä kilpailuttamista.

On tuotu esille, että hankintalainsäädännön vaatimuksesta säännöllisesti tapahtuvat ulkoistuskilpailutukset eivät kiinnosta kaikkia potentiaalisia toimittajia. Nämä jättäytyvät kilpailusta pois, koska pitävät sitä etukäteen ratkaistuna palvelun nykyisen tarjoajan hyväksi.

Toimittajan vaihtumisen mahdollisuus on otettava huomioon jo tarjouspyyntövaiheessa. Tarjoajilta voidaan pyytää luettelemaan referenssejä, joissa he ovat luovuttaneet (tai vastaanottaneet) palvelun tarjoamisen toiselle yritykselle. Tämä osoittaa, että palvelun tarjoaja osaa myös käytännössä toimittajan vaihtamiseen liittyvät asiat. Palvelun käytettävyys ei näin vaarannu tilanteessa, jossa nykyinen toimittaja on menettämässä ainakin osan liiketoiminnastaan kilpailijalle.

Toimittajan vaihtamisen tietoturvaongelmista yleisimpiä ovat käytettävyysongelmat välittömästi palveluntarjoajan vaihtamisen jälkeen. Tietojen luottamuksellisuuteen liittyvät rajoitukset ovat toinen potentiaalinen ongelma. Vanhalle palvelun tarjoajalle jää yleensä luottamuksellista tietoa. On syytä tähdentää NDA- ja muiden sopimusten voimassaolon jatkumista. Tietovälineiden käsittelyn valvominen on myös äärimmäisen vaikeaa. Toimittajan kanssa voidaan sopia kaikkein kriittisintä tietoaineistoa sisältävien tietovälineiden tuhoamisesta, mutta merkittävä osa vastuusta ja medioista jää toimittajalle. Niiden osalta on luotettava toimittajan tietoturvallisuuden hallintajärjestelmän toimivuuteen.

Uuden ja vanhan toimittajan välisen yhteistyön järjestäminen parantaa tietoturvallisen toimittajavaihdon edellytyksiä. Erityisesti palvelun käytettävyyden kannalta tämän merkitystä ei tule aliarvioida. Mikäli väistyvä toimittaja on sopimuksissa sitoutunut palvelun

lopettamisen vaatimaan yhteistyöhön jo sopimusta aikoinaan solmiessaan, ovat mahdollisuudet joustavaan ja tietoturvalliseen toimittajavaihtoon hyvät.

8.4.3 Ulkoistuksen lopettaminen

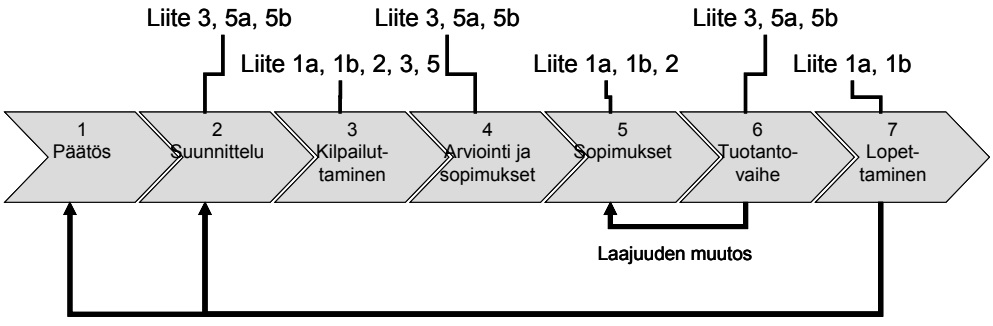
Ulkoistetun palvelun lopettamisen tietoturvaongelmat muistuttavat edellä kuvattuja tilanteita. Toiminto voidaan lopettaa kokonaan tai se voidaan ottaa takaisin sen ulkoistaneelle organisaatiolle. Ensimmäisessä tapauksessa tietoaineiston käsittely korostuu ja käytettävyysongelmat hoidetaan yleensä samalla tavalla kuin palvelussa, joita ei ole ulkoistettu. Palvelun siirtäminen takaisin omaan tuotantoon on ollut melko harvinaista, mutta valtionhallinnon tukitoimintojen keskittämisen myötä kuvatun kaltaisia tilanteita saattaa syntyä.

Ulkoistuksen lopettaminen tulee tarpeelliseksi, kun toiminto muuttuu kokonaan tarpeettomaksi tai se korvaantuu uudella organisaation omalla toiminnolla.

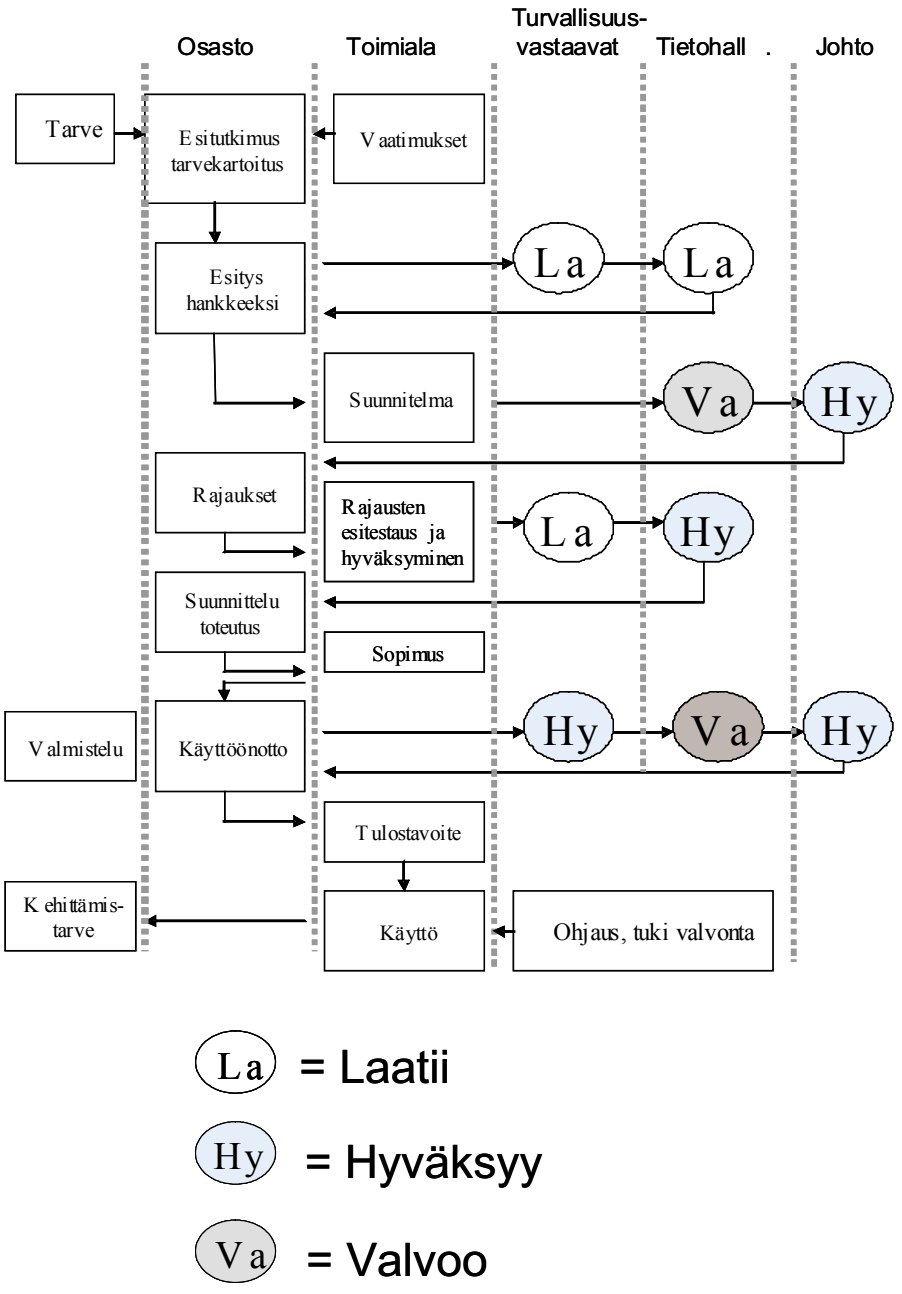
8.5 Liitteiden käyttö ulkoistuksen elinkaaren vaiheissa

Tämän ohjeen liitteenä on sopimusmalleja, tarkistuslistoja ja muuta materiaali, joita voidaan hyödyntää ulkoistuksen elinkaaren eri vaiheissa. Alla oleva kuva kertoo missä elinkaaren vaiheessa kullekin ohjeelle arvioidaan olevan eniten käyttöä. Kuva on viitteellinen, ja tapauskohtaista soveltamista ei saa unohtaa. Tarkistuslistojen ja sopimusten käyttö edellyttää niiden valmistelua. Niinpä esimerkiksi tarkistuslistoja (liite 5) on valmisteltava ulkoistusta suunniteltaessa, jotta ne olisivat käytettävissä kilpailuttamisvaiheessa ja myöhemmin tuotantovaiheessa. Turvallisuussopimukset ovat ajankohtaisia sopimuksia solmittaessa ja niitä purettaessa; turvallisuussopimuksen eräät kohdat ovat voimassa, vaikka varsinainen toimitussopimus (pääsopimus) puretaan.

Kuva 8. Tämän ohjeiden liitemateriaalin käyttö ulkoistuksen elinkaaren vaiheissa.



Kuva 9. Erään valtionhallinnon organisaation käyttämä malli ulkoitusprojektin vaiheista.



9 ERITYISKYSYMYKSIÄ

9.1 Ulkoistamisen suunnittelu ja hallinta henkilötietojen käsittelyssä

Ulkoistettaessa henkilötietojen käsittelyä edellyttäviä tehtäviä on suunnittelussa otettava huomioon erityisesti henkilötietolain vaatimukset. Esimerkiksi henkilötietoja koskevat tietojenkäsittelypalvelut voidaan ulkoistaa palvelut hankkivan viranomaisen (eli rekisterinpitäjän) lukuun. Tällöin palvelujen hankkimisesta tehdään toimeksiantosopimus palvelut tilaavan viranomaisen (toimeksiantaja) ja palveluntuottajan (toimeksisaaja) välillä. Kyseinen viranomainen vastaa tällöin rekisterinpitäjänä tietojenkäsittelyn ja muun toiminnan lainmukaisuudesta. Palvelun tuottaja vastaa käsittelystä osapuolten välillä tehtävän toimeksiantosopimuksen mukaisesti. Toimeksiantajan lukuun sopimuksen perusteella tapahtuva henkilötietojen käsittely on rekisterin käyttöä, eikä henkilötietojen antaminen toimeksisaajalle tietojenkäsittelyä varten ole sellaista henkilötietojen luovuttamista, johon tarvittaisiin asianomaisen rekisteröidyn henkilön suostumus. Toimeksisaajalla ei ole toisaalta oikeutta käyttää toimeksiantosuhteessa saamiaan henkilötietoja omassa toiminnassaan eikä käsitellä niitä vastoin sopimusta.

Tietoturva- ja tietosuojariskit lisääntyvät ja muuttuvat kun tietojenkäsittelypalveluja hankitaan ulkopuoliselta toimijalta. Sen vuoksi on tärkeää, että ulkoistussopimuksessa määritellään riittävän yksityiskohtaisesti, mitä eri käsittelyjä ja tehtäviä palveluntuottaja tekee ja mistä se vastaa sekä mitkä tehtävät ja vastuut jäävät tilaajan tehtäväksi ja vastuulle. Yhtenä sopimukseen kuuluvana osana määritellään, miten tietoturvallisuus yleensä ja eri käsittelyvaiheissa varmistetaan. Henkilötietolain näkökulmasta tietoturvallisuus toteuttaa erityisesti henkilötietolaissa säädettyä suojaamisvaatimusta. Tietoturvallisuuden ja tietojen suojaamisen suunnittelu ja toteutus on henkilötietojen kaikkiin käsittelyvaiheisiin liittyvä vaatimus.

Vastuiden määrittelyn kannalta on tärkeää, että sopimuksen oikeudellinen luonne on selvästi todettu sopimuksessa (toimeksiantosopimus). Tähän liittyen on myös huomattava, että viranomaisen toiminnan julkisuudesta annetun lain 5.2 §:n perusteella viranomaisen toimeksiannosta tuotettaviin asiakirjoihin sovelletaan julkisuuslakia. Tämä seikka on tarpeen todeta toimeksiantosopimuksessa.

Onnistuneen ulkoistamisen ja sopimuksenteon edellytyksenä on, että viranomainen tuntee ja hallitsee ulkoistettavaan tehtäväänsä liittyvät prosessit ja on arvioinut toimintaan liittyvät henkilötietojen käsittelyt henkilötietolain vaatimukset huomioon ottaen. Tähän liittyvinä toimenpiteinä edellytetään, että

- viranomainen on kartoittanut ja kuvannut asiakirja-aineistonsa sekä määritellyt muun ohella tehtävissään eri käyttötarkoituksiin muodostuvat henkilörekisterit
- viranomaisella on kuvaus myös ulkoistettavaksi suunnitellussa toiminnossa käytettävästä henkilörekisteristä, rekisterinpitoon liittyvistä prosesseista ja tehtävien edellyttämistä henkilötietojen käsittelyistä sekä käsittelyn vastuista mukaan lukien tietoturvallisuuden toteuttaminen
- kuvaus on tehty toiminnalliset, tekniset ja lainsäädännön vaatimukset huomioon ottaen, jolloin käsittelyssä toteutuu henkilötietolain edellyttämä hyvä tietojenkäsittelytapa ja julkisuuslain edellyttämä hyvä tiedonhallintatapa. Esim. tarpeettomia ja virheellisiä tietoja ei saa kerätä eikä tallettaa ja käsittelyssä on huomioitu huolellisuus- ja suojaamisvelvoitteet, käyttötarkoitussidonnaisuuden vaatimus sekä rekisteröityjen oikeuksien toteuttaminen.

Esimerkkejä eri tehtävistä, joissa muodostuu henkilörekisteri

- Valtiokonttori hoitaa laissa säädettynä eri tehtävinään:
  1) valtion henkilöstön eläkeasioita
  2) valtion tapaturma-asioita
  3) muita laissa erikseen säädettyjä tehtäviä, joissa kussakin muodostuu erillinen henkilörekisteri.
- Väestörekisterikeskus hoitaa laissa säädettynä tehtävänään:
  1) väestötietojärjestelmän ylläpidon.

Kumpikin mainittu virasto tarvitsee henkilöstönsä palkkaamiseksi ja palvelusuhteeseen liittyvien tehtävien hoitamiseksi:

1) henkilöstöhallinnon rekisterin
2) työnhaussa muodostuvat rekisterit.

Suunnittelussa on hyvä huomata, että samaan henkilörekisteriin kuuluvat kaikki ne tiedot, joita käsitellään kyseisen tehtävän hoitamiseksi (rekisterin käyttötarkoitus). Hyvän tiedonhallinnan aikaansaaminen edellyttää, että kuvattuna on se kokonaisuus, joka tietyssä rekisterinpitäjän tehtävässä muodostuu (looginen henkilörekisteri). Vaikka tietojärjes-

telmä voidaan toteuttaa osatoiminnoittain, toiminnan ja tietojenkäsittelyn tarpeiden suunnittelu ja toteuttaminen edellyttää, että suunnittelun pohjana on kokonaiskuva tehtävästä ja sen eri osatoiminnoista ja prosesseista.

Ulkoistaminen voidaan toteuttaa eri tavoin, esimerkiksi

- viranomainen hankkii tietojenkäsittelypalveluita tai muita palveluja yksityiseltä yritykseltä
- viranomainen voi hankkia tietojenkäsittely- ja muita palveluja toiselta viranomaiselta.

Suunniteltaessa ulkoistettavia tehtäviä ja niihin liittyviä henkilötietojen käsittelyjä ulkoistaminen kuvataan osana kyseistä tehtävään liittyvää rekisterinpitoa:

- tässä yhteydessä suunnitellaan yksityiskohtaisesti, mitä tehtäviä ja vastuita henkilötietojen käsittelyissä mahdollisen palveluntuottajan edellytetään hoitavan, sekä mitkä tehtävät jäävät rekisterinpitäjälle, mitä mahdollisia riskejä ja uhkia järjestelyihin liittyy, miten ne voidaan ratkaista, miten erilaiset menettelyt on tarkoitus hoitaa, sekä mitä palvelun tuottajan edellytetään ottavan huomioon tietoturvallisuuden ja tietojen suojaamisen vaatimusten täyttämiseksi käsittelyjen eri vaiheissa
- huolellisen suunnittelu- ja valmistelutyön pohjalta voidaan tehdä asian edellyttämät tarjouspyynnöt sekä laatia sopimukset riittävän yksityiskohtaisesti
- sopimuksissa osapuolten tehtävät ja vastuut on kuvattava riittävän yksityiskohtaisesti, jotta tiedetään mistä on sovittu ja jotta mahdollisiin sopimusrikkomuksiin voidaan puuttua
- on myös tärkeää ennakoida ja sopimuksessa määritellä sopimuksen päättymiseen liittyvät tilanteet sekä ne tehtävät ja velvoitteet, jotka osapuolten tässä yhteydessä tulee hoitaa.

Kun rekisterinpitäjä suunnittelee ulkoistusta, suunnittelu tulee toteuttaa kuvaamalla, mitkä rekisterinpitäjän tehtävistä ja osatehtävistä ja niihin liittyvistä henkilötietojen käsittelytehtävistä aiotaan ulkoistaa. Jokaiseen käsittelyvaiheeseen liittyy myös tietojen suojaamisen ja tietoturvallisuuden vaatimuksia. Suunnittelu tehdään loogisen rekisterikäsitteen pohjalta siten, että kaikki kyseisessä tehtävässä muodostuvan aineiston (atk ja manuaalinen) käsittely ja työnkulut kuvataan.

Alla oleva taulukko kuvaa, millä tavoin rekisterinpitäjän on tarpeen kuvata ja arvioida rekisterinpidon toiminnallisuus ja lainmukaisuus (kuva 10).

Kuva 10. Yhdistelmä henkilötietojen käsittelyn kuvausmallista (Lähde: Tietosuojavaltuutetun toimisto).

REKISTERINPITÄJÄ: (ks. Henkilötietolaki 3.1§ k4): esim. Virasto X REKISTERIN KÄYTTÖTARKOITUS: (ks. HetiL 3.1.§ k3, 6 §): esim. henkilöstöhallinnon rekisteri					
Käsittelyvaihe	Kuvaa toiminnan edellyttämät käsittely-tarpeet/ toteutus vaiheittain/ osatehtävit-täin +vastuut	Kuvaa ja arvioi tietosuojaan kohdistuvat uhat ja riskit käsittely-vaiheittain	Määrittele käsittelyn menettelytavat, tietoturvan ja tietojen suojaamisen toteutus vaiheittain - kuka tekee - mitä tekee - millä tavoin	Määrittele ja var-mista käsittelyn ja menettelyjen oikeud. edellytykset - arviointi käsittely-vaiheittain HetiL:n ja mahd. erityis-säännösten mukaisesti - Joka kohdassa on otettava huomioon erityissäädökset	Ulkoistetta-vassa toiminnassa palvelun tuottajalle suunnitellut tehtävät ja vastuut
Tietojen kerääminen ja tietosisältö - mitä tietoja - tietolähteet, tiedonsaannin peruste, ym.				- HetiL 9 § - työelämän tietosuojalaki (TyTSL)- mahd. erityissäännökset	
Rekisterin sisäinen käyttö ja suojaaminen (ml. tietoturva)				- HetiL 5 §, 32 § - mahd. erityis-säännökset (esim. JulkL 18 §)	
Luovuttaminen-kenelle - mikä tarkoitus - mitä tietoja - millä perusteella				- HetiL 8 §, 12 §, 5 §, 9 §, 32 § - mahd. erityis-säännökset (esim. JulkL 16.3 §)	
Säilyttäminen ja hävittäminen-säilyttämisaika - aktiivi- ja passiiviaika-menettelytapa				- HetiL 34 §, 5 §, 9 §, 32 § - mahd. erityis-säännökset (esim. ArkistoL)	
Rekisteröityjen informointi - mistä ja miten				- HetiL 24 §, 3.1 § k 7 - TyTSL	
Rekisteröityjen oikeuksien toteutus - tarkastus-, virheen korjaus ja kielto-oikeus				- HetiL 26-29 §, - mahd. erityissäännökset	
Muut tarpeellisten käsittelyvaiheiden kuvaukset				- HetiL 5 §, 9 §, 32 § - TyTSL 16 § - 23 §	

Seuraavassa kuvassa esitetään toisesta näkökulmasta se kokonaisuus ja eri elementit, jotka tulee olla määriteltynä henkilötietojen käsittelyssä ja käsittelyä ylläpitävän tietojärjestelmän suunnittelussa ja toteutuksessa (kuva 11). Samat asiat tulee arvioida palvelun-tuottajan toiminnan osalta, kuitenkin huomioon ottaen käsiteltäväksi annetut tehtävät ja käsittelyt.

Kuva 11. Henkilörekisterin suunnittelu (Lähde: Tietosuojavaltuutetun toimisto).

Esimerkki.
XX-käyttötarkoituksessa perustetun henkilörekisterin ylläpitämiseen suunniteltavasta tietojärjestelmästä.

LOOGINEN REKISTERI
- rekisterinpitäjäorganisaation itsensä toteuttama käsittely
- ulkopuolisen palveluntuottajan rekisterinpitäjän lukuun toimeksiantosopimuksen perusteella toteuttama käsittely
® käsittely kuuluu rekisterinpitäjäorganisaation loogiseen henkilörekisteriin

Rekisterinpitäjän oma toiminta:

Kaavio tietojärjestelmien suunnittelun ja toteutuksen elementeistä HetiL:n vaatimusten kannalta arvioituna:

Käyttötarkoitus, tietosisältö ja tietovirrat: Toiminta-analyysi

Henkilörekisterin käyttötarkoitus, tietosisältö ja rakenne, tietolähteet, käyttö ja luovutukset, säilyttäminen, ml. ulkopuoliset palvelut, rekisteröityjen oikeuksien toteuttaminen

Rekisterin ja sovelluksen rakenne/arkkitehtuuri

Tietorakenteet, tietotasot ja -ryhmät

Tietojen siirto-tarve (käyttö), suojaaminen ja valvonta toiminta-yksikössä eli rekisterinpitäjän omassa toiminnassa

Tietojen siirto-tarve (luovutus) kahden toiminta-yksikön ja rekisterinpitäjän välillä, tiedon luovutustavat, tiedonsiirron "auktorisointi" ja valvonta

Tietojen säilyttämis-tarpeen mukainen rakenne ja hävittäminen

Tietojen päivitys- ja korjaamismenettely

Sovellusrakenne

Laitteistoarkkitehtuuri

Laitteiston ja tiedonsiirtoverkon tekniset tietosuoja- ja tietoturvaratkaisut

Kuva/Tietosuojavaltuutetun toimisto. Laatineet M.K./R-T. P.

TOIMEKSI-ANTO-SOPIMUS

Palveluntuottajalle (toimeksisaajalle) suunnitellut tehtävät:

Kuvaus ja analyysi toimeksisaajalle suunniteltavista tehtävistä ja vastuista, mm.

- henkilötietojen käyttöön ja muuhun käsittelyyn, esim. luovuttamiseen liittyvät tehtävät
  *
  *
  *
- tietoturvaan ja tietojen suojaamiseen liittyvät tehtävät,vaatimukset ja vastuut
- laitteistoon ym. liittyvät vaatimukset ja vastuut
- henkilöstöä koskevat salassapito- ym. vaatimukset
  * käyttäjä- ja vaitiolositoumus
- muut käsittelyyn liittyvät tehtävät ja vastuut (esim. informointi ja rekisteriselosteen saatavillapito)

Tietoturvallisuuden varmistamisen velvoite kuuluu kaikkiin käsittelyvaiheisiin ja kaikkiin tietojärjestelmän toteutuksen tasoihin ja osiin

Liitteenä 5 on henkilötietojen käsittelyä koskevan toimeksiantosopimuksen tekemisen tarkistuslista, jossa esimerkinomaisesti on lueteltu minkä tyyppisistä asioista sopimuksissa tulisi olla sopimusmääräykset.

9.2 Jatkuvuuden turvaaminen[24]

Ulkoistamiseen liittyy aina useita riskejä. Siksi hankkeen alkuvaiheissa on syytä laatia riskikartoitus, jota käydään läpi ja tarkennetaan ulkoistamisprosessin edetessä. Riskienhallinnan hyvä väline kumppanuusvaiheessa on palvelutasosopimus (Service Level Agreement eli SLA), jossa tulisi olla selkeitä mittareita tavoitteineen kartoituksessa esiin tulleista asioista sekä varaus tarkastusoikeuteen.

Kun organisaatio suunnittelee siirtymistä käyttämään palvelutoimittajaa, on otettava huomioon mahdollisimman aikaisessa vaiheessa myös toimintojen jatkuvuuden turvaaminen erilaisten häiriöiden ja poikkeusolojen varalta. Jo tarjouspyyntövaiheessa on selvitettävä toimittajien omat jatkuvuussuunnitelmat. Asiakkaalle saattaa olla aiheellista tietää, miten toimittaja reagoi esimerkiksi suurta asiakasjoukkoa kohtaavassa laajassa palvelukatkostilanteessa.

Toimittajan jatkuvuussuunnitelmien tason selvittäminen tarjousvaiheessa ei aina ole yksinkertaista. Eräitä keinoja tähän ovat:

- Toimittajaa pyydetään esittämään toipumissuunnitelmansa. Mikäli toimittaja vetoaa niiden luottamuksellisuuteen, voidaan pyytää tietoturva- tai valmiuspäällikköä esittelemään suunnitelmat yleisluontoisella tasolla.
- Toimittajan valmiuspäällikön tai tietoturvallisuusjohtajan tapaaminen, jossa arvioidaan toimittajan valmiuksia suunnitelmien pohjalta.
- Pyydetään toimittajaa selvittämään seuraavat asiakokonaisuudet:
  - Milloin toipumissuunnitelmia on viimeksi testattu?
  - Miten suunnitelmien testaus on tehty?
  - Koska toipumissuunnitelmat on laadittu ja koska ne on viimeksi päivitetty?
  - Kuka henkilö vastaa toipumissuunnitelmista? Onko kyseessä tietoturvapäällikkö, vai hoidetaanko asiaa muun työn ohessa?
  - Onko ulkopuolinen taho auditoinut toipumissuunnitelmat?
  - Asiakkaat, joilla on samankaltaisia vaatimuksia toipumis- tai valmiussuunnitelmien suhteen? Näiden arviot toimittajasta?
- Toimittajaa pyydetään arvioimaan, millaiset uhat todennäköisimmin aiheuttavat toipumissuunnitelmiin turvautumisen. Mikäli toimittajan näkemykset poikkeavat suuresti asiakkaan näkemyksistä tai ovat liian yleisluontoisia, on syytä pyytää täsmennyksiä tai ulkopuolista arviointia.

[24] Lisätietoja on löydettävissä Huoltovarmuuskeskuksen verkkosivuilta http://www.huoltovarmuus.fi/ (http://www.nesa.fi/)

Käsiteltäessä toipumissuunnitelmia ulkoistuspalveluita tarjoavan yrityksen kanssa on otettava huomioon, että sanaa ”toipumissuunnitelma” voidaan käyttää kolmessa erilaisessa, mutta toisiinsa liittyvässä merkityksessä:

1. palvelutoimittajan oma toipumissuunnitelma (esim. käyttöpalveluiden toipumissuunnitelma)
2. ulkoistavan organisaation toipumissuunnitelma
3. ulkoistetun toiminnon (esim. tietojärjestelmän) toipumissuunnitelma.

Ulkoistussuhteen alkaessa on palvelutoiminnan osalta oltava myös valmiina vastaava suunnitelma ja sen säännöllisestä päivittämisestä on huolehdittava. Yleensä toimittajat tarjoavat vain normaaliolojen käytettävyyspalveluja, joten vastuu poikkeusolojen jatkuvuus- ja toipumispalveluiden huomioimisesta ja saattamisesta sopimustasolle jää helposti asiakkaan vastuulle. Asiakkaan on tuotava selkeästi esiin poikkeusoloja koskevat vaatimuksensa jo tarjouspyyntövaiheessa.

IT-toimintoihin kaikissa ympäristöissä liittyvistä riskeistä yleisimpiä ovat erilaiset tietoliikennehäiriöt ja -katkokset, haittaohjelmien leviäminen, operointi- ja konfigurointivirheet, sähkönsyötön häiriö tai katkos, järjestelmiin tunkeutuminen, ohjelmistovirheet sekä laiteviat. Inhimilliset virheet ovat myös varsin yleisiä häiriöiden syitä. Näiden lisäksi on olemassa runsaasti organisaatiokohtaisia riskitekijöitä. Ulkoistamisen yhteydessä riskit muuttuvat: joidenkin todennäköisyys kasvaa ja joidenkin pienenee. Poikkeusoloissa riskitekijöiden hallinta on entistä vaikeampaa ja kriittisempää. Siksi ulkoistamisvaiheessa on syytä muistaa seuraavat asiat:

- On luotava selkeä käsitys ulkoistettavasta kokonaisuudesta: toimittajan ja asiakkaan välinen vastuunjako on selvitettävä myös tilanteissa, joissa jommankumman toiminta vaarantuu.
- Oma osaaminen ja toiminnon hallintakyky tulee säilyttää.
- Toimittajan osaamista esimerkiksi varautumissuunnittelun osalta on osattava hyödyntää täysimääräisesti.
- Ulkoistetun toiminnan valvonnan on oltava kattavaa myös jatkuvuussuunnitelmien osalta.
- Vastuut ja velvoitteet on oltava selvitetty ja niistä tulee sopia kirjallisesti myös häiriö- ja poikkeusolojen varalta.
- Muutoksista tulee raportoida ja huomioida niiden vaikutus myös jatkuvuussuunnitelmissa.
- Jatkuvuussuunnitelmat ja poikkeusolojen varalta laaditut suunnitelmat tulee päivittää aina muutosten yhteydessä ja käydä ne vuosittain yhteisesti lävitse.

Silloin kuin palvelutoimittaja on ulkomaalainen tai ulkoistuksesta osa annetaan ulkomaalaisen osapuolen hoidettavaksi, on oleellista selvittää mm. mistä maasta palvelut tuotetaan, missä laitteistot ja niissä oleva tieto sijaitsevat ja minkä maan lakia eri tilanteissa

sovelletaan. Jatkuvuussuunnittelussa näihin kysymyksiin on paneuduttava erityisen huolellisesti.

Esimerkki: *Puolustustaloudellisen suunnittelukunnan teettämä, suurille käyttäjäorganisaatioille kohdistettu selvitys osoitti, että tietojenkäsittelypalveluita ostavista organisaatioista noin 65 % oli sisällyttänyt ulkoistetut palvelut varautumissuunnitelmiinsa, noin puolet oli päivittänyt sen, mutta alle 10 % oli testannut suunnitelman. Palvelutoimittajan kanssa tehty normaaliolojen jatkuvuus- ja toipumissuunnitelma oli noin 10 %:lla vastaajista ja poikkeusolojen osalta vain 3 %:lla*[25].

[25] Tiedonkäsittelypalveluiden keskittymisen vaikutus huoltovarmuuteen (PTS:n tietoyhteis-kuntasektorin tietotekniikkapoolin julkaisu 1/2005; http://www.huoltovarmuus.fi/documents/3/JULK_TJJ_2005-1_TK-palveluiden_keskittymisen_vaikutus_huoltovarmuuteen.pdf)

LIITE 1: TURVALLISUUSSOPIMUS-MALLIT

LIITE 1A: MALLI TURVALLISUUSSOPIMUKSESTA ULKOISTUKSEN YHTEYDESSÄ

Malli perustuu Valtiokonttorin käyttämälle sopimukselle.

TURVALLISUUSSOPIMUS

Ulkoistaja ja [Oy Yritys Ab] ovat tehneet tänään [tarjousta/sopimusta/työtä] koskevan turvallisuussopimuksen. Osapuolet katsovat toistensa olevan luotettavia yhteistyökumppaneita, joka mahdollistaa kaupallisten sopimusten tekemisen.

[Oy Yritys Ab] sitoutuu pitämään salassa kaikki tarjouskilpailu- ja esisuunnitteluyhteistyön aikana sekä varsinaisissa hankkeissa esille tulevat Ulkoistajan salassa pidettävät (luottamukselliset, salaiset, erittäin salaiset) tiedot. Tällaisia ovat muun muassa kaikki salaisiksi luokitellut tiedot, henkilöstöä ja Ulkoistajaa koskevat tiedot sekä turvallisuus- ja varautumisjärjestelyt, rakenteet ja tekniset järjestelmät. [Oy Yritys Ab] käsittelee edellä ja jäljempänä mainittuja asioita vain työn edellyttämässä laajuudessa.

[Oy Yritys Ab] sitoutuu myös säilyttämään ja käsittelemään työhön liittyviä asiapapereita, laitteita, koneita, valokuvia, piirustuksia, tietolevyjä ja vastaavia Ulkoistajan kannalta salassa pidettäviä tavaroita siten, että ne eivät joudu ulkopuolisten haltuun, tutkittavaksi tai tietoon. Edellä mainittujen asiakirjojen tai muiden tallenteiden olemassaolon ilmaiseminen on myös kiellettyä.

[Oy Yritys Ab] vastaa siitä, että Ulkoistajan järjestelmien käyttö on mahdollista ainoastaan niille henkilöille, joille on määritelty oikeudet käyttää järjestelmää. [Oy Yritys Ab] huolehtii käyttövaltuuksien mukaisesta käyttöoikeuksien toteuttamisesta sovittujen toimintatapojen mukaisesti. [Oy Yritys Ab] vastaa käyttöjärjestelmätason määrittelyistä siten, että järjestelmiin kirjautuminen on mahdollista ainoastaan nimetyille henkilöille. [Oy Yritys Ab] seuraa ja raportoi Ulkoistajalle epäonnistuneet yritykset sekä mahdolliset havainnot poikkeavasta toiminnasta.

Edellä mainittujen asiakirjojen tai muiden tallenteiden kopioiminen, vieminen pois toimitiloista tai muistiinpanojen tekeminen turvallisuussalaisuuksista on kielletty ilman erillistä lupaa. Yhteistyön päätyttyä yhteisesti sovittavana ajankohtana [Oy Yritys Ab] ja sille suoritteita tehneet yritykset palauttavat kaikki työhön liittyvät dokumentit ja tallenteet Ulkoistajan hallintaan, tai tuhoavat ne sovitulla tavalla.

[Oy Yritys Ab] vastaa omien tilojensa osalta fyysisestä turvallisuudesta ja ohjeistamisesta siten, että ainoastaan palvelun tuottamiseen tarvittavien henkilöillä on pääsyoikeus Asiakkaan käytössä oleviin laitteistoihin. [Oy Yritys Ab] varmistaa konesalin fyysisen turvallisuuden tulipalon, sähkökatkosten, vesivaurioiden, ulkopuolisten häiriötekijöiden yms. poikkeavien tilanteiden varalta sekä huolehtii konesaleilta edellytettävästä kulunvalvonnasta, ilmastoinnista ja ilman kosteudesta. [Oy Yritys Ab] huolehtii tietoaineistojen turvallisuudesta myös huoltotilanteissa.

[Oy Yritys Ab] saattaa yrityksen työhön liittyvän henkilöstön tietoiseksi tämän sopimuksen vaitiolovelvoitteista sekä sitoutuu valvomaan sitä, että he noudattavat sopimusta. [Oy Yritys Ab] hyväksyttää työhön liittyvän henkilöstön toimittamalla henkilöihin liittyvät tarpeelliset asiakirjat Ulkoistajan turvallisuusjohtajalle luotettavuuslausuntoa varten. Hankkeen henkilöt tekevät oheisen liitteen mukaisen vaitiolositoumukset ennen kaupallisen sopimuksen syntyä.

[Oy Yritys Ab] huolehtii tunnettujen tietoturvaongelmien korjaamisesta, käyttöjärjestelmä- ja varusohjelmistotoimittajien ohjeiden mukaan. [Oy Yritys Ab] huolehtii verkon palvelinten, työasemien ja muiden laitteiden konfiguraation tietoturvallisuuden toteuttamisesta (kirjaa sähköiseen seuranta- tai lokitiedostoon).

Mikäli [Oy Yritys Ab] käyttää alihankkijoita tai -palveluja, sen tulee hyväksyttää ne ja niissä työskentelevä henkilöstö Ulkoistajan turvallisuusjohtajalla ennen aliurakointia. Tämä sopimus on saatettava kyseisten yritysten ja henkilöiden tietoon.

[Oy Yritys Ab] vastaa varmistus- ja palautuskäytännössä siitä, että mahdollisen laiterikon yms. tapahduttua järjestelmät saadaan palautettua ja rakennettua toimivaksi kokonaisuudeksi järjestelmäkohtaisesti ennakkoon sovittavassa ajassa. [Oy Yritys Ab] tulee olla Asiakkaan järjestelmiä koskien elpymis- ja toipumissuunnitelma oman palvelutoimintansa varmistamiseksi. Poikkeusoloihin varautumiseen liittyen [Oy Yritys Ab] huolehtii turvakopioiden valmistelusta ja säilyttämisestä toisella paikkakunnalla kuin varsinainen palvelutoiminta tapahtuu. Kansallisiin poikkeusoloihin varautumisesta tehdään erillinen varautumissuunnitelma.

[Oy Yritys Ab] käyttämän yhteyden kautta eivät saa päästä muut organisaatiot tai muut [Oy Yritys Ab] organisaation osat Asiakkaan tietoverkkoon ja laitteistoihin kuin rakennettavan palvelun toimittamiseen tarkoitetut ja valtuutetut henkilöt. [Oy Yritys Ab] tulee järjestää suojaus mahdollisimman pitkälti teknisin keinoin sekä huolehtia, että kaikki yhteydenotot ja toimenpiteet on todennettavissa jälkikäteen.

[Oy Yritys Ab] tulee toteuttaa tarvittaessa Asiakkaan verkkoyhteyden avaaminen sähköisen tunnistekortin tms. sellaisen sähköisesti yksilöivän tunnistetiedon avulla, jolla voi-

daan luotettavasti rajata verkkoyhteyteen oikeutettujen henkilöiden määrä – ehto ei koske [Oy Yritys Ab] tiloissa olevaa palveluverkkoa. [Oy Yritys Ab] huolehtii, että yhteydenotoista jää kirjaukset seuranta- tai lokitiedostoon. [Oy Yritys Ab] raportoi kuukausiraportoinnin yhteydessä yhteydenotot, selvittää tehdyt toimenpiteet ja raportoi yhteydenottojen syyt.

Tietoliikenneyhteydet Asiakkaan yhteistyökumppaneiden kanssa on [Oy Yritys Ab] tarvittaessa pystyttävä salaamaan. Salausta tarvitaan erityisesti aineistojen siirron yhteydessä. [Oy Yritys Ab] huolehtii tuotetun materiaalin siirron turvallisuudesta (esim. tulosteiden postitus) ja [Oy Yritys Ab] käyttöön tai tiloihin jäävän materiaalin/ aineiston hävityksestä (esim. epäonnistuneet tulosteet).

[Oy Yritys Ab] huolehtii palvelinten virustorjunnasta jatkuvasti ylläpidettävin ajanmukaisin virustorjuntaohjelmistoin sekä pitää Asiakkaan ajan tasalla myös virusriskin kasvamisen osalta.

[Oy Yritys Ab] tai sen aliurakoitsijat eivät saa mainita kaupallisena referenssinä tehneensä työtä Ulkoistajalle, ellei asiasta ole erikseen kirjallisesti sovittu.

Mikäli [Oy Yritys Ab]:lle syntyy tekijänoikeus tai muu immateriaalioikeus kaupallisen sopimuksen perusteella, ei se sisällä oikeutta julkistaa tämän sopimuksen perusteella salassa pidettävää tietoa.

[Oy Yritys Ab] vastaa palvelujensa osalta siitä, että ne ovat viranomaistoimintaa koskevien lakien, määräysten ja suositusten mukaisia. [Oy Yritys Ab] pitää Ulkoistajan ajan tasalla tämän palveluissa käytettävistä tietoturvaratkaisuista ja antaa Ulkoistajalle oikeuden tarkistaa ne.

Ulkoistajalla on oikeus tarkastaa ennalta ilmoittamatta yrityksen turvallisuusjärjestelyjä Ulkoistajaa koskevilta osilta. [Oy Yritys Ab] on velvollinen ilmoittamaan kirjallisesti Ulkoistajalle tämän sopimuksen yhteyshenkilölle, jos sen omistussuhteissa, Ulkoistajan kannalta keskeisissä toiminnoissa, henkilö- tai turvallisuusjärjestelyissä tapahtuu muutoksia tai yritykseen kohdistuu Ulkoistajaa mahdollisesti uhkaavia yhteydenottoja.

[Oy Yritys Ab] on velvollinen ilmoittamaan välittömästi kirjallisesti Ulkoistajalle tämän sopimuksen yhteyshenkilölle sopimuksen vastaisesta tietovuodosta tai muusta turvallisuutta vaarantavasta tapahtumasta.

Ulkoistajan tehtävät tietoturvallisuuden osalta ovat seuraavat:

1) vastaa tietoturvallisuuden periaatteiden määrittelystä
2) vastaa käyttövaltuuksien antamisesta
3) seuraa tietoturvallisuuden tason toteutumista sekä poikkeamia yhteistyössä [Oy Yritys Ab] kanssa
4) valitsee käytettävät tietoturvatuotteet yhteistyössä [Oy Yritys Ab] kanssa
5) päättää toimenpiteistä tietoturvarikkomustapauksissa.

Mikäli [Oy Yritys Ab] tai sen käyttämä alihankkija rikkoo tämän sopimuksen määräyksiä vastaa, on [Oy Yritys Ab] velvollinen korvaamaan rikkomuksesta aiheutuneet vahin-

got. Jos on kysymys kertaluonteisesta tai määräaikaisesta sopimuksesta, on korvauksen yläraja sopimussumman suuruinen. Toistaiseksi voimassa olevassa sopimuksessa korvauksen yläraja on vuosisuorituksen suuruinen.

Tämä sopimus on voimassa niin kauan kuin [tarjousta/sopimusta/työtä] koskeva kaupallinen sopimus on voimassa. Ulkoistaja voi irtisanoa tämän sopimuksen ja kaupalliset sopimukset välittömästi, jos [Oy Yritys Ab] rikkoo tämän sopimuksen määräyksiä.

Vaitiolovelvollisuus on voimassa myös sopimuksen päättyä tai sopimuksen irtisanomisen jälkeen.

Tämän sopimuksen mukainen oikeuspaikka on Ulkoistajan kotipaikan käräjäoikeus.

Tätä sopimusta sovelletaan, mikäli tämä sopimus ja kaupallinen sopimus ovat ristiriidassa keskenään.

Sopimus on laadittu kahtena kappaleena, yksi kummallekin osapuolelle.

[Yhteyshenkilöt ja allekirjoitukset]

LIITE 1B TURVALLISUUSSOPIMUSMALLI

Pohjana Puolustusvoimien malli (lupa käyttöön myönnetty)

TURVALLISUUSSOPIMUS

1. Johdanto

Puolustusvoimat ja Sidosryhmä ovat tänään tehneet maanpuolustukseen liittyvää yhteistyötä koskevan turvallisuussopimuksen (jäljempänä Sopimus). Tämä Sopimus on puolustusvoimien ja Sidosryhmän välinen turvallisuusjärjestelyjä koskeva yleissopimus. Sopimuksessa määritellään sopijaosapuolten kesken noudatettavat turvallisuusjärjestelyt. Sopijaosapuolet sitoutuvat noudattamaan tätä Sopimusta kaikissa hankkeissa (vast.), joissa käsitellään puolustusvoimien tai Sidosryhmän salassa pidettävää tietoa, asiakirjoja ja materiaalia. Tämän Sopimuksen allekirjoittamisen jälkeen Sidosryhmällä on mahdollisuus Sopimuksen määrittämissä rajoissa valmistella ja toteuttaa puolustusvoimien kanssa erikseen määritettäviä hankkeita (vast.).

2. Turvallisuusjärjestelyt

2.1. Luottamuksellisuus

Sidosryhmä sitoutuu pitämään salassa kaikki puolustusvoimien sille luovuttamat tai sillä olevat puolustusvoimien salassa pidettäväksi säädetyt tai sellaisiksi lain nojalla määrätyt tiedot. Salassa pidettävästä tiedosta, asiakirjasta ja materiaalista saa antaa tiedon vain erikseen nimetyille henkilöille. Salassapitovelvollisuus on voimassa myös tämän Sopimuksen päättymisen jälkeen.

Puolustusvoimat sitoutuu pitämään salassa kaikki Sidosryhmän sille luovuttamat tai sillä olevat Sidosryhmän salassa pidettäväksi säädetyt tai sellaisiksi lain nojalla määrätyt tiedot. Salassa pidettävästä tiedosta, asiakirjasta ja materiaalista saa antaa tietoja vain erikseen nimetyille henkilöille tai viranomaiselle. Salassapitovelvollisuus on voimassa myös tämän Sopimuksen päättymisen jälkeen.

Sidosryhmä sitoutuu säilyttämään ja käsittelemään työhön liittyviä tietoja, asiapapereita, laitteita, koneita, valokuvia, työpiirustuksia, tietolevyjä ja vastaavia salassa pidettäviä tavaroita siten, että ne pysyvät vain käsittelyoikeuden omaavien hallinnassa, eivätkä joudu ulkopuolisten haltuun, tutkittavaksi tai tietoon.

Edellä mainittujen asioiden ja materiaalin valokuvaus, kopiointi, vieminen pois toimitiloista tai muistiinpanojen tekeminen salassa pidettävistä tiedoista on kielletty ilman erillistä lupaa. Sopimuksen päätyttyä yhteisesti sovittavana ajankohtana sopijaosapuolet mahdollisine alihankkijoineen palauttavat kaikki toimeksiantoon liittyvät dokumentit, tallenteet ja materiaalin tai tuhoavat ne sovitulla tavalla.

Sidosryhmä vastaa siitä, ettei puolustusvoimien kohteiden tai toiminnan turvallisuus vaarannu Sidosryhmän henkilöstön huolimattomuuden, virheellisten työtapojen tai muun toiminnan johdosta.

Puolustusvoimat vastaa siitä, ettei Sidosryhmän kohteiden tai toiminnan turvallisuus vaarannu puolustusvoimien henkilöstön huolimattomuuden, virheellisten työtapojen tai muun toiminnan johdosta.

2.2. Sidosryhmän henkilöstö

Sidosryhmä saattaa puolustusvoimien kanssa yhteistyötä tekevän ja tämän Sopimuksen vaikutusalaan kuuluvan henkilöstönsä tietoiseksi tämän Sopimuksen salassapitovelvoitteista sekä sitoutuu valvomaan, että henkilöstö noudattaa Sopimusta. Sidosryhmä toimittaa sopimuksen kohteena olevaan toimintaan liittyvän henkilöstönsä täyttämät ja allekirjoittamat henkilötiedot puolustusvoimien turvallisuusviranomaisille turvallisuusselvityksen tekemistä varten (laki turvallisuusselvityksistä, 177/2002 sekä PEturv-os PAK 03:06) puolustusvoimien turvallisuusselvityshakemuslomakkeella. Selvitys tehdään henkilöistä jotka käsittelevät työssään tämän sopimuksen kohteena olevia salassa pidettäviä tietoja tai joilla on pääsy sellaisiin puolustusvoimien hallinnassa oleviin tiloihin, joissa liikkumista on sotilaallisten syiden perusteella syytä rajoittaa[26]. Yhteistyöhön nimettävän ja puolustusvoimien hyväksymän henkilöstön tulee tehdä puolustusvoimien hyväksymälle lomakkeelle laadittu vaitiolovakuutus ennen kaupallisen (vast.) sopimuksen syntyä.

2.3. Alihankkijat

Mikäli Sidosryhmä käyttää alihankkijoita, aliurakoitsijoita tai muita palvelujen toimittajia

[26] Laki puolustusvoimista (402/1974)

puolustusvoimien hankkeissa, tulee Sidosryhmän hyväksyttää alihankkijat (vast.) ja niiden yhteistoimintaan osallistuva henkilöstö puolustusvoimilla edellä kuvattujen menettelyjen mukaisesti ennen aliurakointi- tai muun sopimuksen tekemistä sillä edellytyksellä, että alihankkija (vast.) käsittelee puolustusvoimien salassa pidettävää tietoa tai toimii tiloissa, joissa käsitellään salassa pidettävää tietoa.

Mikäli edellisen kappaleen ehdot täyttyvät, Sidosryhmän tulee tehdä alihankkijansa (vast.) kanssa turvallisuussopimus. Sidosryhmän on tiedotettava alihankkijalleen (vast.), että turvallisuusjärjestelyjen saattamisesta puolustusvoimien vaatimalle tasolle saattaa syntyä kustannuksia. Ennen Sidosryhmän ja alihankkijan (vast.) välisen turvallisuussopimuksen solmimista sopimuksen yksityiskohdat on hyväksytettävä puolustusvoimilla. Hyväksyvä taho on ensisijaisesti Sidosryhmän ja puolustusvoimien välisen turvallisuussopimuksen (puolustusvoimien turvallisuussopimus tai hankintasopimukseen liittyvä turvallisuusliite) valmistelija, joka tarvittaessa avustaa sopimuksen tekemiseen liittyvissä yksityiskohdissa.

Sidosryhmä tai sen alihankkijat saavat mainita referenssinä tehneensä työtä puolustusvoimille, jos asiasta on erikseen kirjallisesti sovittu.

2.4. Turvallisuuden tarkastaminen

Sidosryhmän turvallisuuskartoitus ja -ohjeistus on esitetty liitteessä 1.

Puolustusvoimilla on oikeus tarkastaa etukäteen ilmoitettuna ajankohtana Sidosryhmän turvallisuusjärjestelyt puolustusvoimia koskevilta osilta. Sidosryhmä on velvollinen ilmoittamaan puolustusvoimille, jos sen omistussuhteissa, puolustusvoimien kannalta keskeisissä toiminnoissa, henkilö- tai turvallisuusjärjestelyissä tapahtuu muutoksia tai Sidosryhmään kohdistuu maanpuolustusta mahdollisesti uhkaavia toimenpiteitä, esim. yhteydenottoja tai tietomurtoyrityksiä. Sama ilmoitusvelvollisuus koskee yhteistyöhön liittyvin osin myös puolustusvoimia.

Sidosryhmällä on perustellun syyn esittämällä mahdollisuus tarkastaa etukäteen sovittuna ajankohtana puolustusvoimien turvallisuusjärjestelyt Sidosryhmää koskevilta osilta.

3. Muut Sopimuksen sisältämät asiat

3.1. Yhteyshenkilöt

Sidosryhmän yhteyshenkilönä tämän Sopimuksen toteuttamiseen liittyvissä kysymyksissä toimii Sidosryhmän turvallisuuspäällikkö (vast.). Sopijaosapuolet ilmoittavat yhteyshenkilönsä tämän Sopimuksen allekirjoituksen yhteydessä (liite 2).

3.2. Sopimuksen päivittäminen

Yhteyshenkilöt vastaavat Sopimuksen tarpeellisesta päivittämisestä. Päivittämistarve on arvioitava yhteyshenkilöiden kesken vähintään kahden vuoden välein.

Puolustusvoimien kanssa erikseen sovittavissa hankkeissa ja yhteistoimintajärjestelyissä tulee määritellä yksityiskohtaisemmat turvallisuusjärjestelyt kunkin hankkeen edellyttämässä laajuudessa. Hankkeen sopimuspapereihin tulee liittää kyseistä hanketta koskeva turvallisuusliite.

Tähän Sopimukseen tehtävät muutokset tulee molempien osapuolten vahvistaa allekirjoituksellaan. Tämän Sopimuksen muutokseksi ei katsota yhteyshenkilöiden vaihtumista (liite 2).

3.3. Sopimuksen liitteiden päivittäminen

Sidosryhmä vastaa liitteen 1 ylläpidosta. Liitteen tulee vastata voimassa olevaa tilannetta.

Sekä Sidosryhmä, että puolustusvoimat vastaavat omalta osaltaan liitteen 2 ylläpidosta.

Puolustusvoimat vastaa liitteen 3 ylläpidosta. Liitteessä 3 on esitetty puolustusvoimien hyväksymät menettelyt, tilat ja järjestelmät eri luottamuksellisuusluokkiin kuuluvan tiedon, asiakirjojen ja materiaalin käsittelystä. Siinä ilmaistaan korkein tiedon luottamuksellisuusluokka, johon kuuluvia puolustusvoimien tietoja Sidosryhmässä voidaan käsitellä.

Liitteitä koskevat muutokset tulevat Sopimuksen osaksi, kun molemmat osapuolet ovat ne hyväksyneet ja allekirjoittaneet.

3.4. Sopimussakko

Puolustusvoimilla on oikeus saada sopimussakkoa, mikäli Sidosryhmä rikkoo tämän Sopimuksen turvallisuusmääräyksiä. Sopimussakon laskennassa noudatetaan seuraavaa laskentamallia:

> Puolustusvoimilla on oikeus saada sopimussakkona 10 % kaupallisen sopimuksen kokonaishinnasta tai vähintään 10 000 .
>
> Sopimuksen turvallisuusmääräysten rikkomisesta maksettavan sopimussakon enimmäismäärä voi kuitenkin olla sopimuskohtaisesti enintään sopimuksen kokonaishinta.
>
> Erillisessä hankintasopimuksen turvallisuusliitteessä voidaan tapauskohtaisesti käyttää, hankinnan luonteen niin vaatiessa, jotakin edellä mainitusta laskentamallista poikkeavaa, molempien sopimusosapuolten hyväksymää mallia.

Tämä sopimussakko-oikeus koskee kaikkia niitä sopimuksia, joiden osalta turvallisuusmääräyksiä on rikottu.

Puolustusvoimilla on oikeus saada sopimussakko osoittamatta, että turvallisuusmääräysten rikkomisesta on aiheutunut Puolustusvoimille vahinkoa.

3.5. Sopimuksen irtisanominen ja purkaminen

Kumpikin sopijapuoli voi irtisanoa sopimuksen päättymään kolmen (3) kuukauden kuluessa kirjallisesta irtisanomisilmoituksesta. Irtisanominen ei poista velvollisuutta täyttää ennen irtisanomista syntyneet velvoitteet.

Kumpikin sopijapuoli on oikeutettu purkamaan sopimuksen välittömästi kirjallisella ilmoituksella toiselle sopimuspuolelle, mikäli tämä rikkoo sopimusvelvoitteitaan niin olennaisesti, ettei toisen sopimuspuolen voida kohtuudella edellyttää jatkavan sopimussuhdetta edes irtisanomisaikaa.

Mikäli puolustusvoimat purkaa tämän sopimuksen, se voi välittömästi purkaa myös tähän sopimukseen viittaavat, Sidosryhmän kanssa tehdyt sekä kaupalliset sopimukset että muut sopimukset. Sopimuksen purkamisen seurauksena Sidosryhmälle aiheutuu kaupallisissa ja muissa sopimuksissa sovitut seuraamukset turvallisuusmääräysten rikkomisesta.

3.6 Sovellettava laki ja erimielisyyksien ratkaisu

Tähän sopimukseen sovelletaan Suomen lakia. Tästä sopimuksesta aiheutuneet erimielisyydet pyritään ensisijaisesti ratkaisemaan sopijapuolten välisin neuvotteluin. Mikäli sopijapuolet eivät pääse sovinnolliseen ratkaisuun, erimielisyydet ratkotaan Helsingin käräjäoikeudessa.

3.7. Sopimuksen voimassaolo

Tämä Sopimus on voimassa toistaiseksi.

Tämä Sopimus tulee voimaan, kun kumpikin osapuoli on sen allekirjoittanut.

Sopimus on laadittu kahtena samansanaisena kappaleena, yksi kummallekin osapuolelle.

Helsingissä pv.kk.200n

Sidosryhmän puolesta	Puolustusvoimien puolesta
_____	_____

JAKELU
LIITTEET 3 kpl
LIITE 1 Sidosryhmän turvallisuuskartoitus ja turvallisuusohjeisto
LIITE 2 Sopijaosapuolten yhteydenpitohenkilöstö
LIITE 3 Puolustusvoimien hyväksymät menettelyt, tilat ja järjestelmät

LIITE 2 TURVALLISUUSSELVITYS ULKOISTUSPALVELUJA TARJOAVASTA YRITYKSESTÄ

Mallina Valtiokonttorin selvitys

Ennen turvallisuussopimuksen allekirjoittamista yritys tekee turvallisuusselvityksen turvallisuustoiminnan periaatteistaan, järjestelyistään, tiloistaan ja henkilöstöstään. Turvallisuusselvityksen perusteella Ulkoistaja tekee katselmuksen, jossa tarkastetaan yrityksen turvallisuusjärjestelyt.

Turvallisuusselvitys toimitetaan Ulkoistajalle, joka järjestää katselmuksen yrityksen kanssa sovittavana ajankohtana. Alla olevassa mallissa on esitetty turvallisuusselvityksessä kyseeseen tulevat turvallisuuden osa-alueet. Yrityksen on selvitystä tehdessään yhdessä Ulkoistajan kanssa arvioitava, mitkä osa-alueet on ko. yrityksen osalta turvallisuussopimukseen liittyvän kaupallisen sopimuksen huomioonottaen sisällytettävä selvitykseen.

[Oy Yritys Ab]:n turvallisuusselvitys

1. Tiedot yrityksestä
   * nimi ja kotipaikka
   * kaupparekisterinumero
   * perustamisvuosi
   * toimiala
   * liikevaihto ja tulos viimeiseltä tilikaudelta
   * henkilökunnan lukumäärä
   * osoitetiedot
   * yrityksen johtajat
   * yrityksen omistussuhteet ja ulkomaalaisomistus

2. Turvallisuustoiminnan päämäärä ja tavoitteet
   * hankkeen turvallisuustaso
   * yrityksen turvallisuustavoitteet ja sen liittyminen kokonaistoimintastrategiaan

3. Tiedottaminen
   * ulkoistajan tietojen luovuttaminen yrityksen sisällä
   * hankkeen referointijärjestelyt

4. Turvallisuuteen käytettävät voimavarat vuosittain
   * henkilömäärä ja tehtävät
   * laitehankinnat
   * koulutuspäivät

5. Turvallisuuden organisointi
   * hankkeen vastuuhenkilö
   * turvallisuusvastaava ja apulaiset
   * yhteydenpito VK:n vastuulliseen turvallisuuselimeen
   * turvallisuusvalvonta
   * aliurakoitsijoiden osuus

6. Tiedottaminen ja kouluttaminen
   * koulutusjärjestelyt
   * laatutoiminta ja muu turvallisuusohjeistus

7. Henkilöstöturvallisuus
   * hankkeeseen osallistuvat henkilöt, ml kohdan 5 henkilöstö
   * ulkomaalaiset
   * muut tavaran ja palvelujen toimittajat
   * taustaselvitykset
   * vaitiolositoumukset
   * ulkopuolisista vierailijoista ilmoittaminen Ulkoistajalle

8. Fyysinen turvallisuus
   * kohdesuunnitelmat
     – rakenteellinen suojaus
     – kulku- ja pääsyoikeuksien hallinnointi
     – kulunvalvonnan järjestelyt
     – lukituksen järjestelyt
     – avainten ja kulkukorttien käyttö
     – henkilöstön tunnistaminen

– ajoneuvojen tarkastaminen
– vartioinnin ja valvonnan järjestelyt
– murtosuojaus
– rikosilmoitusjärjestelmä
– muut turvallisuusrakenteet, laitteet ja välineet
– tietoaineiston säilytystilat ja tulostinten valvonta
– salakatselun ja -kuuntelun estäminen
– palo- ja pelastustoiminnan järjestelyt

9. Tietoturvallisuus
   * tietoaineistoturvallisuus
     – tietoaineiston luovutukset ja kirjaaminen
     – tietoaineiston säilyttäminen
     – tietoaineiston hävittäminen
     – luokittelu
     – kopiointi
     – merkitseminen ja kirjaaminen
   * atk-toiminnan turvallisuus
     – ohjelmistoturvallisuus
     – laitteistoturvallisuus
     – lähiverkko
     – käyttöturvallisuus
   * tietoliikenneturvallisuus
     – datan siirto
     – puhelinjärjestelyt
     – matkapuhelinjärjestelyt
     – telekopio
   * salassapitosopimukset

10. Erityisvaatimukset
    * varautumista koskevat lisävaatimukset
    * salaisia hankkeita koskevat erikoisvaatimukset

11. Vierailut ja kokoukset
    * ulkomaalaiset yhteistyökumppanit
    * vierailut ulkomailla
    * vierailut kotimaassa
    * kokoustilat

12. Kuljetukset
    * postilähetykset
    * pakkaaminen
    * kuriirien käyttö

13. Toiminta poikkeusoloissa
    * toipumissuunnitelma
    * poikkeusolojen varautumissuunnitelma

14. Katselmukset
    * tarkastukset
    * uusintatarkastuksen ajankohta.

Turvallisuusselvitys on laadittu kahtena kappaleena turvallisuussopimuksen (ks. Liite 1a) liitteeksi, yksi kummallekin osapuolelle.

LIITE 3 MALLI TIETOTURVA-ASIOIDEN ARVIOINNISTA

TIETOTURVA

37	Onko mahdollista muokata tietokannan tietoja suoraan esim. SQL:llä tai vastaavalla ohi sovellusohjelmiston?	1	Vain DBA
	Käyttäjän tunnistus		
38	Tukeeko järjestelmä korttitunnistusta (esim. HST-kortti)?	2	
	Onko korttitunnistusta mahdollista käyttää seuraavissa toiminnoissa:	-	
39	- sisäänkirjautuminen	2	Oletuksena, että tunnistaminen tapahtuu kertaalleen sisäänkirjautuessa, ja jatkotoimenpiteissä tätä hyödynnetään.
40	- allekirjoittaminen	-	
41	- puollot	-	
42	- tarkastukset	-	
43	- maksumääräykset	-	
44	- muut mahdolliset tilanteet	-	
45	Tukeeko järjestelmä vahvan tunnisteen käyttöä sähköisessä allekirjoituksessa?	2	
46	Perustuuko tunnistus sekä käyttäjätunnukseen että salasanaan?	1	
47	Tukeutuuko tunnistus käyttöjärjestelmän tunnistusmekanismiin?	3	
48	Jos tukeutuu, kuvaa ratkaisun toteutus	-	Informatiivinen tieto
49	Tukeutuuko tunnistus tietokantajärjestelmään määriteltyihin oikeuksiin?	1	
50	Onko tunnistusmekanismi toimittajan itse rakentama (tietokantataulu/tiedosto)?	3	Ei samassa kannassa kuin muu data. Pienen tarjoajan itserakentama kanta ei ehkä toivottava ominaisuus.
	Salasanat		
51	Onko salasanalle on määritelty jokin minimipituus (esim. vähintään 6 merkkiä)?	1	
52	Määrittele mahdollinen minimipituus	1	Yksi piste, jos suurempi kuin 6 merkkiä.
53	Onko sisäänkirjautumisten yrityskerrat rajattu?	1	
54	Voidaanko salasanat vanhentaa automaattisesti (tietyn ajanjakson välein)?	1	
55	Voidaanko salasanat vanhentaa manuaalisesti?	1	
56	Voidaanko salasanat vaihtaa haluttaessa?	1	
57	Voiko käyttäjä vaihtaa salasanansa halutessaan?	1	
58	Onko salasanahistoria jäljitettävissä?	-	
59	Onko samojen salasanojen käyttö estettävissä?	1	
60	Onko helppojen salasanojen käyttö estettävissä?	1	
61	Onko salasanojen kryptaus (ei-selväkielisyys) mahdollista?	1	
62	Näkyvätkö salasanat milloinkaan/missään selvätekstisinä?	1	Kielteinen vastaus antaa pisteen.
	Kirjautumisen yhteydessä näytettävät tiedot		
63	Näytetäänkö kirjautumisen yhteydessä edellisen kirjautumiskerran aikaleima?	2	
64	Näytetäänkö kirjautumisen yhteydessä kyseisen kerran epäonnistuneiden kirjautumisten määrä?	2	
	Tunnuksen lukitus		
65	Onko mahdollista lukita esim. työsuhteensa päättäneiden käyttäjien tunnukset?	1	
66	Onko mahdollista lukittaa tunnus n kpl:een virheellisten perättäisten kirjautumisyrityksen jälkeen?	1	Pääkäyttäjän on pystyttävä määrittelemään, kuinka monen yrityksen jälkeen tunnus lukittuu.
67	Jos käyttäjätunnus voidaan lukita, miten lukitus puretaan?	1	Pisteytys 0-1: Pääkäyttäjän oikeuksissa, toteuduttava välittömästi toimenpiteen jälkeen
	Lokijärjestelmä		
68	Onko tietojärjestelmässä erillinen lokijärjestelmä?	1	Vrt. tietoturvaliite, Käyttöturvallisuus c)
69	Onko lokijärjestelmä eri palvelimella kuin tietojärjestelmä?	1	Vrt. tietoturvaliite, Käyttöturvallisuus c)
70	Voidaanko lokijärjestelmästä ajaa raportteja näytölle?	2	Vrt. tietoturvaliite, Käyttöturvallisuus c)
71	Voidaanko lokijärjestelmästä tulostaa käyttäjän määrittelemiä raportteja?	1	VK:n ja virastojen yhdessä määrittelemät raportit. Vrt. tietoturvaliite,
72	Voidaanko lokijärjestelmästä tulostaa valmiiksimääriteltyjä raportteja paperille?	1	Vrt. tietoturvaliite, Käyttöturvallisuus c)
73	Voidaanko lokijärjestelmästä viedä tietoja muihin järjestelmiin jatkojalostusta varten?	2	Ongelmaratkaisutilanteet ja virheiden jäljitykset. Vrt. tietoturvaliite,
74	Kuvaa kaikki lokiin kirjautuvat tiedot (erilliselle liitteelle)	1	Pisteytys 0-1: Kuka, mitä, milloin; liittymäajot, pankkitili, rahaliikenteeseen liittyvät kysymykset, perustiedot. Vrt. tietoturvaliite,
	Tietoliikenne/Tiedonsalaus		
75	Miten on varmistuttu tietoverkossa välitettävän tiedon luottamuksellisuudesta?	1	Pisteytys 0-1: Tietohallinto määrittelee dokumentin sisältövaatimukset. Vrt. tietoturvaliite, Tietoliikenteen tietoturvallisuus b)
76	Miten on varmistuttu tietoverkossa välitettävän tiedon eheydestä?	1	Pisteytys 0-1: Tietohallinto määrittelee dokumentin sisältövaatimukset. Vrt. tietoturvaliite, Tietoliikenteen tietoturvallisuus b)
77	Miten on varmistuttu välitettävän tiedon saatavuudesta?	1	Pisteytys 0-1: Tietohallinto määrittelee dokumentin sisältövaatimukset. Vrt. tietoturvaliite, Tietoliikenteen tietoturvallisuus b)
78	Onko yhteyksissä käytetty salausta?	1	Pisteytys 0-1: Tietohallinto määrittelee dokumentin sisältövaatimukset. Vrt. tietoturvaliite, Tietoliikenteen tietoturvallisuus b)
79	Kuvaile salausmenettelyt ja tuotteet	1	Pisteytys 0-1: Tietohallinto määrittelee dokumentin sisältövaatimukset. Vrt. tietoturvaliite, Tietoliikenteen tietoturvallisuus b)

LIITE 4 KÄYTETTYJÄ LÄHTEITÄ

Internet

- Outsourcing Institute: http://www.outsourcing.com/
- BITS – Financial Services Roundtable: http://www.bitsinfo.org/
- The Institute for Information Infrastructure Protection (I3P) http://www.thei3p.org/
- Information Systems Audit and Control Association: http://www.isaca.org/
- Vahti-ohjeet: http://www.vm.fi/vm/liston/page.lsp?r=3246&l=fi
- Tietosuojavaltuutetun toimisto: http://www.tietosuoja.fi
- Huoltovarmuuskeskus: http://www.nesa.fi/
- The SANS Intititute: http://www.sans.org/

Lehdet

- The Economist
- McKinsey Review
- Fortune
- Information System Control Journal
- IT-viikko
- Tietoviikko
- Harvard Business Review

Kirjat

- Kiiha, Jarkko: Yritystoiminnan ulkoistaminen ja sopimusvastuu, Kauppakaari, 2002
- Stees, John D: Outsourcing Security, Butterworth Heinemann, 1998
- Axelrod, C. Warren: Outsourcing Information Security, Artech House Books, 2004
- Takki, Pekka: IT-sopimukset – Käytännön käsikirja, Talentum, 2003

LIITE 5 HENKILÖTIETOJEN KÄSITTELYÄ KOSKEVAN TOIMEKSIANTOSOPIMUKSEN TARKISTUSLISTA (LÄHDE: TIETOSUOJAVALTUUTETUN TOIMISTO)

Henkilötietojen käsittelyä koskevan toimeksiantosopimuksen tekemisessä huomioon otettavia asioita.

Henkilötietolain 8 §:n 1 momentin 7 kohta oikeuttaa käsittelemään henkilötietoja rekisterinpitäjän toimeksiannosta tapahtuvaa maksupalvelua, tietojenkäsittelyä tai niihin verrattavia tehtäviä varten. Jäljempänä on listattu kysymyksiä ja muita asioita, joita on otettava huomioon toimeksiantosopimusta tehtäessä. Luettelo ei ole tyhjentävä, vaan sopimuksen sisältö riippuu viime kädessä hankittavista palveluista.

Osapuolet:	Huomioonsopimuksessa
1. Kuka on rekisterinpitäjä/toimeksiantaja? (henkilötietolaki 3 § 1 mom. 4 kohta)	
2. Kuka on se henkilö/toimielin, jolla on oikeus rekisterinpitäjän puolesta päättää toimeksiannon tekemisestä?	
3. Kuka on toimeksisaaja? (henkilö, yhteisö, yritys)	
4. Kuka on se henkilö/toimielin, jolla on oikeus tehdä sopimuksia toimeksisaajan puolesta?	
5. Ketkä ovat sopijapuolten sopimusvastuuhenkilöt ja mitkä ovat heidän tehtävänsä?	
Sopimuksessa määriteltäviä asioita	
1. Henkilötietojen eri käsittelyvaiheet on kuvattava ja määriteltävä mitkä tehtävät ja käsittelyvaiheet kuuluvat toimeksiantosopimuksen piiriin. On myös sovittava mitä menettelytapoja henkilötietoja käsiteltäessä noudatetaan . (Henkilötietojen käsittely voidaan määritellä tarkasti esimerkiksi palvelukuvauksessa tai vastaavassa.)	
2. Toimeksiantajan ja toimeksisaajan vastuut ja tehtävät on määriteltävä käsittelyvaiheittain.	

Osapuolet:	Huomioonsopimuksessa
3. Henkilötietojen käsittelyä koskevat lait ja viranomaisten antamat määräykset ja ohjeet on oltava molempien osapuolten tiedossa. Erityisesti on kiinnitettävä huomioita salassapitoa, vaitiolovelvollisuutta ja tietojen suojaamista koskeviin säännöksiin ja määräyksiin.	
4. Toimeksiantaja ja toimeksisaaja huolehtivat omalta osaltaan siitä, että tietosuojaa tai muuta salassapitoa koskevat säännökset ja viranomaisten määräykset otetaan huomioon.	
5. Toimeksisaaja antaa ennen henkilötietojen käsittelyyn ryhtymistä toimeksiantajalle riittävät sitoumukset henkilötietojen suojaamisesta tämän sopimuksen edellyttämällä tavalla. Myös toimeksisaajan henkilökuntaa koskevista salassapitositoumuksista on huolehdittava.	
6. Toimeksiantaja on henkilötietolain tarkoittama rekisterinpitäjä, jonka käyttöä varten rekisteri on perustettu ja jolla on oikeus määrätä sen käytöstä. Toimeksiantajalla on oltava mahdollisuus valvoa henkilötietojen käsittelyä ja antaa sitä koskevia määräyksiä ja ohjeita toimeksisaajalle.	
7. Toimeksiantaja ja toimeksisaaja osaltaan vastaavat henkilötietojen käytön seurannasta. On määriteltävä millä tavoin ja kuinka usein toimeksiantajalle toimitetaan loki- ja muita tietoja joita se tarvitsee valvoessaan toimeksisaajan työtä.	
8. Toimeksiantaja vastaa rekisterinpitäjänä henkilötietolain asettamista velvoitteista mukaan lukien rekisteriselosteen laatiminen ja saatavillapito, informointi sekä tarkastusoikeuden toteuttaminen. Jos toimeksisaaja avustaa rekisteröityjen oikeuksiin liittyvien toimenpiteiden toteuttamisessa on nämä tehtävät määriteltävä.	
9. Toimeksiantaja ja toimeksisaaja sopivat toimeksiannon piiriin kuuluvaan henkilötietojen käsittelyyn liittyvästä tietoturvasta ja kuinka tietoturvallisuuteen liittyviä järjestelyjä tarkistetaan ja päivitetään. Järjestelyjä on arvioitava säännöllisin määräajoin.	
10. Tietojen suojaaminen ja toimeksisaajan ohjelmistojen, sovellutusten, laitteistojen ja verkkojen käyttöoikeudet ja tietoturvallisuus toimeksiannon piiriin kuuluvissa käsittelyvaiheissa on määriteltävä ja varmistettava. Toimeksiantaja ja toimeksisaaja vastaavat siitä, että ne toteuttavat osaltaan tekniset ja organisatoriset toimenpiteet henkilötietojen suojaamiseksi asiattomien pääsyltä tietoihin ja vahingossa tai laittomasti tapahtuvalta tietojen hävittämiseltä, muuttamiselta, luovuttamiselta siirtämiseltä taikka muulta luvattomalta käsittelyltä.	

Osapuolet:	Huomioonsopimuksessa
11. Toimeksiantaja vastaa siitä, että tietojen korjaukset, poistot ja muutokset henkilötietoihin toimitetaan toimeksisaajalle. Toimeksisaaja ottaa nämä välittömästi huomioon toimeksiannon piiriin kuuluvassa henkilötietojen käsittelyssä.	
12. Toimeksiantaja ja toimeksisaaja kartoittavat toimeksiannon toteuttamiseen liittyvät ongelmatilanteet ja niihin liittyvät menettelytavat ja vastuut.	
13. Jos toimeksisaajalla on mahdollisuus käyttää alihankkijoita tai siirtää sopimus kolmannelle osapuolelle. Mahdollisia alihankkijoita koskevat tietosuojan ja tietoturvan osalta samat vaatimukset kuin varsinaista toimeksisaajalla. On myös määriteltävä millä ehdoilla ja mitä menettelytapoja noudattaen alihankkijoita voidaan käyttää.	
14. Toimeksisaaja ei saa käyttää tietoja hyväkseen tai luovuttaa niitä kenellekään muuten kuin sopimuksen tarkoittamassa laajuudessa ja sopimuksen mukaista tehtävää hoitaessaan. Toimeksisaaja voi käyttää tietoja vain toimeksiantosopimuksessa määritellyillä tavoilla ja sopimuksessa määriteltyihin tarkoituksiin.	
15. Toimeksisaaja sitoutuu siihen, että henkilötietoja käsittelevät vain ne henkilöt, joiden työtehtävien hoitaminen sitä edellyttää. Toimeksiantaja ja toimeksisaaja sopivat käyttöoikeuksien antamisesta henkilötietoihin.	
16. Toimeksisaaja vastaa siitä, että samoja työvälineitä mahdollisesti käyttävät muut asiakkaat eivät pääse käsiksi toimeksiantajan tietoihin.	
17. Toimeksisaaja sitoutuu pitämään luottamuksellisina saamansa aineistot ja tiedot sekä olemaan käyttämättä niitä muihin kuin sopimuksen mukaisiin tarkoituksiin myös sopimussuhteen päättymisen jälkeenkin.	
18. Toimeksisaaja hoitaa vanhentuneet henkilötiedot sovittujen periaatteiden mukaisesti ja vahvistaa hävittämisen toimeksiantajalle. Vanhentuneen tietoaineiston osalta on määriteltävä hävittämisajankohta sekä hävittämistavat. Aineiston hävittämisessä on otettava huomioon aineiston säilyttämistä koskevat lait tai viranomaisten määräykset.	
19. Jos toimeksisaaja siirtää sopimusta tai siihen sisältyviä oikeuksia siirtää edelleen, on sovittava millä edellytyksillä niin voidaan tehdä.	

Osapuolet:	Huomioonsopimuksessa
20. Millä ehdoilla sopimus voidaan peruuttaa tai sen ehtoja muuttaa ja sopimuksen päättymisen vaikutukset henkilötietojen käsittelyyn? Mitkä ovat toimenpiteet ja osapuolten vastuut toimeksiantosuhteen päättyessä?	
21. Kuinka ja missä ajassa toimeksisaajan hallussa olevat henkilötiedot toimitetaan toimeksiantajalle tai mahdolliselle uudelle toimeksisaajalle tai hävitetään?	
22. Mitkä ovat menettelytavat sopimuksen noudattamisen seurannassa ja valvonnassa?	
23. Mitkä ovat sopimusrikkomusten vaikutukset ja mahdolliset vahingonkorvausvastuut ja kuinka sopimusta ja siinä sovittua henkilötietojen käsittelyä koskevat erimielisyydet ratkaistaan?	
23. Toimeksiantajan ja toimeksisaajan on huolehdittava henkilötietolain mukaisten ilmoitusten tekemisestä tietosuojavaltuutetulle: - toimeksiantopalveluja hankkiva rekisterinpitäjä: rekisteri-ilmoitus - toimeksisaaja: toimintailmoitus.	

LIITE 6 TARKISTUSLISTA

Kysymyksiä, joita voi esittää palvelutarjoajalle tuotteen tai tietoturvallisuuden selvittämiseksi.

Kysymykset perustuvat BITS:n *IT Service Provider Expectations Matrix:iin* (2004). BITS on vuonna 1996 perustettu suurten amerikkalaisten pankkien yhteistyöelin (http://www.bitsinfo.org). Kysymyksiä on mukautettu Suomen olosuhteisiin ja yksityiskohtaiset tekniset kysymykset on jätetty suomennoksesta pois. Suomennoksen numerointi ja rakenne noudattavat alkuperäistä.

IT Service Provider Expectations Matrix on käännetty BITS:n luvalla. Alkuperäinen, laaja dokumentti on ladattavissa ilmaiseksi osoitteessa http://www.bitsinfo.org/downloads/Publications%20Page/bitsxmatrix2004.xls. Kysymyslistaa on uudistettu ja laajennettu vuonna 2005.

1. Tietoturvapolitiikka *(Security Policy)*	
1.1.	**Onko toimittajalla kirjallinen tietototurvapolitiikka ja tätä tukeva materiaali?**
1.1.2	Mitkä dokumentit voidaan toimittaa tilaajalle?
1.1.3	**Onko niissä dokumenteista, joita ei voida toimittaa tilaajalle, saatavilla luotettavan kolmannen osapuolen arvio?**
1.2.	Onko seuraavista alueista saatavilla johdon hyväksymä politiikka tai muu toimintaohje? Milloin kyseinen ohje on päivitetty?
1.2.1.	Tietojen luokittelu
1.2.2.	Luottamuksellisten tietojen käsittely
1.2.3.	Internetin käyttöpolitiikka
1.2.4.	Käyttöoikeuksien hallinta
1.2.5.	Henkilökunnan ohje tietotekniikan hyväksyttävistä käyttötavoista?
1.2.6.	Sähköpostipolitiikka
1.2.7.	Salauspolitiikka
1.2.8.	Laitteiden, verkkojen ja sovellusten turvaamisen politiikka

1.2.9	Tietojärjestelmien kehittämisen ja käyttöönoton politiikka
1.2.10	Muutosten hallinnan ohjeistus
1.2.12	Toimintaohjeet tietoturvapoikkeamatilanteissa ja -rikkeissä
1.2.14	Sovelluksilta edellytettävät tietoturvallisuuden tasot
1.2.15	Etäkäyttö- ja etätyöpolitiikka
1.2.16	Rekisteriselosteet (yksityisyyden suojasta annetun lain ja tietosuojavaltuutetun ohjeiden mukaisina)
1.2.17	Ohjeet työsuhteen alkaessa ja sen päättyessä
1.2.18	Toimitilojen fyysisen turvallisuuden ohje
1.2.20	Tietoturvan koulutusohjelma henkilöstölle
1.2.21	Jatkuvuussuunnitelmat
1.3.	**Kuka henkilö omistaa tietoturvapolitiikan?**
1.4.	**Kuinka usein tietoturvaohjeet päivitetään?**
1.5.	**Mistä henkilöstö saa tietoa tietoturvaohjeista?**
1.5.1	Miten tästä huolehditaan niiden henkilöiden osalta, jotka työskentelevät muualla kuin organisaation normaaleissa toimitiloissa?
1.5.2	Edellytetäänkö organisaation alihankkijoilta säännönmukaisesti sitoutumista tietoturvapolitiikkaan? Arvioiko organisaatio omien toimittajiensa tietoturvapolitiikan tasoa?
1.5.3	Saavatko alihankkijoiden työntekijät tietoa organisaation tietoturvapolitiikasta?
1.6.	Kuinka valvotaan, että tietoturvapolitiikkaan tehtävät muutokset vaikuttavat käytännön toimintaan?
1.6.1	Onko alihankkijoille ja työntekijöille selkeästi tuotu esille, mitä toimia saattaa seurata tietoturvapolitiikan rikkomisesta?
2. Hallinnollinen tietoturvallisuus (*Organizational Security*)	
2.1	**Kuka tai ketkä ovat vastuussa tietoturvasta?**
2.2	**Onko ICT-alueen tehtävistä laadittu kirjalliset tehtävänkuvat?**
2.3	**Seuraavat roolit ja vastuut tulee dokumentoida** (henkilöt, ryhmät; myös mikäli toiminto on ulkoistettu):
2.3.1	Käyttäjähallinta
2.3.2	Sovellusten tietoturvallisuus
2.3.3	Tietoturvallisuuden hallinta
2.3.4	Tietoturvallisuuden johtaminen
2.3.5	Tietoturvapolitiikan ja muiden ohjeiden laadinta ja hyväksymistavat
2.3.6	Vastuut tilanteessa, jossa tietoturvallisuus pettää ja asia tulee julkiseen tietoon
2.3.7	Turvallisuuskoulutus
2.3.8	Haavoittuvuuden hallinta ja uhkien arviointi
2.3.9	Turvallisuustapahtumien valvonta
2.3.10	Fyysinen turvallisuus

2.3.11	ICT-infrastruktuurin arkkitehtuurisuunnittelu tietoturvallisuuden näkökulmasta
2.3.12	Toipumis- ja jatkuvuussuunnitelmat
2.2.1	Kuinka hallitaan kolmansien osapuolien pääsyä tietoihin ja tietojärjestelmiin (fyysinen ja looginen pääsy)?
2.2.2	Sovelletaanko tietoturvapolitiikkaa vuokratyövoimaan ja muihin ulkopuolisiin työntekijöihin?
2.2.3	Onko kolmansille osapuolille myönnetty etäkäyttöoikeuksia? Onko näiden tarpeellisuutta harkittu?
2.2.4	Onko oikeuksien myöntämistä koskeva aineisto dokumentoitu?
2.3.1	Käyttääkö toimittaja alihankkijoita palvelun kannalta välttämättömissä toimissa?
2.3.1.1	Jos kyllä, niin mitä palveluita nämä alihankkijat tarjoavat?
2.3.1.2	Valvoko toimittaja alihankkijoidensa tietoturvallisuuden toteutumista? Miten tämä tapahtuu?
2.3.2	Kattavatko palveluntarjoajan alihankkijasopimukset tietoturvanäkökohdat vastuineen?
2.3.2.1	Jos kyllä, niin miten sopimuksen noudattamista valvotaan?
2.3.3	Kuvaa palveluntarjoajan referenssit ja kokemus alihankkijoiden käytöstä?
2.3.4	Sisältävätkö palveluntarjoajan prosessit tavat kommunikoida alihankkijoiden kanssa tietoturvatapahtumista?
2.3.5	Onko tietoturva-asioiden yhteensopivuudesta varmistettu palveluntarjoajan ja alitoimittajan kesken?
2.3.6	Kuvaa, miten sopimussuhteen päättyminen tapahtuu.
2.3.7	Tarkistetaanko laskut asianmukaisesti? Onko olemassa prosessi hintamuutosten hallintaan ja uusien palvelumaksujen hyväksyntään?
2.3.8	Arvioidaanko alihankkijoiden suoritusta suhteessa sovittuun palvelutasoon (SLA) ja muihin ehtoihin. Arvioidaanko tarvetta muokata SLA-sopimusta?
2.3.9	Ylläpidetäänkö asianmukaista dokumentaatiota sopimusehtojen täyttymisestä ja erimielisyyksistä sopimisesta?
2.3.10	Onko palvelusopimukseen sisällytetty selkeä erittely osapuolten vastuista ja velvollisuuksista? Näitä asioita ovat mm. soveltamisperiaatteet, auditointi, muutoshallinta, riskien käsittely, SLA, tiedon omistajuus, vakuutukset, erimielisyyksien ratkaisemisen menettelyt, poikkeamaraportointi, monitorointi ja ulkomaisille osapuolille asetettavat erityisvaatimukset.
3. Tietojen luokittelu ja käyttöomaisuuskirjanpito (*Asset Classification & Control*)	
3.1.1	**Ylläpitääkö palveluntarjoaja käyttöomaisuuskirjanpitoa ja tietoturvapolitiikkaa?**
3.1.2	Kattaako käyttöomaisuuskirjanpito laitteet, ohjelmistot, tiedot ja fyysisen omaisuuden? Onko palvelut kuvattu?
3.1.3	Onko käyttöomaisuuskohteet turvaluokiteltu?
3.1.4.1	Kuinka usein käyttöomaisuuskirjanpito katselmoidaan ja päivitetään?
3.1.7	Edellyttääkö ICT-infrastruktuuriin kohdistuva hankinta tietohallintojohdon hyväksynnän?
3.1.8	Tapahtuvatko kaikki ICT-infrastruktuuriin tehtävät muutokset asianomaisten tiimien tekemänä?

3.2.1	**Tukeeko palveluntarjoajan tarjoama ohjelmisto vaadittua tietojen turvaluokittelua?**
3.2.6	Onko palveluntarjoajalla systemaattinen, laadukas menettely tietojen varmuuskopiointiin?
3.2.6.1	Hoidetaanko varmuuskopiointi paikan päällä vai etäältä?
3.2.6.2	Mikäli varmuuskopiointi hoidetaan etäältä, onko sopimuksessa huomioitu paperitulosteiden turvaluokittelu asiaan liittyvine menettelyineen?
3.2.6.3	Kuinka varmuuskopioiden kierrosta ja tuhoamisesta on huolehdittu?
4. Henkilöturvallisuus Henkilötietojen käsittelyssä on noudatettava lakia yksityisyyden suojasta työelämässä.	
4.1.1	**Mitä taustaselvityksiä palveluntarjoaja tekee ennen henkilöiden palkkausta?**
4.1.4	Onko taustaselvitykset tehty vakinaisen henkilöstön osalta? Mikä on tilanne osapäiväisten, konsulttien, tilapäistyövoiman ja sopimuspohjaisen työvoiman osalta?
4.1.5	Kattaako selvitysprosessi ajoittaiset uudelleentarkistukset ja huomioidaanko selvityksessä tehtäviin liittyvä turvaluokitusvaatimus?
4.1.6	Allekirjoittavatko työntekijät salassapitosopimuksen tai -sitoumuksen?
4.1.7	Onko työehdoissa mainittu selkeästi vaatimukset asioiden luottamuksellisuudesta ja niihin liittyvistä vastuista?
4.1.8	Onko palveluntarjoajan henkilöstön pysyvyys ja vaihtuvuus toimialan normaalia tasoa?
4.1.9	Onko työtekijät sitoutettu yhtiöön jollakin tavalla?
4.1.9.1	Jos, niin millä tasolla ja miten?
4.1.10	Mitä sertifikaatteja tietoturvapalveluja tarjoavan yhtiön työntekijöillä on?
4.2.1	**Onko palveluntarjoajalla tietoturvallisuuteen liittyvää valmennus- tai koulutusohjelmaa?**
4.2.2	Saavatko kaikki uudet työntekijät tehtäviinsä ja vastuisiinsa nähden oikeanlaista tietoturvallisuuteen liittyvää valmennusta?
4.2.3	Sisältääkö tietoturvakoulutus ohjelmistojen testaustoiminnot?
4.2.4	Kuvaa mikä tahansa valmennus, jonka palveluntarjoajan tulisi tarjota tilaajan henkilöstölle.
4.2.5	Onko olemassa käyttäjäseminaareja, joihin tilaajan henkilöstön tulisi osallistua?
4.2.6	Huomioidaanko turvallisuusvalmennuksessa työtehtäviin ja vastuisiin liittyvät asiat? Sisältyykö valmennukseen tietoturvapolitiikka, toimintamallit ja prosessit?
4.2.8	Kattaako valmennus työntekijöiden vastuun tietoturvarikkomusten raportoinnista?
4.2.9	Onko tietoturvavalmennus jatkuvaa?
4.2.10	Tehdäänkö valmennusta toistuvasti ja säännönmukaisesti?
4.2.11	Onko henkilöstölle tarjolla koulutusta tukevaa tietoturvamateriaalia esim. sisäisen intranetin kautta?
4.2.14	Onko henkilöstö tietoinen, kuinka sen tulee toimia katastrofitilanteessa?
4.3.1	**Onko palveluntarjoajan sisäisessä ohjeistuksessa huomioitu vastuut koskien tietoturvarikkomuksia, uhkia, haavoittuvuuksia ja järjestelmien käyttökatkoksia?**
4.3.2	Onko palveluntarjoajan kaikissa sopimuksissa huomioitu mahdolliset tietoturvarikkomukset?

4.3.3	Onko palveluntarjoajalla riittävä vakuutusturva?
4.3.3.1	Jos on, minkä tyyppisiä ja mitä rajoituksia ne sisältävät?
4.3.6	Onko tietoturvarikkomusten raportoinnista sovittu palveluntarjoajan ja asiakkaan kesken?
4.3.7	Onko olemassa prosessia, jolla tietoturvallisuuden tasoa pyritään parantamaan jatkuvasti?
4.3.8	Onko sovittu kurinpidollisista toimenpiteistä tietoturvallisuuden rikkomistapauksissa?
5. Fyysinen ja ympäristöturvallisuus	
5.1.1	**Onko käytössä toimintamallia, jonka mukaisesti huolehditaan kriittisten järjestelmien tietoturvasta?**
5.1.2	Omistaako palveluntarjoaja toimitilansa? Mikäli tilat on vuokrattu, sopimuksen päättymishetki on oltava selvillä.
5.1.3	Onko palveluntarjoaja huolehtinut tilojensa kulunvalvonnasta ym. fyysisestä turvallisuudesta?
5.1.4	Onko palveluntarjoajan toimitilojen läheisyydessä erityistä riskiä aiheuttavaa pysyväisluonteista toimintaa, kuten räjähdysainetehdasta, ydinvoimalaa tai kemian alan yritystä?
5.1.4.1	Jos vastaus on kyllä, uhat tulee selvittää ja arvottaa.
5.1.5	Mikäli palveluntarjoaja toimii yhteisissä tiloissa jonkun toisen yrityksen kanssa, tilan jako on kuvattava.
5.1.6	Onko mahdollista, että palveluntarjoaja voi joutua tekemisiin terrorismin tai muun vastaavan uhan kohteeksi?
5.1.6.1	Mikäli näin on, uhka tulee kuvata tarkemmin.
5.1.7	Näyttävätkö toimitilat mahdollisimman huomaamattomilta?
5.1.8	Onko logistiikkatoimintoja varten varattu alue eristetty?
5.1.8.1	Jos on, onko kulunvalvonta kyseiselle alueelle kunnossa?
5.1.9	Kuvaa miten IT-konesali on suojattu.
5.1.10	Onko konesali muun kulunvalvonnan piirissä?
5.1.10.1	Jos ei ole, kuvaa miten konesalin kulunvalvonta on järjestetty.
5.1.11	Miten konesalin turvallisuutta seurataan?
5.1.11.1	Viimeisen kahden turvallisuustestin tulokset?
5.1.11.2	Miten kulunvalvonta on toteutettu?
5.1.11.3	Onko kulunvalvonnassa käytetty vähintään kahteen erilliseen tunnistamiseen käytettyä menettelyä?
5.1.11.4	Hyväksyvätkö esimiehet kulkuoikeuksien muutokset?
5.1.11.5	Valvotaanko kaikkia kulkuväyliä reaaliaikaisesti?
5.1.11.6	Saavatko vieraat kulkea tiloissa ilman saattajaa?
5.1.11.7	Pidetäänkö satunnaisesti rakennuksessa käyvät henkilöt fyysisesti erossa asiakkaiden luottamuksellisesta aineistosta?
5.1.12	Kuvaile menettelyjä, joiden avulla huolehditaan rakennuksen turvallisuudesta, henkilöstön ja vieraiden pääsystä, kerättävistä lokitiedoista sekä siitä, miten virka-ajan valvontatoimet eroavat muun ajan valvonnasta.

5.1.13	Kuinka turvallisuushenkilöstö huolehtii rakennuksen turvallisuudesta?
5.1.14	Kuinka pitkään järjestelmien lokitietoja säilytetään?
5.1.15	Onko rakennuksessa käytetty turvakameroita ja liiketunnistimia ja pidetäänkö niiden kunnosta huolta?
5.1.15.1	Jos on, kuvaile kunnossapidon ja huollon menettelyt.
5.1.16	Onko ympäristöön liittyvästä suojauksesta huolehdittu (kuten tulipalo, vesivahinko, ilmanvaihto ja sähkönsyöttö)?
5.1.16.1	Jos on, kuvaile miten turvatoimia testataan.
5.1.17	Ovatko konekeskusten ilmastointilaitteet erillään muusta talon ilmastoinnista?
5.1.17.1	Onko riittävästä varavoiman syötöstä huolehdittu?
5.1.17.1.1	Onko varavoiman syöttöä testattu?
5.1.17.2	Onko koko konesalille olevaa varajärjestelmää? Jo on, millainen tämä on (*hot site*, cold site tai vastaava)
5.1.18	Hoidetaanko eri asiakkaiden työt toisistaan erillisissä tiloissa?
5.1.19	Kuvaile voimassa olevat vakuutukset.
5.1.20	Onko kiinteistöjen vakuutusturva riittävä?
5.2.1	**Onko olemassa menettelyjä, joiden mukaan mahdollisen turvallisuusuhan alla olevia laitteita valvotaan?**
5.2.2	Onko tietoliikenneverkko suojattu fyysisesti?
5.2.3	Onko verkon infrastruktuuri suojattu liialta hajasäteilyltä (ns. TEMPEST)?
5.2.4	Ovatko puhelinkaapelointiin liittyvät kaapit ja jakamot suojattu?
5.2.5	Miten katkeamattoman virransyötön järjestelmien toimivuudesta on huolehdittu? Kuinka pitkään UPS-laitteisto pitää yllä järjestelmiä katkon sattuessa? Kuinka nopeasti varavoimala käynnistyy? Kuinka kauan varavoimaa on saatavissa ilman tankkausta tai huoltotoimia?
5.2.6	Ovatko kaikki tuotantolaitteistot sijoitettu konesaliin?
5.2.7	Onko kaikki laitteet yksilöity nimitarralla tai muulla tavoin?
5.2.8	Mitä kokonaisuuteen kuuluvia laitteita on muualla kuin konesalissa?
5.2.8.1	Poikkeavatko politiikat tai toimintaohjeet näiden laitteiden osalta konesalissa voimassa olevista?
5.2.9	Kyetäänkö ylläpitotoimia hoitamaan etäältä?
5.2.9.1	Jos voidaan, kuvaile aiheeseen liittyvien valtuuksien hallinta.
5.2.10	Kuinka laitteiden romutus ja kierrätys on hoidettu?
5.3.1	**Onko tietoturvapolitiikassa tai -ohjeissa huomioitu tietojen turvaluokat ja luokkien edellyttämät asiat? (kuten lukitut kaapistot, ruudunpimennys- ja muut toimenpiteet)?**
5.3.2	Sovelletaanko tietoturvaohjeistoa liikuteltaessa laitteita paikasta toiseen?
5.3.3	Kuinka laitteiden luvaton siirtely on estetty?
6. Tietoliikenteen ja toiminnan johtaminen	
6.2.1	Seuraako palveluntarjoaja kapasiteetin käyttöastetta, suorituskykyä ja tapahtumamääriä?

6.3.1	Millaisia menettelyitä on virusten ja muiden haittaohjelmien torjuntaan?
6.3.2	Onko palveluntarjoajalla menettelyt sovellusten lähdekoodien auditointiin sekä ajettavan koodin toimivuuden varmistamiseen?
6.4.1	Kuvaile palveluntarjoajan menettelyt varmuuskopioinnissa
6.4.2	Otetaanko varmuuskopiot säännöllisesti?
6.4.3	Miten varmuuskopiot on suojattu?
6.4.4	Kuinka usein varmuuskopiot otetaan?
6.4.5	Säilytetäänkö kopioita jossain muualla kuin palveluntarjoajan tiloissa?
6.4.6	Kuinka nopeasti varmuuskopiot ovat saatavilla palautusta varten?
6.4.7	Onko varmuuskopioiden tietoturvallisuus samalla tasolla kuin alkuperäisen aineiston?
6.4.8	Tekeekö varmuuskopioinnin joku siihen erikoistunut osasto tai yksikkö?
6.4.9	Kuinka kontrolloidaan sitä, että varmuuskopiota ei tuhota ennen kuin uusi vastaava korvaa sen?
6.4.10	Kuinka huolehditaan tarpeettomien varmuuskopioiden tuhoamisesta?
6.4.11	Kuinka pitkään lokeja säilytetään?
6.4.12	Kuinka pitkään varmuuskopioita säilytetään? Huolehditaanko pitkäaikaissäilytettävien ajoittaisesta tuoreuttamisesta?
6.4.13	Onko varmuuskopiointimenettely testattu?
6.4.14	Kuinka usein testaus on tehty? Milloin viimeksi?
6.4.15	Ketkä osallistuvat testaukseen?
6.4.16	Onko varmuuskopioiden palautusrutiini auditoitu?
6.4.17	Pidetäänkö järjestelmän päivityksistä (laite- ja ohjelmistopäivitykset) lokia?
6.5.1	Kattaako palveluntarjoajan tietoverkko seuraavat asiat:
6.5.2	Verkon segmentointi, DMZ-vyöhykkeet ja palonmuurit?
6.5.4	Käyttäjille tarjottava tietoturvallinen etäkäyttöratkaisu?
6.5.6	Säännöllinen, toistuva haavoittuvuuksien testaus?
6.5.6.1	Tietoverkon ja järjestelmien monitorointi?
6.5.6.2	Tietoverkon redundanssi ja tärkeimpien laitteiden kahdennus?
6.5.6.3	Kontrollit, joilla estetään asiaton verkon käyttö?
6.5.6.4	Onko käytössä IDS tai IPS -järjestelmiä?
6.5.7	Sisältääkö lokien tai verkon valvonta seuraavia asioita:
6.5.8	Epäonnistuneet sisäänkirjautumisyritykset
6.5.10	Laajoja käyttöoikeuksia sisältävien käyttäjätunnusten käytön ja niiden luomisen tarkkailu
6.5.11	Ennalta määrättyjen tapahtumien jäljittäminen
6.5.12	Arkaluontoisten tietojen tai ohjelmien käyttö
6.5.13	Soittosarjojen aktiivisuus
6.5.14	Palomuurin aktiivisuus

6.5.15	Sisäänkirjautumisyritykset sovelluksiin ja käyttöjärjestelmään
6.5.16	Tietoturvan hallinnan aktiivisuus
6.5.17	Automatisoidut, määräajoin tehtävät turva-arvioinnit
6.5.18	IDS/IPS:n käyttö
6.5.20	Lokitietojen asianmukainen suojaus
6.5.21	Tietoturvapolitiikan vastaisten laitteiden ja palveluiden tunnistus
6.6.1	Onko palveluntarjoajalla menettelytavat erilaisten tietovälineiden käsittelyyn ja tuhoamiseen?
6.6.2	Onko palveluntarjoaja huolehtinut käytöstä poistettujen tietovälineiden asianmukaisesta tuhoamisesta?
6.6.3	Onko palveluntarjoajalla arkistonmuodostussuunnitelma (tai vastaava politiikka) tietoaineiston säilyttämiseen ja hävittämiseen?
6.6.4	Onko palveluntarjoajalla dokumentoituna menettelyt kuinka tietovälineisiin kirjataan tunnistetiedot ja kuinka ne on varastoitu?
6.6.5	Kykeneekö nauhavarmistukset tekevä järjestelmä jäljittämään muualle lähetetyt nauhat?
6.6.5.1	Jos kykenee, mikä nauhavarmistusohjelmisto on käytössä?
6.7.1	Mitä erilaisia tapoja palveluntarjoajalla on tiedonvälitykseen, tiedonsiirtoon ja kommunikointiin?
6.7.2	Mitä turvamenettelyjä on käytössä kussakin välineessä tai tavassa?
6.7.5	Kykeneekö palveluntarjoaja toteuttamaan erilaiset sovelluskoodin varmistukseen liittyvät sopimukset, kuten *escrow*-menettelyn?
6.7.6	Onko julkaistavan informaation hallintaan menettelyä?
6.7.7	Onko sähköisessä asioinnissa huolehdittu tietoturvallisuudesta?
6.7.8	Ulottuuko suojaus tiedon pitkäaikaissäilytykseen? Miten varmistetaan tiedon palautus pitkän ajan kuluttua?
6.7.9	Kattaako tietoturvallisuus koko toimitusketjun?
6.7.10	Onko seuraavat asiat huomioitu sähköisessä kauppapaikassa:
6.7.11	Luottamuksellisuus
6.7.12	Tapahtumiin liittyvä oikeuksien tarkistus
6.7.13	Käyttövaltuudet
6.7.14	Kiistämättömyys
6.7.15	Tapahtumien eheys
6.7.16	Kuinka käyttäjän tunnistus tapahtuu?
6.7.17	Onko online-rekisteröinti hoidettu sähköisten kauppapaikkojen ja verkkopankkijärjestelmissä?
6.7.19	Kykeneekö palveluntarjoaja tietojen salaamiseen? Millä välineellä ja millä salaustasolla?
6.7.20	Ovatko käyttäjätunnukset kryptattuja kaikissa vaiheissa ja paikoissa?
6.8.1	Tarkastetaanko säännöllisesti, onko käytössä tarpeettomia pääkäyttäjätunnuksia (*Admin, Root*) tai pääkäyttäjän oikeuksilla toimivia ohjelmia (kuten *daemons* ja muut taustaprosessit)?

6.8.2	Tarkkaillaanko reitittimien ja palomuurien lokeja säännöllisesti?
6.8.3	Ovatko kaikki tarpeettomat palvelut (esim. Telnet) ja protokollat suljettu?
6.8.4	Käytetäänkö verkon tietoturvallisuuden analysoinnissa säännöllisin väliajoin turvaohjelmistoa, joka käy läpi kaikki keskeiset kohteet ja komponentit?
6.8.4.1	Jos käytetään, mitä tuotteita on käytössä?

LIITE 7 VOIMASSA OLEVA VAHTI-OHJEISTUS JA -JULKAISUT

VAHTI 7/2006: Muutos ja tietoturvallisuus, alueellistamisesta ulkoistamiseen- hallittu prosessi
VAHTI 6/2006: Tietoturvatavoitteiden asettaminen ja mittaaminen
VAHTI 5/2006: Asianhallinnan tietoturvallisuutta koskeva ohje
VAHTI 4/2006: Selvitys valtionhallinnon ympärivuorokautisen tietoturvatoiminnan järjestämisestä
VAHTI 3/2006: Selvitys valtionhallinnon tietoturvaresurssien jakamisesta
VAHTI 2/2006: Electronic-mail Handling Instruction for State Government
VAHTI 1/2006: VAHTIn toimintakertomus vuodelta 2005
VAHTI 3/2005: Tietoturvapoikkeamatilanteiden hallinta
VAHTI 2/2005: Valtionhallinnon sähköpostien käsittelyohje
VAHTI 1/2005: Information Security and Management by Results
VAHTI 5/2004: Valtionhallinnon keskeisten tietojärjestelmien turvaaminen
VAHTI 4/2004: Datasäkerhet och resultatstyrning
VAHTI 3/2004: Haittaohjelmilta suojautumisen yleisohje
VAHTI 2/2004: Tietoturvallisuus ja tulosohjaus
VAHTI 1/2004: Valtionhallinnon tietoturvallisuuden kehitysohjelma 2004-2006
VAHTI 7/2003: Ohje riskien arvioinnista tietoturvallisuuden edistämiseksi valtionhallinnossa
VAHTI 6/2003: Opas julkishallinnon tietoturvakoulutuksen järjestämisestä
VAHTI 5/2003: Käyttäjän tietoturvaohje
Datasäkerhetsanvisning för användaren
User´s Information Security Instruction
VAHTI 4/2003: Valtionhallinnon tietoturvakäsitteistö
VAHTI 3/2003: Tietoturvallisuuden hallintajärjestelmän arviointi
VAHTI 2/2003: Turvallisen etäkäytön arkkitehtuuri
VAHTI 1/2003: Valtion tietohallinnon Internet-tietoturvallisuusohje

VAHTI 4/2002: Arkaluonteisten kansainvälisten aineistojen käsittelyohje
VAHTI 3/2002: Etätyön tietoturvaohje
VAHTI 1/2002: Tietoteknisten laitetilojen turvallisuussuositus
VAHTI 6/2001: Tietotekniikkahankintojen tietoturvallisuustarkistuslista
VAHTI 4/2001: Sähköisten palveluiden ja asioinnin tietoturvallisuuden yleisohje
VAHTI 3/2001: Salauskäytäntöjä koskeva valtionhallinnon tietoturvallisuussuositus
VAHTI 2/2001: Valtionhallinnon lähiverkkojen tietoturvallisuussuositus
VAHTI 1/2001: Valtion viranomaisen tietoturvallisuustyön yleisohje
VAHTI 3/2000: Tietojärjestelmäkehityksen tietoturvallisuussuositus
VAHTI 2/2000: Valtion tietoaineistojen käsittelyn tietoturvaohje (uudistettavana)
VAHTI 2/1999: Valtion tietohallintotoimintojen ulkoistamisen tietoturvallisuussuositus (uudistettavana)

Ohjeisto löytyy VAHTIn Internet-sivuilta *www.vm.fi/vahti* ja ohjeita saa myös tilattua hyvin edullisesti painotalo Editasta.

VAHTI

VALTIOVARAINMINISTERIÖ
Snellmaninkatu 1 A
PL 28, 00023 VALTIONEUVOSTO
Puhelin: (09) 160 01
Telefaksi: (09) 160 33123
www.vm.fi

7/2006
MUUTOS JA TIETOTURVALLISUUS, ALUEELLISTAMISESTA ULKOISTAMISEEN – HALLITTU PROSESSI

ISBN 951-804-624-7 (nid.)
ISBN 951-804-625-5 (PDF)
ISSN 1455-2566