Katastrofinkestävän ICT-järjestelmän toteutus

Case Pirkanmaan sairaanhoitopiirin potilastietovarasto

HAMK
HÄMEEN AMMATTIKORKEAKOULU

Ammattikorkeakoulun opinnäytetyö

Tietojenkäsittelyn koulutusohjelma

Visamäki, syksy 2012

Ismo Pulli

HAMK
HÄMEEN AMMATTIKORKEAKOULU

TIIVISTELMÄ

Hämeenlinna, Visamäki
Tietojenkäsittelyn koulutusohjelma

Tekijä Ismo Pulli **Vuosi** 2012

Työn nimi Katastrofinkestävän ICT-järjestelmän toteutus, case Pirkanmaan sairaanhoitopiirin potilastietovarasto

TIIVISTELMÄ

Työn toimeksiantaja oli Fujitsu Finland Oy, joka tuottaa asiakkailleen tietotekniikan palveluita, joihin sisältyvät muun muassa maantieteellisesti hajautetut, katastrofinkestävät ICT-kapasiteettipalvelut. Katastrofinkestävien ICT-kapasiteettipalveluiden avulla yritykset ja julkishallinnon organisaatiot voivat varmistaa toimintakriittisten ICT-järjestelmien käytettävyyden vakavissa, laajavaikutteisissa häiriötilanteissa.

Työn tarkoituksena oli tuoda esille jatkuvuuden hallinnan tärkeys organisaatioiden toiminnalle ja selvittää katastrofinkestävien ICT-järjestelmien ominaisuuksia ja toteutuksessa huomioitavia asioita. Katastrofinkestävän ICT-järjestelmän käytännön esimerkkinä oli Pirkanmaan sairaanhoitopiirin potilastietovarastojärjestelmä, joka toteutettiin maantieteellisesti hajautettuna kapasiteettipalveluna Fujitsun toimesta. Aiheen taustoittamiseksi työssä selvitettiin aluksi yleisiä jatkuvuuden hallintaan liittyviä periaatteita, säännöstöjä ja ohjeita sekä tuotiin esille tutkimustietoa jatkuvuuden hallinnan tilasta Suomessa. Työssä sovellettiin käytännön työelämässä hankittua tietoa ja aineistona käytettiin asiakkaan ja toimittajan edustajilta haastatteluissa saatuja tietoja sekä aihetta koskevia julkaisuja: kirjallisuutta, web-sivuilla olevia artikkeleita, erilaisia ohjeita ja dokumentteja.

Työn johtopäätöksenä oli, että vaikka organisaatiot ovat enenevässä määrin riippuvaisia ICT-järjestelmien toimivuudesta, merkittävä määrä suomalaisia organisaatioita ei kuitenkaan ole tutkimusten mukaan varautunut suunnitelmallisesti toiminnan jatkuvuutta uhkaaviin häiriötilanteisiin. Korkean käytettävyyden ICT-järjestelmien suunnittelussa ja toteuttamisessa vaaditaan laaja-alaista osaamista tietoliikenteestä, tallennusjärjestelmistä, palvelimista ja sovelluksista. Hyödyntämällä tietoteknistä osaamista ja käyttämällä nykypäivänä saatavilla olevia teknologioita voidaan toteuttaa katastrofinkestäviä ICT-järjestelmiä, joilla varmistetaan organisaatioiden kriittisten tietojärjestelmien toiminta vakavissakin häiriötilanteissa.

Avainsanat ICT-järjestelmä, jatkuvuus, katastrofi, toipuminen

Sivut 38 s. + liitteet 6 s.

HAMK
UNIVERSITY OF APPLIED SCIENCES

Hämeenlinna, Visamäki
Degree Programme in Business Information Technology

Author Ismo Pulli **Year** 2012

Subject of Bachelor's thesis Implementation of disaster tolerant ICT systems, case Pirkanmaa Hospital District's patient record warehouse system.

ABSTRACT

The thesis was commissioned by Fujitsu Finland Oy, which provides its customers with information technology services, including geographically dispersed, disaster tolerant ICT capacity services. Disaster tolerant ICT capacity services help the private and public sector organizations to ensure the continuity of their business critical ICT systems in severe and extensive disruptions.

The purpose of the thesis was to highlight the importance of business continuity management for the organizations' operations and to bring up features of the disaster tolerant ICT systems and things to consider when implementing them. As a practical example of the disaster tolerant ICT-system was Pirkanmaa Hospital District's patient record warehouse system, which was implemented as geographically dispersed capacity service by Fujitsu. In order to give background information around the topic, general practices, regulations and instructions related to business continuity management were explained along with introduced research results on the status of business continuity management in Finland. The knowledge obtained in the working life was applied to the thesis and the interviews with the customer and supplier representatives as well as publications on the subject, such as literature, articles on the web pages, various documents, were used as reference material.

The conclusion of the thesis was that although organizations are increasingly dependent on ICT systems, a significant number of Finnish organizations, according to studies, are not systematically prepared for disruptions that are threatening business continuity. When designing and implementing high availability ICT systems, wide expertise in network communications, storage systems, servers and applications is required. By utilizing the expertise and using technologies available today, one can implement disaster tolerant ICT systems which ensure continuity of organizations' business critical systems in severe disruptions.

Keywords ICT systems, continuity, disaster, recovery

Pages 38 p. + appendices 6 p.

SANASTO

BCM Business Continuity Management. Toiminnan jatkuvuuden hallinta.

BCP Business Continuity Plan. Toiminnan jatkuvuussuunnitelma.

BGP Border Gateway Protocol. Internetin ja MPLS-verkkojen reititysprotokolla.

CDP Continuous Data Protection. Jatkuva tiedon suojaus. Tiedon varmistamisen ja suojaamisen tapa, jossa kaikki sovelluksen kirjoitustapahtumat tallennetaan normaalin levytallennuksen lisäksi erilliseen lokiin. CDP mahdollistaa tietojen palautuksen mihin tahansa ajanhetkeen taaksepäin riippuen historiatiedolle varatusta tallennustilasta.

COBIT Control Objectives for Information and Related Technologies. Kansainvälisen Information Systems Audit and Control Associationin, ISACA, kehittämä ja ylläpitämä hyvän tietohallintotavan kuvausmalli.

CWDM Coarse wavelenght division multiplexing**.** Teknologia, jolla valokuituyhteyden tiedonsiirtokapasiteettia voidaan kasvattaa jakamalla se useisiin eri aallonpituuskanaviin. CWDM-teknologiassa aallonpituuksien kanavaväli on harvempi, jolloin käytettävien kanavien määrä on pienempi kuin DWDM-teknologiassa.

DICOM Digital Imaging and Communications in Medicine. Kansainvälinen, terveydenhuollossa käytetty standardi kuvantamistietojen käsittelyyn ja tiedonsiirtoon.

DRP Disaster Recovery Plan. Toipumissuunnitelma.

DWDM Dense wavelength division multiplexing. Teknologia, jolla yksittäisen valokuituyhteyden tiedonsiirtokapasiteettia voidaan kasvattaa jakamalla se useisiin eri aallonpituuskanaviin. DWDM-teknologiassa aallonpituuksien kanavaväli on tiheämpi, jolloin käytettäviä kanavia on käytettävissä enemmän kuin CWDM-teknologiassa.

FCP Fibre Channel Protocol. Kuitukanavaprotokolla. Tietoliikenneprotokolla, jota käytetään SAN-tallennusverkossa.

HL7 Health Level Seven. Kansainvälisesti toimiva, voittoa tavoittelematon organisaatio, Health Level 7 International, joka kehittää terveydenhuollon standardeja eri järjestelmien yhteensopivuuden edistämiseksi.

IaaS	Infrastructure as a Service. Pilvipalveluna toimitettavat palvelin- ja tallennuskapasiteettipalvelut.
IEC	International Electrotechnical Commission. Kansainvälinen sähköalan standardointikomissio.
IHE	Integrating the Healthcare Enterprise. Kansainvälinen, terveydenhuollon ammattilaisista ja toimijoista koostuva yhteisö, joka määrittelee terveydenhuollon tietojärjestelmien yhteensovittamiseksi standardeihin perustuvia profiileja.
ISO	International Organization for Standardization. Kansainvälinen standardisointijärjestö, joka tuottaa kansainvälisesti tunnustettuja ja hyväksyttyjä standardeja eri osa-alueille.
ITIL	IT Infrastructure Library. Laaja dokumenttikirjasto IT-palveluiden suunnittelun, tuottamisen ja hallinnan parhaista käytännöistä.
MPLS	Multiprotocol Label Switching. Kytkentäinen verkko, jossa verkon käytettävissä olevat reitit on ennalta määritetty. MPLS-verkkoon tuleville datapaketeille asetetaan leima, jonka avulla paketti voidaan kytkeä nopeasti eteenpäin MPLS-verkon reitittimissä.
NAS	Network Attached Storage. Ethernet-verkkoon liitettävä tiedostopohjainen tallennusjärjestelmä.
PaaS	Platform as a Service. Pilvipalveluna toimitettavat tietokanta- ja sovellusalustapalvelut.
PACS	Picture Archiving and Communication System. Kuvantamisen toiminnanohjausjärjestelmä, jolla hallinnoidaan digitaalisia kuvantamistutkimuksia.
Palvelinklusteri	Server Cluster. Kahden tai useamman palvelimen muodostama looginen kokonaisuus. Palvelimet ovat liitetty toisiinsa tietoliikenneväylän välityksellä ja palvelinklusteri näkyy tietoliikenneverkossa yhtenä loogisena palvelimena.
PCI DSS	Payment Card Industry Data Security Standards. Standardi, jota kaikkien luottokorttitietoja käsittelevien tahojen tulee noudattaa toiminnassaan.
SaaS	Software-as-a-Service. Pilvipalveluna tuotettavat sovellusten käyttöpalvelut.
SAN	Storage Area Network. Datablokkipohjaisten tallennusjärjestelmien liitäntäverkko, jossa käytetään Fibre Channel ja iSCSI-tiedonsiirtoprotokollia.

SHARE	SHARE Inc. on yhdysvaltalainen, IBM-tietokoneiden kanssa työskentelevien käyttäjien vuonna 1955 perustama IT-käyttäjäyhdistys.
VAHTI	Valtionhallinnon tietoturvallisuuden johtoryhmä. Toimielin, jonka tarkoituksena on kehittää ja ohjeistaa tietoturvallisuus-työtä valtionhallinnossa sekä edistää valtion viranomaisten yhteistyötä tietoturvallisuuteen liittyvissä asioissa.
XDS	Cross Enterprise Document Sharing. IHEn standardeihin perustuva määrittely, joka mahdollistaa terveydenhuollon dokumenttien tiedonsiirron eri toimijoiden järjestelmien välillä.

SISÄLLYS

1 JOHDANTO 1

2 KATASTROFINKESTÄVÄ ICT-JÄRJESTELMÄ 2

3 TOIMEKSIANTAJAN ESITTELY 3

3.1 Kapasiteettipalvelut 3
3.2 Katastrofinkestävät kapasiteettipalvelut 4

4 JATKUVUUDEN HALLINTA 4

4.1 Jatkuvuussuunnitelma 5
4.2 Toipumissuunnitelma 6
4.3 Suunnitelmien testaaminen 6
4.4 Jatkuvuussuunnittelun vaatimukset 7
4.4.1 Lainsäädännön vaatimukset 7
4.4.2 Eri sidosryhmien vaatimukset 7
4.5 Valtionhallinnon suositukset ja ohjeet 8
4.6 Kunnallishallinnon suositukset ja ohjeet 8
4.7 Rahoitus- ja vakuutusalan määräykset ja ohjeet 9
4.8 Jatkuvuuden hallinnan standardit 9
4.9 Jatkuvuuden hallinnan parhaat käytännöt 10
4.10 Jatkuvuuden hallinnan tilanne Suomessa 10

5 KATASTROFINKESTÄVIEN ICT-JÄRJESTELMIEN TOTEUTTAMINEN 11

5.1 Katastrofista toipumisen luokitustasot 12
5.2 ICT-järjestelmien hajauttamista edellyttäviä säännöstöjä 12
5.3 Katastrofinkestävän ICT-infrastruktuurin ominaisuuksia 14
5.4 Konesali 15
5.5 Tietoliikenne 16
5.6 Tallennusjärjestelmät 17
5.6.1 Varmuuskopioiden käyttö tiedon hajauttamiseen 17
5.6.2 Etäkopiointi 17
5.6.3 Jatkuva tiedon suojaus 19
5.6.4 Toipumistavoitteet tallennusjärjestelmän kannalta 19
5.7 Palvelimet 20
5.8 Palvelinklusterit 20
5.8.1 Maantieteellisesti hajautetun klusterin toiminnan varmistaminen 21
5.8.2 Virtuaalipalvelimet 22
5.9 Tietokannat 24
5.10 Sovellukset 25
5.11 Pilvipalvelut 25

6 CASE PIRKANMAAN SAIRAANHOITOPIIRIN POTILASTIETOVARASTO 26

6.1 Pirkanmaan sairaanhoitopiiri 26
6.2 Asiakkaan järjestelmähankkeen taustaa 26
6.3 Järjestelmälle asetut yleiset vaatimukset 27
6.4 Järjestelmän katastrofinkestävyyden vaatimukset 28
6.5 Valittu järjestelmäratkaisu 28

6.6 Tekninen toteutus 28
6.6.1 Konesali 29
6.6.2 Tietoliikenne 29
6.6.3 Levykapasiteetti 30
6.6.4 Jatkuva tiedon suojaus 31
6.6.5 Palvelinkapasiteetti 32
6.7 Käyttöönotto 32
6.8 Järjestelmän toimintakriittisyys 32
6.9 Kokemukset ja palaute 33

7 YHTEENVETO 33

LÄHTEET 35

Liite 1 Jatkuvuuden hallintaan liittyviä lakeja ja asetuksia
Liite 2 Jatkuvuuden hallintaan liittyviä valtionhallinnon suosituksia ja ohjeita
Liite 3 Katastrofista toipumisen luokitustasot

1 JOHDANTO

Tietoyhteiskunnassa tiedon, ja erityisesti sähköisen tiedon, merkitys korostuu. Tieto ja tiedon hallinta ovat yritysten ja organisaatioiden toiminnan ja kilpailukyvyn kulmakiviä. Tiedon tulee olla saatavilla, tiedon tulee olla luotettavaa ja tiedon eheys pitää pystyä varmistamaan - myös häiriötilanteissa. Tietoyhteiskunnan toiminta riippuu enenevässä määrin erilaisista ICT-järjestelmistä ja niiden käytettävyydestä. ICT-järjestelmien häiriöttömän käytön varmistaminen on siten yhteiskunnan, yritysten ja organisaatioiden toiminnan jatkuvuuden perusedellytys.

Häiriötilanteiden vaikuttavuus ja laajuus ICT-järjestelmien käytettävyyteen vaihtelee. Häiriötilanne voi aiheutua yksittäisen ICT-laitteen vikaantumisesta, jonka vaikutusalue on rajatumpi, ja johon voidaan varautua esimerkiksi käyttämällä monennettuja laitekomponentteja. Pahimmillaan häiriötilanne voi vaikuttaa koko konesalin käytettävyyteen. Tällaisia uhkatekijöitä voivat olla muiden muassa erilaiset luonnonmullistukset, häiriöt energian jakelussa, tulipalot, vakavat laiteviat, inhimilliset erehdykset ja tahalliset vahingonteot. Katastrofinkestävillä järjestelmillä tarkoitetaan tässä opinnäytetyössä sellaisia ICT-järjestelmiä, jotka kestävät konesalin osittaisen tai täydellisen tuhoutumisen.

Työn toimeksiantajana on Fujitsu Finland Oy, ja toimittajan esittelyssä kerrotaan lyhyesti Fujitsun ICT-kapasiteettipalveluista. Asiakasesimerkkinä on Pirkanmaan sairaanhoitopiiri ja asiakkaan potilastietovarasto, jonka toimivuus on asiakkaalle liiketoimintakriittistä. Asiakasesimerkin avulla kerrotaan, mitä vaatimuksia organisaatio ja lainsäädäntö asettivat järjestelmän toiminnalle, miten käytännössä toteutettiin erittäin tiukat käytettävyysvaatimukset täyttävä katastrofinkestävä ICT-järjestelmä kapasiteettipalveluna ja miten valittu ratkaisu täytti asiakkaan asettamat vaatimukset.

Opinnäytetyö sisältää tietoa ICT-teknologioista, joilla on mahdollista toteuttaa katastrofinkestäviä ICT-järjestelmiä. Asiakasesimerkissä tutkimusmenetelmänä käytetään kvalitatiivista menetelmää haastattelemalla asiakkaan sekä järjestelmän toimittajien edustajia. Opinnäytetyön aineisto koostuu haastattelujen ja työelämässä hankitun tiedon lisäksi aiheeseen liittyvistä julkaisuista: kirjallisuus, web-sivuilla olevat artikkelit, erilaiset ohjeet ja dokumentit.

Opinnäytetyö vastaa seuraaviin kysymyksiin:

Mitä on toiminnan jatkuvuuden hallinta ja mitä vaatimuksia lainsäädäntö ja eri sidosryhmät asettavat jatkuvuuden hallinnalle?
Millä teknologioilla ja palveluilla voidaan toteuttaa katastrofinkestäviä ICT-järjestelmiä?
Miten katastrofinkestävä ICT-järjestelmä toteutettiin?

2 KATASTROFINKESTÄVÄ ICT-JÄRJESTELMÄ

Katastrofinkestävillä, engl. Disaster Tolerant, ICT-järjestelmillä tarkoitetaan sellaisia järjestelmiä, jotka kestävät yksittäisen konesalin osittaisen tai täydellisen tuhoutumisen käyttökelvottomaksi. Katastrofinkestävien järjestelmien toteuttaminen perustuu niiden hajauttamiseen kahteen tai useampaan konesaliin, jotka sijaitsevat maantieteellisesti riittävän etäällä toisistaan.

Suomen kielessä katastrofi-sana liitetään usein luonnonmullistuksiin ja suuronnettomuuksiin. Tässä opinnäytetyössä katastrofilla ei kuitenkaan tarkoiteta pelkästään maantieteellisesti tai yhteiskunnallisesti laajavaikutteista ja merkittävää poikkeusolojen häiriötilannetta. Katastrofi voi olla yhteiskunnan normaalioloissa tapahtuva häiriötilanne, joka voi vaarantaa yksittäisen organisaation toiminnan jatkuvuuden, mutta ei vaikuta muiden organisaatioiden toiminnan jatkuvuuteen. Katastrofin sijaan voidaan käyttää myös termiä poikkeustilanne.

Toiminnan jatkuvuuden varmistaminen katastrofitilanteissa edellyttää organisaatioilta suunnitelmallista jatkuvuuden hallintaa. Jatkuvuuden hallintaan liittyy erilaisten riskien ja uhkatekijöiden kartoittaminen ja analysoiminen. Häiriötilanteiden syntymistä ei voida kokonaan poistaa, mutta tunnistettujen uhkien todennäköisyyttä ja vaikutusta voidaan arvioida ja niihin voidaan etukäteen varautua. Aiheen taustoittamiseksi opinnäytetyön alussa kerrotaan lyhyesti, mitä jatkuvuuden hallinta on, mitä lainsäädännöllisiä ja toimialakohtaisia vaatimuksia sille asetetaan ja mitä ohjeita ja standardeja on käytettävissä jatkuvuussuunnittelun avuksi.

Julkista tietoa käytännössä toteutetuista katastrofinkestävistä ICT-järjestelmistä on verrattain vähän saatavilla johtuen todennäköisesti siitä, että organisaatiot eivät halua julkisesti tuoda esille valmiuttaan varautua häiriötilanteisiin. Tässä opinnäytetyössä voidaan kuitenkin asiakkaan ja järjestelmätoimittajan myötävaikutuksella tuoda esille, että katastrofinkestävien ICT-järjestelmien toteuttaminen ei ole mahdollista pelkästään ICT-teknologiatoimittajien myyntikalvoissa, vaan käytännössä toteutettavissa ja esimerkkitapauksessa palveluna ilman, että asiakkaan täytyy itse investoida korkean käytettävyyden IT-teknologiaan.

3 TOIMEKSIANTAJAN ESITTELY

Fujitsu on johtava japanilainen ICT-alan yritys, joka valmistaa tietotekniikka-alan tuotteita ja on maailman kolmanneksi suurin ICT-palveluiden toimittaja. Fujitsu toimii yli 100 maassa ja sen palveluksessa on yli 170 000 työntekijää. (Fujitsu n.d.a.)

Fujitsu Finland Oy on yksi Suomen suurimmista tietotekniikan palvelu- ja laitetoimittajista. Suomessa Fujitsun palveluksessa työskentelee noin 2 900 työntekijää, jotka huolehtivat asiakkaiden tieto- ja viestintätekniikasta sekä sovellusten tukipalveluista, toiminnasta ja kehittämisestä. (Fujitsu n.d.b.)

3.1 Kapasiteettipalvelut

Fujitsu tuottaa palveluna palvelin- ja tallennuskapasiteettia, joka joustaa erilaisten suorituskyky-, käytettävyys- ja kasvutarpeiden mukaan. Kapasiteettipalvelussa asiakas maksaa vain käyttämästään kapasiteetista, asiakkaan ei tarvitse sitoa pääomaa laitehankintoihin eikä henkilöstöresursseja kapasiteetin hallintaan. Fujitsu vastaa palvelun tuottamisesta ja kehittämisestä, jolloin asiakas voi keskittyä omaan toimintaansa.

Palvelinkapasiteettia on saatavana sekä fyysisenä että virtuaalisena. Palvelinkapasiteettipalvelua tuotetaan muiden muassa IBM AIX-, IBM i-, Linux-, Oracle Solaris- ja Windows-palvelinkäyttöjärjestelmille. Palveluvalikoimassa on sekä vakioituja kokoonpanoja että asiakaskohtaisesti määriteltäviä kokoonpanoja. Palvelinkapasiteettipalveluun sisältyy vakiona palvelinkapasiteetin lisäksi palvelimien valvonta 24/7 sekä palvelimen hallintapalvelu asiakkaan kanssa sovittavalla palveluajalla. Palvelinkapasiteettia on saatavana myös pilvipalveluna, jossa hallintaportaalin kautta asiakas voi itse ottaa käyttöön ja hallinnoida virtuaalipalvelinkapasiteettia.

Levykapasiteettia on saatavana eri vaihtoehtoina luokiteltuna ohjeellisten suorituskyky- ja käyttötarpeiden mukaisesti. Levykapasiteettipalvelu tuotetaan korkean käytettävyyden NAS-, SAN- ja arkistolevyjärjestelmillä. Varmistuskapasiteettia on saatavana eri vaihtoehtoina luokiteltuna ohjeellisesti toipumistavoitteiden mukaisesti. Varmistuskapasiteettipalvelua tuotetaan sekä nauha- että levyvarmistuslaitteistoilla.

Kapasiteettipalvelut tuotetaan konesalikäyttöön rakennetuista, turvallisista ja energiatehokkaista palvelinkeskuksista. Palvelinkeskukset ovat korkean käytettävyyden laitetiloja, joissa on varmistettu sähkönsyöttö ja jäähdytys, tilat on varustettu paloilmaisin- ja sammutusjärjestelmällä ja fyysistä turvallisuutta valvotaan kulunvalvonnalla ja hälytysjärjestelmillä.

3.2 Katastrofinkestävät kapasiteettipalvelut

Hajauttamalla asiakkaiden tietojärjestelmät ja niiden tarvitsemat kapasiteettipalvelut maantieteellisesti eri paikoissa sijaitseviin palvelinkeskuksiinsa Fujitsu tuottaa katastrofinkestävää kapasiteettipalvelua, joka täyttää tiukimmatkin käytettävyys- ja toipumisvaatimukset ja turvaa asiakkaiden toiminnan jatkuvuuden poikkeustilanteissa. Katastrofinkestävät kapasiteettipalvelut perustuvat johtavien laite- ja ohjelmistotoimittajien teknologioihin, jotka Fujitsu on huolellisesti arvioinut ja integroinut toimivaksi palvelukokonaisuudeksi.

4 JATKUVUUDEN HALLINTA

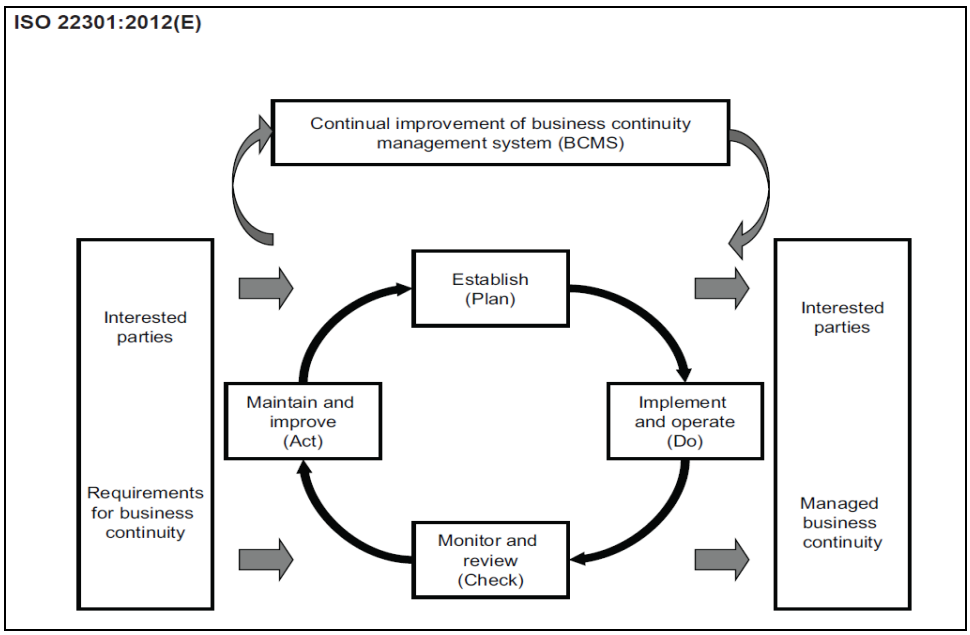
Toiminnan jatkuvuuden hallinnalla tarkoitetaan suunnitelmallisia toimenpiteitä, joilla pyritään kartoittamaan ja ennakoimaan mahdolliset uhat, selvittämään niihin liittyvät riskit, suojaamaan toimintaa erilaisilta uhilta sekä palautumaan ja toipumaan häiriötilanteista. Jatkuvuuden hallinnan tulisi sisältyä jokaisen organisaation toimintastrategiaan. Ilman suunnitelmallista jatkuvuuden hallintaa organisaation kyky selviytyä yllättävistä häiriö- ja poikkeustilanteista on heikko. Pahimmassa tapauksessa organisaatio voi muuttua kokonaan toimintakyvyttömäksi.

Työ- ja elinkeinoministeriön alaisuudessa toimiva Huoltovarmuuskeskus, joka vastaa Suomen huoltovarmuuden suunnittelusta, kehittämisestä ja operatiivisesta toiminnasta, määrittelee jatkuvuuden hallinnan seuraavasti: ”Jatkuvuudenhallinnalla tarkoitetaan kaikkia niitä toimenpiteitä, joiden avulla organisaatio ennalta suunnitelluilla ja toteutetuilla järjestelyillä ja johtamismalleilla hallitsee erilaiset toimintaansa uhkaavat häiriötilanteet. Organisaatioiden jatkuvuudenhallinnan menettelyt takaavat osaltaan kansalaisille, yrityksille ja organisaatioille suunnattujen palveluiden saatavuuden häiriötilanteissa ja poikkeusoloissa.” (Huoltovarmuuskeskus n.d.)

Laajasti käytetty IT-palvelunhallinnan parhaiden käytäntöjen dokumenttikirjasto IT Infrastructure Library, ITIL, määrittelee jatkuvuuden hallinnan seuraavasti: ”Liiketoiminnan jatkuvuudenhallinta on liiketoimintaprosessi, jonka vastuulla on hallita liiketoimintaan vakavasti vaikuttavia riskejä. Prosessi turvaa keskeisten sidosryhmien etuja, mainetta, brändiä ja arvoa tuottavia toimintoja. Prosessi osallistuu riskien pienentämiseen hyväksyttävälle tasolle sekä liiketoimintaprosessien toipumisen suunnitteluun liiketoiminnan keskeytymisen varalle. Liiketoiminnan jatkuvuudenhallinta asettaa tavoitteet, laajuuden ja vaatimukset IT-palvelun jatkuvuudenhallinnalle.” (ITIL 2011, 15.)

Jatkuvuuden hallinta on jatkuva prosessi. Jatkuvuuden hallinnan standardi, ISO 22301:2012 Societal security - Business continuity management systems – Requirements, kuvaa jatkuvuuden hallinnan prosessin Plan-Do-Check-Act –mallin, lyhenne PDCA, mukaisesti (kuva 1). PDCA-mallissa prosessi kuvataan kierrettävänä, ympyränmuotoisena koostuen suunnitteluvaiheesta, toteutusvaiheesta, tarkastusvaiheesta sekä ylläpito- ja kehitysvaiheesta, jonka jälkeen taas aloitetaan suunnitteluvaiheesta. Jatkuvuuden hallinnan prosessi saa syöttötietoina vaatimuksia organisaatiolta ja eri si-

dosryhmiltä. Prosessin tuotoksena on hallittu toiminnan jatkuvuuden varmistaminen ja dokumentoitu ja ylläpidetty jatkuvuussuunnitelma, engl. Business Continuity Plan, BCP.



Kuva 1. ISO 22301:2012 Societal security - Business continuity management systems – Requirements - Jatkuvuuden hallinnan prosessin PDCA-malli.

4.1 Jatkuvuussuunnitelma

Valtionhallinnon tietoturvallisuuden johtoryhmä, VAHTI, määrittelee jatkuvuussuunnitelman seuraavasti: ”Kriittisten ja tärkeimpien toimintaprosessien jatkuvuussuunnitelma. Toimintojen ja niitä mahdollistavan tietojenkäsittelyn ja tiedonsiirron turvaaminen niin, että ne voivat jatkua kriisien, katastrofien, onnettomuuksien, toimintaolosuhteiden merkittävien muutosten ja häiriöiden aikana sekä niiden jälkeen. Kaikki ne toimenpiteet, jotka tulee tehdä kriittisen toimintaprosessin jatkuvuuden turvaamiseksi.” (VAHTI 2008, 43.)

Iivarin ja Laaksosen (2009, 92) mukaan jatkuvuussuunnitelman laatiminen alkaa jatkuvuussuunnittelun perusteiden ja organisaation ja sen toiminnan ymmärtämisestä. Suunnittelun tulee olla koordinoitua ja sillä tulee olla johdon tuki. Tyypillisesti suunnitelmat laaditaan eri tasoille: strateginen taso, prosessitaso ja IT-järjestelmätaso. Suunnitelman laatiminen voidaan aloittaa vasta sen jälkeen, kun vastuut ja suunnitelman taso on päätetty.

Jatkuvuussuunnitteluun liittyvässä riskien kartoituksessa pyritään tunnistamaan sisäiset ja ulkoiset riskitekijät, arvioimaan niiden todennäköisyys ja laajuus sekä vaikutukset toiminnalle, engl. Business Impact Analysis, BIA. Vaikutuksia analysoitaessa tulisi ottaa huomioon sekä välittömiä että välillisiä kustannustekijöitä, kuten esimerkiksi liikevaihdon ja markkinaosuuksien menetykset, toiminnan palauttamisesta aiheutuvat kustannukset, maineen ja luottamuksen menettämisen vaikutukset jne.

4.2 Toipumissuunnitelma

Toipumissuunnitelma on osa liiketoiminnan jatkuvuussuunnitelmaa. Toipumissuunnitelma sisältää ohjeet katastrofista toipumisesta ja normaaliin toimintaan palautumista (Iivari & Laaksonen, 2009, 19). Tietojen, prosessien ja järjestelmien omistajat määrittävät omistamiensa tietojen, prosessien ja järjestelmien suojauksen, toipumisen ja palautumisen vaatimukset sekä toiminnan keskeytymisvaikutukset. Keskeisiä asioita, joihin omistajat toipumissuunnittelussa osallistuvat, ovat järjestelmien ja prosessien tärkeysluokittelu ja toipumistavoitteiden määrittäminen. (Iivari & Laaksonen, 2009, 101.)

Toipumistavoitteet määritellään kahden yleisesti käytetyn määreen perusteella: toipumispistetavoite, engl. Recovery Point Objective, RPO, ja toipumisaikatavoite, engl. Recovery Time Objective, RTO. Toipumispistetavoite määrittelee, kuinka usein tiedot tulisi varmistaa eli kuinka paljon organisaatiolla on varaa menettää tietoa häiriötilanteessa. Esimerkiksi jos tietojärjestelmän RPO-tavoite on neljä tuntia, tulee tiedot varmistaa vähintään neljän tunnin välein. Toipumisaikatavoite määrittelee, missä ajassa järjestelmän tulisi palautua häiriötilanteesta tavoiteltuun tilaan, joka ei välttämättä ole sama kuin normaalitila. Jos esimerkiksi tietojärjestelmän RTO-tavoite on kaksi tuntia, tulee järjestelmän olla käytettävissä organisaation määrittelemällä tavalla ja laajuudessa kahden tunnin sisällä häiriötilanteen alkamisesta.

On virheellistä ajatella, että kaikille prosesseille ja toiminnoille määriteltäisiin mahdollisimman tiukat toipumistavoitteet ja sitten toteutettaisiin niitä vastaavat jatkuvuuden varmistamisen toimenpiteet ja järjestelyt. Käytännössä se ei ole mahdollista, sillä varautuminen aiheuttaa aina kustannuksia, ja mitä tiukemmat toipumistavoitteet, sitä kalliimpaa varautuminen on.

4.3 Suunnitelmien testaaminen

Jatkuvuus- ja toipumissuunnitelmien testaaminen on ensisijaisen tärkeää, jotta voidaan todentaa suunnitelmien tarkoituksenmukaisuus ja saadaan tietoa mahdollisista muutostarpeista. Säännöllisellä testaamisella pyritään siihen, että kaikki suunnitelmaan liittyvät tahot ja erityisesti toipumisesta vastaavat, ovat tietoisia suunnitelmasta, vastuistaan ja rooleistaan toiminnan jatkuvuuden ja tietoturvallisuuden turvaamisessa. (Iivari ja Laaksonen 2009, 189.)

Laajamittaisten testausten suorittaminen verkostoituneessa liiketoimintaympäristössä ja hajautetussa tietojenkäsittely-ympäristössä, organisaation päivittäistä toimintaa haittaamatta, voi olla sekä teknisesti että toiminnallisesti erittäin haastavaa ja merkittävä kustannustekijä. Käytännössä testaus useimmiten suoritetaan rajoitetusti, esimerkiksi testaamalla yksittäisiä kriittisiä toimintoja ja niihin liittyviä tietoteknisiä järjestelmiä.

4.4 Jatkuvuussuunnittelun vaatimukset

Jatkuvuuden hallinta ja suunnittelu on organisaatiokohtaista, eri organisaatioilla on erilaisia vaatimuksia ja tarpeita jatkuvuuden suunnittelulle. Lähtökohtaisesti yksityisten yritysten jatkuvuuden suunnittelua ohjaavat liiketoiminnalliset tavoitteet, mutta nykyisessä verkostoituneessa ja globaalissa toimintaympäristössä tulee liiketoiminnallisten tavoitteiden lisäksi huomioida myös toimintaympäristön vaatimukset.

Toimintaympäristön ja organisaation vaatimukset ja tarpeet määrittelevät jatkuvuussuunnittelun ja -suunnitelman laajuuden ja kattavuuden. Esimerkiksi joissain organisaatioissa saatetaan katsoa riittäväksi varautua vain normaaliolojen häiriötilanteisiin, kun taas erityisesti julkishallinnon organisaatioiden ja valmiuslain piiriin kuuluvien yritysten tulee huomioida jatkuvuussuunnittelussaan normaaliolojen häiriötilanteiden lisäksi myös yhteiskunnan poikkeusolot.

4.4.1 Lainsäädännön vaatimukset

Yhteiskunnan toiminnalle tärkeät toiminnot ovat merkittävissä määrin kotimaisten ja ulkomaisten yritysten tuottamien palveluiden varassa. Tällaisia ovat esimerkiksi tietoverkot, energiahuolto, elintarvikehuolto sekä terveydenhuolto. Turvatakseen yhteiskunnan toiminnan myös poikkeusoloissa lainsäädäntö ja valtionhallinto asettavat vaatimuksia organisaatioille, jotka ovat yhteiskunnan toiminnan tai huoltovarmuuden kannalta kriittisiä tai toimivat tietyllä toimialalla. Näin ollen julkisen hallinnon lisäksi lainsäädännön vaatimukset sitovat myös yksityistä elinkeinoelämää. Liitteessä 1 on lueteltu joitakin tärkeimpiä lakeja ja asetuksia, jotka tulee ottaa huomioon jatkuvuuden suunnittelussa. Suomen lainsäädännön lisäksi globaalisti toimivien yritysten tulee huomioida toiminnassaan kunkin kohdemaan lainsäädännön ja viranomaisten vaatimukset.

4.4.2 Eri sidosryhmien vaatimukset

Yrityksen tärkein sidosryhmä ovat asiakkaat, jotka voivat asettaa vaatimuksia jatkuvuuden suunnitteluun. Esimerkiksi Yritys A:lla voi olla sopimuksellisia tai lainsäädännöllisiä velvollisuuksia toimintansa jatkuvuuden varmistamiseen. Ostaessaan alihankintana tai ulkoistuspalveluna palveluita Yritykseltä B voi Yritys A sopimuksellisesti edellyttää Yritykseltä B sitoutumista oman toimintansa jatkuvuuden varmistamiseen laajuudessa, jota Yritys B:n ei mahdollisesti muuten tarvitsisi tehdä. Asiakasorganisaatiot voivat myös edellyttää, että palveluita tarjoava yritys täyttää tiettyjen säännöstöjen tai standardien vaatimukset. Asiakkaiden lisäksi myös muut sidosryhmät, kuten yrityksen omistajat, yhteistyökumppanit ja vakuutuslaitokset saattavat asettaa vaatimuksia, jotka tulee huomioida toiminnan jatkuvuuden suunnittelussa.

4.5 Valtionhallinnon suositukset ja ohjeet

Valtioneuvoston periaatepäätöksellään vahvistama yhteiskunnan turvallisuusstrategia, YTS, on perusta yhteiskunnan varautumiselle. Strategia kattaa yhteiskunnan varautumisen sekä kriisijohtamisen normaali- ja poikkeusoloissa ja pyrkii yhtenäistämään julkisen hallinnon, elinkeinoelämän ja järjestöjen varautumisen, kriisijohtamisen ja huoltovarmuuden suunnittelun perusteet. (YTS 2010, 5).

Valtionhallinnossa on viime vuosina kiinnitetty erityisesti huomiota tietoturvallisuuden ja jatkuvuuden hallinnan kehittämiseen. Valtionhallinnon toimesta on käynnistetty useita varautumiseen ja tietoturvallisuuteen liittyviä hankkeita, joiden pohjalta on julkistettu ohjeita ja suosituksia, joita voidaan pääosin hyödyntää myös yksityisellä sektorilla. VAHTI on julkaissut useita ohjeita, joita voidaan käyttää valtionhallinnon lisäksi hyväksi myös kunnallishallinnossa ja yksityisessä elinkeinoelämässä. Liitteessä 2 on lueteltu jatkuvuuden hallintaan oleellisesti liittyviä valtionhallinnon suosituksia ja ohjeita.

4.6 Kunnallishallinnon suositukset ja ohjeet

Kunnallishallinnolla on tärkeä rooli yhteiskunnan palveluiden järjestämisessä, joista tärkeimpänä ovat lainsäädännöllä kuntien hoidettavaksi asetetut sosiaali- ja terveydenhuollon palvelut. Valtiovarainministeriön toimesta toteutettiin vuonna 2010 kuntien ICT-varautumisen esitutkimushanke, KVARE, joka oli osa valtionhallinnon eVARE-hanketta. Esitutkimuksesta julkistettiin raportti, jossa asetettiin tavoitteeksi, että kunnat kykenisivät takaamaan tuottamiensa palvelujen jatkuvuuden häiriötilanteissa ja poikkeusoloissa. Raportissa määriteltiin tavoitteiden saavuttamiselle vaiheistettu aikataulu siten, että ensimmäisessä vaiheessa vuoden 2016 loppuun mennessä ICT-varautumisen ohjaus olisi osana kuntien yleisiä ohjausmenetelmiä, vaatimustasot olisi määritelty ja ICT-varautumisen toteuttaminen olisi käynnistetty. Toisessa vaiheessa vuoden 2020 loppuun mennessä kunnissa olisi saavutettu ICT-varautumisen perustaso kriittisissä toiminnoissa ja kunnille palveluja tuottavien tahojen vaatimusten hallinta ja sopimuskäytännöt olisivat yhtenäistetty. (KVARE 2011). Edellä mainittuja tavoitteita ei ole ainakaan toistaiseksi asetettu pakottaviksi määräyksiksi lainsäädännön keinoin.

Osana YTS:n toimeenpanoa, Turvallisuus- ja puolustusasiain komitean sihteeristö julkaisi vuonna 2012 oppaan ”Varautuminen ja jatkuvuudenhallinta kunnassa”, jonka tarkoituksena on auttaa kuntia ottamaan huomioon varautumista koskevat kysymykset kunnan toimintojen johtamisessa ja palveluiden jatkuvuudenhallinnassa. Oppaassa esitetään toimintamalli, jonka mukaisesti kunnissa voidaan tarkistaa varautumiseen kuuluvien hallinto- ja palvelurakenteiden toimivuus erilaisissa häiriötilanteissa ja poikkeusoloissa sekä tarvittaessa kehittää ja yhdenmukaistaa niitä. (Yhteiskunnan turvallisuus 2012, 3.)

Sosiaali- ja terveydenhuolto on nyky-yhteiskunnassa hyvin riippuvainen tietojärjestelmien toiminnasta ja kuntien on erittäin vaikeaa, jollei mahdo-

tonta turvata keskeisten sosiaali- ja terveystoimen palvelujensa toiminta ilman, että kunnat varautuvat niihin liittyvien tietojärjestelmien toiminnan jatkuvuuden varmistamiseen. Sosiaali- ja terveysministeriön vuonna 2011 julkaisemassa oppaassa sosiaali- ja terveydenhuollon johdolle ja turvallisuusasiantuntijoille ohjeistetaan, että tietojenkäsittelyn toipuminen ja toiminnan jatkuminen mahdollisissa häiriötilanteissa tulee varmistaa jatkuvuus- ja elpymissuunnitelmin (STM 2011, 33).

Sosiaali- ja terveysministeriön terveydenhuollon valmiussuunnitteluopas, joka on jo vuodelta 2002, neuvoo kuntia kuvaamaan, mihin terveyskeskuksen toimintoihin atk-häiriöt voivat vaikuttaa, ja miten toimintatavoilla voidaan estää atk:sta johtuvia häiriötekijöitä. Oppaassa todetaan, että atk-häiriöiden vaikutuksia voidaan vähentää työtapojen avulla. Esimerkiksi vastaanoton jatkaminen voidaan varmistaa tekemällä listaukset vastaanottopotilaista paperille ja myös laboratorio ja röntgen voivat käyttää erilaisia listauksia varmistamaan työn jatkumisen. (STM 2002, 82.) Vaikea on kuvitella, että terveydenhuollon valmiussuunnitteluoppaan ohjeet listausten tekemisestä toimisivat käytännössä. Mikäli potilastietojärjestelmässä tapahtuisi käyttökatko, ei potilastietojärjestelmästä saataisi tarvittavia tietoja tulostettua. Lisäksi julkishallinnon työntekijöiden työtaakka on monesti huomattavan suuri ilman IT-järjestelmien aiheuttamia lisätöitä, eikä listauksia voida etenkään päivystysvastaanotoilla tulostaa etukäteen.

4.7 Rahoitus- ja vakuutusalan määräykset ja ohjeet

Finanssivalvonta (entinen Rahoitustarkastuslaitos ja Vakuutusvalvontavirasto) on rahoitus- ja vakuutusalan valvontaviranomainen, joka antaa määräyksiä ja ohjeita Suomessa toimiville raha- ja vakuutuslaitoksille ja valvoo niiden toimintaa. Finanssivalvonnan määräyksen mukaan rahoitusmarkkinoilla toimiva rahalaitos täyttää sille laissa säädetyn varautumisvelvollisuuden, mikäli se noudattaa Huoltovarmuuskeskuksen alaisen Rahoitushuoltopoolin laatimaa Rahoitusmarkkinoiden varautumisohjetta ja Rahalaitoksen Standardi 4.4b – Operatiivisten riskien hallinta -standardia (Finanssivalvonta 2012, 23). Vakuutuslaitoksille asetetaan määräyksiä jatkuvuuden hallinnasta ja poikkeustilanteisiin varautumisesta Finanssivalvonnan määräys- ja ohjekokoelmassa 1/101/2009 (Finanssivalvonta 2011, 169-170).

PCI DSS –tietoturvastandardin noudattaminen on pakollista kaikille yrityksille, jotka käsittelevät korttimaksutapahtumia. Standardin kohdassa 12.9 vaaditaan, että organisaatioilla on toimintasuunnitelma, jossa kuvataan toiminnan jatkuvuuden ja toipumisen menetelmät ja varmuuskopioinnin prosessit. Suunnitelma pitää myös testata vähintään kerran vuodessa. (PCI DSS 2010, 68-69.)

4.8 Jatkuvuuden hallinnan standardit

Jatkuvuuden hallinnasta on luotu standardeja, joita koskevista ohjeista ja määrityksistä organisaatiot voivat saada tukea omaan jatkuvuuden hallintaan ja arvioida omaa toimintaansa standardien näkökulmasta. Organisaa-

tiot voivat myös pyytää valtuutettua tarkastajaa auditoimaan jatkuvuuden hallintaansa ja hakea sertifiointia standardin mukaiselle toiminnalleen. Viralliset standardeja koskevat dokumentit ovat maksullisia, eivätkä siten esimerkiksi internetistä vapaasti ladattavissa. Taulukossa (taulukko 1) on lueteltu joitakin jatkuvuuden hallintaan liittyviä ISO-standardeja. Tietotekniikka-alaan liittyvät standardit ISO tekee yhteistyössä IEC:n kanssa.

Taulukko 1. Jatkuvuuden hallinnan standardeja.

Standardi	Nimi	Kuvaus
ISO 22301:2012	Societal security - Business continuity management systems – Requirements	Standardi määrittelee vaatimukset toiminnan jatkuvuuden hallintaan ja sen ylläpitoon. Vaatimukset ovat yleispätevät kaikille organisaatioille.
ISO/IEC 27031:2011	Information technology - Security techniques - Guidelines for information and communications technology readiness for business continuity	Standardi sisältää ehdotuksen jatkuvuuden hallinnan rakenteesta ja viitekehyksestä (prosessit ja toimintatavat). Identifioi ja määrittelee kaikki oleelliset tekijät, joilla ICT:n valmiutta voidaan parantaa osana organisaation jatkuvuuden hallintaa. Auttaa organisaatiota mittaamaan jatkuvuuden hallintaa ja valmiutta selviytyä häiriötilanteesta. Standardia voidaan hyödyntää kaikissa organisaatioissa.
ISO/IEC 24762:2008	Guidelines for information and communications technology disaster recovery services	Sisältää ohjeita katastrofista toipumiseen liittyvien ICT-palveluiden käyttöön ja käyttöönottoon osana toiminnan jatkuvuuden hallintaa. Hyödynnettävissä sekä organisaation oman IT-yksikön tuottamiin että ulkoistettuihin palveluihin.

4.9 Jatkuvuuden hallinnan parhaat käytännöt

IT-palvelunhallinnan ja tietohallinnon parhaat käytännöt on kuvattu ITIL- ja COBIT-viitekehysmalleissa, jotka ovat käytössä useissa organisaatioissa ympäri maailmaa. ITILin version 3 osiossa Palvelusuunnittelu, engl. Service Design, sisältää IT-palvelun jatkuvuuden hallinnan, engl. IT Service Continuity Management, parhaat käytännöt. COBIT-mallissa prosessit on jaettu neljään toimialueeseen, engl. domains, jossa Deliver, Service and Support-toimialue, DSS, sisältää muun muassa jatkuvuuden hallintaan liittyvät parhaat käytännöt.

4.10 Jatkuvuuden hallinnan tilanne Suomessa

Suomessa ei juurikaan ole tehty laajamittaisia tutkimuksia organisaatioiden jatkuvuuden hallinnasta. Market-Visio Oy:n vuonna 2009 tekemän ja

vuonna 2010 julkistaman tutkimuksen keskeisimpiä havaintoja oli, että suuret yritykset ja huoltovarmuuden kannalta kriittiset julkiset organisaatiot olivat jatkuvuuden hallinnassa vahvimpia osaajia ja myös finanssialan organisaatiot edustivat jatkuvuussuunnittelun kärkeä. Tutkimuksen mukaan ääripäiden väliset erot olivat merkittäviä pienissä ja keskisuurissa yrityksissä, joissa jatkuvuussuunnittelua toteutettiin keskimääräistä heikommin kuin suurissa yrityksissä. Pienissä ja keskisuurissa yrityksissä esiintyi myös selkeitä puutteita liiketoiminnan ja ICT:n välisten riippuvuuksien ymmärtämisessä ja ICT-riskien tunnistamisessa. Keskisuurissa yrityksissä johdon sitoutuneisuus jatkuvuussuunnitteluun ja ICT-riskien hallintaan vaihteli, ja osa organisaatioista ei ollut selvittänyt ollenkaan ICT:hen liittyviä liiketoimintariskejä. (Market-Visio 2010, 6.)

Sofigaten ja Tietotekniikan liiton yhteistyössä toteuttamassa, vuosittaisessa tutkimuksessa koskien tietohallintojen johtamista Suomessa, 42 %:lla kyselyyn vastanneista ei ollut suunnitelmaa ICT-palveluiden laadunvarmistukseen. Tuloksen mukaan tilanne ei ollut muuttunut vuoteen 2011 nähden. (Tietotekniikan liitto 2012, 27.)

Computer Associatesin vuonna 2011 eurooppalaisissa yrityksissä teettämän tutkimuksen mukaan vain 26 %:lla haastatelluista organisaatioista oli muodollinen ja kattava toipumissuunnitelma ja 55 %:lla organisaatioista oli jonkinlainen toipumissuunnitelma, mutta se ei ollut muodollinen ja kattava. Tutkimuksen mukaan huonoiten varautuneet organisaatiot olivat Suomessa ja Alankomaissa. (CA Technologies 2011, 10.)

Computer Associatesin vuonna 2010 eurooppalaisiin yrityksiin kohdistuneessa tutkimuksessa arvioitiin käyttökatkoista aiheutuvia kustannuksia ja liikevaihdon menetyksiä. Tutkimuksen mukaan suomalaiset organisaatiot menettävät arviolta noin 440 miljoonaa euroa vuodessa ICT-järjestelmien käyttökatkojen takia. Tutkimukseen osallistui 1018 eurooppalaista organisaatiota, joista 102 oli Suomesta. Tutkimuksessa arvioitiin, että koko Euroopan tasolla käyttökatkoista aiheutuu vuosittain yli 17 miljardin liikevaihdon menetykset. (CA Technologies 2010.)

Vaikka edellä esitettyjen tutkimusten tulokset eivät suoraan ole verrannollisia toisiinsa, on tulosten perusteella pääteltävissä, että suomalaisten organisaatioiden tulisi kiinnittää enemmän huomiota jatkuvuuden hallintaan ja parantaa valmiuksiaan varautua häiriötilanteisiin. Tutkimustietojen perusteella voidaan myös olettaa, että organisaatiot eivät ole riittävästi varmistaneet toimintakriittisten ICT-järjestelmien käytettävyyttä ja nopeaa toipumista häiriötilanteissa.

5 KATASTROFINKESTÄVIEN ICT-JÄRJESTELMIEN TOTEUTTAMINEN

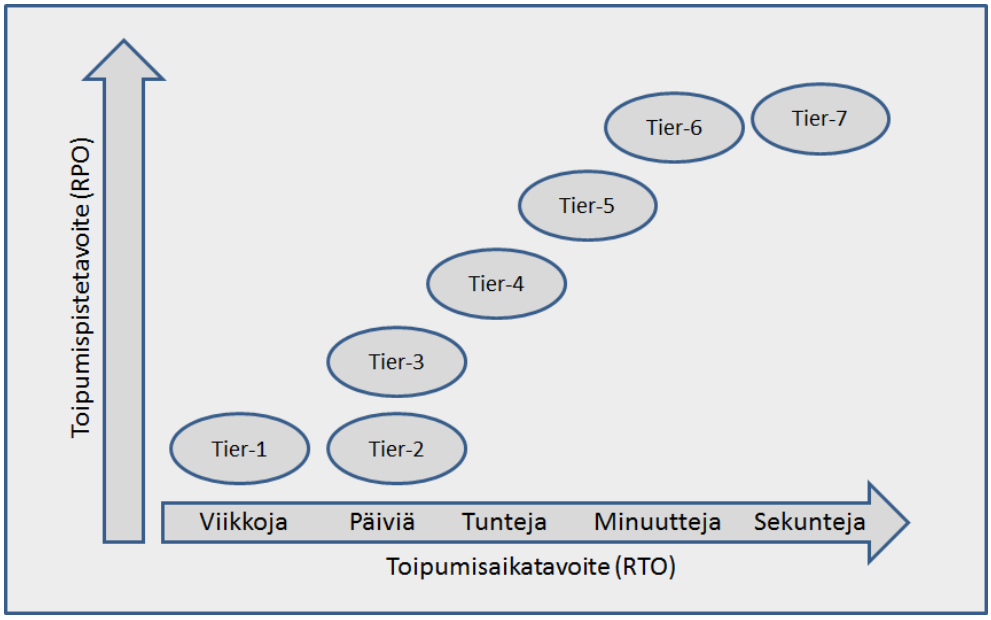
Katastrofinkestävien ICT-järjestelmien tavoitteena on mahdollistaa toipumistavoitteiden mukainen katastrofista toipuminen ja varmistaa organisaation tietojen saatavuus ja toiminnan jatkuminen. Katastrofista toipumisella, engl. Disaster Recovery, tarkoitetaan tässä opinnäytetyössä sellaisten

laitteiden, ohjelmistojen, tilojen ja palveluiden käyttöä ja niihin liittyviä toimenpiteitä, jotka mahdollistavat ICT-järjestelmän toipumisen katastrofitilanteissa.

5.1 Katastrofista toipumisen luokitustasot

ICT-alalla ei ole virallista standardia tai luokitusta katastrofista toipumisen eri tasoille, mutta usein viitataan yhdysvaltalaisen IT-käyttäjäyhdistyksen, SHAREn vuonna 1992 määrittelemään seitsemän tason luokitukseen, engl. Seven Tiers of Disaster Recovery, kun halutaan kuvata eritasoisia toipumisen mahdollistavia toteutustapoja. SHAREn mallissa on itse asiassa kahdeksan tasoa (0-7), mutta taso nolla on lähtötaso, joka ei täytä katastrofista toipumisen vaatimuksia. SHAREn luokitus- eli tier-tasot on kerrottu tarkemmin liitteessä 3.

SHAREn katastrofista toipumisen luokitustasoja voidaan tarkastella toipumistavoitteiden näkökulmasta. Eri luokitustasot mahdollistavat erilaisten toipumistavoitteiden saavuttamisen. Käytännön toteutusten pitäisi aina perustua järjestelmän toipumistavoitteisiin. Seuraava kuva (kuva 2) havainnollistaa luokitustasojen suhdetta ohjeellisiin toipumistavoitteisiin.



Kuva 2. Katastrofista toipumisen luokitustasojen suhde toipumistavoitteisiin.

5.2 ICT-järjestelmien hajauttamista edellyttäviä säännöstöjä

Kuten aiemmin on todettu, katastrofinkestävät järjestelmät perustuvat IT-järjestelmien hajauttamiseen kahteen tai useampaan konesaliin, jotka sijaitsevat maantieteellisesti riittävän etäällä toisistaan. Tietojärjestelmien hajauttamista koskevia ja organisaatioita sitovia vaatimuksia on kirjattu eri säännöstöihin, mutta niissä ei kuitenkaan aseteta vaatimuksia konesalien väliselle minimietäisyydelle.

Rahoituslaitoksia koskevassa Finanssivalvonnan Standardissa 4.4 b ”Operatiivisten riskien hallinta”, todetaan seuraavaa: ”Varautumisvelvollisen keskitetyn tietojenkäsittelyn infrastruktuurin tulee olla sellainen, että poikkeusoloissa tietojenkäsittelyn tulee olla kahdessa erillisessä toimipisteessä, joiden kapasiteetti on sellainen, että poikkeusoloissa ylläpidettäviä palveluita voidaan tarjota, vaikka toinen toimipiste ei olisi käytettävissä.” (Finanssivalvonta 2012, 26.)

Vakuutuslaitoksia koskevassa Finanssivalvonnan määräyksessä 1/01/2009 todetaan seuraavaa: ”Rakennettaessa tietojenkäsittelyn infrastruktuuria on otettava huomioon, että häiriötilanteiden varalle on varmuuskopiointi toipumisjärjestelmineen. Toiminnan jatkuvuuden kannalta riittävä tietojen ja ohjelmien suojakopiointi toipumisjärjestelmineen on järjestetty riittävän etäälle ja eri paikkakunnilla oleviin turvatiloihin. Suunniteltua perushuoltotasoa varten on käytettävissä riittävä määrä tietojenkäsittelykapasiteettia (varsinaisessa tuotanto- tai varakonekeskuksessa). Suunniteltua perushuoltotasoa varten on käynnistettävissä tietojenkäsittelytoiminta uudessa ympäristössä (varakonekeskuksessa). Erityisesti suojakopioiden käyttö tulee suunnitella siten, että suojakopioiden tietojen ja käytettävissä olevien ohjelmistojen pohjalta kyetään käynnistämään liiketoiminta uudelleen siinäkin tilanteessa, että varsinainen tietojenkäsittelykeskus ja sen lähialueet ovat pysyvästi tuhoutuneet. Tämä edellyttää suojakopioiden käyttövalmiuden varmistamista.” (Finanssivalvonta 2011, 171-172.)

PCI DSS –tietoturvastandardi ei edellytä maantieteellisesti kahdennettua tietojenkäsittely-ympäristöä. Standardin kohdassa 9.5 kuitenkin on vaatimuksena, että varmuuskopiot säilytetään turvallisessa paikassa ja suosituksena, että varmuuskopiot olisivat maantieteellisesti eri paikassa kuin varmistettavat tiedot. (PCI DSS 2010, 53.)

Valtioneuvoston päätöksessä huoltovarmuuden tavoitteista 21.8.2008/539 määrätään, että keskeisissä valtakunnallisissa tieto- ja viestintäjärjestelmissä yksittäisen kohteen lamautuminen tai vaurio ei saa lamauttaa koko järjestelmää. Päätöksessä myös määrätään, että yhteiskunnan keskeisimmät tietojärjestelmät ja tietovarannot on hajautettava maantieteellisesti vähintään kahteen paikkaan. (VNp 21.8.2008/539, kpl 2.2)

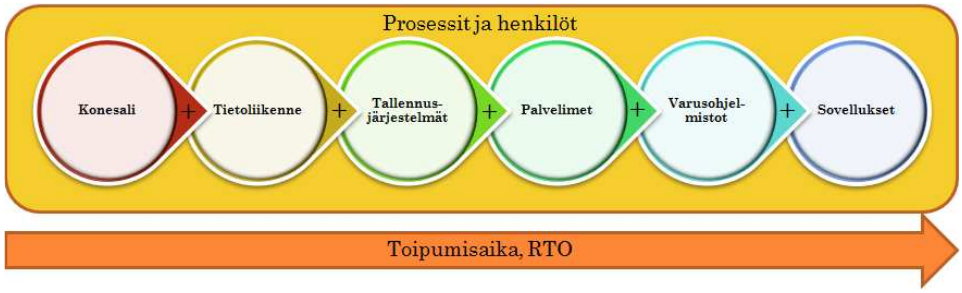
Viestintäviraston määräyksessä 54 A/2012M, koskien viestintäverkkojen ja –palvelujen varmistamista, luokitellaan viestintäverkon ja –palveluiden komponentit 1-5 tärkeysluokkaan. Tärkeysluokkien 1 ja 2 osalta edellytetään, että toisiaan varmistavat komponentit on sijoitettu eri rakennuksissa oleviin laitetiloihin, tai mikäli se ei ole kohtuullisin kustannuksin mahdollista, niin vähintään saman rakennuksen eri palotiloihin. (Viestintäviraston määräys 54 A/2012M, 4 §)

VAHTI-ohjeessa 2/2012 ”ICT-varautumisen vaatimukset” määritetään korkean varautumistason vaatimuksena, että kriittisten toimintojen tiedot on hajautettu maantieteellisesti vähintään kahteen eri paikkaan Suomessa. (VAHTI 2012, 76.) Lisäksi samassa ohjeessa todetaan korotetun varautumistason vaatimuksena, että organisaatiolla on suunnitelma ICT-palvelujen siirtämiseksi toisiin tiloihin. (VAHTI 2012, 77.)

5.3 Katastrofinkestävän ICT-infrastruktuurin ominaisuuksia

ICT-järjestelmän, joka voi olla yksittäinen sovellus tai järjestelmäkokonaisuus, käytettävyys riippuu monen eri osatekijän käytettävyydestä: konesali-infrastruktuuri, tietoliikenne, tallennusjärjestelmät, palvelimet, varusohjelmistot, sovellusohjelmistot. Lisäksi tulee huomioida ICT-järjestelmien keskinäiset riippuvuudet. Lähtökohtana katastrofinkestävien ICT-järjestelmien toteuttamisessa on, että ensin varmistetaan yksittäisten laitteistokomponenttien mahdollisimman hyvä vikasietoisuus, ja vasta sen jälkeen toteutetaan järjestelmien maantieteellinen hajauttaminen.

Järjestelmälle asetettavan toipumisaikatavoitteen laskennassa ja toipumisaikatavoitteen mahdollistavaa katastrofinkestävää järjestelmää suunniteltaessa on huomioitava koko palveluketju, unohtamatta prosessien ja henkilöstön osuutta (kuva 3). Koko järjestelmän käytettävyysvaatimus ei voi olla parempi kuin palveluketjun heikoimman komponentin käytettävyys, ja toipumisaikatavoite ei voi olla pienempi kuin palveluketjun heikoimman komponentin toipumisaikatavoite.



Kuva 3. ICT-järjestelmän palveluketju

Nykyisessä tietoyhteiskunnassa tietojenkäsittely on hajautettua koostuen monista eri järjestelmistä ja teknologioista. Hajautetussa ympäristössä katastrofinkestävien ICT-järjestelmien toteuttaminen on haastavaa, mutta laitteisto- ja ohjelmistovalmistajat ovat kehittäneet ratkaisuja, jotka auttavat haasteissa. Esimerkkinä virtualisointi, joka toisaalta tuo yhden hallittavan kerroksen lisää, mutta lisää joustavuutta ja parhaimmillaan integroi monitoimittajaympäristöjä yhtenäiseksi hallittavaksi kokonaisuudeksi.

ICT-järjestelmien toipumisvalmiutta kuvataan yleisesti englanninkielisillä termeillä cold standby, warm standby ja hot standby. Cold standby-valmiustilassa toipumisaika on pisin ja vastaavasti hot standby-valmiustilassa lyhin. ITIL v3 suomenkielisessä sanastossa termit on käännetty ja määritelty seuraavasti (taulukko 2).

Taulukko 2. ITIL-sanasto: cold standby, warm standby ja hot standby

Eng.kielinen termi	Suomenkielinen termi	Selitys
Gradual recovery, cold standby	Asteittainen toipuminen, ”kylmä valmiustila”	”Toipumisvaihtoehto, joka tunnetaan myös nimellä ’kylmä valmiustila’. Asteittainen toipuminen käyttää tyypillisesti siirrettävää tai kiinteää tilaa, jossa on

		ympäristön tuki ja verkkokaapelointi, mutta ei tietokonejärjestelmiä. Laitteisto ja ohjelmistot asennetaan osana IT-palvelun jatkuvuussuunnitelmaa. Asteittainen toipuminen vie tyypillisesti enemmän kuin kolme päivää, mutta voi viedä merkittävästi kauemminkin." (ITIL 2011, 57.)
Intermediate recovery, warm standby	Keskitason toipuminen, "lämmin valmiustila"	"Toipumisvaihtoehto, joka tunnetaan myös 'lämpimänä valmiustilana'. Keskinopea toipuminen käyttää yleensä jaettua siirrettävää tai kiinteää tilaa, jossa on tietokonejärjestelmät ja verkon komponentit. Laitteisto ja ohjelmistot on konfiguroitava ja tiedot palautettava osana IT-palvelun jatkuvuussuunnitelmaa. Tyypilliset keskinopeat toipumisajat ovat yhdestä kolmeen päivään." (ITIL 2011, 62.)
Fast recovery, hot standby	Nopea toipuminen, "kuuma valmius"	"Toipumisvaihtoehto, joka tunnetaan myös nimellä 'kuuma valmius'. Nopea toipuminen käyttää tavallisesti dedikoituja kiinteitä varatiloja, jossa on tietojärjestelmät ja ohjelmistot valmiiksi konfiguroituna IT-palvelujen tuotantoon. Välitön toipuminen kestää tyypillisesti 24 tuntia, mutta voi olla nopeampikin jos ei ole tarvetta palauttaa tietoja varmuuskopioista." (ITIL 2011, 52.)

5.4 Konesali

Konesaleille asetettavia turvallisuus- ja käytettävyysvaatimuksia määriteltäessä viitataan Suomessa yleisesti valtionhallinnon VAHTI-ohjeeseen 1/2002 "Tietoteknisten laitetilojen turvallisuussuositus" tai yhdysvaltalaisen Uptime Instituten tier-luokitukseen tai ANSI/TIA-942 -standardin "Telecommunications Infrastructure Standard for Data Centers" tier-luokitukseen. VAHTI-ohjeessa 1/2002 laitetilat on jaettu neljään eri luokkaan: perustaso, tehostettu perussuojaus, erityissuojaus ja täyssuojaus. Käytännössä katastrofinkestävyyden vaatimus on tasolla erityissuojaus, koska se edellyttää varatiloja. (VAHTI 1/2002, 7.) Uptime Instituten ja ANSI/TIA-942-standardin luokitukset määrittävät yksittäisten konesalien ominaisuuksia ja konesalin laitteistokomponenttien monentamisvaatimuksia, mutta luokitukset eivät edellytä konesalien maantieteellistä hajauttamista.

Yksittäisen konesalin toiminnan kannalta tärkeiden laitteistokomponenttien monentamiseen kannattaa panostaa, vaikka organisaatiolla olisikin toinen konesali käytettävissä. Panostamalla yksittäisen konesalin käytettävyyteen, voidaan minimoida laitteistokomponenttien vikaantumisesta johtuvat käyttökatkot ja tarve siirtää palvelut toiseen konesaliin. Esimerkiksi

Uptime Instituten Tier III-luokitus edellyttää, että konesalin toiminnan kannalta tärkeät laitteistot, kuten sähkönsyöttö ja jäähdytys, voidaan huoltaa ilman käyttökatkoja.

Konesalitilojen rakentaminen ja ylläpitäminen on kallista, eikä konesalien varustuksesta ja käytettävyysominaisuuksista kannata tinkiä. Täysin kalustettu ja aktiivisesti käytössä oleva toinen konesali, niin sanottu kuuma konesali, engl. hot-site, on kallein ylläpidoltaan. Toisaalta kuuma konesali mahdollistaa lyhyimmän toipumisajan ja kapasiteetti on aktiivisesti hyötykäytössä, eivätkä vain odottamassa mahdollista häiriötilannetta. Vaihtoehtona oman konesalin tai varakonesalin rakentamiselle on vuokrata konesalitilaa, sijoittaa IT-järjestelmät palvelutoimittajien konesaleihin tai käyttää palvelutoimittajien konesaleja varakonesalina.

5.5 Tietoliikenne

Tietoyhteiskunnassa tietoliikenne ja sen toimivuus ovat perusedellytys julkisten ja yksityisten organisaatioiden tuottamien palveluiden käytölle ja organisaatioiden sisäiselle ja ulkoiselle tiedonvälitykselle. Katastrofinkestävien IT-järjestelmien suunnittelussa tietoliikenneyhteyksien kahdentaminen on keskeinen tekijä. Konesalien väliset tietoliikenneyhteydet tulee kahdentaa, ja konesalin runkoverkon sekä palvelimien kytkentäverkon aktiivilaitteiden tulee olla kahdennettuja tai muuten vikasietoisia. Konesalien välisissä yhteyksissä kannattaa selvittää mahdollisuus käyttää CWDM- tai DWDM-teknologiaa, joilla yksittäisen kuituyhteyden kapasiteettia saadaan tehokkaasti laajennettua.

Ei riitä, että konesalin sisäiset ja konesalien väliset tietoliikenneyhteydet on varmistettu, sillä konesalissa olevia ICT-järjestelmiä pitää myös päästä käyttämään konesalin ulkopuolelta. Verkon topologia tulee toteuttaa niin, että tietoliikenneyhteydet konesaleihin on toteutettu toisistaan erillisinä eivätkä ne kulje toisen konesalin kautta. TCP/IP-verkkoon liitettyjen ICT-järjestelmien käyttö sekä Windows-käyttöympäristöissä koko Windows toimialueen toimivuus perustuu verkon nimipalvelun, engl. Domain Name System, DNS, toimintaan. Tästä syystä nimipalveluiden hajauttaminen maantieteellisesti on ensisijaisen tärkeää. Hajauttamisessa voidaan myös hyödyntää teleoperaattoreiden tai IT-palveluntarjoajien palveluna tuottamia nimipalveluita. Vikatilanteessa, jossa ICT-järjestelmien toiminta joudutaan siirtämään toisessa konesalissa oleville palvelimille, nimipalvelu nopeuttaa toipumista ohjaamalla tietoliikenneyhteydet automaattisesti toisessa konesalissa oleville palvelimille ilman manuaalisesti tehtäviä osoitemuutoksia.

Kuormantasauksella, engl. load balancing, voidaan tasata palvelinpalvelujen kuormitusta ohjaamalla tietoliikenne kulloinkin vähiten kuormitetulle palvelimelle ja optimoida siten kapasiteetin käyttöä ja palvelun vasteaikoja. Lisäksi kuormantasauksella voidaan toteuttaa korkean käytettävyyden verkkopalveluja, sillä palvelimen vikaantuessa tietoliikenne ohjataan toiselle palvelimelle. Konesalien välisessä, maantieteellisessä kuormantasauksessa periaate on sama kuin palvelimien välisessä kuormantasauksessa. Konesalien välisessä kuormantasauksessa, engl. Global Server Load Ba-

lancing, käytetään tyypillisesti nimipalveluihin tai verkkoliikenteen reititykseen perustuvaa kuormanjakotapaa.

5.6 Tallennusjärjestelmät

Hajautettujen, katastrofinkestävien järjestelmien tarkoituksena on varmistaa organisaation tarvitseman tiedon saatavuus häiriötilanteissa. Tiedot on tallennettuna palvelimien sisäisille levyille tai ulkoisiin levyjärjestelmiin, josta ne pitää siirtää maantieteellisesti toisessa paikassa olevaan konesaliin. Miten ja kuinka usein tiedot pitää siirtää, riippuu järjestelmälle asetetuista toipumistavoitteista.

5.6.1 Varmuuskopioiden käyttö tiedon hajauttamiseen

Yksinkertaisin ja kustannuksiltaan edullisin tapa hajauttaa tiedot maantieteellisesti kahteen eri paikkaan on siirtää varmuuskopiomediat fyysisesti toiseen paikkaan tai varmuuskopioida tiedot etäkonesalissa olevaan varmistuslaitteeseen. Varmistetut tiedot voidaan myös replikoida paikallisesta varmistuslaitteesta etäkonesalissa olevaan varmistuslaitteeseen. Varmuuskopioihin perustuva tiedon hajauttaminen ei sovi organisaation toiminnan jatkuvuuden kannalta järjestelmille, joiden toipumistavoitteet ovat tiukat, koska järjestelmän palauttaminen varmuuskopioilta voi kestää pahimmillaan useita tunteja, jopa päiviä, ja menetettävien tietojen määrä riippuu siitä, kuinka usein varmuuskopiot otetaan tai siirretään fyysisesti toiseen paikkaan.

5.6.2 Etäkopiointi

Jos toipumistavoitteet ovat vaativat, pitää tiedot etäkopioida, engl. remote copy, maantieteellisesti toiseen paikkaan. Tietojen etäkopiointi voidaan toteuttaa hallitummin ja helpommin, mikäli palvelimet käyttävät tallennustilanaan yhteiskäyttöisiä, ulkoisia SAN- tai NAS-levyjärjestelmiä sen sijaan, että tallennustilana käytettäisiin palvelimien sisäisiä levyjä. Etäkopiointi voi olla yhdensuuntaista, jolloin yhdessä maantieteellisessä paikassa olevat levyosiot ovat aktiivisesti käytössä luku- ja kirjoitustilassa ja data kopioidaan toisessa maantieteellisessä paikassa oleville passiivisille levyosioiden kopioille, jotka ovat vain lukutilassa. Tällöin puhutaan aktiivi/passiivi–konfiguraatiosta. Etäkopiointi voi olla toteutettu myös kahdensuuntaisesti, jolloin maantieteellisesti molemmissa paikoissa on eri sovellusten käytössä luku- ja kirjoitustilassa olevia levyosioita ja data kopioidaan ristiin toisessa maantieteellisessä paikassa oleville levyosioiden kopioille, jotka ovat vain lukutilassa. Tällöin puhutaan aktiivi/aktiivi–konfiguraatiosta.

Tietojen etäkopiointi toteutetaan joko synkronisesti tai asynkronisesti. Synkronisessa etäkopioinnissa levylle kirjoitus suoritetaan ensin paikalliseen levyjärjestelmään ja sen jälkeen maantieteellisesti toisessa konesalissa olevaan etälevyjärjestelmään. Vasta kun etälevyjärjestelmä on tallentanut tiedot, kuitataan kirjoitustapahtuma suoritetuksi. Synkronisessa etäkopioinnissa tietojen kopiointi tapahtuu reaaliaikaisesti, jolloin vikatilantees-

sa tietoja ei menetetä ollenkaan tai korkeintaan vain ne kirjoitustapahtumat, joiden suoritus oli kesken. Synkronisessa etäkopioinnissa paikalliseen ja etälevyjärjestelmään tallennetut tiedot ovat aina keskenään ajan tasalla.

Asynkronisessa etäkopioinnissa levylle kirjoitus suoritetaan ensin paikalliseen levyjärjestelmään, minkä jälkeen kirjoitustapahtuma kuitataan suoritetuksi. Sen jälkeen kirjoitustapahtuma kopioidaan taustatoimintona etälevyjärjestelmään, jossa se tallennetaan levylle. Vikatilanteessa, jossa työkuorma jouduttaisiin siirtämään toiseen konesaliin, menetetään kaikki ne kirjoitustapahtumat, joita ei vielä ollut tallennettu etälevyjärjestelmään. Asynkronista etäkopiointia käytettäessä onkin mahdollista, etteivät paikalliseen levyjärjestelmään ja etälevyjärjestelmään tallennetut tiedot ole keskenään ajan tasalla, jolloin tietojen menetyksen riski on suurempi kuin synkronisessa kopioinnissa. Asynkroninen etäkopiointi voidaan tehdä lähes reaaliaikaisesti tai erikseen määritellyin väliajoin. Riski menetettävän tiedon määrästä riippuu siitä, kuinka usein kopiointi suoritetaan.

Synkroninen etäkopiointi mahdollistaa asynkronista etäkopiointia varmemman tietojen suojauksen, mutta synkronista etäkopiointia voidaan käyttää vain silloin, kun konesalien välinen maantieteellinen etäisyys ei aiheuta liian suurta tiedonsiirron viivettä, latenssia. Tiedonsiirron latenssi kasvaa tietoliikenneyhteyden etäisyyden pidentyessä. Mikäli latenssi on liian suuri, joudutaan käyttämään asynkronista etäkopiointia. Erityisesti vasteaikakriittiset tapahtumankäsittelyjärjestelmät ovat herkkiä latenssille. Vaikka eräät teknologiatoimittajat tukevat jopa 200-300 kilometrin etäisyyksiä synkronisena etäkopiointina, käytännön toteutukset voivat jäädä ICT-järjestelmien latenssiherkkyyden takia paljon alle 100 km.

Datan etäkopiointi voidaan toteuttaa sovellustasolla, erillisillä laitteistoilla, ja levyjärjestelmillä. Levyjärjestelmätason etäkopiointi edellyttää, että sekä lähde- ja kohdepäässä käytetään saman valmistajan levyjärjestelmäteknologiaa. Levyjärjestelmäkohtaisia, eri toimittajien etäkopiointiratkaisuja ovat muun muassa Fujitsun Remote Equivalent Copy, EMC:n Symmetrix Remote Data Facility (SRDF) ja MirrorView, HP:n 3PAR Remote Copy ja Continuous Access EVA, IBM:n Metro Mirror ja GlobalMirror sekä NetAppin SnapMirror.

Organisaatioilla voi kuitenkin olla käytössään eri valmistajien levyjärjestelmiä tai saman valmistajan eri levyjärjestelmäteknologioita, jolloin etäkopioinnin toteuttaminen ei välttämättä ole joustavasti ja kustannustehokkaasti toteutettavissa. Tällaisessa ympäristössä voidaan käyttää virtualisointilevyjärjestelmiä, jotka virtualisoivat eri levyjärjestelmissä olevan fyysisen levykapasiteetin ja näyttävät sen loogisesti yhtenäisenä levykapasiteettina. Virtualisointikerros mahdollistaa etäkopioinnin eri merkkisten levyjärjestelmien välillä edellyttäen, että lähde- ja kohdepäässä käytetään saman valmistajan virtualisointiteknologiaa. Virtualisointilevyjärjestelmiä, joilla voidaan toteuttaa myös etäkopiointitoiminnot, ovat muun muassa EMC VPLEX, Hitachi USP-V/VSP, IBM SAN Volume Controller (SVC) ja NetApp V-Series.

5.6.3 Jatkuva tiedon suojaus

Tietojen reaaliaikainen tai lähes reaaliaikainen kopiointi mahdollistaa nopean toipumisen ja nopean tietojen saatavuuden häiriötilanteissa, mutta tiedot ovat kuitenkin haavoittuvaisia tietosisällön loogiselle rikkoontumiselle. Jos paikallisessa levyjärjestelmässä olevan tiedon tietosisältö rikkoontuu, niin rikkoontunut tietosisältö kopioituu etälevyjärjestelmään ennen kuin asia huomataan. Tällöin tiedot joudutaan palauttamaan varmuuskopioilta, ja se pidentää toipumisaikaa. Tietosisällön rikkoontuminen ei ole kovinkaan yleistä, mutta se on mahdollista, ja mitä kriittisemmästä sovelluksesta on kyse ja mitä vaativampi toipumisaikatavoite on, sitä tärkeämpää on suojautua tietosisällön rikkoontumista vastaan.

Tiedon loogiselta rikkoontumiselta voidaan suojautua käyttämällä jatkuvaa tiedon suojausta, engl. Continuous Data Protection, CDP. CDP perustuu siihen, että kaikki kirjoitustapahtumat tallennetaan normaalisti käytössä oleville levyosioille ja sen lisäksi erilliseen lokiin, josta ne kopioidaan käytössä olevien levyosioiden kopioille. Lokin avulla voidaan tiedot palauttaa taaksepäin haluttuun ajan hetkeen. Se, kuinka pitkälle taaksepäin voidaan palata, riippuu päivittäisten muutosten määrästä ja lokitiedolle varatusta levytilasta. Esimerkkejä CDP-tuotteista ovat FalconStorin Continuous Data Protector ja EMC:n RecoverPoint. Molemmat CDP-tuotteet ovat erillisiä laitteita, engl. appliance, jotka tukevat useiden eri toimittajien levyjärjestelmiä. Katastrofinkestävyys voidaan toteuttaa siten, että tiedot etäkopioidaan paikallisessa konesalissa olevan CDP-laitteiston kautta asynkronisesti tai synkronisesti maantieteellisesti toisessa konesalissa olevalle CDP-laitteistolle. CDP-laitteistojen etuna on jatkuvan tiedon suojaamisen lisäksi datan etäkopiointi, vaikka lähde- ja kohdepäässä käytettäisiin eri valmistajien levyjärjestelmiä.

5.6.4 Toipumistavoitteet tallennusjärjestelmän kannalta

Etäkopiointia käytettäessä on mahdollista toteuttaa vaativimmillaan ratkaisu, jonka toipumispistetavoite on nolla tai lähes nolla riippuen siitä käytetäänkö synkronista vai asynkronista etäkopiointia ja mikä on asynkronisen etäkopioinnin aikasykli. Toipumisaikatavoitteen osalta ratkaisevaa on, miten levykapasiteetin käyttö on toteutettu, ja mikä on palvelinkapasiteetin toipumisen valmiusaste. Mikäli levykapasiteetti on aktiivi/passiivi – tyyppisesti käytössä, voi kestää useita minuutteja ennen kuin järjestelmät ovat käytettävissä, sillä vikatilanteessa toisessa konesalissa olevat etäkopioidut levyosiot pitää ensin osoittaa toisessa konesalissa oleville palvelimille, asettaa luku- ja kirjoitustilaan ja palvelimien tulee käynnistää palvelut uudelleen. Mikäli levykapasiteetti voidaan maantieteellisesti hajauttaa kahden konesalin välille siten, että levyosiot näkyvät molemmissa konesaleissa oleville palvelimille, saadaan palvelinpalveluiden toipumisaikaa nopeutettua. Mitä automaattisemmin työkuorman siirto ja palveluiden käynnistys voidaan tehdä, sitä lyhyempi on käyttökatko, ja sitä vaativampi toipumisaikatavoite voidaan saavuttaa. Parhaimmillaan voidaan toteuttaa ratkaisu, jonka toipumisaikatavoite on nolla tai lähes nolla.

5.7 Palvelimet

Katastrofinkestävässä toteutuksessa palvelimet hajautetaan maantieteellisesti eri konesaleihin. Palvelimien hajauttamisessa voidaan käyttää sekä fyysisiä palvelimia että hyödyntää palvelinvirtualisointia. Esimerkiksi aktiivi/passiivi-konfiguraatiossa primäärissä konesalissa olevat palvelimet voivat olla fyysisiä ja sekundäärissä konesalissa olevat varapalvelimet virtuaalisia, jolloin ei tarvita investointeja tai palveluhankintoja fyysiseen palvelinkapasiteettiin, jota ei mahdollisesti tarvita koskaan. Toisaalta varalla olevia fyysisiä tai virtuaalisia palvelimia voidaan käyttää normaalitilanteessa testi-, kehitys- ja koulutuskäyttöön, jolloin ne saadaan hyötykäyttöön.

Palvelimien toipumisen valmiutta voidaan kuvata termeillä: kylmä palvelin, lämmin palvelin ja kuuma palvelin. Järjestelmän toipumisaikatavoite määrittelee, riittääkö kylmä palvelin vai tarvitaanko kuuma palvelin. Kylmä palvelin on valmiina toisessa konesalissa, mutta se ei ole aktiivisesti käytössä ja siinä ei ole sähkövirta päällä. Kylmä palvelin on tyypillisesti varalla oleva fyysinen räkki- tai korttipalvelin. Kylmän palvelimen käyttöönoton nopeuttamiseksi voidaan käyttää asennusohjelmistoja, joilla käyttöjärjestelmä- ja varusohjelmistojen asennus saadaan automatisoitua.

Lämmin palvelin on valmiina toisessa konesalissa, siinä on virrat päällä ja tiedot päivitetään säännöllisin väliajoin. Haasteena on lämpimän palvelimen pitäminen ajan tasalla, jos palvelimia on paljon eikä käytössä ole teknologiaa päivitysten automatisoimiseksi. Lisäksi viimeisimmät tiedot saatetaan joutua palauttamaan varmuuskopioilta. Markkinoilla on olemassa teknologioita, joilla lämpimien palvelimien käyttöönotto voidaan automatisoida ja lämpimät palvelimet saavat käynnistyessään vikaantuneen palvelimen identiteetin. Edellytyksenä on, että palvelimien käynnistyslevyosio on yhteiskäyttöisessä levyjärjestelmässä, jolloin varapalvelin voidaan käynnistää vikaantuneen palvelimen käynnistyslevyosiolta.

Kuuma palvelin on valmiina toisessa konesalissa, se on aktiivisesti käytössä ja sen tiedot ovat ajan tasalla. Esimerkkinä kuumista palvelimista ovat palvelinklusterit, jonka jäsenet hajautetaan maantieteellisesti eri konesaleihin. Mikäli toipumisaikatavoitteet ovat vaativat, tarvitaan kuumiin palvelimiin perustuva ratkaisu.

5.8 Palvelinklusterit

Maantieteellisesti hajautetuilla palvelinklustereilla voidaan toteuttaa vaativimmat palvelinpalveluita koskevat toipumisaikatavoitteet. Klusteriteknologiasta riippuen klusterin jäsenet voivat olla aktiivisia eli niissä kaikissa ajetaan työkuormaa tai osa jäsenistä voi olla passiivisia, jolloin ne odottavat, että vikatilanteessa työkuorma siirtyy niiden hoidettavaksi. Data pidetään ajan tasalla etäkopioimalla data synkronisesti tai asynkronisesti. Esimerkkejä yleisimmistä klusteriteknologioista, joilla voidaan toteuttaa maantieteellisesti hajautettuja palvelinklustereita, ovat HP-UX Serviceguard, IBM AIX PowerHA, Microsoft Windows Server Failover Clustering, RedHat Enterprise Linux Clustering, SUSE Linux Enterprise High Avai-

lability sekä Symantecin Veritas Cluster Server, joka tukee useita eri käyttöjärjestelmiä.

Palvelinklustereiden jäsenet liitetään toisiinsa erillisellä tietoliikenneyhteydellä, jota kutsutaan heartbeat-yhteydeksi. Heartbeat-yhteyden välityksellä klusterin jäsenet kommunikoivat tilatietojaan muille klusterin jäsenille. Palvelinklusterin sisäisen tilatietojen välittäminen on erittäin tärkeää klusterin toiminnan kannalta, sillä mikäli heartbeat-yhteys katkeaisi, niin klusterin jäsenet luulisivat olevansa ainoita toimintakykyisiä klusterin jäseniä ja jatkaisivat edelleen klusterin palveluiden tarjoamista itsenäisesti, josta aiheutuisi klusterin joutuminen epästabiiliin tilaan. Ongelman ehkäisemiseksi heartbeat-yhteydet tulee aina olla kahdennettuja. Heartbeat-yhteyden kahdennuksen lisäksi klusteriteknologioiden toimittajat ovat kehittäneet erilaisia metodeja, joilla pyritään varmistamaan klusterin toimintakykyisyys ja asettamaan automaattisesti osa klusterin jäsenistä offline-tilaan, mikäli klusterin välinen tilatietojen välitys katkeaisi. Metodeista käytetään yleisesti englanninkielisiä termejä cluster witness tai cluster quorum. Klusteriteknologiasta riippuen cluster witness tai quorum voivat olla erillinen levyosio, tiedostojako tai palvelin. Yhteistä kaikille metodeille on, että jokaisella klusterin jäsenellä ja cluster witnessillä tai quorumilla on yksi ääni. Klusteri on toimintakykyinen, mikäli klusterin toiminnassa olevat jäsenet ja cluster witness tai quorum muodostavat yhteenlaskettuna äänienemmistön.

5.8.1 Maantieteellisesti hajautetun klusterin toiminnan varmistaminen

Maantieteellisesti hajautetuissa palvelinklustereissa on entistä tärkeämpää pystyä tunnistamaan klusterin toimintakelpoisuus, mikäli klusterin jäsenten välinen yhteys katkeaa. Klusteriteknologiasta riippuen maantieteellisesti hajautettu klusteri voidaan toteuttaa siten, että toinen konesali ja siellä olevat klusterin jäsenet määritellään ensisijaisiksi tai niillä on äänienemmistö ja vastaavasti toisessa konesalissa olevat klusterin jäsenet määritellään toissijaisiksi tai niillä on äänivähemmistö. Edellä mainituilla määrityksillä estetään klusterin joutuminen epästabiiliin tilaan, mikäli yhteys konesalien välillä katkeaa. Jos yhteyden katkeaminen johtuu ainoastaan heartbeat-yhteyden katkeamisesta, niin ensisijaiset tai äänienemmistön omaavat klusterin jäsenet jatkavat toimintaansa ja toissijaiset tai äänivähemmistön omaavat klusterin jäsenet menevät automaattisesti offline-tilaan. Jos yhteyden katkeaminen johtuu toissijaisten tai äänivähemmistön omaavan klusterin jäsenten muuttumisesta toimintakyvyttömiksi, siirtyy työkuorma automaattisesti ensisijaiseen konesaliin tai äänienemmistön omaaville klusterin jäsenille. Jos sen sijaan yhteyden katkeaminen johtuu ensisijaisten tai äänienemmistön omaavien klusterin jäsenten toimintakyvyttömyydestä, niin koko klusterin toiminta katkeaa, sillä ensisijaisuuteen tai äänienemmistöön perustuvan säännön mukaan toissijaiset tai äänivähemmistön omaavat klusterin jäsenet menevät automaattisesti offline-tilaan. Tällaisissa tapauksissa tarvitaan järjestelmänhallinnan toimenpiteitä, joilla toissijaiset tai äänivähemmistön omaavat klusterin jäsenet määritellä aktiivisiksi. Manuaalisesti tehtävät toimenpiteet lisäävät klusterin toipumisaikaa.

Edellä kuvatun ongelman ratkaisemiseksi ja maantieteellisesti hajautetun klusterin käytettävyyden varmistamiseksi klusteriteknologioiden valmistajat suosittelevat, että cluster witness tai cluster quorum sijoitetaan maantieteellisesti kolmanteen paikkaan, johon molemmista hajautetuista konesaleista on tietoliikenneyhteydet. Cluster witness tai cluster quorum –toiminnon avulla klusterin maantieteellisesti hajautetut jäsenet voivat päätellä, onko klusteri toimintakykyinen, pitääkö toisessa konesalissa olevat klusterin jäsenet asettaa offline-tilaan vai onko kyseessä aito vikatilanne, joka edellyttää työkuorman siirtämistä. Palvelinklusterin toipumisen automaattisuus edellyttää, että myös palvelinklusterin käyttämän levykapasiteetin toipuminen voidaan automatisoida.

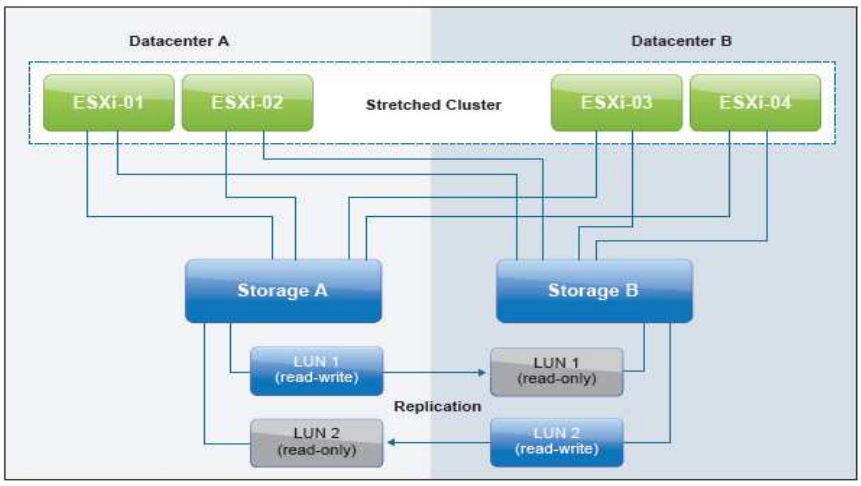
5.8.2 Virtuaalipalvelimet

Palvelinvirtualisointi edesauttaa katastrofinkestävien palvelinjärjestelmien toteuttamista, sillä virtuaalipalvelimia voidaan siirtää joustavasti virtualisointialustojen välillä, jotka voivat sijaita maantieteellisesti eri konesaleissa. Palvelinvirtualisointiin on olemassa useita eri teknologioita palvelimien suoritinarkkitehtuurista riippuen. Esimerkiksi IBM PowerPC-suoritinarkkitehtuuriin perustuvien käyttöjärjestelmien virtualisointiteknologia on IBM PowerVM ja Oracle SPARC-suoritinarkkitehtuurin perustuvien käyttöjärjestelmien Oracle VM for SPARC. Intel x86-arkkitehtuuriin perustuville palvelimille on olemassa useita eri virtualisointiteknologioita, joista kaksi yleisintä ovat VMware vSphere ja Microsoft Hyper-V, joita tässä opinnäytetyössä tarkastellaan lähemmin.

VMware-ympäristöissä katastrofinkestävät virtuaalipalvelinympäristöt voidaan toteuttaa usealla eri tavalla riippuen käyttötarkoituksesta. Yksinkertaisin tapa suojata virtuaalipalvelimia on käyttää vSphere Replication –toimintoa, jolla voidaan replikoida virtuaalipalvelimia VMware ESXi-virtualisointipalvelimilta maantieteellisesti toisessa paikassa oleville VMware ESXi-palvelimille. Ensimmäisellä kerralla siirretään kaikki tiedot ja sen jälkeen replikoidaan vain muuttuneet tietolohkot. vSphere Replication sopinee pienille organisaatioille, joiden toipumistavoitteet eivät edellytä automaattisesti toipumista ja toipumispistetavoitteet sallivat osittaisen tietojen menetyksen, koska replikointi voidaan määritellä tapahtuvaksi minimissään 15 minuutin välein ja maksimissaan 24 tunnin välein. Toipumispistetavoite, RPO, on näin ollen 15 minuutista 24 tuntiin.

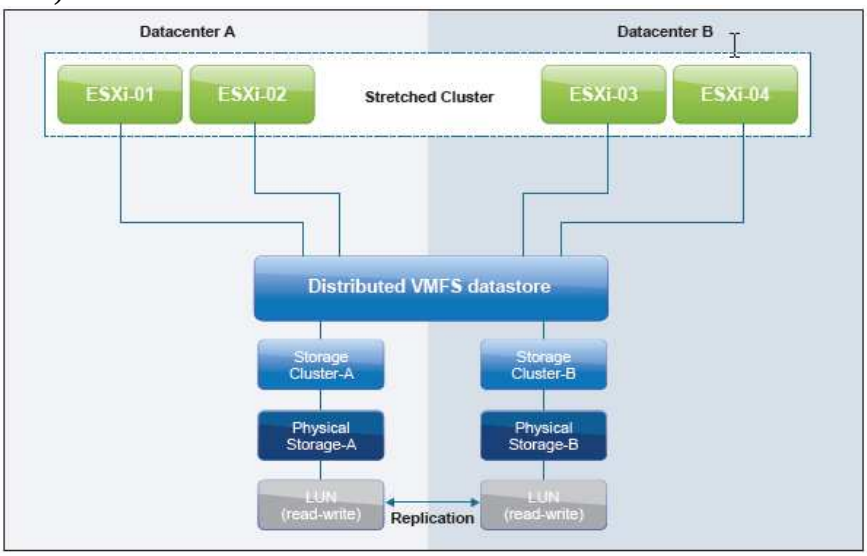
Toinen tapa on hajauttaa erilliset VMware ESXi-palvelimien muodostamat VMware HA-palvelinklusterit maantieteellisesti eri konesaleihin, etäkopioida tiedot konesalien välillä ja automatisoida virtuaalipalvelimien siirtyminen VMware HA-klusterilta toiselle VMware Site Recovery Manager (SRM) -ohjelmiston avulla. Siirtyminen ei vikatilanteessa tapahdu täysin automaattisesti, vaan järjestelmän hallinnasta vastaavan tulee käynnistää SRM-hallintakonsolilta site failover -toiminto, jolloin SRM siirtää virtuaalipalvelimet toisessa konesalissa olevalle VMware HA-palvelinklusterille ja käynnistää ne ennalta määritetyssä järjestyksessä. VMware SRM:n avulla voidaan myös testata site failover-toiminnallisuutta tuotantoa häiritsemättä.

Kolmas tapa on hajauttaa VMware HA-palvelinklusteri maantieteellisesti kahteen eri konesaliin. VMware julkisti keväällä 2012 uuden tuetun arkkitehtuurin nimeltään vSphere Metro Storage Cluster, vMSC. vMSC perustuu maantieteellisesti hajautettuun VMware HA-palvelinklusteriin ja levyjärjestelmien etäkopiointiin. vMSC tukee VMware HA-palvelinklusterin ominaisuuksia, kuten kuormanjakoa ja työkuormien siirtoa VMware ESXi-palvelimien välillä, mutta erona tavalliseen VMware HA-palvelinklusteriin on, että ESXi-palvelimet voivat olla maantieteellisesti kahdessa eri paikassa. vMSC-arkkitehtuurilla voidaan toteuttaa maantieteellisesti kahteen konesaliin hajautettujen ESXi-palvelimien aktiivi/aktiivi-käyttö. vMSC-konfiguraatiot jaetaan kahteen eri konfiguraatioluokkaan: uniform host access-konfiguraatiot ja non-uniform host access-konfiguraatiot. Uniform host access-konfiguraatiossa molemmissa konesaleissa olevat ESXi-palvelimet voivat käyttää molemmissa konesaleissa olevia levyjärjestelmiä ja levyosioita (kuva 4).



Kuva 4. vMSC – uniform host access (VMware 2012)

Non-uniform host access-konfiguraatiossa ESXi-palvelimet käyttävät ensisijaisesti samassa konesalissa olevaa levyjärjestelmää ja etäkopioitua levyosiota, joka on luku- ja kirjoituskäytössä molemmista konesaleista (kuva 5).



Kuva 5. vMSC – non-uniform host access (VMware 2012)

Eri levyjärjestelmävalmistajat voivat hyväksyttää omat teknologiaratkaisunsa, joilla voidaan toteuttaa vMSC-arkkitehtuurin mukaiset konfiguraatiot, ja saada siten omat järjestelmänsä VMwaren HCL-listalle (HCL = Hardware Compability List). Opinnäytetyötä tehtäessä HCL-listalla olivat seuraavat levyjärjestelmäratkaisut: EMC VPLEX, HP LeftHand Multi-Site, IBM SVC ja NetApp MetroCluster.

Microsoft Windows Server 2008 Hyper-V-ympäristön maantieteellinen hajauttaminen perustuu Microsoftin Windows Server Failover Clustering-palvelinklusterointiin. Hyper-V -palvelimista muodostetaan Windows-palvelinklusteri, jonka jäsenet hajautetaan eri konesaleihin ja data etäkopioidaan. Syksyllä 2012 julkistettu Microsoft Windows Server 2012 toi lisää vaihtoehtoja Hyper-V –ympäristön maantieteelliseen hajauttamiseen, sillä Failover Clustering –toiminnallisuuden lisäksi Windows Server 2012 Hyper-V sisältää Hyper-V Replica –toiminnon. Hyper-V Replican avulla voidaan virtuaalipalvelimet replikoida maantieteellisesti toisessa paikassa olevalle Hyper-V –palvelinklusterille tai yksittäiseen Hyper-V –palvelimeen. Tiedonsiirto tapahtuu asynkronisesti, ensimmäisellä kerralla siirretään kaikki virtuaalipalvelimen tiedot ja sen jälkeen muutokset kirjoitetaan erilliseen lokitiedostoon, josta virtuaalipalvelimen kopio eli replika päivittää tiedot. Samoin kuin VMwaren vSphere Replication, Hyper-V Replica sopinee pienemmille organisaatioille, joiden toipumisaikatavoitteet eivät edellytä esimerkiksi tiedon synkronista etäkopiointia ja automaattista toipumista.

5.9 Tietokannat

Katastrofinkestävässä toteutuksessa tietokannat eli käytännössä tietokantapalvelimet hajautetaan maantieteellisesti eri konesaleihin. Tietokantapalvelimien hajauttamiseksi voidaan käyttää käyttöjärjestelmätoimittajan tai kolmannen osapuolen palvelinklusterointia ja lisäksi eri tietokantatuotteet sisältävät omia toiminnallisuuksia katastrofikestävyyden toteuttamiseksi. Esimerkiksi Microsoft SQL Server-tietokantapalvelimen Log Shipping –toiminnolla tietokannan transaktioloki voidaan siirtää tuotantopalvelimelta säännöllisin väliajoin maantieteellisesti toisessa paikassa olevalle SQL Server-palvelimelle ja päivittää tietokantakopioon. Tällöin voidaan puhua niin sanotusta lämpimästä tietokantapalvelimesta.

Kuuma tietokantapalvelin -toteutuksessa voidaan käyttää tietokantatuotteen omaa teknologiaa tietokantojen etäkopiointiin ja tietokantapalvelimien klusterointiin. Esimerkkinä tietokantatuotteen omalla replikointiteknologialla toteutettavasta tietokannan kopioinnista ovat Microsoftin SQL Server Data Mirroring ja Oracle Data Guard. Esimerkkinä tietokantatuotteen omasta klusteriteknologiasta on Oracle Real Application Clusters, RAC, joka on kahden tai useamman Oracle-tietokantapalvelimen muodostama klusteri, joka voi tuottaa tietokantapalvelua samalle tietokannalle. Hajauttamalla RAC-klusterin jäsenet maantieteellisesti eri konesaleihin voidaan toteuttaa erittäin vikasietoinen aktiivi/aktiivi -tietokantaklusteri, jonka suorituskykyä voidaan kasvattaa lisäämällä tietokantapalvelimia RAC-klusteriin.

5.10 Sovellukset

Organisaation tietojenkäsittelyn kannalta tärkein osuus palveluketjussa on sovellus, jota käytetään organisaation jonkin toiminnon suorittamiseksi. Sovellus voi liittyä organisaation ydintoimintaan tai se voi olla toimintaa tukeva. Tärkeintä on tunnistaa sovelluksen merkitys organisaation toiminnan jatkuvuudelle ja toteuttaa varmistus- ja suojaustoimenpiteet sen mukaisesti. Maantieteellinen hajauttaminen voidaan periaatteessa tehdä sovellusriippumattomasti hyödyntäen edellä mainittuja palvelin- ja tallennuskapasiteetin hajauttamismahdollisuuksia. Sovellusarkkitehtuurin suunnitteluvaiheessa kannattaa kuitenkin ottaa huomioon mahdolliset hajauttamistarpeet ja huomioida esimerkiksi kuormantasauksen käyttömahdollisuus ja erityisesti tietokantapohjaisissa sovelluksissa transaktioiden eheyden varmistaminen ja sovelluksen toipuminen.

5.11 Pilvipalvelut

Pilvipalvelut jaetaan kolmeen palvelukokonaisuuteen IaaS-, PaaS- ja SaaS-palveluihin. Riippumatta siitä, mitä pilvipalvelua ollaan hankkimassa, tulee organisaation huomioida palvelun tärkeys organisaation toiminnan jatkuvuudelle, ja mitkä ovat palvelun toipumistavoitteet. Pilvipalveluita hankkivien organisaatioiden kannattaa aina selvittää, täyttävätkö pilvipalvelutoimittajilta hankittavat IaaS-, PaaS- ja SaaS-palvelut organisaation toipumisvaatimukset ja ovatko palvelut katastrofinkestäviä.

Suurimmat julkiset pilvipalvelut, joista esimerkkinä Amazon, Google ja Microsoft Azure, ovat perusarkkitehtuuriltaan hajautettuja eli palvelut tuotetaan useista maantieteellisesti hajautetuista konesaleista eikä käyttäjä välttämättä tiedä kuin maanosan tarkkuudella, mistä hänen käyttämänsä palvelut tuotetaan ja missä data sijaitsee. Markkinoille on tullut myös toimijoita, jotka ovat erikoistuneet tarjoamaan pilvipalvelukapasiteettia katastrofista toipumiseen. Toteutustapana voi olla esimerkiksi, että organisaation tuotantojärjestelmät ovat organisaation paikallisessa konesalissa olevilla palvelimilla, ja varapalvelin- ja –tallennuskapasiteetti on pilvipalvelussa, jonne tiedot kopioidaan säännöllisesti asynkronisesti.

Pilvipalveluiden hyödyntäminen ICT-järjestelmien maantieteellisessä hajauttamisessa voi olla taloudellisesti houkutteleva vaihtoehto verrattuna omaan tai palveluna hankittuun konesali-, palvelin- ja tallennuskapasiteettiin, mutta kustannusten lisäksi tulee ottaa huomioon erityisesti tietoliikenteeseen ja tietojen hallintaan liittyvät asiat sekä pilvipalvelutoimittajan luotettavuus: markkinat elävät vielä voimakkaasti, toimijoita on paljon, uusia toimijoita tulee markkinoille, ja osa poistuu markkinoilta hyvinkin pian. Pilvipalveluiden kapasiteettitarjonta asettaa myös omat rajoituksensa, kapasiteettia on saatavissa pääsääntöisesti vain virtuaalisena ja tallennuskapasiteettivaihtoehdot voivat olla rajalliset.

6 CASE PIRKANMAAN SAIRAANHOITOPIIRIN POTILASTIETOVARASTO

Kuntien vastuulle on lainsäädännöllä siirretty sosiaali- ja terveyshuollon palveluiden järjestäminen. Terveydenhuollon osalta kuntien vastuulle kuuluu sekä perusterveydenhoito että erikoissairaanhoito. Erikoissairaanhoidosta vastaa sairaanhoitopiirin kuntayhtymät ja jokaisen kunnan on kuuluttava johonkin sairaanhoitopiiriin. Toimiva terveydenhuolto on hyvinvointiyhteiskunnan kulmakiviä ja sen toiminta pitää pystyä turvaamaan myös poikkeustilanteissa. Käytännön esimerkkinä katastrofinkestävän ICT-järjestelmän toteuttamisesta on Pirkanmaan sairaanhoitopiirin hankkima potilastietovarasto, joka perustuu EMC:n ohjelmisto- ja laitteistoteknologiaan ja Fujitsun SaaS-palveluun.

6.1 Pirkanmaan sairaanhoitopiiri

Pirkanmaan sairaanhoitopiiri on 22 kunnan muodostama kuntayhtymä, jonka tehtävänä on tuottaa terveyttä ja toimintakykyä edistäviä terveydenhuollon palveluja sekä luoda edellytyksiä tätä tukevalle tieteelliselle tutkimukselle ja koulutukselle. Vuonna 2011 Pirkanmaan sairaanhoitopiirissä hoidettiin 179 565 eri potilasta, joista erikoissairaanhoidossa 147 814. Sairaanhoitopiirin sairaaloissa oli yhteensä 1 288 sairaansijaa ja henkilöstöä oli vuoden aikana keskimäärin 7 118. Sairaanhoitopiirikonserniin kuuluu lisäksi Kuvantamiskeskus- ja apteekkiliikelaitos sekä osakeyhtiömuotoiset Coxa Oy, Fimlab Laboratoriot Oy ja Tays Sydänkeskus Oy. Sairaanhoitopiirin tunnuslause ”Elämän tähden” heijastaa sairaanhoitopiirin strategiaa, joka perustuu seuraaviin eettisiin periaatteisiin: hyvä hoito, ihmisen kunnioittaminen, osaamisen arvostaminen ja yhteiskuntavastuullisuus (PSHP-vuosikertomus 2011.)

Sairaanhoitopiirin yhtymähallintoon kuuluva tietohallintoyksikkö ohjaa, suunnittelee ja valvoo tiedon, tietojärjestelmien ja tietotekniikan hyödyntämistä Pirkanmaan sairaanhoitopiirissä ja hankkii sairaanhoitopiirin yhteiset tietojärjestelmä- ja tietotekniikkapalvelut (PSHP-tietohallinto 2012). Sairaanhoitopiirin tietohallintopäällikön, Tuomo Mujusen (haastattelu 3.10.2012) mukaan Pirkanmaan sairaanhoitopiirissä on käytössä hajautettu tietohallintomalli, jossa konsernin liikelaitos ja osakeyhtiöt sekä toimialueet käyttävät itsenäistä päätäntävaltaa omaan erikoisalaansa kuuluvien ICT-ratkaisuiden kuten järjestelmien, ohjelmistojen sekä työasemien hankinnassa sekä muissa elinkaaren vaiheissa.

6.2 Asiakkaan järjestelmähankkeen taustaa

Vuonna 2009 käynnistettiin Kuvantamis- ja apteekkiliikelaitoksessa PACS-järjestelmän uusimiseen liittyvä selvityshanke. Käytössä oli kaksi erillistä PACS-järjestelmää, joista toinen oli käytössä sairaanhoitopiirissä ja toinen alueen kunnissa. Lisäksi Tampereen kaupungilla oli oma PACS-

järjestelmä. Hankkeessa selvitettiin mahdollisuutta yhdistää erilliset PACS-järjestelmät ja tultiin siihen johtopäätökseen, että vanhoja järjestelmiä ei kannata korvata perinteisellä PACS-järjestelmällä, vaan pyrkiä toimittajariippumattomaan yleisarkistoon, jota eri PACS-järjestelmätoimittajat voisivat hyödyntää ja jossa tiedot olisivat paremmin yhteisesti käytettävissä. Selvityksen jälkeen Tampereen kaupungin kanssa sovittiin, että kaupunki jatkaa toistaiseksi oman PACS-järjestelmän käyttöä, mutta sairaanhoitopiirissä jatkettiin kahden erillisen PACS-järjestelmän uudistamishanketta. (Mujunen, haastattelu 3.10.2012.)

Uudistamishankkeen tavoitteena oli toteuttaa mahdollisimman avoin, nykystandardeja tukeva järjestelmä. Silloiselta PACS-järjestelmätoimittajalta ei löytynyt laitteisto- ja ohjelmistoratkaisua, joka olisi vastannut kaikkia tavoitteita ja samaan aikaan oli myös tarve uusia kuvantamisaineiston tallennuskapasiteettia. Siitä syystä päädyttiin hankkimaan uusi, avointa rajapintaa tukeva PACS-järjestelmä sekä avointa rajapintaa tukeva potilastietovarasto, joka olisi myös muiden terveydenhuollon järjestelmien käytettävissä. (Mujunen, haastattelu 3.10.2012)

6.3 Järjestelmälle asetut yleiset vaatimukset

Avoimuuden lisäksi hankittavan potilastietovaraston tuli olla kapasiteetin osalta skaalautuva, tietosisällön tukea muutakin kuin kuvantamistiedon tallentamista ja tietojen piti olla paremmin eri järjestelmien yhteisesti hyödynnettävissä integraatiokerroksen avulla. Tärkeätä oli myös huomioida lainsäädäntö, muun muassa terveydenhuoltolain, vaatimukset hankinnan vaatimusmäärittelyissä. (Mujunen, haastattelu 3.10.2012.)

Terveydenhuoltolaissa asetetaan sairaanhoitopiirin kuntayhtymille velvoite päättää yhteistyössä alueen kuntien kanssa varautumisesta suuronnettomuuksiin ja terveydenhuollon erityistilanteisiin (Terveydenhuoltolaki 30.12.2010/1326, 38 §). Varautumisvelvoite vaikuttaa siten myös terveydenhuoltojärjestelmien toiminnan varmistamiseen.

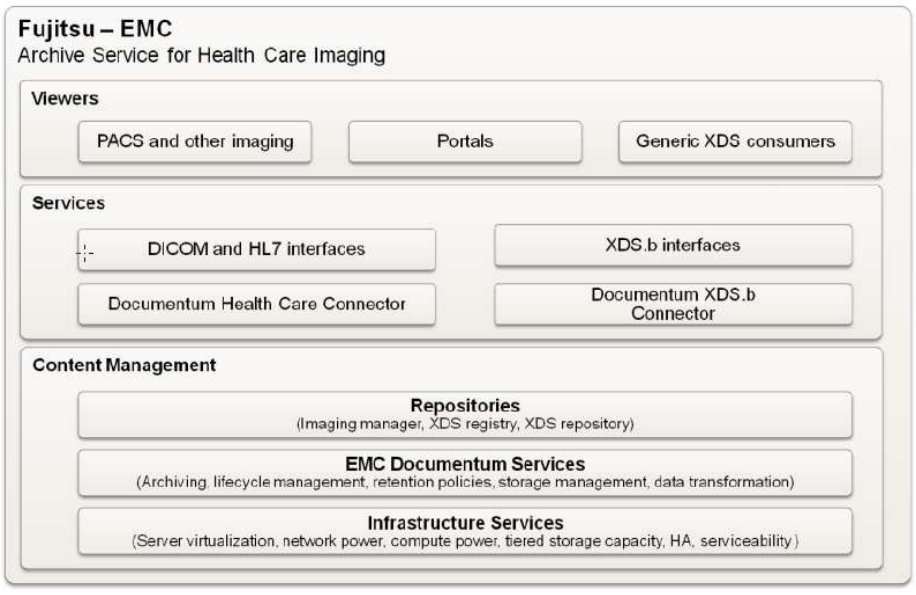
Potilasasiakirjojen säilyttämistä koskevassa asetuksessa määrätään, että potilasasiakirjat tulee laatia ja säilyttää sellaisia välineitä ja menetelmiä käyttäen, että asiakirjoihin sisältyvien tietojen eheys ja käytettävyys voidaan turvata tietojen säilytysaikana (STM 298/2009, 3 §). Asetuksen 298/2009 liitteessä määrätään pysyvästi säilytettävistä potilasasiakirjoista sekä määräajan säilytettävistä asiakirjoista. Julkisessa terveydenhuollossa pysyvästi säilytettäviä potilastietoja ovat kaikki 18. ja 28. päivinä syntyneiden potilasasiakirjat. Määräajan säilytettävissä potilasasiakirjoissa yleisin säilytysaika on 12 vuotta potilaan kuolemasta tai 120 vuotta potilaan syntymästä, jos kuolinaika ei ole tiedossa. Asetuksessa 298/2009 määrätään myös, että potilasasiakirjojen lisäksi sähköisten potilastietojen käyttöön ja luovutukseen liittyvät lokitiedot tulee säilyttää eheinä ja muuttumattomina vähintään 12 vuotta niiden syntymisestä (STM 298/2009, 24 §). Asiakastietojen sähköisestä käsittelystä määrätään, että asiakastietojen tulee säilyä eheinä ja muuttumattomina koko niiden säilytysajan. (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä 159/2007,4 §).

6.4 Järjestelmän katastrofinkestävyyden vaatimukset

Järjestelmän toipumistavoitteet käytiin läpi yhdessä liiketoiminnan kanssa ja sen pohjalta asetettiin vaatimukset järjestelmän korkealle käytettävyydelle, katastrofinkestävyydelle. Lähtökohtaisesti järjestelmän tuli olla maantieteellisesti hajautettu, ja sen lisäksi asetettiin vaatimukseksi, että maantieteellisesti hajautetun järjestelmän toinen puoli piti olla sairaalan kampusalueella sijaitsevassa konesalissa, jotta järjestelmän käyttö ei olisi kokonaan riippuvainen ulkopuolisista tietoliikenneyhteyksistä. (Mujunen, haastattelu 3.10.2012.)

6.5 Valittu järjestelmäratkaisu

Uudeksi potilastietovarastojärjestelmäksi asiakas valitsi EMC:n Open Systems Architecture (OSA) Solution for Healthcare –järjestelmän. EMC OSA-ratkaisun ytimenä on EMC:n Documentum-sisällönhallintajärjestelmä, joka on sovitettu terveydenhuollon tarpeisiin. Documentum-järjestelmä sisältää toiminnallisuudet tallennettujen tietojen elinkaaren hallintaan, ja tietojen ja metadatan tallentamisessa tuetaan toimittajariippumattomia, terveydenhuoltoalan standardoituja määrityksiä, kuten IHEn XDS-integraatioprofiilit ja DICOM- ja HL7-standardit. Palvelun toimittajaksi asiakas valitsi Fujitsun, joka tuottaa palvelun SaaS-tyyppisesti kokonaispalveluna sisältäen EMC OSA -järjestelmän ja tarvittavan palvelin- ja tallennuskapasiteetin (kuva 6).

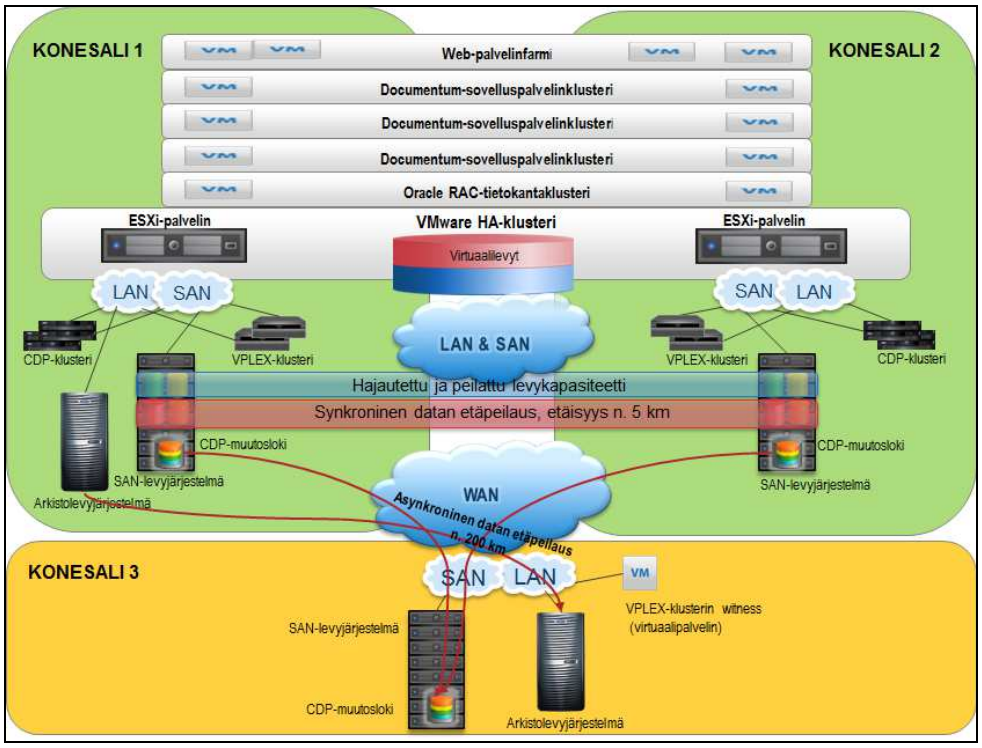


Kuva 6. EMC OSA-järjestelmän komponentit (EMC OSA 2011)

6.6 Tekninen toteutus

Hankkeessa pääsuunnittelijana toimineen Teemu Sunan (haastattelu 9.10.2012) mukaan katastrofinkestävän ICT-järjestelmän toteuttamisessa on tärkeää huomioida, että sovelluskomponentit ja ICT-infrakomponentit toimivat hyvin yhdessä, jolloin järjestelmän toimivuus voidaan varmistaa

myös poikkeustilanteissa. OSA-järjestelmän ja ICT-infrastruktuurin suunnittelu tehtiin yhteistyössä alihankkijana toimineen EMC:n kanssa lähtökohtana asiakkaan ja lainsäädännön vaatimukset toiminnallisuudelle, asiakirjojen säilyttämiselle, käytettävyydelle ja toipumiselle. Suunnittelun tuloksena päädyttiin kolmen konesalin ratkaisuun (kuva 7).



Kuva 7. Katastrofinkestävän potilastietovaraston ICT-infrastruktuurin periaatekuva

Järjestelmän tekninen ratkaisu täyttää toipumispistetavoitteen, joka on nolla tai lähes nolla, koska synkronisen etäkopioinnin ansiosta datan hävikki on lähes olematon. Lisäksi jatkuvalla tiedon suojauksella voidaan suojautua tietosisällön loogiselta rikkoontumiselta ja palata tarvittaessa tilanteeseen, jolloin tietosisältö oli ehyttä. Tekninen toteutus täyttää myös toipumisaikatavoitteen, joka on lähes nolla. Vaativiin toipumisaikatavoitteisiin päästään vain aktiivi/aktiivi –toteutuksella, jossa työkuorman ja tietojenkäsittelyn siirto konesalista toiseen voidaan tehdä täysin automaattisesti.

6.6.1 Konesali

Järjestelmä on sijoitettu kolmeen maantieteellisesti eri paikassa sijaitsevaan konesaliin, joista kaksi on aktiivi/aktiivi–käytössä ja kolmas toimii potilastietovaraston päivittäisen käytön kannalta passiivisena konesalina. Aktiivi/aktiivi–konesalien välinen maantieteellinen etäisyys on noin 5 kilometriä ja aktiivisten ja passiivisen konesalin välinen etäisyys on noin 200 kilometriä.

6.6.2 Tietoliikenne

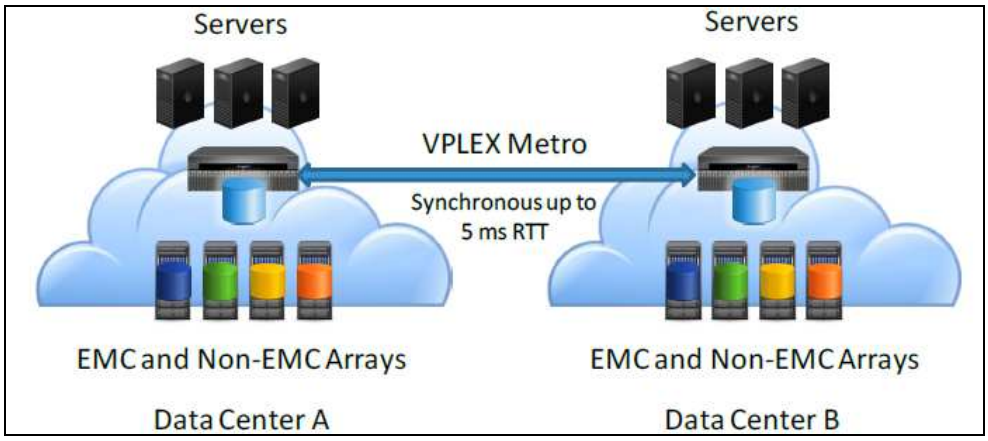
Aktiivi/aktiivi-konesalien välillä on kahdennetut, eri kaapelireittiä kulkevat valokuituyhteydet, jotka ovat CWDM-teknologialla jaettu eri aallonpi-

tuuskanaviin. SAN-levyjärjestelmien FCP-tietoliikenneyhteyksille on varattu omat aallonpituuskanavat, samoin kuin ethernet-verkon TCP/IP-tietoliikenneyhteyksille. Asiakkaan verkko ja aktiiviset konesalit ovat liitetty MPLS-verkkoon, jossa käytetään dynaamista BGP-reititystä. Vikatilanteessa tietoliikenneyhteydet reititetään automaattisesti toiseen konesaliin. Molemmista aktiivisista konesaleista on erilliset tietoliikenneyhteydet passiiviseen konesaliin. (Heinonen, haastattelu 31.10.2012.)

6.6.3 Levykapasiteetti

Potilastietovaraston aktiivisessa käytössä oleva levykapasiteetti perustuu kahteen konesaliin sijoitettuun EMC VMAX-levyjärjestelmään ja EMC VPLEX-virtualisointiteknologiaan (Tiihonen, haastattelu 16.10.2012). EMC:n vuonna 2010 julkistama VPLEX-virtualisointiteknologia mahdollistaa luku- ja kirjoituskäytön loogisesti samalle levyosiolle kahdesta maantieteellisesti eri paikasta, jolloin sen avulla voidaan toteuttaa kahden konesalin aktiivi/aktiivi-käyttö ja nopea toipuminen. VPLEX perustuu palvelimien ja SAN-levyjärjestelmien väliin liitettäviin erillisiin laitteisiin, engl. appliance. VPLEX virtualisoi SAN-levyjärjestelmien levykapasiteetin muodostaen virtuaalisen levyosion, joka osoitetaan palvelimille. SAN-levyjärjestelmät voivat olla maantieteellisesti kahdessa eri paikassa ja VPLEX huolehtii datan kahdensuuntaisesta etäkopioinnista. Koska virtualisoitu levyosio näkyy molemmissa konesaleissa oleville palvelimille, on ICT-järjestelmän toipuminen mahdollisissa häiriötilanteissa nopeampaa kuin aktiivi/passiivi-käytössä.

VPLEX tukee EMC:n omien levyjärjestelmien lisäksi myös muiden toimittajien kuten Fujitsun, HP:n ja IBM:n levyjärjestelmiä. VPLEX-teknologiasta on julkistettu kolme eri versiota. VPLEX Local on tarkoitettu paikalliseen yhden konesalin käyttöön, VPLEX Metro kahden konesalin välille, kun synkroninen etäkopiointi on mahdollista, ja VPLEX Geo kahden konesalin välille, kun tarvitaan asynkronista etäkopiointia. Potilastietovaraston arkkitehtuuri perustuu VPLEX Metroon, koska konesalien välinen etäisyys mahdollistaa synkronisen tiedonsiirron (kuva 8).



Kuva 8. VPLEX Metro (EMC VPLEX 2011)

VPLEX koostuu yhdestä, kahdesta tai neljästä vikasietoisesta niin sanotusta Engine-yksiköstä, jotka muodostavat VPLEX-klusterin. Maantieteellisesti hajautettu VPLEX koostuu kahdesta erillisestä VPLEX-klusterista, jotka ovat liitetty toisiinsa kahdennetulla tietoliikenneyhteydellä, joita käytetään datan etäkopioimiseen. Sen lisäksi VPLEX-klusterien välillä on erillinen kahdennettu tietoliikenneyhteys, jota käytetään hallintaan ja klusterin tilatietojen välittämiseen. Kuten palvelinklustereiden yhteydessä todettiin, niin oikea tilatietojen välittäminen on käytettävyyden ja toipumisen kannalta erittäin tärkeää. Sen varmistamiseksi VPLEX-arkkitehtuuri sisältää VPLEX Witness-toiminnallisuuden. VPLEX Witness on VMware ESXi-palvelimella oleva virtuaalipalvelin, joka liitetään VPLEX-klusterien kanssa samaan hallintaverkkoon ja sijoitetaan maantieteellisesti eri paikkaan kuin VPLEX-klusterit. Potilastietovaraston ICT-arkkitehtuurissa VPLEX Witness on sijoitettu kolmanteen eli passiiviseen konesaliin. VPLEX Witness-toiminnallisuudella varmistetaan automaattinen toipuminen klusterin vikatilanteissa ja tilanteessa, jossa VPLEX-klusterien välinen tilatietojen välitykseen tarkoitettu tietoliikenneyhteys katkeaisi.

Aktiivisen levykapasiteetin lisäksi ratkaisuun sisältyy arkistolevykapasiteetti tietojen pitkäaikaista säilytystä varten. Potilasasiakirjat siirretään Documentum-järjestelmään määriteltyjen säännöstöjen mukaisesti automaattisesti aktiivisesta levykapasiteetista arkistolevykapasiteettiin. Arkistolevykapasiteetti perustuu EMC Centera-levyjärjestelmään, joka takaa tiedon muuttumattomuuden ja täyttää lainsäädännön vaatimukset kertakirjoitteisesta tallennustilasta. Katastrofinkestävyyden varmistamiseksi arkistoitavat tiedot tallennetaan kahteen erilliseen Centera-levyjärjestelmään, joista toinen on toisessa aktiivisessa konesalissa ja toinen 200 kilometrin päässä olevassa passiivisessa konesalissa. Maantieteellisen etäisyyden vuoksi tiedon replikointi tehdään asynkronisesti.

6.6.4 Jatkuva tiedon suojaus

Toimitettuun ratkaisuun sisältyy jatkuva tiedon suojaus toteutettuna EMC RecoverPoint-laitteistolla. Kaikki suojattuihin levyosioihin kohdistuvat kirjoitustapahtumat monistetaan SAN-verkon kytkimessä kahdeksi identtiseksi kirjoitustapahtumaksi, joista toinen kirjoitetaan tuotantolevyosiolle ja toinen siirretään RecoverPoint-laitteistolle. RecoverPoint-laitteisto tallentaa kirjoitustapahtuman CDP-lokitiedostoon, josta se kopioidaan tuotantolevyosion kopiolle. Lisäksi aktiivisissa konesaleissa olevat RecoverPoint-laitteistot replikoivat kirjoitustapahtumat passiivisessa konesalissa olevalle RecoverPoint-laitteistolle, joka vastaavasti tallentaa tiedon ensin CDP-lokiin, josta se kopioidaan passiivisessa konesalissa olevan levyjärjestelmän levyosiolle. (Tiihonen, haastattelu 16.10.2012.) Maantieteellisen etäisyyden vuoksi tiedon replikointi RecoverPoint-laitteistojen välillä tehdään asynkronisesti. Jatkuvan tiedon suojauksen avulla varaudutaan tietosisällön mahdolliseen rikkoontumiseen sekä suojataan tiedot siltä varalta, että katastrofin vaikutukset ulottuisivat molempiin aktiivisiin konesaleihin.

6.6.5 Palvelinkapasiteetti

Palvelinkapasiteetti perustuu palvelinvirtualisointiin ja -klusterointiin, jotka mahdollistavat korkean käytettävyyden lisäksi nopean toipumisen sekä palvelinkapasiteetin lisäämisen kustannustehokkaasti. Palvelinkapasiteetin käyttötapa on aktiivi/aktiivi. Ratkaisu koostuu VMware ESXi-palvelimien muodostamasta VMware HA-palvelinklusterista, joka on hajautettu kahteen konesaliin VMwaren vMSC-arkkitehtuurin mukaisesti. ESXi-palvelimille on osoitettu VPLEX-klusterin kautta virtualisoidut datastore-levyosiot, joille kaikilla ESXi-palvelimilla on luku- ja kirjoitusoikeus. VMware HA-palvelinklusterissa toimivat virtuaalipalvelimet ovat joko jäseninä palvelinklusterissa tai kuormantasausryhmässä korkean käytettävyyden ja nopean toipumisen varmistamiseksi. (Tiihonen, haastattelu 16.10.2012.)

Potilastietovaraston web-palvelimien vikasietoisuus on toteutettu kahdennetulla, laitteistopohjaisella kuormantasauksella ja web-palvelimet on hajautettu tasaisesti eri konesaleissa oleville ESXi-palvelimille. Documentum-sovelluspalvelimet on kahdennettu käyttäen Documentumin omaa ohjelmistopohjaista klusterointia ja hajautettu eri konesaleissa oleville ESXi-palvelimille. Documentum-sovellus käyttää Oracle-tietokantaa ja korkea käytettävyys ja vikasietoisuus on toteutettu Oracle Real Application Clusters (RAC) –teknologialla, joka mahdollistaa tietokannan aktiivi/aktiivi-käytön. Oracle RAC-tietokantaklusterissa olevat tietokantapalvelimet on hajautettu eri konesaleissa oleville ESXi-palvelimille. (Suna, haastattelu 9.10.2012.)

6.7 Käyttöönotto

Uuden järjestelmän käyttöönotto aloitettiin palvelin- ja tallennuslaitteistojen asennuksilla ja konfiguroinneilla vuoden 2011 syksyllä ja aineiston migraatio käynnistyi vuoden 2012 alussa. Tuotantoon siirto tapahtui kesällä 2012. Opinnäytetyötä tehtäessä käyttöönotto on migraatiovaiheessa eli tietoja siirretään vanhan PACS-järjestelmän tallennuslaitteilta uuteen potilastietovarastoon.

Mujusen (haastattelu 3.10.2012) mukaan tavoitteena on saada siirrettyä kuvantamistiedot vanhasta PACS-järjestelmästä potilastietovarastoon vuoden 2012 loppuun mennessä sekä liitettyä ja siirrettyä potilastietovarasto tuotantokäyttöön uuden PACS –järjestelmän yhteyteen. Samoin tavoitteena on saada siirrettyä Tays Sydänkeskus Oy:n kardiologian kuvantamistiedot potilastietovarastoon vuoden 2012 loppuun mennessä. Alueen kuntien PACS-järjestelmä säilyy toistaiseksi käytössä, mutta sen tiedot migratoidaan potilastietovarastoon vuoden 2013 aikana.

6.8 Järjestelmän toimintakriittisyys

PACS-järjestelmä ja potilastietovarasto ovat integroitu toisiinsa ja molemmat ovat kriittisiä toiminnalle. PACS-järjestelmästä kuvat siirretään potilastietovarastoon ja sen lisäksi PACS-järjestelmän levyllä kuvat säily-

tetään noin 30 päivää eli kaikki 30 päivää vanhemmat kuvat haetaan potilastietovarastosta. Potilastietovaraston käytettävyyden merkitys korostuu myös sitä mukaa, kun potilastietovarastoon liitettyjen terveydenhuollon järjestelmien määrä lisääntyy, ja sairaanhoitopiirissä otetaan käyttöön potilastietovaraston yleinen käyttöliittymä, jolloin ei tarvita erillisiä sovelluskohtaisia client-ohjelmistoja. (Mujunen, haastattelu 3.10.2012.)

6.9 Kokemukset ja palaute

Hajautetun ICT-infrastruktuurin käyttöönotto onnistui asiakkaan näkökulmasta hyvin. Varsinaisen potilastietovaraston käyttöönotossa oli teknologian osalta pieniä haasteita, jotka saatiin korjattua. Tietojen migraatio ei ole mennyt asiakkaan näkökulmasta ihan toivotulla tavalla, koska vanhalta PACS-järjestelmätoimittajalta ei ole saatu riittävästi migraatiossa tarvittavaa tietoa, ja uusi toimittaja ei ole toisaalta pystynyt riittävästi vaikuttamaan vanhaan toimittajaan migraation yhteydessä. Uusi toimittaja on kyllläkin aktiivisesti pyrkinyt ratkaisemaan eteen tulleita ongelmia. Vanhan PACS -järjestelmän tietosisältöjen läpikäynti sekä standardointi ja sen yhteydessä tehtävät määrittelyt ovat olleet kaikille osapuolille haasteellisia. (Mujunen, haastattelu 3.10.2012.)

Hankkeen tavoitteiden toteutumista itse potilastietovaraston toiminnallisuuden osalta ei voida tällä hetkellä vielä täysin arvioida, sillä migraatiovaihe on kesken. Tähän mennessä on kuitenkin voitu todeta, että erilaiset tiedostomuodot on saatu tallennettua järjestelmään ja ne ovat käytettävissä. Vaikka toteutetussa ratkaisussa käytettiin varsin uutta VPLEX-teknologiaa, eikä aikaisemmin Suomessa ollut vastaavaa toteutettu, luotti asiakas siihen, että Fujitsu ja EMC suurina järjestelmätoimittajina panostavat asiaan ja reagoivat nopeasti mahdollisiin teknologiaongelmiin. (Mujunen, haastattelu 3.10.2012.)

Järjestelmän vikasietoisuutta testattiin simuloimalla ensin yhdessä konesalissa tapahtuvia yksittäisiä laitteistovikoja ja palvelimien ja tallennusjärjestelmän välisten tietoliikenneyhteyksien katkeamista, ja sen jälkeen testaamalla katastrofinkestävyyttä katkaisemalla konesalien välisiä tietoliikenneyhteyksiä. Testauksen perusteella voitiin todeta, että valittu arkkitehtuuri täyttää sille asetetut korkean käytettävyyden vaatimukset ja toimii suunnitellulla tavalla. (Suna, haastattelu 9.10.2012.)

7 YHTEENVETO

”Vahinko ei tule kello kaulassa”, sanoo vanha suomalainen sananlasku. Suomalaiset yritykset ja julkishallinnon organisaatiot toimivat lähtökohtaisesti vakaassa ja turvallisessa toimintaympäristössä, mutta äkilliset ja odottamattomat häiriöt voivat yllättäen muuttaa tilanteen. Mitä paremmin organisaatio tuntee oman toimintansa ja toiminnan jatkuvuuteen vaikuttavat uhkatekijät, sitä paremmin organisaatiolla on mahdollisuus varautua niihin ja selvitä niistä. Lainsäädäntö ja toimialakohtaiset määräykset velvoittavat julkishallintoa ja huoltovarmuuden kannalta tärkeitä yrityksiä jatkuvuuden hallintaan ja varautumiseen. Muissa organisaatioissa jatku-

vuuden hallinnan ja varautumisen taso riippuu kyseisten organisaatioiden omasta päätöksenteosta. Saatavilla olevat tutkimustulokset osoittavat, että suomalaisten yritysten ja julkisen hallinnon organisaatioiden jatkuvuuden hallinnassa ja varautumisessa häiriötilanteisiin on vielä paljon parantamisen varaa. Jatkuvuuden suunnittelu ja jatkuvuussuunnitelmien ylläpito aiheuttaa toki lisätöitä organisaatioille, mutta paremman varautumisvalmiuden lisäksi se auttaa organisaatioita tehostamaan muutoshallintaa ja ICT-järjestelmien konfiguraationhallintaa.

Jatkuvuuden hallintaan kuuluu olennaisena osana toipumissuunnitelma, jonka lähtökohtana on organisaation toiminnoille ja niitä tukeville ICT-järjestelmille asetettavat toipumistavoitteet. Kun toipumistavoitteet on määritetty, voidaan niiden pohjalta toteuttaa tavoitteet täyttävät tekniset ratkaisut ja toimenpiteet. Nyrkkisääntönä voidaan todeta, että ei ole olemassa vain yhtä oikeaa tapaa varmistaa toimintojen ja niitä tukevien ICT-järjestelmien käytettävyys, vaan kustannustehokkainta on käyttää eritasoisia ratkaisuja. Varautuminen häiriötilanteisiin aiheuttaa lisäkustannuksia, mutta toisaalta mahdolliset käyttökatkot voivat aiheuttaa huomattavasti enemmän kustannuksia. Toipumistavoitteita määritettäessä tulisikin häiriötilanteista koituvat kustannukset suhteuttaa varautumisen aiheuttamiin kustannuksiin.

Ilman testausta ei voida todentaa toipumistavoitteiden toteutumista. Esimerkiksi jollekin kriittiselle ICT-järjestelmälle voidaan asettaa liian vaativa toipumisaikatavoite, jota käytössä oleva tekninen toteutus ei todellisuudessa täytä. Ellei toipumista testata ja sen pohjalta tehdä korjaavia toimenpiteitä joko toipumisaikatavoitteeseen, tekniseen toteutukseen tai prosesseihin, niin toipumissuunnitelma antaa virheellisen kuvan organisaation valmiudesta. Testausten käytännön toteuttaminen ei kuitenkaan ole helppoa, sillä mitä laajemmin testaus toteutetaan, sitä enemmän se maksaa ja vaatii henkilöstöresursseja. Lisäksi testaaminen voi olla vaikeasti toteutettavissa siten, ettei se vaikuta ICT-järjestelmien normaaliin käyttöön.

Toiset organisaatiot ovat enemmän riippuvaisia tietotekniikasta kuin toiset. Verraten harvassa ovat kuitenkin ne organisaatiot, jotka selviytyisivät pitkäkestoisista ICT-järjestelmien käyttökatkoista ilman merkittäviä tappioita tai uhkaa koko toiminnan jatkuvuudelle. Organisaatioiden toiminnalle kriittisten järjestelmien määrä on kasvanut, ja nykyään yhä useamman järjestelmän pitää olla saatavilla vuorokauden ympäri. Käytettävyysvaatimusten tiukentuessa ei yksittäisten ICT-infrastruktuurin komponenttien monentaminen välttämättä enää riitä, vaan tarvitaan järjestelmien maantieteellistä hajauttamista. Maantieteellinen hajauttaminen on vaativaa ja edellyttää huolellista suunnittelua, jossa kaikki palveluketjuun liittyvät ICT-infrastruktuurin komponentit on otettava huomioon. Hyödyntämällä uusinta teknologiaa voidaan hajautus tehdä korkealuokkaisesti, mutta silti kustannustehokkaasti, täyttäen vaativimmatkin toipumistavoitteet.

LÄHTEET

CA Technologies 2010. The Avoidable Cost of Downtime. Julkaistu syyskuu 2010, pdf-tiedosto. Viitattu 7.9.2012.
http://mjf.ie/wp-content/uploads/white-papers/acd_report_2011.pdf

CA Technologies 2011. Insight: Data Protection and the Cloud. Viitattu 15.9.2012.
http://www.arcserve.com/~/media/Files/supportingpieces/ca_dpatc_eu.ashx

EMC OSA 2011. Tampere region, Finland, pdf-tiedosto. Viitattu 27.10.2012.
http://finland.emc.com/collateral/customer-profiles/tampere-region-finland.pdf

EMC VPLEX 2011. EMC VPLEX 5.0 Architecture Guide, April 2011, pdf-tiedosto. Viitattu 27.10.2012.
http://www.emc.com/collateral/hardware/white-papers/h8232-vplex-architecture-wp.pdf

eVARE 2009. ICT-varautumisen kehittämishanke, pdf-tiedosto. Viitattu 15.9.2012.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20090318CTvara/03_eVARE_info_11_3_2009.pdf

Finanssivalvonta 2011. Päivitetty määräys- ja ohjekokoelma 1/101/2009 vakuutusyhtiöille, työeläkevakuutusyhtiöille, vakuutusyhdistyksille, vakuutusomistusyhteisöille, kolmannen maan vakuutusyhtiöiden sivuliikkeille ja lailla perustetuille eläkelaitoksille, päivitetty 13.4.2011, pdf-tiedosto. Viitattu 7.9.2012.
http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Vakuutussektori/Vakuutusyhtiot_yhdistykset_edustustot/Documents/maarays_3-102-2011_lausunnolle.pdf

Finanssivalvonta 2012. Rahalaitoksen Standardi 4.4b – Operatiivisten riskien hallinta, versio 3, pdf-tiedosto. Viitattu 7.9.2012.
http://www.finanssivalvonta.fi/fi/Saantely/Maarayskokoelma/Rahoitussektori/4_Vakavaraisuus_ja_riskien_hallinta/Documents/4.4b.std3.pdf

Fujitsu n.d.a. Fujitsu at a Glance. Viitattu 12.9.2012.
http://www.fujitsu.com/global/about/profile/info/

Fujitsu n.d.b. Fujitsu Suomessa. Viitattu 12.9.2012.
http://www.fujitsu.com/fi/about/finland/index.html

Heinonen, Ari 2012. Tietoliikennearkkitehti. Fujitsu Finland. Haastattelu 31.10.2012.

Huoltovarmuuskeskus n.d. Jatkuvuuden hallinta. Viitattu 6.9.2012.
http://www.huoltovarmuus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/

HUOVI n.d. Huoltovarmuuskeskuksen HUOVI-portaali. Viitattu 7.9.2012.
http://www.huoltovarmuus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/huovi/

Iivari, M ja Laaksonen, M, 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. 1. painos. Helsinki: Tietosanoma

ITIL 2011. ITIL Suomenkielinen sanasto v1.0, julkaistu 29.7.2011, pdf-tiedosto. Viitattu 12.9.2012.
http://www.itsmf.fi/doc/sanasto/ITIL_2011_Finnish_Glossary_v1.0.pdf

KATAKRI 2011. Kansallinen turvallisuusauditointikriteeristö, versio II, pdf-tiedosto. Viitattu 15.9.2012.
http://www.defmin.fi/files/1870/KATAKRI_versio_II.pdf

KVARE 2011. Valtionvarainministeriön julkaisuja 5/2011, Kuntien ICT-varautumisen esitutkimushanke, pdf-tiedosto. Viitattu 15.9.2012.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/03_kunnat/20110118Kuntie/Kuntien_ICT-varautuminen.pdf
Laki huoltovarmuuden turvaamisesta 18.12.1992/1390
http://www.finlex.fi/fi/laki/ajantasa/1992/19921390

Market-Visio 2010. Liiketoiminnan riippuvuus ICT:sta kasvaa, hallitaanko riskit? Julkaistu 19.4.2010, pdf-tiedosto. Viitattu 12.9.2012.
http://powerquality.eaton.com/suomi/ICT_Continuity_FINAL_REPORT.pdf

Mujunen, Tuomo 2012. Tietohallintopäällikkö. Pirkanmaan sairaanhoitopiiri. Haastattelu 3.10.2012.

PCI DSS 2010. PCI DSS 2.0 - Vaatimukset ja turvallisuuden arviointimenetelmät, pdf-tiedosto. Viitattu 7.9.2012.
http://www.luottokunta.fi/fi/toimialatietoa/pci_standardit/standardit/pci_dss_standardi/PCI%20DSS%20v2.0_FI.pdf

PSHP-vuosikertomus 2011, pdf-tiedosto. Viitattu 8.9.2012.
http://www.pshp.fi/download.aspx?ID=24197&GUID={743725C8-767C-419D-A39B-489BB39165E5}

PSHP-tietohallinto n.d. Viitattu 8.9.2012.
http://www.pshp.fi/default.aspx?contentid=252&contentlan=1

Recovery Specialties n.d. Business Continuity: The 7-tiers of Disaster Recovery. Viitattu 7.9.2012.
http://recoveryspecialties.com/7-tiers.html

SOPIVA n.d. Sopimuksiin perustuva varautuminen. Viitattu 7.9.2012.
http://www.huoltovarmuus.fi/tietoa-huoltovarmuudesta/jatkuvuudenhallinta/sopiva/

STM 2002. Sosiaali- ja terveysministeriön julkaisuja 2002:5, Terveydenhuollon valmiussuunnitteluopas. Viitattu 15.9.2012.
http://pre20031103.stm.fi/suomi/hao/julkaisut/stmopas2002-15.pdf

STM 2011. Sosiaali- ja terveysministeriön julkaisuja 2011:15, pdf-tiedosto. Viitattu 15.9.2012.
http://www.stm.fi/c/document_library/get_file?folderId=2765155&name=DLFE-16622.pdf

Suna, Teemu 2012. Chief Information Officer. Fujitsu Finland. Haastattelu 9.10.2012.

Tietotekniikan liitto 2012. Tietohallintojen johtaminen Suomessa, julkaistu 14.3.2012, pdf-tiedosto. Viitattu 15.9.2012.
http://www.ttlry.fi/sites/ttl.ttlry.mearra.com/files/file-uploads/Tutkimus/THJ/Sofigate-TTL_tutkimusraportti_2012_www.pdf

Tietoturvatasot 2008. Tietoturvatasot-käsikirjan luonnos 29.10.2008, pdf-tiedosto. Viitattu 7.9.2012.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/03_muut_asiakirjat/20081103Lausun/02_TTT-kaesikirja-20081029.pdf

Tiihonen, Olli 2012. Järjestelmäarkkitehti. Fujitsu Finland. Haastattelu 16.10.2012.

VAHTI 2008. VAHTI-ohje 8/2008, valtionhallinnon tietoturvasanasto, pdf-tiedosto. Viitattu 15.9.2012.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20081211Valtio/Vahti_8_NETTI%2b_KANNET.pdf

VAHTI 2009. VAHTI-ohje 2/2009. ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin, pdf-tiedosto. Viitattu 15.9.2012.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtionhallinnon_tietoturvallisuus/20090410ICTtoi/Vahti_2_NETTI_%2b_KANNET.pdf

VAHTI 2010. VAHTI-ohje 2/2010. Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta, pdf-tiedosto. Viitattu 15.9.2012.

http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/05_valtion hallin-
non_tietoturvallisuus/20101028Ohjeti/02_Ohje_tietotuvallisuudesta_valtionhallinnossa.pdf

VAHTI 2012. VAHTI-ohje 2/2012. ICT-varautumisen vaatimukset, pdf-tiedosto. Viitattu 12.10.2012.
http://www.vm.fi/vm/fi/04_julkaisut_ja_asiakirjat/01_julkaisut/076_ict/20120925ICTvar/vahti_2_2012_NETTI_PDF.pdf

Valmiuslaki 29.12.2011/1552
http://www.edilex.fi/stuklex/fi/lainsaadanto/20111552

Viestintävirasto 54 A/2012M. Viestintäviraston määräys 54 A/2012M viestintäverkkojen ja –palvelujen varmistamisesta, pdf-tiedosto. Viitattu 7.9.2012.
http://www.ficora.fi/attachments/suomimq/67NiBOcnn/M54_A_2012.pdf

VMware 2012. VMware vSphere Metro Storage Cluster Case Study, pdf-tiedosto. Viitattu 24.10.2012.
http://www.vmware.com/files/pdf/techpaper/vSPHR-CS-MTRO-STOR-CLSTR-USLET-102-HI-RES.pdf

VNp 21.8.2008/539. Valtioneuvoston päätös huoltovarmuuden tavoitteista 21.8.2008/539.
http://www.finlex.fi/fi/laki/ajantasa/2008/20080539

Yhteiskunnan turvallisuus 2012. Varautuminen ja jatkuvuuden hallinta kunnassa, pdf-tiedosto. Viitattu 15.9.2012.
http://www.yhteiskunnanturvallisuus.fi/fi/materiaalit/doc_download/31-varautuminen-ja-jatkuvuudenhallinta-kunnassa

YTS 2010. Yhteiskunnan turvallisuusstrategia, pdf-tiedosto. Viitattu 15.9.2012.
http://www.defmin.fi/files/1705/yts_2010_fi_nettiin.pdf

JATKUVUUDEN HALLINTAAN LIITTYVIÄ LAKEJA JA ASETUKSIA

Seuraavassa taulukossa on mainittu joitakin tärkeimpiä lakeja, asetuksia ja päätöksiä, jotka tulee huomioida huoltovarmuuskriittisten ja tietyllä toimialalla toimivien organisaatioiden jatkuvuuden hallinnan suunnittelussa:

Laki/Asetus/Päätös	Mitä koskee ja velvoittaa
Valmiuslaki 29.12.2011/1552	Viranomaisten varautumista poikkeusoloihin ja viranomaisten toimivaltuuksia poikkeusoloissa. Laki velvoittaa yhteiskunnan toiminnan kannalta tärkeitä laitoksia varautumaan poikkeusoloihin.
Laki huoltovarmuuden turvaamisesta 18.12.1992/1390	Laki on tarkoitettu turvaamaan poikkeusoloissa väestön toimeentulo ja talouselämän ja maanpuolustuksen kannalta välttämättömät toiminnot ja tekniset järjestelmät.
Valtioneuvoston päätös huoltovarmuuden tavoitteista 21.8.2008/539	Päätöksessä määritellään tavoitteet yhteiskunnan kriittisen infrastruktuurin ja tuotannon turvaamiseksi.
Laki televisio- ja radiotoiminnasta 9.10.1998/744 15a §	Lain 15a § velvoittaa toimiluvan saaneita organisaatioita huolehtimaan, että toimiluvan alainen toiminta jatkuu mahdollisimman häiriöttömästi myös valmiuslaissa tarkoitetuissa poikkeusoloissa sekä normaaliolojen häiriötilanteissa.
Viestintämarkkinalaki 23.5.2003/393 90 §	Lain 90 § velvoittaa teleyrityksiä huolehtimaan, että toiminta jatkuu mahdollisimman häiriöttömästi myös valmiuslaissa tarkoitetuissa poikkeusoloissa sekä normaaliolojen häiriötilanteissa.
Valtioneuvoston asetus viestintämarkkinoihin liittyvästä varautumisvelvollisuudesta ja viranomaistiedotteiden välittämisvelvollisuudesta 838/2003.	Asetuksen 7 § velvoittaa yhteiskunnan johtamisen tai turvallisuuden tai elinkeinoelämän toimintakyvyn varmistamisen kannalta merkityksellisessä asemassa olevia teleyrityksiä laatimaan varautumissuunnitelman normaaliolojen häiriötilanteita sekä valmiuslaissa tarkoitettuja poikkeusoloja varten.
Sähköisen viestinnän tietosuojalaki 16.6.2004/516 19 §	Laki velvoittaa teleyrityksiä huolehtimaan palvelujensa tietoturvasta ja palveluita käyttäviä yrityksiä ja yhteisöjä käyttäjiensä tunnistamistietojen ja paikkatietojen käsittelyn tietoturvasta. Lain 19 §:ssä todetaan, että tietoturvasta huolehtiminen tarkoittaa sellaisia toimia, joilla varmistetaan toiminnan turvallisuus, tietoliikenneturvallisuus, laitteisto- ja ohjelmistoturvallisuus sekä tietoaineistoturvallisuus. Lieventävänä kohtana todetaan kuitenkin, että turvaamistoimet on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin.

Laki/Asetus/Päätös	Mitä koskee ja velvoittaa
Sähköisen viestinnän tietosuojalaki 16.6.2004/516 19 §	Laki velvoittaa teleyrityksiä huolehtimaan palvelujensa tietoturvasta ja palveluita käyttäviä yrityksiä ja yhteisöjä käyttäjiensä tunnistamistietojen ja paikkatietojen käsittelyn tietoturvasta. Lain 19 §:ssä todetaan, että tietoturvasta huolehtiminen tarkoittaa sellaisia toimia, joilla varmistetaan toiminnan turvallisuus, tietoliikenneturvallisuus, laitteisto- ja ohjelmistoturvallisuus sekä tietoaineistoturvallisuus. Lieventävänä kohtana todetaan kuitenkin, että turvaamistoimet on suhteutettava uhkien vakavuuteen, tekniseen kehitystasoon ja kustannuksiin.
Valtioneuvoston asetus 681/2010	Asetus koskee valtionhallinnon viranomaisten asiakirjojen käsittelyn tietoturvallisuutta. Asetus sisältää säädökset asiakirjojen käsittelyä koskevista yleisistä tietoturvallisuusvaatimuksista sekä asiakirjojen luokittelun perusteista ja luokittelua vastaavista asiakirjojen käsittelyn tietoturvallisuusvaatimuksista. Asetus velvoittaa valtionhallintoa toteuttamaan 30.9.2013 mennessä tietojenkäsittelyssään asetuksessa säädetyt perustason tietoturvallisuusvaatimukset. Vaatimuksena on muiden muassa tietojen saannin ja käytettävyyden turvaaminen eri tilanteissa ja menettelytapojen luominen poikkeustilanteiden varalta.
Terveydenhuoltolaki 30.12.2010/1326 38 §	Laki koskee kunnan järjestämisvastuuseen kuuluvan terveydenhuollon toteuttamista ja lain 38 §:ssä säädetään terveydenhuollon alueellisesta varautumisesta suuronnettomuuksiin ja terveydenhuollon erityistilanteisiin ja velvoitetaan sairaanhoitopiirin kuntayhtymät laatimaan yhteistyössä alueensa kuntien kanssa terveydenhuollon alueellisen valmiussuunnitelman.

JATKUVUUDEN HALLINTAAN LIITTYVIÄ VALTIONHALLINNON SUOSITUKSIA JA OHJEITA

Seuraavassa taulukossa on lueteltu tärkeimpiä jatkuvuuden hallintaan liittyviä valtionhallinnon hankkeita ja ohjeita:

Hanke/asiakirja	Mitä sisältää
Tietoturvatasot-hanke, 2008	Valtionvarainministeriön asettamassa hankkeessa määritettiin hallinnollisen ja teknisen tietoturvan eri tasot: avoin taso, perustaso, korotettu taso, korkea taso ja erityistaso. Hankkeen tavoitteena oli auttaa valtionhallinnon organisaatioita sekä valtionhallinnon palveluntarjoajia kehittämään tietoturvakäytäntöjään täyttämään perustason vaatimukset 31.12.2010 mennessä. Sittemmin siirtymäkautta muutettiin Valtioneuvoston asetuksen 681/2010 julkistuksen yhteydessä ja siirtymäkautta pidennettiin 30.9.2013 asti. Huomioitavaa on, että perustasolta lähtien organisaatiolta edellytetään jatkuvuussuunnitelmaa. Hankkeen yhteydessä luotiin Tietoturvatasot-käsikirja, joka on tarkoitettu valtionhallinnolle ja organisaatioille, jotka tuottavat palveluita valtionhallinnolle. (Tietoturvatasot 2008)
Valtionhallinnon ICT-varautumisen kehittämishanke, eVARE, 2009	Valtionvarainministeriön käynnistämä hanke, jonka yhtenä tavoitteena oli mahdollistaa julkishallinnon yhtenäinen ja koordinoitu erityistilanteisiin varautuminen. (eVARE 2009)
Kansallinen turvallisuusauditointikriteeristö, KATAKRI	KATAKRIn päätavoitteena on yhtenäistää viranomaistoimintoja viranomaisen toteuttaessa yrityksessä tai muussa yhteisössä kohteen turvallisuustason todentavan auditoinnin. Toisena päätavoitteena on auttaa yrityksiä ja muita yhteisöjä sekä myös viranomaisia sidosryhmineen sisäisessä turvallisuustyössään. Tästä syystä kriteeristö sisältää erilliset suositukset myös elinkeinoelämälle. (KATAKRI 2011)
VAHTI-ohje 2/2010, Ohje tietoturvallisuudesta valtionhallinnossa annetun asetuksen täytäntöönpanosta	Ohjeen tarkoituksena on yhdenmukaistaa ja tehostaa valtioneuvoston tietoturvallisuusasetuksen (681/2010) täytäntöönpanoa valtion virastoissa. (VAHTI 2010)
VAHTI-ohje 2/2012, ICT-varautumisen vaatimukset.	Ohjeen tavoitteena on tehostaa ja yhdenmukaistaa ICT-varautumista ministeriöissä ja hallinnonalojen organisaatioissa. Ohje korvaa VAHTI 2/2009 –yleisohjeen ”ICT-toiminnan varautuminen häiriö- ja erityistilanteisiin”. (VAHTI 2012)

Hanke/ohje	Mitä sisältää
SOPIVA-hanke (SOPIVA = sopimuksiin perustuva varautuminen)	Julkishallinnon ja elinkeinoelämän yhteinen hanke, jonka tuloksena on laadittu suosituksia toiminnan jatkuvuuden hallintaan sekä tehty valmiita sopimuslausemalleja, joiden tarkoituksena on auttaa organisaatioita ottamaan jatkuvuuden hallintaan liittyvät suositukset huomioon palveluntuottajien kanssa tehtävissä hankinta- ja yhteistyösopimuksissa. (SOPIVA 2012)
HUOVI	Huoltovarmuuskeskuksen ylläpitämä portaali, jonka tarkoituksena on edistää huoltovarmuusorganisaatioiden välistä yhteistyötä ja kommunikaatiota. Portaali tarjoaa työkaluja, ohjeita ja koulutusta riskienhallinnan ja jatkuvuudenhallinnan kehittämiseen. (HUOVI 2012)

KATASTROFISTA TOIPUMISEN LUOKITUSTASOT

SHARE Inc, katastrofista toipumisen luokitustasot. (Recovery Specialties 2012)

Luokitustaso ja nimi	Kuvaus
Tier 0: Ei tiedon offsite-varmistusta (engl. No off-site data)	Organisaatioilla ei ole offsite-varmistusta, eikä voida arvioida, kuinka kauan toipuminen poikkeustilanteissa kestää. Hyvin todennäköistä on, ettei poikkeustilanteesta pystytä toipumaan ollenkaan. Käytännössä Tier 0 ei täytä katastrofista toipumisen vaatimuksia.
Tier 1: Tiedon varmistaminen maantieteellisesti toiseen paikkaan (off-site), ei varapalvelinkeskusta käytettävissä. (engl. Data backup with no hot-site)	Tiedot varmistetaan säännöllisesti ja varmuuskopiot (nauha tai muu siirrettävä media) kuljetetaan maantieteellisesti toiseen paikkaan. Menetettävän tiedon määrä riippuu siitä, kuinka usein varmuuskopiointi suoritetaan, ja kuinka usein kopiot siirretään toiseen paikkaan. Toipuminen kestää kuitenkin useita päiviä tai viikkoja, koska organisaatiolla ei ole valmiina toista palvelinkeskusta ja palvelin- ja tallennusjärjestelmiä, joihin tiedot palautetaan.
Tier 2: Tiedon varmistaminen maantieteellisesti toiseen paikkaan (off-site), varapalvelinkeskus on käytettävissä (engl. Data backup with hot-site)	Tiedot varmistetaan säännöllisesti ja varmuuskopiot (nauha tai muu siirrettävä media) kuljetetaan maantieteellisesti toiseen paikkaan. Menetettävän tiedon määrä riippuu siitä, kuinka usein varmuuskopiointi suoritetaan, ja kuinka usein kopiot siirretään toiseen paikkaan. Toipuminen kestää useita tunteja tai päiviä, mutta toipumisaika on paremmin arvioitavissa, sillä organisaatiolla on käytettävissään toinen palvelinkeskus, jossa palvelin- ja tallennuskapasiteettia.
Tier 3: Sähköinen tiedon siirtäminen ja säilyttäminen (engl. Electronic vaulting)	Täydentää Tier 2 –tasoa siten, että varmuuskopiot siirretään sähköisesti tietoliikenneyhteyksiä hyväksi käyttäen maantieteellisesti toiseen paikkaan. Ratkaisu edellyttää riittävän nopeaa tietoliikenneyhteyttä palvelinkeskusten välillä ja kohteessa fyysisiä tai virtuaalisia nauhakirjastoja ja/tai muita levyvarmistuslaitteita. Poikkeustilanteessa menetettävän tiedon määrä on todennäköisesti pienempi kuin Tier 2 –tasossa ja toipumisaika on lyhyempi.
Tier 4: Tietyn ajankohdan kopiot datasta. (engl. Point-in-time copies)	Tietyn ajankohdan klooni- ja/tai snapshot-kopiot mahdollistavat varmuuskopioinnin suorittamisen useammin ja nopeammin kuin perinteinen nauha- tai levyvarmistus ja siten myös toipuminen on nopeampaa. Klooni-kopio on alkuperäisen levyosion identtinen fyysinen kopio ja snapshot-kopio on alkuperäisen levyosion looginen kopio. Menetettävän tiedon määrä riippuu siitä, kuinka usein kloonitai snapshot-kopio otetaan.

Luokitustaso ja nimi	Kuvaus
Tier 5: Transaktioiden eheyden varmistaminen (engl. transaction integrity)	Menetettävän tiedon määrä on hyvin pieni tai sitä ei ole lainkaan. Toiminnallisuus edellyttää sovelluksilta ja tietokannoilta tukea transaktioiden eheyden varmistamiselle poikkeustilanteissa.
Tier 6: Ei tiedon hävikkiä tai pieni tiedon hävikki (engl. Zero or little data loss)	Ratkaisu ei välttämättä edellytä sovelluksilta ja tietokannoilta erityistä tukea tiedon eheyden varmistamiseksi, mutta edellyttää jossain muodossa tapahtuvaa tiedon etäkopiointia.
Tier 7: Automatisoitu, liiketoimintaan integroitu ratkaisu (engl. Highly automated, business-integrated solution)	Tier 7 –tason ratkaisut perustuvat pääosiltaan Tier 6 –tason teknologiaratkaisuihin, joihin on lisätty automatisoitua toiminnallisuutta, joilla toipumisaikaa voidaan lyhentää ja vähentää manuaalisten vaiheiden määrää ja inhimillisten erehdysten mahdollisuutta.