TOIPUMISSUUNNITELMAN LAATIMINEN TAMPEREEN SÄRKÄNNIEMI OY:LLE

Tanja Hämäläinen

Opinnäytetyö
Marraskuu 2014
Tietojenkäsittely

TAMPEREEN AMMATTIKORKEAKOULU
Tampere University of Applied Sciences

TIIVISTELMÄ

Tampereen ammattikorkeakoulu
Tietojenkäsittely

HÄMÄLÄINEN, TANJA:
Toipumissuunnitelman laatiminen Tampereen Särkänniemi Oy:lle

Opinnäytetyö 51 sivua
Marraskuu 2014

Tämän opinnäytetyön tarkoituksena oli kartoittaa Tampereen Särkänniemi Oy:n liiketoiminnan kannalta kriittisimmät tietojärjestelmät sekä laatia tietohallinnon käyttöön toipumissuunnitelma, jonka avulla liiketoiminta saataisiin palautettua normaalitilaan mahdollisimman nopeasti katastrofitilanteen jälkeen. Tavoitteena oli myös selvittää mahdollisia puutteita yrityksen tietojärjestelmien varmistuksessa ja palauttamisessa, tietojärjestelmien kannalta oleellisten laitteistojen sijoittelussa ja mahdollisten onnettomuuksien ennaltaehkäisyssä sekä antaa kehitysehdotuksia olosuhteiden parantamiseksi.

Työn tuloksena laadittiin Tampereen Särkänniemi Oy:n tietohallinnon käyttöön toipumissuunnitelma. Toipumissuunnitelma rajattiin sisältämään ainoastaan liiketoiminnan sekä lakisääteisten tietojen ja toimintojen kannalta välttämättömimmät järjestelmät. Siihen kirjattiin kunkin järjestelmän palauttamiseksi tehtävät toipumistoimenpiteet ja niiden vastuuhenkilöt sekä järjestelmien palauttamisessa oleellisten yhteistyökumppanien ja järjestelmätoimittajien yhteystiedot.

Työtä tehtäessä selvisi, että yrityksessä on toteutettu ja dokumentoitu riskienhallintaa hyvin jo pidemmän aikaa. Yrityksessä on varauduttu esimerkiksi tulipaloihin laajalla paloilmaisin- ja sammutinverkostolla, toteutettu hyvin kriittisten tietojen varmistus sekä dokumentoitu toipumisessa tarvittavat tiedot. Samalla kuitenkin selvisi myös, että liiketoiminnan jatkuvuuden kannalta oleelliset rutiinit ja testaukset puuttuvat. Esimerkiksi varmistusten palautuksia ei testata säännöllisesti ja kaikkia tärkeitä tietoja ei ole sijoitettu niin, että ne olisivat aina häiriötilanteessa helposti saatavilla riippumatta häiriön aiheuttajasta.

Jatkossa yrityksen kannattaa kiinnittää huomiota lakisääteisten ja toipumisen kannalta tärkeiden tietojen turvalliseen säilyttämiseen, niin että ne sijaitsevat useammassa paikassa ja ovat helposti saatavilla myös verkkoyhteyksien katkettua. Yrityksen tulisi myös laatia suunnitelma varmistusten ja palautusten säännölliselle testaamiselle sekä luoda rutiineja muille jatkuvuuden kannalta tärkeille toimenpiteille.

Opinnäytetyö on toteutettu tapaustutkimuksena ja tässä raportissa julkaistaan toipumissuunnitelman sisällysluettelo.

Asiasanat: tietojärjestelmät, jatkuvuussuunnittelu, toipumissuunnitelma

ABSTRACT

Tampereen ammattikorkeakoulu
Tampere University of Applied Sciences
Degree Programme in Business Information Systems

HÄMÄLÄINEN, TANJA:
Compiling a Disaster Recovery Plan for Tampereen Särkänniemi Ltd.

Bachelor's thesis 51 pages
November 2014

The objective of this thesis was to find out the most important information systems for Tampereen Särkänniemi Ltd.'s business and compile a disaster recovery plan to help restore the systems to normality after a disaster. The purpose was also to find out if there are any inadequacies in the company's practices concerning back-up and restoration of data or prevention of disasters and how they could be improved.

The result of this thesis was a disaster recovery plan for Tampereen Särkänniemi Ltd.'s data administration. It was limited to include only the most important information systems of the company's business. The plan contains the actions necessary for recovering each information system and the personnel responsible for carrying them out. It also contains important contact information of the system deliverers and partners.

The findings indicate that Tampereen Särkänniemi Ltd. has prepared itself well for disasters with monitoring and back-up systems for critical data. Based on the results it is recommended that the company creates a plan for regular testing of data restoration and pay attention to the storage of critical information to be recovered.

This thesis utilised a case study approach. This report contains the table of contents of Tampereen Särkänniemi Ltd.'s disaster recovery plan.

Key words: information systems, business continuity planning, disaster recovery plan

SISÄLLYS

LYHENTEET JA TERMIT

BIA	Business Impact Analysis, liiketoiminnan keskeytysvaikutusanalyysi. Liiketoiminnan keskeytysvaikutusanalyysillä pyritään selvittämään erilaisten riskien liiketoiminnalle aiheuttamat vahingot. Keskeytysvaikutusanalyysi eroaa riskianalyysistä siinä, että se keskittyy erilaisten keskeytysten liiketoiminnalle aiheuttamiin vaikutuksiin eikä keskeytysten syihin.
DNS	Domain Name System, verkon nimipalvelu. Nimipalvelu muuttaa helpommin muistettavat verkko-osoitteet numeerisiksi ip-osoitteiksi. Esimerkiksi ip-osoite 123.123.123.123 voitaisiin määrittää vastaamaan verkko-osoitetta www.yritys.fi.
RPO	Recovery Point Objective, tavoiteltu toipumispiste. Tavoiteltu toipumispiste määrittelee tilan, johon toiminta, järjestelmä tai tieto tulee saada palautettua häiriön jälkeen. Tavoiteltu toipumispiste ei välttämättä ole sama kuin tila, jossa oltiin juuri ennen häiriön alkamista.
RTO	Recovery Time Objective, tavoiteltu toipumisaika. Tavoitellulla toipumisajalla tarkoitetaan määriteltyä aikaa, jonka kuluessa kyseinen toiminto tulee saada palautettua toimintaan häiriön jälkeen.
UPS	Uninterruptible Power Supply, varavirtalähde.

1 JOHDANTO

Yrityksissä on varauduttu erilaisiin riskeihin kirjaamalla toimintaohjeet vaaratilanteita, kuten esimerkiksi tulipaloa, varten. Lakisääteisenä on tehty suunnitelmat käytettävistä varauloskäynneistä, evakuointi- ja pelastussuunnitelmat jne. Samalla tavoin tulisi varautua ennalta myös erilaisiin tietojärjestelmiä koskeviin katkoksiin ja kriisitilanteisiin, sillä nykyään tietojärjestelmät ovat yhä suuremmassa roolissa kaikessa liiketoiminnassa. Tietojärjestelmäkatkokset voivat aiheuttaa merkittäviäkin tappioita liiketoiminnalle ja kriittisimpien järjestelmien katkosten jatkuessa pidempään tai kriittisen tiedon hävitessä saattavat ne jopa lakkauttaa liiketoiminnan kokonaan.

Yrityksissä on jo pitkään tehty riskianalyyseja ja pyritty varautumaan erilaisiin riskeihin ennalta. Tätä tulisi jatkossa laajentaa koskemaan paremmin myös organisaatioiden tietojärjestelmiä ja kirjata ylös, kuinka niihin voitaisiin varautua ennalta ja kuinka tulisi toimia häiriötilanteen sattuessa. Suunnitelmia, joihin kirjataan jatkuvuuden takaamiseksi tai häiriötilanteista palautumiseksi tehtävät toimenpiteet, kutsutaan jatkuvuus- ja toipumissuunnitelmiksi. Suunnitelmia tehtäessä organisaatiossa tulisi pyrkiä tunnistamaan muun muassa kriittisimmät liiketoimintaan vaikuttavat järjestelmät sekä niiden mahdollisten käyttökatkosten aiheuttamat vaikutukset liiketoimintaan. Kun suunnitelmat on laadittu huolellisesti ja niissä on määritelty häiriötilanteissa tehtävät toimenpiteet ja vastuuhenkilöt, voidaan liiketoiminta saada jatkumaan mahdollisimman pienin taloudellisin tappioin mahdollisista häiriötilanteista huolimatta.

Tampereen Särkänniemi Oy:ssä on toteutettu riskianalyyseja eri toimintoihin liittyen ja sellainen on laadittu myös tietohallinnon käyttöön. Tähän saakka yrityksestä on kuitenkin puuttunut laajempi virallinen suunnitelma häiriötilanteissa tehtävistä toimenpiteistä ja toimenpiteet toteuttavista yhteyshenkilöistä. Tietojärjestelmien lisääntyessä ja laajentuessa koskemaan yhä useampia organisaation toimintoja ja niiden vaikuttaessa entistä vahvemmin myös liiketoimintaprosesseihin, on huomattu aiheelliseksi kirjata ylös toipumissuunnitelma tietohallinnon käyttöön.

Opinnäytetyön tavoitteena on tutustua liiketoiminnan jatkuvuussuunnitteluun ja sen osa-alueisiin sekä laatia Tampereen Särkänniemi Oy:n tietohallinto-osaston käyttöön toipumissuunnitelma liiketoiminnan kannalta kriittisimpien järjestelmien osalta. Toipumissuunnitelmasta rajataan pois järjestelmät, jotka ovat mahdollisesti suunnitteilla, mutta

joita ei vielä ole otettu käyttöön. Jatkossa on tarkoitus päivittää toipumissuunnitelmaa järjestelmien lisääntyessä tai vaihtuessa sekä laatia myös laajempi jatkuvuussuunnitelma koko yrityksen käyttöön.

1.1 Tampereen Särkänniemi Oy

Tampereen Särkänniemi Oy on Tampereen kaupungin kokonaan omistama osakeyhtiö, joka on perustettu vuonna 1966. Yhtiö on kuitenkin itsenäinen liiketoimintayksikkö, jonka johdossa on toimitusjohtaja, joka puolestaan vastaa hallitukselle. Yrityksen henkilöstöön kuului vuonna 2013 98 vakituista työntekijää, lisäksi kesäkaudeksi 2013 yrityksen palvelukseen palkattiin 520 kesätyöntekijää. (Särkänniemi 2014.)

Särkänniemen Elämyspuisto koostuu Tampereen Särkänniemi Oy:n kuudesta kohteesta (Akvaario, Delfinaario, huvilaitealue, Särkänniemen Koiramäki, Näsinneulan näkötorni ja Planetaario) sekä Tampereen kaupungin hallinnoimasta Sara Hildénin taidemuseosta. Särkänniemen Elämyspuistossa vierailee vuosittain noin 600 000 - 700 000 asiakasta, joista suurin osa kesäkauden (pääsääntöisesti toukokuusta elokuuhun) aikana. Vuonna 2013 Särkänniemen Elämyspuistossa vieraili yhteensä n. 586 000 asiakasta, joista n. 78 % kesäkauden aikana. (Särkänniemi 2014.)

Tampereen Särkänniemi Oy on sertifioitu yritys, jolla on laatu-, ympäristö- ja turvallisuussertifikaatit (ISO 9000, ISO 14 001 ja OHSAS 18001). Laatusertifikaatti edellyttää muun muassa yrityksen laadunhallintajärjestelmän dokumentointia. Tämän opinnäytetyön tuloksena laadittu toipumissuunnitelma on toteutettu täyttäen yrityksen dokumentaatiolle asettamat vaatimukset.

Tampereen Särkänniemi Oy:n käytössä on useita eri tietojärjestelmiä. Tietojärjestelmät liittyvät kaikkiin yrityksen toimintoihin tavalla tai toisella. Liiketoiminnan kannalta tärkeimpiä järjestelmiä ovat kassajärjestelmä ja taloushallinnon järjestelmät, jotka vastaavat yrityksen rahaliikenteestä. Yritys harjoittaa liiketoimintaa myös omassa verkkokaupassa, joka on toistaiseksi ollut vain yksi pieni lipunmyyntipiste muiden joukossa, mutta tulevaisuudessa se on toivottavasti yksi yrityksen tärkeimmistä myyntikanavista. Yrityksen käytössä on myös monia muita järjestelmiä, joita käytetään esimerkiksi työvuorosuunnit-

teluun, asiakkuuksienhallintaan, asiakaspalautteiden käsittelyyn ja poikkeamien kirjaamiseen, kunnossapidon huoltopyyntöjen käsittelyyn ja huvilaitteiden tarkistusten kirjaamiseen, yrityksen sisäiseen viestintään, luovutettujen lipputuotteiden seurantaan sekä valokuvien ottamiseen ja tulostamiseen esim. Tukkijoen kyydissä olevista asiakkaista. Osa järjestelmistä on ostettu valmiina, osa on tilattu räätälöitynä ja osan on suunnitellut ja toteuttanut yrityksen omat työntekijät.

1.2 Opinnäytetyön tavoitteet ja toteuttaminen

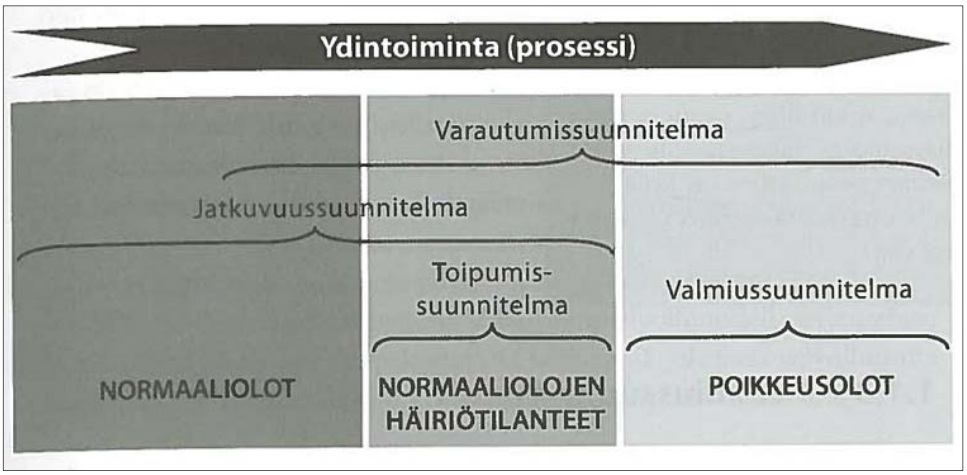
Opinnäytetyön tavoitteena on luoda toipumissuunnitelmapohja Tampereen Särkänniemi Oy:n tietohallinnolle sekä dokumentoida siihen liiketoiminnan kannalta kriittisimmät tietojärjestelmät. Opinnäytetyön tuloksena tuotetaan yrityksen dokumentoinnille asetettujen vaatimusten mukaisesti laadittu kirjallinen toipumissuunnitelma, jossa määritellään esimerkiksi tärkeimpien tietojärjestelmien varmistuskeinot ja varajärjestelmät sekä kirjataan toimintaohjeet ja vastuuhenkilöt sekä tärkeimpien yhteistyökumppaneiden ja järjestelmätoimittajien yhteystiedot poikkeustilanteiden varalle.

Yrityksen tietohallinnolle on tehty riskienhallintasuunnitelmia, mutta muutosten myötä riskikartoitusten päivittäminen on tullut ajankohtaiseksi. Viime vuosina yrityksen tietojärjestelmät ovat laajentuneet, minkä myötä myös mahdollisten riskien vaikutukset ovat kasvaneet. Erityisesti kriittisten järjestelmien osalta vaikutukset liiketoimintaan voivat olla hyvinkin vahingollisia. Toipumissuunnitelmaa tietohallinnolla ei ole ollut dokumentoituna, joten sellaisen laatiminen on katsottu yrityksessä erityisen tarpeelliseksi ja toteutettavaksi pikimmiten – ennen kuin vahinkoa ehtii tapahtua.

Opinnäytetyön tutkimusote tulee olemaan kvalitatiivinen eli laadullinen. Opinnäytetyö tulee olemaan tapaustutkimus, sillä sen laatiminen liittyy hyvin vahvasti tietyn yrityksen tutkimiseen ja heille suunnitellun lopputuloksen toteuttamiseen. Työn tavoitteena on laatia yrityksen käyttöön konkreettinen, kirjallinen toipumissuunnitelma, joten opinnäytetyötä voidaan pitää myös konstruktiivisena. Aineistona käytetään haastatteluja, havainnointia sekä yrityksellä jo olemassa olevaa kirjallista aineistoa.

2 JATKUVUUSSUUNNITTELU

Jatkuvuussuunnitteluun liittyy useita eri käsitteitä. Ongelmana on, että eri käsitteitä ei aina käytetä täysin johdonmukaisesti vaan käyttötavoissa voi olla eroja. Eri käsitteitä ei voikaan täysin erottaa toisistaan, sillä ne liittyvät tiiviisti toisiinsa ja kuten kuviosta 1 näkee, menevät ne osittain myös limittäin. Käsitteiden määrittelyssä tärkeään asemaan nousevat liiketoiminnan normaaliolosuhteiden, normaaliolojen häiriötilanteiden sekä poikkeusolojen erottaminen toisistaan. (Iivari & Laaksonen 2009, 18.)



KUVIO 1**.** Jatkuvuussuunnitelman, toipumissuunnitelman, valmiussuunnitelman ja varautumissuunnitelman suhde (Iivari & Laaksonen 2009, 19)

2.1 Jatkuvuussuunnittelu

Jatkuvuussuunnittelu on prosessi, joka on osa yrityksen toiminnan laadunvarmistusta, riskienhallintaa sekä tietoturvallisuutta. Sen tarkoituksena on varautua ennalta mahdollisiin häiriötilanteisiin ja turvata liiketoiminnan jatkuminen niin normaaliolosuhteissa kuin häiriötilanteissakin. Häiriötilanteet voivat olla vakavuudeltaan erisuuruisia ja niitä voivat aiheuttaa esimerkiksi tietojärjestelmähäiriö, tietoliikennekatkos, sähkökatkos, inhimillinen virhe, tulipalo, vesivahinko, toimitilojen tuhoutuminen tai avainhenkilöiden menetys. Häiriötilanteisiin varaudutaan jatkuvuussuunnitteluprosessiin kuuluvissa toipumissuunnitelmissa sekä normaaliolojen aikana toteutettavissa liiketoiminnan tukiprosesseissa. (Iivari & Laaksonen 2009, 18–19)

"Yrityksen liiketoiminnan jatkuvuuden suunnittelu tulee olemaan yhä tärkeämpää. On tiedettävä, kuinka bisnestä pyöritetään, jos joku tietojärjestelmä ei toimi. Ja mitä tehdään

silloin, jos katkos kestää minuutin, tunnin, päivän tai viikon", toteaa Fortumin tietohallintojohtaja Jouni Keronen ennaltaehkäisevän tietoturvatyön merkityksestä. Kun aiemmin tukijärjestelminä pidettyjen järjestelmien, kuten asiakashallinta- ja laskutusjärjestelmät sekä sähköposti, merkitys on kasvanut, on myös toipumiskyvyn tärkeys korostunut. (Muukkonen 2003.)

2.1.1 Tavoitteet

Jatkuvuussuunnittelun avulla pyritään ensisijaisesti turvaamaan organisaation toiminta häiriöiltä sekä minimoimaan mahdollisten keskeytysten liiketoiminnalle aiheuttamat haitat ja kustannukset. British Standards Institutionin julkaiseman jatkuvuuden hallinnan standardin mukaan jatkuvuussuunnittelun tarkoituksena on määrittää ja huomioida liiketoiminnan jatkuvuuden edellytykset, organisaation tavoitteet ja velvoitteet, hyväksyttävissä oleva riskitaso, lakien ja sopimusten asettamien velvoitteiden noudattaminen sekä sidosryhmien etujen valvonta. (Iivari & Laaksonen 2009, 27.)

2.1.2 Hyödyt

Jatkuvuussuunnittelu on yhteydessä organisaation riskienhallintaan ja sen avulla pyritäänkin takaamaan liiketoiminnan jatkuminen kaikissa olosuhteissa ja siten vähentämään liiketoiminnalle mahdollisista häiriötilanteista aiheutuvia kustannuksia. Tuomas Linnake (2010) toteaa suomalaisten yritysten kärsivän yhteensä 440 miljoonan euron tappiot vuosittain tietojärjestelmien pettämisten vuoksi, yritystä kohden menetys on kesimäärin 263 314 euroa vuodessa. Hyvin suunniteltuna jatkuvuussuunnittelun avulla voidaan myös parantaa organisaatioiden IT-järjestelmien muutosten ja konfiguraation hallintaa hyvän dokumentoinnin ansiosta. (Iivari & Laaksonen 2009, 20–21)

Iivari ja Laaksonen (2009, 29–33) mainitsevat jatkuvuussuunnittelun hyödyiksi riskitietoisuuden lisääntymisen organisaatiossa, katastrofien vaikutusten minimoimisen, taloudellisten vaikutusten rajaamisen, organisaation imagon hallinnan ja positiivisen yrityskuvan ylläpitämisen sekä vaatimusten noudattamisen. Jatkuvuus- ja toipumissuunnitelmien laatiminen voi hyödyttää yritystä muutenkin, sillä yrityksen liiketoimintaprosesseja ana-

lysoitaessa saatetaan löytää kehityskohteita, mikä johtaa prosessien parantamiseen. Monesti liiketoiminnan palautumisen tavoitteiden saavuttamiseksi joudutaan tekemään parannuksia myös tietojärjestelmiin ja näin saavutetaan yhtenäisempi ja helpommin hallittava it-ympäristö. Muutosten myötä voidaan saavuttaa vakaampi it-ympäristö ja parantaa tarjottavien it-palvelujen tasoa sekä mahdollisesti saavuttaa kilpailuetua alan muihin toimijoihin. (Gregory 2008, 13.)

Jatkuvuussuunnitelmaa ja erityisesti toipumissuunnitelmaa laadittaessa tehdään riskianalyyseja organisaation toiminnasta ja liiketoiminnan keskeytysvaikutusanalyysi, jolla pyritään selvittämään erilaisten riskien liiketoiminnalle aiheuttamat vahingot. Useimmiten analyysien tekemiseen osallistuu useita eri toiminnoista vastaavia henkilöitä riippuen toki siitä, tarkastellaanko koko organisaation toimintaa, tiettyä prosessia vai prosessin osaa, kuten esimerkiksi tietojärjestelmää. Eri ihmiset saavat esittää omat näkemyksensä erilaisiin riskeihin liittyen, jolloin saatetaan löytää riskejä, joita ei aiemmin välttämättä ole huomattu. Riskianalyysin tekemiseen osallistuneet ihmiset yleensä jakavat riskitietoisuutta organisaatiossa, jolloin koko organisaation riskitietoisuus lisääntyy. (Iivari & Laaksonen 2009, 29–30.)

Toimialoilla voi olla erilaisia toimialakohtaisia vaatimuksia esimerkiksi tietoturvallisuuteen, riskienhallintaan ja jatkuvuussuunnitteluun liittyen, joita organisaation on noudatettava. Yleisemmin tällaisia vaatimuksia asetetaan toiminnoille, jotka ovat välttämättömiä yhteiskunnallisen toiminnan kannalta. Yritysmaailmassa vaatimuksia saattavat asettaa asiakkaat, jotka haluavat varmistua toimittajiensa toimitusvarmuudesta myös mahdollisissa ongelmatilanteissa. Toimittajat puolestaan pyrkivät vastaamaan vaatimuksiin kehittämällä toimintansa jatkuvuuden hallintaa sekä rajaamalla vastuutaan esimerkiksi sopimusten force majeure -pykälillä. Kun eri tahojen asettamat vaatimukset tunnistetaan ja toteutetaan ilman päällekkäisyyksiä, pystytään vaatimuksia noudattamaan kustannustehokkaasti kaikkia osapuolia miellyttävällä tavalla. (Iivari & Laaksonen 2009, 33.)

2.2 Toipumissuunnittelu

Toipumissuunnitelma on jatkuvuussuunnitelman osa ja se koskee lyhyempää aikaväliä kuin jatkuvuussuunnitelma. Toipumissuunnitelma sisältää ohjeita katastrofista toipumiseen, normaalitoimintaan palaamiseen sekä liiketoiminnan jatkamiseen. Toipumissuunnitelmassa määritellään liiketoimintaprosesseille ja niihin liittyville tärkeimmille tietojärjestelmille varajärjestelmävaatimukset, vastuut ja toimet valmiuden luomiseksi sekä ohjeet toiminnasta normaaliolojen häiriötilanteissa. Toipumissuunnitelmiin voidaan liittää muun muassa käsitteet riskienarviointi, liiketoiminnan keskeytysvaikutusanalyysi, toipumisstrategia sekä harjoittelu ja testaaminen. (Iivari & Laaksonen 2009, 19–20.)

2.3 Valmiussuunnittelu

Valmiussuunnittelu määritellään yleisimmin osaksi varautumissuunnittelua. Valmiussuunnittelulla pyritään varautumaan mahdollisiin poikkeusoloihin, kuten esimerkiksi sotatilaan, ja sen pohjana on valmiuslaki (1080/1991), joka puolestaan määrittelee viranomaisten toimintavaltuudet poikkeusoloissa. Valmiussuunnittelua toteutetaan pääosin julkishallinnon piirissä. (Iivari & Laaksonen 2009, 20–21.)

Finanssivalvonnan määritelmän mukaan valmiussuunnitelma on ”normaaliaikana laadittava ja ylläpidettävä kuvaus toimenpiteistä, joiden avulla toimija varmistaa toimintansa jatkamisen vakavissa häiriötilanteissa ja poikkeusoloissa. Suunnitelmassa kuvataan:

- toimintaperiaatteet häiriötilanteita ja poikkeusoloja varten
- normaaliaikana suoritettavat varautumistehtävät
- häiriötilanteiden ja poikkeusolojen toiminnot ja palvelut
- tarvittava yhteistyö sidosryhmien kanssa.” (Iivari & Laaksonen 2009, 20.)

Varautumisvelvoitteen piiriin kuuluviin organisaatioihin tehdään virallisia valmiustarkastuksia viranomaisten toimesta. Tarkastuksissa voi olla mukana esimerkiksi puolustusvoimien, palo- ja pelastustoimen tai toimialaa ohjaavan ministeriön edustaja riippuen tarkastuksen alaisen yrityksen toimialasta. Valmiustarkastuksissa arvioidaan varautumistoimenpiteiden riittävyyttä säädöksissä asetettuihin velvoitteisiin nähden, ja tarkastuksista raportoidaan kirjallisesti. (Miettinen 2002, 184–185.)

2.4 Varautumissuunnittelu

Varautumissuunnittelulla tarkoitetaan yleensä julkishallinnon ja tiettyjen yritysten varautumisvelvoitetta ja sen täyttämiseksi tehtävää suunnittelua. Varautumissuunnittelu sisältää valmiussuunnittelun lisäksi normaaliolojen häiriötilanteista toipumiseksi tehtävät toimenpiteet. Varautumissuunnitelman avulla pyritään turvaamaan yhteiskunnalle elintärkeät toiminnot niin normaali- kuin poikkeusolosuhteissa. Nämä toiminnot määrittelee valtioneuvosto ja niihin kuuluvat muun muassa valtion johtaminen, sotilaallinen puolustus, sisäinen turvallisuus, talouden ja yhteiskunnan toimivuus sekä väestön toimeentuloturva ja toimintakyky. (Iivari & Laaksonen 2009, 21.)

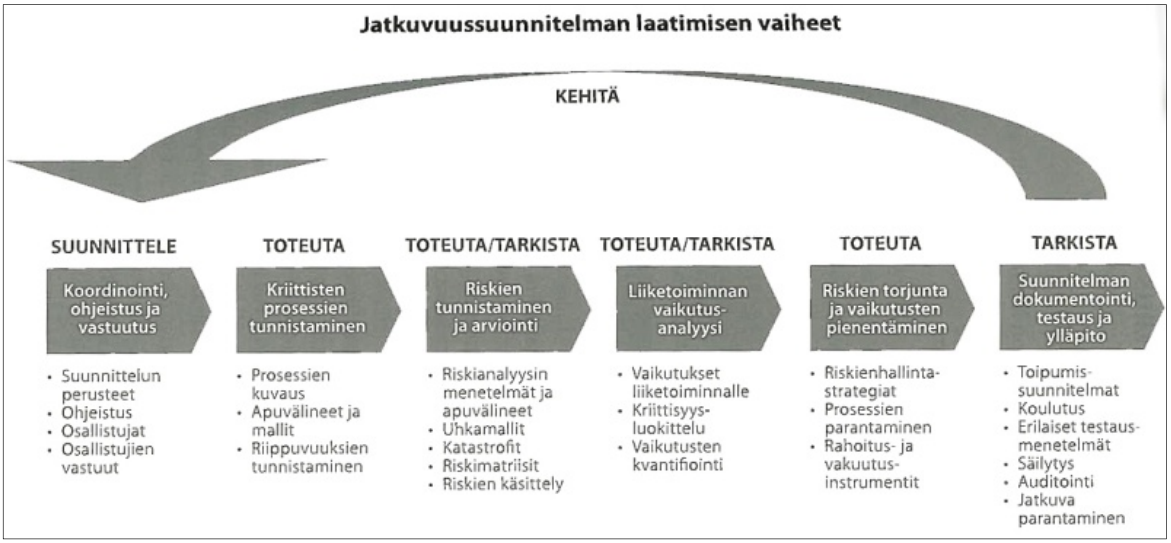
3 JATKUVUUS- JA TOIPUMISSUUNNITELMAN LAATIMINEN

Wallace & Webber (2004, 22) antavat yhden esimerkin, kuinka jatkuvuussuunnitteluprojekti voitaisiin yrityksessä toteuttaa. Projekti alkaa siitä, kun yrityksen johto päättää, että yrityksessä tarvitaan liiketoiminnan jatkuvuussuunnitelma. Tähän lopputulokseen voidaan päätyä, koska suunnitelman puute huomataan esimerkiksi yrityksen auditointien yhteydessä tai jonkun valveutuneen työntekijän toimesta. Pahimmassa tapauksessa yrityksessä on jo ehtinyt tapahtua jokin liiketoiminnan keskeytyminen, jonka jälkeen päätetään laatia suunnitelma, jotta jatkossa mahdolliset ongelmatilanteet saataisiin hoidettua nopeammin ja tehokkaammin vähäisemmillä vaikutuksilla liiketoimintaan. Jatkuvuussuunnitelmaprojektin käyntiin laittaneesta johtajasta tulee yleensä projektin tukija ja hänen ensimmäisenä tehtävänään on valita sopiva henkilö projektin johtoon. Yhdessä he määrittelevät jatkuvuussuunnitelmaprojektin tavoitteet, määräajan ja toivotut tulokset. Tässä vaiheessa tarkistetaan myös, että suunnitelman laatimiseen on olemassa riittävästi resursseja.

Tämän jälkeen valitaan tiimi laatimaan suunnitelma. Tiimin valitsemisessa on tärkeää ottaa huomioon niin tekniset kuin sosiaalisetkin tekijät, jotta se pystyy yhdessä tuottamaan toimivan liiketoiminnan jatkuvuussuunnitelman. Tiimin valitsemisen jälkeen tehdään projektisuunnitelma, jossa määritellään ja jaetaan tehtävät sekä määritellään tehtävien kestot ja jaksotetaan ne. Suunnitelman mukaisesti toteutetaan sitten tarvittavat tehtävät, jotta saadaan luotua jatkuvuussuunnitelma. Projektin aikana siitä vastuussa oleva projektipäällikkö pitää huolen, että tehtävät tulevat tehdyiksi ja projektin etenemisestä tiedotetaan tarpeellisille tahoille. Kun suunnitelmat on laadittu ja testattu, projektipäällikkö päättää projektin ja varmistaa, että se on dokumentoitu oikein ja luovuttaa tulokset niille, joiden tehtävänä on jatkossa ylläpitää suunnitelmaa. Lisäksi projektipäällikkö raportoi projektin onnistumisesta ja saavutetuista tuloksista projektin tukijalle. (Wallace & Webber 2004, 22.)

Jatkuvuussuunnitelman laatimisessa voi hyödyntää erilaisia hyviä käytänteitä. Iivari ja Laaksonen (2009, 92) mainitsevat esimerkiksi USA:ssa toimivan National Institute of Standards and Technologyn (NIST) Continuity Planning Guide for Information Technology Systems:n. Jatkuvuussuunnittelun laatimisen perustana on organisaation ja sen liiketoiminnan ymmärtäminen, ja se tulee toteuttaa suunnitellusti ja johdonmukaisesti or-

ganisaation johdon tukemana. Yleensä suunnitelmia laaditaan strategisella tasolla, prosessitasolla sekä tietojärjestelmätasolla. Kun on määritelty vastuut suunnitelman laatimisessa, aloitetaan varsinaisen jatkuvuussuunnitelman laatiminen ja tehdään muun muassa uhka- ja riskianalyysi sekä liiketoiminnan keskeytysvaikutusanalyysit. Kuvio 2 antaa yhden esimerkin jatkuvuussuunnittelun eri vaiheista. Välttämättä vaiheet eivät kuitenkaan aina ole peräkkäisiä, vaan osaa niistä voidaan tehdä myös rinnakkain. (Iivari & Laaksonen 2009, 292.)



KUVIO 2. Jatkuvuussuunnitelman laatimisen vaiheet (Iivari & Laaksonen 2009, 93)

3.1 Suunnitelman perusteet

Jatkuvuussuunnittelua tarvitaan varmistamaan yrityksen toiminnan jatkuminen kaikissa mahdollisissa olosuhteissa tai sen nopea palauttaminen mahdollisten ongelmatilanteiden jälkeen. Suunnitelmaa tehtäessä on tärkeä tuntea organisaation toiminta: kuinka liiketoimintaprosessit toimivat, niiden riippuvuudet muihin prosesseihin sekä prosessien kannalta olennaiset IT-järjestelmät. Prosessit tulee kuvata ja niiden toiminta tulee tuntea alusta loppuun saakka, jotta ne osataan rakentaa tarvittaessa uudelleen. (Iivari & Laaksonen 2009, 94–95.)

Prosessien normaalin toiminnan lisäksi tulee tuntea myös prosessien toiminta erilaisissa häiriötilanteissa ja poikkeusolosuhteissa. Normaalioloilla tarkoitetaan tilaa, jossa organisaatio toimii vakaasti ja liiketoimintaa voidaan harjoittaa häiriöittä. Hetkellisiä normaa-

liolojen häiriöitä saattavat aiheuttaa esimerkiksi laiterikot tai lyhytaikaiset sähkö- tai tietoliikennekatkokset, mutta näistä selvitään yleensä normaalein työrutiinein. Jatkuvuussuunnittelussa tulisi kuitenkin ottaa huomioon myös nämä normaalitilanteissa tapahtuvat liiketoiminnan jatkuvuutta edistävät asiat (kuten järjestelmien ja toimintatapojen dokumentointi, tehtävien kierto, normaalit varmistusprosessit ja järjestelmien huoltaminen), niiden kuvaaminen sekä toteuttaminen. (Iivari & Laaksonen 2009, 95–96.)

Normaaliolojen häiriötilanteissa organisaatiossa ilmenee hieman vakavampi häiriö, jonka vuoksi liiketoiminnan harjoittaminen hankaloituu ja toimintaa joudutaan muuttamaan. Kyseinen ongelma koskee lähinnä yksittäistä organisaatiota, mutta välillisesti se saattaa toki vaikuttaa muihinkin toimijoihin. (Iivari & Laaksonen 2009, 95–96.)

Vakavan yhteiskunnallisen häiriön, esimerkiksi sotatilan, aikana organisaation toiminta hankaloituu huomattavasti ja liiketoimintaa saatetaan joutua supistamaan. Poikkeusolot vaikuttavat koko yhteiskunnan toimintaan ja yleensä toimintaa säätelevät viranomaiset erillisen lainsäädännön avulla. Organisaatiot voivat varautua poikkeusoloihin laatimalla erillisen valmiussuunnitelman. (Iivari & Laaksonen 2009, 96.)

3.2 Vastuiden määrittely

Organisaation johdon tulee määrittää jatkuvuussuunnittelun käytännön työtä ohjaava henkilö. Hänen lisäkseen suunnittelussa tulee olla mukana organisaation eri toiminnoista vastaavia ja eri tehtävissä toimivia henkilöitä, jotta organisaation toiminnasta saadaan mahdollisimman oikea kuva ja jatkuvuussuunnittelussa keskitytään oikeisiin asioihin. (Iivari & Laaksonen 2009, 98.)

Jatkuvuudenhallintaprosessin omistajuuden olisi hyvä olla aina organisaation ylimmällä johdolla. Johdon tehtävänä on ennen jatkuvuussuunnitelman laatimisen aloittamista määritellä, mitkä liiketoiminta-alueet suunnitelman halutaan kattavan sekä suojattavat liiketoimintaprosessit. Lisäksi johto osallistuu niihin suunnitelman vaiheisiin, jotka koskevat keskeisiä liiketoiminnallisia päätöksiä tai vaativat analysointia. Suunnitelman valmistumisen jälkeen johdon tulee myös päättää, milloin toipumistoimenpiteet aloitetaan mahdollisissa häiriötilanteissa. (Iivari & Laaksonen 2009, 98–99.)

Käytännön suunnittelusta vastaa usein tietoturva- tai IT-yksikkö, mutta vastuuhenkilönä tai -yksikkönä voi myös olla jokin muu organisaatioyksikkö. Vastuutahon tehtävänä ei ole laatia suunnitelmia tai tehdä päätöksiä yksin vaan pitää huolta, että kaikki tarvittavat asiat tulevat tehdyksi. Lisäksi vastuutahon tehtävänä on suunnitelman valmistumisen jälkeen varmistaa sen ylläpito ja testaaminen. (Iivari & Laaksonen 2009, 9.)

Jatkuvuussuunnittelua tehtäessä avainhenkilöinä ovat prosessien, järjestelmien ja tietojen omistajat, jotka määrittävät niiden suojaustarpeet, toipumis- ja palautumisvaatimukset sekä liiketoiminnan keskeytysvaikutukset. He osallistuvat muun muassa prosessikuvausten laatimiseen, mikäli sellaisia ei jo ole ennestään, prosessien ja järjestelmien tärkeysluokitteluun sekä tavoitellun toipumisajan ja -pisteen määrittelyyn. (Iivari & Laaksonen 2009, 101.)

Jatkuvuussuunnittelun tietojärjestelmiä koskevissa asioissa tärkeässä asemassa on luonnollisesti organisaation IT-yksikkö. Sen tehtävänä on miettiä tarvittavat toimenpiteet, jotta saavutetaan prosessien omistajien määrittelemät vaatimukset. IT-yksikkö vastaa pitkälti myös normaalitilanteissa tehtävistä jatkuvuutta turvaavista toimenpiteistä, kuten järjestelmien ylläpidosta, varmistuksista ja kehittämisestä. Mikäli mahdollista, kannattaa nämä asiat pohtia jo järjestelmää rakennettaessa ja sen vaatimusmäärittelyä tehtäessä. (Iivari & Laaksonen 2009, 102.)

3.3 Kriittisten prosessien ja järjestelmien tunnistaminen

Jatkuvuussuunnittelun perustana on prosessien tunnistaminen ja niiden toiminnan tunteminen. Organisaation prosesseista tulee erityisesti tunnistaa liiketoiminnan kannalta välttämättömimmät kriittiset prosessit, jotta keskitytään turvaamaan oikeita asioita. Kriittisten prosessien tunnistamisen jälkeen on niiden omistajien määriteltävä, kuinka pitkän käyttökatkon tai muun häiriön ja kuinka suuren tietomäärän menettämisen liiketoimintaprosessi ja organisaatio kestävät, ja millaisia tappioita mahdolliset häiriöt aiheuttavat. (Iivari & Laaksonen 2009, 104.)

Organisaation ydin- ja tukiprosessit tulee kuvata, jotta tiedetään mihin kaikkeen mahdollinen häiriötilanne voi vaikuttaa. Kuvaukset tulee tehdä sekä operatiivisella että strategi-

sella tasolla. Operatiivisella tasolla kuvataan prosessit, joita käytetään päivittäisessä toiminnassa. Tällaisia voivat olla esimerkiksi palvelujen tai tuotteiden tuotantoprosessi, tilausprosessi tai lähetysprosessi. Strategisella tasolla organisaation prosessit laitetaan tärkeysjärjestykseen ja selvitetään niiden väliset suhteet ja mitkä ovat välttämättömiä muiden prosessien toiminnalle. (Iivari & Laaksonen 2009, 104.)

Nykyään lähes kaikkiin prosesseihin liittyy erilaisia tietojärjestelmiä, jolloin kriittisiksi määriteltyjen prosessien toiminnalle olennaisia tietojärjestelmiä tulee myös pitää kriittisinä. Kriittisten järjestelmien tulisi olla sellaisia, että ne kestävät lyhyitä häiriötilanteita, kuten sähkökatkoksia, toiminnan keskeytymättä. (Iivari & Laaksonen 2009, 105.)

3.4 Kriittisten prosessien ja järjestelmien riskianalyysit

Kriittisille prosesseille ja järjestelmille tulee tehdä riskianalyysi säännöllisesti. Hyvä käytäntö on tarkistaa riskianalyysi vähintään kerran vuodessa ennalta määriteltynä ajankohtana tai aina toimintaympäristön muuttuessa, esimerkiksi uusien prosessien syntyessä tai vanhojen prosessien muuttuessa. Riskianalyysissä kartoitetaan mahdolliset uhat, niiden toteutumisen todennäköisyydet sekä siitä aiheutuvia vaikutuksia. Riskianalyysi voidaan toteuttaa kvantitatiivisesti tai kvalitatiivisesti. Määrällisessä riskianalyysissä uhan todennäköisyys määritellään prosentteina ja vaikutus euroina, jolloin niiden tulosta saadaan uhan toteutumisen aiheuttama riski. Mikäli tarkkojen lukujen märittäminen ei ole mahdollista tai edes järkevää, voidaan tehdä laadullinen riskianalyysi. Tällöin riskit määritellään halutulla asteikolla, esimerkiksi ei riskiä, matala riski, keskimääräinen riski ja korkea riski. (Iivari & Laaksonen 2009, 118–119.)

Riskianalyysin laatiminen koostuu seuraavista vaiheista: riskienhallintakehikon määrittely, uhkien tunnistaminen, uhkien toteutumisen todennäköisyyksien arviointi, riskien vaikutusten arviointi sekä riskien käsittely. Aluksi määritellään kehikko uhkien tunnistamiselle sekä todennäköisyyksien ja vaikutusten laajuuden määrittelylle. Tämän jälkeen pyritään tunnistamaan kaikki ne mahdolliset uhkat, jotka voivat aiheuttaa vahinkoa tutkinnan kohteena oleville prosesseille ja järjestelmille. Kun uhkat on tunnistettu, arvioidaan niiden toteutumisen todennäköisyys sekä uhan toteutuessa aiheutuvien vahinkojen ja tappioiden suuruus. Lopuksi pyritään kehittämään toimintatapoja, joilla pystytään en-

naltaehkäisemään riskejä tai pienentämään niiden vaikutusta tai päättämään, mikä riskeistä on ns. pienempi paha ja mitkä riskeistä taas pitäisi pyrkiä estämään kokonaan. (Iivari & Laaksonen 2009, 124–128.)

Riskianalyysin laadinnan tuotoksena on esimerkiksi taulukkomuodossa esitetty listaus organisaation toimintaa uhkaavista riskeistä, niiden todennäköisyyksistä ja vaikutuksista sekä toimenpiteistä, joilla niihin pyritään varautumaan. Ei kuitenkaan riitä, että riskianalyysi tehdään kerran vaan se tulee päivittää säännöllisesti esimerkiksi kerran vuodessa tai aina silloin, kun organisaation toiminta muuttuu. Riskianalyysiä tarkistettaessa tulee aina pohtia, ovatko muutokset mahdollisesti luoneet uusia uhkia, jolloin ne tulee lisätä riskianalyysiin. Riskianalyysiä tehtäessä tulee huomioida myös organisaation ulkopuolisten tahojen aiheuttamat riskit, jolloin myös organisaation sidosryhmissä tapahtuvien muutosten jälkeen tulee riskianalyysi päivittää niihin liittyvien riskien osalta. (Iivari & Laaksonen 2009, 135.)

3.5 Liiketoiminnan keskeytysvaikutusanalyysi

Liiketoiminnan keskeytysvaikutusanalyysin tavoitteena on selvittää eri riskien liiketoiminnalle aiheuttamat vaikutukset, jotta tunnistetaan liiketoiminnalle kriittisimmät osa-alueet ja valitaan oikeat toimintatavat niiden jatkuvuuden turvaamiseen ja ongelmatilanteista toipumiseen. Keskeytysvaikutusanalyysin tekemisessä hyödynnetään jo aiemmin laadittuja prosessikuvauksia sekä riskianalyyseja. Keskeytysvaikutusanalyysin lopputuloksena on organisaation toimintaan vaikuttavat toiminnot laitettu tärkeysjärjestykseen sen mukaan, mitkä voivat aiheuttaa eniten vahinkoa liiketoiminnalle mahdollisissa ongelmatilanteissa. Toimintojen kriittisyyttä määriteltäessä otetaan huomioon liiketoiminnan sietämä enimmäiskatkoaika, häiriön vaikutukset tuottavuuteen, taloudelliset vaikutukset, mahdolliset säädöksistä johtuvat vastuut sekä organisaation maine. (Iivari & Laaksonen 2009, 138–140.)

Keskeytysvaikutusanalyysin tekeminen on tärkeää, jotta tunnistetaan oikeasti liiketoiminnalle kriittiset prosessit ja järjestelmät. Mikäli analyysia ei ole tehty, saattaa kriittisiksi valikoitua prosesseja tai järjestelmiä väärien syiden takia, kuten esimerkiksi ne, jotka ovat tutuimpia, uusimpia, helpoimpia tai johdon suosimia. Kaikkia prosesseja ja

järjestelmiä ei yleensä kuitenkaan voida sisällyttää toipumissuunnitelmaan, koska se vaatisi resursseja ja aikaa enemmän kuin on järkevää käyttää. Tämän vuoksi onkin tärkeää, että toipumissuunnitelmassa on mukana nimenomaan liiketoiminnan jatkuvuuden kannalta tärkeimmät järjestelmät. (Gregory 2008, 51–53.)

Keskeytysvaikutusanalyysin perusteella organisaatiossa voidaan pohtia, millaisia liiketoiminnan jatkuvuutta varmistavia toimenpiteitä on kannattavaa käyttää. Jatkuvuuden turvaamiseksi tehtävien toimenpiteiden tulisi olla järkevässä suhteessa riskien liiketoiminnalle aiheuttamiin vaikutuksiin. Mikäli keskeytysvaikutuksen perusteella todetaan jonkin toiminnon olevan välttämätöntä liiketoiminnalle, kannattaa siihen panostaa enemmän kuin sellaisten riskien ennaltaehkäisyyn, joiden vaikutukset eivät ole niin suuret. (Iivari & Laaksonen 2009, 140–142.)

3.6 Suunnitelman rungon laatiminen

Laadittaessa jatkuvuussuunnitelmaa tehdään ensin strategisen tason suunnitelma, jonka perusteella laaditaan operatiivisen tason suunnitelma. Strategisessa suunnitelmassa määritellään, mitä operatiivisen tason jatkuvuussuunnitelmia aletaan toteuttaa ja mitä toimintoja palautetaan ensimmäiseksi ongelmatilanteessa. (Iivari & Laaksonen 2009, 152.)

Jatkuvuussuunnitelmia laadittaessa kannattaa ensin suunnitella mallirunko, johon varsinainen suunnitelma rakentuu. Iivari & Laaksosen (2009, 153–156) mukaan jatkuvuussuunnitelma voi rakentua esimerkiksi seuraavista tiedoista:

- versionhallintatiedot
- tavoite ja rajaukset
- riskienhallinta ja riskianalyysi
- liiketoiminnan keskeytysvaikutusanalyysi
- jatkuvuuden turvaaminen
- toipumissuunnitelmat
- toipumisryhmän vastuut ja tehtävät
- yhteystiedot
- jatkuvuussuunnitelman testaaminen
- koulutus
- jatkuvuussuunnitelman ylläpito.

Kun suunnitelma on laadittu, tulee se julkaista sellaisessa muodossa, jossa se on toipumisryhmän käytettävissä tarpeen vaatiessa. Toipumissuunnitelma ei voi olla vain yrityksen intranetissä tai tiedostopalvelimella, koska katastrofin sattuessa nämä saattavat olla pois käytöstä. Toipumissuunnitelman tulisikin siis olla useammassa eri muodossa ja eri paikoissa, jotta se on helposti saatavilla tarpeen vaatiessa. (Gregory 2008, 24.)

4 JATKUVUUS- JA TOIPUMISSUUNNITELMIEN TESTAAMINEN JA YLLÄPITO

Jatkuvuussuunnitelma tulisi laatia niin, että se sisältää olennaiset tiedot, mutta ei liikaa yksityiskohtia. Liian monimutkainen tai laaja suunnitelma vaikeuttaa sen noudattamista kriisitilanteissa sekä sen päivittämistä. Jatkuvuussuunnitelma tulisi käydä läpi ja tarvittaessa päivittää säännöllisesti, esimerkiksi vuoden välein, tai aina silloin, kun esimerkiksi liiketoimintaympäristössä, liiketoimintaprosesseissa, organisaatiossa, tietojärjestelmissä tai vastuuhenkilöissä tapahtuu jonkinlaisia muutoksia. Suunnitelmaa tulee päivittää vastaamaan tapahtuneita muutoksia, sillä muuten suunnitelma antaa kuvan ainoastaan sen laatimishetken tilanteesta eikä enää välttämättä päde muutosten jälkeisissä tilanteissa. Suunnitelman päivittäminen tulisi osoittaa selkeästi tietyille vastuuhenkilöille, jotta se varmasti tulee hoidettua asianmukaisesti. (Iivari & Laaksonen 2009, 156–157.)

4.1 Toipumissuunnitelman testaaminen

Pelkät kirjalliset suunnitelmat eivät auta organisaatiota millään tavalla, elleivät ne toimi myös käytännössä. Jatkuvuus- ja toipumissuunnitelmia tulisi myös testata, jotta vastuuhenkilöt osaavat toimia oikein mahdollisissa häiriötilanteissa. Suunnitelmia testatessa voidaan myös varmistua siitä, että niissä ilmaistut toimenpiteet ovat tarkoituksenmukaisia eikä yrityksessä ole tuhlattu rahaa vääriin asioihin. Mikäli suunnitelmassa huomataan puutteita tai virheitä kriisitilanteen sattuessa, on se jo liian myöhäistä ja liiketoiminnalle on saattanut aiheutua huomattaviakin tappioita, jotka olisi voitu välttää suunnitelman testaamisella etukäteen. (Toigo 2003, 424–425.)

Testaamisessa ei riitä pelkästään teoreettinen testaus vaan se tulee toteuttaa konkreettisesti esimerkiksi laajana katastrofiharjoituksena tai pienemmissä osissa. Testauksessa tulisi selvittää muun muassa onko suunnitelmassa käsitelty kaikki tarpeelliset asiat, onko vastuut määritelty tarpeeksi selkeästi ja kattavasti sekä onko suunnitelmassa määritellyt resurssit riittävät ja kohdistettu oikein. (Miettinen 2002, 193.) Jotta testaukset tulee tehtyä säännöllisesti, kannattaa sitä varten laatia kirjallinen aikataulu, johon kirjataan suoritettavien testien määrä, tyyppi sekä ajankohdat (Iivari & Laaksonen 2009, 189).
Ennen toipumissuunnitelman testaamista asetetaan testaukselle tavoitteet, joiden tulee olla tarpeeksi rajatut: esimerkiksi testataanko koko toipumissuunnitelma vai jokin tietty

järjestelmä. Lisäksi määritetään tietyt olettamukset, joiden mukaan testausta lähdetään toteuttamaan, kuten onko kyseessä esimerkiksi tulipalo pääjakamossa vai koko toimitilan tuhoutuminen, ovatko kaikki toipumisryhmän jäsenet tavoitettavissa testitilanteen aikana sekä testataanko kaikkien tietojen palauttamista vai ainoastaan joidenkin tiettyjen. Testitulosten pitäisi olla ainakin osittain mitattavissa, esimerkiksi kauan tietojen palauttamisessa kestää tai kuinka nopeasti tietyt prosessit saadaan jälleen toimintaan katastrofitilanteen jälkeen. (Sandhu 2002, 173–175)

Tämän jälkeen suunnitellaan käytettävät testitavat. Erilaisia tapoja suunnitelmien testaamiseen ovat esimerkiksi työpöytätarkastus, strukturoitu läpikäynti, simulointi, rinnakkaistestaus ja täyskeskeytys. Kaikkein helpoin testaustapa on työpöytätarkastus, joka tarkoittaa lähinnä suunnitelman sisällön arviointia: onko suunnitelmassa otettu huomioon kaikki organisaation tärkeimmät toiminnot ja järjestelmät ja ovatko vastuuhenkilöt ja yhteystiedot ajan tasalla. Työpöytätarkastus voidaan tehdä esimerkiksi suunnitelman päivityksen tai auditoinnin yhteydessä, mutta kuitenkin vähintään kerran vuodessa. (Iivari & Laaksonen 2009, 195–196.)

Strukturoidussa läpikäynnissä käydään järjestyksessä läpi koko suunnitelman sisältö ja testataan tarkistettavien asioiden, yhteystietojen jne. ajantasaisuus. Osana strukturoitua läpikäyntiä tehdään myös työpöytätarkastukseen kuuluvat tarkastukset suunnitelman kattavuudesta. Strukturoitu läpikäynti tulisi tehdä vähintään kerran vuodessa, ja siinä ovat mukana kaikki suunnitelmaan kirjatut vastuuhenkilöt sekä palautustilanteisiin merkityt henkilöt. Strukturoitu läpikäynti on organisaation tärkeimpiä jatkuvuus- ja toipumissuunnitelman testaustapoja, sillä sen tuottama hyöty on suuri verrattuna testaukseen kuluvaan aikaan ja käytettyihin resursseihin, eikä se myöskään aiheuta liiketoiminnan keskeytyksiä. (Iivari & Laaksonen 2009, 196–197.)

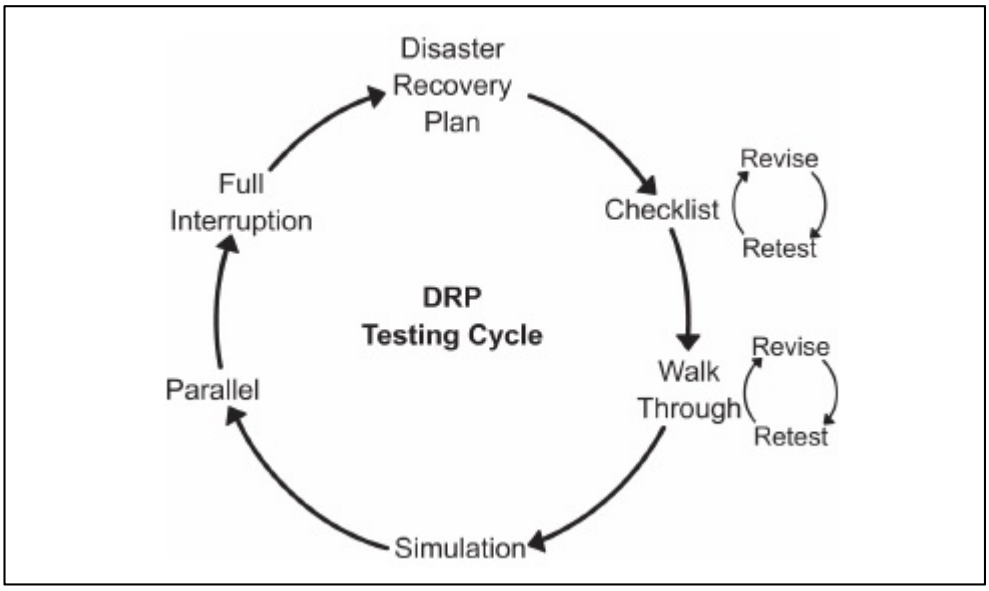
Simuloinnissa käydään läpi kaikki suunnitelmaan kuuluvat toimenpiteet kuitenkaan keskeyttämättä liiketoimintaa. Testitilanteina kannattaa käyttää riskienhallinnassa tunnistettuja uhkia varioiden niitä eri testitilanteissa. Jokaisessa testitilanteessa tulee olla testin vetäjä sekä sihteeri, joka pitää kirjaa testitilanteen kulusta ja siitä, miten testiryhmän jäsenet tuntevat ryhmän vastuut ja oman roolinsa ryhmän jäsenenä. Sihteeri laatii muistiinpanojensa perusteella pöytäkirjan, joka analysoidaan toipumisryhmän kesken. Pöytäkirjan analysoinnilla pyritään havaitsemaan jatkuvuus- tai toipumissuunnitelman kehitys- ja

ylläpitotarpeet sekä tekemään suunnitelma niiden toteuttamiseksi. (Iivari & Laaksonen 2009, 197.)

Rinnakkaistestaus tarkoittaa sitä, että yksittäisen toiminnon tai prosessin jatkuvuutta testataan rinnakkain normaalin toiminnan kanssa esimerkiksi huoltokatkon aikana. Testauksesta ei tällöin aiheudu haittaa liiketoiminnalle, koska testauksen kohteena olevat liiketoiminnot hoidetaan jonkin muun organisaatioyksikön toimesta tai huoltokatko on suunniteltu ennalta pidettäväksi sellaisena ajankohtana, jolloin sen vaikutukset liiketoiminnalle ovat mahdollisimman vähäiset. Rinnakkaistestausta ei välttämättä tarvitse tehdä kovin usein, kerran vuodessa tai jopa harvemmin riittää. Mutta mikäli huoltokatko on suunniteltu pidettäväksi, kannattaa se toki käyttää hyödyksi ja testata samalla myös jatkuvuussuunnitelman toimivuutta. Rinnakkaistestaus on erityisen hyödyllinen tapa otettaessa käyttöön uusia IT-järjestelmiä. (Iivari & Laaksonen 2009, 198.)

Testaustavoista laajin ja myös vaativin on täyskeskeytys, jossa liiketoiminnan osa keskeytetään kokonaan jatkuvuussuunnitelman testaamista varten. Täyskeskeytystä ei kannata tehdä kovin usein, korkeintaan kerran vuodessa. Tällöinkin täyskeskeytys kannattaa tehdä liiketoiminnan kannalta hiljaisena aikana, varavirtalaitteistojen testauksen yhteydessä tai otettaessa käyttöön uusi toimipaikka tai IT-laitetila. Täyskeskeytyksessä on aina omat riskinsä, sillä liiketoimintaa palautettaessa tulee aina ottaa huomioon mahdolliset ongelmat, joiden vuoksi toiminnan jatkaminen ei onnistukaan aivan suunnitelmien mukaisesti.

Kaikkein parhaimmat tulokset saadaan, kun suunnitelma testataan syklissä useita kertoja erilaisia testaustapoja käyttäen. Kunkin testivaiheen jälkeen suunnitelma arvioidaan uudelleen ja siihen tehdään tarvittavat muutokset ennen kuin siirrytään seuraavaan vaiheeseen. Testit monipuolistuvat aina seuraavaan vaiheeseen siirryttäessä, mikä on esitetty kuviossa 3. Kun kaikki testit on suoritettu, raportoidaan tulokset kirjallisesti ja jos tarpeen, esitetään vielä muutosehdotuksia toipumissuunnitelman parantamiseksi. (Sandhu 2002, 169–170.)



KUVIO 3. Toipumissuunnitelman testaussykli (Sandhu 2002, 170)

4.2 Toipumissuunnitelman ylläpito

Toipumissuunnitelman laatimisen jälkeen sitä ei saa unohtaa siihen saakka kunnes sitä mahdollisesti joskus tarvitaan, vaan suunnitelmaa tulee ylläpitää aktiivisesti, jotta se pysyy ajantasaisena ja siitä on mahdollisessa ongelmatilanteessa oikeasti hyötyä. Toipumissuunnitelma tulee päivittää aina, kun yrityksen liiketoimintaprosesseissa tai niitä tukevissa tietojärjestelmissä tapahtuu muutoksia. Toipumissuunnitelman ylläpitoa voi toteuttaa joko säännöllisten testausten tai muutostenhallinnan avulla. (Sandhu 2002, 177.) Ja jotta toipumissuunnitelman päivittäminen saadaan varmistettua, tulee sillä olla nimetty omistaja tai vastuuhenkilö, joka on myös mukana toteuttamassa toipumissuunnitelmaa mahdollisen vahingon sattuessa (Doughty 2000, 263).

Yrityksen liiketoimintaprosessit ja it-infrastruktuuri voivat muuttua henkilöstön, tiedon ja ohjelmistojen, rakennusten, järjestelmien ja laitteistojen tai viestintäyhteyksien muutosten vuoksi. Yrityksen tietovaatimukset muuttuvat usein ja tietokannat päivittyvät säännöllisesti. Tietokantojen koko kasvaa koko ajan samoin kuin tiedon lisääntyessä myös niiden arvo. Tämän vuoksi myös tiedon varastointi ja varmistus sekä niihin käytettävät laitteistot tulee pitää vaatimusten tasalla koko ajan. (Sandhu 2002, 178.)

Yrityksen ohjelmistomuutokset tulee yleensä myös päivittää toipumissuunnitelmaan, sillä vaikka ne eivät vaikuttaisikaan suoranaisesti toipumistoimenpiteisiin, vaikuttavat ne

monesti suunnitelmaan jollain tavalla. Ohjelmistomuutokset saattavat esimerkiksi vaatia käyttöjärjestelmäpäivityksiä ja mikäli samalla myös niiden muistin tarve kasvaa, saattavat ne vaatia laitepäivityksiä tai laitteistoja saatetaan joutua vaihtamaan esimerkiksi laitteiden rikkoutumisen vuoksi. Mikäli yrityksellä on varmistuskeinona varajärjestelmä eli ns. hot site mahdollisia katastrofitilanteita varten, tulee tarvittavat laite- ja ohjelmistomuutokset tehdä myös sinne, jotta yrityksen toimintoja pystytään tarvittaessa pyörittämään siellä. (Sandhu 2002, 179–180.)

Yrityksen henkilöstössä tapahtuvat muutokset tulee myös päivittää toipumissuunnitelmaan, mikäli he ovat osallisina toipumistoimenpiteissä mahdollisen katastrofin jälkeen. Heidän roolinsa toipumisprosessissa tulee määrittää ja perehdyttää heidät prosessin kulkuun. Toipumisryhmän jäsenten yhteystietojen tulee myös aina olla ajan tasalla toipumissuunnitelmassa. (Sandhu 2002, 180.)

Mitä tahansa muutoksia tapahtuukin, tulee ajantasaiset tiedot päivittää myös kaikkiin tarvittaviin dokumentteihin ja varmistaa, että katastrofitilanteen varalta ajantasaiset dokumentit on toimitettu kaikkiin tarpeellisiin paikkoihin ja vanhentuneet tiedot on hävitetty. Tämä koskee niin yrityksen omissa prosesseissa, laitteissa, ohjelmistoissa tai henkilöstössä kuin ulkopuolisten toimittajien yhteystiedoissakin tapahtuvia muutoksia. Tämän varmistamiseksi tulee toipumissuunnitelman päivittämisestä vastuussa olevan henkilön saada ajantasainen tieto kaikista yrityksen toimintaan vaikuttavista muutoksista. On siis tärkeää että hänen ja tiimien vetäjien, osastopäälliköiden ja johtajien välinen yhteydenpito on säännöllistä ja sujuvaa. (Sandhu 2002, 179–181.)

4.3 Toipumissuunnitelman säilytys

Jatkuvuus- ja toipumissuunnitelmien säilytykseen tulee myös kiinnittää huomiota, jotta ne ovat helposti saatavilla kriisin sattuessa. Suunnitelmien tulee olla vähintään kahdessa fyysisesti eri paikassa, kuten organisaation päätoimitiloissa, strategisesti tärkeässä paikassa, kuten laitetilassa tai tärkeässä sivukonttorissa sekä mahdollisessa arkistossa, jossa säilytetään muitakin organisaation tärkeitä asiakirjoja ja varmuuskopioita. (Iivari & Laaksonen 2009, 157.)

5 TOIMINTA KRIISITILANTEESSA

Kriisitilanteissa toimimiseen kuuluvat juuri ennen toipumissuunnitelman täytäntöönpanoa toteutettavat sekä toipumissuunnitelman mukaiset toimenpiteet. Ennen toipumissuunnitelman täytäntöönpanoa tulee huolehtia sattuneen katastrofin edellyttämistä toimenpiteistä, kuten ihmisten turvaan saattamisesta ja esimerkiksi tulipalon sammuttamisesta. Tämän jälkeen aletaan toteuttaa toipumissuunnitelman mukaisia toimenpiteitä ja pyritään palauttamaan liiketoimintakyky mahdollisimman nopeasti. (Iivari & Laaksonen 2009, 202.)

Iivari ja Laaksosen (2009, 204.) mukaan katastrofitilanteesta toipuminen sisältää seuraavat vaiheet:

- tilanteen tunnistaminen
- toipumissuunnitelmaa toteuttavan työryhmän koollekutsuminen
- katastrofitilanteesta aiheutuneiden vahinkojen määrän ja laadun kartoitus sekä niiden liiketoimintavaikutusten mahdollinen rajoittaminen
- yksityiskohtaisempi vahinkojen määrän arviointi muun muassa omaisuuden, tilojen, järjestelmien ja dokumenttien osalta
- palautumissuunnitelman valmistelu, halutun palautumistilan määrittäminen ja palautumisprosessin etenemisen valvonta
- tilanteesta informointi kaikille tarpeellisille osapuolille
- toimintojen palauttaminen niiden normaalille johdolle liiketoiminnan palautuessa normaalitilaan
- palautumisprosessin raportointi, analysointi sekä jälkihoito.

Toipumissuunnitelmaa toteuttaa ennalta määritelty toipumisryhmä, joka tulee kutsua koolle heti katastrofitilanteen huomaamisen jälkeen. Toipumisryhmä aloittaa toipumisprosessin kartoittamalla katastrofin aiheuttamat vahingot sekä estämällä lisävahinkojen syntymisen mahdollisesti yhteistyössä viranomaisten kanssa ja heidän ohjeitaan noudattaen. Kartoitusvaiheessa on erityisen tärkeää erottaa nimenomaan organisaation ydinliiketoiminalle aiheutuneet vahingot ja keskittyä niihin. (Iivari & Laaksonen 2009, 204.)

6 TOIMENPITEITÄ TIETOHALLINNON JATKUVUUDEN VARMISTAMISEKSI

Monet liiketoimintaprosessit ovat nykyään riippuvaisia erilaisista tietojärjestelmistä ja mahdollisiin häiriötilanteisiin tulisi varautua jo ennalta, jotta liiketoimintaa pystyttäisiin jatkamaan myös häiriöiden aikana tai ainakin mahdollisimman nopeasti niiden jälkeen. Häiriöihin voidaan varautua ennalta jo monin eri keinoin esimerkiksi teknisten tai muiden toimenpiteiden tai kaupallisten sopimusten avulla. (Iivari & Laaksonen. Tallinna 2009. s. 159–160.)

6.1 Palvelinympäristön varmistaminen monistamalla

Jotta tietojärjestelmien käytettävyys voitaisiin taata mahdollisimman hyvin, on niitä rakennettaessa huomioitava vikasietoisuus ja korkea käytettävyys. Tämä voidaan toteuttaa esimerkiksi varajärjestelmillä ja laitteistoilla, jolloin pääjärjestelmän vikaantuessa ottaa varajärjestelmä sen tehtävät hoitaakseen. Päällekkäisiä tai ylimääräisiä laitteita kutsutaan redundanssiksi ja se voi olla passiivista tai aktiivista. Passiivisessa redundanssissa varakomponentit otetaan käyttöön vasta pääjärjestelmän vikaantuessa ja järjestelmä palautetaan vikatilanteesta. Tällöin palvelu on yleensä pois käytöstä palautukseen kuluvan ajan. Aktiivisessa redundanssissa varakomponentit osallistuvat yleensä palvelun tuottamiseen koko ajan ja vikatilanteessa järjestelmän toiminta jatkuu niiden avulla, jolloin käyttäjä ei edes huomaa vikatilannetta. (Iivari & Laaksonen. Tallinna 2009. s. 167–168.)

Tietojärjestelmien käytettävyyden varmistamiseksi voidaan palvelinlaitteistot esimerkiksi kahdentaa tai klusteroida. Kahdennuksessa palvelinten mekaaniset osat sekä ohjelmistot monistetaan, jolloin palvelimen toiminnan keskeytyessä sen tehtävät ottaa hoitaakseen varapalvelin. Kahdennuksella pyritään takaamaan käyttäjille häiriötön palvelu ja mahdollisimman nopea palautuminen vikatilanteesta, vaikka palvelimen vaihtuessa yleensä pieni käyttökatkos käyttäjille tuleekin. Kahdennus aiheuttaa yritykselle lisäkustannuksia, mutta se on varteenotettava vaihtoehto, kun kyseessä on liiketoiminnan kannalta kriittinen järjestelmä, jonka tulisi olla käytettävissä ympäri vuorokauden ilman katkoja. (Iivari & Laaksonen. Tallinna 2009. s. 169.)

Paras käytettävyyden varmistaminen saadaan aikaiseksi silloin, kun vikatilanteessa pääasiallisen palvelimen ja varapalvelimen välinen vaihto saadaan toteutettua täysin automaattisesti ja käyttäjien huomaamatta. Tällöin tarvitaan kahdennuksen lisäksi klusterointia, jolla tarkoitetaan palvelinten sisältämän tietojen reaaliaikaista ja kahdensuuntaista varmentamista. Klusteroinnissa useampi palvelin toimii yhtäaikaisesti jakaen palvelun kuormaa. Vikatilanteessa toimiva palvelin ottaa koko tehtävän hoitaakseen ja palvelu pysyy koko ajan käyttäjien käytettävissä ilman katkoja. Tilanteen korjaannuttua kopioituvat katkon aikana tapahtuneet muutokset automaattisesti korjattuun palvelimeen. (Iivari & Laaksonen. Tallinna 2009. s. 169–170.)

Levyjärjestelmien ollessa kyseessä levyjärjestelmän klusteroinnista puhutaan peilauksena. Peilaukseksi kutsutaan saman datan tallentamista useammalle levylle, jolloin yhden levyn hajoaminen ei hävitä tärkeää dataa. Peilausta käytetään erityisesti silloin, kun levyjärjestelmän vasteaika tai virheettömyys sekä tietojen säilyminen on tärkeää. Levy on mahdollista vaihtaa myös palvelinta sammuttamatta, jonka jälkeen levylle tallennetaan rikkoutuneen levyn data ilman, että mitään siitä on menetetty. Näin tieto on koko ajan palvelun käytettävissä eivätkä käyttäjät huomaa katkosta laisinkaan. (Iivari & Laaksonen. Tallinna 2009. s. 171.)

6.2 Virtualisointi

Virtualisoinnilla voidaan yksi fyysinen resurssi saada näkymään useana loogisena resurssina, jolloin sitä kutsutaan myös osioinniksi, tai päinvastoin useat fyysiset resurssit saada näkymään yhtenä loogisena resurssina. Virtualisointia hyödynnetään usein laskenta- ja tallennuskapasiteetin lisäämisessä, mutta myös ohjelmia ja laitteita voidaan virtualisoida. (Iivari & Laaksonen. Tallinna 2009. s. 175.)

Virtualisoinnin avulla voidaan saada fyysisen resurssin, kuten palvelimen, kapasiteettia hyödynnettyä paremmin, parannettua sen viansietokykyä, helpottamaan sen hallinnointia ja uudelleenasennuksia sekä säästämään energiaa ja kustannuksia (Ranta 2011). Esimerkiksi rakennuspalveluita tarjoavan Staran tietohallintojohtaja Jari Kähkölän mukaan 310 työaseman vaihtaminen virtualisoituihin kevytpäätteisiin säästää vuodessa pelkästään sähkökuluissa n. 10 000 euroa. Lisäksi kevytpäätteen käyttöikä on arviolta noin puolet perinteistä työasemaa pidempi eli jopa kuusi vuotta. (Kolehmainen. 2014)

6.3 Virransaannin varmistaminen

Tietojärjestelmät sekä erityisesti niiden jäähdyttämiseen tarkoitetut laitteistot kuluttavat paljon sähköä, mikä tarkoittaa sitä, että virransaanti on taattava myös vikatilanteissa tai ainakin järjestelmät olisi hyvä saada ajettua alas hallitusti sähkökatkon aikana. Jo rakennusvaiheessa kannattaa sähkönjakelun suunnittelussa huomioida virransaanti sekä mahdollinen varavoiman tarve. Mikäli mahdollista, olisi IT-tiloihin hyvä tuoda sähkö kahden erillisen reitin kautta ja jopa kahdesta erillisestä lähteestä. (Iivari & Laaksonen. Tallinna 2009. s. 172.)

Lyhytkestoisesti varavirtaa saadaan esimerkiksi UPS-laitteesta. UPSin paikka on sähkölaitteen ja sähköverkon välissä ja jos sähkönsyöttö keskeytyy tai jännite on epätasaista, saa laite sähköä UPSin akkujen kautta. UPSin turvaaman sähkönsyötön aika riippuu sen akkujen koosta ja siinä kiinni olevien laitteiden määrästä, mutta yleensä se on alle kaksi tuntia. (Iivari & Laaksonen. Tallinna 2009. s. 173.)

Mikäli tarvetta on myös pidempiaikaiseen sähkönsyöttöön, kannattaa silloin harkita erillisen varavoimalaitteiston, kuten generaattorin, hankkimista. Dieselsähkögeneraattori muuttaa polttoaineella tuotetun mekaanisen liike-energian sähkövirraksi. Mikäli generaattorien yhteyteen saadaan liitettyä polttoainetankit, voidaan niiden avulla taata virransaanti jopa viikoksi. Dieselsähkögeneraattorit ovat nykyään luotettavia ja varmoja sähkönsyöttäjiä ja lisälaitteiden avulla niitä voidaan hallinnoida etänä esimerkiksi matkapuhelimen välityksellä. (Iivari & Laaksonen. Tallinna 2009. s. 173–174).

6.4 Verkkoyhteyksien varmistaminen

Virransaannin ohella ovat tietoliikenneyhteydet järjestelmien käytettävyyden kannalta merkittävässä roolissa. Mikäli verkkoyhteys katkeaa, ovat järjestelmät tavoittamattomissa, vaikka palvelin ja järjestelmä itsessään olisivatkin kunnossa. Virransaanti voidaan varmistaa omilla varavoimalähteillä, mutta verkkoyhteyksien suhteen ollaan toisten organisaatioiden varassa. Poikkeuksena on organisaation sisäinen tietoverkko, mikäli se ei ole riippuvainen internetverkosta. (Iivari & Laaksonen. Tallinna 2009. s. 182.)

Yleensä ongelmia tietoliikenteen kanssa aiheuttavat yhteys internetiin tai verkon DNS-nimipalvelut. Internetyhteyden varmistamiseksi olisi hyvä kahdentaa verkkoyhteys käyttäen kahta eri reittiä ja kahta eri palveluntarjoajaa. Molempien ei tarvitse olla yhtä tehokkaita yhteyksiä, vaan riittää, että tietoliikenneyhteyttä käyttävät järjestelmät on priorisoitu ja varayhteyden avulla pystytään hoitamaan kriittisimpien järjestelmien yhteydet. (Iivari & Laaksonen. Tallinna 2009. s. 183–184.)

6.5 Tietojen varmistaminen ja palauttaminen

Olennainen osa yritysten jatkuvuussuunnittelua on tietojen varmistaminen. Sillä tarkoitetaan tietojen kopioimista jollekin toiselle tallennusmedialle, kuten nauhalle. Varmistuksella tarkoitetaan yleisesti sähköisiä varmistustapoja, mutta varmistusta voi myös olla tietojen tulostaminen tai kirjaaminen paperille ja niiden säilyttäminen arkistossa, kuten toimitaan esimerkiksi kuittien kanssa. Mikäli levyjärjestelmä on rakennettu peilattuna, kopioituu sama tieto automaattisesti kahdelle tai useammalle levylle, mutta sekään ei poista varsinaisen varmistuksen tarvetta. (Iivari & Laaksonen. Tallinna 2009. s. 177.)

Sopivien varmistustapojen valintaan vaikuttavat tietojen sijainti, määrä ja tyyppi sekä elinkaari, mahdolliset lakisääteiset velvoitteet, varmistusajojen vaikutus järjestelmien käytettävyyteen ja niiden aikataulutus sekä auditoitavuus. Varmistusten tulisi aina sijaita eri tilassa kuin varmistettavat järjestelmät, jolloin molemmat eivät tuhoudu samalla kertaa esimerkiksi tulipalossa. Varmistusaikatauluihin vaikuttaa se, kuinka tuoreen varmistuksen palauttaminen on tarpeellista mahdollisessa toipumistilanteessa, sillä edellisen varmistuksen ja ongelmatilanteen väliset tiedot menetetään. (Iivari & Laaksonen. Tallinna 2009. s. 177–178.)

Otettava varmistus voi olla täysvarmistus, jolloin järjestelmän kaikki tiedot kopioidaan, tai inkrementaalinen, jolloin varmistetaan ainoastaan edellisen varmistuksen jälkeen muuttuneet tiedot. Inkrementaalisen varmistuksen hyötyjä ovat varmistustilan ja varmistukseen kuluvan ajan säästäminen, mutta palautuksessa se tarkoittaa, että ensin on palautettava järjestelmän täysvarmistus ja sen jälkeen muuttuneet tiedot kaikilta täysvarmistuksen jälkeisiltä inkrementaalivarmistuksilta. (Iivari & Laaksonen. Tallinna 2009. s. 178.)

Jotta varmistuksista on hyötyä, tulee myös varmistua siitä, että tiedot saadaan palautettua oikein. Tämä voidaan todeta testaamalla, että varmistettavat tiedot siirtyvät varmistusmedialle oikein, järjestelmään on mahdollista palauttaa joko kaikki tai jokin yksittäinen tieto ja varmistetut tiedot myös toimivat palautetussa järjestelmässä. Testaus tulisi suorittaa varmistamalla ja palauttamalla kaikki tieto vähintään kerran vuodessa, jolloin sitä voidaan hyödyntää myös toipumissuunnitelman testaustilanteena sekä valmiusryhmän koulutus- ja harjoittelutilanteena. Testauksessa saadaan selvitettyä myös, mikä on järjestelmän todellinen toipumisaika. (Iivari & Laaksonen. Tallinna 2009. s. 180–181.)

Palauttamisessa tarvitaan varmistettujen tietojen lisäksi myös järjestelmä, johon tiedot palautetaan, sekä mahdolliset tukijärjestelmät. Mikäli kyseessä on esimerkiksi laiterikko, jonka vuoksi alkuperäiset tiedot ovat hävinneet, tarvitsee ensin rakentaa laiteympäristö, ellei valmiina ole toimintakuntoista varalaitetta. Tämän jälkeen asennetaan tarvittavat sovellukset joko varmistuksista, levykuvista eli imageista tai alkuperäisistä asennustiedostoista. Tämän jälkeen palautetaan sovelluksen tiedot varmistusmedioilta. (Iivari & Laaksonen. Tallinna 2009. s. 181–182.)

Kaikkien edellä mainittujen varmistuskeinojen lisäksi tulee huolehtia myös laitteiston varmistuksista ja valvonnasta. Tämä voidaan varmistaa esimerkiksi laitetoimittajien kanssa tehtävillä huoltosopimuksilla, joissa määritellään tarvittavat määräaikaishuollot ja valvontapalvelut. Sopimuksiin voidaan sisällyttää myös toimittajan velvollisuus varautua ongelmatilanteisiin tiettyjä varaosia säilyttämällä tai palvelutasovaatimuksilla, jolloin toimittajan vastuulla on saada hankittua tarvittavat varaosat ja saada järjestelmä kuntoon tiettyjen vasteaikojen rajoissa. Näissä on kuitenkin huomioitava, onko varmuus riittävä ja korvaako toimittajan sopimuksessa oleva sanktio mahdolliset viivästykset ja menetykset omalle liiketoiminnalle. (Iivari & Laaksonen. Tallinna 2009. s. 185–186.)

Yritys voi varautua laiterikkoihin myös hankkimalla itselleen tiettyjä varaosia, mikä saattaa olla järkevää esimerkiksi sellaisten laitteiden kohdalla, joiden varaosien saaminen on hankalaa esimerkiksi vanhentuneen laitekannan vuoksi. Silloin täytyy kuitenkin huomioida varaosien oikeanlainen säilytys sekä säilymisaika. Yritys voisi varautua katastrofitilanteisiin myös varalaitetilalla, jolla voitaisiin korvata esimerkiksi tulipalossa palanut pääjakamo. Varalaitetilan tarve ja sen tuomat hyödyt on kuitenkin mietittävä tarkkaan, sillä monessakaan tapauksessa ei ole järkevää tai kustannustehokasta pitää kokonaista

laitetilaa kunnossa vain mahdollisen katastrofin varalta. Järkevämpää on suunnitella yrityksen infrastruktuuri ja it-ympäristö siten, että kriittisimmät järjestelmät on kahdennettu ja hajautettu kahteen fyysisesti erillään sijaitsevaan tilaan, jotka ovat aktiivisessa käytössä koko ajan, mutta joista toisen avulla saadaan tarvittaessa pidettyä liiketoiminnan kannalta olennaiset järjestelmät käynnissä myös toisen vikaannuttua tai tuhouduttua. (Iivari & Laaksonen. Tallinna 2009. s. 186–187.)

7 TOIPUMISSUUNNITELMAN LAATIMINEN TAMPEREEN SÄRKÄNNIEMI OY:N TIETOHALLINNOLLE

Toipumissuunnitelman laatiminen alkoi tutustumalla aihetta käsittelevään kirjallisuuteen ja kartoittamalla, löytyykö valmiita toipumissuunnitelmapohjia, joita voisi hyödyntää suunnitelman laatimisessa. Toipumissuunnitelmapohjia löytyi useita erilaisia ja niistä valittiin kaksi sopivimmaksi arvioitua, joiden pohjalta laadittiin Särkänniemen toipumissuunnitelman runko. Toipumissuunnitelman laatimista vaikeutti se, että toipumissuunnitelmat ovat yritysten salaisia dokumentteja, joten valmiisiin suunnitelmiin tutustuminen ei ollut mahdollista.

Työn aluksi kartoitettiin Särkänniemen tietojärjestelmien nykytilanne, laitteiston sijoittelu, käytössä olevat varmennusvälineet ja varalaitteistot sekä toimintatavat ja välineet, joilla on varauduttu onnettomuuksien ennaltaehkäisyyn. Seuraavaksi määriteltiin yrityksen liiketoiminnan kannalta tärkeimmät tietojärjestelmät ja niiden tärkeysjärjestys, jonka perusteella kirjattiin toipumissuunnitelmaan palauttamisen toimenpiteet ja missä järjestyksessä ne toteutetaan.

Pääsääntöisesti toipumissuunnitelma on tarkoitettu isojen katastrofien varalle, mutta koska esimerkiksi suuret luonnonkatastrofit ovat Suomessa harvinaisia, on Särkänniemen toipumissuunnitelma laadittu siten, että sitä voidaan hyödyntää myös pienemmissä vahinkotilanteissa. Esimerkit eriasteisista vahinkotilanteissa ja niissä tehtävistä toipumistoimenpiteistä on kuvattu kunkin järjestelmän kohdalla erilaisissa skenaarioissa.

7.1 Toipumissuunnitelman pohja

Erilaisia toipumissuunnitelmapohjia löytyi useita erilaisia. Useimmiten jokaisesta järjestelmästä oli tehty oma toipumissuunnitelmansa, mutta Särkänniemen toimintatapoihin soveltui paremmin se, että kirjoitetaan yksi toipumissuunnitelma, joka sisältää kaikki kriittiset tietojärjestelmät. Toipumissuunnitelmaan on sisällytetty perustiedot myös palvelimista ja verkkoyhteyksistä, sillä monet mahdollisista tietojärjestelmien ongelmista liittyvät niihin, mutta niiden tarkemmat tekniset kuvaukset on kirjattu muihin tietohallinnon dokumentteihin, jotka on mainittu toipumissuunnitelmassa.

Pohjana Särkänniemen toipumissuunnitelman laatimisessa on käytetty valtiokonttorin sekä valtiovarainministeriön toipumissuunnitelmapohjia, sillä niiden runko vaikutti selkeältä ja sisällössä oli huomioitu toipumisen kannalta olennaiset asiat. Suunnitelmapohjista on otettu mukaan Särkänniemen käytäntöihin ja tarpeisiin parhaiten sopivat kohdat ja Särkänniemen toipumissuunnitelman sisällysluettelosta tuli seuraavanlainen:

1. Johdanto
    1.1. Suunnitelman tarkoitus
    1.2. Versiohistoria ja suunnitelman päivittäminen
    1.3. Muut liittyvät dokumentit
2. Valmiusorganisaatio
    2.1. Vastuut toipumissuunnitelman käynnistämisestä ja toimenpiteistä
    2.2. Vastuuhenkilöiden hälyttäminen
    2.3. Organisaation yhteystiedot
    2.4. Päävastuuhenkilöt
    2.5. Muut vastuuhenkilöt
    2.6. Viestintä
        2.6.1. Toipumissuunnitelman viestintä
        2.6.2. Viestintä toipumistilanteen aikana
3. Järjestelmä X
    3.1. Yhteystiedot
        3.1.1. Yritys X
        3.1.2. Yritys Y
    3.2. Tekninen kuvaus
        3.2.1. Palvelin
        3.2.2. Ohjelmisto
        3.2.3. Riippuvuudet muihin järjestelmiin
        3.2.4. Varmuuskopiot
        3.2.5. Asennuslevykkeet
    3.3. Toipumistoimenpiteet
        3.3.1. Toipumisen tavoiteaika
        3.3.2. Toipumisessa tarvittava tieto
        3.3.3. Toipumistoimenpiteiden käynnistäminen
        3.3.4. Toipumistoimenpiteet
            - Skenaario 1. Palvelimen uudelleenkäynnistys

- Skenaario 2. Laite hajoaa
- Skenaario 3. Tietokanta korruptoituu
- Skenaario 4. Palvelin vikaantuu/tuhoutuu

3.3.5. Varmuus- ja suojakopiointi ja käytön palauttaminen

3.3.6. Ohjeet laitteiden, ohjelmistojen, tiedostojen ja tarvikkeiden palauttamisesta

3.3.7. Normaalijärjestelmään palautumisen edellyttämät hankinnat, kunnostus- ja toimitus

3.3.8. Tiedottaminen ja asiakkaisiin liittyvät toimenpiteet

3.3.9. Toiminnan uudelleenkäynnistys ja tietojärjestelmien kunnostus

3.3.10. Järjestelmän testaus palautumisen jälkeen

3.4. Paluu normaaliin toimintaan

3.4.1. Toipumisenaikaiset toimenpiteet

3.4.2. Siivoustoimenpiteet

- Skenaario 1.
- Skenaario 2.
- Skenaario 3.
- Skenaario 4.

4. Järjestelmä Y

4.1. Yhteystiedot

4.1.1. Yritys Z

4.2. Tekninen kuvaus

4.2.1. Palvelin

4.2.2. Ohjelmisto

4.2.3. Riippuvuudet muihin järjestelmiin

4.2.4. Varmuuskopiot

4.2.5. Asennuslevykkeet

4.3. Toipumistoimenpiteet

4.3.1. Toipumisen tavoiteaika

4.3.2. Toipumisessa tarvittava tieto

4.3.3. Toipumistoimenpiteiden käynnistäminen

4.3.4. Toipumistoimenpiteet

- Skenaario 1. Palvelimen uudelleenkäynnistys
- Skenaario 2. Palvelin vikaantuu/tuhoutuu

4.3.5. Varmuus- ja suojakopiointi ja käytön palauttaminen

4.3.6. Ohjeet laitteiden, ohjelmistojen, tiedostojen ja tarvikkeiden palauttamisesta

4.3.7. Normaalijärjestelmään palautumisen edellyttämät hankinnat, kunnostus- ja toimitus
4.3.8. Tiedottaminen ja asiakkaisiin liittyvät toimenpiteet
4.3.9. Toiminnan uudelleenkäynnistys ja tietojärjestelmien kunnostus
4.3.10. Järjestelmän testaus palautumisen jälkeen
4.4. Paluu normaaliin toimintaan
4.4.1. Toipumisenaikaiset toimenpiteet
4.4.2. Siivoustoimenpiteet
…
9. Toipumissuunnitelman kopiot
10. Historia
10.1. Toipumissuunnitelman testaukset
10.2. Häiriöt

7.2 Tietojärjestelmien nykytilanne

Särkänniemessä on tehty vuosien varrella paljon töitä prosessien sujuvoittamiseksi ja tehostamiseksi tietojärjestelmiä hyödyntämällä. Viime aikoina on erityisesti alettu kiinnittää huomiota myyntiä tukeviin järjestelmiin ja muutaman vuoden sisällä on yrityksessä otettu käyttöön uusi kassajärjestelmä, verkkokauppa-alusta ja asiakkuuksienhallintajärjestelmä, ja parhaillaan on käynnissä varausjärjestelmän vaihto. Nykyään huomiota kiinnitetään entistä enemmän myös järjestelmien välisiin yhteyksiin ja sitä helpottamaan on tänä vuonna otettu käyttöön erillinen integraatiojärjestelmä. Esimerkiksi myynnin järjestelmät tulevat pääsääntöisesti olemaan kaikki yhteydessä kassajärjestelmään integraatiojärjestelmän kautta.

Särkänniemessä tietojärjestelmiä hyödynnetään kaikissa toiminnoissa. Esimerkiksi yrityksen sisäisessä viestinnässä käytetään sähköpostia ja intranetiä, työvuorot suunnitellaan työvuorosuunnittelujärjestelmässä, huollon vikailmoitukset käsitellään kunnossapitojärjestelmässä, asiakaspalautteet sekä toiminnan poikkeamat ja ideat käsitellään laadunvalvontajärjestelmässä ja kulunvalvonta hoidetaan oman tietojärjestelmän kautta. Tietojärjestelmät ja tietokoneet ovat siis tärkeitä työkaluja niin yrityksen liiketoiminnalle kuin lähes jokaiselle Särkänniemessä työskentelevälle ympärivuotiselle työntekijälle. Tämän

vuoksi onkin erittäin tärkeää, että tietojärjestelmien käytettävyys on mahdollisimman korkea.

7.2.1 Kriittiset tietojärjestelmät

Tässä opinnäytetyössä on keskitytty Tampereen Särkänniemi Oy:n liiketoiminnan kannalta keskeisimpiin tietojärjestelmiin, joita ovat kassajärjestelmä sekä taloushallinnon järjestelmät, joiden kautta kulkevat kaikki yrityksen rahavirrat eli korttimaksuista ja laskutuksesta saatavat tulot, maksettavat laskut, osto- ja myyntireskontra sekä palkanmaksuohjelmisto. (Paasikoski 2013.)

Kassajärjestelmä on kaikista tietojärjestelmistä kriittisin, sillä sen kautta yritys saa tulot Särkänniemen Elämyspuistossa tapahtuvasta myynnistä. Mikäli esimerkiksi maksupäätteet ovat pois käytöstä tietoliikenneyhteysongelmien vuoksi, voidaan tuotteita myydä käteismyynnillä. Tämä kuitenkin hankaloittaa asiakaspalvelua huomattavasti, sillä nykyään yleisimmin käytetty maksutapa on maksukortti. Särkänniemen alueella on yksi pankkiautomaatti, mutta rahat saattaisivat loppua siitä kesken ongelmatilanteen jatkuessa pidempään. Jos kassajärjestelmä on pois käytöstä eikä myyntejä pystytä syöttämään kassaan ostohetkellä, hidastuu asiakaspalvelu, koska myydyt tuotteet tulee kirjata käsin ylös ja kuittipakon mukaan asiakkaalle tulee antaa ostoksesta aina kuitti hänen niin halutessa. Tällöin myyjän tulee muistaa eri tuotteiden arvonlisäveroluokat ja eritellä ne kuittiin. Asiakaspalvelun hidastuessa jonot kasvavat, mikä puolestaan vaikuttaa negatiivisesti asiakkaiden ostokäyttäytymiseen ja yrityksen saamiin tuloihin.

Tietojärjestelmien datan varmistuksessa ja palautuksessa tulee huomioida, että yrityksellä on lakisääteinen velvollisuus säilyttää tiettyjä aineistoja pitkiäkin aikoja. Säilytysvelvollisuus on esimerkiksi palkkalaskelmilla, jotka tulee säilyttää 50 vuoden ajan, sekä maksukorttien kauppiaan kuiteilla, jotka tulee säilyttää kahden vuoden ajan. (Paasikoski 2013.) Kirjanpitokirjat ja tililuettelot on säilytettävä vähintään 10 vuotta tilikauden päättymisestä. Muu kirjanpitoaineisto, kuten tilikauden tositteet, koneellisen kirjanpidon täsmäytysselvitykset ja liiketapahtumia koskeva kirjeenvaihto on säilytettävä vähintään kuusi vuotta tilikauden päättymisvuoden lopusta laskettuna. (Kirjanpitolaki 1997.)

7.2.2 Palvelimet

Särkänniemen pääjakamo, jossa palvelimet sijaitsevat, ja nauhavarmistukset sijaitsevat eri rakennuksissa. Pääjakamossa on kolme fyysistä palvelinta, joilla toimii yhteensä 37 virtuaalipalvelinta, sekä yksi hallintapalvelin. Näiden lisäksi esimerkiksi kulunvalvontajärjestelmällä on oma palvelin. Jos yksi pääjakamon kolmesta fyysisestä palvelimesta hajoaa, siirtyvät virtuaalipalvelimet automaattisesti muille palvelimille. Tällöin virtuaalipalvelimilla olevat palvelut jatkuvat keskeytyksettä eli käyttäjät eivät huomaa palvelimen sammumista. Virtuaalisia palvelimia on tällä hetkellä käytössä niin monta, että palvelinten nykyinen muistikapasiteetti mahdollistaa vain yhden palvelimen sammumisen palvelujen vaarantumatta. (Minkkinen 2013.)

Palvelinten valvonta on ostettu palveluna ulkopuoliselta palveluntarjoajalta. Valvontapalvelu valvoo palvelimista mm. seuraavia asioita: muisti, resurssit, prosessorin käyttö, kovalevyn tila ja käyttö, palvelimien lämpötila, SQL-prosessit, SQL-tehtävät, ylläpitosuunnitelmat sekä palvelimien palvelujen ja prosessien toimiminen. Valvonta seuraa myös tiettyjä määriteltyjä prosesseja, jolloin esimerkiksi kassajärjestelmän tietyn prosessin sammuessa nostaa päivystäjä hälytyksen saatuaan sen automaattisesti takaisin päälle. (Leino 2014.)

Pääjakamossa on automaattinen lämpötilan seuranta sekä jäähdytysjärjestelmä. Lämpötilan noustessa käynnistyy jäähdytysjärjestelmä automaattisesti ja alkaa jäähdyttää tilaa. Jos jäähdytysjärjestelmä esimerkiksi vikaantuu ja lämpötila nousee määriteltyjen raja-arvojen yli, ajavat palvelimet itsensä automaattisesti ylikuumenemisen ja hajoamisen välttämiseksi alas. Näin saattaa tapahtua esimerkiksi talvella kovilla pakkasilla. (Minkkinen 2013.)

Pääjakamossa on kahden eri kytkimen avulla varmistuslevyjärjestelmään kytketty varmistuspalvelin. Palvelin on lisäksi kytketty vikasietoisesti kahteen eri Ethernet-kytkimeen varmistusten ottamista varten. Palvelimelle on näytetty kiintolevyä toisessa rakennuksessa sijaitsevan jakamon levyjärjestelmästä varmistuskäyttöä varten. Lisäksi pääjakamossa on nauhakirjasto, johon varmistukset kopioidaan arkistointia ja mahdollista off-site -säilytystä varten. Tällä hetkellä nauhakirjastossa tosin käytetään samoja varmistusnauhoja uudelleen eikä niitä siirretä off-site -säilytykseen. Jatkossa kannattaa miettiä nauhojen vaihtamista suurempiin, jotta saadaan otettua talteen enemmän dataa. Tietokantojen

varmistus tapahtuu ottamalla tietokannasta DUMP-tiedosto tietokantavalmistajien työkaluilla. DUMP-tiedoston varmistus tapahtuu normaalin tiedostovarmistuksen mukana ja kopiona nauhakirjastoon. (Särkänniemi varmistuskäytäntö 2013.)

7.3 Uhkiin varautuminen

Tampereen Särkänniemi Oy:ssä on tehty monia toimenpiteitä varmistamaan katastrofien ennaltaehkäisy esimerkiksi varmistamalla laitteiden virransaanti ja tietoliikenneyhteydet. Yrityksessä on myös kiinnitetty huomiota katastrofien tunnistamiseen esimerkiksi laajan paloilmaisinverkoston muodossa. Jos jotain tapahtuisi, saataisiin siitä tieto mahdollisimman nopeasti, mikä toivottavasti auttaisi rajaamaan katastrofin laajuutta.

7.3.1 Virransaanti

Särkänniemessä ei ole sattunut suuria sähkökatkoja kovinkaan usein ja pisin aika ilman sähköä on ollut pari tuntia. Viimeksi tällainen isompi sähkökatkos sattui 90-luvulla kaupungin sähkömuuntamon tulipalon vuoksi. Pienempiä, paikallisia sähkökatkoja tapahtuu aina silloin tällöin, ja useimmiten ne johtuvat ukkosen ja salamaniskujen aiheuttamista vaurioista. (Patala 2013.)

Särkänniemen Elämyspuiston sähkönsaanti on varmistettu rengassyötöllä. Sähkö johdetaan Särkänniemeen kahta eri reittiä, joten sähkönsyötön estyessä toisesta suunnasta, pystytään se turvaamaan toisen reitin kautta. Sähkö saadaan palautettua melko nopeasti, reitin vaihtaminen kestää n. 1-2 h. (Patala 2013.)

Näsinneula-rakennuksessa on varavoimakone, joka käynnistyy automaattisesti sähkökatkon sattuessa. Varavoiman avulla pystytään ylläpitämään hätävalaistusta ja sumusammutinjärjestelmää sekä ajamaan Näsinneulan näkötornin hissejä puolinopeudella. Varavoimakone myös sammuttaa itsensä automaattisesti sähkövirran palattua toimintaan. Myös huvilaitteissa on huomioitu mahdolliset sähkökatkot ja esimerkiksi Tornado, Trombi ja Hurricane on varustettu varavoimakoneilla, jotta mahdollisen sähkökatkon aikana saadaan laite ajettua alas ja ihmiset poistettua laitteesta. (Patala 2013.)

Pääjakamon virransaanti on varmistettu kahdentamalla sähkönsyöttö kahdella UPSilla. Niiden avulla pystytään takaamaan virransaanti noin tunnin ajaksi, jolloin ehditään tarvittaessa ajaa palvelimet alas hallitusti. Pääjakamoon on mietitty myös oman aggregaatin hankkimista virransaannin varmistamiseksi. (Minkkinen 2013.)

7.3.2 Tulipalo

Tulipaloihin on varauduttu laajalla paloilmaisin- ja sammutusjärjestelmällä. Paloilmaisinkeskuksia Särkänniemen Elämyspuiston alueella on kuusi ja paloilmaisimia on kaiken kaikkiaan 762 kpl. Käytössä on savu- ja lämpöilmaisimia sekä yhdistelmäilmaisimia, joissa yhdistyy molemmat ominaisuudet ja joilla pyritään vähentämään virheellisiä ilmoituksia. Lisäksi käytössä on joitakin ioni-ilmaisimia, mutta ne tullaan vaihtamaan savu-/lämpöilmaisimiin. (Lastunen 2013.)

Paloilmoittimet testataan kuukausittain ja yhteystesteillä todetaan laitteiston kunto ja niissä mahdollisesti havaitut viat, kuten ilmaisimien likaisuus tai laitteiden fyysinen kunto, korjataan pikaisesti. Palohälytyksiä Särkänniemessä tulee vuodessa keskimäärin 2 - 4 kertaa. Vuoden 2013 aikana hälytyksiä aiheutui kuusi kertaa ja ne johtuivat pääosin pölyn tai vesihöyryn vaikutuksesta sekä yksi ukkosen johdosta. Varsinaista tulipaloa ei Särkänniemessä tähän mennessä onneksi ole ollut. (Lastunen 2013.)

Sammutusjärjestelmänä käytössä on sprinklerijärjestelmä sekä sumusammutinjärjestelmä Näsinneula-rakennuksessa. Sumusammutinjärjestelmä käyttää hienojakoista vesisumua ja se viilentää sekä liekkiä että ympäröiviä kaasuja ja vähentää happipitoisuutta haihduttamalla sekä lieventää säteilevää kuumuutta pienten vesipisaroiden avulla. Sumusammutinjärjestelmän etuja ovat muun muassa pienempi veden kulutus sekä vähäisemmät vesivahingot. (Marioff 2013.)

Pääjakamon paloluokitus on korkea, sillä tilaa ympäröivät betoniseinät ja se on suojattu palo-ovella sekä palokatkoilla. Mikäli toimistorakennuksessa syttyisi tulipalo, ei se pääse leviämään kovin helposti pääjakamoon. Mikäli palo taas sattuisi syttymään pääjakamossa, ei se myöskään pääse leviämään sieltä helposti ulospäin muihin tiloihin. Pääjaka-

mossa on paloilmaisimet ja lisäksi tilan lämpötilaa seurataan koko ajan. Mikäli pääjakamon paloturvallisuutta halutaan parantaa entisestään, voidaan tilan kaapelit vaihtaa palosuojattuihin kaapeleihin. (Patala 2014.)

7.3.3 Vesivahinko

Palvelintilassa ei kulje vesi- tai viemäröintiverkostoa, joten vesivahingon syntyminen ei ole todennäköistä. Jäähdytysjärjestelmästä voi muodostua kondensoitua vettä, mutta määrät ovat niin pieniä ja palvelimet on sijoitettu jakamossa niin, ettei siitä ole vaaraa laitteistolle. (Patala 2014.)

Pääjakamossa ei ole automaattista sprinklerijärjestelmää tai nestesammuttimia, joten palohälytys ei aiheuta vesivahinkoa. Tulipalon varalle pääjakamon luona on hiilidioksidisammutin, joka puhtaana kaasuna ei sotke ympäristöä eikä johda sähköä ja näin ollen sopii erityisen hyvin sähköpalojen sammuttamiseen (Länsi-Uudenmaan pelastuslaitos 2012).

7.3.4 Tietoliikenneyhteydet

Särkänniemen tietoliikenneyhteydet on varmistettu kahden eri reittiä tulevan verkkoyhteyden kautta. Molemmat yhteydet ovat kuitenkin saman palveluntarjoajan, joten mikäli verkkoyhteys katkeaa toimittajasta johtuvasta viasta, saattaa se vaikuttaa molempiin yhteyksiin. (Minkkinen 2013.) Jatkossa yrityksen kannattaa miettiä pää- ja varayhteyksien hankkimista eri palveluntarjoajilta.

Särkänniemen varayhteys on hitaampi kuin pääyhteys, joten mikäli joudutaan siirtymään varayhteyden käyttöön, tulee sen käyttö priorisoida eri tietojärjestelmien kesken. Pääsääntöisesti tällaisessa tapauksessa koko verkkoliikenne pyhitetään maksuliikenteen käyttöön, jotta myyntipisteissä voidaan ottaa vastaan myös korttimaksuja. (Leino 2014.)

7.3.5 Laiterikot

Laiterikot ovat todennäköisin uhka Särkänniemen tietojärjestelmille. Niitä voivat aiheuttaa esimerkiksi ukkonen ja salamaniskut sekä laitekannan vanhetessa tapahtuvat laiterikot. Laiterikkoihin on varauduttu hankkimalla yleisimpiä ja tärkeimpiä varaosia. Esimerkiksi kytkimiä on varalla useampaa erilaista mallia, sillä käytössäkin on useampaa erilaista mallia. (Minkkinen 2013.)

Särkänniemessä on myös pohdittu varaympäristön rakentamista, jolloin pääjakamon tuhoutuessa saataisiin kaikki tietojärjestelmät pyörimään hyvinkin nopeasti. Tällaisen rakentaminen on kuitenkin todella kallista, joten sen tarve tulee miettiä hyvin tarkkaan. (Minkkinen 2013.)

7.4 Toipumissuunnitelman testaus ja käyttö

Toipumissuunnitelman valmistumisen jälkeen tulee se seuraavaksi testata, jotta mahdollisen katastrofin sattuessa voidaan olla varmoja sen toimivuudesta. Varmistusten palautuksia on testattu jonkin verran, mutta niille ei ole luotu säännöllistä aikataulua eikä niitä ole dokumentoitu. Virtuaalipalvelimista otetaan kerran viikossa snapshot eli koneen sen hetkinen tila tallennetaan kokonaisuudessaan tiedostoon. Sen palauttamista ei kuitenkaan ole testattu, sillä snapshotia ei pysty palauttamaan vanhan päälle. (Minkkinen 2013.)

Toipumissuunnitelma tulisi testata ensimmäisen kerran talven 2014–2015 aikana, jotta mahdollisen uhkan toteutuessa kesäkaudella 2015 on suunnitelma testattu ja valmis käyttöön. Lisäksi testauksille tulee luoda aikataulu, jotta ne tulee tehtyä jatkossa säännöllisesti. Testausten avulla voidaan löytää kehityskohteita, kuinka toipumista saadaan parannettua tai nopeutettua, tai huomataan, mikäli suunnitelmassa on jotain puutteita. Testaukset voivat toimia myös mahdollisten uusien tietohallinnon työntekijöiden koulutustilaisuuksina, jolloin he saavat paremman kuvan toipumistoimenpiteiden toteuttamisesta. Testaukset ja niissä mahdollisesti huomatut kehitysehdotukset tulee kirjata toipumissuunnitelmaan.

Toipumissuunnitelmaa tulee päivittää säännöllisesti. Toipumissuunnitelmaan tulee päivittää kaikki tietojärjestelmissä tapahtuneet muutokset, kuten kriittisten järjestelmien lisääntyminen tai järjestelmien vaihtuminen. Toipumissuunnitelma olisi kuitenkin hyvä käydä läpi säännöllisesti kerran tai kaksi vuodessa, vaikka suurempia muutoksia toiminnassa ei tapahtuisikaan, ja varmistaa sen ajantasaisuus. Tärkeätä on päivittää toipumissuunnitelma aina ennen kesäkauden alkua, sillä kesäkaudella liiketoiminnalle tapahtuvat keskeytykset voivat olla kohtalokkaita ja tällöin tulee olla varma että toipumissuunnitelma on ajan tasalla.

Toipumissuunnitelmaan tulee kirjata myös kaikki tapahtuneet häiriötilanteet, jolloin toipumissuunnitelma on jouduttu ottamaan käyttöön. Häiriötilanteista tulisi kirjata suunnitelmaan ajankohta, vikatilanne, tehdyt toimenpiteet sekä mahdolliset kommentit tai kehitysehdotukset.

8 POHDINTA

Tämän opinnäytetyön tavoitteena oli laatia toipumissuunnitelmapohja Tampereen Särkänniemi Oy:lle ja kirjata siihen liiketoiminnan kannalta kriittisimmät järjestelmät ja niiden käyttöön palauttamiseksi tarvittavat toimenpiteet, vastuuhenkilöt sekä tärkeimpien yhteistyökumppaneiden yhteystiedot. Opinnäytetyön valmistumisen jälkeen toipumissuunnitelmasta tulee olennainen osa yrityksen riskienhallintaa ja sitä tullaan toivottavasti käyttämään ja päivittämään säännöllisesti, sillä pelkkä paperidokumentin olemassaolo ei vielä takaa nopeaa katastrofista toipumista. Toipumissuunnitelman ulkoasu ja rakenne on pyritty laatimaan niin, että sen päivittäminen ja laajentaminen on helppoa, ja mielestäni suunnitelman lopullisesta rakenteesta tuli selkeä.

Opinnäytetyön haasteena oli aluksi liiketoiminnan jatkuvuussuunnitteluun liittyvien käsitteiden hahmottaminen sekä toipumissuunnitteluun liittyvien asioiden rajaaminen. Jatkuvuussuunnittelusta löytyi lähdekirjallisuutta, mutta monissa teoksissa varsinaista toipumissuunnitelmaa oli käsitelty melko suppeasti. Jatkuvuussuunnittelusta on liiketoiminnan tietojärjestelmien yleistyessä kuitenkin tullut yhä suositumpi ja ajankohtaisempi aihe, ja materiaalia alkoi löytyä enemmän opinnäytetyön edetessä. Myös toipumissuunnitelman mallipohjia löytyi useita, mikä toi myös oman haasteensa, kuinka valita niistä Särkänniemen toipumissuunnitelmaan parhaiten sopivat kohdat. Lopulta Särkänniemen toipumissuunnitelman pohjana käytettiin kahta eri toipumissuunnitelmamallia, joista yhdistettiin Särkänniemelle sopiva malli. Opinnäytetyöraportti on laadittu niin, että se toimii myös jatkuvuus- ja toipumissuunnittelun esittelynä esimerkiksi yrityksen johdolle.

Toipumissuunnitelmat ovat yritysten salaista tietoa, joten aihetta tutkiessa ei ollut mahdollisuutta tutustua yhteenkään valmiiseen suunnitelmaan. Tämä aiheutti suunnitteluun hieman haasteita, sillä valmis suunnitelma olisi ollut hyödyllinen aiheeseen tutustuessa ja se olisi varmasti selkeyttänyt asioita. Tämän opinnäytetyön tuloksena syntynyt toipumissuunnitelma on kuitenkin vasta Särkänniemen ensimmäinen ja sitä testatessa ensimmäistä kertaa saatetaan heti huomata kehitettäviä asioita. Oli esimerkiksi vaikea arvioida, paljonko tietoa tarvitaan kuhunkin suunnitelmassa olevaan kohtaan. Suunnitelman käyttökelpoisuuden vuoksi kirjallinen tuotos ei saisi olla liian raskas, mutta sen tulisi silti sisältää kaikki toipumiselle tarvittavat toimenpiteet ja tiedot.

Särkänniemi on tunnettu yritys, joka herättää paljon keskustelua ja mielipiteitä. Esimerkiksi Delfinaario on säännöllisesti esillä yleisön mielipidekirjoituksissa ja viime aikoina myös kaupungin valtuuston esityslistoilla, ja se herättää paljon niin positiivisia kuin negatiivisiakin tunteita ihmisissä. Tämä saattaa tulevaisuudessa johtaa pahimmassa tapauksessa esimerkiksi ilkivaltaan Särkänniemeä kohtaan.

Särkänniemessä on jo tehty monia toimenpiteitä, joilla on varauduttu mahdollisiin tahallisiin tai tahattomiin uhkiin, kuten tulipaloihin, tietoliikenneyhteyksien katkeamiseen sekä laiterikkoihin. Yrityksessä on esimerkiksi laaja paloilmaisin- ja sammutinjärjestelmä tulipalojen nopeaan havaitsemiseen, varalaitteita laiterikkoja varten ja tietojärjestelmien varmistusjärjestelmä kriittisten tietojen varmistamiseksi ja palauttamiseksi. Lisäksi esimerkiksi tietoliikenneyhteydet sekä virransaanti on varmistettu kaksinkertaisilla kaapeloinneilla. Jatkossa näitä voidaan kehittää edelleen esimerkiksi palosuojaamalla pääjakamon kaapelit, varmistamalla tietoliikenneyhteydet hankkimalla pää- ja varayhteydet eri palveluntarjoajilta sekä lisäämällä fyysisten palvelinten kapasiteettia kahdentamalla palvelinympäristö, mikäli se katsotaan tarpeelliseksi ja kustannustehokkaaksi ratkaisuksi.

Särkänniemen kriittisistä tietojärjestelmistä moni toimii yrityksen omilla palvelimilla, jolloin yrityksen vastuulla on huolehtia palvelinten varmistamisesta ja korkean käytettävyyden takaamisesta. Tämä vaatii laitteiston ylläpitämistä ja päivittämistä ja saattaa tulla kalliiksi. Tällöin yrityksellä on itsellään myös tietojen säilyttämisvelvollisuus.

Tulevaisuudessa voisi miettiä, olisiko järkevämpää ja kannattavampaa hankkia osa järjestelmistä pilvipalveluina. Tällöin järjestelmätoimittajan vastuulla olisi varmistaa tiedot ja palvelujen käytettävyys, sekä niin sovittaessa myös lakisääteisten tietojen säilyttäminen olisi palveluntarjoajan vastuulla. Pilvipalveluiden tuoma etu olisi, jos palveluntarjoaja pystyisi takaamaan turvallisemman ja vikasietoisemman ympäristön tietojärjestelmille. Mutta uhkana on, kuinka pystyttäisiin varmistamaan palveluntarjoajan vastuu ja käytettävyystoimenpiteiden riittävyys, sekä kumpi tapa olisi pidemmällä aikavälillä luotettavampi ja edullisempi.

Tällä hetkellä monien kriittisten järjestelmien käyttöön palauttaminen vaatii järjestelmätoimittajan tai ulkopuolisen palveluntarjoajan osallistumista eikä Särkänniemen tietohallintohenkilökunnalla ole tarvittavaa osaamista tai mahdollisuutta kriittisimpien järjestel-

mien palauttamiseen. Epävarmaa on, tavoitetaanko ulkopuolinen palveluntarjoaja varmasti juuri katastrofin aikaan tai onko kaikilla henkilöillä riittävä osaaminen juuri Särkänniemen ympäristöstä. Tämä on ilmennyt jo nyt pienempien ongelmien kanssa, sillä kesäkaudella yksi Särkänniemen liiketoiminnan kiireisimmistä viikonpäivistä on lauantai, jolloin tukipalvelujen saavuttaminen on yleensä vaikeampaa. Päivystäjät saattavat olla kesätyöntekijöitä, joilla ei ole riittävää osaamista ja tuntemusta Särkänniemen järjestelmäympäristöstä, jolloin ongelman ratkaiseminen jää mahdollisesti odottamaan arkea ja oikean henkilön palaamista töihin. Toisaalta, mikäli Särkänniemen tietohallinto olisi vahvemmin vastuussa itse kaikista toipumistoimenpiteistä, voisi riittävän osaamisen hankkiminen kuormittaa pientä osastoa liikaa ja siinäkin vaarana on, että toipuminen kohdistuu liikaa yksittäiseen henkilöön, mikä luo haavoittuvuutta jatkuvuudelle. Ulkopuolisten toimijoiden kanssa tulee aina laatia yhteistyösopimukset tarkkaan ja kiinnittää erityistä huomiota esimerkiksi tuen palveluaikoihin sekä vasteaikoihin, joihin he sitoutuvat.

Toipumissuunnitelmaa laadittaessa huomattiin, että monet yrityksen ohjeista, materiaaleista ja tunnuksista on tallennettuna ainoastaan intranetiin. Näin ollen esimerkiksi pääjakamon tuhoutuessa ei niihin ole pääsyä ennen palvelimen palauttamista. Tärkeimpiä ohjeita ja materiaaleja tulisi säilyttää myös kirjallisina kappaleina useammassa fyysisessä sijainnissa, josta ne ovat helposti ja nopeasti saatavilla mahdollisessa toipumistilanteessa. Toipumissuunnitelmaan kirjataan henkilöt, joille toipumissuunnitelma toimitetaan, sekä fyysiset sijainnit, joissa suunnitelmaa tullaan säilyttämään. Näin suunnitelmaa päivitettäessä muistetaan vaihtaa kaikki kopiot uusiin versioihin.

Osa Särkänniemen lakisääteisesti säilytettävistä tiedoista sijaitsee tällä hetkellä ainoastaan paperikappaleena arkistossa. Mikäli arkisto sattuisi esimerkiksi palamaan, tarkoittaisi se silloin tietojen täydellistä tuhoutumista. Jatkossa tulisikin pohtia, kannattaisiko tärkeimmät tiedot muuttaa sähköiseen muotoon tai kopioida säilytettäväksi jossain toisessa fyysisessä sijainnissa, vaikka se olisi työläs projekti.

Toipumissuunnitelman valmistuttua tulee se seuraavaksi testata. Testaus tulisi suorittaa ennen kesäkauden alkua, jotta liiketoiminnan ollessa kriittisimmillään voidaan luottaa toipumissuunnitelman toimivuuteen mahdollisen katastrofin sattuessa. Toipumissuunnitelman testaus tulisi ottaa yrityksessä säännölliseksi rutiiniksi ja testauksissa huomatut puutteet tai muutostarpeet tulisi aina päivittää heti suunnitelmaan. Testauksilla voidaan

paitsi varmistaa toipumistoimenpiteiden riittävyys myös kouluttaa toipumisesta vastaavaa henkilöstöä, sillä rutiinit tuovat varmuutta tekemiseen.

Pelkkä toipumissuunnitelman laatiminen ei riitä, vaan sitä pitää ylläpitää jatkuvasti. Toipumissuunnitelma olisi hyvä käydä läpi kerran tai kaksi vuodessa tai aina tietojärjestelmien ja muiden toipumissuunnitelmassa mainittujen tietojen muuttuessa. Toipumissuunnitelman päivitys voisi tapahtua samaan aikaan riskikartoituksen päivityksen kanssa.

LÄHTEET

Doughty, K. 2000. Best Practices, Volume 15: Business Continuity Planning: Protecting Your Organization's Life. Boca Raton, FL, USA: Auerbach Publications.

Gregory, P. 2008. IT Disaster Planning For Dummies. Hoboken, NJ: Wiley Publishing, Inc.

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

Kirjanpitolaki 30.12.1997/1336.

Kolehmainen, A. 2014. Luettu 31.10.2014. Stara vaihtoi työasemat kevytpäätteisiin - sähkölasku putosi 10 000 euroa vuodessa. Tietoviikko. http://summa.talentum.fi/article/tv/uutiset/104568

Lastunen, P. sähköasentaja. 2013. Paloilmaisimista. Sähköpostiviesti. Luettu 19.11.2013.

Leino, M. IT-asiantuntija. 2014. Haastattelu 30.10.2014. Haastattelija Hämäläinen, T. Tampere.

Linnake, T. 2010. It-katkot maksavat 440 miljoonaa vuodessa. It-viikko. Luettu 17.11.2010. http://www.itviikko.fi/tietoturva/2010/09/16/it-katkotmaksavat-440-miljoonaa-vuodessa/201012873/7.

Länsi-Uudenmaan pelastuslaitos. 2012. Erilaiset sammuttimet. Luettu 3.11.2014. http://www.lup.fi/fi-FI/Turvallinen_arki/Alkusammutusvalineet/Erilaiset_sammuttimet

Marioff Corporation. 2013. HI-FOG. Water Mist Fire Protection. Luettu 15.11.2013. http://www.marioff.com/

Miettinen, J. 2002. Yritysturvallisuuden käsikirja. Helsinki: Kauppakaari.

Minkkinen, A. järjestelmäsuunnittelija. 2013. Haastattelu 15.11.2013. Haastattelija Hämäläinen, T. Tampere.

Muukkonen, H. 2003. Taitava osaa ennakoida. Tietoviikko. Luettu 28.10.2010. http://lehtiarkisto.talentum.com/lehtiarkisto/search/show?eid=469274

Paasikoski, H. talouspäällikkö. 2013. Haastattelu 15.11.2013. Haastattelija Hämäläinen, T. Tampere.

Patala, T. työnjohtaja. 2013. Haastattelu 15.11.2013. Haastattelija Hämäläinen, T. Tampere.

Patala, T. työnjohtaja. 2014. Keskustelu 31.10.2014. Tampere.

Rinta, N. 2011. 7 syytä virtualisoida. Tietoviikko. Luettu 31.10.2014. http://www.tivi.fi/cio/7+syyta+virtualisoida/a704130

Sandhu, R. 2002, Disaster Recovery Planning. Cincinnati, Ohio: Premier Press.

Särkänniemi. 2014. Särkänniemi yrityksenä. Luettu 9.10.2014. http://www.sarkanniemi.fi/fi/sarkanniemi-yrityksena

Särkänniemi varmistuskäytäntö. 2013. Tampereen Särkänniemi Oy:n sisäinen dokumentti.

Toigo, J. 2003. Disaster Recovery Planning. Preparing for the unthinkable. Uppre Sadle River, NJ: Prentice Hall.

Wallace, M & Webber, L. 2004. Disaster Recovery Handbook. New York, NY: AMACOM Books.

Valtiokonttori. 2013. Järjestelmän toipumissuunnitelma. Luettu 4.12.2013. http://valtiokonttori.fi/download/noname/%7b3982F2A5-9079-4E74-BD3B-F02A51044E2C%7d/84858

Valtiovarainministeriö. 2013. VAHTI-ohje 3/2007 Tietoturvallisuudella tuloksia. Luettu 3.12.2013. https://www.vahtiohje.fi/web/guest/liite-1.-mallipolitiikat-ja-suunnitelma-rungot.

Viitanen, K. pääkirjanpitäjä ja HR-asiat. 2013. Haastattelu 15.11.2013. Haastattelija Hämäläinen, T. Tampere.