LAUREA
AMMATTIKORKEAKOULU
Uuden edellä

Toipumissuunitelma palvelimille ja työasemille

Kuokkanen, Antti

2013 Laurea Kerava

Laurea-ammattikorkeakoulu
Laurea Kerava

Toipumissuunnitelma palvelimille ja työasemille

Antti Kuokkanen
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Maaliskuu, 2013

Sisällys

Laurea-ammattikorkeakoulu **Tiivistelmä**
Laurea Kerava
Tietojenkäsittelyn koulutusohjelma

Antti Kuokkanen

Toipumissuunnitelma palvelimille ja työasemille

Vuosi 2013 Sivumäärä 26

Toipumissuunnitelu on kaikessa suuruudessa todella laaja käsite. Palvelimet ja työasemat ovat pieni, mutta tärkeä osa-alue toipumissunnittelua ja siksi niiden toipumisselle kannattaakin tehdä täysin oma suunnitelma. Tämä opinnäytetyö käsittelee toipumissuunnittelua ja erityisesti palvelimille ja työasemille tarkoitettua toipumissuunnittelua.

Tässä opinnäytetyössä käydään läpi toipumissuunnittelun eri vaiheet pääpiirteittäin ja paneudutaan tarkemmin palvelimille ja työasemille tarkoitetun toipumissuunnitelman rakentamiseen. Toipumisuunnitelman rakentamista palvelimille ja työasemille käydään läpi Storage IT:n mallipohjan avulla.

Opinnäytetyö projektin tavoitteena oli luoda Helsinkiläiselle Storage IT Oy:lle palvelimien ja työasemien toipumissuunnitteluun mallipohja. Tätä mallipohjaa hyödyntämällä Storage IT pystyy tulevaisuudessa helpommin tarjoamaan toipumsisuunnitelmaa omana tuotteena varmuuskopiointipalvelunsa lisänä asiakkailleen. Mallipohjan tarkoituksena on toimia asiakkaan ja Storage IT:n apuna toipumissuunnitelmaa tehtäessä.

Asiasanat: Toipumissuunnittelu, varmuuskopiointi, riskienhallinta

Laurea University of Applied Sciences **Abstract**
Laurea Kerava
Information technology

Antti Kuokkanen

Disaster Recovery Plan for Servers and Workstations

Year 2013 Pages 26

Disaster recovery planning is a big concept. Servers and workstations are just small but important pieces of disaster recovery planning and that is why it is recommended to have a completely own plan for it. This bachelor´s thesis deals with disaster recovery planning and particularly focuses on disaster recovery planning for servers and workstations.

This bachelor´s thesis goes through the different phases of disaster recovery planning and delves particularly for making disaster recovery planning for servers and workstations. Disaster recovery plan developed for servers and workstations is scrutinized with the Storage IT template.

The main goal of this bachelor´s thesis project was to create a disaster recovery planning template for Storage IT Ltd. By using this template, Storage IT can offer Disaster recovery planning for their backup customers in the future. The purpose of this template is to help customers and Storage IT to create a disaster recovery plan.

Keywords: Disaster recovery planning, back up, risk management

1 Johdanto

Mitä tekisit jos virus tai tulipalo tuhoaisi yrityksesi tärkeän palvelimen. Mikäli sinulla sattuu olemaan varmuuskopioit tallessa ei hätä välttämättä ole pahin mahdollinen. Tilannetta helpottaisi vielä enemmän, jos olisit osannut varautua katastrofitilanteeseen etukäteen luodulla ja testatulla suunnitelmalla. Häiriötilanteen sattuessa ei ole aikaa miettiä kovin tarkasti, miten siitä selviydytään.

Suurin osa yritysten liiketoiminnasta on nykypäivänä riippuvainen teknologiasta ja sen automaattisuudesta. Häiriöt yrityksen laitteistossa voivat koitua todella kalliiksi ja pahimmillaan uhata koko yrityksen tulevaisuutta. Häiriötilanteiden varalle tehtyä tarkkaa suunnitelmaa kutsutaan disaster recovery planiksi eli toipumissuunnitelmaksi. Toipumissuunnitelma on suunnitelmakokonaisuus, joka kattaa häiriötilanteeseen varautumisen, häiriötilanteeseen reagoimisen sekä häiriöstä elpymisen. Hyvänä vertauskuvana toipumissuunitelman tärkeydestä voidaan pitää mitä tahansa vakuutusta. Se on periaatteessa täysin hyödytön, jos yrityksen arki sujuu ongelmitta, kunnes jonain päivänä se voi osoittautua lähes korvaamattomaksi.

Toipumissuunnittelu on jatkuvuussuunnittelun yksi osa, jolla varaudutaan normaaliolojen häiriötilanteisiin. Normaaliolotilalla tarkoiteteaan tilaa, jossa liiketoimintaa pystytään harjoittamaan stabiilissa liiketoimintaympäristössä ilman häiröitä. Normaaliolotilan vallitessa ilmenee ajoittain ongelmia jotka hankaloittavat liiketoimintaa hetkellisesti. Tällaisia ongelmia ovat esimerkiksi lyhyet sähkökatkokset tai tietoliikennekatkokset. Kun ongelmasta selvitään normaalilla työrutiinilla, ei tilanteessa tarvita vielä toipumissuunnitelmaa. Vasta kun liiketoimintaympäristössä havaitaan häiriö, jonka takia toimintaa joudutaan muuttamaan ja liiketoiminnan harjoittaminen vaikeutuu, olisi syytä turvautua toipumissuunnitelmaan. (Iivari & Laaksonen 2009, 97.)

1.1 Tutkimuksen taustaa

Työskentelen tällä hetkellä varmuuskopiointipalvelua tarjoavassa IT-alan yrityksessä nimeltä Storage IT. Yrityksen pääasiakkaita ovat pienet ja keskisuuret suomalaiset yritykset. Storage IT:n tarjoama varmuuskopiointipalvelu voidaan jakaa kahteen tuotteeseen: Coreen ja Terastorageen. Näiden varmuuskopiointisovellusten avulla tapahtuu itse varmuuskopiointi. Sovellus asennetaan asiakkaan palvelimelle tai työasemalle ja se hoitaa varumuuskopioinnin automaattisesti käyttäjän tarvitsematta huolehtia siitä sen kummemmin. Tästä päästäänkin hyvin opinnäytetyöaiheeseeni. Mitä sitten tehdään jos palvelin esimerkikiksi hajoaa tai

varastetaan? Kaikki tieto on tietenkin tallessa Storage IT:n tietovarastossa, mutta miten edetään häiriötilanteen sattuessa. Tässä muutama pohdinnan arvoinen asia:

- Kenelle täytyy soittaa ja onko tärkeät yhteystiedot heti saatavilla?
- Kuinka nopeasti kriittinen data saadaan takaisin?
- Miten kriittinen data saadaan takaisin?
- Kuinka kauan kestää uuden palvelimen hankinta ja asennus?
- Olisiko edellämainittuihin kysymyksiin voitu hankkia tyydyttävä vastaus etukäteen ja säästetty rahaa sekä aikaa?

Keväällä 2011 suoritin Storage IT:llä myös työharjottelujaksoni. Harjoitteluni sujui mukavasti ja syksyllä 2011 aloimme kesksutella opinnäytetyöstäni ja siitä, olisko Storage IT:llä tarjota siihen aihetta. Hyvä aihe löytyi melko nopeasti ja sitä rajattiin pikkuhiljaa sopivammaksi.

1.2 Tutkimuksen tarkoitus ja rajaus

Opinnäytetyötutkimukseni tarkoituksena on luoda toipumissuunnitelman mallipohja palvelimille ja työasemille. Sen avulla Storage IT pystyy tarjoamaan toipumissuunnitelmaa asiakkailleen varmuuskopiointipalveun ohessa. Mallipohjan avulla voidaan siis lähteä suunnittelemaan palvelimille ja työasemille suunnattua toipumissuunnitelmaa yhdessä asiakkaan kanssa.

Toipumissuunnittelu on aiheena todella laaja ja siksi olen rajannut aihetta siten, että suunnittelemani toipumissuunnitelman mallipohja on tarkoitettu vain palvelimien ja työasemien toipumiseen. Toki tämä rajaus oli tärkeä myös Storage IT:lle, sillä yrityksellä ei ole intressiä lähteä toteuttamaan asiakkailleen kokonaisvaltaisia toipumissuunnitelmia.

1.3 Palvelin ja työasema

Palvelimet toimivat yrityksen tiedon jakajina, tallennuspaikkana ja niillä pyörivät usein yrityksen tärkeimmät sovellukset. Kaikki tärkeä tieto on siis sullottu yhteen ja samaan paikkaan. Tästä voikin jo päätellä, mitä tapahtuu, jos yrityksen tärkeä palvelin hajoaa. Pienin murhe ei välttämättä ole siitä aiheutuva käyttökatkos. Mikäli tärkeätä dataa pääsee katoamaan, eikä sitä pystytä palauttamaan, niin seuraukset voivat olla katastrofaaliset.

Sama tilanne on työasemien suhteen, tosin ei usein niin suuressa mittakaavassa. Työasemilla voi olla esimerkiksi tärkeätä tietoa jota työntekijä ei ole vielä kerennyt tallentamaan palvelimille. Työasemalla tarkoitetaan tänäpäivänä henkilökohtaista yrityskäytössä olevaa tietokonetta joka on kytkettävissä LAN-verkkoon. (Judson 2010, 54; Wikipedia 2012.)

2 Riskit ja Riskianalyysi

Yksi tärkeimmistä ellei jopa tärkein osa toipumissuunnitelmaa on riskianalyysin tekeminen. Ilaman riskianalyysiä toipumissuunnitelmaa ei voida tehdä. Riskianalyysin tarkoituksena ei ole riskien poistaminen tai pienentäminen, vaan sen avulla saatua tietoa voidaan hyödyntää riskeihin varautumiseen. Mikäli yritykseltä löytyy jo entuudestaan joitakin riskianalyysejä, kannattaa niitä hyödyntää ja etsiä jo mahdollisesti tunnistettuja riskejä. Riskien analysointiin sisältyy kolme vaihetta:

- Riskien tunnistaminen
- Riskien vaikutusten analysointi
- Riskejä vähentävien toimenpiteiden ehdottaminen (Iivari & Laaksonen 2009, 100; Juvonen, Korhonen, Ojala, Salonen & Vuori, 2005, 25.)

Palvelimiin ja työasemiin kohdistuvien uhkien aiheuttjien ymmärtäminen on ensisijaisen tärkeätä tehtäessä riskianalyysiä nimenomaan kyseisille laitteille. Tällaisia uhkia ovat esimerkiksi tekniset ongelmat tai laitteen vaurioituminen, yrityksen oma henkilöstö, ulkopuoliset toimijat ja onnettomuudet. (Iivari ym. 2009, 100.)

2.1 Uhkien tunnistaminen

Riskianalyysin ensimmäinen vaihe on kaikkien mahdollisten uhkien tunnistaminen ja käsittely laajaalaisesti, sivuttamatta yhtäkään keskeistä uhkaa. Lähdettäessa tekemänä riskianalyysiä palvelimille tai työasemille, mietitään tietenkin vain niihin mahdollisesti kohdistuvia uhkia. Tällaisia uhkia voisivat olla esimerkiksi virukset tai tulipalo.

Tehokas apuväline uhkien tunnistamisessa on uhkataulukko. Iivari ja Laaksonen (2009, 119) mainitsevat yhden yleispätevän uhkatalukon, joka on standardin ISO 27005:2008 liitteen C uhkataulokko. Uhkia olisi hyvä miettiä ensin itse ja vasta sitten turvautua yleisiin taulukoihin, etteivät ne turhaan rajaisi omaa ajattelua. (Iivari & Laaksonen 2009, 100.)

2.2 Uhkien toteutumisen arviointi

Vasta kun kaikki mahdolliset uhkatekijät on tunnistettu, voidaan lähteä miettimään niiden toteutumisen todennäköisyyttä. Riskejä arvioitaessa voidaan apuna käyttää kokemusperäistä tietoa ja erilaisia tilastoja. Kaikki tieto yritystä aijemmin koetelleista häiriöistä tai katastrofeista on siis hyvää materiaalia arvioitaessa uhkien toteutumista. Lisäksi voidaan turvautua asiantuntioiden apuun. (Iivari & Laaksonen 2009, 100; Juvonen ym. 2005, 25.)

Uhkien toteutumista voidaan arvioida siis esimerkiksi erilaisten olemassa olevien tilastojen avulla. Esimerkiksi voisi kuvitella, että VR:llä löytyy tilasto tietoa siitä, kuinka moni on jäänyt kiinni liputta matkustamisesta. Tilastojen puuttuessa voidaan todennäköisyyttä arvioida itse tehdyllä asteikolla.

1. Ei ole riski
2. Riskien toteutuminen erittäin epätodennäköistä
3. Riskin toteutuminen epätodennäköistä
4. Riskin toteutuminen kohtalainen
5. Riskin toteutuminen suuri (Iivari & Laaksonen 2009.)

2.3 Riskien käsittely

Vasta kun riskit on kartoitettu mahdollisimman hyvin, voidaan aloittaa niiden käsittely. Riskejä tulee käsitellä tapauskohtaisesti, sillä ne voidaan ratkaista useamalla eri tavalla.

- Riskin pienentäminen tai kasvattaminen
- Riskin välttäminen tai poistaminen
- Riskin huomioimatta jättäminen / hyväksyminen
- Riskin jakaminen tai siirtäminen (Juvonen ym. 2005, 32-35.)

Ehkä yleisin ja merkittävin tapa riskien käsittelyssä on niiden pienentäminen. Niiden toteutumisen mahdollisuutta voidaan lähteä pienentämään usella eri tavalla. Esimerkiksi henkilöstä voidaan kouluttaa tai paloturvallisuutta parantaa. Mikäli riskiä ei voida poistaa pyritään sitä useimmiten pienentämään tiettyyn pisteeseen saakka. Kustannusten kasavaessa täytyy raja laittaa jonnekkin. Näin ollen vakavuudeltaan kohtalaisten tai merkityksettömien riskien kohdalla on hyvä miettiä onko pienentäminen kannattava toimenpide. Riskin todennäköisyyttä voidaan tietoisesti lähteä myös kasvattamaan taloudellisista syistä. Otetaan esimerkiksi yritys, jolla on kaksi yövartijaa, joista toinen päätetään irtisanoa. (Juvonen ym. 2005, 32.)

Vakavuudeltaan merkittävät riskit kannattaa ensisijaisesti pyrkiä välttämään. Riskien välttäminen on kuitenkin kallista puuhaa, sillä se usein merkitsee yrityksen pidättäytymistä jostkin riskialttiista toiminnasta. Yrityksen johdon pohdittavaksi ja päätettäväksi jääkin, saavuttaako kustannukset hyödyn. Poistamista pidetään riskien välttämisen äärimmäisenä muotona ja se on harvoin edes mahdollista. Riskien poistaminen on kallis toimenpide, mutta se voi osoittautua kannattavaksi vaikka riskiä ei saataisi edes kokonaan poistettua, koska sen todennääisyyttä saadaan pienennettyä. (Juvonen ym. 2005, 34.)

Riskin voi jättää kokonaan huomioimatta, jos sen todennäköisyys tai vaikutus on huomattavan pieni. Tämä tarkoittaa uhan tietoista hyväksymistä ja sen voi lisätä, budjettiin. (Iivari & Laaksonen 2009.)

Riskejä voidaan jakaa tai siirtää esimerkiksi vakuuttamalla. Näillä keinoilla pyritään usein vaikuttamaan riskien taloudellisiin seurauksiin (Wikipedia 2012).

2.4 Riskit ja mobiililaitteet

”Työasema on väline, jolla käyttäjä hyödyntää verkonvälityksellä tarjolla olevia palveluja”. Tänäpäivänä se kulkee yhä useammalla ihmisellä mukana. Verkkopalveluihin ei pääse ainoastaan käsiksi kannettavalla tietokoneella, vaan älypuhelimella tai tabletilla. Näihin mukana kulkeviin laitteisiin kohdistuu suuri tietoturvariski. (Kuusela & Ollikainen 2005, 253-254.)

Varkaudet ja laitteiden katoamiset yleistyvät jatkuvasti tietokoneiden mobiilisoituessa. Tämän päivän älypuhelimet sekä tabletit ovatkin perusominaisuuksiltaan melkein samalla tasolla kannettavien tietokoneiden kanssa. Yhdysvalloissa varastetaan tai katoaa 113 puhelinta joka minuutti. Mikäköhän varastettujen tai kadonneinen puhelinten määrä mahtaa olla maailman laajuisesti? Näyttäisi siltä, että laitteen koolla on suora vaikutus katoamisen todennäköisyyteen ja mitä pienemmästä laitteesta on kyse, sitä suurempi todennäköisyys on siihen kohdistuvalla katoamisella tai varkaudella. Mobiililaitteen käyttäjän huolenpidolla onkin tärkeä merkitys niihin kohdistuvien riskien minimoimisessa. (Kuusela & Ollikainen 2005, 253-254; Vänninen 2012, 36.)

3 Toipumissuunnitelman suunnittelu

Toipumissuunnitelmissa ei yleisesti ottaen ole mitään virallista kaavaa, miten ne tulisi tehdä tai millaisia niiden tulisi olla. Toipumissuunnitelman voi tehdä koskemaan jotain tiettyä tärkeätä yrityksen aluetta, kuten palvelimia tai verkkoja. Olemassa on standardeja ja yleisesti hyväksi havaittuja malleja, jotai voidaan käyttää toipumissuunnitelman suunnittelussa ja tekemisesä. Toipumissuunnitelmat räätälöidään aina kuitenkin jokaisen yrityksen omiin tarpeisiin ja ympäristöihin, eikä standardeja näinollen tule noudattaa aivan sanasta sanaan. Yleisesti hyväksi havaittujen mallien osia voidaan muokata tai jättää kokonaan poiskin, jos jokin vaikuttaa tarpeettomalta.

Suunnitteluvaiheessa määritellään yleensä suunnitelman rakenne ja laaditaan template eli mallipohja (jos ei käytetä valimista pohjaa). Toipumissuunnitelman tekemisen ohjeistukseksi kelpaavat hyvin esimerkiksi erilaiset riskienhallinta- ja arviointimenetelmät sekä jo valmiiksi olemassa olevat järjestelmien toipumiseen liittyvät ohjeistukset. Suunnittelua ei kuitenkaan tule aloittaa ennen kuin kunnollinen riskianalyysi on tehty. (Iivari & Laaksonen 2009, 97.)

Miten toipumissuunnitelmasta yleisesti hyödytään? Tässä ainakin muutama hyöty:

- Häiriöin aiheuttaman vahingon laajuuden minimointi
- Häiriöin aiheuttaman taloudellisen vahingon minimointi
- Vaihtoehtoisen toimintamallin suunnittelu etukäteen
- Henkilökunnan koulutus häiriötilannetta varten
- Nopea ja sujuva palautuminen häiriöitilanteesta

Suunnitelman hyödyt on aina hyvä kirjoittaa toipumissuunnitelman alkupäähän josta ne helposti löytyvät ja muistuttavat lukijaansa sen tärkeydestä.

3.1 Vastuu

Yrityksen johdon mukana olo on tärkeätä lähdettäessä tekemään toipumissuunnitelmaa. Yrityksen johodon tulee tukea ja olla mukana koko prosessin aikana, sillä se on viimekädessä vastuussa sen suunnasta ja koko suunnitelman onnistumisesta. Johdon tehtävänä on myös määritellä suunnitelman kattamat alueet sekä olla mukana tehtäessä tärkeitä päätöksiä tai analyysejä.

Yrityksen johdon tulisi nimetä toipumissuunnittelman suunnittelusta ja koordinoinnista vastaava henkilö. Tällä henkilöllä tulisi olla riittävä kokemus ja auktoriteetti tehtävänsä hoitamiselle. Suunnitelman kokonaisvastuun olisi hyvä kuitenkin säilyä yrityksen johdolla. (Iivari & Laaksonen 2009, 97-98; Wold 1997.)

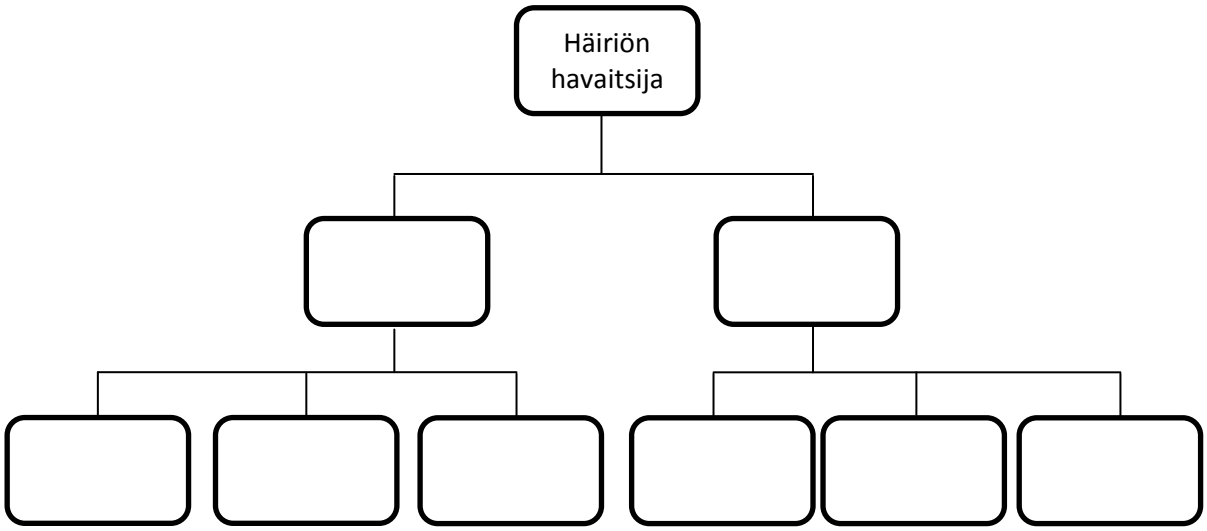
3.2 Toipumissuunnitelmatiimi

Yleisesti olisi hyvä, että toipumissuunnitelmatiimiin kuuluisi henkilöstä yrityksen eri alueilta. Tärkeätä on yrityksen prosessien ja sovellusten tunteminen sekä ymmärtäminen. (Wold 1997.)

Toipumissuunnitelmatiimin tehtävät:

- Roolien ja vastuualueiden jakaminen
- Suunnitelman laajuudesta päättäminen
- Tarvittavien voimavarojen hankkiminen
- Elpymis strategioiden suunnittelu
- Testaaminen
- Päivittäminen ja kehittäminen
- Mahdollisen elpymisen toteuttaminen (Judson 2010, 28.)

Jokainen toipumissuunnitelmatiimiin kuuluva kirjataan suunnitelman yhteystietoluetteloon. Luettelosta nähdään helposti ketä tiimiin kuuluu ja siitä tulisi myös löytyä jokaisen yhteystiedot.(Wold 1997.)



Kaavio 1: Häiriötilanteen soittopuu.

Yhteystietoluettelon lisäksi tulee suunnitella niin sanottu soittopuu (kaavio 1). Häiriötilanteen sattuessa noudatetaan soittopuun järjestystä. Näin vältytään väärinkäsityksiltä ja tieto häiriöstä kulkeutuu nopeasti oikeille henkilöille. Soittopuuta luetaan ylhäältä alaspäin. Ylimpänä soittopuussa on luonnollisesti häiriön havaitsija. Häiriön havaitsija ottaa yhteyden päivystäjään tai muuhun soittopuussa heti hänen alapuolella olevaan henkilöön, joka puolestaan ottaa yhteyden hänen alapuoleltaan löytyviin henkilöihin.

3.3 Mallipohja

Suunnitteluvaihetta helpottaa suuresti mikäli käytettävissä on jonkilainen mallipohja. Niitä myyvät useat yritykset, mutta tarjolla on myös ilmaisia versioita. Pohjan voi rakentaa myös itse. Mallipohjia myyvillä yrityksillä on pohjia useaan eri tarpeeseen, mutta nekään eivät aina ole täydellisesti asiakkaan tarpeita vastaavia. Jonkun toisen tekemää pohjaa voi aina muokata omien tarpeiden mukaiseksi ja siitä voidaan poistaa tai lisätä osia.

Mallipohja koostuu ohjeista ja erilaisista taulukoista. Taulukoihin kerätään tarpeellista informaatiota kuten tärkeitä yhteystietoja sekä palvelinten tietoja. Taulukoita on helppo täyttää sitä mukaa, kun tarvittavaa informaatiota saadaan selvitettyä.

3.4 Kriittiset laitteet

Lähdettäessä tekemään toipumissuunnitelmaa palvelimille ja työasemille, saattaa jo alkumetreillä juolahtaa mieleen, ettei kaikkea ole järkevää jo pelkästään kustannussyistä lähteä sisällyttämään suunnitelmaan. Oleellista on arvioida, mitkä laitteet ovat kriittisiä ja elintärkeitä yritykselle. Erityisesti palvelimet ja työasemat joilla sijaitseva data on korvaamatonta yritykselle, tulee sisällyttää toipumissuunnitelmaan. Hyvänä esimerkkinä yrityksen sähköpostipalvelin. (Wold 1997.)

Kun kriittiset laitteet on arvioitu, voidaan alkaa pohtimaan kuinka kauan jokaisen yksittäisen laitteen voidaan sallia maksimissaan olevan poissa käytöstä. Tätä aikaväliä kutsutaan myös nimellä RTO. RTO:lla tarkoitetaan aika väliä, jolloin häiriöstä palautumisen on tapahduttava, jotta vältyttäisiin vakavilta tappioilta tai jopa konkurssilta. Olennaisinta on siis pyrkiä välttämään sellainen vahinko, jota ei missään nimessä voida ottaa vastaan. Toisinsanoen, koska häiriötilanteessa yleisestiottaen koituu jonkinlaista vahinkoa yritykselle, tulee palvelimille ja työasemille suotavaa palautumisaikaa miettiä realistisesti. (Judson 2010, 141; Wold 1997.)

4 Palautumis strategiat (Elpymissuunnittelu)

Palautumis strategioiden suunnittelun tarkoituksena on tehokas ja nopea palautminen häiriötilanteesta. Strategioita on hyvä suunnitella useampia erilaisten tilanteiden varalle. Häiriö on voinut aiheutua useasta eri syystä, eikä palautumista välttämättä voida tehdä samalla tavalla jokaisessa tilanteessa. Palautumis strategian valintaan voi vaikuttaa myös RTO. Esimerkiksi jos kahdella palvelimilla on merkittävä ero vaadittavassa palautumisajassa, saattaa järkevämpää olla käyttää erilaista palautumisstrategiaa. Näin yritys voi säästää aikaa, rahaa ja vaivaa. (Judson 2010, 32.)

Palautmiseen vaikuttavia seikkoja tulee tutkia tarkasti. Esimerkiksi palvelimien ja työasemien toimittajien kanssa kannattaa keskustella mahdollisen häiriötilanteen toimitusajoista. Yksittäisten komponenttien vaihtaminen sujuu yleensä mutkitta ja suhteellisen nopeasti, mutta jos koko palvelin hajoaa käyttökelvottomaksi, edessä on kokonaan uuden laitteen hankinta. Tällöin kauppiaan kanssa valmiiksi tehty sopimus nopeasta toimituksesta saattaa osoittautuu arvokkaaksi. Tärkeätä on myös muistaa, että laitteiston ei tarvitse palautua priima kuntoon ennen kuin sitä voidaan jo käyttää. Hienosäätöä voidaan jatkaa, kun laite on saatu takaisin käyttökuntoon ja yritykselle tärkeät palvelut (esimerkiksi sähköposti) on saatu toimimaan. (Judson 2010, 141; Wold 1997.)

5 Varmuuskopiointi

Varmuuskopiointi on tärkeän tiedon kopioimista ja varastoimista. Tietokadon sattuessa vaikkapa kannettavassa tietokoneessa, tärkeät tiedostot voidaan palauttaa varmistetusta kopiosta ja hommia voidaan jatkaa normaaliin tapaan. Varmuuskopiointi on tärkeä osa toipumissuunnitelmaa, mutta sitä ei tule pitää toipumissuunnitelmana yksinään. (Wikipedia 2012.)

Tärkeät tiedostot tulee varmuuskopioida säännöllisesti. Mitä tiheämmin varmuuskopiointi tapahtuu, sitä varmemmin tiedostot ovat tallessa eikä ikäviä yllätyksiä pääsee tapahtumaan. Yrityksen tulisi sopia varmuuskopioinnin säännöllisyydestä ja varmistustavasta varmistettavan datan perusteella (päivittäinen, kerran viikossa, inkrementaalinen varmistus, täydellinen varmistus). Täydellinen varmistus tehdään aina ensimmäisellä varmistus kerralla, jolloin kaikki valitut tiedostot varmuuskopioidaan. Tämä saattaa luonnollisesti kestää useitakin päiviä riippuen varmistettavan datan määrästä. Inkrementaalinen varmistus suoritetaan yleisesti ottaen joka päivä. Inkrementaalisessa varmituksessa varmistetaan vain tiedoston muuttunut osa. Tästä syystä inkrementaali voidaan ottaa usein päivittäin, koska varmistettavan datan siirtyminen vie huomattavasti vähemmän aikaa verrattuna täydelliseen varmistukseen. Inkrementaaleista säilytetään usein muutama versio vähintään. Näin ollen jos yritys varmuuskopioi datansa esimerkiksi päivittäin ja he säilyttävät kolme versiota inkrementaaleista, pystyvät he aina paluttamaan tiedoston jopa kolmen päivän takaisessa olomuodossa. Yrityksen varmuuskopiointi toimenpiteisiin tulisi vaikuttaa varmistettavan datan kriittisyys sekä tiedostoissa tapahtuvan informaation muuttuminen. (Judson 2010, 32; Secmeter 2008.)

Yleisesti ottaen tärkeän datan tulisi olla vähintään kahdessa eri paikassa. Käyttöarkiston lisäksi tieto tulisi siis varmistaa toiseen paikkaan, josta se voidaan tarpeen tullen palauttaa.

Varmuuskopioden tietovarastona voi yritys käyttää vaikka siihen vartavasten hankittua palvelinta. Toipumussuunnittelun näkökulmasta tämä ei kuitenkaan riitä. Datan varmentaminen kiinteistön ulkopuolelle takaa huomattavasti paremman, lähes täydellisen suojan tiedon menetykseltä. Varmuuskopiointipalvelua tarjoavat yritykset tulevat tässä tilanteessa apuun, tarjoamalla offsite ja muuta tiedonvarmennuspalvelua.

Tänäpäivänä useissa yrityksissä varmuuskopionti hoituu päivittäin automaattisesti kenenkään siitä kummemmin murhetimatta. Varmuuskopioinnista hyödytään kahdella eri tavalla. Yleisin hyöty on selvästi tiedostojen normaali palautus niiden kadottua. Varmuuskopioinnista hyödytään myös siten, että käyttäjä voi palauttaa tiedoston aikaisemman version inkrementaalista. (Wikipedia 2012.)

6 Testaus

Testaaminen osoittaa toipumissuunnitelman tehokkuuden. Tästä syystä testaamiselle tulee antaa vähintäänkin saman verran painoarvoa kuin suunnitelman tekemiselle. Aika kuluttaa toipumissuunnitelman tehokkuutta, koska teknologia kehittyy ja laitteisto sekä sovellukset uudistuvat. Ei siis riitä, että testausta tehdään vain toipumissuunnittelua rakennettaessa, vaan suunnitelmaa tulisi testata sännöllisesti. (Wold 1997.)

Testausta voidaan tehdä esimerkiksi seuraavilla tavoilla:

- Jäsenneltyllä suullisella läpikäymisellä yhdessä toipumissuunnittelutiimin jäsenien kanssa. Tarkoituksena on varmistaa suunnitelman tehokkuus ja löytää sen pullonkaulat ja heikkoudet.
- Toipumissuunnitelma dokumentin uudelleen läpikäymällä voidaan tarkistaa, että yritys kohtaa sen vaatimusten kanssa.
- Katastrofi skenaarioita läpi käymällä.
- Kokonaisvaltaisilla harjoituksilla. Nämä saattavat kuitenkin tulla kalliiksi ja vaikuttaa yrityksen arkiseen toimintaan. (Wold 1997.)

7 Suunnitelman päivittäminen

Toipumissuunnitelma tulee dokumentoida ja sitä on hyvä päivittää säännöisesti. Yleisenä sääntönä voidaan pitää, että suunnitelma tulisi tarkistaa ja päivittää kerran vuodessa. Mikäli jokin olennainen asia muuttuu, on päivitys syytä tehdä välittömästi. Tällaisia asioita voivat olla esimerkiksi muutokset elpymistiimissä tai laitteistossa. (Judson 2010, 99.)

Toipumissuunnitelman ajantasalla pitäminen on siis erittäin tärkeätä. Pahimmillaan päivittämisen laiminlyönti tekee toipumissuunnitelman täysin hyödyttömäksi. Se saattaa jopa pahentaa vahingon laajuutta väärällä ja vanhentuneella tiedolla.

8 Storage IT toipumissuunnitelma

Storage IT:n toipumissuunnitelma on tarkoitettu heidän varmuuskopiointipalvelun liitteeksi asiakkaan halutessa varautua paremmin katastrofitilanteiden ja muiden pienenpien häiriöiden varalle. Tarkoituksena olisi, että siitä tulisi jossakin vaiheessa myytävä tuote. Suomessa toipumissuunnittelu on vielä niin sanotusti lasten kengissä ja varmuuskopiointia itseseään pidetään jo jonkinmoisena toipumissuunnitelmana. Olen kehittänyt Storage IT:n avustuksella varsin riisuttua ja olennaiseen keskittyvää toipumissuunnitelmaa palvelimille ja työasemille. Suunnitelmalla pyritään pienentämään katastrofista elpymiseen kuluvaa aikaa, jotta asiakas yritys välttyisi suuremmilta tappioilta ja pahimmissa tapauksissa konkurssilta.

Suunnittelin Storage IT:lle mallipohjan, jonka avulla voidaan lähteä rakentamaan yhdessä asiakkaan kanssa heidän tarpeidensa mukaista toipumissuunnitelmaa. Aihe kuulosti minusta aluksi suhteellisen helpolta, kun en ollut vielä syventynyt siihen tarkemmin. Pian minulle kuitenkin valkeni, kuinka suuresta kokonaisuudesta oli kyse. Rajaus helpotti kuitenkin asiaa ja se oli oikeastaan itsestäänselvyys. Storage IT tekisi asiakkailleen vain palvelimille ja työasemille suunnattuja toipumissuunnitelmia.

Mallipohjaa voidaan käyttää toipumissuunnitelman pohjana, jolloinka toipumissuunnitelma rakennetaan suoraan mallipohjan päälle. Vaihtoehtoisesti sitä voidaan käyttää vain tärkeiden tietojen keräämiseen suunnitteluvaiheessa jolloin itse suunnitelma tehdään erilliseen dokumenttiin. Mallipohja sisältää taulukoita, joihin on helppoa syöttää niihin kuuluvaa tietoa sitä mukaan kun sitä saadaan kerättyä. Mallipohjaan voidaan lisätä tai siitä voidaan karsia kohtia asiakkaan niin halutessa.

9 Mallipohjan analysointi ja toipumissuunnitelman rakentaminen

Mallipohjan rakentaminen oli melko hankala projekti. Lähes kaikki aineisto oli englanninkielistä ja jouduinkin tilaamaan kirjoja ulkomailta. Internetistä löytyi paljon aineistoa, mutta monet käsittelivät aihetta hieman eritavalla kuin toiset. Yhdistelin toisten ideoita ja jätin pois sellaista mikä ei ollut välttämätöntä. Yleisesti ottaen lähes kaikessa

aineistossa puhuttiin suurista amerikkalaisista yrityksistä, joten lukeemansa piti miettiä tarkkaan ja kuinka sitä soveltaisi pienempiin Suomalaisiin yrityksiin. Mallipohjan rakennuksessa minun tuli erityisesti ottaa huomioon Storage IT:n tarpeet, sillä heille olin kyseistä pohjaa tekemässä. Suuri painoarvo olisi näin ollen myös varmuuskopioinnilla.

Suunnittelemani mallipohjan rakenne on pääpiirteittäin seuraavanlainen:

1. Riskianalyysi
2. Toipumissuunnitelma tiimin perustaminen
3. Ympäristön kuvaus
4. Varmuuskopiointisuunnitelma
5. Valvontasuunnitelma
6. Elpymissuunnitelma
7. Testaussuunnitelma

9.1 Riskianalyysi

Riskianalyysi on edellytys sille, että koko toipumissuunnitelmaa voidaan lähteä edes tekemään. Riskien käsittelyn pohjalta voidaan päätyä esimerkiksi sellaiseen tulokseen, että yrityksen on panostettaava enemmän häiriötilanteisiin jolloin koko liiketoiminnan jatkuminen saattaa olla vaakalaudalla. Nyt kun kyse on palvelimista ja työasemista, voidaan riskianalyysiäkin rajata sen mukaan. Mallipohja ei sen erityisemmin kuitenkaan puutu riskianalyysin tekemiseen, vaan siihen kirjataan riskianalyysin tulokset. Yleisesti ottaen voidaan ajatella, että kun asiakas ottaa yhteyttä varmuuskopiointipalvelua tarjoavaan yritykseen, niin riskejä ollaan jo käsitelty ja päätetty lähteä pienentämään. Riskeistä varmasti kuitenkin vielä keskustellaan toipumissuunnitelmaa rakennettaessa Storage IT:n kanssa.

Riskianalyysin tulokset kirjataan mallipohjassa olevaan taulukkoon. Tämä auttaa hahmoittamaan toipumissuunnitelman tarpeellisuutta. Riskit näkyvät aina toipumissuunnitelmaa luekvalle ja ovat muistuttamassa, siitä miksi koko suunnitelma on olemassa. Aivan ensimmäiseksi kirjataan huomioon otetut riskit. Tämän jälkeen riskin kriittisyysaste ja todennäköisyys. Lopuksi kirjataan vielä, onko riskin torjunta mahdollista.

9.2 Toipumissuunnitelmatiimi ja elpymistiimi

Mallipohjani ei määrittele sitä, montako henkilöä toipumissuunnitematiimiin tulisi kuulua. Tämän kaltaisessa toipumissuunnitelmatiimissä ei kuitenkaan tarvita montaa kymmentä eri osa-alueista huolehtivaa henkilöä.

Tiimi koostuu pääasiassa asiakkaan vastuuhenkilöstä ja muista projektiin kuuluvasta henkilöstöstä (tietoturvavastaavat ja muut IT-asiantuntijat), Storage IT:n asiakaspalvelusta sekä Storage IT:n toipumissuunnitelma vastaavasta. Asiakasyrityksen johdon mukana olo projektissa on myös ensijaisen tärkeätä.

Mallipohjasta löytyy kenttä johonka merkitään asiakkaan vastuuhenkilö/t. Tämän lisäksi erilliseen taulukkoon kirjataan jokaisen tiimin kuuluvan yhteystiedot. Taulukko helpottaa niin tiimin jäseniä kuin muitakin asiakkaan työntekijöitä tiedostamaan, keitä tiimiin kuuluu.

Toipumissuunnitelmatiimin jäsenistä kootaan erikseen niin sanottu elpymistiimi, jonka tehtävänä on toimia itse häiriötilanteessa. Elpymistiimiin kuuluvista kootaan häiriötilanteen soittopuu, josta mahdollisen häiriön havaitsija pystyy nopeasti katsomalla ottamaan yhteyttä elpymistiimin päivystäjään. Päivystäjä puolestaan osaa ottaa yhteyttä soittopuussa seuraavan tason henkilön jne. Ideana on kuitenkin se, että elpymistiimin jokainen jäsen olisi mahdollisimman nopeasti tietoinen häiriöstä ja elpyminen voitaisiin aloittaa ripeästi. Hyvänä esimerkkinä tärkeän palvelimen epäkuntoon meno viikonloppuna.

9.3 Muut tärkeät yhteystiedot

Se, että kaikki tärkeät yhteystiedot löytyvät häiriön sattuessa samasta paikasta, säästää jo aikaa ja vaivaa. Tällaisia yhteystietoja ovat esimerkiksi laitteiden toimittajat, vakuutusyhtiö ja yhteistyökumppanit. Tärkeätä on myös pohtia mihin muihin ulkopuolisiin tahoihin häiriö saattaa vaikuttaa ja tuleeko heihin ottaa yhteyttä häiriön sattuessa.

Toipumissuunnitelmaan tulee siis kirjata kaikki tärkeät yhteystiedot. Yhteystiedoista kannattaa tehdä yksi lista, josta löytyy kunkin yhteystiedon puhelinnumero, yhteyshenkilö ja yritys / nimi.

9.4 Sovellusluettelo

Sovellusluetteloon kerätään kaikki tärkeät sovellukset, jotka pyörivät palvelimilla ja työasemilla. Luetteloon kirjataan onko kyseessä kriittinen sovellus ja onko sen lisenssi voimassa tai CD tallella.

Sovellusluetteloon on hyvä kirjata käyttöjärjestelmät samalla tavalla kuin muutkin sovellukset. Mikäli esimerkiksi käyttöjärjestelmälisenssi on päässyt vanhentumaan ja samanaikaisesti virus turmelee työaseman, saattaa työaseman kuntoon saanti viivästyä vanhentuneen lisenssin takia.

9.5 Ympäristön kuvaus

Laiteluetteloon kerätään tärkeät laitteet eli tässä tapauksessa palvelimet ja työasemat joilla on kriittistä dataa. Mallipohjan taulukkoon kirjataan jokaisesta laitteesta toimittaja, onko laite kriittinen, onko laite oma sekä RTO. Tärkeätä on muistaa myös se, että jokainen näistä laitteista tulee varmuuskopioida.

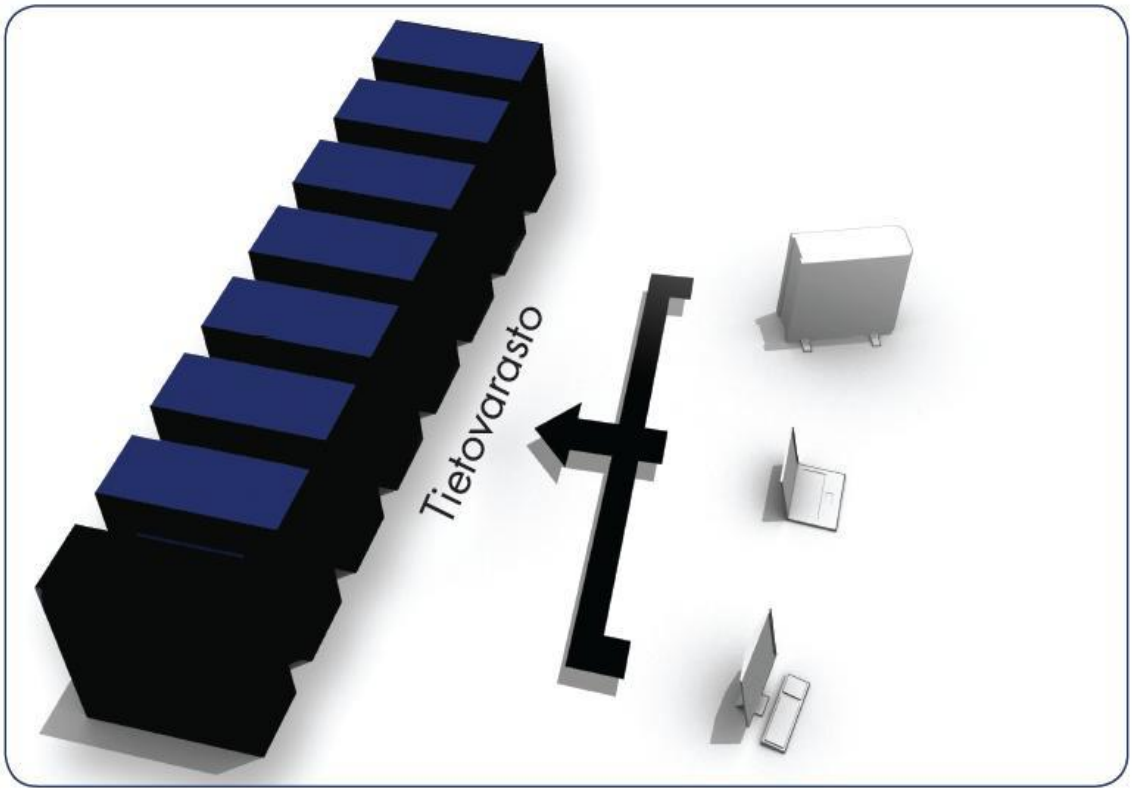
Laiteluetteloa kannattaa päivittää säännöllisesti ja se tulee pitää ajantasalla. Uudet laitteet, tulee sisällyttää suunnitelmaan ja vanhat on syytä poistaa siitä. Näin vältytään turhilta ongelmilta.

9.6 Varmuuskopiointisuunnitelma

Varmuuskopioinnilla on suuri merkitys pohdittaessa ja rakennettaessa elpymisstrategioita. Kaikki varmuuskopioitavat laitteet löytyvät jo laiteluettelosta, jotenka niitä ei tarvitse enää tässä vaiheessa sen kummemmin miettiä. Varmuuskopioinnin osalta mallipohjaan kerätään varmuuskopioitavat tiedostotyypit, yhteensä varmistettu datan määrä, Storage IT:tä ostetun lisenssin koko, versioiden määrä, RPO, varmistusajankohta sekä turva-avain.

Tiedostotyypit vaikuttavat pakkaustehoon, joka yleisesti ottaen on todella tehokas. Käytettäessa Storage IT:n varmuuskopiointisovellusta, perinteisten tekstitiedostojen pakkausteho on noin 70 %, kun puolestaan kuvilla se on vain 1-2% verran. Pakkausteho vaikuttaa suoraan lisenssin kokoon, sillä jos asiakkaan tiedostot pakkautuvat tehokkaasti, heidän varmuuskopiointi kustannukset pienenevät huomattavasti.

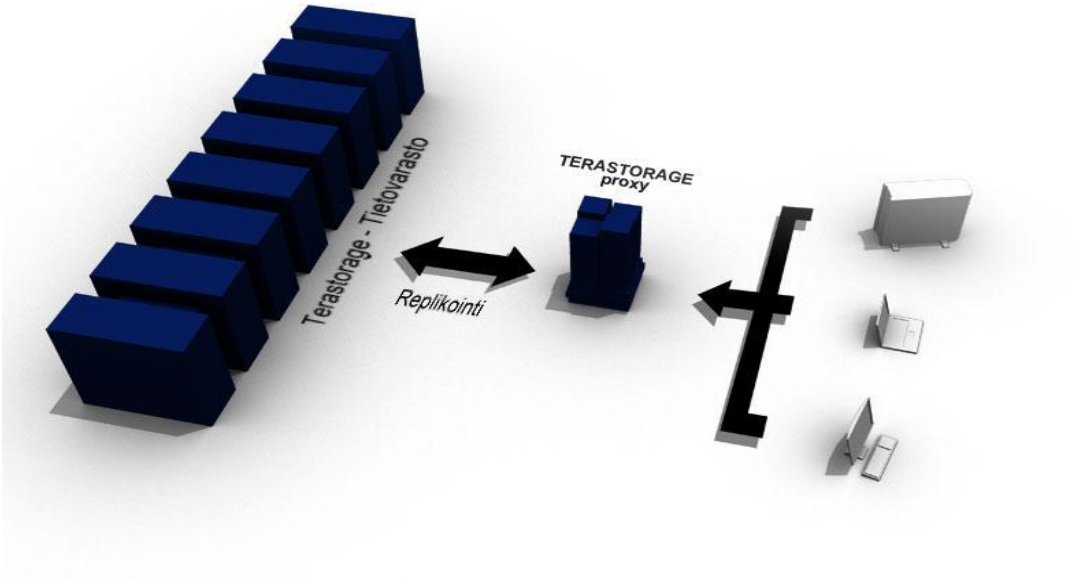
Varmuuskopiointi tapahtuu, joko Core- tai Terastoragesovelluksen avulla. Käytettäessä niin sanottua peruspalvelua eli Corea (kuvassa 2), tapahtuu varmuuskopiointi työasemalta tai palvelimelta suoraan Internetin yli Storage IT:n tietovarastoon.



Kuva 1: palvelukuvaus - Storage IT.

Asiakas voi halutessaan sisällyttää varmuuskopiointikokonaisuutensa välityspalvelimen eli proxyn (kuvassa 3). Proxy asennetaan asiakkaan omaan lähiverkkoon ja sen tarkoitus on toimia yrityksen paikallisena tietovarastona, josta varmistettu data replikoidaan Storage IT:n tietovarastoon. Tämä tarkoittaa sitä, että data sijaitsee palvelimella tai työasemalla, proxyllä ja Storage IT:n tietovarastossa samanaikaisesti. Datan sijaitessa kolmessa eri paikassa, on erittäin epätodennäköistä, että jotakin tietoa pääsisi katomaan.

Replikointia tehdään yleensä yöaikaan tai sellaiseen aikaan jolloin verkon kuormitus on hiljaisimmillaan. Yleensä kuitenkin pyritään siihen, että asiakas saisi täydellisen turvakopioin yrityksen ulkopuolelle kerran viikossa. Hyvä ajankohta replikoinnille on usein myös viikonloppu. Tätä turvakopiota voidaan käyttää katastrofipalautumiseen, tilanteeseen, jossa palautuksia ei voida tehä asiakkaan lähiverkoon kytketyltä proxyltä.



Kuva 2: Terastorage palvelukuvaus – Storage IT.

Proxyn pääasiallinen tehtävä on suorittaa nopeat paikalliset palautukset. Jos erimerkiksi kannettava tietokone hajoaa, voi asiakas toteuttaa palautustoimenpiteet itsenäisesti ilman, että tarvitsisi turvautua Storage IT:hen. Vasta kun ongelmia on itse proxyssä joudutaan ottamaan yhteys Storage IT:hen. Storage IT valvoo jatkuvasti proxy-plavelimen tilaa ja pystyy ilmoittamaan asiakkaalle, jos jokin on siinä vialla.

9.7 Valvontasuunnitelma

Jotta koko suunnitelmasta olisi mitään hyötyä, täytyy valvonnan toimia. Tässä kohtaa puhutaan varmuuskopioinnin valvonnasta ja sen raportoinnista. Valvonnan tulee olla järjestelmällistä ja huolellista, niin että varmuuskopioinnissa tapahtuvat häiriöt ja ongelmat huomataan ajoissa ja niihin pystytään reagoida.

Asiakkaille lähetetään viikoittain myös raportti kuluneen viikon varmistustapahtumista. Raportissa ilmoitetaan esimerkiksi, jos varmistus ei ole onnsitunut jonain päivänä. Lisäksi valvonnasta lähtee hälytysraportteja, mikäli työaseman varmistusta ei olla suoritettu yli kahdeksaan vuorokauteen. Tämä on tärkeätä siksi, että esimerkiksi kannettavallatietokoneella työskentelevät eivät aina huomaa tarkistaa onko varmuuskopiointi suoritettu kyseisenä päivänä ja sulkevat kannettavansa kesken varmuuskopioinnin tai jopa ennen kuin koko varmistusa on keretty aloittamaan.

Edellä mainittu oli niin sanottua automaattista valvontaa. Lisäksi valvontaa voidaan suorittaa valvonnasta vastaavien ihmisten toimesta niin asiakkaan kuin Storage IT:n puolella. Valvonta on laaja alue toipumissuunnittelussa ja siitä onkin syytä sopia asiakkaan kanssa tarkkaan, kuinka se toteutetaan. Valvonnan tehtävänä on pitää huoli siitä, että asiakkaan palvelinten ja työasemien varmistus toimii.

Mallipohjaan kirjataan valvonnan ja raportoinnin osalta siitä vastuussa olevat henkilöt yhteystietoineen. Lisäksi tärkeätä on kirjata sovitut valvonta ja raportointi rutiinit. Erityisen tärkeille palvelimille voidaan kirjata omat valvontarutiinit, joiden tarkoitus on esimerkiksi pitää huoli siitä, että varmuuskopiointi on onnistunut jokaisena päivänä.

9.8 Elpymissuunnitelma

Se miten häiriötilanteessa ja nimenomaan arvokkaan datan menetystilanteessa toimitaan, ratkaistaan elpymissuunnitelmalla. Elpymissuunnitelmia havainnollistetaan helpoiten erilaisilla katastrofi skenaarioilla ja niihin pohjautuvilla elpymis strategioilla. Jokaiselle skenaariolle luodaan siis oma elpymis strategia. Kun riskianalyysi on tehty huolella, on elpymissuunnitelmaakin helpompaa lähteä suunnittelemaan. Mitkä ovat ne todennäjöisimmat riskit, jotka uhkaavat yritystä? Mitä voi tapahtua? Riskeistä voidaan rakentaa katastrofi-skenaarioita, jotka auttavat yritystä hahmoittamaan, kuinka niihin voidaan varautua. Kaikkiin riskeihin on mahdotonta varautua, joten tärkeintä on arvioida todennäköisimmät ja vaarallisimmat riskit, joista lähdetään rakentamaan skenaarioita.

Katastrofiskenaarioita lähdettäessä tekemään on tärkeätä miettiä, mitä voi tapahtua ja mikä on pahin mahdollinen, mitä voi tapahtua. Pahimpia mahdollisia uhkia voisi olla esimerkiksi:

- Palvelimen / työaseman kakkien tietojen menetys niin, että jäljellä ovat vain varmuuskopiot
- Palvelimen kaikki levyt hajoaa
- Tulipalo
- Varkaus

Havainnollistetaan elpymissuunnitelmaa esimerkki skenaariolla jossa yrityksellä on Storage IT:n varmuuskopiointipalvelu, mutta ei toipumissuunnitelmaa. Esimerkeissä palautettavan datan määräksi on asetettu 1TB jolloinka, palautuksia ei voida tehdä suoraan Internetin yli järkevässä ajassa.

1. Työntekijä huomaa maanantaiaamuna kello 8.00, että palvelin on varastettu.

2. Hän ilmoittaa asiasta toimitusjohtajalle, joka ottaa yhteyttä Storage IT:n asiakaspalveluun kello 9.00, jolloinka se aukeaa.
3. Toimitusjohtaja ja Storage IT:n asiakaspalvelu sopivat, että data toimitetaan fyysisellä medialla asiakkaalle 48 tunnin sisällä (peruspalvelutaso).
4. Tämän jälkeen toimitusjohtaja soittaa it-palveluyritykseen ja tilaa uuden palvelimen ja saa sen asennuksen kahden päivän päähän.
5. Kahden päivän päästä keskiviikkona aamulla varmuuskopiot on toimitettu asakkaalle-IT-palveluyrityksen palvelimen asentaja saapuu paikalle samana aamuna uusi palvelin kainalossa ja aloittaa asennustyöt.
6. Asennuksessa menee koko päivä.
7. Työntekijät pääsenvät jatkamaan töitä seuraavana aamuna, torstaina kello 8.00

Palvelimen varkauden seurauksena on siis kolmen päivän käyttökatko, jossa saattaa todellisuudessa kestää vielä pitempäänkin. Tästä voi lähteä miettimään paljonko rahaa on kulunut hukkaan pelkästään siinä, että esimerkiksi 10 työntekijää ovat istuneet kolme päivää taukotilassa kahvia juoden, koska eivät ole voineet tehdä töitä.

Mitä voidaan siis tehdä, jotta käyttökatkos saataisiin supistettua kolmen päivän sijaan vain yhteen päivään:

1. Kuinka saadaan menetetty data nopeammin takaisin?
   - Data saadaan nopeasti takaisin jos yrityksellä on välipalvelin eli proxy. Näin ollen data saadaan takasin muutamassa tunnissa.
   - Jos yrityksellä ei ole proxyä, data joudutaan tuomaan siis fyysisellä medialla. Asiakas voi valita Storage IT:tä myös korotetun pavelutason, jolloinka data toimitetaan nopeammin asiakkaalle.
2. Kuinka saadaan uusi palvelin + asennus nopeammin?
   - Voidaanko sopia it-palveluntarjoajan kanssa kiiretoimitus mahdollisuudesta?
   - Voiko it-palveluntarjoaja ylläpitää varapalvelinta?
   - Yritys voi myös itse säilyttää vara palvelinta.
   - katastrofitilanteessa jossa tärkeä palvelin on varastettu, voidaan myös katsoa parhaaksi valjastaa jokin vähemmän kriittinen palvelin varastetun palvelun rooliin.

Esimerkkjä ja skenaarioita kannattaa tehdä erilaisten tilanteiden varalle. Tarkka suunnittelma helpottaa elpymistä, sillä häiriön hetkellä ei tarvitse enää lähteä tuhlaamaan aikaa miettimiseen tai suunnittelemiseen sen kummemmin.

Halutesaan yritys voi tehdä muita järjestelyjä elpymisen nopeuttamiseksi. Esimerkiksi palvelimien ja sovellusten konfigurointi asetukset voidaan kirjoittaa muistiin.

Elpymissuunnitelman osalta mallipohjaan kirjataan elpymis strategioita erilaisten katastrofitilanteiden varalle. Katastrofi skenaarioita käydään läpi myös testauksessa.

9.9 Testaussuunnitelma

Testaussuunnitelmaan kerätään katastrofiskenaariot sekä muut testattavat asiat. Jokainen testattava asia merkitään taulukkoon, josta voidaan seurata, mitä on testattu, koska on testattu ja onko testi onnistunut.

Tässä vaiheessa voidaan siis käydä läpi uudemman kerran katastrofiskenaarioita ja erityisesti testataan kuinka niihin varautuminen onnistuu. Esimerkiksi datan siirtonopeutta voidaan testata helposti ilman, että se vaikuttaisi yrityksen muuhun toimintaan. Lisäksi voidaan harjoitella esimerkiksi palvelimen ja sovellusten asennusta sekä niiden konfigurointia niin, että niiden kanssa ei tule ongemia katastrofitilanteessa.

10 Yhteenveto ja loppusanat

Tästä aiheesta opinnäytetyön tekeminen on avannut minulle aivan uuden puolen liiketoiminnan jatkuvuuden turvaamisesta. Monimutkaisuudestaan ja laajuudestaan huolimatta, toipumissuunnittelu on miestäni mielenkiintoinen aihe alue, joka tuo hyvin esille yrityksen ongelma kohtia. Tavoitteenani oli luoda Storage IT:lle toipumissuunnittelun mallipohja, jota hyödyntämällä Storage IT voisi lähteä myymään toipumissuunnitelmaa varmuuskopiointipalvelu asiakkailleen. Projekti onnistui hyvin, vaikka varsinaisia tuloksia joudutaankin jäädä vielä odottelemaan, sillä toipumissuunnitteluprojekti on vielä kesken Storage IT:llä.

Toipumissuunnittelua voidaan pitää tänä päivänä tärkeänä asiana harjoitettaessa liiketoimintaa. Varisinkin kun elämme taantuma aikaa ja pienetkin virheet saattavat kostautua vakavilla seuraamuksilla. Useat yritykset saattavat ajatella säästävänsä sillä, etteivät halua tuhlata aikaa ja rahaa moiseen suunnitteluun, koska kokevat isopmpien ongelmien olevan niin epätodennäköisiä. Tästä voisikin leikkisästi ajatella, että tällaiset yritykset säästävät väärässä päässä ja pelaavat lottoa panoksenaan yrityksen tulevaisuus.

Lähteet

Iivari, M. & Laaksonen, M. 2009. Liiketoiminnan jatkuvuussuunnittelu ja ICT-varautuminen. Tallinna:Tallinna Raamatutrükikoda.

Judson, J. 2010. Disaster Recovery Best Practices – Templates. Washington: U.S. Government printing office.

Juvonen, M. ,Korhonen H. ,Ojala, ,V-M. Salonen, T. & Vuori, H. 2005. Yrityksen riskienhallinta. Helsinki: Yliopistopaino.

Kuusela, H. & Ollikainen R. 2005. Riskit ja riskienhallinta. Tampere: Tampereen yliopistopaino-Juvenes Print Oy.

Vänninen, T. 2012. Mobiiliturvan ABC. MikroPC 4/2012.

Internet lähteet

IBM. 2002. Iseries Information Center. Viitattu 4.4.2012.
http://publib.boulder.ibm.com/iseries/v5r2/ic2924/index.htm?info/rzaj1/rzaj1sampleplan.htm

Secmeter. 2008. Varmuuskopiointi. Viitattu 30.5.2012.
http://www.secmeter.com/varmuuskopiointi.html

Wikipedia. 2012. Riskienhallinta. Viitattu 22.5.2012.
http://fi.wikipedia.org/wiki/Riskienhallinta

Wikipedia. 2012. Backup. Viitattu 25.5.2012. http://en.wikipedia.org/wiki/Backup

Wikipedia. 2012. Työasema. Viitattu 25.5.2012. http://fi.wikipedia.org/wiki/Ty%C3%B6asema

Wold, G. 1997. Disaster recovery planning process. Viitattu 22.5.2012.
http://www.drj.com/new2dr/w2_002.htm

Kuvat

Kaaviot