



**LAUREA**  
AMMATTIKORKEAKOULU

*Uuden edellä*

# PK-yrityksen varmuuskopioinnin automati- sointi

Sillanmäki, Tomas

2014 Laurea Leppävaara

Laurea-ammattikorkeakoulu  
Laurea Leppävaara

## PK-yrityksen varmuuskopioinnin automatisointi

Tomas Sillanmäki  
Tietojenkäsittelyn tradenomi  
Opinnäytetyö  
Joulukuu, 2014

Tomas Sillanmäki

**PK-yrityksen varmuuskopioinnin automatisointi**

Vuosi 2014

Sivumäärä 55

---

Tämän opinnäytetyön tavoitteena oli kohdeorganisaation varmuuskopioinnin kehittäminen ja uudistaminen sekä sitä kautta yrityksen työntekijöiden työmäärän vähentäminen. Työmäärän vähentäminen onnistui vertailemalla varmuuskopiointiohjelmia ja valitsemalla sellainen, jossa varmistukset pystyi ajastamaan menemään automaattisesti päivittäin.

Varmuuskopiointiohjelmia vertailtiin Kepner & Tregoen-päätöksentekomallin perusteella. Mallia varten selvitettiin yrityksen tietoaineiston varmistuksen kannalta tärkeimmät ominaisuudet ohjelmalle sekä asetettiin ne tärkeysjärjestykseen. Tutkimukseen valittuja ohjelmia vertailtiin niiden ominaisuuksien perusteella ja näin saatiin valittua soveltuvin ohjelma yrityksen tiedostojen varmistamiseen.

Tässä työssä tutkittiin myös erilaisia tallennuslaitteita, joille varmuuskopioinnin voi suorittaa. Tallennuslaitteiden vertailu suoritettiin Benchmarkingin avulla. Benchmarkingin avulla vertailtiin tallennuslaitteiden hyviä sekä huonoja puolia ja tällä tavalla selvitettiin mikä olisi paras tallennuslaite yrityksen käyttöön ja mitä vaaditaan sen käyttöönottoon. Näiden kahden vertailun avulla valittiin ohjelma varmistukseen ja saatiin selville erilaisia laitteita, joille varmistukset voi suorittaa.

Tutkimuksen perusteella opinnäytetyön asiakas voi ottaa käyttöönsä uuden varmuuskopiointiohjelman, joka helpottaa varmistusten suorittamista, koska ne tapahtuvat automaattisesti työntekijöiden ulkopuolella työntekijöistä riippumatta eivätkä vaadi manuaalista työtä. Lisäksi asiakkaalle tarjotaan erilaisia tallennuslaitteivaihtoehtoja, jotka voivat myös nopeuttaa ja helpottaa varmistusten suorittamista. Uuden ohjelman ja mahdollisten uusien laitteiden käyttöönotto on toteutettavissa helposti ja suhteellisen pienellä budjetilla.

Tomas Sillanmäki

**Automating Backup for a Small and Medium-sized business**

Year

2014

Pages

55

---

The object of this thesis is the development and renewal of a backup system of the target organization and therefore the easing of the workload of the employees. Lightening the workload was achieved by comparing and choosing a backup software that offered the possibility of automatic backups.

The backup software were compared based on Kepner & Tregoe decision making model. The most critical features for the backup software were discovered and put into order of importance. The software chosen for the research were compared based on their features and therefore the best possible backup software was chosen to insure the safe keeping of the company's data.

Also, during the research different storage devices were compared. The comparison was done with the aid of benchmarking. Benchmarking was used to compare the advantages and disadvantages of the devices to indicate what would be the best storage device for the company and what is required for the deployment of the device. With these two comparisons the best backup software was chosen and the offering of suitable devices, to which to perform the backups, was found out.

Based on the research the customer can implement the new backup system which will make it easier to perform the backups, because they are done automatically outside the office hours and they do not require manual maintenance. Also, a variety of storage device options which will speed up and make backups easier will be offered to the customer. The deployment of the new backup system and possible new devices will be easily achieved and the budget will stay at a fairly moderate level.

Keywords: backup, automation, Kepner & Tregoe, Benchmarking, storage device

## Sisällys

1	Johdanto.....	7
1.1	Kohdeyritys.....	7
1.2	Tavoite.....	8
1.3	Aiheen rajaus.....	8
2	Teoreettinen viitekehys.....	8
2.1	Keskeiset käsitteet.....	9
2.2	Aineisto.....	10
3	Menetelmät.....	10
3.1	Tutkimusongelmat.....	10
3.2	Benchmarking.....	11
3.3	Kepner & Tregoe.....	12
3.4	Asiantuntijahaastattelu.....	12
4	Varmuuskopiointi.....	12
4.1	Suunnittelu.....	14
4.2	Riskienhallinta.....	14
4.3	Erytyypiset varmuuskopioinnit.....	15
4.4	Tiedostojen palautus.....	16
4.5	Varmuuskopioinnin merkitys tietoturvassa.....	17
4.6	Varmuuskopioiden säilyttäminen.....	17
4.7	Yrityksen laitteisto.....	18
4.8	Varmuuskopioinnin nykytila.....	18
4.9	Varmuuskopioinnin tarve.....	19
5	Tallennusmediat.....	20
5.1	Optiset tallennusvälineet.....	20
5.2	Haihtumaton muisti.....	21
5.3	Magneettiset tallennusvälineet.....	23
5.4	Etävarmistus.....	29
5.5	Vertailut.....	31
5.5.1	Tallennuslaitteiden Benchmarking-vertailu.....	34
5.5.2	Ohjelmien Kepner & Tregoe-vertailu.....	36
5.5.3	Tulokset.....	37
6	Yhteenveto.....	39
	Lähteet.....	41
	Kuvat.....	46
	Kuviot.....	47
	Taulukot.....	48
	Liitteet.....	49



## 1 Johdanto

Tämän opinnäytetyön aiheena on kohdeorganisaation varmuuskopiointin kehittäminen ja uudistaminen. Näillä kehittämistoimilla yritys pyrkii liiketoiminnan aikaisempaa parempaan suojaukseen. Yrityksen nykyiseen varmuuskopiointiin tutustuttiin haastatteluiden pohjalta ja todettiin, että nykyinen toimintatapa on aikaa vievää ja työllistää yrityksen työntekijöitä päivittäin. Esille nousi tarve kehittää yritykselle automaattinen varmuuskopiointi. Yritykselle valittiin varmuuskopiointiohjelma sekä käytettävä tallennusmedia Benchmarkingin ja Kepner & Tregoen-mallin avulla.

Työn toimeksiantaja on koulu- ja päiväkotikuvauksiin erikoistunut valokuvausyritys. Yrityksen toiminta keskittyy syksyyn, kun kouluissa alkaa uusi lukukausi ja päiväkoteihin tulee uudet lapset ja on aika ottaa luokka- ja ryhmäkuvat. Tämän lisäksi toiminta on vilkkaampaa jouluna, syksyn ja kevään ylioppilasjuhlien aikaan sekä vanhojen tanssien yhteydessä helmikuussa. Yrityksen asiakkaita ovat koululaisten ja päiväkotilasten vanhemmat.

Työssä tutustutaan erilaisiin varmuuskopiointiohjelmiin ja näiden piirteisiin. Lisäksi vertaillaan erilaisia tallennuslaitteita, joihin varmuuskopiointin voi suorittaa sekä tutkitaan etävarmistuksen ominaisuuksia. Saatujen tulosten perusteella valittiin yritykselle sopivin ohjelma ja varmistuslaite.

Opinnäytetyössä valitun ohjelman on tarkoitus automatisoida yrityksen varmuuskopiointi. Tavoitteena on, että varmistus suoritetaan taustalla ilman, että työntekijöiden tarvitsee tehdä sitä manuaalisesti. Tämä vähentää huomattavasti varmuuskopioiden suorittamiseen käytettävää aikaa.

Tässä luvussa käydään läpi opinnäytetyön tavoitteet ja aiheen rajaus sekä kuvaillaan tarkemmin kohdeyritystä ja sen toimintaa.

### 1.1 Kohdeyritys

Opinnäytetyön aiheen valinta on työelämälähtöinen. Kohdeyritys on päiväkoti- ja koulukuvausyritys, joka ottaa satojatuhansia digitaalisia valokuvia vuosittain. Valokuvia otetaan useilla eri digijärjestelmäkameroilla ja ne kulkevat useamman eri tallennusvälineen kautta ennen kuin lopullinen fyysinen tuote on toimitettu asiakkaalle.

Tallennusvälineen, kuten tietokoneen sisäisen kiintolevyn, hajoaminen olisi kriittistä yrityksen toiminnalle. Yrityksen liiketoiminnan kannalta on ehdottoman tärkeää taata luotettavat var-

muuskopiot yrityksen tuotteista, asiakastiedoista ja tilauksista. Tallennusvälineen rikkoutessa, ilman varmuuskopioita, yritys menettää tuotteensa.

Yrityksen valokuvista tehdään monenlaisia fyysisiä tuotteita. Valokuvia saa perinteisten valokuvapaperille tulostettujen kuvapakettien lisäksi erilaisina lisätilaustuotteina. Asiakkaat voivat tilata esimerkiksi viivoittimia, kahvimukeja ja hiirimattoja omilla kuvillaan.

## 1.2 Tavoite

Tämän opinnäytetyön tarkoituksena on löytää kohdeyritykselle sopivin varmuuskopiointiohjelma. Opinnäytetyössä tarkastellaan mikä ohjelma on yrityksen vaatimusten mukainen: säännöllisesti ajastettava ja mahdollisimman helppokäyttöinen työntekijöille. Työn tavoitteena on helpottaa ja yksinkertaistaa yrityksen varmuuskopiointia.

Yhtenä tavoitteena on myös, että varmuuskopiointi vaatisi mahdollisimman vähän ylläpitoa yrityksen henkilökunnalta. Opinnäytetyö tulee muuttamaan yrityksen varmuuskopiointia nykyistä toimivammaksi ja samalla suojelemaan yrityksen liiketoimintaa. Liiketoimintaa suojellaan varmistamalla yrityksen kriittinen data.

## 1.3 Aiheen rajaus

Opinnäytetyö painottuu yrityksen tietoaineiston varmuuskopiointiin ja sen automatisointiin. Tavoitteena on selvittää yritykselle sopivin varmuuskopiointiohjelma ja tallennusmedia, jolle varmuuskopiot voi tehdä. Opinnäytetyö ei ota kantaa sen syvällisemmin yrityksen tietoturvan muihin osa-alueisiin.

Tässä opinnäytetyössä keskitytään Windows-koneiden varmuuskopiointiin kohdeyrityksen toiveesta. Yritys on tyytyväinen Mac-koneiden omaan Time Machine-varmuuskopiointiohjelmaan, joten opinnäytetyö rajataan Windows-koneiden varmuuskopiointiin. Jos ohjelma on kuitenkin yhteensopiva sekä Windows- että OS X-käyttöjärjestelmien kanssa ja se osoittautuu toimivaksi niin tämä helpottaa siirtymistä yhteen valittuun ohjelmaan.

## 2 Teoreettinen viitekehys

Teoreettisella viitekehityksellä tarkoitetaan sitä, mistä näkökulmasta työtä käsitellään ja mikä on taustalla oleva teoreettinen tieto. Tässä opinnäytetyössä näkökulmana on yrityksen työntekijän näkökulma. Tutkimuksessa selvitetään mitä varmuuskopion suorittaminen vaatii työntekijältä nyt ja miten muutokset tulevat vaikuttamaan prosessiin. Teoriapohja muodostuu IT-alan kirjallisuudesta, jonka avulla pystytään arvioimaan varmuuskopiointin vaatimuksia.



## 2.1 Keskeiset käsitteet

Automaatio	Itsetoimiva laite, järjestelmä tai ohjelma.
Blu-ray	Korkeatarkkuuksinen optinen levy. Tallennustilaa noin 25 Gt.
Cd-levy	Compact Disc. Tallennustilaa noin 700 Mt.
DVD-levy	Digital Video Disc. Tallennustilaa noin 4,7 Gt.
Etävarmistus	Data varmuuskopioidaan asiakkaan päätelaitteelta tai palvelimelta palveluntarjoajan pilveen.
Flash-muisti	Muisti, joka ei tyhjennä tallennettuja tietoja vaikka laitteen virta katkaistaan.
IDE	Kiintolevyn liitântä. Tunnetaan myös nimellä EIDE, ATA & PATA.
iSCSI	iSCSI-liitântä käyttää IP-protokollaa tallennuslaitteiden yhdistämiseen.
NAS	Network Area Storage. Ulkoinen verkkokiintolevy.
Optinen media	Optiset tallennuslaitteet ovat levyjä, joita luetaan laserilla. CD-DVD- ja Blu-Ray-levyt.
Provisiointi	Uusien palveluiden käyttö on joustavaa ja jopa automaattista eikä uusia asiakkaita, palveluiden lisäämistä tai käytön lopettamista varten tarvitse ostaa uusia laitteita.
RAID	Redundant Array of Independent Disks. Useita kiintolevyjä yhdistetty toisiinsa yhdeksi loogiseksi levyksi.
RPM	Rotations per minute eli pyörimisnopeus.
SAN	Storage Area Network. Tallennusverkko tiedon tallennukseen.
SAS	Serial Attached SCSI. Kiintolevyn liitântätapa.

SATA	Serial-ATA. Kiintolevyn liitännätapa.
SCSI	Small Computer System Interface. Kiintolevyn liitännätapa.
SD	Secure Digital- muistikortti.
SDHC	Secure Digital High Capacity-muistikortti.
SDXC	Secure Digital Extended Capacity-muistikortti.
SSD	Solid-State-Drive. Kiintolevy, joka ei sisällä liikkuvia osia.
Time Machine	OS X-käyttöjärjestelmän varmuuskopiointiohjelma.
Varmuuskopiointi	Kopio siltä varalta, että alkuperäinen tieto häviää tai tuhoutuu.

## 2.2 Aineisto

Opinnäytetyön aineistona käytetään IT-alan kirjallisuutta, lehtiartikkeleita ja internet-lähteitä, joiden avulla tutustutaan varmuuskopioinnin käsitteisiin, varmistuskeinoihin ja tallennuslaitteisiin. Erilaisiin varmuuskopiointikeinoihin ja niihin liittyviin tekniikkoihin lähdettiin tutustumaan asiantuntijahaastattelun avulla. Lisäksi työtä varten etsittiin tietoa tutkimusmenetelmistä.

## 3 Menetelmät

Tässä luvussa kerrotaan opinnäytetyössä käytettävistä tutkimusmenetelmistä ja kuinka niitä käytetään tässä työssä. Lisäksi käydään läpi työn tutkimusongelmat. Tutkimusongelmat jaetaan osiin, jotta niitä on helpompi lähteä tarkastelemaan.

### 3.1 Tutkimusongelmat

Tutkimusongelmina opinnäytetyössä on selvittää minkälaisia ovat varmuuskopioinnin pääkäsitteet ja kriteerit sekä miten niitä tulee käyttää ja hyödyntää yrityksen tietojen ja tiedostojen suojaamisessa. Opinnäytetyö vastaa myös kysymykseen, millä eri keinoilla varmuuskopioinnin voi suorittaa. Lisäksi tulee selvittää mitkä ovat epäonnistuneen varmuuskopioinnin tai laitteiston hajoamisen seuraukset kohdeyritykselle ja sen liiketoiminnalle.

Tähän tutkimusongelmaan on päädytty, koska valokuvat ovat kohdeyrityksen liiketoiminnan ydin ja niiden menettämällä voi olla suuria seurauksia. Tämä ongelma herätti kysymyksiä siitä kuinka tältä voisi välttyä ja mikä olisi paras keino välttää tietojen menettäminen. Tutkimusongelman ratkaiseminen antaa vastaukset esitettyihin kysymyksiin.

Tutkimusongelmaa rajaavat kysymykset jakavat tutkimusongelman pienempiin osiin, joita on yksinkertaisempi lähteä tarkastelemaan ja joihin on helpompaa löytää mahdollisia vastauksia. Tämä myös helpottaa opinnäytetyön lopussa vertaamaan onko opinnäytetyössä vastattu tutkimusongelmassa esitettyihin kysymyksiin.

- Mitä on varmuuskopiointi?
- Mikä on varmuuskopioinnin tarkoitus?
- Mitä tarkoitetaan varmuuskopioinnin automatisoinnilla?
- Mitä varmuuskopioinnin käsitteitä ja toimintatapoja voidaan soveltaa tässä opinnäytetyössä?
- Millaisia uhkia on, jos kohdeyrityksellä ei ole varmuuskopiointia tai se pettää?
- Millä keinoilla varmuuskopion voi suorittaa?
- Millaisille erilaisille tallennuslaitteille varmuuskopiot voi tehdä?
- Onko opinnäytetyössä onnistuttu tavoitteessa vahvistaa kohdeyrityksen varmuuskopiointia?

Tutkimusongelman ratkaisemiseksi tullaan tutustumaan tietoturvaan ja varmuuskopiointiin liittyvään kirjallisuuteen ja artikkeleihin. Näiden lähdemateriaalien avulla pyritään löytämään varmuuskopioinnin peruskäsitteitä ja keinoja ja erottelemaan niistä ne, joita voi käyttää hyväksi tässä opinnäytetyössä. Varmuuskopioinnin positiivisiin vaikutuksiin sekä uhkakuviin pyritään löytämään parhaita käytäntöjä alan kirjallisuudesta.

### 3.2 Benchmarking

Benchmarking on prosessi, jonka avulla mitataan sekä analysoidaan tuotteiden, palvelujen sekä prosessien suorituskykyä. Benchmarkingin tarkoituksena on auttaa löytämään parhaat menetelmät ja toimintatavat. Prosessiin kuuluu määrittää organisaatiolle tärkeä kohde ja selvittää paras käytäntö sen suorittamiseen (Niva & Tuominen 2005).

Tässä opinnäytetyössä selvitetään mikä on paras ohjelma yrityksen varmuuskopioinnin suorittamiseen ja mille tallennusmedialle se kannattaa tehdä. Vertailtavat ohjelmat valitaan alan kirjallisuuden ja artikkeleiden sekä ohjelmien suosion perusteella. Ohjelmien suosion näkee

arvosteluiden ja latausmäärien perusteella. Tutkimuksen Benchmarking-osuudessa vertaillaan tallennusmedioiden ominaisuuksia käyttämällä mittarina Pros & Cons-vertailua eli hyviä ja huonoja puolia (Wisegeek 2014).

### 3.3 Kepner & Tregoe

Kepner & Tregoe on päätöksentekomalli, jonka avulla voidaan kerätä, priorisoida ja arvottaa informaatiota. Mallin avulla on tarkoitus löytää paras mahdollinen ratkaisu mahdollisimman vähillä negatiivisilla seurauksilla. Mallin perusteella eri vaihtoehdot jaotellaan pakollisiin (Must) ja haluttuihin (Want) ominaisuuksiin (Decision Making Confidence).

Tässä tutkimuksessa käytetään Kepner & Tregoen-mallia apuna parhaan ohjelman valitsemiseksi. Malli auttaa vertailemaan missä ohjelmassa on parhaat ominaisuudet yrityksen tiedostojen varmistamiseen. Mallin avulla pystytään laittamaan ominaisuudet tärkeysjärjestykseen sekä pisteyttämään ne ja eniten pisteitä saanut ohjelma täyttää yrityksen vaatimukset parhaiten.

### 3.4 Asiantuntijahaastattelu

Asiantuntijahaastattelu tarkoittaa haastattelun erityismuotoa, jossa haastateltavat ovat valittuja heidän osaamisensa perusteella tutkittavaa kohdetta ajatellen. Haastateltavilla on mahdollisuus antaa laaja-alaisesti tietoa teknisistä, taloudellisista ja juridisista seikoista. He osaavat hahmottaa asiantuntija-alueitaan monipuolisesti.

Asiantuntijana toimi IT-alalla 15 vuotta työskennellyt Janne Kekkonen, joka toimii tällä hetkellä System Administratorina Accenturella. Kekkonen on aikaisemmin työskennellyt Unix-/Linux-kouluttajana ja näiden käyttöjärjestelmien tallennusympäristöjen asentamis- ja ylläpitoprojekteissa monikansallisissa yrityksissä. Viime vuosina hän on työskennellyt erilaisten pilviratkaisujen suunnittelu- ja koulutustehtävissä, joissa hänen tehtäviinsä on kuulunut myös varmuuskopiointi- ja palautusjärjestelmien suunnittelu, käyttöönotto ja koulutus. Haastattelun avulla selvitetään varmuuskopiointin peruskäsitteitä ja ominaisuuksia.

Haastattelun avustuksella valitaan sopivat ohjelmat vertailua varten. Valittuja ohjelmia vertaillaan Kepner & Tregoen mallin perusteella ja valittuja tallennuslaitteita Benchmarkingin avulla. Näiden vertailujen perusteella valitaan yritykselle sopivin varmuuskopiointiohjelma ja -laite.

## 4 Varmuuskopiointi

Varmuuskopiointi tarkoittaa yhden tai useamman tiedoston kopioimista siltä varalta, että alkuperäinen tieto katoaa tai muuttuu käyttökelvottomaksi. Varmuuskopio on siis vaihtoehtoinen kopio alkuperäiselle tiedostolle. Varmuuskopioita tulee ottaa siltä varalta, että esimerkiksi kiintolevy hajoaa. Varmuuskopion pohjimmainen tarkoitus on pelastaa yrityksen tiedot.

Varmuuskopio otetaan yleensä erilaisilta kiintolevyiltä, joita ovat IDE, FC, SAS, SATA tai SSD-levyt. Varmuuskopiot voidaan ottaa yksittäisistä kansioista, erillisistä levyosioista tai kokonaisista kiintolevyistä. Lisäksi peilatuista levyjärjestelmistä, tietokannoista ja jopa kokonaisista datakeskuksista otetaan varmuuskopioiteja. Näin varmistetaan, että yrityksen toiminta voi jatkua levy- tai laitevikojen jälkeenkin mahdollisimman nopeasti (Kekkonen 2014).

Varmuuskopion tulee sijaita eri tallennusmedialla kuin alkuperäinen tiedosto. Varmuuskopioiksi ei riitä se, että tiedosto sijaitsee eri kansiossa samalla kiintolevyllä. Alkuperäinen kopio sijaitsee luultavasti tietokoneen kiintolevyllä, mutta varmuuskopion tai varmuuskopioiden tulee sijaita jollain ulkoisella tallennusmedialla.

Tiedostot voivat kadota laitteiston hajoamisen, teknisen virheen, haittaohjelman tai inhimillisen virheen takia. Käyttäjä voi myös vahingossa poistaa tiedostoja ja näin menettää tärkeitä tiedostoja. Varmuuskopiot otetaan siltä varalta, että mahdollisesti menetetyt tiedot ja tiedostot saadaan takaisin myöhemmin.

Varmuuskopiot tulee suorittaa säännöllisesti. Varmuuskopioiden onnistuminen tulee myös varmistaa siltä varalta, että tiedot menetetään. Tietojen menettämisen varalta pitää olla myös tietojen palautussuunnitelma eli suunnitelma siitä kuinka tiedot palautetaan.

Vaikka varmuuskopiointi olisi suoritettu, niin silti on useita syitä miksi se on voinut epäonnistua tai sitä ei saa noudettua. Varmuuskopiointitiedosto saattaa olla korruptoitunut ja sitä ei saa noudettua tämän takia. Tämän takia on tärkeää testata, että varmistukset toimivat. Dynamic Questin mukaan (2013) 34 % yrityksistä ei ikinä kokeile nauhavarmuuskopioitaan ja niissä tapauksissa, kun testataan, huomataan, että 77 %:ssa nauhoista löytyy virheitä tai ne ovat käyttökelvottomia.

Varmuuskopioita menetetään usein tai jätetään tekemättä kokonaan inhimillisten virheiden takia. Usein on käynyt niin, että yrityksen työntekijä on unohtanut käynnistää varmuuskopiointin. Ei ole myöskään harvinaista, että varmuuskopioita ja niiden sisältämiä arkaluontoisia dokumentteja on unohdettu väärin paikkoihin, joista ne ovat sitten kadonneet tai joutuneet väärin käsiin.

Yksi syy sille, että varmuuskopioihin ei pääse käsiksi on salaussalasanojen unohtaminen. Muita yleisiä virheitä on se, että varmuuskopioidaan vain osa tiedostoista eikä varauduta siihen, että joitain tiettyjä tiedostoja tarvittaisiin tulevaisuudessa. Usein on käynyt myös niin, että varmuuskopioita on vain yksi kappale ja sen sijoitettu samaan fyysiseen sijaintiin kuin alkuperäiset versiot. Tällä tavalla sekä alkuperäinen tiedosto että varmuuskopio voivat tuhoutua esimerkiksi tulipalossa (Dynamic Quest 2013).

#### 4.1 Suunnittelu

Varmuuskopioinnin suunnittelussa tulee pohtia mitä varmuuskopioidaan, milloin varmuuskopioidaan ja miten varmuuskopioidaan. Suunnittelussa tulee olla selvillä mitkä ovat kriittisimmät tiedostot yrityksen kannalta, jotta kaikista tärkeimmät tiedostot tulevat varmasti varmuuskopioitua. Tätä varten pitää myös selvittää missä nuo tärkeimmät tiedostot sijaitsevat ja mihin sijaintiin ne varmuuskopioidaan.

Kun nuo asiat on selvitetty, voi suunnitella varmuuskopiointikeinon-, ohjelman ja ajastuksen. Ensimmäisenä tulee valita ohjelma, jolla varmuuskopiointi suoritetaan ja ajankohta, jolloin varmuuskopiointi suoritetaan sekä kuinka usein se suoritetaan. Ennen varmuuskopioinnin suorittamista on päätettävä millaisia varmuuskopioita otetaan: differentiaalisia, inkrementaalisia vaiko esimerkiksi pelkkä kopio tiedostoista. Lisäksi tulee valita mihin kohteeseen varmuuskopiointia suoritetaan: meneekö varmuuskopio esimerkiksi verkkokiintolevylle tai pilveen.

#### 4.2 Riskienhallinta

Uhalla tarkoitetaan mahdollisia vaaroja tai haittoja. Uhat liittyvät tiedon luottamuksellisuuteen, eheyteen tai saatavuuteen. Tieto voi paljastua väärälle taholle, se voi muuttua tai vääristyä, se voi kadota tai tuhoutua. Alla lista erilaisista uhkakuvista yrityksen tietoaaineistoille:

- Virukset
- Inhimillinen virhe
- Luonnonilmiöt
- Virran katkeaminen
- kiintolevyn hajoaminen
- Tietokone varastetaan
- virhe ohjelmassa
- Käyttöjärjestelmän kaatuminen
- Tiedostot voidaan menettää, vaikka ne olisivat pilvessä, jos pilviyritys menee konkurssiin.

Alla lista riskeistä yrityksen liiketoiminnalle Wallacen ja Webberin mukaan (2010, 318-319):

- Yrityksen tietoja voi päätyä väärin käsiin
- Tuottavuus laskee
- Data joudutaan luomaan uudestaan, tässä tapauksessa kuvaamaan uudestaan
- Häiriöaika, kun työntekijät eivät voi tehdä töitään eli palkka juoksee, mutta töitä ei voi tehdä.
- Asiakastietojen menetys. Voi vaikeuttaa kykyä palvella asiakasta.
- Taloudellinen tappio
- Maineen tai luottamuksen menetys: tämä voi johtaa myös menetettyihin mahdollisuuksiin. Kun tieto leviää, että yrityksellä on tapahtunut tietovuoto tai vastaava niin moni ei välttämättä halua tehdä bisnestä tällaisen yrityksen kanssa.
- Joutuu mahdollisesti palkkaamaan yrityksen palauttamaan menetetyt tiedot

#### 4.3 Erityyppiset varmuuskopioinnit

Ruohosen mukaan (2002, 211) mukaan varmuuskopiointikeinoja on viisi erilaista: Normaali, kopiointi, erotus eli differentiaalinen, lisäys eli inkrementaalinen ja päivittäinen varmuuskopiointi. Normaali varmuuskopiointi tarkoittaa sitä, että joka ikinen tiedosto varmuuskopioidaan ja merkataan varmuuskopioiduksi poistamalla tiedostoista arkisto-merkintä. Arkisto-merkintä tarkoittaa, että tiedosto on muuttunut edellisen varmuuskopioinnin jälkeen ja se täytyy varmuuskopioida. Kopiointi varmuuskopioinnissa tiedostoja ei merkitä varmuuskopioiduksi.

Erotus eli differentiaalisessa varmuuskopioinnissa kopioidaan kaikki edellisen varmuuskopioinnin jälkeen muuttuneet tiedostot, mutta niitä ei merkitä varmuuskopioiduksi. Lisäys eli inkrementaaliossa varmuuskopioinnissa kopioidaan kaikki muuttuneet tiedostot ja merkitään ne varmuuskopioiduksi. Päivittäisessä varmuuskopioinnissa kopioidaan kaikki päivän aikana muuttuneet tiedostot, mutta niitä ei merkitä varmuuskopioiduksi. (Ruohonen 2002, 211)

Yleisin varmuuskopiointikäytäntö on ottaa normaali eli täysi varmuuskopio sekä tämän rinnalla inkrementaalinen tai differentiaalinen varmuuskopiointi. Näin tehdään, koska täysi kopiointi vie pidemmän aikaa ja vaatii enemmän tallennustilaa. Tämän takia täydet kopiointit tehdään vain tiettyinä aikoina ja tämän lisäksi tehdään pienempi erotus- tai lisäysvarmuuskopiointeja.

Varmuuskopioinnin	Normaali	Inkrementaalinen	Differentiaalinen
-------------------	----------	------------------	-------------------

numero			
Varmuuskopiointi 1	kaikki tiedostot	--	--
Varmuuskopiointi 2	kaikki tiedostot	Muutokset varmuuskopiointi 1:stä.	Muutokset varmuuskopiointi 1:stä.
Varmuuskopiointi 3	kaikki tiedostot	Muutokset varmuuskopiointi 2:sta.	Muutokset varmuuskopiointi 1:stä.
Varmuuskopiointi 4	kaikki tiedostot	Muutokset varmuuskopiointi 3:sta.	Muutokset varmuuskopiointi 1:stä.

Taulukko 1: Varmuuskopiointikeinojen vertailu

Normaali varmuuskopiointi otetaan yleensä viikoittain ja tämän lisäksi otetaan differentiaalinen tai inkrementaalinen varmuuskopiointi. Viikoittainen normaali ja inkrementaalinen varmuuskopiointi toimii seuraavalla tavalla: Ensin otetaan normaali varmuuskopiointi ja tämän jälkeen inkrementaalinen kopio normaalista varmuuskopiointista. Seuraavana päivänä otetaan inkrementaalinen varmuuskopio edellisen päivän inkrementaalisesta varmuuskopiosta. Seuraavana päivänä otetaan taas inkrementaalinen varmuuskopio edellisen päivän inkrementaalisesta varmuuskopiosta.

Tämä toistuu kunnes otetaan taas viikoittainen normaali varmuuskopio ja tämän jälkeen inkrementaalisia varmuuskopiota otetaan tästä viikoittaisesta varmuuskopiosta. Differentiaalinen varmuuskopio ottaa kopion aina normaalista varmuuskopiosta (TechTarget 2008).

#### 4.4 Tiedostojen palautus

Varmuuskopioiden palauttamisella tarkoitetaan varmuuskopioitujen tiedostojen palauttamista. Ensisijaisesti tiedostot palautetaan varmuuskopioista. Varmuuskopiointiohjelmissa on mukana ominaisuus, joilla kopiot voidaan palauttaa tai sitten tiedostot voi vain kopioida varmuuskopiointikansiosta haluttuun kohteeseen.

Jos varmuuskopiot pettävät, niin on eri vaihtoehtoja tiedostojen takaisin saamiseksi, mutta nämä eivät ole yhtä luotettavia eikä ole mitään takuita, että tiedostot saadaan palautettua. Jos varmuuskopioita ei ole otettu tai tiedostoja on kadonnut jostain syystä, niin tätä varten on erilaisia tiedostojen palautus-ohjelmia, kuten Recuva, joka palauttaa poistettuja tai ka-



donneita tiedostoja. Recuva voi mahdollisesti palauttaa osan tiedostoista, mutta siitä ei ole takeita.

Tämän lisäksi on kolmansia osapuolia, jotka voivat palauttaa menetettyjä tiedostoja esimerkiksi hajonneelta kiintolevytä, mutta tässäkin on riskinsä, että kaikkia tiedostoja ei saada palautettua. Lisäksi tämä voi olla erittäin suuri lisäkulu yritykselle, jos joudutaan palkkaamaan ulkoinen tekijä palauttamaan tiedostoja. Varmuuskopiot on hyvin tärkeää suorittaa ja niiden toimivuus pitää tarkastaa säännöllisesti. Lisäksi tiedostoilla tulee olla palautussuunnitelma, joka määrittää miten tiedostot palautetaan ja mihin.

#### 4.5 Varmuuskopioinnin merkitys tietoturvassa

Kohdeyrityksen tietoaineiston varmuuskopiointi on tärkeää yrityksen liiketoiminnan kannalta, mutta se on myös erittäin tärkeä osa yrityksen tietoturva. Liiketoiminnan lisäksi tietoturvan taso vaikuttaa myös yrityksen maineeseen. Rouskun mukaan (2014, 47) tietoturvallisuudella tarkoitetaan tiedon luottamuksellisuuden, eheyden sekä saatavuuden varmistamista.

Rousku kuvailee (2014, 47-49) luottamuksellisuutta, eheyttä ja saatavuutta seuraavalla tavalla: Luottamuksellisuudella tarkoitetaan sitä, että salassa pidettävään tietoon pääsee käsiksi ainoastaan ne henkilöt, joilla on siihen käyttöluupa. Luottamuksellisuus tietojärjestelmissä toteutetaan yleisesti käyttöoikeuksienhallinnalla. Tämä tarkoittaa sitä, että käyttäjille annetaan heille tarvittavat ja riittävät oikeudet. Kohdeyrityksen kohdalla tämä tarkoittaisi sitä, että yrityksen ulkopuoliset tahot eivät pääsisi käsiksi valokuviiin.

Eheys tarkoittaa sitä, että tieto ei saa muuttua hallitsemattomasti. Tällä tarkoitetaan sitä, että tietoa saa käsitellä ja muokata ainoastaan ne tahot, joilla on siihen käyttöoikeudet. Jotta eheys saavutetaan, tulee alkuperäisestä tietoaaineistoista olla varmuuskopio, että se saadaan palautettua alkuperäiseen tilaan, jos tietoaaineisto on muuttunut hallitsemattomasti.

Tiedon saatavuudella tarkoitetaan sitä, että tietoaaineiston tulee olla saatavilla siihen oikeuteuille käyttäjille silloin kuin he sitä tarvitsevat. Jotta tieto olisi hyödynnettävissä, tulee sen olla saatavilla ja käytettävissä. Käytännössä tiedon tulee olla saatavilla jatkuvasti ilman pitkiä viiveitä tai ongelmia.

#### 4.6 Varmuuskopioiden säilyttäminen

Ruohosen mukaan (2002, 210) varmuuskopioita tulee säilyttää eri paikassa kuin alkuperäisiä kopioita, jotta ne eivät mahdollisen onnettomuuden myötä tuhoudu yhdessä alkuperäisten kanssa. Varmuuskopioiden säilyttämiselle on useita erilaisia riskejä kuten varkaus, tulipalo tai

vaikka vesivahinko. Tämän takia varmuuskopioita tulisi säilyttää joko eri sijainnissa, tulenkestävässä kassakaapissa tai siitä tulisi olla useampia kopioita ja mielellään eri sijainneissa.

Varmuuskopioiden säilyttämisessä tulee ottaa huomioon myös lakisyys. ”Varmuuskopioita joudutaan yritysmaailmassa ottamaan myös laki- ja veroteknisistä syistä ja tällaisissa tilanteissa jopa tahattomista laiminlyönneistä voi olla seurauksena rikosoikeudellisia toimenpiteitä ja korvaus- ja sanktioseuraamuksia” (Kekkonen 2014).

Laaksonen, Nevasalo ja Tomula (2006, 170) tarkentavat, että varmuuskopioiden säilyttämisessä pitää ottaa huomioon tietosisällön tallennusaikaan ja lukukelpoisuuteen liittyvät määräykset. Esimerkiksi tilinpäätösinformaatiota tulee säilyttää kymmenen vuoden ajan ja datan tulee olla helposti luettavissa tai sen tulee olla muutettavissa luettavaan muotoon. Varmistettua tietoa tulee testata ja palauttaa säännöllisesti, jotta voidaan varmistua siitä, että varmistus on onnistunut ja data on vielä luettavissa.

#### 4.7 Yrityksen laitteisto

Yrityksen laitteisto koostuu useammasta eri valmistajan laitteesta ja käyttöjärjestelmästä. Eri työtehtävissä käytetään eri käyttöjärjestelmiä. Nämä riippuvat tehtävän työn vaatimuksista ja saatavilla olevista sovelluksista.

Yrityksellä on käytössä Windows 7- ja 8-käyttöjärjestelmällä toimivia kannettavia tietokoneita. Applen tuotteista yrityksellä on käytössä iMac-pöytä tietokoneita ja MacBook Pro-kannettavia. Macien käyttöjärjestelmäversiot ovat Mac OS X 10.6 Snow Leopard ja Mac OS X 10.9 Mavericks.

Varmuuskopiointia varten yrityksellä on kolme ulkoista kiintolevyä. Yrityksellä on myös verkkolevy, joka ei ole tällä hetkellä kuitenkaan käytössä hitauden takia. Lisäksi käytössä on kameroiden muistikortteja ja muistitikkuja.

#### 4.8 Varmuuskopioinnin nykytila

Tällä hetkellä Windows-varmuuskopiot suoritetaan manuaalisesti siirtämällä tiedostot ulkoiselle kiintolevylle ja Mac-koneiden varmuuskopiointiin käytetään Time Machinea. Time Machine ottaa varmistaa tiedostot inkrementaalisesti. Se ottaa varmuuskopion tunneittain, päivittäin ja viikoittain. (iMore 2014)

Tämän luvun tiedot perustuvat yrityksen omistajan kanssa käytyyn henkilökohtaiseen keskusteluun. Yrityksen kuvaajat ottavat valokuvia noin 30 000 asiakkaasta kuvausten aikana ja ku-

via kertyy yli 200 000 kappaletta kuvausten aikana. Kuvat tallentuvat kameroiden muistikortteille kuvauspaikoilla ja ne siirretään manuaalisesti ulkoiselle kiintolevyille lajiteltavaksi ja käsiteltäväksi yrityksen toimipisteessä kuvausten päätteeksi.

Käytössä on kaksi Mac-tietokonetta ja kaksi ulkoista kiintolevyä. Kuvaajat siirtävät valokuvat näille kahdelle ulkoiselle kiintolevyille. Kerran päivässä kuvanmuokkaaja siirtää kuvat näiltä ulkoisilta kiintolevyiltä kuvanmuokkukseen tarkoitetun tietokoneen sisäiselle kiintolevyille. Kuvanmuokkaaja karsii epäonnistuneet otokset pois sekä muokkaa virheitä tarvittaessa. Kuvanmuokausvaiheen jälkeen valitut kuvat ladataan verkkokaupan tarjoajan pilveen, josta asiakkaat voivat valita ja tilata haluamansa kuvat. Nämä kuvat ovat tarjolla asiakkaille kymmenen kuukauden ajan.

Muokatut kuvat siirretään tallentajien Windows-koneille, joissa ne kohdistetaan oikeisiin tiluksiin siihen tarkoitettulla ohjelmalla. Kohdistuksessa asiakkaan nimi, tilauslomake ja kuvat yhdistetään oikeaan henkilöön. Kun tallentajat saavat työn valmiiksi, he lataavat tilaukset verkkokauppaan, josta asiakas voi käydä valitsemassa mieleisensä kuvan ja tilata tuotteita sen perusteella. Näitä kuvia säilytetään verkkokaupassa 10 kuukauden ajan.

Verkkokaupan tarjoajan pilvessä pidetään siis tallessa vain muokatut kuvat, joista asiakkaat saavat valita haluamansa kuvat. Alkuperäisiä kuvia ei tallenneta pilveen. Niiden varmuuskopiot sijaitsevat näillä kahdella ulkoisella kiintolevyllä.

Käyttäjärjestelmistä ei oteta varmuuskopioita eli jos tietokone kaatuu tai tulee joku muu tilanne, jonka takia järjestelmä pitäisi palauttaa niin näistä tietokoneista ei ole varmuuskopioita. Tällaisissa tilanteissa tietokoneet ja niiden käyttäjärjestelmät joudutaan uudelleen asentamaan ja keskeneräiset työt joudutaan aloittamaan alusta. Tämän takia joudutaan myös asentamaan sovellukset uudestaan ja määrittelemään tietokoneen asetukset.

#### 4.9 Varmuuskopioinnin tarve

Yritys ottaa vuodessa noin 200 000 digitaalista kuvaa. Oppilaita kuvataan noin 30 000 ja luokkia tai päiväkotiryhmiä on yhteensä noin 1500 kappaletta. Yksityisten eli tavallisten henkilökuvienvälikuvien sekä kaverikuvienvälikuvien koko on noin 1-2 megatavua. Luokkakuvien koko on 10-20 megatavua.

Vuoden aikana otettujen valokuvien säilöminen vie yhteensä noin yhden teratavun verran eli noin 1000 gigatavua kiintolevytilaa. Varmuuskopioinnissa tulee myös ottaa huomioon asiakkaiden yhteystiedot, näille lähetetyt tarjoukset sekä tehdyt sopimukset. Näiden lisäksi yrityksen

sisäiseen toimintaan liittyvät tulee varmuuskopioida, kuten palkkatiedot ja muut työsuhteisiin liittyvät asiakirjat.

Yritys haluaa varmuuskopioiden olevan päivittäisiä ja toivoo myös, että varmistetut tiedostot olisivat saatavissa nopeasti ja helposti. Yritykselle tärkeintä on varmuuskopioida kansiot, joissa sijaitsee kaikki kriittinen data. Ensisijaista on, että yksittäiset tiedostot ovat nopeasti palautettavissa varmuuskopioista.

Yrityksen toiminnan kannalta tärkeimpiä varmuuskopioitavia tiedostoja ovat valokuvat, kouluille ja päiväkodeille lähetetyt tarjoukset, näiden kanssa tehdyt sopimukset sekä yhteystiedot. Tämän lisäksi tärkeitä tiedostoja ovat kaikki yrityksen työntekijöihin liittyvät asiat, kuten työsopimukset ja palkkatiedot.

## 5 Tallennusmediat

Tässä luvussa käydään läpi erilaiset tallennusmediat ja kohteet mihin varmuuskopioita voi suorittaa. Varmuuskopioita voi suorittaa monenlaisille tallennuslaitteille ja jokaisessa on hyviä ja huonoja puolia. Tallennusmedioita ovat CD-, DVD- ja Blu-ray-levyt, ulkoiset- ja verkkokiintolevyt sekä useat erilaiset nauhat. Lisäksi varmuuskopiot voi etävarmistaa pilvipalveluntarjoajan palvelimille.

Luvussa kerrotaan taustatietoja tallennuslaitteista ja niiden toiminnasta. Tallennuslaitteet on jaettu alalukuihin, joissa kerrotaan tarkemmin laitteiden teknisistä ominaisuuksista. Alaluvut ovat optiset tallennusvälineet, haihtumaton muisti, magneettiset tallennusvälineet ja etävarmistus.

### 5.1 Optiset tallennusvälineet

Optisella tallennusvälineillä tarkoitetaan levyjä, joita luetaan laserilla. CD- ja DVD-ROM-levyt ja näiden eri versiot sisältyvät optisiin tallennusvälineisiin. Eri versioita ovat uudelleenkirjoitettavat CD- ja DVD-RW-levyt sekä Blu-ray. Näiden lukemiseen tarvitaan optinen asema eli lukulaite, joka osaa lukea optista mediaa (Techterms 2008).

Levyille luvataan jopa 30 vuoden kestävyyttä valmistajien puolesta, mutta tämä vaatisi täydellisiä olosuhteita tallennusvälineiden säilyttämiselle. Optiset tallennusvälineet kestävät huonosti auringonvaloa sekä lämpötilan vaihtelua kylmästä kuumaan. Lisäksi levyille kirjoittamisvaiheessa tieto ei välttämättä kopioitu sellaisena kuin sen kuuluisi (Worldstart 2011).

Optisissa tallennusvälineissä on sekä hyviä että huonoja puolia. Niiden hyviin puoliin kuuluu halpa hinta ja koko, jonka johdosta niitä on helppo kuljettaa paikasta toiseen. Tämä sopii tiedon väliaikaiseen säilyttämiseen, mutta pidempää säilytystä varten tiedot on parasta tallentaa jonnekin muualle.

Cd-levyihin (Compact Disk) mahtuu dataa noin 700 Mt. CD-ROM-levyt ovat ainoastaan luettavia eli niissä olevaa dataa ei voi muokata. CD-Recordable-levyille (CD-R) voi kirjoittaa dataa itse. CD-ReWritable-levyille (CD-RW) voi kirjoittaa dataa ja ne voi tyhjentää sekä uudelleen kirjoittaa (Paananen 2003, 95-98). Kymmenen 700Mt CD-RW-levyn hinta alkaa noin 10 eurosta.

Yleisimmät DVD-levyt (Digital Versatile Disc tai Digital Video Disc) ovat 4,7 Gt:n kokoisia. Tämän lisäksi on yksipuolisia ja kaksikerroksia DVD-levyjä, joiden koko on 8,5 Gt, kaksipuolisia ja yksikerroksia, joiden koko on 9,4 Gt sekä kaksipuolisia ja kaksikerroksisia, joiden koko 17,08 Gt (Flyktman 2010, 226). Kymmenen 4,7 Gt DVD-levyn hinta on noin 15 euroa.

Blu-ray on korkeatarkkuuksinen optinen levy, johon mahtuu huomattavasti enemmän dataa kuin CD- ja DVD-levyille. Blu-ray-tekniikka perustuu sinivioletteihin lasereihin, joissa on lyhyempi aaltopituus kuin perinteisissä CD- ja DVD-levyissä käytettävissä punaisissa lasereissa. Tämä mahdollistaa sen, että laser voi keskittyä pienempään alueeseen ja näin fyysisesti samankokoiselle levyille voidaan laittaa huomattavasti enemmän dataa (TechTerms). Blu-ray-levyjä on 25, 50 tai 100 Gt:n kapasiteetilla ja kymmenen kappaletta 25 Gt Blu-ray-levyjä maksaa noin 20 euroa.

## 5.2 Haihtumaton muisti

Haihtumattomalla muistilla tarkoitetaan muistia, joka ei tyhjennä tallennettuja tietoja vaikka virta katkaistaisiin. Haihtumaton muisti tunnetaan myös nimellä Flash-muisti. Esimerkkejä Flash-muistia käyttävistä laitteista ovat USB-muistit, kameroiden muistikortit ja MP3-soittimet (Flyktman 2010, 53).

SSD:llä (Solid-state-drive) tarkoitetaan massamuistia, joka ei sisällä ollenkaan liikkuvia osia. SSD:tä käytetään nykyään useasti tavallisen kiintolevyn korvaajana tietokoneissa. SSD-massamuisti kuluttaa vähemmän virtaa, se on äänetön ja se hakee tietoja nopeammin eli tietokone toimii nopeammin (PC Magazine 2014).



Kuva 1: Samsungin SSD-kiintolevy (PC Magazine 2014)

Russell Kayn mukaan (Computer World 2010) SSD-kiintolevyt korvaavat perinteisiä kiintolevyjä netbookkeissa, pöytäkoneissa ja myös jossain palvelinasennuksissa. SSD-levyjen suosio perustuu siihen, että ei tarvita ulkoista virtalähdettä ja tietokone käynnistyy ja toimii nopeammin. SSD-levyt ovat kuitenkin vielä paljon kalliimpia kuin perinteiset kiintolevyt ja niissä on myös vähemmän tallennustilaa. 500 Gt:n ulkoinen SSD-kiintolevy maksaa halvimmillaan noin 600 euroa.

SSD-kiintolevyt käyttävät samoja liitäntöjä kuin kiintolevytkin. Lukunopeus saattaa olla jopa 550 Mt/s ja kirjoitusnopeus 150 Mt/s. Luku- ja siirtonopeudet saattavat vaihdella huomattavasti eri valmistajien välillä ja nopeuksiin vaikuttaa myös se, että yhdistetäänkö ulkoiset SSD-levyt koneisiin USB 2.0 vai 3.0-liitännällä.

SD (Secure Digital) on muistikortti, jota käytetään autojen navigaattoreissa, älypuhelimissa, digikameroissa, tietokoneissa ja monissa muissa laitteissa. Siinä on nopea siirtonopeus ja pieni virrankulutus. SD-korttien maksimikoko on 2Gt (TechTarget 2006).

SDHC (Secure Digital High Capacity) kehitettiin HD-laadun ja korkeiden resoluutioiden kysynnän takia. SDHC on samankokoinen ja muotoinen kuin SD-kortti, mutta se ei toimi SD-laitteissa. SHDC-korttien muistikapasiteetti on 4-32Gt (Integral).

SDXC (Secure Digital Extended Capacity) on uusin muistikorttistandardi. Se kehitettiin lisäämään mukana kuljetettavan tallennuskapasiteetin määrää ja siirtonopeutta. Se pystyy käsit-

telemään suuria määriä data ja tallennuskapasiteetti on nostettu 32 Gt:sta jopa 2Tt asti (SD Association).

### 5.3 Magneettiset tallennusvälineet

Tässä luvussa kerrotaan erilaisista magneettisista tallennusvälineistä. Tällaisia ovat erilaiset ulkoiset kiintolevyt ja verkkokiintolevyt. Erilaisia nauhatekniikoita on muun muassa DLT, DAT ja LTO.

Kiintolevyä käytetään tietokoneissa pysyvämuistina ja siellä säilytetään kaikki käytettävät ohjelmat ja tiedostot. Kiintolevyille asennetaan myös tietokoneessa käytettävä käyttöjärjestelmä. Kun tietokoneesta katkaistaan virta niin keskusmuistissa olevat tiedot katoavat, mutta kiintolevyllä olevat tiedot säilyvät ennallaan (Flyktman 2010, 49).

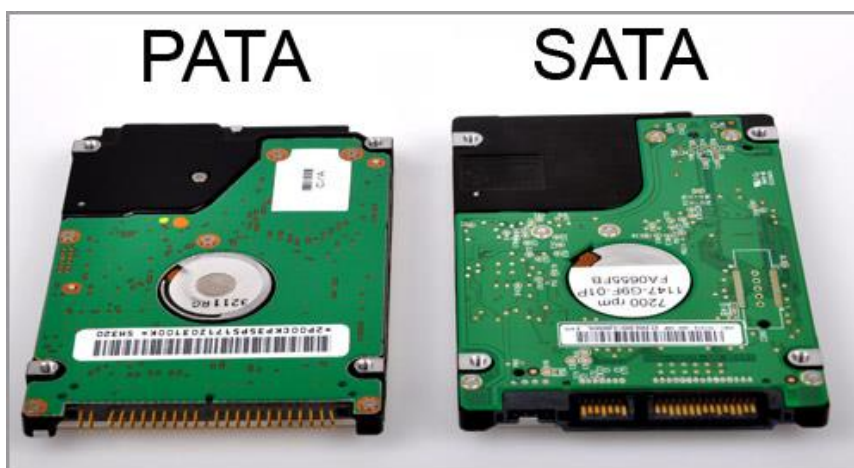
Data tallennetaan magneettisesti kiintolevyn sisällä oleviin kiekkoihin. Kiekkoihin tallennetaan ja niistä myös luetaan dataa mekaanisella lukupäällä. Lukupää muuttaa datan signaaleiksi (Muropaketti 2008).

Kiintolevyjen koot vaihtelevat 2,5 tuumasta 3,5 tuumaan. 1,8” levyjä käytetään harvoin ja silloinkin niitä käytetään vain erittäin pienissä ja kevyissä kannettavissa tietokoneissa. Kiintolevyjä on kahdella eri nopeudella: 5400 rpm ja 7200 rpm. Tuon luvun avulla saa selville kuinka nopeasti kiintolevyjen kiekot pyörivät ja tämä vaikuttaa suoraan siihen kuinka nopeasti dataa voi siirtää levyllä tai levyltä. Nopeammat kiintolevyt kuluttavat enemmän virtaa ja kuumenevat helpommin (LapTech).

Kiintolevyn ongelma on sen liikkuvat osat, jotka saattavat hajota helposti. Lukupää on lähellä kiekkoa ja huonolla tuurilla pienet kolaukset saattavat hajottaa joko lukupään tai kiekon pinnalla olevaa magneettista materiaalia. Hajonneen pinnan kohdalle tallennetut datat menetetään.

Kiintolevyjen liitännät ovat FC, IDE/ATA, SAS, SATA ja SCSI. Nämä kaikki ovat erilaisia tapoja liittää kiintolevy tietokoneen emolevyyn. Ulkoiset kiintolevyt liitetään tietokoneisiin USB-liittimillä.

IDE-liitäntä (Integrated Drive Electronics) tunnetaan myös nimillä ATA (AT Attachment), PATA (Parallel AT Attachment) ja EIDE (Enhanced Integrated Drive Electronics). IDE-liitäntää käytetään vanhemmissa tietokoneissa ja se on hitaampi ja äänekkäämpi esimerkiksi SATA. Yhteen IDE-kaapeliin voi kiinnittää kaksi kiintolevyä tai vaikka kiintolevyn ja optisen asemaan (Manuaali).



Kuva 2: PATA & SATA (Freegeek 2013)

SATA eli Serial-ATA:n (Serial Advanced Tecnology Attachment) siirtonopeus on alkaen 150Mt/S eli se on huomattavasti nopeampi kuin PATA, jonka siirtonopeus oli parhaimmillaan 100Mt/s. SATA:n muita hyviä puolia ovat ohuemmat ja pidemmät kaapelit, jotka mahdollistavat paremman ilmankulun tietokoneen sisällä. SATA-kaapelit ovat parhaimmillaan metrin pituisia, kun taas PATA-kaapelit olivat maksimissaan 40 cm. Tämä lisäpituus on antaa lisää pelivaraa, kun tietokoneita suunnitellaan (Techterms).

SCSI (Small Computer System Interface) on tarkoitettu nauha-asemien, kiintolevyjen, skanneerien ja muiden ulkoisten laitteiden yhdistämiseen. SCSI:n ensimmäisessä versiossa (SCSI-1) kaapelin pituus oli kuusi metriä, siirtonopeus oli 5Mt/s ja siihen pystyi yhdistämään maksimissaan kahdeksan laitetta. SCSI:n uusimmassa versiossa (Fast-320) kaapelin pituus on 12 metriä, siirtonopeus 640MB/s ja siihen voi yhdistää 16 laitetta (Webopedia).

SAS (Serial Attached SCSI) on suorituskyvyltään parannettu versio SCSI:stä. Kaapelit ovat pidempiä ja ohuempia, siirtonopeus on jopa 3Gt/s ja siihen voi liittää 128 erilaista laitetta. SAS-laitteet voi yhdistää SATA ja SCSI-laitteisiin, koska SAS:issa on samanlaiset piirilevyt kuin SATA-laitteissa (Webopedia).

FC (Fibre Channel) on ensisijaisesti tarkoitettu palvelimien ja jaettujen tallennuslaitteiden yhdistämiseen. FC:n siirtonopeus on jopa 4Gt/s ja tulevaisuudessa jopa 10Gt/s. Se on kolme kertaa nopeampi kuin SCSI ja onkin alkanut korvaamaan sen palvelinkäytössä. Laitteet voivat olla jopa 10 kilometrin päässä toisistaan valokuitukaapelin avulla ja lyhyemmällä etäisyydellä riittää koaksiaalikaapeli (Techtarget 2005).



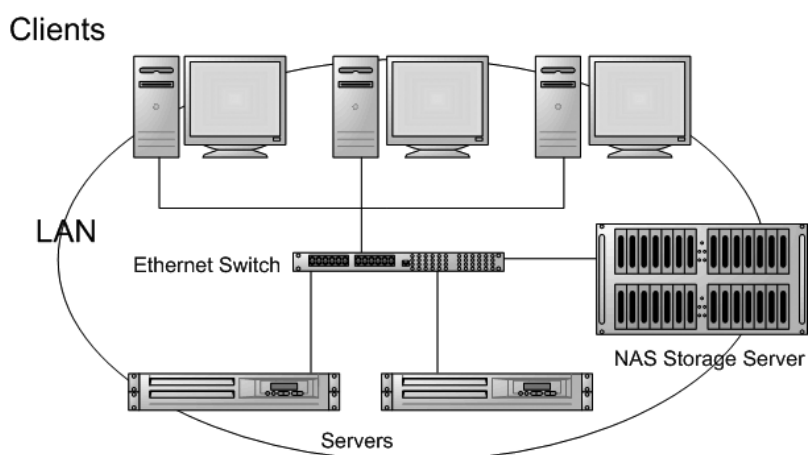
Ulkoisia kiintolevyjä saa nykyään erittäin halvalla. 1 Tt:n kiintolevyn voi saada alle 100 eurola. Näiden hintoihin vaikuttaa pääasiassa kiintolevyn koko ja tarvitseeko se erillistä virtalähdettä. Kiintolevyt, jotka saavat virran USB-liitännän kautta ovat hieman kalliimpia.

NAS (Network Attached Storage) eli verkkokiintolevy on verkkoon liitetty tallennuslaite, jota voi käyttää samanaikaisesti usealla eri laitteella, kuten tietokoneilla, älypuhelimilla tai pelikonsoleilla. NAS-laitteisiin sisältyy kiintolevy IDE-tai SATA-liitännällä, RJ-45-liitäntä (perinteinen kaapeli, jolla laite liitetään verkkoon) ja tai WLAN-tuki. Näin laitteen saa yhdistettyä lähiverkkoon. Monissa NAS-laitteissa on myös DLNA-ominaisuus (Digital Living Network Alliance), jonka avulla voi jakaa tiedostoja laitteiden välillä (Afterdawn).

Verkkokiintolevyt voi ostaa joko valmiina paketteina eli niissä on kiintolevyt valmiina koteloissa tai sitten voi ostaa pelkän kotelon ja siihen erikseen haluamansa kiintolevyt. Jälkimmäisellä tavalla voi rakentaa juuri sellaisen kokoonpanon kuin halua, mutta valmiissa paketissa on taas etuna se, että kaikki on jo asennettu ja käyttöönotto on helppoa.

Halvimmat RAID-ominaisuutta tukevat verkkokiintolevyt ovat alkaen 200 euroa. 200 eurolla voi saada myös RAID 5- ja RAID 10-tuetun kotelon, joka tukee viittä 3.5” kiintolevyä 10 teravuun asti. Halvin RAID 5-tasoa ja sitä ”ylempiä” tasoja tukeva valmispaketti on BUFFALO TeraStation 3400 ja se maksaa noin 700 euroa. Siinä on valmiina 4TB tallennustilaa ja sen voi laajentaa 16TB asti.

## Network Attached Storage



Kuva 3: Network Attached Storage (iPoint 2014)

RAID (Redundant Array of Independent Disks) on tekniikka, jonka avulla monista kiintolevyistä saadaan tehtyä yksi looginen asema. RAIDiin luomiseen tarvitaan vähintään kaksi kiintolevyä tai SSD-asemaa, jotka yhdistetään joko siihen tarkoitetulla raudalla tai ohjelmistolla. RAID oli

aikaisemmin kallis, mutta nykyiset SATA-kiintolevyt ovat tehneet RAIDista kohtuuhintaisen vaihtoehdon kiintolevyjen suorituskyvyn ja luotettavuuden parantamiseen. (Mato78 2012)

RAID:ssa on seitsemän perustasoa (RAID 0-6), joita käytetään datan turvallisuuden parantamiseen tai suorituskyvyn nopeuttamiseen. Lisäksi on olemassa erilaisia RAID-variaatiota tai yhdistelmiä. Jokainen taso ja yhdistelmä eroavat toisistaan.

RAID:ssa on kolme perusominaisuutta: peilaus, raidoitus ja pariteetti. Peilaus kopioi tiedot useammalle kiintolevylle, raidoituksessa tiedot jaetaan useammalle eri kiintolevylle ja pariteetti, joka käyttää ylimääräistä kiintolevyä pariteetti-informaation säilyttämiseen. Pariteetin avulla tarkastetaan onko dataa kadonnut tai ylikirjoitettu.

RAID 0-taso jakaa datan kahden fyysisen kiintolevyn kesken ja näin parantaa kiintolevyjen suorituskykyä. Kaikki tiedostot jaetaan pienempiin osiin ja jaetaan osat kiintolevyjen kesken. Ensimmäinen osa menee yhdelle kiintolevylle, toinen osa menee toiselle kiintolevylle. Tällä tavalla tietokone pääsee käsittelemään tietoja nopeammin, mutta samalla on suurempi riski tietojen menettämisestä, koska jos toinen kiintolevy hajoaa niin kaikki tiedot häviävät.

RAID 1-taso kirjoittaa datan yhtä aikaa kahdelle kiintolevylle. Toinen kiintolevy toimii isäntä-asemana ja toinen varmuuskopiona (tai peilinä.) Tässä tasossa tiedot kahdennetaan eli kirjoitetaan kokonaisuena kummallekin kiintolevylle eli vaikka toinen kiintolevy hajoaisi, niin tieto olisi tallessa toisella. RAID 1-taso parantaa tiedon lukunopeutta verrattuna yhteen kiintolevyyn, mutta samalla tiedon kirjoitusnopeus on vähän hitaampi.

RAID 3-taso on suhteellisen harvinainen eikä sitä juurikaan käytetä nykypäivänä, koska RAID 5-taso on toimivampi vaihtoehto nopeutensa ja pariteetti-informaation käsittelytavan takia. RAID 3-tasossa on käytössä vähintään kolme fyysistä kiintolevyä, joista yksi on varattu pariteettia varten ja kaksi tiedoille. Tiedot kirjoitetaan lohkoissa ” lohkoissa, vuorotellen jokaiselle fyysiselle kiintolevylle sekä käytetään lisäksi yhtä fyysistä kiintolevyä pariteettitarkastustietojen tallentamiseen”(Mato78 2012). Tiedot voidaan palauttaa vaikka mikä tahansa kiintolevyistä hajoaisi.

RAID 4-tason toimintaperiaate on samanlainen kuin RAID 3:ssa, mutta erona on se, että lohkokoot ovat suurempia ja suorituskyky parempi. RAID 4-tason positiiviset puolet ovat samat kuin RAID 3-tasonkin eli se kestää kiintolevyn hajoamisen. RAID 3- ja 5-tasoissa on paremmat suorituskyvyt kuin RAID 4:ssä ja lisäksi siihen on vaikea löytää sopivia ohjaimia.

RAID 5-taso nopeuttaa suorituskykyä ja parantaa datan turvallisuutta. Se vaatii vähintään kolme kiintolevyä, joiden kesken jaetaan pariteettibitit ja tällä tavalla saadaan käyttöön

enemmän kiintolevytilaa. Kolmesta kiintolevystä on käytettävissä kahden kiintolevyn tallennuskapasiteetti ja neljän kiintolevyn järjestelmässä on käytössä kolmen kiintolevyn edestä tallennustilaa.

Jos RAID 5-tason kiintolevyistä yksi hajoaa, voidaan sen sisältö palauttaa muille kiintolevyille tallennetuista pariteettibiteistä uudelle kiintolevylle. RAID 5-tasossa on suorituskykyä ja se on turvallinen datan kannalta. Miinuksena on kuitenkin huono kirjoitusnopeus, joka tarkoittaa sitä, että varmuuskopiointi kestää kauemmin.

RAID 6-tasossa vaaditaan vähintään neljä fyysistä kiintolevyä, joista käytetään kaksi kiintolevyä pariteettidataa varten ja kaksi jää tallennuskapasiteettia varten. RAID 6-konfiguraatio mahdollistaa tallennustilan laajentamisen helposti. Kiintolevyjä voi olla esimerkiksi kymmenen kappaletta, joista edelleen vain kaksi käytettäisiin pariteettidataa varten ja kahdeksan kiintolevyä olisi tallennuskapasiteettia varten.

RAID 6 kestää kahden fyysisen kiintolevyn hajoamisen. Sen suorituskyky on kohtuullinen, mutta huonompi kuin RAID 5-tasossa. Suorituskyky on kuitenkin parempi kuin yksittäisen kiintolevyn (Mato78 2012).

Lisäksi erilaisia yhdistelmiä ovat RAID 0+1 ja RAID 10-tasot sekä JBOD (Just a Bunch of Disks). RAID 0+1-tasossa yhdistyy kummankin tason ominaisuuksia ja vikasietoisuus ja nopeus parantuu. RAID 0+1-taso vaatii vähintään neljä kiintolevyä toimiakseen. RAID 10-taso tarjoaa tuon lisäksi vielä parantuneen suorituskyvyn ja luotettavuuden. JBOD näkyy yhtenä asemana käyttöjärjestelmässä, mutta toisin kuin RAID, se ei tarjoa turvaa tiedoille.

SAN (Storage Area Network) tekniikka on ollut käytössä jo 90-luvun loppupuolelta. Alun perin se oli kuitenkin niin kallis vaihtoehto, että pienemmillä yrityksillä ei ollut siihen varaa. Tekniikan kehittyessä hinnat ovat laskeneet, mutta hinta on edelleen tuhansia euroja (PCWorld 2013).

SAN on tallennusverkko, jota käytetään tiedon tallennukseen. SANiin liitetyt laitteet, kuten kiintolevyt, voidaan jakaa yhteiskäyttöön verkossa eli tarkoituksena on, että kaikki voivat käyttää samaa tallennuslaitetta samaan aikaan. NASin ja SANin ero on siinä, että NAS-levyt näkyvät käyttöjärjestelmissä verkkolevyinä, mutta SAN-levyt näkyvät kuin ne olisivat järjestelmän levyosioita.

SAN on helposti laajennettavissa. Jos yrityksellä tulee tarve hankkia lisää tallennustilaa, onnistuu tämä ostamalla lisää tallennustilaa. Tällä tavalla säästyy rahaa, kun jo olemassa olevaa

järjestelmää voi laajentaa sen sijaan, että lähtisi hankkimaan uutta sen takia, että tallennus-tila loppuu.

SAN voi käyttää Fibre Channel-liitäntää tai iSCSI-liitäntää. iSCSI-liitäntä käyttää IP-protokollaa tallennuslaitteiden yhdistämiseen. iSCSI SAN käyttää perus ethernet-kaapeleita, verkkokortteja ja kytkimiä.

Magneettinauhat muodostuvat ohuesta muovisesta materiaalista, jossa on päällä rautaoksidia. Granlundin mukaan (2004, 295) nauhoja käytettiin ennen viihde-elektroniikassa, mutta muiden laitteiden siirtonopeudet ja tallennustiheydet kiristivät kilpailua. Nykyään magneettinauhoja ja erilaisia kasetteja käytetään pääasiassa varmuuskopioinnissa niiden tallennuskapasiteetin takia.

Nauhaformaattia käytetään varmuuskopiointiin, koska se on luotettava ja pitkäikäinen tallennuslaite. Se vaatii jonkun henkilön vaihtamaan nauhoja ja varmuuskopioiden palauttaminen on hidasta, mutta yhdessä nauhassa on suurempi tallennuskapasiteetti kuin kiintolevyssä. Näiden positiivisten ominaisuuksien takia nauha on suosittu varmuuskopioinnissa ja varsinkin arkistoinnissa eli tiedostojen pidempiaikaisessa säilytyksessä.

Nauhojen pääformaattit ovat: LTO, DLT-S, DAT, AIT ja QIC. LTO (Linear Tape-Open) on ylivoimaisesti suosituin formaatti markkinaosuudeltaan. LTO-nauha-asemien osuus oli 91,18 % ja LTO-nauhakasettien osuus 83,58 %. LTO-nauhojen kehittämiseen osallistuvat muun muassa HP, IBM ja Quantum (Techtarget 2011).

Nauhavarmistus vaatii nauha-aseman, joka lukee ja kirjoittaa dataa. Nauha-asemista ylivoimaisesti käytetyimpiä ovat LTO-asemat ja ne ovat edenneet jo viidenteen sukupolveen. Viidennen sukupolven LTO-asemat ovat osittain yhteensopivia kahden aikaisemman sukupolven kanssa. Nauha-asema voidaan liittää palvelimiin SAS-liitännällä (Fujitsu).



Kuva 4: Fujitsun LTO-nauha-asema (Fujitsu)

LTO:n ensimmäinen versio julkaistiin vuonna 2000 ja siitä on tullut uusia versioita suuremmalla tallennuskapasiteetilla parin vuoden välein. Tämän hetkinen versio on LTO-6, jonka siirtonopeus on 160 Mt/s. LTO-7 tulee siirtämään dataa jopa 315,2 Mt/s siirtonopeudella ja LTO-8 472 Mt/s. LTO-9 ja LTO-10 ovat myös suunnitteilla (Techtarget 2014).

LTO:n ensimmäisen version tallennuskapasiteetti oli 100 Gt ja 200 Gt pakattuna. Viidennessä versiossa tallennuskapasiteetti oli jo 3 Tt pakattuna 280 Mt/s siirtonopeudella. Tämän hetkessä vuonna 2012 julkaistussa LTO6-versiossa kapasiteetti on pakattuna 6,25 Tt ja siirtonopeus 400 Mt/s.

DLT:n (Digital Linear Tape) ensimmäinen versio julkaistiin vuonna 1993. Siinä oli tallennuskapasiteettia 10 Gt ja pakattuna 20 Gt. DLT:n viimeisin versio SuperDLT2 on vuodelta 2004 ja siinä on 300/600 Gt tallennuskapasiteettia.

DAT (Digital Audio Tape) tunnetaan myös nimellä DDS (Digital Data Standard). Ensimmäinen versio DDS1 tai DAT julkaistiin vuonna 1989. DAT-nauhoissa on pienempi todennäköisyys palauttaa tiedot onnistuneesti kuin muissa uudemmissa formaateissa ja tämän takia DAT-asetat vaativat säännöllistä siivousta. Näin voidaan yrittää estää varmuuskopioiden ja tiedostojen palautuksen epäonnistuminen.

AIT (Advanced Intelligent Tape) on Sonyn suunnittelema 8mm nauha, joka tukee WORM-tekniikkaa (Write-Once Read-Many). WORM tarkoittaa, että nauhoille voi kirjoittaa dataa vain kerran, mutta sitä voi lukea useamman kerran eli se toimii samalla tavalla kuin CD-R-levyt. Tässä on tavoitteena arkistoida data, mutta ei palauttaa sitä.

QIC (Quarter Inch Cartridge) suunniteltiin alun perin tietokoneiden kotikäyttäjille, mutta tekniikka on sen verran vanhentunutta, että sitä ei näe enää markkinoilla. Tallennustilaa on ollut maksimissaan pakattuna 5 Gt. Erilaiset kiintolevyt ja muistitikut ovat korvanneet QIC:n käyttäjien kodeissa (Discover Tape).

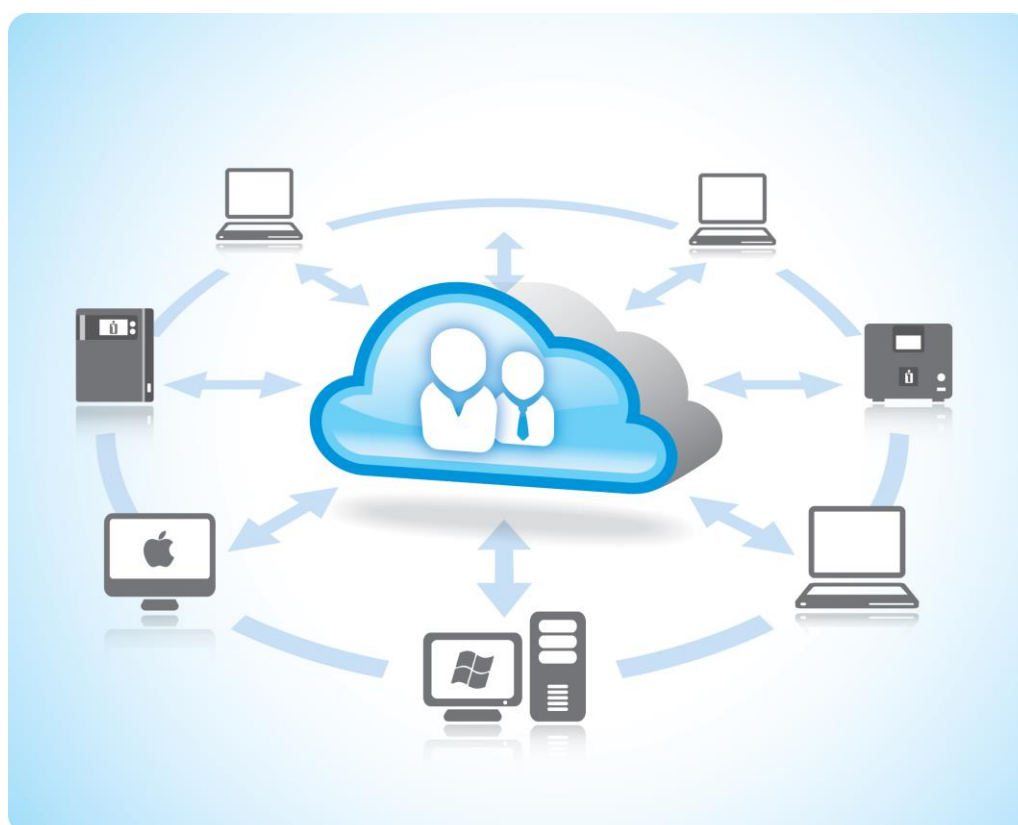
Nauhavarmistuksen suurin ongelma on sen kallis hinta eikä se sovi välttämättä kaikille pienille tai keskisuurille yrityksille. DAT-asemien hinnat alkavat noin 500 eurosta ja uusinta tekniikkaa olevat LTO6-asetat alkavat 2500 eurosta. Yhden LTO6-nauhan hinta on noin 50 euroa.

#### 5.4 Etävarmistus

Volasen mukaan (Artikkeli Suomi 2012) etävarmistuksella tarkoitetaan sitä, että data varmuuskopioidaan asiakkaan päätelaitteelta tai palvelimelta keräämällä, pakkaamalla ja salaa-

malla data palveluntarjoajan ”pilveen”. Etävarmistus suoritetaan automaattisesti ja säännöllisesti ilman asiakkaan osallistumista.

Pilvipalveluilla tarkoitetaan esimerkiksi internetin kautta hankittavaa tietokonekapasiteettia, kuten tallennustilaa. Pilvipalvelu voisi myös tarkoittaa palvelua tai sovellusta. Sen avulla voidaan vähentää tai jopa luopua fyysisistä konesaleista, koska sovellukset tai data ovat pilvipalveluntarjoajan palvelimilla eikä asiakkaalla itsellään tarvitse olla tehokkaita tietokoneita sovellusten pyörittämiseen tai tallennustilaa datan säilyttämiseen (Pilvipalvelut 2010, 32).



Kuva 5: Pilvi (Businesswebdevs 2014)

Pilvipalveluihin kuulu elastinen provisiointi. Tämä tarkoittaa, että palveluiden käyttö on joustavaa ja jopa automaattista eikä uusia asiakkaita, palveluiden lisäämistä tai käytön lopettamista varten tarvitse ostaa uusia laitteita. Pilvipalveluiden käyttöönotto on helppoa eikä sitä varten tarvitse pitkäaikaisia projekteja ja uusien ympäristöjen luomista. Pilvipalvelut voi ottaa helposti käyttöön ja niiden lopettaminen on myös helppoa.

Pilvipalveluiden positiivisiin ominaisuuksiin kuuluu se, että koska palveluntarjoajalla on tarvittavat resurssit, ei asiakkaan itse tarvitse panostaa tehokkaisiin laitteisiin, vaan kapasiteetti löytyy pilvestä. Kohdeyrityksen tapauksessa ei tarvitsisi itse ostaa tallennuslaitteita, koska vaadittava tallennuskapasiteetti löytyy palveluntarjoajan palvelimilta. Pilvipalvelut ovat myös

päätelaite- ja paikkariippumattomia eli periaatteessa laitteita voi käyttää missä tahansa millä tahansa laitteella, kunhan käytössä on internet-yhteys.

Pilvipalveluiden hinnat perustuvat palveluntarjoajan määrittämien kriteerien mukaisesti. Hinta määräytyy kuukausi-, tunti- tai muun ajan mukaan tai käytettävän kapasiteetin perusteella. Hintaan voi myös vaikuttaa palvelin- tai tallennuskapasiteetin määrä tai tietoliikennekulut.

## 5.5 Vertailut

Opinnäytetyössä vertailtavien ohjelmien valintaan vaikutti varmuuskopiointiohjelmien ominaisuudet. Tärkeää oli, että ohjelmassa oli kaikki luotettavuuden, eheyden ja saatavuuden saavuttamiseen vaadittavat ominaisuudet. Toinen tärkeä kriteeri oli ohjelmien saamat arvostelut sekä suosittuus, koska näiden perusteella sai hyvää pohjatietoa ohjelmista. Tällä pohjatiedolla sai rajattua ohjelmien suurta määrää ja selvitettyä mitkä niistä olivat toimivia ja vertailun arvoisia.

Ohjelmien suosittuutta lähdettiin selvittämään tutustumalla alan kirjallisuuteen, erilaisiin verkkojulkaisuihin ja blogeihin. Varmuuskopiointiohjelmiä löytyi suuri määrä, mutta tutustumalla tarkemmin aiheeseen löytyi suosittuja ohjelmia, joiden perusteella valitsin opinnäytetyössä vertailtavat ohjelmat. Ohjelmien suosittuuden ja arvostelujen perusteella opinnäytetyöhön valittiin kaksi vertailtavaa ohjelmaa: EaseUs Todo Backup ja AOMEI Backupper Standard.

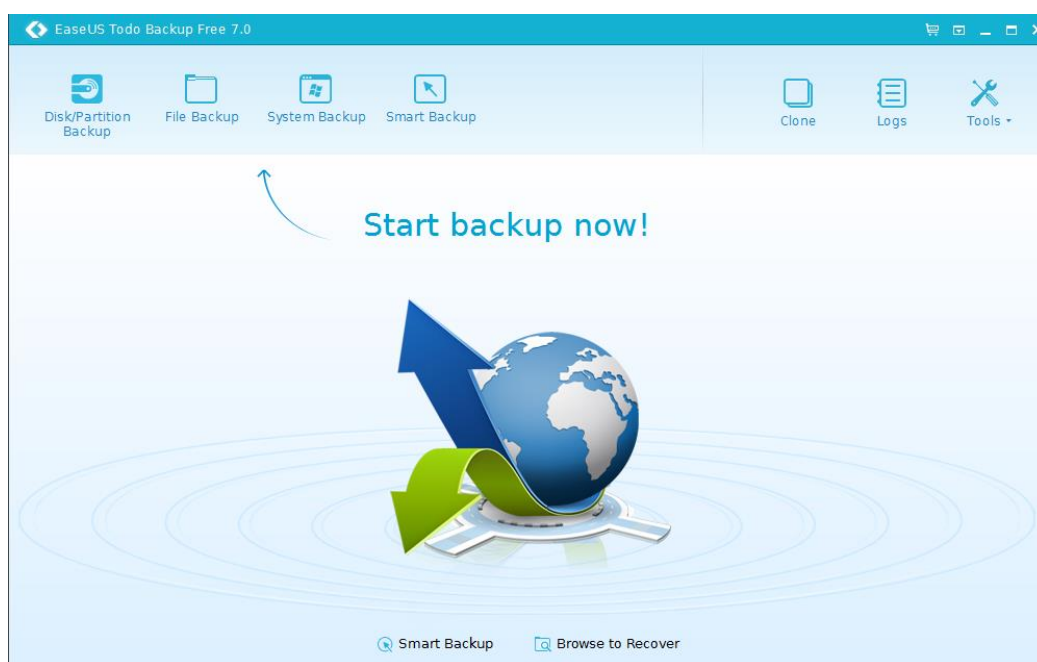
Opinnäytetyöhön valittuja ohjelmia kaikkia koekäytettiin kirjoittajan omalla koneella. Tällä tavalla saatiin kokemusta siitä kuinka helposti käytettäviä ohjelmistot olivat ja kuinka nopeasti varmuuskopiointi onnistui kullakin ohjelmistolla. Lisäksi saatiin arvokasta tietoa ohjelmien toiminnasta käytännössä ja myös tiedostojen palautuksesta.

Lisäksi oli tärkeää, että ohjelmat olivat yhteensopivia kohdeyrityksen laitteiston ja käyttöjärjestelmien kanssa. Tarkoituksena oli tutkia mikä on paras mahdollinen varmuuskopiointiohjelma Windows-käyttöjärjestelmään. Mac-yhteensopivuus on hyvä, mutta ei pakollinen. Näitä tärkeitä ominaisuuksia selvitettiin tutustumalla alan kirjallisuuteen ja artikkeleihin.

Valitut ohjelmat olivat useilla sivuilla parhaiden varmuuskopiointiohjelmien listoilla. Williams (TechRadar 2013) oli kirjoittanut 11 parhaan varmuuskopiointiohjelman listan ja valitut ohjelmat olivat sijalla 1. ja 2. Kummallakin ohjelmalla on suuret lataajamäärät ja hyvät arvostelukeskiarvot. Download.com antoi EaseUS Todo:lle neljä tähteä (2014) ja Jacobi kehui (PC World 2013) sitä kaikista kattavimmaksi vaihtoehdoksi.

EaseUS Todo Backup on EaseUS:n kehittämä varmuuskopiointiohjelma, jolla on yli kuusi miljoonaa käyttäjää ympäri maailman. Se on tuettu Windows XP-, Vista-, 7-, 8- ja 8.1-käyttöjärjestelmissä. Ohjelmasta on ilmainen versio sekä maksullisia versioita, kuten EaseUS Todo Backup Workstation 7.5 ja palvelinkäyttöön tarkoitettu EaseUS Todo Backup Server 7.5.

EaseUS Todo pystyy tekemään varmuuskopioita optiselle medialle, ulkoisille kiintolevyille, SCSI-laitteille tai verkkolevyille. Ohjelma mahdollistaa tiedostojen pakkaamisen mahdollisimman pieneen kokoon. Varmuuskopiot voi pakkaamisen lisäksi myös salata halutessaan.



Kuva 6: EaseUS Todo Backup Free 7.0-aloitusnäky

EaseUS Todo:lla voi varmistaa koko käyttöjärjestelmän ja palauttaa sen ongelmatilanteissa. Se pystyy myös varmistamaan koko kiintolevyn tai levyosion sekä yksittäisiä tiedostoja tai kansioita (Kuva 5). Ohjelma tukee myös ns. kuumia varmuuskopioita eli se voi varmuuskopioida käytössä tai avoinna olevia tiedostoja.

Ohjelma ottaa täysiä varmuuskopioita, joista voi sitten ottaa inkrementaalisia tai differentiaalisia varmuuskopioita. Varmistukset voi ajastaa menemään päivittäin, viikoittain, kuukausittain tai jopa pidemmällä aikavälillä. Lisäksi varmuuskopiot voi ottaa intervalleissa eli ohjelman voi laittaa tarkastamaan kopioitavat tiedostot esimerkiksi tunnin välein klo 8-16 välillä (EaseUS 2014).

EaseUS Todo:lla varmuuskopiot luodaan sillä tavalla, että niiden palauttamiseen ei tarvita itse ohjelmaa. Tämä mahdollistaa sen, että varmuuskopiot voi palauttaa myös tietokoneella, jo-



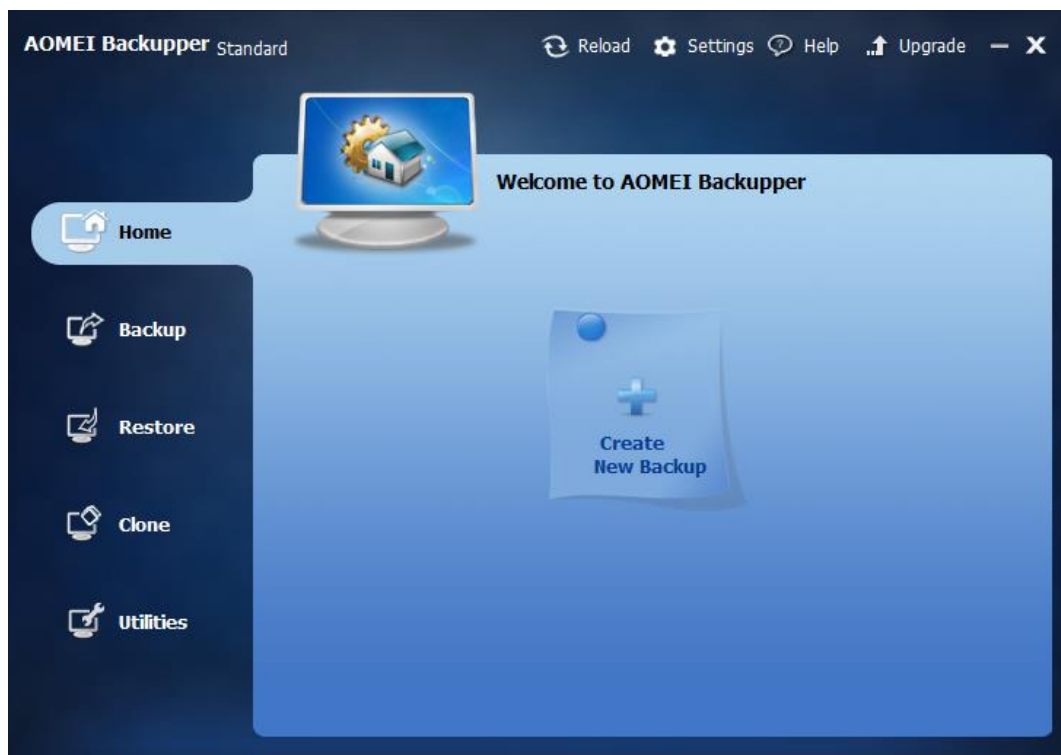
hon ohjelmaa ei ole asennettu. Varmuskopioista voi myös palauttaa yksittäisiä tiedostoja joko siihen alkuperäiseen sijaintiin tai sitten sen voi siirtää Copy+paste-toiminnolla toiseen sijaintiin.

AOMEI Backupper Standard on kiinalaisen AOMEI Technologyn kehittämä varmuuskopiointi ohjelma Windows-käyttöjärjestelmälle. Se on tuettu Windows XP-, Vista-, 7-, 8- ja 8.1-käyttöjärjestelmissä. Ohjelmasta on ilmainen versio sekä maksullisia versioita, kuten AOMEI Backupper Professional ja AOMEI Backupper Server, joka on tarkoitettu palvelimille.

Yrityksen sivujen mukaan ohjelma tukee kaikkia Windows-käyttöjärjestelmän tunnistamia tallennuslaitteita, kuten IDE, SATA, SCSI-liitäntäisiä kiintolevyjä, SSD-levyjä, ulkoisia kiintolevyjä ja muistitikkuja, joissa on Flash-muistia. Lisäksi se tukee myös RAID:in eri versioita, verkkokiintolevyjä ja jaettuja levyjä. Siinä on myös tuki virtuaalikoneille.

AOMEI Backupperilla voi ottaa järjestelmän näköistiedoston eli kopioida koko Windows-käyttöjärjestelmän asennettuine sovelluksineen ja asetuksineen. Sillä voi myös kopioida koko kiintolevyn tai vain levyosion. Näiden lisäksi voi varmistaa vain yksittäisiä tiedostoja tai kansioita.

AOMEI Backupperin käyttöliittymä on hyvin selkeä ja helppokäyttöinen. Aloitusnäkyvästä voi joko valita uuden varmuuskopiointin, tiedostojen palautuksen, kloonauksen tai asetukset (Kuva 6). Uuden varmuuskopion tekeminen on helppoa: valitaan 'Create New Backup' ja valitaan mistä kansioista varmistus tehdään ja mille laitteelle.



Kuva 7: AOMEI Backupper Standard-aloitusnäky

Ohjelmalla voi ottaa inkrementaalisia ja differentiaalisia varmuuskopioita täydestä varmuuskopiosta. Näin säästetään aikaa ja levytilaa, kun varmistetaan vain uudet tai muuttuneet tiedostot. Varmuuskopiot voidaan ajastaa menemään intervalleissa esimerkiksi tunnin välein, päivittäin, viikoittain tai kuukausittain

AOMEI Backupperiin saa päälle sähköposti-ilmoitukset. Asetuksista voi säätää missä tapauksissa ilmoitus lähetetään. Esimerkiksi, jos varmuuskopio epäonnistuu tai se vaatii toimenpiteitä käyttäjältä, niin siitä lähtee ilmoitus. Halutessaan voi pyytää ohjelmaa lähettämään ilmoituksen onnistuneista varmistuksista (AOMEI Technology 2014).

AOMEI Backupper-ohjelmalla tehtyjä varmuuskopioita ei voi palauttaa ilman itse ohjelmaa. Se hankaloittaa tiedostojen palautusta, koska jokaisella koneella pitää olla asennettuna tuo ohjelma tai se täytyy asentaa ennen kuin kopiot voi palauttaa.

#### 5.5.1 Tallennuslaitteiden Benchmarking-vertailu

Vertailuun ei otettu mukaan kaikkia erilaisia tallennuslaitteita, koska niissä ei ole tarpeeksi tallennustilaa yrityksen tiedoille suurten tiedostomäärien takia ja osalle niistä ei voi varmuuskopioida ilman manuaalista työtä. Lisäksi osa vaihtoehdoista oli liian kalliita. Vertailuun otettiin mukaan ulkoiset kiintolevyt, verkkokiintolevyt, nauhat ja etävarmistus.

<b>Ulkoiset kiintolevyt</b>	<b>Plus</b>	<b>Miinus</b>
	Helppous	Kestävyys
	Nopeus	Saatavuus (ei etänä)
	Tiedostojen hallinta	Yrityksen tiloissa
	Hinta	Laitteen siirtely paikasta toiseen

Taulukko 2: Ulkoiset kiintolevyt

<b>Verkkokiintolevyt (NAS)</b>	<b>Plus</b>	<b>Miinus</b>
	RAID	Riippuvainen verkosta
	Tiedostojen saatavuus	Yrityksen tiloissa
	Turvallinen	
	Hinta	

Taulukko 3: Verkkokiintolevy (NAS)

<b>Nauhat</b>	<b>Plus</b>	<b>Miinus</b>
	Pitkäikäisyys	Nauhojen vaihto
	Suuri tallennuskapasiteetti	Hinta

	Luotettava	Palautus hidasta
		Yrityksen tiloissa

Taulukko 4: Nauhat

Etävarmistus	Plus	Miinus
	Tiedot eri sijainnissa.	Hinta
	Varmuuskopiointi helppoa sijainnista riippumatta.	Saatavuus kiinni internet-yhteydestä
	Palveluntarjoaja hoitaa ylläpitotehtävät, laitteet ja näiden kulut	Joku muu hallinnoi tiedostoja
	Saatavuus	

Taulukko 5: Pilvi

### 5.5.2 Ohjelmien Kepner & Tregoe-vertailu

Vertailun on tarkoitus auttaa valitsemaan paras varmuuskopiointiohjelma sen ominaisuuksien perusteella. Mining Manin (2010) mukaan valitut ominaisuudet on jaettu pakollisiin eli Must ja toivottaviin tai haluttuihin eli Want-kategorioihin. Tämän jälkeen pitää valita kumpaan kategoriaan ominaisuudet kuuluvat. Ensin valitaan mitkä ominaisuudet ovat pakollisia (Must) ja muut ominaisuudet menevät Want-kategoriaan. Want-kategorian ominaisuudet pisteytetään asteikolla 0-10 ja lopuksi pisteet lasketaan yhteen. Eniten pisteitä saanut ominaisuus on paras Want-ominaisuuksista.

Seuraavat ominaisuudet valittiin tärkeiksi varmuuskopiointiohjelman kannalta.

- Helppokäyttöisyys
- Graafinen käyttöliittymä
- Kustannukset(ilmainen)
- Päivittäinen ajastettu varmistus

- Yksittäisten tiedostojen ja kansioiden varmuuskopiointi
- Windows-tuki
- Salaus
- yksittäisten tiedostojen tai kansioiden palautus

Must	EaseUS Todo	AOMEI Backupper
Helppokäyttöisyys	x	x
Graafinen käyttöliittymä	x	x
Kustannukset (Ilmainen)	x	x
Päivittäin ajastettu varmistus	x	x

Taulukko 6: Ohjelmien Must-ominaisuudet

Want	Painoarvo	EaseUS Todo	AOMEI Backupper
Yksittäisten tiedostojen & kansioiden varmuuskopiointi	8	x	x
Salaus	7	x	x
Yksittäisten tiedostojen & kansioiden palautus	8	x	
EaseUS Todo=23			
AOMEI Backupper=15			

Taulukko 7: Ohjelmien Want-ominaisuudet

### 5.5.3 Tulokset

Kumpikin ohjelma täytti Must-vaatimukset. EaseUs Todo sai Want-ominaisuuksista 23 pistettä, AOMEI Backupper sai 15. Ratkaiseva tekijä oli yksittäisten tiedostojen ja kansioiden palautus.

Kummastakin ohjelmasta on ilmainen versio sekä erilaisia maksullisia versioita lisäominaisuuksilla. Molemmissa ohjelmissa datan voi myös salata tarvittaessa. Ajastettu varmistus on mahdollinen kummassakin.

EaseUS Todo-ohjelma on helppoin käytettävä, koska siinä tarvittavat asetukset ovat muutamman säädön takana verrattuna AOMEI Backupperiin, jossa asetuksia täytyy käydä määrittämässä useammassa eri paikassa. Lisäksi AOMEI:ssa ei voi suoraan valita, että varmuuskopioidaan esimerkiksi Valokuvat-kirjasto koneelta, vaan se vaatii, että tämän alla on kansio. Jos halutaan varmuuskopioida kaikkien asiakkaiden eri kansioissa olevat kuvat, niin tätä toimenpidettä varten tulee luoda esimerkiksi kansio nimeltä Koulut ja päiväkodit, jonka alle sitten sijoitetaan kaikki valokuvat. Useasta kansioista ei voida ottaa varmuuskopiota samaan aikaan vaan kaikki kansiot tulee sijoittaa yhden kansion alle.

Kummassakin ohjelmassa on hyviä lisäominaisuuksia. AOMEI Backupper lähettää sähköposti-ilmoituksen epäonnistuneista varmistuksista tai jos käyttäjältä vaaditaan jotain toimenpiteitä. EaseUS Todo taas tekee niin sanottuja kuumia varmuuskopioita eli se varmuuskopioi myös muokattavana olevat tiedostot. Tämä on hyödyllinen ominaisuus, mutta yrityksen kannalta sillä ei ole suurta merkitystä, jos varmuuskopiot otetaan työajan ulkopuolella.

EaseUS Todo:lla varmuuskopioiden palauttaminen on erittäin yksinkertaista. Kun AOMEIlla kopiot tulee palauttaa samalla ohjelmalla kuin ne on tehtykin, EaseUS Todolla riittää, että tallennusmedia on kiinni koneessa. Ohjelmaa ei tarvita palautukseen ja yksittäisiäkin tiedostoja, kuten vaikka vain yhden valokuvan voi käydä palauttamassa joko siihen sijaintiin mistä se on kopioitu tai sitten sen voi siirtää Copy+paste-toiminnolla haluamaansa uuteen sijaintiin.

Benchmark-tulosten perusteella verkkokiintolevyt sekä etävarmistus ovat sopivimmat tallennusmediat yrityksen varmuuskopioille. Nauhat ja ulkoiset kiintolevyt jäivät vertailussa jälkeeseen, koska niillä oli enemmän negatiivisia puolia ja vähemmän positiivisia. Nauhoissa hyviä puolia olivat niiden pitkäikäisyys, yhden nauhan tallennuskapasiteetti ja luotettavuus, mutta negatiivisina puolina oli nauhojen vaihto, muita vaihtoehtoja huomattavasti korkeampi hinta ja palautusten hitaus.

Ulkoiset kiintolevyt ovat helppokäyttöisiä, suhteellisen nopeita USB 3.0-kaapelilla, tiedostojen hallinta on helppoa ja hinta on huomattavasti halvempi kuin muilla vaihtoehdoilla. Kiintolevyissä ongelmana on kuitenkin laitteiden lyhytikäisyys sekä tiedostojen saatavuus. Tämän lisäksi varmuuskopiot sijaitsevat yrityksen toimitiloissa ja useamman koneen varmistaminen vaatii joko useamman kiintolevyn tai kiintolevyn siirtelyä tilasta toiseen.

Etävarmistuksessa on hyvää se, että tiedot sijaitsevat eri sijainnissa ja palveluntarjoaja hoitaa kaikki ylläpitotehtävät, laitehankinnat ja näiden kulut. Hinta on sekä hyvä että huono puoli. Kuukausimaksut voivat olla hyvinkin halpoja, mutta pitkällä aikavälillä niiden yhteissumma kasvaa isoksi.

Etävarmistuksessa saatavuus on sekä myös hyvä että huono ominaisuus, sillä tietoihin voi päästä käsiksi mistä tahansa laitteesta ja sijainnista kunhan siinä on internet-yhteys. Tämä on myös sen huono puoli, koska jos internet-yhteyttä ei ole saatavilla niin myöskään tiedostoihin ei pääse käsiksi. Lisäksi on omat riskinsä, kun joku ulkopuolinen tekijä hallinnoi yrityksen tietoja.

Verkkokiintolevyissä on positiivisina ominaisuuksina RAIDin lisäämä turvallisuus, tiedostojen saatavuus eri laitteilla ilman kaapeleita ja hinta. Miinuksena on laitteen riippuvaisuus verkosta ja sen sijainti yrityksen toimipisteessä.

## 6 Yhteenveto

Opinnäytetyön tavoitteeksi asetettiin yrityksen varmuuskopioinnin uudistaminen ja kehittäminen. Liiketoimintaa suojattiin varmistamalla, että yrityksen kriittinen data on varmistettu. Yritykselle valittiin varmuuskopiointiohjelma, joka suorittaa varmistukset automaattisesti.

Opinnäytetyössä päästiin asetettuihin tavoitteisiin. Tavoitteena oli löytää vastaukset tutkimusongelmien kysymyksiin sekä kehittää kohdeyrityksen varmuuskopiointia tutkimalla mitä varmuuskopiointi on, miksi varmistuksia tehdään ja millä erilaisilla keinoilla ne voi tehdä. Lisäksi käytiin läpi eri tallennuslaitteita ja varmuuskopioiden puuttumisen tai pettämisen seurauksia.

Vertailtavat ohjelmat valittiin niiden suosittuuden ja arvosteluiden perusteella. Vertailuun valittuja ohjelmia vertailtiin niiden ominaisuuksien perusteella Kepner & Tregoe-mallin avulla. Kumpikin ohjelma täytti Kepner & Tregoen MUST-vaatimukset, mutta lopulta sopivimmaksi vaihtoehdoksi todettiin EaseUS ToDo Backup, koska sen tekemistä varmuuskopioista on helppo palauttaa yksittäisiä tiedostoja. Se ei onnistu AOMEI Backupperilla vaan tiedostojen palauttamiseen vaaditaan sama ohjelma, jolla varmistus on tehtykin.

Yrityksen varmistuksia helpottaisi eri tallennusmedian käyttöönotto. Tällä hetkellä käytössä on ulkoiset kiintolevyt, joita siirrellään tietokoneesta ja huoneesta toiseen. Joku verkon yli tapahtuva varmuuskopiointi karsisi tuon manuaalisen työn pois ja tiedostojen hallinta olisi helpompaa.

Yrityksen kannattaa panostaa joko verkkokiintolevyyn tai etävarmistukseen. Kummassakin vaihtoehdossa on negatiivinen puoli siinä mielessä, että varmuuskopioinnin onnistuminen on riippuvainen internet-yhteydestä. Lisäksi yritys voi joutua panostamaan nopeampaan laajakaistayhteyteen.

Jos yritys päätyy verkkokiintolevyyn, niin sen kannattaa panostaa vähintään RAID 5-tason varmistukseen. Yrityksellä kertyy dataa noin yhden teratavun verran vuodessa, joten yrityksen kannattaisi kerralla panostaa suurempaan tallennuskapasiteettiin. Joistain verkkokaupoista voi saada 8 teratavun verkkokiintolevyn RAID 5-tasolla alkaen 550 eurolla.

Yhden teratavun etävarmistuksen voi saada halvimmillaan alle 10 eurolla kuussa tai noin 100 eurolla vuodessa. 10 euroa kuussa saattaa tuntua pieneltä summalta, mutta kun varmistukset suoritetaan tällä tavalla kuukausien ja vuosien ajan, on loppusumma jo huomattavasti suurempi. Etävarmistuksen hyvänä puolena on se, että tiedot ovat poissa yrityksen toimitiloista, mutta samalla on olemassa riski, kun joku muu hallinnoi tietojasi.

Suositukseni on, että tiedostoista otetaan kerran viikossa täysi varmuuskopio ja päivittäin inkrementaalinen kopio eli varmistetaan vain muuttuneet tiedostot. Inkrementaaliset varmuuskopiot kannattaa ottaa illalla tai yöllä työajan päätyttyä. Tällä tavalla toimittaessa tiedostot saadaan varmistettua ilman, että työnteko häiriintyy. Lisäksi on suositeltavaa, että tietokoneiden käyttöjärjestelmistä otetaan näköistiedosto.

Varmuuskopioita tulee säilyttää mielellään eri tilassa kuin alkuperäistä dataa, mutta aina tämä ei ole mahdollista. Suositeltavaa on, että varmuuskopioita säilytettäisiin yrityksen toimitilojen ulkopuolella, mutta jos tämä ei onnistu niin niitä tulisi säilyttää tulenkestävässä tilassa. Lisäksi olisi kannattavaa olla useampia varmuuskopioita kaiken varalta.

Opinnäytetyötä varten haastateltu asiantuntija suositteli, että yritys ottaisi käyttöön SAN-verkkoon kytketyn levyjärjestelmän, jossa olisi vähintään RAID 5-tason varmistus. SAN-verkko on kuitenkin liian hintava vaihtoehto yritykselle eikä yrityksestä löydy myöskään teknistä osaamista sen asentamiseen ja ylläpitoon. Yrityksellä ei ole myöskään niin paljon laitteistoa, että SAN-verkko olisi tarpeellinen.

Koska kiintolevyt kestävät vain tietyn ajan, on suositeltavaa harkita nauhojen hankkimista arkistointia varten niiden pitkäikäisyyden takia. Jos yritys päättää säilyttää arkistoitavat tiedostot kiintolevyllä, voi tiedon joutua siirtämään eri tallennuslaitteille vuosien aikana, koska kiintolevyt säilyvät lyhemmän aikaa. Nauha-aseman ja nauhojen hankkiminen on kalliimpi vaihtoehto, mutta pitkäikäisempi, koska kiintolevyt voi joutua korvaamaan useamman kerran vuosien aikana.



## Lähteet

Ruohonen, M. 2002. Tietoturva. Jyväskylä: Docendo Finland.

Rousku, K. 2014. Kyberturvaopas tietoturvaa kotona ja työpaikalla. Helsinki: Talentum Media.

Flyktman, R. 2010. Suuri PC-käsikirja - Windows 7. Helsinki: Readme.fi.

Paananen, J. 2003. Tietotekniikan peruskirja. Jyväskylä: Docendo Finland.

Rountree, D. 2011. Security for Microsoft Windows System Administrators: Introduction to Key Information Security Concepts. Burlington: Syngress.

Niva, M. & Tuominen, K. 2005. Benchmarking käytännössä: Itsearviointin työkirja. Turku: Oy Benchmarking Ltd.

Wallace, M. & Webber, L. 2010. The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets. New York: AMACOM

Granlund, K. 2004. Laitetekniikka. Jyväskylä: Docendo Finland.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja - Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita Publishing.

TechTerms. 2008. Backup. Viitattu 28.7.2014 <http://www.techterms.com/definition/backup>

<http://www.mv.helsinki.fi/home/psaukkon/tutkielma/Tutkimusongelma.html> 29.7.2014

<https://koppa.jyu.fi/avoimet/hum/menetelmapolkuja/menetelmapolku/tutkimusstrategiat/laadullinen-tutkimus> 5.8.2014

Dynamic Quest. 2013. 5 Common Reasons for Data Backup Recovery Failure. Viitattu 18.8.2014.

<http://www.dynamicquest.com/5-common-reasons-data-backup-recovery-failure/>

McMahon, M. 2014. What Are Pros and Cons?. Viitattu 28.9.2014.

<http://www.wisegeek.org/what-are-pros-and-cons.htm>

Rudy, M. 2013. Cloud vs. Local Backup: Which Do You Need?. Viitattu 13.10.2014.

<http://www.techopedia.com/2/29440/trends/cloud-computing/cloud-vs-local-backup-which-do-you-need> 13.10.2014

Conboy, J. 2011. Flash Drive Vs Hard Drive Vs Optical Media. Viitattu 15.10.2014.

<http://www.worldstart.com/flash-drive-vs-hard-drive-vs-optical-media/>

TechTerms. 2008. Optical Media. Viitattu 15.10.2014.

<http://www.techterms.com/definition/opticalmedia>

PCMag. Definition of: DVD storage capacities. Viitattu 16.10.2014.

<http://www.pcmag.com/encyclopedia/term/63259/dvd-storage-capacities>

TechTerms. Blu-ray. Viitattu 17.10.2014.

<http://www.techterms.com/definition/bluray>

Volanen, J. 2012. Etävarmistus turvaa kriittisen tiedon palveluna. Viitattu 23.10.2014.

<http://artikkelisuomi.com/2012/05/09/etavarmistus-turvaa-kriittisen-tiedon-palveluna/>

Kay, R. 2010. Flash Memory. Viitattu 26.10.2014.

<http://www.computerworld.com/article/2550624/data-center/flash-memory.html>

Santo Domingo, J. 2014. SSD vs. HDD: What's the Difference?. Viitattu 26.10.2014.

<http://www.pcmag.com/article2/0,2817,2404260,00.asp>

Williams, M. 2013. Best free backup software: 11 programs we recommend. Viitattu 6.11.2014. <http://beta.techradar.com/news/software/applications/best-free-backup-software-11-programs-we-recommend-1137924>

Download.com. 2014. EaseUS Todo Backup Free. Viitattu 6.11.2014.

[http://download.cnet.com/EaseUS-Todo-Backup-Free/3000-2242\\_4-10964460.html](http://download.cnet.com/EaseUS-Todo-Backup-Free/3000-2242_4-10964460.html)

Jacobi, J. 2013. Review: Easeus Todo Backup Free is the most comprehensive free backup. Viitattu 6.11.2014.

<http://www.pcworld.com/article/2040484/review-easeus-todo-backup-free-is-the-most-comprehensive-free-backup.html>

Decision making confidence. Kepner Tregoe Decision Making The Steps, The Pros and The Cons. Viitattu 11.11.2014.

<http://www.decision-making-confidence.com/kepner-tregoe-decision-making.html>

Mining Man. 2010. Simple Guide to KT Analysis A Great Decision Making Tool. Viitattu 11.11.2014.

<http://www.miningman.com/Blog/January-2010/Simple-Guide-KT-Analysis-Decision-Making-Tool>

Mato78. 2012. Opas RADin maailmaan. Viitattu 11.11.2014.

<http://www.mato78.com/arvostelut/muistit-ja-massamuistit/opas-raidin-maailmaan/>

<http://businesswebdevs.com/wp-content/uploads/2014/04/Personal-Cloud-Storage1.jpg>

LapTech- Kannettavatietokone.fi. Kannettavien kiintolevyt (kovalevyt) ja SSD. Viitattu 16.11.2014. <http://www.kannettavatietokone.fi/info/kiintolevy.html>

Manuaali.fi. SATA vai PATA?. Viitattu 17.11.2014.

<http://manuaali.fi/tietokone/tietokoneen-osat/kiintolevy/>

Techterms.com. SATA. Viitattu 17.11.2014.

<http://www.techterms.com/definition/sata>

Beal, V. Small Computer System Interface - SCSI. Viitattu 17.11.2014.

<http://www.webopedia.com/TERM/S/SCSI.html>

Freegeek. 2013. Viitattu 17.11.2014.

<http://wiki.freegeek.org/images/2/21/Pata-vs-sata.jpg>

Beal, V. SAS. Viitattu 17.11.2014.

[www.webopedia.com/TERM/S/SAS.html](http://www.webopedia.com/TERM/S/SAS.html)

Rouse, M. 2005. Fibre Channel. Viitattu 17.11.2014.

<http://searchstorage.techtarget.com/definition/Fibre-Channel>

Muropaketti.com. 2008. HDD, SSD, SSD-asemien MLC- SLC-valmistustekniikat & SSD-HDD-kokoverailu. Viitattu 17.11.2014.

<http://muropaketti.com/artikkelit/ssd-asetat/hdd-ja-ssd-asetat-testissa>

Techtarget. 2008. Full, incremental or differential: How to choose the correct backup type. Viitattu 17.11.2014.

<http://searchdatabackup.techtarget.com/feature/Full-incremental-or-differential-How-to-choose-the-correct-backup-type>)

Rouse, M. 2006. Secure Digital card (SD card). Viitattu 17.11.2014.

<http://searchstorage.techtarget.com/definition/Secure-Digital-card>

Integral Memory. CARDS - What is the difference between SDHC and SD Cards?. Viitattu 17.11.2014.

<http://www.integralmemory.com/faq/cards-what-difference-between-sdhc-and-sd-cards>

SD Association. SDXC Standard. Viitattu 17.11.2014.

[https://www.sdcard.org/consumers/sdxc\\_capabilities/](https://www.sdcard.org/consumers/sdxc_capabilities/)

AOMEI Technology. 2014. AOMEI Backupper Standard 2.0.3. Viitattu 18.11.2014.

<http://www.backup-utility.com/free-backup-software.html>

Cohen, P. 2014. How to easily back up and restore your Mac with Time Machine on OS X Mavericks. Viitattu 18.11.2014.

<http://www.imore.com/how-set-and-restore-time-machine-backup>

Scalisi, M. 2010. Within Reach of Most IT Budgets, Storage Area Networks Pay Off. Viitattu 20.11.2014.

[http://www.pcworld.com/article/199173/how\\_storage\\_area\\_networks\\_benefit\\_business.html](http://www.pcworld.com/article/199173/how_storage_area_networks_benefit_business.html)

Sharwood, S. 2011. Five types of tape for backup or archive. Viitattu 25.11.2014.

<http://searchstorage.techtarget.com.au/feature/Five-types-of-tape-for-backup-or-archive>

Afterdawn. NAS. Viitattu 25.11.2014.

<http://fin.afterdawn.com/sanasto/selitys.cfm/nas>

iPoint. 2014. Network Attached Storage- 4 Reasons Why Your Business Could Benefit. Viitattu 25.11.2014.

<http://ipoint-tech.com/network-attached-storage>

Burton, A. 2014. LTO tape vendors announce LTO-9 and LTO-10. Viitattu 25.11.2014.

<http://searchdatabackup.techtarget.com/news/2240230680/LTO-tape-vendors-announce-LTO-9-and-LTO-10>

Fujitsu. Ulkoinen LTO-nauha-asema. Viitattu 27.11.2014.

<http://www.fujitsu.com/fi/products/computing/storage/tape/lto/>

Discover Tape. List of Tape Backup Technologies. Viitattu 27.11.2014.

<http://www.discovertape.com/tape-technologies.html>

Kekkonen, J. 2014. Asiantuntijahaastattelu 15.10.2014. Accenture Oy. Helsinki.

## Kuvat

Kuva 1: Samsungin SSD-kiintolevy (PC Magazine 2014).....	22
Kuva 2: PATA & SATA (Freegeek 2013).....	24
Kuva 3: Network Attached Storage (iPoint 2014) .....	25
Kuva 4: Fujitsun LTO-nauha-asema (Fujitsu) .....	28
Kuva 5: Pilvi (Businesswebdevs 2014) .....	30
Kuva 6: EaseUS Todo Backup Free 7.0-aloitusnäkyä .....	32
Kuva 7: AOMEI Backupper Standard-aloitusnäkyä.....	34

Kuviot

Kuvioluettelon ensimmäinen rivi alkaa tästä, riviväli 1

## Taulukot

Taulukko 1: Varmuuskopionitkeinojen vertailu.....	16
Taulukko 2: Ulkoiset kiintolevyt.....	35
Taulukko 3: Verkkokiintolevy (NAS) .....	35
Taulukko 4: Nauhat .....	36
Taulukko 5: Pilvi .....	36
Taulukko 6: Ohjelmien Must-ominaisuudet.....	37
Taulukko 7: Ohjelmien Want-ominaisuudet.....	37



## Liitteet

Liite 1 Asiantuntijahaastattelu .....	50
---------------------------------------	----

## Liite 1 Asiantuntijahaastattelu

### 1 Kerro itsestäsi. Mikä on työnkuvasi?

Olen Janne Kekkonen, koulutukseltani datanomi ja työskennellyt viimeiset 15 vuotta Unix-/Linux-kouluttajana ja System Administrator -tehtävissä sekä Unix-/Linux-käyttöjärjestelmien että tallennusympäristöjen asentamis- ja ylläpitoprojekteissa monikansallisissa yrityksissä. Viimeiset neljä vuotta olen työskennellyt erilaisten pilviratkaisujen suunnittelu- ja koulutus-tehtävissä, missä tehtäviini on kuulunut myös varmuuskopiointi- ja palautusjärjestelmien suunnittelu, käyttöönotto ja käyttöönoton koulutus.

### 2. Mitä on varmuuskopiointi ja miksi niitä kannattaa tehdä?

Varmuuskopiointi takaa, että esimerkiksi yrityksen toiminnan kannalta kriittinen data ei häviä odottamattomissa tilanteissa kuten kiintolevyjen, palvelinten tai jopa kokonaisen datakeskusten vaurioituessa tai jopa tuhoutuessa kokonaan. Varmuuskopio otetaan yleensä kiintolevyltä (IDE, FC, SAS, SATA tai SSD) käsittäen yksittäisten hakemistojen, erillisten levypartitioiden, kokonaisten kiintolevyjen, peilattujen levyjärjestelmien, tietokantojen ja jopa kokonaisten datakeskusten varmuuskopioinnin. Varmuuskopioinneilla mahdollistetaan toiminnan jatkuminen levy- ja laitevikojen jälkeen minimoiden aika, jolloin tieto-järjestelmät ovat alhaalla.

### 3. Mitä seurauksia sillä voi olla, jos yritys ei ole ottanut varmuuskopioita ja menettää jostain syystä tiedostonsa?

Ajatellaan tilanne, että yrityksellä ei ole varmuuskopioita otettu koskaan yhdestäkään järjestelmästä, joissa kaikki yrityksen liiketoiminnan kannalta kriittiset asiakas- ja tuotetiedot olivat tallennettuina ennen kuin esimerkiksi tulipalo tuhosi koko laitekannan. Pahimmillaan tämä voisi johtaa yrityksen toiminnan loppumiseen, koska toiminnan jatkumisen kannalta kriittistä dataa ei enää ole tulipalon jälkeen olemassa ei missään eikä missään formaatissa. Varmuuskopioita joudutaan yritysmaailmassa ottamaan myös laki- ja veroteknisistä syistä ja tällaisissa tilanteissa jopa tahattomista laiminlyönneistä voi olla seurauksena rikosoikeudellisia toimenpiteitä ja korvaus- ja sanktioseuraamuksia.

### 4. Mitä erilaisia varmuuskopiointikeinoja on?

Varmuuskopiointikeinoja on erilaisia alkaen täydestä varmuuskopiosta (Full Backup), millä varmistetaan koko ensisijaisen tallennusvälineen data aina kokonaisuudessaan. Differentiaali varmuuskopiosta (Differential Backup) täyden varmuuskopion ottamisen jälkeen varmistetaan jokaisessa erillisessä differentiaali varmuuskopiosta kaikki täyden varmuuskopion jälkeen

muuttunut data omina tallenteina ja inkrementaali varmuuskopiossa (Incremental Backup) täyden varmuuskopion ottamisen jälkeen varmistetaan portaittain alkaen täydestä varmuuskopiosta inkrementaaleihin, joissa varmistetaan vain edellisen inkrementaali varmuuskopion jälkeen muuttunut data.

#### 5. Differentiaalinen vai inkrementaalinen varmuuskopio? Kumpaa suosittelet?

No ei näitä voi oikeastaan suositella kuin etelän lomamatkaa mieltymyksensä mukaan. Molemmille on omat käyttötarkoituksensa ja joissakin tapauksissa kriteereinä voi toimia nopeus ja toisissa kustannustehokkuus tallennuskapasiteetin näkökulmasta tarkasteltuna. Differentiaali varmuuskopio on vaivattomampi palauttaa ja näin ollen myös nopeampi palauttaa kuin inkrementaali, koska differentiaali varmuuskopiossa on aina vain kaksi tallennetta, mitkä pitää palauttaa, täysi ja viimeisin differentiaali varmuuskopio. Näin, koska jokainen differentiaali sisältää kaiken muuttuneen datan täyden varmuuskopion ottamisen jälkeiseltä ajalta ja palautuksessa halutaan palata viimeisimpään vallinneeseen tilanteeseen. Haittapuolena tässä on, että ajan kanssa varmuuskopioiden käyttämä tallennuskapasiteetti kasvaa huomattavasti suuremmaksi kuin inkrementaalin.

Inkrementaalin varmuuskopioinnin etuja on varmuuskopion ottamisen nopeus täyden varmuuskopion ottamisen jälkeen, koska inkrementaali tallentaa vain edellisen version jälkeiset muutokset jokainen inkrementaali kerrallaan joten tarvittava tallennuskapasiteetti, riippumatta inkrementaalien lukumäärästä, on vain täysi varmuuskopio + delta (alkuperäiseen dataan tulleet muutokset) verrattuna differentiaali varmuuskopioon, missä alkuperäisestä datasta otetaan täysi varmuuskopio + kaikki muutokset omalle erilliselle differentiaali varmuuskopiolle ei siis pelkkää deltaa kuten inkrementaalissa tehdään. Inkrementaalin haittapuolet tulevatkin sitten esiin, kun siltä joudutaan tekemään täysi palautus. Tässä operaatiossa pitää palauttaa ensin alkuperäinen täysi varmuuskopio sekä lisäksi jokainen inkrementaali erikseen kronologisessa järjestyksessä ensimmäisestä viimeisimpään ja tämä voi olla inkrementaalien lukumäärästä riippuen aikaa vievä prosessi. Tosin yhtenä etuna on myös seikka, että inkrementaali varmuuskopioista voidaan palauttaa myös eri versioita datasta eri ajankohdilta (sama pätee tietysti rajoituksin myös differentiaaliin).

Inkrementaali varmuuskopioinnissa on sellainen nyrkkisääntö, että kun inkrementaalien lukumäärä kasvaa liian suureksi esimerkiksi kymmeneen (täysi + kymmenen inkrementaalia), tulisi varmuuskopio nollata eli aloittaa sykli uudestaan koko järjestelmän täydestä varmuuskopiosta ja sitä seuraavat inkrementaalit alkaisivat uudestaan järjestyksessä ensimmäisestä eteenpäin, jotta mahdollinen palauttaminen ei olisi turhan työläs prosessi

#### 6. Millaisille tallennuslaitteille varmuuskopioinnit tehdään?

Varmennusvälineinä voivat olla erikokoiset magneettinauhat (dat), optiset levyt (CD-ROM, DVD), kiintolevyt, RAID0-kiintolevyt (Redundant Array of Inexpensive Disks, useamman levyn järjestelmä, missä kaikkien levyjen yhteenlaskettu tallennuskapasiteetti näyttäytyy kuin yksi levy) tai viimeisimpänä uusimman tekniikan SSD-levyt (Solid-State Disk) SAP HANA - järjestelmässä varmuuskopiot voivat olla myös muistinvaraisia kunnes ne siirretään niin sanotulle toisiolaitteelle, mikä voi olla esimerkiksi RAID-1 (peilattu levyjärjestelmä) levytilaa SAN-verkossa (Storage Area Network, tallennusverkko). Usein arkistoitavat varmuuskopiot menevät toisiolaitteilta myös magneettinauhalle, joita voidaan joutua säilyttämään useita vuosia ja joissakin tapauksissa jopa vuosikymmeniä vero- ja lakiteknisistä syistä palosuojatuissa kassakaapeissa. Pilveenkin voidaan varmuuskopioita tallentaa, mutta silloin tekniikat ovat edellä mainittujen kaltaisia, vain siirtotie on eri joko suoraan Internetin yli IPsec- tai VPN-tunnelin läpi tai joissain tapauksissa myös MPLS-kytkennäisen (MPLS, Multiprotocol Label Switching, yritysten eri paikkakunnilla sijaitsevien runkoverkkojen yhdistämistekniikka) verkon läpi. Yleensä pilvipalvelu on jonkin kolmannen osapuolen toimittama palvelu eli tallennuslaitteet sijaitsevat palveluntarjoajan datakeskuksessa eivätkä ole enää asiakasyritysten omissa konealeissa.

7. Mitkä ovat mielestäsi tiedostojen varmuuskopioinnin parhaat käytännöt? Eli mikä on paras keino varmuuskopioida tiedostoja?

Yksittäisten tiedostojen varmuuskopiointiin voidaan käyttää (liian) montaa erilaista tekniikkaa riippuen aina käyttöjärjestelmästä, missä operoidaan. Eri MS Windows -käyttöjärjestelmissä voidaan käyttää paikallisen varmistuksen ottamiseen yksinkertaisimmillaan WinZip-ohjelmaa. Linux- ja MAC OS -koneissa voidaan käyttää WinZip-ohjelmaa vastaavan zip-ohjelman lisäksi myös jar- ja tar-ohjelmia, mutta valikoima on laaja varsinkin kun tutkitaan Open Source - yhteisön valmistamia ohjelmia varmuuskopioiden ottamista varten (<http://www.linuxlinks.com/article/20090105114152803/Backup.html>).

Varmuuskopioinnin parhaina käytäntöinä pitäisin kuitenkin seuraavia seikkoja: ota varmuuskopio liian usein mieluummin kuin liian harvoin, älä säilytä varmuuskopioita koskaan koneen vieressä (CD-ROM, DVD, USB-levy, USB-muistitikku), mistä varmuuskopio otettiin, varmista aina, että kenelläkään ulkopuolisella ei ole pääsyä varmuuskopioihin, salaa varmuuskopiot silloin, kun ne eivät ole omassa hallinnassa (pilvessä, kolmannen osapuolen konealissa) ja ennen kaikkea varmista, että varmuuskopio on TOIMIVA eli siltä voidaan myös palauttaa tiedot!

8. Miten PK-yritysten (pienet ja keskisuuret yritykset, alle 250 työntekijää) ja isojen satojen tai tuhansien työntekijöiden yritysten varmuuskopioinnit, tekniikat ja tallennuslaitteet eroavat toisistaan?

No tämäkin riippuu ihan puhtaasti siitä, että puhutaanko IT-alasta, millä varmuuskopioasiantuntijat voivat löytyä omasta talosta vai puhutaanko perinteisestä savupiipputeollisuudesta, missä kaikki IT-alan palvelut ovat todennäköisesti ulkoistettu jollekin suurelle alan toimijalle. Pienissä IT-alan yrityksissä suositaan todennäköisesti Open Source -ohjelmistoja, joiden käyttämiseen ei tarvita kaupallisia lisenssejä. Talosta voi löytyä asiantuntija, joka hoitaa varmuuskopioiden ottamiseen liittyvät tehtävät. Vastaavan kokoisessa ei IT-alan yrityksessä palvelut on ulkoistettu ja silloin käytössä on kaupalliset varmuuskopiointijärjestelmät.

Tekniikat tuskin poikkeavat toisistaan paljoakaan, koska monet kaupalliset varmistusohjelmistotuotteet ovat sukua jollekin Open Source -projektille ja lisenssin hintaan sisältyvät kattavat tuki- ja ylläpitopalvelut. Monille Open Source -tuotteillekin löytyy erikseen toimitettavia maksullisia tuki- ja ylläpitopalveluita vaikka tuote itsessään olisikin ilmainen. Kun IT-yritysten koko skaalautuu suurten monikansallisten yritysten kokoluokkaan, niin tekniikat pysyvät pitkälti samoina, yleensä myös tuotteetkin, mutta usein tässä kokoluokassa on jo kyseessä jonkin mahdollisesti Open Source -tuotteena aloittaneen varmistusjärjestelmän (esim. NetApp) tallennussovellusympäristön rautaratkaisun käyttöönotosta, missä varmistusjärjestelmä palvelee eri maantieteellisissä solmuissa koko yritystä globaalilla tasolla. Tällöin kyseiset yritykset voivat käyttää jonkin laitetoimittajan (esim. NetApp, EMC, IBM, HP) järjestelmiä itse sisäisesti oman IT-järjestelmänsä varmistuksiin kuin myös toimia partnerina tai jälleenmyyjänä kyseisen tallennussovellusympäristön suhteen myydessään saman kokoluokan savupiipputeollisuuden asiakkailleen esimerkiksi SAP-järjestelmien asennuksia ja ylläpitosopimuksia tarjoten samalla myös kokonaispakettiin samaa varmistusjärjestelmää kuin itse käyttävät.

Valitettavasti kaikista kokoluokista ja joskus myöskin teollisuuden alastakin riippumatta, yritysten käyttämät tallennusjärjestelmät, varmistusjärjestelmät ja varmuuskopiojärjestelmät ovat jääneet ajasta jälkeen ja näistä valitettavista tapauksista saa lukea surullisia tarinoita alan julkaisuista, kun esimerkiksi antiikkiset 90-luvulla hankitut magneettinauhat osoittautuivatkin tyhjiksi siinä vaiheessa, kun niitä viimein tarvittaisiin. Kukaan ei tullut ajatelleeksi missään vaiheessa, että 90-luvun lopun dat-nauhat kestävät noin 50-100 luku- tai kirjoitusoperaatiota ja niitä on saatettu käyttää katastrofin iskiessä jo satoja jopa tuhansia kertoja.

9. Mikä on mielestäsi paras tallennusmedia varmuuskopioille, kun tiedostoja kertyy noin teran verran vuodessa?

Ensisijaisena tallennusmediana tällaisessa teran/vuosi kierrossa käyttäisin ehdottomasti SAN-verkkoon kytkettyä levyjärjestelmää, missä on vähintään RAID5-tason (Single Distributed Parity) varmistus, mielellään RAID6 tai RAID DP (molemmat Double Parity), toisiojärjestelmänä eli ensimmäisenä varmuuskopion tallennusmediana voisi olla esimerkiksi halvoista SATA-levyistä rakennettu RAID5-, RAID6- tai RAID DP -NAS tallennusjärjestelmä (Network Attached Storage, verkkolevyjärjestelmä), missä levytilaa tulisi olla vähintään kaksi kertaa ensiojärjestelmän verran ja lisäksi arkistoitavaa dataa varten uusimpia dat-magneettinauhoja, jotta arkistoitava data olisi sellaisella medialla, että sitä voidaan lukea vielä kymmenen vuoden jälkeen.

10. Miten itse suoritat varmuuskopiosi? Kuinka usein otat varmuuskopiot?

Kotona olevista testijärjestelmistä joka yö (inkrementaali), kotikäytössä olevista kannettavista tietokoneista clonezilla-nimisellä varmistusohjelmalla koko levyn varmuuskopio NAS-verkkolevyille vähintään kerran kuussa toisinaan jopa useamminkin. Itse käytän kaikissa kotona olevissa koneissa Linux Mint -käyttöjärjestelmää, joten niitä varmistelen myös aina silloin, kun päivitän uuden käyttöjärjestelmäversion. Työssäni joudun valvomaan SAP-järjestelmiä, joista varmuuskopioita otetaan eri tasolla tunneittain, päivittäin, viikoittain ja kuukausittain etukäteen määriteltyjen profiilien ja sääntöjen mukaan. Nämä ovat operatiivisiä varmuuskopioita, joista järjestelmien palautus pitää pystyä toteuttamaan 24 tunnin kuluessa. Lisäksi tulee puolivuositteiset ja vuotuiset arkistovarmuuskopiot, mitkä menevät toisiojärjestelmistä magneettinauhoille ja toimitetaan asiakkaille kassakaappeihin arkistoitaviksi. Ja meinasin unohtaa mainita, että kotikäytössä oleva NAS-järjestelmä on RAID1 peilattu.

11. Mitä ohjelmaa tai ohjelmia käytät?

No osa tulikin jo aikaisemmin mainittua eli ihan arkisissa pikavarmistuksissa WinZip, tar, jar, zip ja cpio, mutta kun pitää ottaa talteen koko levy, niin clonezilla on nopein ja varmatoimisin tällaiseen tarkoitukseen. Toki silläkään ei voi ottaa käynnissä olevasta käyttöjärjestelmästä varmuuskopiota, vaan tietokone täytyy uudelleenkäynnistää joko CD-ROM:lta, DVD:ltä tai GRUB-osiolta (GRand Unified Bootloader) clonezilla-ympäristöön, missä itse varmuuskopion ottaminen on suhtkoht nopea operaatio. 120 GB:n SSD-levyn varmuuskopio syntyy 1 Gb:n verkon yli noin kymmenessä minuutissa ja usko tai älä, koko Linux Mint -käyttöjärjestelmän palauttaminenkin kestää tyhjälle levyille myös sen noin kymmenen minuuttia.

12. Miten toimit itse, jos menetät tiedot? Kuinka palautat varmuuskopiot?

En panikoi, varmuuskopiot löytyvät joten palautus on nopea ja kivuton toimenpide kotioloissa. Tietokone uudelleenkäynnistetään clonezilla-ympäristöön ja jo edellä mainitsemani reilun kymmenen minuutin kuluttua tietokoneeni on turvallisesti taas Linux Mint -käyttöjärjestelmän

voimin käytössä. Varsinaista loppukäyttäjän datan hukkumisen pelkoa minulla ei kotiloissa ole, sillä tallennan kaiken tärkeän tiedon kannettavan tietokoneeni paikallisen levyaseman sijasta NAS-levyjärjestelmän CIFS-tiedostojärjestelmään (Common Internet File System, entinen Samba-levyjakojärjestelmä), mikä oli siis RAID1-peilatuilla levyillä.

Sellaiset tiedostot, jotka haluan matkoille mukaan, tallennan salattuina DropBox-pilvipalvelun levyille ja itseasiassa paikallinen CIFS-jakoni sisältää jo sellaisen hakemiston, mikä peilautuu suoraan vastaavaan hakemistoon DropBox-pilvessä, joten tarvitsemiani tiedostoja ei tarvitse kopioida manuaalisesti edes DropBoxiin. Työssäni minun ei tarvitse välittää yrityksen kannettavan tietokoneen varmistuksista itse, kone varmuuskopioi kaikki uudet My Documents -hakemiston tiedostot automaattisesti yrityksemme verkossa ollessani verkkolevyille. Jos sitten vahingossa poistan jonkun tiedoston kannettavalta tietokoneeltani, voin helposti palauttaa kyseisen tiedoston toimistolla ollessani. Toki varmistan tärkeimmät tiedostot silloin tällöin yrityksen politiikan mukaisesti salatulle USB-muistitikulle.

Asiakkaidemme järjestelmien palautukset hoituvat tarkoin säädelyjen prosessien mukaisesti ja data on varmennettu niin moneen kertaan, että varsinaista datan häviämistä ei ole vielä koskaan eteeni tullut. Toki loogisia virheitähän nämä edellä mainitut RAID-tasot, varmistukset ja varmuuskopiot eivät suojaa, mutta se onkin jo sitten ihan toinen tarina se.