Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoliikenne

2012

Janne Aavasalo

HENKILÖKOHTAINEN TIEDON-VARMENNUS

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

Turun ammattikorkeakoulu

Tietojenkäsittely | Tietoliikenne

Elokuu 2012 | 78 sivua

Esko Vainikka

Janne Aavasalo

HENKILÖKOHTAINEN TIEDONVARMENNUS

Arvokkaan tiedon suojaaminen on yrityksissä arkipäivää. Varmuuskopiointiin liittyvät käytännöt on usein kirjattu joko yrityksen tietoturvastrategiaan tai niitä varten on laadittu täysin erillinen, tarkempi varmuuskopiointistrategia.

Kotikäytössä tällaisia käytäntöjä, tai edes niiden osia on harvoin käytössä ja jos varmuuskopiointia tehdään, pidetään sitä hyvin usein vain välttämättömänä pahana. Usein alkusysäys tietojen varmennukseen saadaan vasta ensimmäisen kiintolevyrikon jälkeen, joka saattaa johtaa esim. useiden vuosien aikana otettujen valokuvien tuhoutumiseen.

Vaikka kiintolevyt ovatkin koeteltua tekniikkaa ja niiden luotettavuus on nykyään erittäin hyvällä tasolla, ovat ne silti mekaanisia laitteita, joilla on rajallinen elinikä. Voidaan siis todeta, että kysymys ei ole siitä hajoaako kiintolevy, vaan milloin se hajoaa.

Vaikka yrityksissä tietoturvakäytännöt sekä -järjestelmät saattavat olla hyvinkin monimutkaisia, niin itse käytännön toteutus saattaa olla silti helpompi kuin kotiympäristössä. Yrityksissä toimitaan lähes poikkeuksetta verkkoympäristössä, jolloin varmuuskopioitava tieto on keskitetty palvelimille. Myös yrityksen resurssit kehittää ja ylläpitää näitä järjestelmiä ovat lähes poikkeuksetta paremmat kuin kotikäyttäjällä.

Kotikäyttäjän tilanteessa tiedot saattavat sijaita hyvinkin hajanaisesti useammalla tietokoneella, kännykässä, kameran muistikortilla, CD- tai DVD-levyillä tai vaikkapa USB-muistitikuilla. Tämän lisäksi saattaa olla epävarmuutta siitä, mitä tietoja loppujen lopuksi pitäisi varmuuskopioida, miten usein ja millä tavalla varmennus toteutetaan.

Otsikkoon on valittu sana ”tiedonvarmennus”, koska työssä ei tutkita ainoastaan pelkkää varmuuskopiointia, vaan myös mm. käyttöjärjestelmän suojaamista levykuvien avulla sekä järjestelmän palauttamista toimintakuntoon ongelmatilanteen jälkeen.

Varmuuskopioiden osalta tässä työssä käsitellään erilaiset varmuuskopiotyypit, tallennusmediat ja – sijainnit sekä kopioiden saatavuus sekä eheys ja niiden varmentaminen.

Esimerkkitapauksena rakennetaan tiedonvarmennusjärjestelmä valokuvausta harrastavalle yksityishenkilölle.

ASIASANAT:

varmuuskopio, kotikäyttäjä, henkilökohtainen, pilvipalvelu, levykuva, tiedostopalvelin, palautus, valokuvaaja

BACHELOR´S THESIS | ABSTRACT
TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data Communications

August 2012 | 78 pages

Esko Vainikka

Janne Aavasalo

PERSONAL DATA SECURITY

Although securing information and backing up data is considered an invaluable and important function in the corporate world, home users often neglect this aspect completely.

This is largely due to lack of knowledge, since implementing a sufficient backup and data safety system requires a bit more than just basic knowledge of computing. It might also need a monetary investment, although a basic system should not be out of anyone's reach.

Often the average users have also too much trust in their computers and especially regarding the hard drive. Since the hard drive is a mechanical component, one can say that it's not "if", but "when" it breaks down.

With luck, a hard drive can last as long as the computer itself, but it can also malfunction at any given time. At this point, a well implemented backup and recovery system would prove to be invaluable. Sadly this is often not realized until a malfunction actually happens and that can lead to the loss of all the personal data stored on the device.

Because companies work with local area networks, the implementation of a backup system might actually be simpler than at home. The data is usually centralized to one or more servers, which makes it easier to back up. A company may also have better resources to implement and maintain these systems than a home user.

Home users might have data scattered around on CDs or DVDs, memory cards, different computers and in some cases, even on floppy disks. On top of that, there's often confusion about what kind of data needs to be backed up and how often.

The title says "data security", because this thesis covers not only backup systems, but also imaging the operating system and how to recover after a disaster.

There is also a closer look at different types of backups, media selection for storing the backups. Concepts like availability and data integrity are also covered. A case study covers building a data security system, which is tailored for the needs of a photographer.

KEYWORDS:

backup, home user, personal, cloud, imaging, recovery, file server, photographer

SISÄLTÖ

KUVAT

KUVIOT

1 JOHDANTO

Tämän opinnäytetyön aihetta valitessani päädyin käsittelemään tiedonvarmennusta ja sen tärkeyttä kotikäyttäjän näkökulmasta.

Tiedon varmennukseen tai pikemminkin sen puutteen aiheuttamiin ongelmiin olen joutunut törmäämään lähinnä työelämässä, mutta aiheesta on myös omakohtaista kokemusta epähuomiossa tehdyn väärän osion alustuksen sekä kiintolevyn rikkoutumisen muodossa. Työssäni tietokoneita myyvän liikkeen huollossa pääsin tutustumaan aiheeseen mm. hajonneiden kiintolevyjen, haittaohjelmien tekemien tuhojen sekä käyttäjien itsensä suorittamien virheiden kautta. Tietojen menetykseen johtaneita tapauksia yhdisti lähes poikkeuksetta asiakkaan tietämättömyys, huolimattomuus sekä liian suuri luottamus laitteita kohtaan. Suurimmassa osassa näitä tapauksia olisi säästytty suurelta harmilta, mikäli tiedoista olisi aika-ajoin otettu yksinkertaisia varmuuskopioita esim. ulkoiselle kiintolevylle.

Kysyin usein asiakkaalta varmuuskopioiden tilanteesta konetta huoltoon tuotaessa, johon vastaus oli yleensä, että tietoja ei ole varmennettu missään vaiheessa. Tietojen varmennuksen vaikeus osoittautui usein syyksi tilanteeseen. Ei tiedetä, missä tiedostot levyllä sijaitsevat, mitä tietoja pitäisi varmentaa, kuinka usein ja miten varmennus yleensäkin kannattaisi hoitaa. Myös fyysisten sekä loogisten asemien erot eivät olleet selviä, eli varmuuskopioita oli saatettu tehdä saman levyn toiselle osiolle.

Opinnäytetyössä selvitetään tiedonvarmennuksen peruskäsitteet ja käsitellään varmuuskopioinnin ja tietojen palautuksen lisäksi myös RAID-järjestelmät sekä käyttöjärjestelmän varmuuskopiointi levykuvien avulla. Näiden peruskäsitteiden lisäksi käsitellään asiat, jotka on hyvä tietää jo järjestelmän suunnitteluvaiheessa, jotta pystytään välttämään esim. tarpeisiin nähden alimitoitetun järjestelmän rakentaminen. Varmuuskopiointijärjestelmän oikeanlaiseen mitoitukseen liittyy myös pohdinta siitä, mitä tietoja yleensä pitäisi varmentaa, kuinka usein ja mihin varmuuskopiot olisi parasta tallettaa.

Aiheenvalinnan taustalla on myös henkilökohtainen kiinnostus palvelimia, RAID- sekä verkkojärjestelmiä kohtaan ja siihen, miten näitä tekniikoita voidaan soveltaa tiedonvarmennusjärjestelmän rakentamisessa. Yhdistettynä nämä kokemukset sekä kiinnostuksen aiheet antoivat oman sysäyksensä aihevalintaan.

Työn empiirisessä osuudessa rakennetaan teoriaosuuden tietoja hyväksikäyttäen valokuvaajan käyttöön soveltuva tiedonvarmennusjärjestelmä. Käytössä on siis soveltava eli konstruktiivinen tutkimusmenetelmä. Järjestelmän suurimpina linjanvetoina toimivat käytön helppous, kustannustehokkuus sekä oikeanlainen mitoitus alati kasvavan valokuvakokoelman varmennukseen.

Työn tarkoitus on tutustuttaa lukija keskeisimpiin tiedonvarmennukseen liittyviin termeihin sekä tekniikoihin ja antaa vastaukset mm. edellä mainittuihin kysymyksiin: mitä tietoja pitäisi varmentaa, kuinka usein ja ennen kaikkea miten varmuuskopiointi suoritetaan. Varmennusjärjestelmän rakentamisen esimerkkitapaus on valittu siten, että siinä yhdistyvät hyvin yksinkertaisen, useimmille kotikäyttäjille riittävän järjestelmän lisäksi hieman edistyneempiä tekniikoita. Työ kattaa siis tiedonvarmennuksen perusteet, mutta siinä esitellään myös ratkaisuja, joita voidaan soveltaa myös vaativammissa kohteissa.

2 VARMUUSKOPIOINTI

Varmuuskopioinnin tarkoitus on tuottaa tiedosta kopio, jolla voidaan suojautua sitä uhkaavia sisäisiä sekä ulkoisia uhkia vastaan. Sisäisiä uhkia ovat mm. laitevauriot sekä käyttäjän tekemät virheet. Ulkoisiin uhkiin voidaan lukea mm. haittaohjelmien aiheuttama tiedon menetys sekä luonnonkatastrofit, tulipalot ja vesivahingot.

Varmuuskopiointijärjestelmä on toimiva, mikäli tällaisen tiedon menetyksen jälkeen tieto voidaan palauttaa varmuuskopiosta siten, että kaikki alkuperäinen tieto saadaan uudelleen käyttöön. Yleensä varmuuskopiot ovat kuitenkin ajallisesti hieman alkuperäistä tietoa jäljessä, joten katastrofitilanteesta toivuttaessa aivan uusinta dataa ei välttämättä saada palautettua. (Leikomaa 2005.)

2.1 Varautuminen ongelmatilanteisiin

Ongelmatilanteisiin voidaan varautua laatimalla kirjallisia ohjeistuksia, joiden avulla palautuminen poikkeustilanteesta voidaan suorittaa mahdollisimman nopeasti ja tehokkaasti. Näihin suunnitelmiin lukeutuvat mm. jatkuvuus-, toipumis-, varmennus- ja palautussuunnitelmat.

Mahdollisimman kattavien suunnitelmien tekeminen on erittäin tärkeää suuremmissa yrityksissä sekä organisaatioissa, sillä ongelmatilanteen pitkittyminen tarkoittaa yleensä merkittäviä rahallisia tappioita. Pienemmissä yrityksissä ei välttämättä tarvita kovin laajoja suunnitelmia, mutta ongelmatilanteissa sekä esim. vastuuhenkilön vaihtuessa hyvin tehty dokumentaatio auttaa pitkälle. (Laaksonen ym. 2006, 227.)

Kotikäyttäjän näkökulmasta varsinaisten suunnitelmien laatiminen ei välttämättä ole pakollista, ellei ongelmatilanteista toipuminen vaadi kovin monimutkaisia menetelmiä. On silti hyvä miettiä, mitä nämä menetelmät ovat, mitä niiden toteuttaminen vaatii ja missä järjestyksessä ne toteutetaan. Näiden menetelmien testaamista käytännössä ei myöskään ole syytä unohtaa.

Jatkuvuussuunnitelma

Hyvä jatkuvuussuunnitelma on ajantasainen, mahdollisimman kattava kokoelma arvioituja riskejä sekä toimintaohjeita, joiden mukaan toimitaan mikäli jokin näistä riskeistä toteutuu. Jatkuvuussuunnitelmaa pitää ajatella ennemmin prosessina kuin yksittäisenä dokumenttina, sillä sitä pitää kehittää, ylläpitää ja testata jatkuvasti, mikäli sen halutaan toimivan mahdollisimman tehokkaasti ongelmatilanteissa. Suunnitelman testaaminen kaikkien riskien varalta ei kuitenkaan ole aina mahdollista. (Raggad 2010, 217.)

Suunnitelma pitää laatia siten, että ensin kirjataan tavoitteet ja syyt jatkuvuussuunnitelman laatimiselle. Mikäli tavoitteita ei ole selkeästi määritelty, saattaa suunnitelmasta lopulta puuttua tärkeitä osa-alueita. Jatkuvuussuunnitelmassa määritellään myös ongelmatilanteiden aikana käytettävissä olevat resurssit sekä nimetään vastuuhenkilöt eri toimenpiteille. Myös muun henkilöstön kouluttaminen kuuluu olennaisena osana jatkuvuussuunnitelmaan, jotta ongelmatilanteen tullen osataan ottaa yhteys oikeisiin henkilöihin, jotka sitten alkavat toteuttaa suunnitelmiin kirjattuja toimenpiteitä. (Laakso 2011.)

Toipumissuunnitelma

Siinä missä jatkuvuussuunnitelmaan kirjataan käytäntöjä ja ohjeistuksia melko yleisellä tasolla, käsittelee toipumissuunnitelma yksittäisten segmenttien palauttamista toimintakuntoon ongelmatilanteen jälkeen. Jokaiselle tällaiselle segmentille pitäisi olla oma toipumissuunnitelmansa, jonka avulla se voidaan palauttaa toimintaan riippumatta toisista järjestelmistä. Nämä eri osa-alueet kannattaa myös järjestää tärkeysjärjestykseen, jolloin ydintoiminnot saadaan palautettua mahdollisimman nopeasti. Esimerkkinä ensimmäisenä palautettavasta ydintoiminnosta on vaikkapa yrityksen tiedostopalvelimen toimintakuntoon saattaminen kiintolevyrikon jälkeen. Toipumissuunnitelmia pitää myös testata, jotta ne toimisivat odotetulla tavalla oikeissa ongelmatilanteissa. (Raggad 2010, 217-218.)

Varmennus- ja palautussuunnitelma

Varmennus- ja palautussuunnitelmat liittyvät sekä jatkuvuus- että toipumissuunnitelmiin, mutta keskittyvät suurempien kokonaisuuksien sijaan tietokantoihin ja jopa yksittäisiin tiedostoihin ja niiden varmuuskopiointiin sekä palauttamiseen. Näiden suunnitelmien avulla voidaan suojautua tietoja uhkaavilta sisäisiltä sekä ulkoisilta uhkilta.

Varmennus- ja palautussuunnitelmaa laadittaessa pitää selvittää, mitä tietoja varmennetaan ja miten usein. Seuraavien asioiden selvittäminen antaa pohjatietoja suunnitelman laatimista varten.

- **Tietojen tärkeys järjestelmässä.** Tietojen tärkeysasteen määrittäminen on välttämätöntä, jotta voidaan määritellä mitä tietoja, miten usein ja miten nämä tiedot varmennetaan.
- **Tietojen muuttumistaajuus.** Kun tiedetään miten usein tiedot järjestelmässä muuttuvat, voidaan määrittää tarvittava varmennustiheys. Kaikkien tietojen varmuuskopiointi esim. päivittäin vie turhaan aikaa sekä varmennusjärjestelmän resursseja.
- **Varmennettujen tietojen säilytys.** Tiedon luottamuksellisuus, saatavuus sekä eheys luovat kriteereitä varmennettujen tietojen säilytystavoille. Näitä ovat mm. tietojen saatavuusnopeuden varmistaminen palautustilanteessa ja käytönvalvonta sekä järjestelmässä että fyysisissä tallennusmedioissa. Tulipaloihin tai muihin vastaaviin vahinkoihin voidaan parhaiten varautua säilyttämällä kopioita tiedoista toimipaikan ulkopuolella.
- **Tarvittava palautusnopeus tietojen tärkeysasteen mukaan.** Jotta kriittiset toiminnot saadaan palautettua mahdollisimman nopeasti, pitää ne nimetä ja määritellä suunnitelmassa.
- **Paras ajankohta varmennukselle.** Tietojen varmennusajankohta kannattaa ajoittaa siten, että järjestelmän kuormitus on pienimmillään.
- **Vastuuhenkilöt.** Suunnitelmassa pitää nimetä henkilöt, jotka vastaavat tietojen varmennuksesta, palautuksesta sekä näiden suunnitelmien ylläpidosta ja testauksesta.

- **Tarvittavat laitteet.** Mikäli käytössä ei vielä ole varmennusjärjestelmää tai sen kapasiteetti on riittämätön, määritellään suunnitelmaan tarvittavat laitehankinnat.

Edellä mainitut asiat auttavat suunnitelman hahmottelussa, mutta muitakin tapauskohtaisia asioita on syytä ottaa huomioon suunnitelmaa laadittaessa. (Stanek 2001, 307-308.)

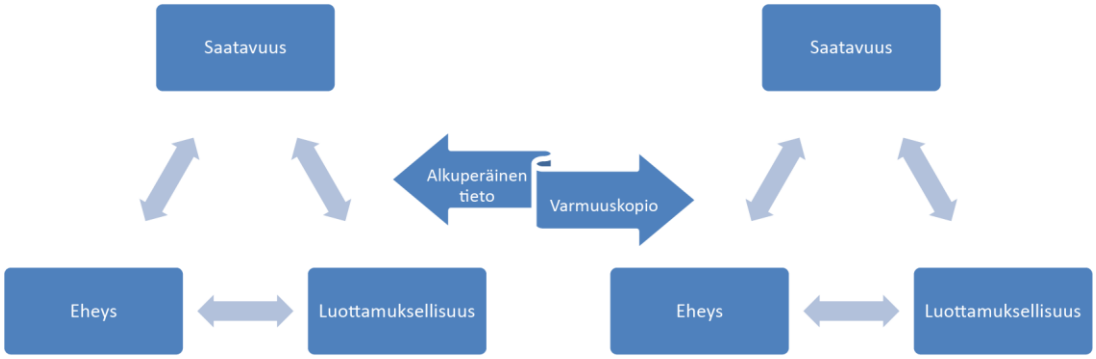
2.2 Varmuuskopiointi ja tietoturva

Varmuuskopiointi on olennainen osa tietoturvaa. Seuraavissa luvuissa käsitellään lähemmin niitä tietoturvallisuudelle asetettuja tavoitteita, jotka liittyvät lähimmin varmuuskopiointiin. (Leikomaa 2005.)

Nykyaikaisessa määrittelyssä tietoturvallisuudelle on asetettu kuusi tavoitetta:

- Luottamuksellisuus
- Eheys
- Saatavuus
- Todennus
- Pääsynvalvonta
- Kiistämättömyys.

Edellämainituista tavoitteista luottamuksellisuus, eheys sekä saatavuus ovat avainasemassa varmennusjärjestelmää toteutettaessa. Näiden tavoitteiden tulisi täyttyä alkuperäisessä ja varmuuskopioidussa tiedossa sekä niiden välillä kuvion 1 mukaisesti.



Kuvio 1. Varmennusjärjestelmän tavoitteet.

Nämä tavoitteet on esitelty tarkemmin seuraavissa luvuissa. (Järvinen 2002, 22-28.)

Luottamuksellisuus

Tiedon luottamuksellisuudella tarkoitetaan sitä, että tiedot ovat ainoastaan siihen oikeutettujen nähtävillä, luettavissa ja muokattavissa. Tieto suojataan asiatonta paljastamista vastaan. Luottamuksellisuutta tukevat mm. salaus- sekä pääsynvalvontamenetelmät. Luottamuksellisuus liittyykin tiedon tai resurssien salaamiseen ja/tai piilottamiseen.

Mikäli varmuuskopioiden luottamuksellisuus on kärsinyt, voidaan olettaa myös niiden eheyden kärsineen. Ongelmat luottamuksellisuuteen liittyen saattavat näin ollen tehdä varmuuskopioista käyttökelvottomia riippuen hieman varmuuskopioidun tiedon luonteesta. Näihin ongelmiin voidaan vastata salaamalla otetut varmuuskopiot ohjelmallisesti sekä säilyttämällä ne esim. kassakaapissa, jonka yhdistelmän tietävät vain ne, joilla on käyttöoikeus ko. resursseihin. (Virmajoki 2011.)

Saatavuus

Saatavuudella tarkoitetaan kykyä käyttää tietoa sekä resursseja silloin, kun niitä tarvitaan. Saatavuuteen liittyy myös käyttöoikeuksien rajoittaminen siten, että tieto on vain siihen oikeutettujen ihmisten käytettävissä. Toisin sanoen tieto ja siihen liittyvät resurssit suojataan asiatonta käyttöä vastaan.

Saatavuudella on suuri merkitys varmennusjärjestelmän toimivuuden kannalta. Jotta ongelmatilanteesta toipuminen olisi tehokasta, pitää varmuuskopioiden olla käytettävissä mahdollisimman nopeasti. Tämä edellyttää osaltaan myös sitä, että nopeasti saatavilla tulee olla henkilö, jolla on käyttöoikeudet em. resursseihin. (Virmajoki 2011.)

Eheys

Eheydellä tarkoitetaan sitä, että tieto on alkuperäistä, täydellistä ja muuttamatonta. Tieto ja siihen liittyvät resurssit suojataan asiatonta muuttamista tai poistamista vastaan.

Varmuuskopioiden eheyden varmistaminen ja sen säilyttäminen on niiden palauttamisen vuoksi erittäin tärkeää. Mikäli varmuuskopioiden eheys on kärsinyt, saattaa se johtaa tietojen palautuksen epäonnistumiseen ja näin ollen myös koko järjestelmän toimimattomuuteen. (Virmajoki 2011.)

2.3 Tiedon migraatio

Tiedon migraatiolla tarkoitetaan tiedon siirtämistä järjestelmästä tai formaatista toiseen. Yleensä syy siirrolle on järjestelmän tai formaatin vanheneminen, jolloin tiedot siirretään uuteen järjestelmään. Tiedon migraatio liittyy siis sekä saatavuuteen että eheyteen.

Migraatio on syytä toteuttaa hyvissä ajoin ennen laitteisto- tai ohjelmistotuen loppumista, jotta edellä mainitut saatavuus ja eheys eivät joudu missään vaiheessa vaaraan. Ennen migraation toteuttamista suoritetaan yleensä ns. tiedon puhdistus, joka koostuu useista eri toiminnoista. Näitä toimintoja ovat mm. tiedon yhtenäistämisen, duplikaattien poisto sekä vanhentuneen tiedon poisto järjestelmästä.

Varmuuskopioita voidaan joutua siirtämään uusiin järjestelmiin tai formaatteihin, mikäli tallennusmedioiden saatavuus on huonoa tai niiden koko ei riitä varmuuskopioiden tekemiseen. Tiedon siirto uudemmille tallennusmedioille on myös ajankohtaista, mikäli tietoa on säilötty vanhentuneille medioille, esim. magneettinauhoille tai ”korpuille”. (Datpro Oy 2011.)

3 VARMUUSKOPIOINTITAVAT

Varmuuskopiointitapoja on useita ja niillä on omat vahvuutensa sekä heikkoutensa. Tämän vuoksi hyvässä varmuuskopiointijärjestelmässä käytetään useamman menetelmän yhdistelmää, jolloin järjestelmän turvallisuus ja tehokkuus saadaan optimoitua. (Stanek 2001. 308-309.)

Seuraavissa luvuissa tutustutaan lähemmin paikalliseen ja etävarmuuskopiointiin sekä eri varmuuskopiointitapoihin.

3.1 Paikallinen varmuuskopiointi

Paikallisena varmuuskopiointina voidaan pitää kaikkea tiedonvarmennusta, jossa varmennettu tieto säilytetään fyysisesti samassa tilassa kuin lähdetieto. Tämäntyyppisen varmuuskopioinnin huonona ominaisuutena on herkkyys mm. tulipaloille, vesivahingoille, lähiverkossa leviäville haittaohjelmille tai virransyötön ongelmista johtuville laitteistovioille.

Hyvinä ominaisuuksina voidaan pitää kopiointijärjestelmän käytön helppoutta sekä yleensä huomattavasti nopeampaa kopiointiaikaa kuin esim. pilvipalveluun tai lähiverkon ulkopuoliselle palvelimelle tehtävässä etävarmuuskopioinnissa. Paikallisia varmuuskopiointimedioita ovat mm. ulkoiset kiintolevyt, optiset levyt sekä paikalliset tiedostopalvelimet. (Stanek 2001. 307-309.)

3.2 Etävarmuuskopiointi

Etävarmuuskopioinnissa varmennettu tieto siirretään toimipaikan ulkopuolelle siten, että tiedon tallennusmedia ei sijaitse fyysisesti samassa paikassa lähdetiedon kanssa.

Yrityksissä tieto siirretään useimmiten yrityksen omalle palvelimelle, joka ei sijaitse samassa toimipaikassa. Mikäli toimipaikkoja on useampia, voidaan tiedot kopioida hajautetusti ja ristiin eri toimipaikkojen kesken. Tällainen varmuuskopiointi ei kuitenkaan poista paikallisen varmuuskopioinnin tarvetta, sillä esim. hait-

taohjelmat saattavat päästä leviämään yrityksen verkon kautta kaikkien toimipisteiden palvelimille. (Stanek 2001. 307-309.)

Toinen vaihtoehto etävarmuuskopioinnille ovat ns. pilvitallennuspalvelut, joissa tieto siirretään ulkopuolisen palveluntarjoajan palvelimille. Tällaisen palvelun etuna on etävarmuuskopioiden siirtyminen kauemmas toimipaikasta, jopa kokonaan toiselle mantereelle. Tällöin paikalliset ongelmatilanteet eivät pääse vaikuttamaan varmuuskopioiden säilymiseen. Tiedot ovat myös saatavilla lähes missä tahansa, kunhan käytössä on toimiva Internet-yhteys.

Tätä tallennustapaa voidaan käyttää myös henkilökohtaisessa tiedonvarmennuksessa, mutta verkon nopeus nousevaan suuntaan on usein alimitoitettu, mikäli varmuuskopioitava tietomäärä on suuri. Pilvipalveluihin liittyy myös riskejä, sillä tieto siirretään kolmannen osapuolen haltuun. Tämän vuoksi kaikki pilvipalveluihin siirrettävä tieto pitäisi suojata vahvalla salausalgoritmilla, jotta sen päätyminen vääriin käsiin pystyttäisiin minimoimaan. On myös mahdollista, että palveluntarjoaja päätyy konkurssiin, jolloin tiedot saattavat hävitä kokonaan. (Vähimaa 2010.)

Ongelmaksi pilvitallennuspalvelun käytölle saattaa muodostua myös tallennettavan tiedon sisältö. Mikäli tieto sisältää esim. henkilötietoja sisältävän asiakasrekisterin, pitää näiden osalta toimia henkilötietolain säännösten mukaisesti. Henkilötietoja voidaan siirtää EU:n toiseen jäsenvaltioon tai Euroopan talousalueen sisällä melko vapaasti samoilla perusteilla kuin niitä voidaan Suomessakin luovuttaa tai antaa käsiteltäviksi. Tässäkin tapauksessa rekisterinpitäjän on varmistettava, että vastaanottaja noudattaa tarpeellisilta osin kansallisia tietosuojasäännöksiä. Tiedon siirrossa on myös huomioitava kansallisen lainsäädännön salassapitosäännökset, eli tieto on suojattava siirron aikana.

EU-alueen ulkopuolelle henkilötietoja voidaan siirtää vain, mikäli komissio on henkilötietodirektiivin mukaisesti todennut, että kohdemaassa taataan tietosuojan riittävä taso. Tämän lisäksi siirron tulee täyttää henkilötietolaissa määritellyt, EU-alueen ulkopuolelle tapahtuvaa siirtoa koskevat edellytykset. Suurimmaksi ongelmaksi näissä tapauksissa nousee pilvitallennuspalveluiden luon-

ne, eli yleensä ei voida tietää missä maassa tallennuspalvelin sijaitsee. Tämän lisäksi tiedosta säilytetään yleensä useita kopioita eri palvelimilla, jotka saattavat sijaita eri maissa. (Tietosuojavaltuutetun toimisto 2010.)

Mikäli riittävän nopeaa verkkoa pilvitallennuspalvelun käyttämiseksi ei ole käytettävissä, voidaan varmuuskopiointi toteuttaa myös paikallisesti, mutta tallennusmedia siirretään säilytettäväksi kopioinnin jälkeen toimipaikan ulkopuolelle. Tämä on usein helpoin tapa toteuttaa etävarmuuskopiointi henkilökohtaisessa tiedonvarmennuksessa. Tallennusmedia voidaan toimittaa esim. pankin tallelokeroon varmuuskopioinnin jälkeen.

3.3 Täydellinen varmuuskopiointi

Täydelliseen varmuuskopioon kopioidaan kaikki valitut tiedostot. Varmuuskopiosarjaa luotaessa suoritetaan ensimmäisenä täydellinen varmuuskopiointi, minkä jälkeen voidaan käyttää seuraavissa luvuissa esitettyjä tekniikoita kopioinnin nopeuttamiseksi ja tilantarpeen pienentämiseksi.

Tietojen palauttamiseen täydellisestä varmuuskopiosta tarvitaan vain viimeisin varmuuskopiosukupolvi, mutta menetelmän huonona puolena on suuri tilantarve sekä suuren tietomäärän kopioinnin aiheuttama pitkä varmuuskopiointiaika. Tiedosta kannattaa kuitenkin luoda ja säilyttää useampia täydellisiä varmuuskopioita, vaikka muita tekniikoita käytettäisiinkin niiden välillä. (Secmeter 2008.)

3.4 Lisäävä varmuuskopiointi

Lisäävä eli inkrementaalinen varmuuskopiointi kopioi kaikki viimeisen täydellisen tai lisäävän varmuuskopion jälkeen luodut tai muutetut tiedostot. Tietoja palautettaessa tarvitaan viimeisin täydellinen varmuuskopio sekä kaikki sen jälkeen luodut lisäävät varmuuskopiot.

Lisäävän ja täydellisen varmuuskopioinnin yhdistetty käyttö on usein nopein tapa suorittaa varmuuskopiointi, mutta tietojen palautus on melko hidasta, koska se pitää suorittaa yleensä useasta eri lähteestä. (Secmeter 2008.)

3.5 Eroavuusvarmuuskopiointi

Eroavuusvarmuuskopioinnissa kopioidaan kaikki viimeisen täyden varmennuksen jälkeen luodut tai muokatut tiedostot. Mikäli edellisestä täydellisestä varmennuksesta on kulunut aikaa, saattaa tällä menetelmällä luotu varmuuskopio kasvaa kooltaan melko suureksi.

Tietoja palautettaessa tarvitaan vain viimeisin täydellinen varmuuskopio sekä viimeisin eroavuusvarmuuskopio. (Secmeter 2008.)

4 VARMUUSKOPIOINTILAITTEET JA –MEDIAT

Erot varmuuskopiointiin käytettävissä olevien laitteiden sekä tallennusmedioiden välillä ovat suuria niin luotettavuuden kuin aloitus- ja käyttökustannustenkin puolesta. Seuraavissa luvuissa käsitellään yleisimmät kotikäyttäjälle soveltuvat varmuuskopiointilaitteet sekä -mediat ja niiden vahvuudet ja heikkoudet. Varsinkin järjestelmien heikkoudet on hyvä tietää ja sisäistää ennen varmennusjärjestelmän toteutusta, jotta virhehankinnoilta vältyttäisiin. (Stanek 2001. 310-311.)

4.1 Varmuuskopiointijärjestelmän valinta

Ennen järjestelmän valintaa ja toteutusta on hyvä arvioida omia tarpeitaan koskien varmuuskopiointia. Mikäli arviointia ei suoriteta, saattaa esim. järjestelmän tallennuskapasiteetti olla liian pieni tarvittavien varmuuskopioiden ottamiseen.

Ainakin seuraavat asiat tulee ottaa mukaan arvioon:

- kapasiteetti
- luotettavuus
- skaalautuvuus
- nopeus
- hinta.

Arviota tehdessä tulee myös ottaa huomioon, että varmuuskopioista pitäisi säilyttää useampia sukupolvia. Tämä moninkertaistaa varmuuskopiointijärjestelmän tilantarpeen verrattuna alkuperäiseen tiedon määrään. (Stanek 2001. 310-311.)

4.2 Mediat

Seuraavissa luvuissa käsitellään yleisimmät mediatyypit, joita voidaan käyttää varmuuskopioiden säilytykseen sekä niiden vahvuuksia ja heikkouksia.

Optiset levyt

Optisilla levyillä tarkoitetaan tässä CD-, DVD- sekä BluRay-levyjä sekä niiden eri variaatioita (-R, +R, RW). Vaikka optiset levyt ovat viime vuosina menettäneet suosiotaan tallennusmediatyyppinä, on levyjen saatavuus vielä melko hyvällä tasolla. Optisten levyjen käyttö on vähentynyt, koska levyjen hinta–kokosuhde verrattuna esim. kiintolevyihin on huono ja niiden tallennustilan koko on jäänyt liian pieneksi datamäärien ja tiedostokokojen kasvaessa.

Levyjen kirjoitus- ja lukuluotettavuuden kanssa on myös havaittu ongelmia, varsinkin halvempien aihioiden kanssa. Yleisimpiä ongelman aiheuttajia ovat levyjen fyysiset vauriot, esim. naarmut. Ongelmat saattavat myös olla seurausta joko aihioiden ja kirjoittavien asemien epäyhteensopivuudesta tai liian suuresta kirjoitusnopeudesta levyä luotaessa, jonka seurauksena datan eheys kärsii. Myös levyjen pitkäaikainen säilytys saattaa muuttaa levyn rakennetta siten, että siitä tulee lukukelvoton. Vastauksena näihin ongelmiin on kehitetty suurempikapasiteettisia ja luotettavampia levytyyppejä (esim. BluRay). Näiden levytyyppien yleistyminen on ollut hidasta ja varsinaista läpilyöntiä ei välttämättä koskaan tule tapahtumaan, koska optisten levyjen käyttöä pidetään nykyään melko kömpelönä tapana tallentaa tietoa.

Edellä mainittujen luotettavuusongelmien vuoksi varmuuskopiointiin ei kannata käyttää muita kuin hyvälaatuisia levyjä. Varmuuskopioita sisältävien levyjen luettavuus kannattaa myös tarkastaa aika-ajoin ja mikäli lukuongelmia alkaa esiintyä, on syytä suorittaa varmuuskopioiden migraatio joko uusille levyille tai kokonaan toisenlaiselle medialle. Optiset levyt sopivatkin lähinnä satunnaiseen varmuuskopiointiin silloin, kun varmennettavan tiedon määrä ei ole kovin suuri. (Suutari 2011.)

Nauha-asemat

Perinteiset nauha-asemat perustuvat magneettinauhakasetteihin, jotka edullisuutensa sekä melko suuren kapasiteettinsa vuoksi olivat vielä 90-luvulla käyttökelpoisia datan tallennusvaihtoehtoja myös kotikäyttäjien parissa. Huonona puolena on, että magneettinauhojen luotettavuus on vain kohtalainen. Nauhat saattavat venyä tai pahimmassa tapauksessa katketa, jolloin nauhan sisältökin on pilalla.

Nykyään nauha-asemia käytetään pääasiassa yrityksissä, mutta tekniikka on muuttunut digitaaliseksi (DAT), väylä on muuttunut SCSI-väylästä SAS-väylään ja nauhojen kapasiteetti on kasvanut siten, että yhden nauhan tallennustila voi olla nykyään 1,6 teratavua. Kasvaneen tilantarpeen vuoksi on yrityksissä usein siirrytty käyttämään ns. nauharobotteja, jotka pitävät sisällään useita tallennusnauhoja ja vaihtavat niitä tarvittaessa. Näiden ominaisuusmuutosten myötä nauhavarmennusjärjestelmien hinta on noussut siten, että niitä ei voida pitää enää järkevänä vaihtoehtona kotikäyttäjälle. (Stanek 2001. 310-311.)

Flash-muistit

Flash-muisteihin voidaan lukea erilaiset muistitikut, muistikortit, SSD-levyt sekä laitteisiin integroidut tiedon tallennukseen tarkoitetut muistipiirit (kuva 1). Näille muistipiireille voidaan kirjoittaa tietoa ja se voidaan myös poistaa ja uudelleenkirjoittaa. Flash-muisti on suunniteltu siten, että se säilyttää tiedon useiden vuosien ajan vaikka virta kytketään pois.

Flash-muisteihin perustuvissa tallennuslaitteissa ei ole liikkuvia mekaanisia osia, joka parantaa niiden luotettavuutta verrattuna esim. perinteisiin kiintolevyihin. Vaikka laitteiden mekaaninen luotettavuus on parempi verrattuna kiintolevyihin, on muistipiirien elinikä kuitenkin rajallinen. Ajan myötä muistipiirissä olevia muistisoluja vioittuu ja ne poistetaan käytöstä ja korvataan ohjaamalla data varalla oleville muistisoluille. Kun kaikki varalla olleet muistisolut on otettu käyttöön, pitää laite lopulta vaihtaa uuteen.

Kuva 1. Flash-tekniikkaan perustuvia tallennuslaitteita.

Flash-tekniikkaan perustuvat laitteet ovat käytössä täysin hiljaisia ja niiden lämmöntuotanto on kiintolevyihin verrattuna hyvin pientä. Muihin hyviin ominaisuuksiin voidaan lukea muistipiirien verrattain pieni koko sekä keveys, joka mahdollistaa flash-muistien käyttämisen esim. matkapuhelimissa ja muissa kannettavissa laitteissa. Vaikka muistipiirien kapasiteetti kasvaa ja hinta alenee jatkuvasti lisääntyneen kysynnän seurauksena, eivät ne vielä sovellu laajamittaisempaan varmuuskopiointiin verrattain huonon hinta–koko-suhteensa vuoksi. (Kay 2010.)

Kiintolevyt

Kiintolevyt ovat vielä nykyisin yleisimpiä massamuistilaitteita. Kapasiteettinsa, nopeutensa sekä hintansa puolesta ne ovat paras vaihtoehto suurempien tietomäärien tallentamiseen yksityiskäytössä. Kiintolevyt ovat monipuolisia tallennuslaitteita ja niitä on mahdollista yhdistää suuremmiksi levyjärjestelmiksi mikäli yksittäisten levyjen kapasiteetti tai luotettavuus ei käyttötarkoitukseen nähden ole riittävällä tasolla. Saatavilla on myös useita liitäntävaihtoehtoja, jotka mahdollistavat kiintolevyjen sovittamisen eri käyttötarkoituksiin. Levy voidaan liittää

tietokoneen sisäisiin liittimiin (ATA, SATA, SCSI, SAS) tai se voidaan asentaa ulkoiseen kiintolevykoteloon, jolloin liitäntätapa on yleensä USB, FireWire, eSATA tai Thunderbolt. Kiintolevy voidaan myös asentaa verkkoliitäntäiseen NAS-asemaan, jolloin levyn tallennuskapasiteetti saadaan kaikkien lähiverkon koneiden käyttöön.

Kiintolevyjen fyysinen koko vaihtelee kannettaviin tietokoneisiin sekä pienikokoisiin ulkoisiin kiintolevyihin tarkoitetuista ns.1,8”- sekä 2,5”-levyistä pöytäkoneisiin suunnattuihin ns. 3,5”-levyihin. Niiden kapasiteetit vaihtelevat muutamasta kymmenestä gigatavusta neljään teratavuun. Muita muuttuvia ominaisuuksia ovat kierrosnopeus (5400-15000 rpm) sekä levyn sisältämä välimuistin määrä.

Tieto tallennetaan levystä riippuen yhdelle tai useammalle pyörivälle, ei-magneettisesta materiaalista tehdylle levylle (platter), joka on päällystetty 10-20 nanometrin paksuisella kerroksella magneettista materiaalia. Levyt on jaettu samankeskeisiin ympyröihin eli uriin (track). Jokainen ura on jaettu edelleen sektoreihin, joihin informaatio tallennetaan. Levyn kirjoituspää tallentaa tiedon koodatussa binäärimuodossa muuttamalla levyn pinnalla olevien magneettisten alueiden magnetisoinnin suuntaa. Nämä muutokset edustavat bittejä. Levyltä luettaessa lukupää tulkitsee nämä muutokset magneettisissa alueissa ja ne muunnetaan jälleen tietokoneen ymmärtämään muotoon.

Kiintolevyt ovat mekaanisia laitteita ja vaikka luotettavuus onkin saatu verrattain hyvälle tasolle, on niiden hajoaminen silti edessä ennemmin tai myöhemmin. Mikäli levyssä on valmistusvika tai sitä käytetään vääränlaisissa olosuhteissa, saattavat kiintolevyt hajota hyvinkin nopeasti. Ne eivät siis poista varmuuskopioinnin tarvetta, mutta edullisuutensa vuoksi niitä voidaan käyttää useamman levyn RAID-järjestelmissä, jolloin tiedon päällekkäisyyttä voidaan lisätä ja näin ollen varautua myös levyjen rikkoutumista vastaan. (Hard disk drive 2012.)

NAS-järjestelmät

NAS eli Network Attached Storage tarkoittaa verkkoon liitettyä tallennuslaitetta. Tarkoituksena on saada lähiverkkoon helposti hallinnoitava ja luotettava tallennustila, joka on käytettävissä kaikilta verkkoon kytketyiltä koneilta niiden käyttöjärjestelmästä huolimatta. Näin tiedosta ei tarvitse säilyttää useita päällekkäisiä kopioita eri koneilla. Kotikäyttäjille NAS-laitteita markkinoidaan usein keskitettynä tallennusvälineenä ja mediapalvelimena esim. valokuville sekä musiikki- ja videotiedostoille.

Yksinkertaisimmillaan NAS voi olla melko edullinen ulkoinen kiintolevykehikko, jossa on verkkoliitäntä. Keskihintaiset laitteet tukevat yleensä kahta tai useampaa kiintolevyä sekä RAID-järjestelmiä tai valmistajan itsensä kehittämiä teknologioita levyjen rikkoutumisen varalle. Kalliimman hintaluokan laitteisiin on myös lisätty palvelinominaisuuksia, kuten tuki DLNA-, FTP-, BitTorrent- sekä varmuuskopiointitekniikoille. Näissä laitteissa on myös usein kaksi verkkoliitintä sekä USB-liittimiä, joiden avulla on esim. mahdollista jakaa tulostin lähiverkon käyttöön tai laajentaa tallennustilaa liittämällä ulkoinen USB-kiintolevy laitteeseen.

Laitteiden käyttöjärjestelmät ovat usein juuri niille räätälöityjä, kevyitä ohjelmistoja ja niiden hallinnointi tapahtuu normaalisti verkkokäyttöliittymän avulla asiakaskoneelta. NAS-laitteiden hallinnointiin ei siis tarvita monitoria, näppäimistöä eikä hiirtä erikseen. Perinteisiin tiedostopalvelimiin verrattuna näiden laitteiden tarkoituksena on siis olla hankinta- ja ylläpitokustannuksiltaan edullisempia sekä yksinkertaisia asentaa ja käyttää. Riippuen kuitenkin laitteen ominaisuuksista saattaa hinta nousta tuhansiin euroihin. Mikäli erillistä NAS-laitetta ei haluta hankkia, on nykyisin mahdollista valjastaa vaikkapa hieman vanhempi tietokone tähän käyttötarkoitukseen. Saatavilla on useita Linux-pohjaisia käyttöjärjestelmiä, jotka tarjoavat samat ominaisuudet kuin NAS-laitteetkin, usein jopa ominaisuuksia, joita ei kaupallisista laitteista löydy.

Varmuuskopioinnin kannalta NAS-laitteet ovat erittäin käytännöllisiä, varsinkin jos käytössä on laite, jossa on useampi kiintolevy sekä RAID- tai vastaava jär-

jestelmä, jolloin varmuuskopiot ovat paremmassa turvassa levyrikkoja vastaan. NAS-laitteet pidetään usein jatkuvasti päällä, joten varmuuskopiot voidaan helposti toteuttaa yöllä, jolloin koneet eivät ole käytössä ja verkon kuormitus on pienimmillään. (Mitchell 2012.)

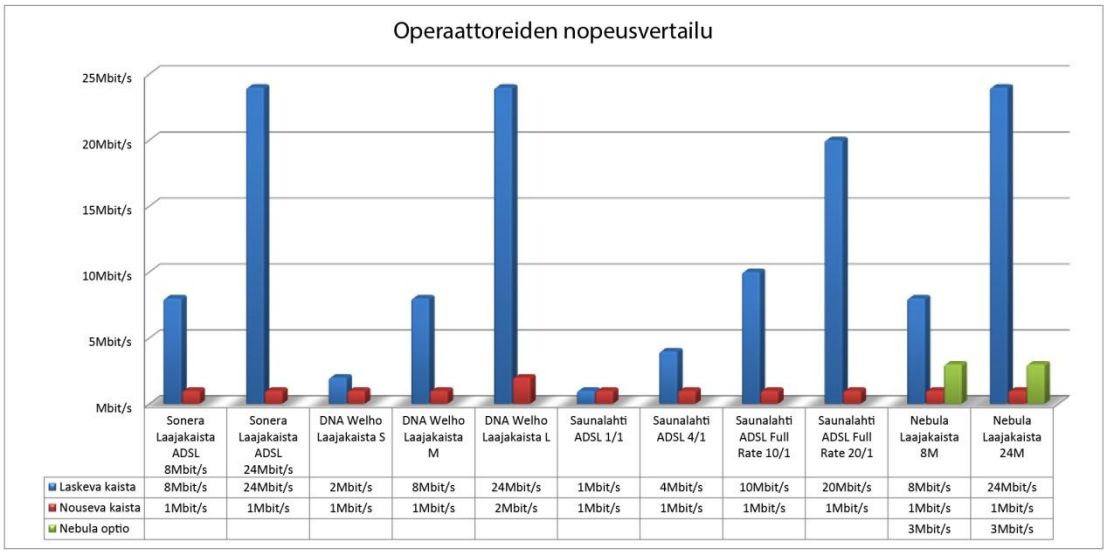
SAN-järjestelmät

Lyhenne SAN tulee sanoista Storage Area Network, joka suomennetaan yleensä muotoon tallennusverkko. SAN on oma erillinen verkkoratkaisunsa, jonka tarkoitus on yhdistää käytössä olevat levyjärjestelmät yhtenäiseksi verkkotallennustilaksi ja siirtää tiedontallennukseen tarvittava liikenne erilleen muusta verkkoliikenteestä.

SANiin voidaan liittää mm. kiintolevyjä, levyjärjestelmiä, optisia tallennuslaitteita sekä nauha-asemia. Koska tarkoituksena on siirtää tietoa mahdollisimman nopeasti, toteutetaan järjestelmä yleensä kuitukanavaprotokollan avulla. Toteutustapa mahdollistaa 10 Gbps:n nopeuden sekä pitkät, jopa 10 km etäisyydet verkkoa rakennettaessa. Tämäntyyppisiä järjestelmiä käytetään lähinnä keskitettynä tietovarastona suurten tietomäärien käsittelyssä. (Moilanen 2004.)

Pilvitallennuspalvelut

Pilvitallennuspalvelun eli kolmannen osapuolen palveluntarjoajan palvelimella sijaitsevan tallennustilan yksityiskäyttö on haasteellista, varsinkin mikäli palveluun siirrettävä tietomäärä on suuri. Suomessa yleisesti käytössä olevat ADSL -liittymät tarjoavat yleensä niin rajallisen nousevan kaistan, että suuremman tietomäärän kopiointi saattaa kestää useita päiviä tai jopa viikkoja.



Kuvio 2. Operaattoreiden nopeusvertailu kevät 2012.

Kuviossa 2 on esitetty keväällä 2012 tarjolla olleiden ADSL-liittymien nopeusvertailu. Mukana vertailussa ovat suurimpien operaattoreiden tarjoamat liittymät. Ylivoimaisesti yleisin käytössä oleva nousevan kaistan nopeus on 1 Mbit/s ja ainoastaan DNA tarjoaa 2 Mbit/s nopeutta nopeimman liittymänsä kanssa. Nebula erottuu muista operaattoreista tarjoamalla maksullisena lisäpalveluna 3 Mbit/s paluukaistaa. Tarvittaessa nopeampi nouseva kaista on kuitenkin mahdollista saavuttaa useiden operaattoreiden tarjoamien kaapeli- ja valokuituliittymien avulla. Tällöin paluukaistan nopeudet vaihtelevat 2-100 Mbit/s välillä. ADSL-liittymiä haluttiin vertailla niiden hyvän saatavuuden vuoksi, sillä nopeiden kaapeli- ja valokuituliittymien saatavuus on vielä toistaiseksi melko rajoitettua ainakin kaupunkialueiden ulkopuolella.

Pilvitallennuspalveluiden muihin huonoihin puoliin voidaan lukea myös tietoturvariskit sekä palvelun mahdollinen poistuminen markkinoilta. Hyvinä puolina varmuuskopioinnin kannalta voidaan pitää tietojen tallennusta toimipaikan ulkopuolelle sekä sitä, että tiedostot ovat käytettävissä missä tahansa ja että tarvittaessa tiedot voidaan synkronoida automaattisesti kaikille käytössä oleville koneille. (Vähimaa 2010.)

5 RAID-JÄRJESTELMÄT

RAID on lyhenne sanoista Redundant Array of Independent Disks, mutta joskus näkee myös käytettävän vanhempaa nimitystä, Redundant Array of Inexpensive Disks. Järjestelmän kehitystyö sai alkunsa tallennettavan tiedon määrän lähdettyä voimakkaaseen nousuun yrityksissä 1980-luvun loppupuolella. Tavoitteena oli alkuperäisen nimityksen mukaan rakentaa levyjärjestelmä useista pienempikapasiteettisista kiintolevyistä, jotka luonnollisesti olivat edullisempia verrattuina suurempiin levyihin. Sana ”inexpensive” (edullinen) vaihtui kuitenkin sanaan ”independent” (itsenäinen, yksittäinen), koska huomattiin, että RAID-järjestelmät olivat lopulta erittäin kalliita. Hankinta- ja ylläpitokulut rajasivatkin RAID-järjestelmät alkuvaiheessa lähes yksinomaan yrityskäyttöön.

Projektin alkuperäisenä tavoitteena oli levyjärjestelmän suorituskyvyn parantaminen verrattuna yksittäisiin levyihin, mutta melko pian havaittiin mahdollisuudet lisätä myös sen luotettavuutta käyttämällä pariteetti-informaatiota. RAID-järjestelmän tarkoituksena on siis rakentaa kustannustehokas ja skaalautuva tallennusratkaisu, jossa voidaan painottaa vikasietoisuutta, suorituskykyä tai tietyin rajoituksin molempia. (Hayes 2003.)

RAID-järjestelmät eivät siis ole aiemmin päässeet yleistymään kuluttajalaitteissa kalleutensa vuoksi. Viime vuosina tämä tilanne on kuitenkin muuttunut kiintolevyjen hinnanlaskun, ohjelmistopohjaisten RAID-järjestelmien kehityksen sekä emolevyihin integroitujen, yleisimmät RAID-tasot osaavien kiintolevyohjaimien yleistymisen myötä. Nykyisin lähes kaikista emolevyistä löytyy RAID-tasoja tukeva levyohjain ja useimmat käyttöjärjestelmät sisältävät mahdollisuuden RAID-järjestelmän toteuttamiseen ohjelmallisesti.

RAID-järjestelmiä ei voida eikä niitä tule pitää varmuuskopiointimenetelmänä, mutta niiden avulla voidaan lisätä tietojen päällekkäisyyttä (redundanssia). Riippuen toteutetun järjestelmän tyypistä voidaan tällöin suojautua yhden tai useamman kiintolevyn rikkoutumiselta siten, että tiedot säilyvät tallessa ja ne pystytään palauttamaan rikkoutuneen kiintolevyn vaihdon jälkeen. (Kyrnin 2012.)

5.1 RAID-ohjaimet

Kiintolevyjen lisäksi RAID-järjestelmä tarvitsee ohjaimen. Ohjaimen tehtävänä on jakaa tieto oikealla tavalla käytetylle levyjärjestelmälle sekä suorittaa pariteettidataan liittyvät laskutoiminnot. Ohjain myös hallitsee kiintolevyjä siten, että kun levy hajoaa, ohjain tekee levyrikosta ilmoituksen sähköpostitse järjestelmänvalvojalle. Riippuen hieman järjestelmästä voidaan siihen myös liittää varalevyjä (hot spare), jolloin ohjain poistaa hajonneen levyn järjestelmästä ja ottaa automaattisesti uuden levyn käyttöön. Tämän jälkeen hajonneen levyn sisältö generoidaan uudelle levylle käyttäen muiden levyjen sisältämää pariteettiinformaatiota. Mikäli järjestelmässä ei ole varalevyjä, pitää rikkoutunut levy vaihtaa manuaalisesti, jotta korjausprosessi voidaan aloittaa.

RAID-ohjain voidaan toteuttaa täysin ohjelmallisesti käyttöjärjestelmässä tai laitteistotasolla erillisen ohjainkortin avulla. RAID-ohjaimet jaetaankin usein ominaisuuksiensa puolesta kahteen eri ryhmään, ohjelmisto- ja laitteistotasolla toimiviin ohjaimiin. (Viitanen 2004.)

Ohjelmistotason RAID-ohjaimet

Ohjelmistotason RAID-ohjaimiin voidaan lukea kaikki ohjelmallisesti toteutettavat ratkaisut, emolevylle integroidut RAID-levyohjaimet sekä erilliset ohjainkortit, joissa ei ole omaa suoritinta tai muistia pariteettidatan laskemiseksi. Pariteettidatan laskentaan käytetään näissä tapauksissa koneen omaa prosessoria sekä muistia, joka yleensä hidastaa jonkin verran levyjen luku- ja kirjoitustoimintoja. (Viitanen 2004.)

Ohjelmallisesti toteutettavien RAID-järjestelmien hyviin puoliin lukeutuvat yksinkertaisuus sekä edulliset aloituskustannukset koska erillistä ohjainkorttia ei tarvitse hankkia ja tarvittava ohjelmisto on yleensä integroitu käyttöjärjestelmään. Omalla tavallaan myös laitteistoriippumattomuus voidaan lukea näiden järjestelmien eduksi, sillä hajonnut RAID-ohjainkortti pitää yleensä korvata toisella samanlaisella tai saman ohjainpiirin sisältävällä kortilla, jotta levyjärjestelmä voidaan ottaa uudelleen käyttöön. Ongelmaksi tämä saattaa muodostua kustannusten ja jo markkinoilta poistuneiden ohjaimien kohdalla.

Aiemmin ohjelmalliset RAID-ratkaisut eivät pystyneet kilpailemaan nopeudeltaan tai ominaisuuksiltaan erillisten RAID-ohjainkorttien kanssa, mutta nykyiset prosessorit ovat kuitenkin niin tehokkaita, että ohjelmisto-RAID on noussut varteenotettavaksi vaihtoehdoksi jopa yrityskäytössä. RAID-tasojen tuki on lähes samalla tasolla lukuun ottamatta muutamia eksoottisempia vaihtoehtoja ja esim. Linuxin MD-RAID tukee mm. varalevyjä sekä levyjen vaihtoa järjestelmän ollessa käynnissä mikäli se on mahdollista laitteiston osalta. (Gite 2009.)

Laitteistotason RAID-ohjaimet

Laitteistotason RAID-ohjainkortit eroavat toiminnallisuudeltaan muista toteutustavoista siten, että korteissa on omaa muistia ja suoritin pariteettidatan laskemista varten. Näissä ohjaimissa tarvitut laskutoiminnot tehdään siis laitetasolla, jolloin ne eivät rasita palvelimen omia resursseja ja yleisesti ottaen järjestelmän luku- ja kirjoitusnopeudet ovat ohjelmallisia järjestelmiä nopeampia. (Viitanen 2004.)

Nykyaikaiset ohjaimet tukevat lähes poikkeuksetta palvelinkäytössä yleisiä SAS-levyjä, joita ei muutamaa poikkeusta lukuun ottamatta pystytä liittämään kuluttajaluokan emolevyihin. Ohjaimissa käytetään nykyisin sisäisiä sekä ulkoisia mini-SAS-liittimiä, joihin voidaan liittää sekä SAS- että SATA-väyläisiä laitteita. Yksi liitin voidaan jakaa ns. Multilane SAS-kaapelilla siten, että siihen voidaan liittää neljä laitetta. Edistyneimmät ohjaimet tukevat yleensä 24 laitteen liittämistä ohjaimen omiin liittimiin, mutta ne pystyvät ohjaamaan jopa yli 200 laitetta, jotka sijaitsevat ulkoisissa levytallennuskoteloissa ja jotka on liitetty kortin ulkoisiin mini-SAS-liittimiin. Tällä tavoin pystytään rakentamaan erittäin hyvin skaalautuva tallennusjärjestelmä.

Edistyneemmissä ohjaimissa on myös usein akkuvarmennus sekä laajennettavissa oleva välimuisti, jotka takaavat tiedon eheyden sähköverkon virhetilanteidenkin aikana. Tämän tason ohjaimissa on yleensä myös mahdollisuus hallita levyjärjestelmiä verkon muilta koneilta, vaihtaa levyjä järjestelmän ollessa käynnissä (hot swap) sekä käyttää varalevyjä (hot spare), jotka ohjain ottaa automaattisesti käyttöön levyrikon jälkeen. Tällöin ohjain aloittaa automaattisesti

levyjärjestelmän korjaamisen. Mikäli varalevyä ei ole käytettävissä, pitää rikkoutunut levy vaihtaa käsin ennen kuin järjestelmä pääsee aloittamaan korjausprosessin. (Hewlett Packard 2012.)

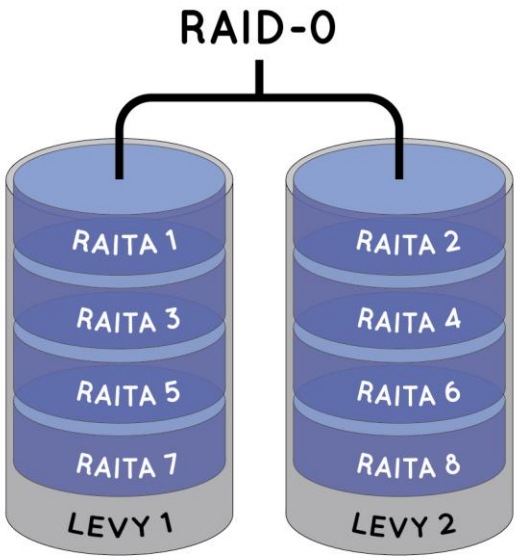
5.2 RAID-tasot

RAID-järjestelmät on jaettu seitsemään eri tasoon suunnitteluarkkitehtuurien mukaan. Näitä tasoja voidaan myös tietyissä tilanteissa yhdistää, jolloin voidaan yhdistää kahden eri tason parhaat puolet. Kaikille tasoille on kuitenkin yhteistä se, että joukkoa fyysisiä levyasemia tarkastellaan yhtenä loogisena asemana käyttöjärjestelmässä.

Seuraavissa luvuissa käsitellään yleisimmät RAID-tasot, jotka on mahdollista toteuttaa ohjelmallisesti tai erillisen ohjainkortin avulla. (Viitanen 2004.)

RAID-0 (striping)

RAID-0 on levyjärjestelmä, jossa kaksi tai useampia (max. 32kpl) kiintolevyjä yhdistetään yhdeksi loogiseksi asemaksi. Levyjärjestelmälle kirjoitettava tieto jaetaan lohkoihin ja kirjoitetaan hajautetusti sarjaan kuuluville levyille (kuvio 3). Järjestelmän hyödyt ovat nopeampi luku- ja kirjoitusnopeus, koska tietoja voidaan hakea ja kirjoittaa levyille samanaikaisesti. Tällä tavoin voidaan myös yhdistää useamman pienemmän kiintolevyn kapasiteetti siten, että se näkyy käyttöjärjestelmässä yhtenä suurena loogisena asemana.

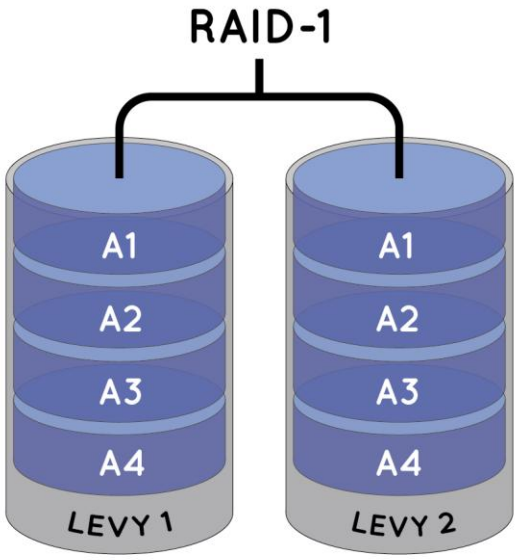


Kuvio 3. RAID-0.

Poiketen muista RAID-järjestelmistä, taso 0 ei kuitenkaan tarjoa redundanssia, eli yhden levyn rikkoutuessa menetetään koko sarjan sisältämä tieto. Tämän ominaisuuden vuoksi se ei sovellu käyttötarkoituksiin, joissa pyritään turvaamaan asemille tallennettu tieto mahdollisimman hyvin. Mikäli levyjärjestelmä menee epäkuntoon esim. kiintolevyrikon tai tiedostojärjestelmän vaurioitumisen vuoksi, pitää se luoda uudelleen ja palauttaa tiedot varmuuskopioista. (Viitanen 2004.)

RAID-1 (mirroring)

RAID-1 koostuu kahdesta tai useammasta samankokoisesta kiintolevystä, mutta useimmiten käytössä on kuitenkin vain kaksi levyä. Tämä järjestelmä ei käytä redundanssin saavuttamiseksi muiden RAID-tasojen tapaan pariteettidataa, vaan järjestelmä yksinkertaisesti monistaa (peilaa) kaiken tiedon levyjen kesken (kuvio 4). Tällöin sarjasta muodostuu redundantti tietojoukko. Kahta levyä käytettäessä tämä mahdollistaa tietojen säilymisen sekä järjestelmän toiminnan, vaikka toinen kiintolevyistä rikkoutuisi.



Kuvio 4. RAID-1.

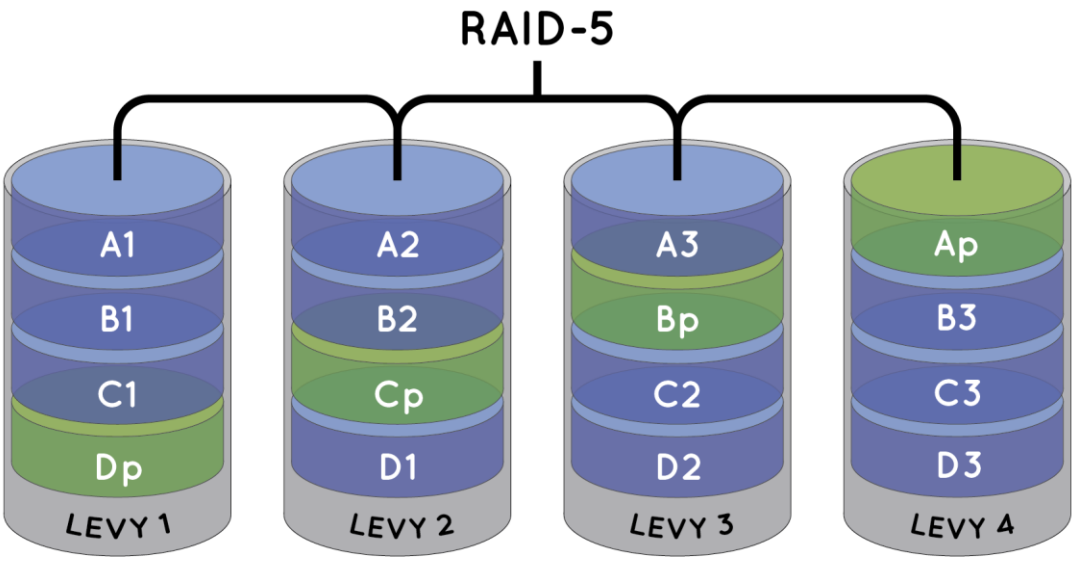
Mikäli peilaus toteutetaan ohjelmallisesti, voidaan lukunopeutta parantaa liittämällä levyt eri levyohjaimiin. Tällöin puhutaan levyjen samanaikaisesta käytöstä (disk duplexing), jolloin lukutoimintoja voidaan tehdä kummaltakin levyltä yhtä aikaa.

RAID-1 on melko yksinkertainen järjestelmä, jossa esim. kiintolevyn rikkoutumisesta toipuminen vaatii ainoastaan rikkoutuneen levyn vaihtamisen, jonka jälkeen tiedot kopioidaan ehjältä levyltä uudelle levylle. Sen etuihin kuuluu myös ,

että tarvittaessa levyt voidaan irrottaa koneesta ja käyttää niitä yksittäin toisessa koneessa esim. RAID-ohjaimen rikkoutumisen jälkeen. Haittapuoliin lukeutuvat levytilan kaksinkertainen tarve normaaliin verrattuna ja siitä johtuva kustannusten kasvu sekä tietojen peilauksesta johtuva vähäinen hidastuminen kirjoitusnopeuksissa. (Viitanen 2004.)

RAID-5

RAID-5 koostuu vähintään kolmesta samankokoisesta kiintolevystä, mutta yleensä järjestelmässä käytetään useampia levyjä. Se on samalla yleisin käytössä oleva RAID-järjestelmä jossa käytetään pariteettidataa (kuvio 5).



Kuvio 5. RAID-5.

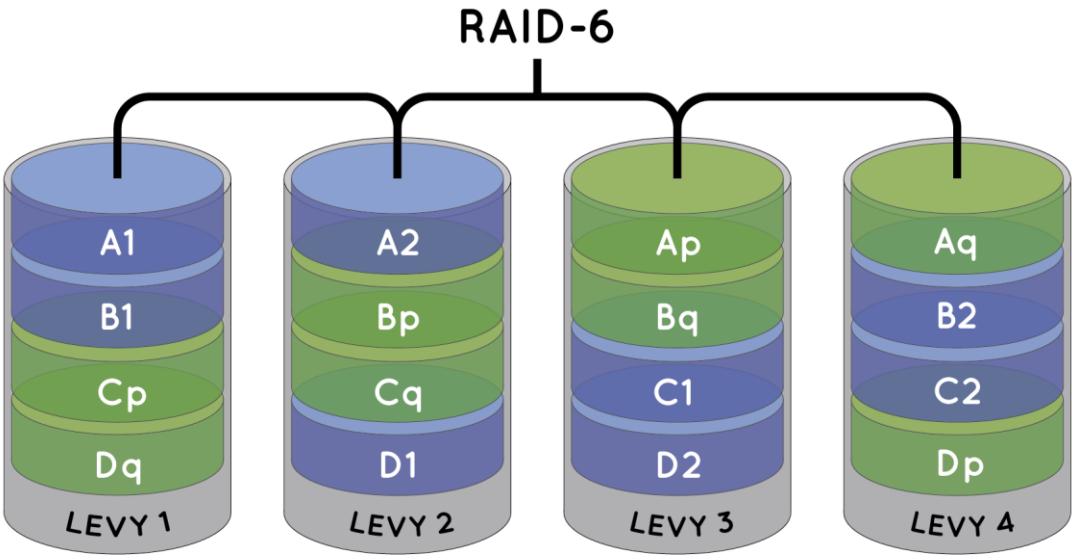
Tieto tallennetaan järjestelmän kaikille levyille lohkoittain yhdessä pariteettidatan kanssa. Tiedon tallentaminen lohkoittain nopeuttaa levyjärjestelmän toimintaa, mutta samalla ohjainkortilta tai tietokoneelta vaaditaan laskentatehoa pariteettidatan laskemiseksi. Nopeusetua ei siis normaalisti nähdä muilla kuin aidoilla RAID-ohjaimilla tai Linuxilla toteutetuilla ratkaisuilla, joissa koko kone on pyhitetty vain palvelinkäyttöön. Koska järjestelmä tallentaa pariteettidataa varsi-

naisen tiedon lisäksi, menetetään yhden levyn kokoa vastaava tila kokonaistallennuskapasiteetista.

Levyjärjestelmä kestää siis yhden levyn rikkoutumisen, joka voi olla mikä tahansa levyistä. Tämän RAID-tason ongelma on suurten kiintolevykokojen mukanaan tuoma pitkä toipumisaika, jolloin on melko todennäköistä, että toipumisaikana toinenkin kiintolevy rikkoutuu ja kaikki tieto menetetään. Ongelma korostuu, jos levyjärjestelmän kaikki levyt on ostettu samaan aikaan ja ne kuuluvat samaan kiintolevyerään. Tällöin niiden odotettu elinikä saattaa täyttyä jotakuinkin samaan aikaan. (Viitanen 2004.)

RAID-6

RAID-6 on kehitetty alkuperäisten RAID-tasojen jälkeen ja se eroaa RAID-5:stä siten, että pariteettidatan määrä on kaksinkertaistettu ja sen luomisessa käytetään kahta erillistä pariteettilaskukaavaa (kuvio 6). Näin ollen järjestelmä pystyy toipumaan kahden kiintolevyn samanaikaisesta rikkoutumisesta.



Kuvio 6. RAID-6.

Pariteettidatan lisääminen lisää myös tarvetta laskentateholle, eli kirjoitustoiminnoissa RAID-5-järjestelmät ovat yleensä nopeampia. Järjestelmän avulla voidaan kuitenkin pienentää edellä mainittua tiedon menetyksen riskiä huomattavasti, koska tietojen menetys vaatisi kaikkiaan kolmen levyn hajoamisen samanaikaisesti. (Viitanen 2004.)

6 KÄYTTÖJÄRJESTELMÄN VARMENNUS

Käyttöjärjestelmän varmennus levykuvien avulla on verrattain helppo tapa lisätä yksi turvallisuustaso puhuttaessa henkilökohtaisesta tiedonvarmennuksesta. Niin sanottujen merkkikoneiden kiintolevyltä löytyy yleensä piilotettu palautusosio tai koneen mukana tulee palautuslevy, jonka avulla koneen käyttöjärjestelmä voidaan palauttaa alkuperäiseen tilaansa. Komponenteista kasattujen koneiden kohdalla tällaista levykuvaan perustuvaa palautusmetodia ei yleensä toimiteta koneen mukana, vaikka se toisikin lisäarvoa koneen ostajalle. Sama koskee myös itse koottuja koneita, joten näissä tapauksissa levykuva on luotava itse, mikäli sellaista haluaa hyödyntää.

Kotikäytössä voidaan levykuvien avulla palauttaa käyttöjärjestelmä aikaisempaan tilaan esim. käyttäjän tai viruksen aiheuttaman ongelman jälkeen. Yleisimmät syyt käyttöjärjestelmän palautukselle ovat kuitenkin kiintolevyn rikkoutuminen sekä käyttöjärjestelmän uudelleenasennuksen tarve sen hidastuessa riittävästi. (Spector 2008.)

6.1 Levykuvien käyttö

Levykuvalla tarkoitetaan tiedostoa, joka sisältää täydellisen kopion halutun kiintolevyn sisällöstä. Levykuva voidaan tehdä joko koko kiintolevyn sisällöstä tai vain halutuista osioista. Yleensä myös kiintolevyllä sijaitseva käynnistyssektori (MBR) voidaan sisällyttää levykuvaan, jolloin käynnistysongelmainen konekin saadaan palautettua toimintakuntoiseksi levykuvan avulla. (Kayne 2012.)

Levykuvan luominen

Yrityksissä levykuvien käyttäminen on arkipäivää ja tarjoaa huomattavia säästöjä varsinkin konekantaa uudistettaessa. Mikäli kaikki hankitut koneet ovat samanlaisia, voidaan tällöin valmistella vain yksi kone ja siitä tehdyn levykuvan avulla voidaan käyttöjärjestelmä tarvittavine ohjelmineen asentaa kaikille koneille samanaikaisesti verkon (multicasting) kautta. Levykuva ja sen asennus voidaan tehdä joko Microsoftin RIS- (Remote Installation Services), WDS- (Windows Deployment Services) palvelimen tai ns. kolmannen osapuolen ohjelmis-

ton avulla. Yrityskäytössä Active Directory - verkossa toimivat WDS-palvelimet ovat syrjäyttäneet kolmannen osapuolen ohjelmat lähes kokonaan, mutta kotikäyttäjälle erilliset tai käyttöjärjestelmään sisäänrakennetut ohjelmistot ovat yleensä ainoa vaihtoehto levykuvan luomiseen. (Microsoft 2012.)

Levykuvaohjelmistot toimivat pääosin samalla tavalla, mutta levykuvan luomistavoissa on eroja eri ohjelmien välillä. Osa ohjelmista toimii siten, että ne asennetaan käyttöjärjestelmään ja levykuva luodaan käyttöjärjestelmän ollessa käynnissä ohjelman käyttöliittymän avulla (hot imaging). Nämä ohjelmat käyttävät Windowsin VSS-palvelua (Volume Shadow Copy Service), joka mahdollistaa levykuvan luomisen koneen ollessa käynnissä. Myös Windowsin oma varmuuskopiointiohjelma käyttää tätä palvelua. Suurin ongelma tätä menetelmää käytettäessä on se, että osa tiedoista on käyttöjärjestelmän käytössä, jolloin ne pitää hetkellisesti poistaa käytöstä kopioinnin ajaksi. Konetta voidaan kuitenkin käyttää levykuvan luonnin aikana. (Symantec 2009.)

Toiset ohjelmat toimivat siten, että ohjelmiston mukana toimitetaan käynnistysmedia tai se voidaan luoda ohjelmiston asennuksen jälkeen missä tahansa koneessa. Tämän käynnistysmedian avulla kohdekone voidaan käynnistää levykuvaohjelmiston omaan käyttöliittymään siten, että käyttöjärjestelmä ei ole ladattuna (cold imaging). Kun käyttöjärjestelmä varmennetaan tällä tavoin, mahdollistaa se ns. täysin puhtaan levykuvan luomisen, koska levykuvaohjelmistoa ei tarvitse asentaa kohdekoneeseen. Tätä menetelmää pidetään myös luotettavampana kuin edellä mainittua, koska levykuvaa luotaessa mikään käyttöjärjestelmälevyn tiedosto ei ole käytössä. (Thomas 2012.)

Käyttöjärjestelmän palautus levykuvan avulla

Käyttöjärjestelmän palautus on yleisimmin toteutettu siten, että kone käynnistetään käynnistysmedian avulla palautusohjelmistoon. Ohjelman käynnistyttyä voidaan valita haluttu levykuva palautusta varten. Mikäli kyseessä on normaalisti käynnistyvä kone, voidaan palautus käynnistää myös käyttöjärjestelmän kautta mikäli palautusohjelmisto tukee tätä vaihtoehtoa. Levykuva voidaan yleensä palauttaa paikalliselta tai ulkoiselta kiintolevyltä, tiedostopalvelimelta, NAS-

asemalta tai yhdeltä tai useammalta optiselta levyltä. Joissain ohjelmissa on myös mahdollista luoda käynnistettävä optinen levy, joka sisältää myös levykuvan.

On huomattava, että palautettaessa käyttöjärjestelmä levykuvasta korvaa se kaiken kiintolevyllä tai osioilla olevan tiedon palautusvaiheessa. Näin ollen omat tiedostot pitää varmuuskopioida ennen palautuksen tekemistä ja halutun palautussijainnin valinnan kanssa pitää olla tarkkana. (Shultz 2011.)

6.2 Migraatio levykuvan avulla

Migraatiolla tarkoitetaan tässä käyttöjärjestelmän sekä ohjelmien siirtämistä sellaisenaan toiselle kiintolevylle. Kotikäyttäjälle saattaa joskus tulla tarve siirtää käyttöjärjestelmä sellaisenaan uudelle kiintolevylle esim. siirryttäessä käyttämään suurempaa ja/tai nopeampaa kiintolevyä. Tällöin levykuvan avulla voidaan luoda uudelle kiintolevylle tarvittavat osiot sekä kopioida kaikki vanhalla kiintolevyllä ollut data uudelle levylle. Yleensä kiintolevyn vaihto on hyvä ajankohta asentaa käyttöjärjestelmä uudelleen, mutta levykuvan avulla voidaan tarvittaessa säästää aikaa ja vaivaa.

Levykuvan avulla voidaan myös siirtää vanhan koneen käyttöjärjestelmä sekä ohjelmat uuteen koneeseen, mutta vaikka esim. Windows 7 toipuu melko hyvin siirrosta täysin erilaiseen laiteympäristöön, ei tätä metodia voi kuitenkaan suositella. Käyttöjärjestelmän nopeuden sekä vakauden säilyttämiseksi on suositeltavaa asentaa käyttöjärjestelmä uuteen koneeseen alkuperäiseltä asennusmedialta sekä asentaa koneeseen uusimmat ajurit valmistajien verkkosivuilta. (Spector 2010.)

7 CASE: TIEDONVARMENNUSJÄRJESTELMÄ

Projektin tarkoituksena oli toteuttaa kustannustehokas, mutta silti mahdollisimman kattava varmennusjärjestelmä harrastelijavalokuvaajan käyttöön. Järjestelmän rakentamis- ja ylläpitokulut pyrittiin pitämään mahdollisimman pieninä hyödyntämällä jo olemassa olevaa laitteistoa sekä ilmaisohjelmia.

Valokuvaajaa käytetään tässä esimerkkinä siksi, että kuvilla saattaa olla muutakin kuin pelkkää tunnearvoa. Tämän lisäksi RAW-muodossa olevien valokuvien koko nykyisillä kameroilla kasvaa melko suureksi. Kohdekoneen valokuvaarkiston tämänhetkinen koko on lähes 400 gigatavua, joka tuo oman haasteensa järjestelmän toteutukselle. Erityisesti huomioitavia seikkoja olivat riittävän tallennuskapasiteetin sekä tiedonsiirtonopeuden tarjoaminen järjestelmässä.

7.1 Varmennusjärjestelmän suunnittelu ja visualisointi

Varmennusjärjestelmä kannattaa suunnitella tarkasti etukäteen, jotta resurssit ja investoinnit osataan kohdistaa oikein toteutusvaiheessa. Kappaleessa ”Varmennus- ja palautussuunnitelma” esitettiin lista asioista, joiden avulla pystytään hahmottelemaan järjestelmän resurssivaatimuksia. Suunnitelma laadittiin listan pohjalta ja siinä pyrittiin ottamaan huomioon mahdollisimman tarkasti järjestelmältä halutut ominaisuudet sekä jo olemassa olevat resurssit.

Tietojen tärkeys järjestelmässä

Ensimmäisenä laadittiin lista kaikista tiedoista, jotka järjestelmässä halutaan varmentaa:

- käyttöjärjestelmän varmennus levykuvien avulla
- valokuvat sekä muut kuvatiedostot
- office –dokumentit
- sähköpostit
- työpöydän sisältö
- verkkosivuston sisältö
- selaimen kirjanmerkit.

Lista ei ole tärkeysjärjestyksessä, mutta valokuvat ovat luonnollisesti tärkein varmennettava tietotyyppi. Koska niistä halutaan säilyttää useita varmuuskopiosukupolvia sekä päällekkäisiä varmuuskopioita eri tallennusvälineillä, muodostavat ne suurimman osan varmuuskopioitavasta tietomäärästä. Näin ollen valokuvat ja niiden varmuuskopiot ovat suurin määräävä tekijä varmennusjärjestelmän tilantarvetta ajatellen. On myös muistettava, että tilantarve ei pysy vakiona vaan varmennettavan tiedon määrä lisääntyy jatkuvasti.

Valokuvien lisäksi käytännössä kaikki itse luodut tiedostot, sähköpostit, selaimen kirjanmerkit sekä verkkosivuston sisältö halutaan varmentaa. Kohdekoneen työpöytää käytetään usein väliaikaisena tallennussijaintina esim. ladatuille tiedostoille, joten nekin on järkevää sisällyttää varmuuskopioihin.

Työaseman käyttöjärjestelmä varmennetaan levykuvien avulla. Näin ollen voidaan varautua käyttöjärjestelmäkiintolevyn rikkoutumiseen sekä nopeuttaa ja helpottaa Windowsin uudelleenasennusta tarvittaessa.

Tietojen muuttumistaajuus

Tiedot järjestelmässä muuttuvat melko usein, koska esim. valokuvia muokataan, lisätään ja myös poistetaan lähes päivittäin. Varmuuskopiointi pitää siis suorittaa melko usein, jotta tietojen menetys ongelmatilanteessa olisi mahdollisimman pieni. Normaalien ajastettujen varmuuskopioiden lisäksi hyödynnetään ns. jatkuvaa varmuuskopiointimenetelmää. Sen avulla muuttuneet tiedostot varmuuskopioidaan lähes reaaliajassa, jolloin on mahdollista palauttaa valokuva esim. kuvanmuokkausohjelman kaatumista edeltävään tilaan. Tiedostojen eri versioista muodostuu käytössä aikajana, jonka avulla niitä voidaan palauttaa päivämäärän ja muokkaushetken mukaan.

Varmistettujen tietojen säilytys

Esimerkkitapauksen toimipisteenä on yksityinen asunto, joten paikallisia varmuuskopioita ei tarvitse salata. Käytössä olevalla työasemalla sekä palvelimella otetaan käyttöön normaali käytönvalvonta, mutta itse tietosisältöä ei salata. Varmuuskopiot tallennetaan paikallisesti ulkoisille kiintolevyille sekä tiedostopalvelimelle.

Valokuvien etävarmuuskopiot tallennetaan ulkoiselle kiintolevylle, jota säilytetään pankin tallelokerossa. Tässäkään tapauksessa levyn sisältöä ei tarvitse salata, koska ainoastaan valokuvaajalla itsellään on oikeus ko. tallelokeron sisältöön. Pienemmät tiedostot etävarmuuskopioidaan myös pilvitallennuspalveluun, joten ne salataan vahvalla salausalgoritmilla ennen palveluun siirtämistä.

Paikallisten varmuuskopioiden saatavuus on luonnollisesti hyvällä tasolla, koska ne sijaitsevat samassa toimipisteessä ja esim. tiedostopalvelin kytketään työaseman kanssa samaan verkkoon. Valokuvien etävarmuuskopioiden osalta saattaa uusien varmuuskopioiden luomiseen tai valokuvien palauttamiseen otetuista varmuuskopioista muodostua muutaman päivän viive, koska tallelokerossa säilytettävä ulkoinen kiintolevy voidaan noutaa ainoastaan pankin aukioloaikoina. Pilvitallennuspalveluun tallennetut varmuuskopiot ovat saatavilla aina, mikäli Internet-yhteys toimii ja tallennuspalvelussa ei ole käyttökatkosta.

Tarvittava palautusnopeus tietojen tärkeysasteen mukaan

Esimerkkitapauksessa kyse ei ole ammattimaisesta valokuvaustoiminnasta, eivätkä ongelmatilanteet näin ollen aiheuta rahallisia tappioita. Järjestelmässä halutaan painottaa ensisijaisesti luotettavuutta ja vasta toissijaisesti palautusnopeutta varmuuskopioista. Mahdollisista ongelmatilanteista pyritään kuitenkin toipumaan mahdollisimman nopeasti.

Paras ajankohta varmennukselle

Varmuuskopiointi tapahtuu ajastetusti yöllä, jolloin työasemaa ei tarvita muihin tehtäviin. Myös manuaalisesti käynnistettävät varmuuskopiotehtävät pyritään suorittamaan yön aikana. Jatkuvan varmuuskopioinnin tarkoituksena on toimia huomaamattomasti käyttöjärjestelmän taustalla ja varmentaa muuttuneet ja uudet tiedot ulkoiselle kiintolevylle aina kun työasema on käytössä.

Vastuuhenkilöt

Tässä tapauksessa ei varsinaisia vastuuhenkilöitä tarvitse erikseen nimetä, koska ainoastaan yksi henkilö vastaa järjestelmän toiminnasta.

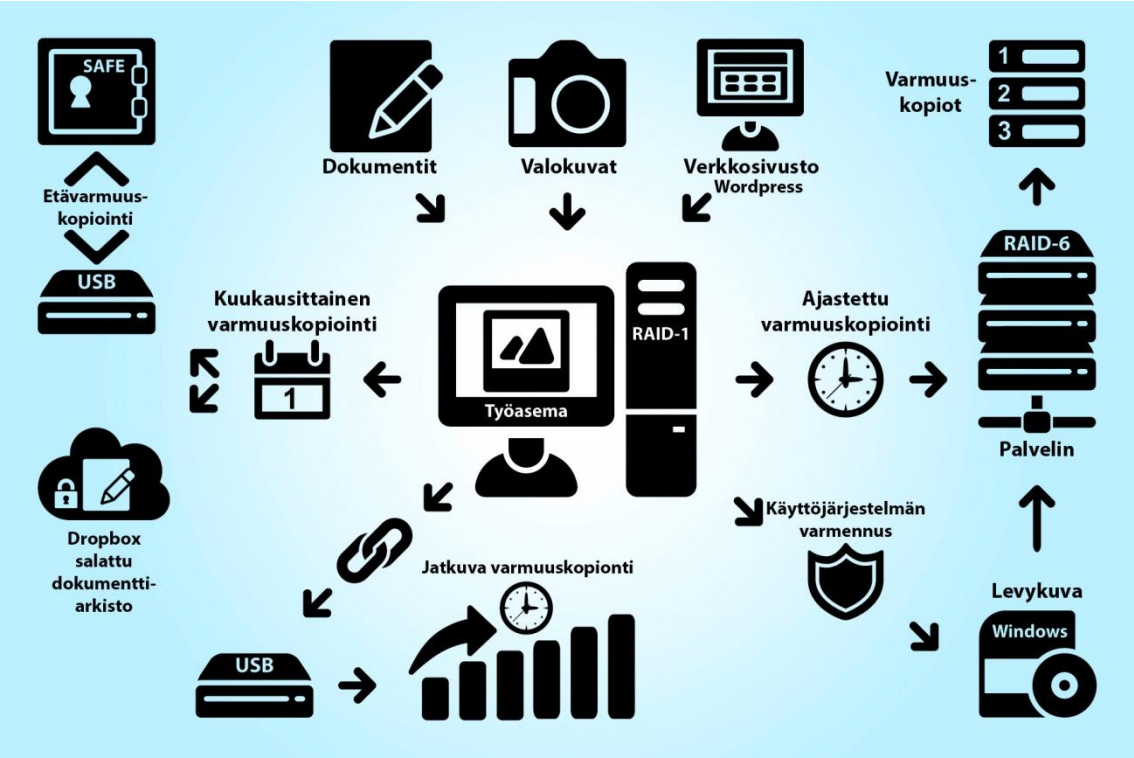
Tarvittavat ohjelmistot ja laitteet

Varmennusjärjestelmässä pyritään mahdollisuuksien mukaan käyttämään ilmaisia ohjelmistoja sekä palveluja, mutta mikäli toimivaa ilmaisvaihtoehtoa ei löydy, voidaan tarvittaessa myös hankkia kaupallisen ohjelmiston lisenssi. Tarvittavien ohjelmistojen vähimmäisvaatimuksina ovat ajastettujen sekä manuaalisesti käynnistettävien varmuuskopiointitehtävien suorittaminen sekä jatkuvan varmuuskopioinnin toteutus.

Laitteiston osalta hyödynnetään jo hankittuja sekä käytöstä poistettuja komponentteja, jolloin investoinnit pystytään pitämään mahdollisimman pieninä. Järjestelmän toteuttamiseksi hankitaan pääasialliseksi tallennustilaksi verkkoon liitettävä NAS-laite tai tiedostopalvelin. Lisäksi tarvitaan ulkoiset kiintolevyt valokuvien etävarmuuskopioita sekä jatkuvaa varmuuskopiointia varten. Koska tallennusratkaisut perustuvat kiintolevyihin, halutaan niiden rikkoutumiseen varautua käyttämällä RAID-tekniikoita sekä työasemassa että hankittavassa NAS-laitteessa tai tiedostopalvelimessa.

Varmennusjärjestelmän visualisointi

Varmennusjärjestelmän suunnitteluvaiheessa mainitut ominaisuudet haluttiin esittää mahdollisimman yksinkertaisesti, joten järjestelmä jaettiin tehtävien mukaan osiin ja puhtaaksipiirrettiin allaolevaan kuvioon 7. Osaa järjestelmään halutuista toiminnoista myös tarkennettiin kuvion luomisen yhteydessä. Kuviossa nuolet kuvaavat tiedon liikkumista järjestelmässä.



Kuvio 7. Tiedonvarmennusjärjestelmä.

Kuvion keskustassa on työasema, jonka kautta kaikki varmuuskopioitava tieto kulkee. Oikeaan alakulmaan on merkitty käyttöjärjestelmän varmennus levykuvin, joka toteutetaan puhtaalle Windows – asennukselle. Työasema voidaan tällöin helposti palauttaa asennuksen jälkeiseen tilaan. Levykuvat tallennetaan verkkoon liitetylle palvelimelle, josta niitä voidaan käyttää palautuksen tekemiseen.

Työaseman RAID-1 levyjärjestelmälle siis tallennetaan mm. luodut dokumentit, uudet ja käsitellyt valokuvat sekä verkkosivuston varmuuskopiot. Nämä tiedot

kopioituvat ulkoiselle USB-kiintolevylle aina kun niitä muutetaan tai tietoja lisätään. Jatkuva varmuuskopiointi mahdollistaa varmuuskopioiden versioinnin ajan myötä, eli samasta tiedostosta voidaan palauttaa eri versioita.

Varsinainen varmuuskopiointi tapahtuu ajastetusti viikoittain verkkoon liitetylle palvelimelle, jossa niistä säilytetään useita varmuuskopiosukupolvia. Täydellisen varmuuskopion luomisen jälkeen seuraavina kahtena viikkona luodaan lisäävät kopiot. Neljäntenä viikkona luodaan jälleen uusi täydellinen varmuuskopio. Täydellisiä varmuuskopiosukupolvia säilytetään palvelimella kolme kappaletta, minkä jälkeen varmuuskopiointiohjelma poistaa automaattisesti vanhimman täydellisen ja sitä seuranneet kaksi lisäävää varmuuskopiota palvelimelta.

Valokuvat etävarmuuskopioidaan jokaisen kuukauden ensimmäisenä työpäivänä USB-kiintolevylle, joka toimitetaan kopioinnin jälkeen takaisin pankkiin. Dokumentit sekä muut pienemmät tiedostot pakataan, salataan ja siirretään jo käytössä olleeseen Dropbox-pilvitallennuspalveluun.

7.2 Linux-tiedostopalvelin

Tiedostopalvelin haluttiin rakentaa mahdollisimman kustannustehokkaasti käyttäen mahdollisuuksien mukaan jo hankittuja komponentteja. Palvelimen tärkein tehtävä oli vastata kasvaneeseen tilantarpeeseen, mutta samalla lisätä redundanssia kiintolevyjen rikkoutumista vastaan RAID-järjestelmää hyväksi käyttäen. Yhtenä kriteerinä oli myös mahdollisuus kasvattaa tallennustilaa joko lisäämällä järjestelmään levyjä tai vaihtamalla niitä suurempiin, mikäli tilantarve kasvaisi tulevaisuudessa.

Aluksi harkittiin kaupallista NAS-järjestelmää, mutta koska useampaa kuin kahta levyä tukevien laitteiden hinta kohoaa nopeasti todella korkeaksi jopa ilman levyjä, päädyttiin palvelin rakentamaan itse. NAS-järjestelmiä tutkittaessa todettiin, että suuri osa laitteista sisältää myös haluttuun käyttötarkoitukseen tarpeettomia ominaisuuksia, kuten mediapalvelimia. Tämäntyyppiset ominaisuudet ovat varmasti hyödyllisiä, mikäli tarkoituksena on rakentaa esim. aina päällä oleva kodin keskitetty tallennusratkaisu, jonka kautta voidaan mm. toistaa tal-

lennettuja mediatiedostoja kotiteatterijärjestelmän kautta. Järjestelmään haluttiin kuitenkin mahdollisimman yksinkertainen sekä varmatoiminen palvelinratkaisu, jonka ei tarvitse olla päällä jatkuvasti.

Tiedostopalvelimen kokoonpano

Palvelinkone koottiin Antecin valmistamaan P182B tornikoteloon, jonka jäähdytys- sekä äänenvaimennusominaisuudet ovat vielä nykyäänkin erittäin hyvät, vaikka kotelo itsessään onkin jo noin viisi vuotta vanha. Myös koteloon sisäänrakennetut pölysuodattimet toimivat paljon päällä olevassa koneessa erittäin hyvin.

Kone koostuu seuraavista komponenteista:

- Prosessori: Intel Core2 Quad Q6600
- Emolevy: Asus P5E3 Deluxe
- Keskusmuisti: 4Gb DDR3 1333MHz
- Näytönohjain: nVidia GeForce 6200 LE
- Virtalähde: Cougar 550W modular
- Kiintolevy (käyttöjärjestelmä): Western Digital WD3200AAJB, 320Gb
- Kiintolevyt (Raid): 6x Samsung HD103SJ, 1TB.

Ainoa kuluerä palvelimen rakennuksen osalta muodostui neljän uuden HD103SJ-kiintolevyn hankinnasta.

Kaikki kotelotuulettimet sekä prosessorijäähdytin ovat Noctuan valmistamia, käytössä hiljaisiksi todettuja tuotteita. Äänenvaimennukseen haluttiin panostaa siksi, että kone sijaitsee muiden koneiden tavoin työhuoneessa.

DVD-asema sekä käyttöjärjestelmälle varattu kiintolevy ovat IDE-väyläisiä, koska koneen kaikki kuusi SATA-liitäntää haluttiin varata RAID-6-järjestelmää varten. Kotelon kiintolevykapasiteetti riittää vielä tulevaisuudessakin, mikäli järjestelmää halutaan laajentaa esim. erillisen SATA-ohjaimen avulla.

Käyttöjärjestelmän valinta

Käyttöjärjestelmäksi palvelinkoneeseen valittiin Linux, koska se täytti tärkeimmän valintakriteerin, eli mahdollisuuden rakentaa toimiva sekä testattu ohjelmistopohjainen RAID-6-järjestelmä. Myös käyttöjärjestelmän maksuttomuus oli tärkeä kriteeri. Palvelin haluttiin pitää mahdollisimman yksinkertaisena, eli valmiit NAS-käyttöön tarkoitetut jakeluversiot sivuutettiin ja koneeseen asennettiin Ubuntu Server v. 10.04 LTS. Minimaalisen asennuksen päälle voidaan tällöin helposti asentaa vain tarvittavat komponentit. Uudemmalle käyttöjärjestelmän versiolle ei ollut tarvetta, koska koneen komponentit ovat hieman iäkkäämpiä. Käyttöön haluttiin myös viiden vuoden ajan tuettu LTS-versio.

RAID-järjestelmä

Käyttöön haluttiin RAID-6-taso vikasietoisuuden parantamiseksi ja ennen kaikkea siksi, että järjestelmään liitettävät levyt ovat usein samasta levyerästä ja ne on ostettu samaan aikaan. Tämä tarkoittaa usein sitä, että ne saattavat myös hajota samaan aikaan tai ainakin melko nopeasti ensimmäisen levyn hajoamisen jälkeen. Tällöin riski toisen levyn hajoamiselle esim. levyjärjestelmän uudelleensynkronoinnin aikana on merkittävä. RAID-5-tasoa käytettäessä menetettäisiin tässä tapauksessa kaikki levyjärjestelmälle tallennetut tiedot.

Aluksi käytössä oli vain neljä kuudesta kiintolevystä. Kaksi muuta levyä olivat käytössä toisessa tietokoneessa sekä ulkoisessa kiintolevykotelossa. Koska ohjelmistopohjainen RAID-ratkaisu antaa mahdollisuuden lisätä tai korvata levyjä jälkikäteen, päätettiin koneeseen asennetuista neljästä kiintolevystä luoda ensin RAID-6-levyjärjestelmä ja lisätä siihen jäljelle jääneet kaksi levyä myöhemmin.

Koska RAID-6-järjestelmässä varataan kahden kiintolevyn tila pariteettidataa varten, jäi järjestelmään alustettuna hieman alle 4 teratavua käytettävissä olevaa tallennustilaa. Varmennettavan tiedon määrän ollessa noin 500 gigatavua, voidaan palvelimelle tarvittaessa tallentaa useita varmuuskopiosukupolvia.

7.3 Käyttöjärjestelmän varmennus levykuvin

Työaseman mahdollisiin käynnistymisongelmiin tai kiintolevyn rikkoutumiseen haluttiin varautua varmentamalla käyttöjärjestelmä levykuvien avulla. Koska Windowsin suorituskyky laskee ajan myötä, antavat levykuvat myös mahdollisuuden palauttaa käyttöjärjestelmä helposti ja nopeasti asennuksen jälkeiseen tilaan.

Käyttöjärjestelmän uudelleenasennus ei ole edellytys tiedonvarmennusjärjestelmän käyttöönotolle, mutta koska kohdekoneen käyttöjärjestelmä oli joka tapauksessa uudelleenasennuksen tarpeessa, saatiin näin järjestelmän pohjaksi täysin uusi Windows-asennus. Seuraavissa luvuissa käsitellään levykuvaohjelmiston valinta, uudelleenasennuksen esivalmistelut, käyttöjärjestelmän asennus sekä sen varmennus levykuvien avulla.

7.3.1 Levykuvaohjelmiston valinta.

Käyttöjärjestelmän varmennus levykuvien avulla on yleistynyt viime vuosina ja markkinoilta löytyy kaupallisten ohjelmistojen lisäksi myös useita ilmaisia vaihtoehtoja. Levykuvaohjelmistolle asetettiin vaatimuksiksi tuki levykuvan luomiselle käynnistysmedian avulla sekä levykuvien tallennus- ja asennusmahdollisuus lähiverkkoon liitetyn tallennusvälineen avulla.

Vertailuun otettiin seuraavat viisi ilmaista vaihtoehtoa:

- Macrium Reflect Free
- Paragon Backup & Recovery 2012 Free
- Active Image Protector Personal Edition
- Keriver 1-Click Restore Free 3.0
- Redo Backup and Recovery.

Yllä olevista ohjelmistoista Macrium Reflect, Paragon Backup & Recovery sekä Active Image Protector ovat erittäin suosittuja ja hyvin toimivia ratkaisuja, mutta niiden avulla ei voida luoda levykuvia asentamatta ohjelmistoa ensin järjestelmään.

Vaikka Keriver 1-Click Restorea voidaan pitää levykuvaohjelmistona, on se suunnattu enemmänkin järjestelmän varmuuskopiointiin kuin puhtaiden levykuvien luomiseen. Sen avulla voidaan luoda täydellisiä tai lisääviä varmuuskopioita, mutta poiketen varsinaisista varmuuskopiointiohjelmista Keriver luo varmuuskopiot levykuvina. Ohjelmisto tukee verkkosijainteja levykuvien tallennukseen ja asennukseen sekä levykuvien luomista palautuskonsolin avulla. Näin ollen ohjelmisto itsessään täyttäisi asetetut vaatimukset, mutta koska sen aktiivinen kehitystyö on lopetettu ja uusin versiokin on jo yli vuoden takaa, ei ohjelmistoa haluttu ottaa käyttöön. (Keriver 2011.)

Redo Backup and Recovery on itse asiassa Linux-pohjainen ns. live-CD, jonka avulla kone käynnistetään. Ohjelmistoa ei siis ole edes mahdollista asentaa, vaan kaikki toiminnot suoritetaan käynnistämällä kohdekone käynnistyslevyn tai USB-muistitikun avulla Linux-ympäristöön. Se tarjoaa normaalien levykuvatoimintojen lisäksi myös mm. mahdollisuuden palauttaa poistettuja tiedostoja sekä esim. käyttää Internetiä, joka saattaa olla hyödyllinen ominaisuus, mikäli koneen oma käyttöjärjestelmä ei enää suostu käynnistymään.

Koska Redo Backup and Recovery tarjoaa kaikkien haluttujen ominaisuuksien lisäksi vielä mahdollisuuden luoda levykuvia myös Linux-järjestelmistä sekä suorittaa muita hyödyllisiä tehtäviä käynnistysmedian avulla, päätettiin se ottaa käyttöön kohdejärjestelmässä. (Redobackup 2012.)

7.3.2 SSD-levyn suorituskyvyn palauttaminen

Koneen käyttöjärjestelmä on asennettu hieman vanhemmalle SSD-levylle, jossa ei ole suorituskykyä ylläpitävää sisäistä TRIM-ominaisuutta. Tämä aiheuttaa levyn toiminnan hidastumista ajan sekä kirjoitus- ja lukutoimintojen myötä, joten käyttöjärjestelmän uudelleenasennuksen yhteydessä suoritettiin levylle suorituskyvyn palautus Parted Magic Linux-live-CD:n avulla. Useimpien SSD-levyjen suorituskyky saadaan palautettua ajamalla levyille ns. secure erase-käsky, joka tyhjentää levyn ja palauttaa niiden suorituskyvyn alkuperäiselle tasolle. (Rhee 2011.)

7.3.3 Käyttöjärjestelmän asennus

Käyttöjärjestelmänä toimiva Windows 7 asennettiin koneeseen siten, että vain näppäimistö, hiiri sekä näyttö olivat liitettyinä koneeseen. Tällöin saadaan tehtyä ajuripohjaltaan mahdollisimman puhdas asennus. Kone ei myöskään ollut liitettynä verkkoon asennuksen aikana, joten mahdolliset virukset eivät näin ollen pääse koneelle ennen kunnollisten suojausten asentamista. Nämä toimenpiteet eivät ole pakollisia, mutta uudelleenasennus tehtiin edellä mainitulla tavalla, jotta ensimmäisestä levykuvasta saataisiin mahdollisimman puhdas ja käyttökelpoinen tulevaisuutta ajatellen.

7.3.4 Käyttöjärjestelmän varmennus

Käyttöjärjestelmän varmennus toteutettiin Redo Backup and Restore -ohjelmistoa käyttäen. Sen avulla koneen käyttöjärjestelmän eri asennusvaiheista tehtiin kolme erillistä levykuvaa. Levykuvien luonti oli nopeaa ja vaivatonta ja kolme asennuksen eri vaiheissa otettua levykuvaa antavat mahdollisuuden valita paras levykuva palautusta varten riippuen halutusta lopputuloksesta. (Redobackup 2012.)

Levykuva 1.

Ensimmäinen levykuva luotiin välittömästi asennuksen jälkeen, eli sen avulla on mahdollista palauttaa kone täysin puhtaaseen Windows-asennukseen, mikäli esim. ohjelmien tai ajureiden asennuksen aikana havaitaan ongelmia. Tätä levykuvaa voidaan hyödyntää myös, jos järjestelmään tehdään esim. laitteistomuutoksia. Ensimmäisen levykuvan kooksi muodostui noin 3,8 gigatavua.

Levykuva 2.

Ennen toisen levykuvan luontia asennettiin koneelle Windows 7 Service Pack 1 sekä palomuuri- ja virustorjuntaohjelmistot. Tässä vaiheessa konetta ei kuitenkaan vielä kytketty verkkoon. Toisen levykuvan koko asennusten jälkeen oli noin 4,5 gigatavua.

Levykuva 3.

Ennen viimeisen levykuvan luontia kone kytkettiin kiinni verkkoon ja siihen asennettiin kaikki saatavilla olevat päivitykset Windows Update-palvelusta. Tämä kasvatti levykuvan koon noin 6,9 gigatavuun, eli koko lähes kaksinkertaistui asennuksesta, jossa ei ole mukana päivityksiä.

Varsinaiset asennukset tehtiin muutamaa poikkeusta lukuun ottamatta vasta viimeisen levykuvan luomisen jälkeen, koska ohjelmista sekä ajureista julkaistaan melko usein uusia versioita. Näin vältytään vanhojen ohjelmien ja ajureiden poistamiselta tai päivittämiseltä, mikäli käyttöjärjestelmä halutaan asentaa uudelleen levykuvaa käyttäen.

7.4 Työaseman valmistelu

Työaseman valmisteluvaiheessa toteutettiin suunnitelman mukainen RAID-1-levyjärjestelmä varastolevyille. Samalla toteutettiin myös tallennettujen tietojen uudelleenjärjestely siten, että niiden varmuuskopiointi olisi helpompaa.

RAID-1-järjestelmän käyttöönotto

Koska järjestelmän tietojen pääasiallisena tallennussijaintina toimii käytössä oleva työasema, haluttiin koneen tallennuslevyjen rikkoutumiseen varautua ottamalla käyttöön RAID-1-levyjärjestelmä. Tällöin kiintolevyn rikkoutuessa ei menetetä edes edellisen varmuuskopiointikerran jälkeen luotuja tai muokattuja tiedostoja. Myös ongelmatilanteesta palautuminen on lähes välitöntä, koska levylle tallennetut tiedot säilyvät koko ajan käytettävissä, vaikka levyjärjestelmä korjaakin itse itseään taustalla.

Levyjärjestelmän ohjaimena toimii työaseman emolevyn ICH10R-piirisarja. Järjestelmä olisi voitu toteuttaa myös puhtaasti käyttöjärjestelmässä, sillä työasemassa käytössä oleva Windows 7 Ultimate tukee RAID-1:n käyttöä. Aikaisempien kokemusten mukaan emolevyn RAID-ohjaimella toteutettu järjestelmä on käytössä kuitenkin vakaampi. Windowsissa toteutettu RAID mm. aloittaa aikaavievän levyjärjestelmän uudelleensynkronoinnin erittäin helposti esim. koneen

kaatumisen tai sähkökatkon jälkeen, jota emolevyn RAID-ohjaimella toteutettu järjestelmä ei yleensä tee. Huonona puolena emolevyn RAID-ohjain sitoo levyjärjestelmän käytössä olevan emolevyn piirisarjaan. Toisin sanoen mikäli emolevy rikkoutuu, saadaan levyjärjestelmä palautettua ainoastaan samantyyppisellä piirisarjalla varustetun emolevyn avulla. Myös piirisarjan versiolla on merkitystä, vaikkakin Intelin piirisarjojen avulla toteutetut RAID-järjestelmät tuntuvat olevan sekä alas- että ylöspäin yhteensopivia ainakin muutaman piirisarjaversion verran. Mitään takeita toimivuudesta ei kuitenkaan ole yritettäessä palauttaa levyjärjestelmää toimintakuntoon toista piirisarjaa käyttävän emolevyn avulla. RAID-1 on kuitenkin siinä mielessä turvallinen ratkaisu, että kummankin levyn sisältö on luettavissa erikseen missä tahansa koneessa.

Tietojen uudelleenjärjestely

Valmistauduttaessa varsinaiseen varmuuskopiointivaiheeseen toteutettiin työasemalla melko kattava tietojen uudelleenjärjestely. Hyvin usein ongelmana on tietojen sirpaloituminen järjestelmässä. Tiedostoista saattaa olla tallennettuna useita eri versioita ja niistä suurimman osan sijaintia kiintolevyllä ei välttämättä edes tiedetä. Tämäntyyppisen hakemisto- ja tiedostorakenteen varmuuskopioiminen on erittäin hankalaa ja tehotonta. Lisäksi varmuuskopioiden koot kasvavat, koska samoja ja tarpeettomia tiedostoja varmuuskopioidaan useaan kertaan. Uudelleenjärjestelyn ideana on siirtää kaikki varmuuskopioitaviksi halutut tiedostot yksinkertaisten hakemistorakenteiden sisään. Tällöin varmuuskopiointitehtävien laatiminen helpottuu ja ennen kaikkea tiedostoille on aina olemassa oma paikkansa.

Kohdekoneen tapauksessa luotiin kolme eri päätason kansiota, jonka sisään kaikki varmuuskopioitaviksi halutut tiedot siirrettiin. Koska koneella tehtävä työ on usein projektiluontoista, luotiin ensin näille keskeneräisille projekteille oma kansionsa. Tämän kansion sisään siirrettiin kaikki keskeneräisten projektien kansiot, jotka siirron yhteydessä nimettiin yhtenäisesti ja siten, että ne kertovat mahdollisimman paljon kansion sisällöstä. Seuraavaksi luotiin arkistokansio, johon siirrettiin valokuvia lukuunottamatta lähes kaikki muu järjestelmässä oleva tieto. Sinne siis siirrettiin esim. valmistuneet projektit ja yksittäiset dokumentit

omiin kansioihinsa. Valokuvat sekä Lightroomin kuvatietokanta sijaitsevat jo omissa päätason kansioissaan, joten niille ei tehty mitään. Valokuvat sijaitsevat omissa kansioissaan, jotka on nimetty kuvauspäivämäärän ja -kohteen mukaisesti. Nämä kansiot on vielä jaoteltu vuosien mukaan omiin kansioihinsa.

7.5 Varmuuskopiointi

Varmuuskopiointi toteutettiin paikallisen sekä etävarmuuskopioinnin yhdistelmänä käyttäen ulkoisia kiintolevyjä, ilmaista pilvitallennuspalvelua sekä paikallista tiedostopalvelinta. Ajastettujen varmuuskopioiden lisäksi haluttiin järjestelmässä hyödyntää myös ns. jatkuvaa tiedonvarmennusjärjestelmää.

7.5.1 Varmuuskopiointiohjelmiston valinta

Varmuuskopiointiohjelmistoksi haluttiin ilmainen, helppokäyttöinen ja monipuolinen ohjelmisto. Valintaprosessia helpottamaan kirjattiin halutut ominaisuudet listaksi:

- tuki useille varmuuskopiointitehtäville
- tehtävien ajastusmahdollisuus
- täyden- ja lisäävän varmuuskopioinnin tuki
- varmuuskopioiden tallennus lähiverkkoon liitettyyn tallennuslaitteeseen
- yleisen tallennusformaatin käyttö (suora kopio, zip)
- muistutukset suorittamattomista varmuuskopiointitehtävistä
- varmuuskopioiden salaus- ja pakkausmahdollisuus
- mahdollisuus suorittaa ulkoisia ohjelmia ja komentosarjoja
- varmuuskopiointitehtävien tallennusmahdollisuus käyttöjärjestelmän uudelleenasennuksen tai levyrikon varalta.

Ominaisuudet listattiin tarkoituksella rajaamaan melko tarkasti mahdollisia vaihtoehtoja, sillä ilmaisia varmuuskopiointiohjelmistoja on saatavilla todella paljon. Yleisesti tavoitteena olisi löytää haluttuun käyttötarkoitukseen sopiva ohjelmisto ja opetella sen toiminnot hyvin, jotta se voitaisiin pitää käytössä mahdollisimman kauan. Mikäli ohjelmistoa vaihdetaan usein, aiheuttaa se helposti var-

muuskopioiden eheyden heikentymistä. Jokainen ohjelmisto toimii kuitenkin hieman eri tavalla ja varmuuskopiot eivät ole yleensä yhteensopivia keskenään. Varsinkin ongelmatilanteesta palautuminen saattaa olla vaikeaa, mikäli varmuuskopioiden luomiseen on käytetty useita eri ohjelmistoja.

Vaihtoehtoja etsittäessä keskityttiin ohjelmistoihin, joilla on hyvä maine käyttäjien keskuudessa ja joita kehitetään aktiivisesti. Seuraavat kuusi ohjelmistoa otettiin lähempään tarkasteluun:

- Ocster Backup free
- Cobian Backup
- FBackup
- Backup Maker
- Bitreplica
- Duplicati.

Ocster Backup free

Ocster Backup free on kaupallisen ohjelmiston ominaisuuksiltaan rajoitettu ilmaisversio, joka vaikuttaa erittäin yksinkertaiselta ja käyttäjäystävälliseltä varmuuskopiointiratkaisulta. Valitettavasti se ei täytä haluttuja vaatimuksia, sillä ilmaisversiosta on poistettu mm. tuki varmuuskopioiden verkkotallennukseen. (Ocster 2012.) Koska tarkoituksena on tallentaa varmuuskopiot lähiverkon kautta tiedostopalvelimelle, ei tätä ohjelmistoa voitu ottaa järjestelmässä käyttöön.

FBackup

FBackup on täysin ilmainen ohjelmisto sekä yksityis- että yrityskäyttöön. Ohjelmisto tukee kaikkia muita haluttuja ominaisuuksia, mutta jostain syystä tuki lisäävien- tai eroavuusvarmuuskopioiden luomiseen on jätetty kokonaan pois. Sen avulla voidaan siis luoda ainoastaan pakattuja tai pakkaamattomia täydellisiä varmuuskopioita. (Fbackup 2012.) Pienempien varmuuskopioitavien tietomäärien kanssa tämä ei ehkä muodostaisi ongelmaa, mutta kohdejärjestelmän tapauksessa varmuuskopioitavaa tietoa on niin paljon, ettei ohjelmiston käyttöä voitu edes harkita.

Backup Maker

Backup Maker on yksi suosituimmista ilmaisista varmuuskopiointiohjelmistoista. Se tarjoaa kattavat ominaisuudet ollen kuitenkin helppokäyttöinen. Ohjelmisto on ilmainen henkilökohtaisessa käytössä, mutta valitettavasti ilmaisversio kuitenkin kehottaa hankkimaan maksullisen version ohjelmistosta aina koneen käynnistyksen yhteydessä. Lisenssi itsessään ei ole kallis, mutta maksua vastaan ei saada uusia ominaisuuksia, vaan ainoastaan kehotusruutu poistuu näkyvistä.

Ohjelmiston sivuilta löytyvän ominaisuuslistan mukaan tehtävien automaattisen uudelleenajastuksen pitäisi olla mahdollista silloin, kun tehtävää ei pystytä esim. tallennussijainnin puuttumisen vuoksi suorittamaan. (Ascomp 2012.) Tämä ominaisuus olisi kohdejärjestelmässä tarpeellinen, sillä tiedostopalvelin ei ole välttämättä päällä ajastetun tehtävän aikaan. Varmuuskopiointi saattaa siirtyä myöhempään ajankohtaan myös esim. sähkökatkosten tai lomamatkojen vuoksi. Uudelleenajastusta ei kuitenkaan saatu testeissä toimimaan eikä ohjelmisto edes huomauttanut ”unohdetusta” varmuuskopiointikerrasta millään tavalla. Ohjelmistoa ei valittu tehtävien uudelleenajastuksen ja muistutusten toimimattomuuden vuoksi.

Bitreplica

Bitreplica on ohjelmistona melko uusi tulokas, mutta se vaikutti aluksi ominaisuuksiensa valossa todella lupaavalta. (Bitreplica 2012.) Ohjelmistoa testatessa ongelmaksi muodostuivat ilmeisesti ohjelman väärin tulkitsemat tiedostojen aikamerkinnät työaseman ja palvelimen välillä. Tämä aiheutti sen, että vaikka edellisen täydellisen varmuuskopion jälkeen ei tietoja ollut muutettu lainkaan, ohjelmisto kopioi lisäävään varmuuskopioon turhaan n. 30% kaikista alkuperäisistä tiedostoista. Ilmiö ei toistunut kun varmuuskopio tehtiin työaseman toiselle levylle. Samaan aikaan testattu Cobian Backup suoriutui lisäävän varmuuskopion luonnista palvelimelle moitteetta. Ohjelmistoa ei valittu verkkotallennuksen toimimattomuuden vuoksi.

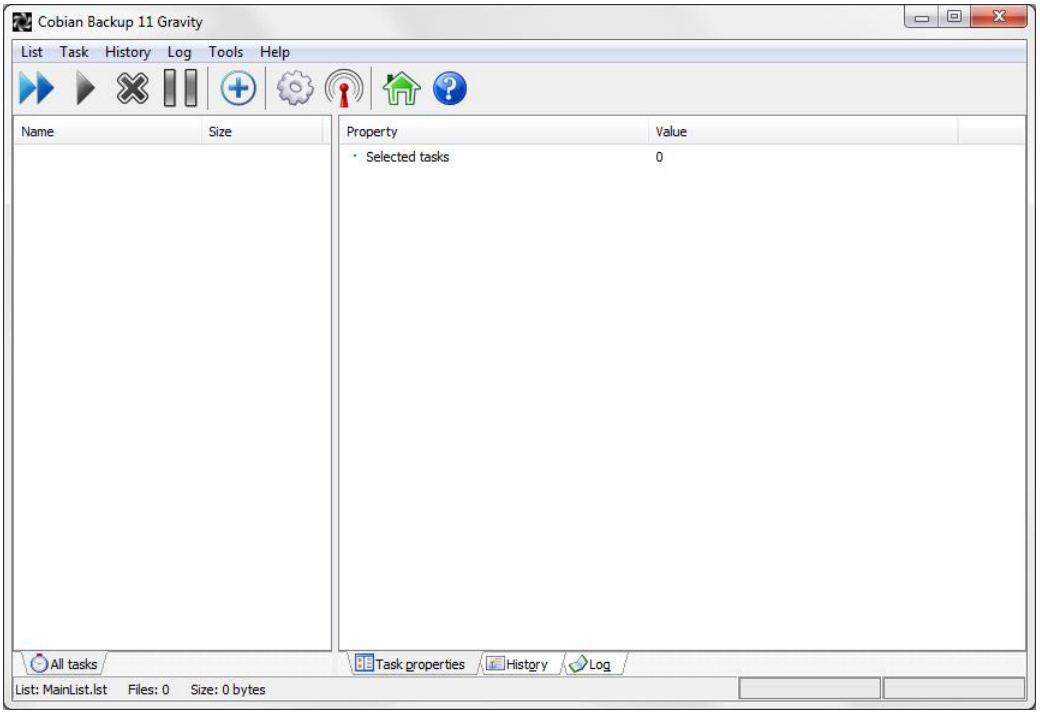
Duplicati

Duplicati on yksinkertainen ja pieni avoimeen lähdekoodiin perustuva varmuuskopiointityökalu. Ohjelmisto on selkeästi suunnattu pilvitallennuspalveluiden käyttöön ja se tarjoaakin suoran tuen varmuuskopioiden siirtoon tallennuspalveluihin sekä niiden pakkaus- ja salausmahdollisuuden. (Duplicati 2012.) Duplicati vaikutti erittäin mielenkiintoiselta, mutta valitettavasti varmuuskopioiden luominen ohjelmiston avulla on todella hidasta. Ohjelmistoa ei valittu varmuuskopioinnin hitauden vuoksi.

Cobian Backup

Cobian Backup on yksi vanhimmista ja kattavimmista ilmaisista varmuuskopiointiohjelmistoista. Sen tämänhetkinen versionumero on 11 ja ensimmäinen versio julkaistiin jo vuonna 2000. Ohjelmisto ei perustu avoimeen lähdekoodiin, mutta sitä kehitetään silti aktiivisesti. Cobian Backup on todettu käytössä erittäin vakaaksi ja luotettavaksi ja sen ominaisuuslista yleensä kasvaa uusien versioiden myötä. (Cobiansoft 2012.) Se tarjoaakin kaikki ominaisuudet, jotka ohjelmistolta alun perin haluttiin.

Verrattuna muihin testattuihin varmuuskopiointiohjelmistoihin suoriutui Cobian Backup nopeimmin täydellisten- ja lisäävien varmuuskopioiden luonnista tiedostopalvelimelle. Testeissä ei myöskään havaittu minkäänlaisia ongelmia, vaan varmennus onnistui jokaisella testikerralla erittäin hyvin. Ohjelmiston käyttöliittymä on hieman karu (kuva 2), mutta tärkeimmät toiminnot ja tiedot ovat selkeästi esillä.

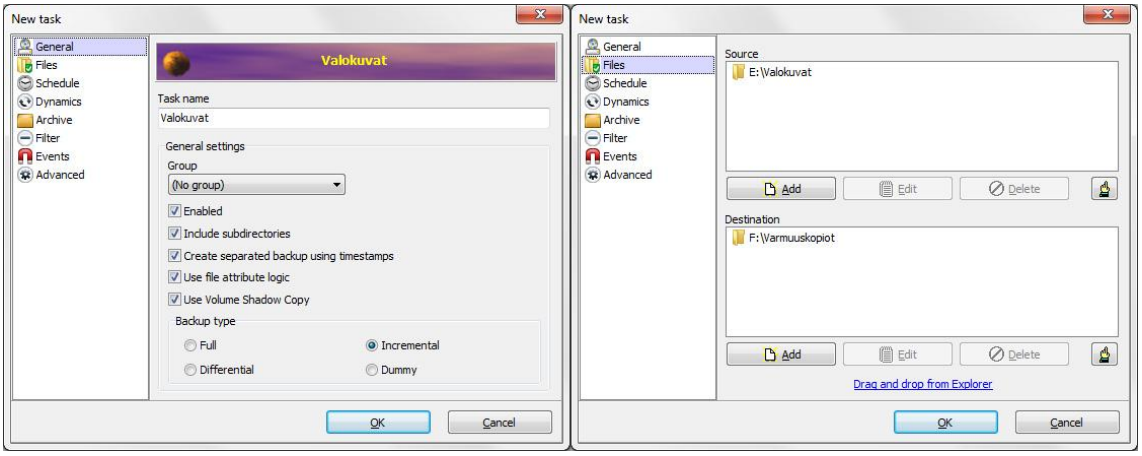


Kuva 2. Cobian Backup käyttöliittymä.

Cobian Backup valittiin järjestelmän varmuuskopiointiohjelmistoksi sen tarjoamien ominaisuuksien sekä hyvien testitulosten ansiosta.

Varmuuskopiointitehtävän luominen

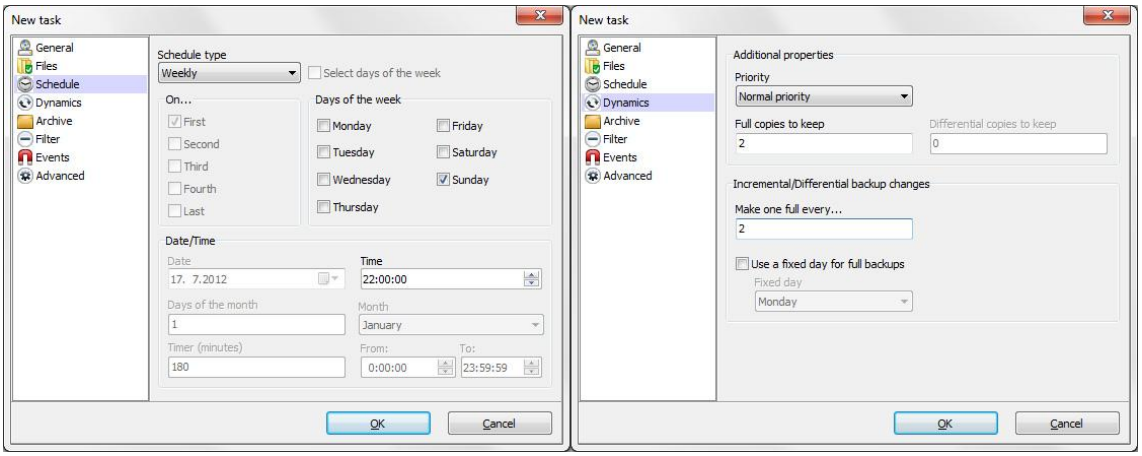
Uuden tehtävän luominen aloitetaan valitsemalla käyttöliittymän työkaluriviltä ympyröity plusmerkki, joka avaa uuden ikkunan tehtävän luomista varten. Esimerkissä luodaan uusi varmuuskopiointitehtävä sekä käydään läpi tärkeimmät asetukset (kuva 3).



Kuva 3. Cobian Backup - Uusi tehtävä, välilehdet 1-2.

Ensimmäisellä välilehdellä on mahdollisuus antaa varmuuskopiointitehtävälle nimi. Nimeäminen kannattaa tehdä johdonmukaisesti ja siten, että se kuvastaa parhaiten tehtävän tarkoitusta. Tehtäviä voidaan myös jaotella ryhmiin, joka selkeyttää ohjelmiston käyttöä mikäli tehtäviä luodaan runsaasti. Oletusarvoisesti alihakemistot sisällytetään varmuuskopioihin, mutta joskus voi olla tarve varmuuskopioida vain valitun päähakemiston sisältö. Alihakemistojen poissulkeminen onnistuu poistamalla valinta kohdasta ”Include subdirectories”. Välilehden alaosasta valitaan haluttu varmuuskopiointitapa. Valittavina ovat täysi-, lisäävä- sekä eroavuusvarmuuskopionti. Täysi varmuuskopio luodaan aina ensimmäisellä kerralla sekä halutuin aikavälein vaikka tässä valittaisiinkin tyypiksi lisäävä- tai eroavuusvarmuuskopiointi. Viimeisenä vaihtoehtona oleva ”Dummy” ei luo varmuuskopiota lainkaan, mutta sitä voidaan käyttää mm. erilaisten tehtävien ajastukseen sekä luodun varmuuskopiointitehtävän simulointiin.

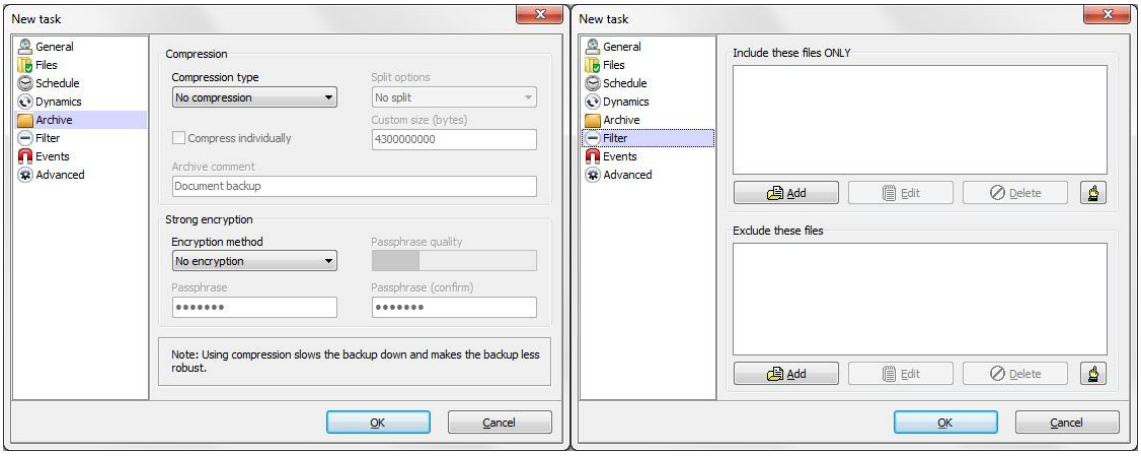
Files-välilehdellä on mahdollisuus valita, mitkä tiedot varmuuskopioidaan ja minne ne tallennetaan. Varmuuskopioitaviksi tiedoiksi on mahdollista valita yksittäisiä tiedostoja, hakemistoja sekä myös FTP-lähteitä. Ohjelmiston avulla on siis mahdollista varmuuskopioida esimerkiksi kokonainen verkkosivusto palveluntarjoajan palvelimelta. Tallennuskohteeksi voidaan valita hakemisto miltä tahansa koneeseen liitetyltä tallennuslaitteelta. Vaihtoehtoisesti varmuuskopioiden tallennussijainniksi voidaan valita myös FTP-palvelin.



Kuva 4. Cobian Backup - Uusi tehtävä, välilehdet 3-4.

Cobian Backup tarjoaa erittäin kattavat ajastusmahdollisuudet varmuuskopiointitehtäville (kuva 4). Tehtäviä on mahdollisuus ajastaa toimimaan päivittäin, viikoittain, kuukausittain ja vuosittain. Näiden lisäksi on mahdollista asettaa tehtävä suoritettavaksi joka kerta kun kone käynnistetään, vain kerran tai tietyin aikavälein, jolloin määritetään aikaväli minuuteissa sekä aloitus- ja lopetuskellonaika. Ajastustyypin valinnan alla näkyvät lisävalinnat muuttuvat riippuen siitä, mikä ajastustapa on valittuna. Mikäli tehtävää ei haluta ajastaa, voidaan valita asetus ”manually”, jolloin käyttäjä käynnistää tehtävän suorituksen halutessaan.

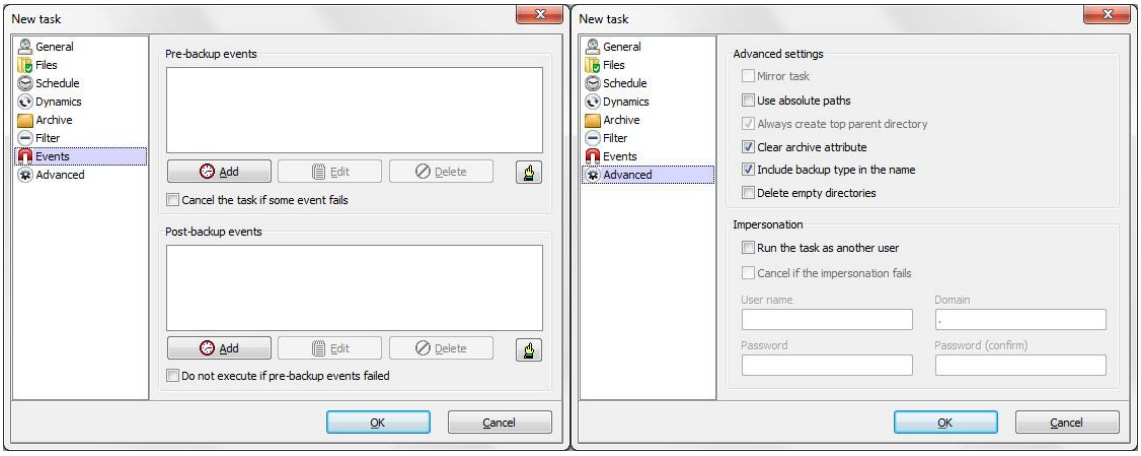
Seuraavalla välilehdellä voidaan valita, miten monta täydellistä varmuuskopiota halutaan säilyttää. Kun tallennussijainnissa on haluttu määrä täydellisiä varmuuskopioita, poistaa Cobian Backup automaattisesti vanhimman täydellisen sekä sitä seuranneet lisäävät- tai eroavuusvarmuuskopiot uuden täydellisen varmuuskopion luonnin yhteydessä. Mikäli käytössä on lisäävä- tai eroavuusvarmuuskopiointityyppi, määritetään täydellisten varmuuskopioiden luontitaajuus kohdassa ”Incremental/Differential backup changes”. Täydellinen varmuuskopio voidaan myös määrittää luotavaksi aina tiettynä päivänä.



Kuva 5. Cobian Backup - Uusi tehtävä, välilehdet 5-6.

Välilehdeltä ”Archive” voidaan valita varmuuskopion pakkaustapa (kuva 5). Oletusarvoisesti Cobian Backup ei pakkaa varmuuskopioita, eli tiedostot kopioidaan käytännössä sellaisinaan kohdehakemistoon, mutta tarvittaessa valittavina ovat zip- ja 7zip-pakkausmetodit. Pakattu varmuuskopio voidaan myös jakaa halutunkokoisiin osiin, joka on hyödyllinen ominaisuus mikäli varmuuskopio halutaan tallentaa esim. optisille levyille. Mikäli varmuuskopio halutaan salata, voidaan kohdasta ”Strong encryption” valita salaustapa sekä määrittää salaukselle haluttu salasana. Käytettävissä ovat 128bit, 192bit sekä 256bit AES-salausmetodit.

Varmuuskopioihin voidaan ”Filter”-välilehdellä sisällyttää tai poissulkea yksittäisiä tiedostoja tai hakemistoja luomalla ns. sääntöjä. Sääntöjen avulla voidaan valita tiedostoja tai hakemistoja esim. niiden koon tai iän perusteella. Tiedostoja voidaan myös valita tiedostopäätteen mukaan.



Kuva 6. Cobian Backup - Uusi tehtävä, välilehdet 7-8.

Events-välilehdellä voidaan määritellä haluttuja toimintoja, jotka toteutetaan joko ennen varmuuskopiointitehtävän suoritusta tai sen jälkeen (kuva 6). Ennen varmuuskopioinnin toteutusta on mahdollista mm. suorittaa komentosarjoja tai käynnistää ja sulkea ulkopuolisia ohjelmia. Tehtävän suorituksen jälkeen voidaan lisäksi esim. sammuttaa kone tai asettaa se lepotilaan. Koneen automaattinen sammutus varmuuskopioinnin jälkeen on hyödyllinen ominaisuus, mikäli tehtävä on ajastettu suoritettavaksi esimerkiksi yön tai viikonlopun aikana.

Viimeiseltä välilehdeltä ei yleensä tarvitse muuttaa mitään, mutta kohdassa ”Impersonation” voidaan syöttää toisen käyttäjän tunnus sekä salasana, jota käytetään varmuuskopion luomiseen. Asetus voi olla hyödyllinen, mikäli koneen käyttäjällä ei ole järjestelmänvalvojan oikeuksia. (Cobiansoft 2012.)

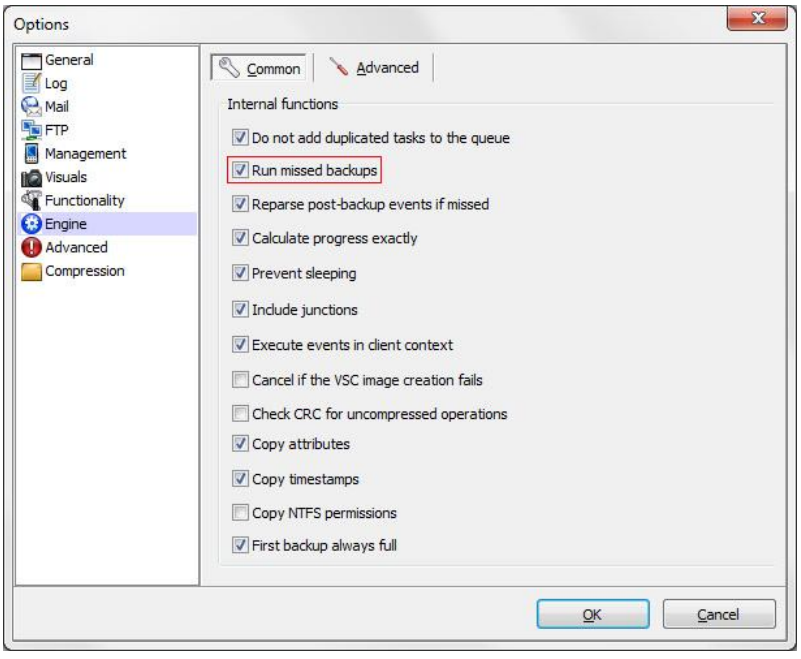
Tiedostojen palauttaminen varmuuskopioista

Cobian Backup eroaa palautusprosessin osalta muista testatuista ohjelmistoista siten, että siinä ei ole sisäänrakennettua tapaa palauttaa varmuuskopioituja tiedostoja. Luodut varmuuskopiot sijaitsevat varmennusajankohdan mukaan nimetyissä hakemistoissa ja tiedostojen palautus tapahtuu yksinkertaisesti kopioimalla ne uuteen sijaintiin halutusta varmuuskopiohakemistosta. Lisäävien varmuuskopioiden palautus suoritetaan kopioimalla ensin edellisen täydellisen varmuuskopion sisältö haluttuun kohdehakemistoon. Tämän jälkeen lisäävien

varmuuskopioiden sisältö kopioidaan samaan hakemistoon ylikirjoittaen tiedostojen vanhemmat versiot aloittaen vanhimmasta ja edeten uusimpaan. Täydellisiä varmuuskopioita suositellaankin luotavaksi melko usein, koska lisäävistä varmuuskopioista palautettaessa myös edellisen täydellisen varmuuskopion luonnin jälkeen tarkoituksellisesti poistetut tiedostot kopioidaan takaisin kohdehakemistoon. Tämä saattaa muodostua ongelmaksi, mikäli edellisestä täydellisestä varmuuskopiosta on kulunut paljon aikaa ja tiedostoja on sen jälkeen poistettu runsaasti. Alun perin tarkoituksellisesti poistetut tiedostot pitää siis poistaa uudelleen kohdehakemistosta palautuksen jälkeen. (Cobiansoft 2012.)

Ohitettujen varmuuskopiotehtävien uudelleenajastus

Cobian Backup ei oletusarvoisesti suorita ohitettuja varmuuskopiotehtäviä automaattisesti, mutta ominaisuus voidaan ottaa käyttöön ohjelman asetuksista allaolevan kuvan 7 mukaisesti.



Kuva 7. Cobian Backup asetukset.

Kun asetus ”Run missed backups” on valittuna, tarkistaa ohjelmisto varmuuskopiotehtävälistan kolmen tunnin välein ja suorittaa ohitetut tehtävät automaattisesti. (Cobiansoft 2012.)

7.5.2 Paikallinen varmuuskopiointi

Paikallinen varmuuskopiointi suoritetaan Cobian Backupin avulla ajastetusti lähiverkon kautta tiedostopalvelimelle. Varmennusta varten luotiin kaksi erillistä varmuuskopiointitehtävää. Valokuvat sekä Lightroomin kuvatietokanta varmuuskopioidaan viikoittain siten, että täydellinen varmuuskopio luodaan aina kolmen lisäävän varmuuskopion jälkeen. Täydellisiä varmuuskopiosukupolvia säilytetään palvelimella yhtä aikaa neljä kappaletta. Cobian Backup poistaa automaattisesti vanhimman täydellisen ja sitä seuranneet kolme lisäävää varmuuskopiota viidennen täydellisen varmuuskopion luonnin yhteydessä.

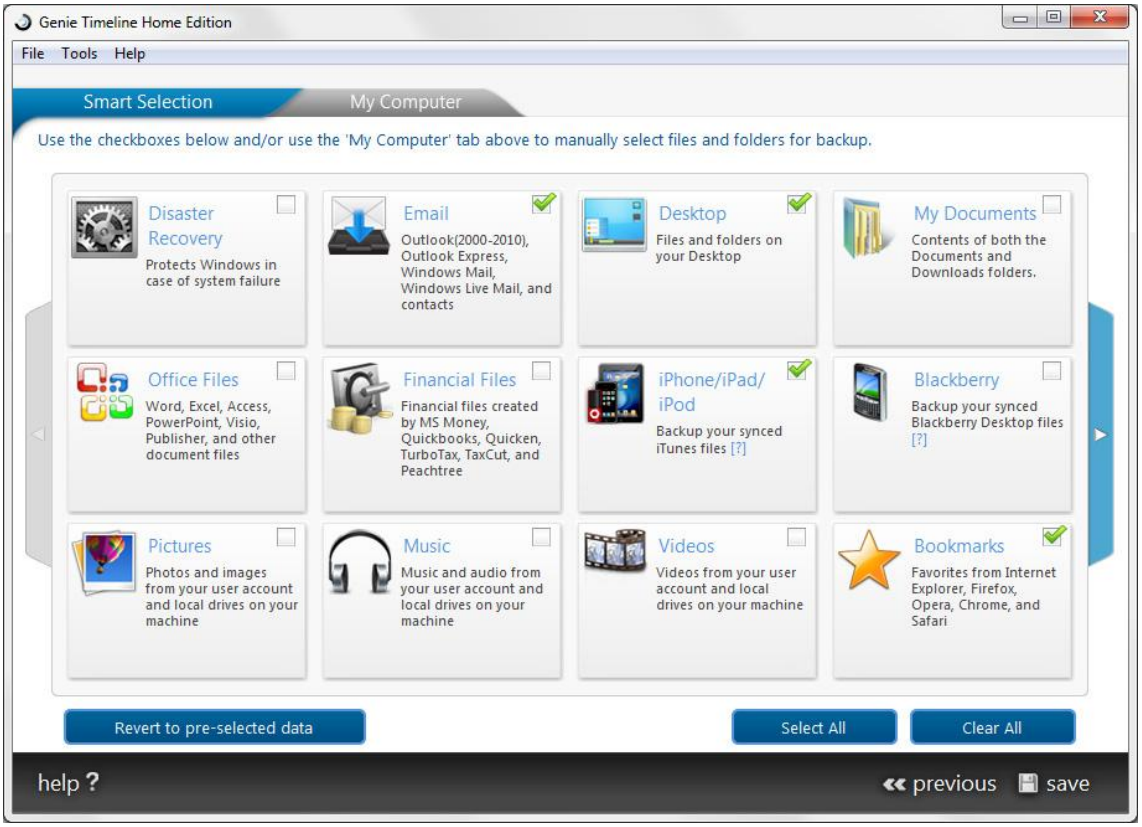
Muut varmennettaviksi halutut tiedostot, kuten dokumentit, varmuuskopioidaan myös viikoittain, mutta koska niiden muuttumistaajuus on huomattavasti valokuvakokoelmaa hitaampi, luodaan uusi täydellinen varmuuskopio vasta 12 lisäävän varmuuskopiokerran jälkeen. Käytännössä täydellinen varmuuskopio luodaan siis kolmen kuukauden välein. Varmuuskopiosukupolvia voidaan valokuvakokoelmaa pienemmän tilantarpeen vuoksi säilyttää useampia. Järjestelmässä säilytetään kymmenen täydellistä varmuuskopiosukupolvea, jolloin tietoja voidaan palauttaa edellisen kahden vuoden ajalta.

7.5.3 Jatkuva varmuuskopiointi

Järjestelmän normaalin varmuuskopioinnin tueksi haluttiin ottaa käyttöön ns. jatkuva varmuuskopiointimenetelmä. Sen tarkoituksena on entisestään vähentää tietojen menetyksen riskiä mahdollisissa ongelmatilanteissa. Jatkuvan varmuuskopioinnin tekniikka poikkeaa hieman muista menetelmistä, koska ensimmäisen täydellisen varmuuskopion luomisen jälkeen luodaan ainoastaan lisääviä varmuuskopioita. Ohjelmiston tarkoituksena on toimia automaattisesti taustalla koneen ollessa käytössä ja varmentaa tietojen muutokset lähes reaaliajassa tai käyttäjän valitsemin väliajoin. Varmennetut tiedostot muodostavat ajan myötä ns. aikajanan, jolle tiedostojen eri versiot sijoittuvat. Sen avulla voidaan siis palauttaa saman tiedoston eri versioita niiden muokkausajankohdan perusteella.

Mikäli työasemana toimisi Applen Mac-tietokone, olisi ohjelmiston valinta ollut helppo, koska Mac OS -käyttöjärjestelmään on sisäänrakennettu Time Machine-ohjelmisto, jonka avulla jatkuva varmuuskopiointi voidaan toteuttaa. Windows-koneissa tällaista ohjelmistoa ei vakiona ole, eli ainoaksi vaihtoehdoksi jäi kolmannen osapuolen ohjelman käyttäminen. Ohjelmavaihtoehtoja tutkittaessa kävi kuitenkin nopeasti ilmi, että markkinoilla ei ollut ilmaisohjelmistoja, joilla jatkuvan varmuuskopioinnin toteuttaminen onnistuisi. Ohjelmiston valinnan aikaan vain Genie Timeline tarjosi halutun toiminnallisuuden Windows-koneille. Sittemmin markkinoille on tullut Genie Timeline free, eli ilmainen, mutta rajoitettu versio edellä mainitusta ohjelmistosta (Genie9 2012.) sekä Altaro Oops!Backup (Altaro 2012.). Myös Comodo tarjoaa ilmaista Time Machine-ohjelmistoaan (Comodo 2012.), mutta se poikkeaa käyttötarkoitukseltaan muista ohjelmistoista ja soveltuu ennemminkin palautuspisteiden luomiseen, kuin tiedostojen jatkuvaan varmuuskopiointiin niiden muuttuessa. Ohjelmiston valinnan suhteen päädyttiin siis ostamaan Genie Timeline-lisenssi.

Genie Timelinen käyttöönotto ja toiminta on pyritty tekemään mahdollisimman yksinkertaiseksi. Käynnistettäessä ensimmäistä kertaa ohjelma kysyy varmuuskopioiden tallennusaseman, mitä tallennetaan ja käytetäänkö varmuuskopioiden säilytyksessä pakkausta. Tallennustilaksi valittiin ulkoinen 1 teratavun kiintolevy, joka annettiin kokonaisuudessaan ohjelman käyttöön. Tallennustilan säästämiseksi ohjelman ehdottamista varmuuskopioitavista tiedoista valittiin vain osa kuvan 8 mukaisesti.



Kuva 8. Genie Timeline varmennettavien tietojen valinta.

Varmistettaviksi tiedoiksi valittiin siis kuvatiedostojen lisäksi sähköpostit, työpöydällä olevat tiedostot, puhelimen tietokoneelle synkronoidut tiedot sekä selaimen kirjanmerkit. Ohjelman avulla voidaan myös toipua esim. Windowsin käynnistysongelmista. Tätä varten ohjelman avulla tehdään käynnistysmedia, jonka avulla käyttöjärjestelmän palauttaminen toimivaan tilaan on mahdollista. Koska esimerkkitapauksen työaseman käyttöjärjestelmä on jo varmennettu levykuvien avulla, ei Windows-varmennusta haluttu ottaa käyttöön tässä ohjelmistossa.

Ensimmäisen varmuuskopion luominen vei runsaasti aikaa, koska varmennettavaa tietoa oli melko paljon. Kun ensimmäinen varmennus on tehty, jää ohjelma taustalle tarkkailemaan muuttuneita tiedostoja. Mikäli ohjelman käyttöön annettu tallennustila on käytettävissä, pitää ohjelma varmuuskopion ajan tasalla tietyin väliajoin. Ohjelma osaa myös jäädä odottamaan varmuuskopioinnin suorittamista, mikäli tallennustila ei ole juuri sillä hetkellä käytettävissä. Kun tallen-

nustila palautuu käyttöön, aloittaa ohjelma varmuuskopioinnin automaattisesti. Valmistaja tarjoaa myös ilmaisen ohjelman iPhonelle, josta voidaan tarkastella varmuuskopioinnin edistymistä, tallennusmedian vapaata tilaa sekä saada tietoa eri tiedostotyyppien jakaumasta levyllä. Kommunikointi tapahtuu sähköpostin välityksellä, joten varmuuskopiointitilanteen seuraaminen onnistuu lähes mistä vain.

7.5.4 Etävarmuuskopiointi

Valokuvien etävarmuuskopioinnissa päätettiin käyttää hyväksi jo olemassa olevaa pankin tallelokeroa sekä ulkoista kiintolevyä. Pienemmät tiedostot haluttiin etävarmuuskopioida ilmaiseen Dropbox-pilvitallennuspalveluun.

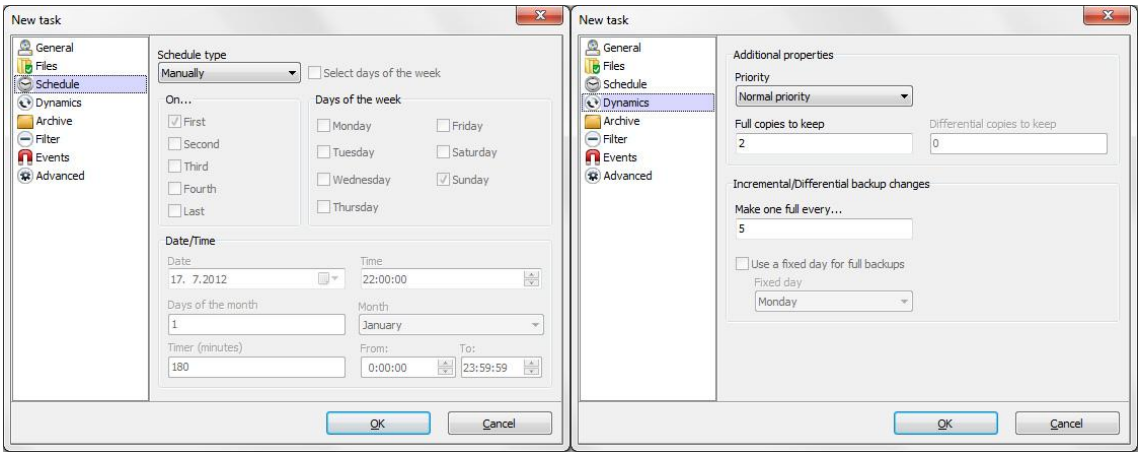
Valokuvien etävarmuuskopiointi

Varmuuskopioitavat valokuvat sekä Adobe Photoshop Lightroomin käyttämä kuvatietokanta eli katalogi muodostavat niin suuren tietomäärän, ettei sen varmentaminen pilvitallennuspalveluun ole järkevää. Vaikka markkinoilla onkin riittävän suuren kapasiteetin tarjoavia palveluja, ovat ne yleensä erittäin kalliita. Myös käytössä olevan ADSL-liittymän 1Mb:n nouseva kaista on rajoittava tekijä, sillä jo tämänhetkisen tietomäärän kopiointi kestäisi optiminopeudellakin reilusti yli viisi viikkoa.

Etävarmuuskopiointi päädyttiin suorittamaan kerran kuukaudessa, joten kiintolevy noudetaan jokaisen kuukauden ensimmäisenä pankin aukiolopäivänä tallelokerosta. Varmuuskopiointitaajuuden suhteen piti tehdä kompromissi varmennettavan tiedon kertymisen ja pankissa käymisen välillä. Mikäli valokuvia kertyy tulevaisuudessa nykyistä enemmän, voidaan varmennusväliä lyhentää esim. kahteen viikkoon.

Varmuuskopiointiohjelmassa luotiin tarkoitusta varten uusi tehtävä. Koska kuukauden ensimmäinen pankkipäivä kuitenkin vaihtelee ja levyn nouto ei välttämättä onnistu muiden menojen vuoksi aina samana päivänä, ei tehtävää voida suorittaa ajastetusti. Yhtä aikaa säilytettävien täydellisten varmuuskopioiden määrä rajoitettiin kahteen, koska tallennusvälineenä toimii vain yksi 1,5 terata-

vun ulkoinen kiintolevy. Samalla myös varmuuskopioiden sisältämää aikaväliä haluttiin pidentää siten, että tiedostoja on palautettavissa aina vähintään puolen vuoden ajalta. Täydellisen varmuuskopion jälkeen luodaan siis viisi lisäävää varmuuskopiota kuukauden välein, jonka jälkeen luodaan uusi täydellinen varmuuskopio. Näillä asetuksilla voidaan parhaimmillaan palauttaa ajankohdasta riippuen 6-11 kuukautta vanhoja tiedostoja. Kolmannen täydellisen varmuuskopion luonnin yhteydessä Cobian Backup poistaa automaattisesti vanhimman täydellisen- sekä viisi sen jälkeen luotua lisäävää varmuuskopiota levyltä (kuva 9).

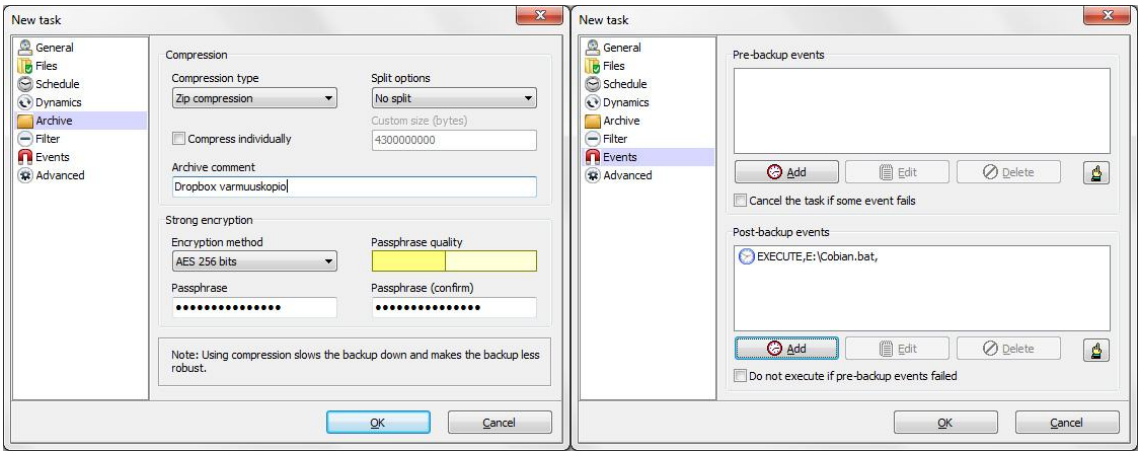


Kuva 9. Cobian Backup - Valokuvien etävarmuuskopioasetukset.

Muiden tiedostojen etävarmuuskopiointi

Pienemmät tiedostot kuten Word-dokumentit sen sijaan haluttiin varmentaa myös pilvitallennuspalvelun avulla. Koska käytössä oli jo ilmaista tallennustilaa Dropbox-palvelusta, haluttiin varmuuskopiot kohdistaa sinne. Cobian Backup ei tue suoraan varmuuskopioiden tallentamista Dropboxin kaltaisiin tallennuspalveluihin, mutta valmiiksi pakatun ja salatun varmuuskopion siirto palveluun onnistuu käyttämällä yksinkertaista bat-tiedostoa. Mikäli varmuuskopiota ei haluta pakata tai salata, onnistuu sen siirto Dropbox-kansioon myös suoraan. Salaamattoman tiedon siirtäminen tämäntyyppiseen tallennuspalveluun ei ole kuitenkaan suositeltavaa, joten varmuuskopiot toteutettiin pakattuina ja salattuina zip-tiedostoina.

Tätä tarkoitusta varten luotiin uusi varmuuskopiointitehtävä, joka eroaa tietyiltä osin muista tehtävistä. Tehtävä luo pakatun ja salatun varmuuskopiotiedoston väliaikaiseen hakemistoon, josta se siirretään Dropbox-kansioon yksinkertaisen bat-tiedoston avulla. Tiedostoista luodaan aina täydellinen varmuuskopio, koska Cobian Backup ei siirron jälkeen enää tiedä missä alkuperäinen tiedosto sijaitsee, eikä näin ollen pysty luomaan esim. lisäävää varmuuskopiota sarjaan. Yhtä aikaa säilytettäviksi asetettiin kaksi täydellistä varmuuskopiota, mutta asetuksella ei ole varsinaisesti merkitystä koska Cobian Backup ei pysty varmuuskopioversioita hallitsemaan. Vanhempia varmuuskopioita pitääkin poistaa käsin Dropboxista tallennustilan täyttyessä. Itse kopiointi toimii kuitenkin täysin automaattisesti, joten tehtävä ajastettiin luomaan varmuuskopio jokaisen kuukauden ensimmäisenä päivänä.



Kuva 10. Cobian Backupin Dropbox-asetukset.

Varmuuskopioiden pakkausasetuksista valittiin pakkausmuodoksi zip ja salausmetodiksi vahvin tarjottu AES 256bit salaus (kuva 10). Tässä vaiheessa syötetään myös kansiolle haluttu salasana kahdesti. Cobian Backup voi suorittaa mm. ulkopuolisia ohjelmia tai komentosarjoja ennen- tai jälkeen varsinaisen tehtävän suoritusta. Esimerkkitapauksessa haluttiin suorittaa varmuuskopion siirron hoitava bat-tiedosto heti varmuuskopioinnin jälkeen. Tehtävään tarvittava bat-tiedosto on hyvin yksinkertainen. Sen tarkoituksena on ainoastaan siirtää luotu varmuuskopiotiedosto move-käskyn avulla Dropbox-kansioon.

```
@echo off

move E:\Cobian\*.zip C:\Users\Admin\Dropbox\Backup
```

Tämä bat-tiedosto siis siirtää kaikki zip-päätteiset tiedostot kansiosta E:\Cobian järjestelmän Dropbox-kansioon.

7.5.5 Verkkosivuston varmuuskopiointi

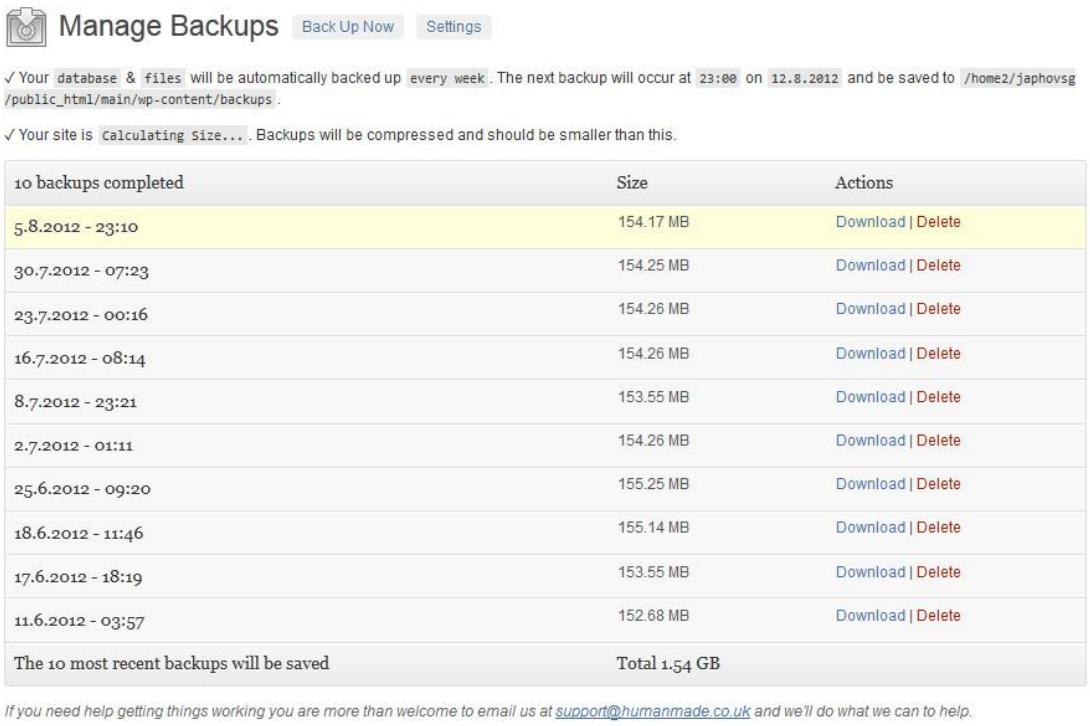
Vaikka useimpiin webhotellipalveluihin on sisällytetty palvelintasolla toimivia RAID- ja varmuuskopiointiratkaisuja, kannattaa sivustosta silti luoda itsenäisiä varmuuskopioita. Tällöin sivuston sisältö voidaan tallentaa myös muualle kuin palveluntarjoajan palvelimille. Ongelmatilanteista palautumisen lisäksi voidaan varmuuskopioiden avulla usein siirtää koko sivuston sisältö esim. uuden palveluntarjoajan palvelimelle. Verkkosivuston varmuuskopiointitapa riippuu pitkälti itse sivuston toteutustavasta. Niin sanotut sisällönhallintajärjestelmät tarjoavat yleensä mahdollisuuden automaattiseen ja ajastettuun varmuuskopiointiin joko suoraan hallintapaneelista tai erikseen ladattavan lisäosan avulla. Muussa tapauksessa varmuuskopionti voidaan suorittaa manuaalisesti käyttäen FTP-ohjelmistoa. Mikäli sivusto käyttää tietokantaa, pitää sekin varmuuskopioida muiden tiedostojen lisäksi. (WordPress 2012.)

Esimerkkitapauksessa verkkosivusto on toteutettu käyttämällä WordPress-sisällönhallintajärjestelmää. Sivuston varmuuskopiointi voidaan suorittaa manuaalisesti tai käyttäen automatisoitua varmuuskopiointiin tarkoitettua lisäosaa. Koska WordPress on avoin kehitysympäristö, on lisäosia tarjolla kymmenittäin. Lisäosat ovat myös yleensä ilmaisia, joten suurimmaksi ongelmaksi muodostuikin valinnan vaikeus.

Lisäosan valintaa rajattiin määrittelemällä siltä haluttuja ominaisuuksia:

- yksinkertaisuus, helppokäyttöisyys
- mahdollisuus automaattisiin varmuuskopioihin palvelimelle
- mahdollisuus käynnistää varmuuskopiointi manuaalisesti
- automaattisten varmuuskopioiden ajastusmahdollisuus.

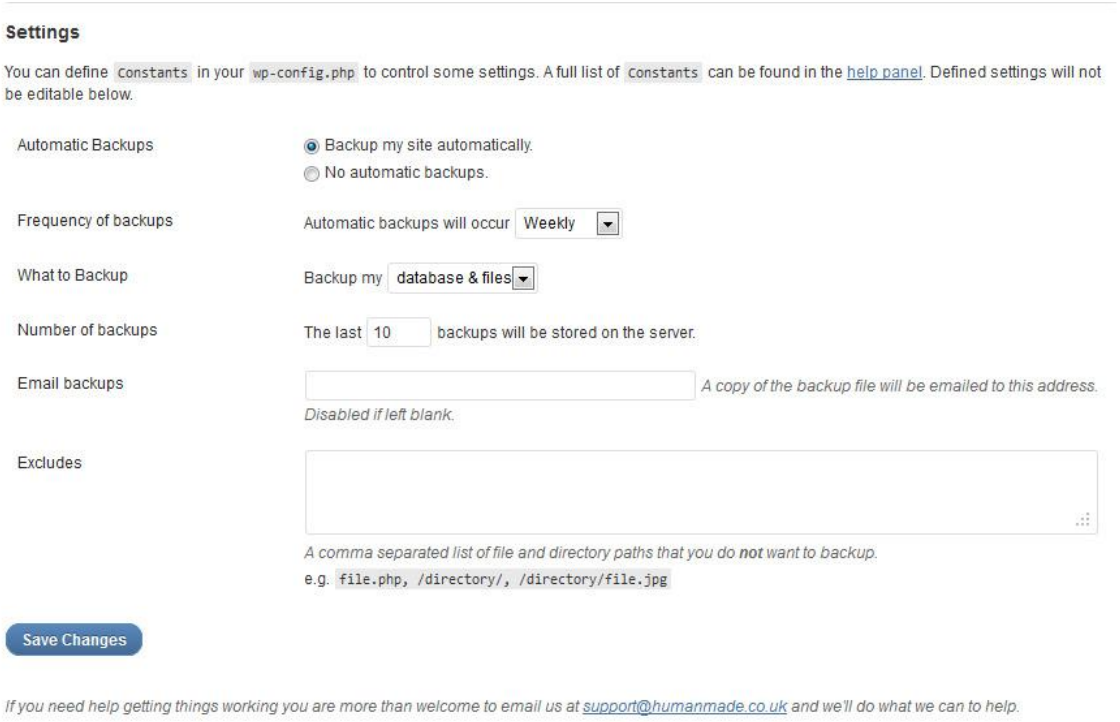
Valinnassa käytettiin myös apuna WordPressin omaa lisäosahakemistoa, josta löytyy käyttäjien arvosteluja sekä kommentteja ko. lisäosista. Lisäosa nimeltä BackUpWordPress sisälsi kaikki halutut ominaisuudet ja oli saanut hyviä arvosteluita muilta käyttäjiltä, joten sivuston varmuuskopiointi päätettiin toteuttaa sen avulla. Valittu lisäosa integroituu täydellisesti WordPressin hallintapaneeliin ja on erittäin helppokäyttöinen. Lisäosan asetuksia ei ole edes välttämätöntä säätää asennuksen ja käyttöönoton jälkeen. Oletusarvoisesti sivusto varmennetaan automaattisesti kerran viikossa ja palvelimella säilytetään kymmenen viimeisintä varmuuskopiota.



Kuva 11. BackUpWordPress-käyttöliittymä.

BackUpWordPressin käyttöliittymän yläosan painikkeilla voidaan käynnistää varmuuskopiointi manuaalisesti tai siirtyä asetusruutuun (kuva 11). Sieltä nähdään myös, mitkä tiedot on valittu sisällytettäviksi varmuuskopioihin ja kuinka usein ne varmennetaan. Myös seuraavan varmennuksen ajankohta, tallennussijainti palvelimella sekä sivuston koko on helposti nähtävillä. Näiden tietojen alla on taulukko viimeisestä kymmenestä varmuuskopiosta. Varmuuskopioita voi-

daan poistaa tai ladata palvelimelta omalle koneelle käyttämällä oikean reunan painikkeita.



Kuva 12. BackUpWordPressin asetukset.

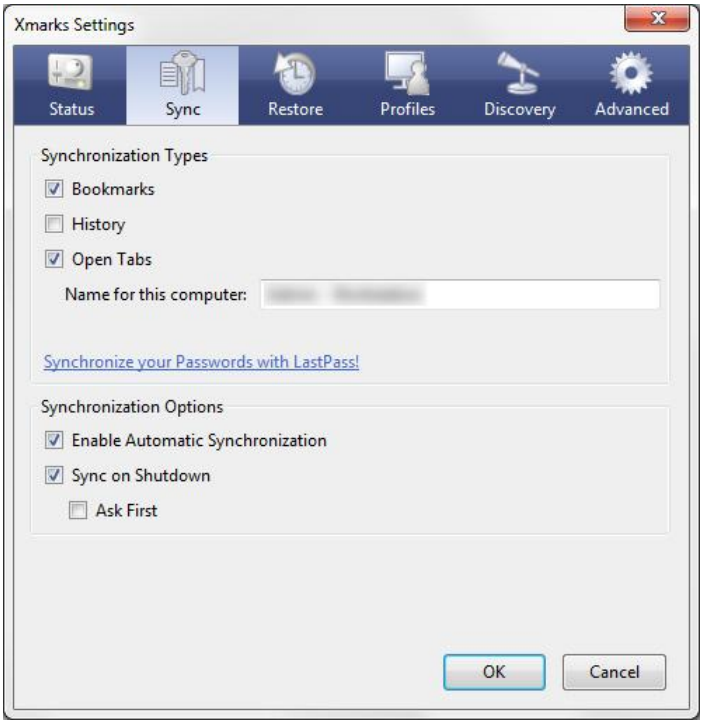
Asetuksista voidaan säätää automaattiset, ajastetut varmuuskopiot päälle tai pois sekä ajastaa ne halutulla tavalla (kuva 12). Varmuuskopioihin voidaan myös sisällyttää pelkät tiedostot, pelkkä tietokanta tai kummatkin. Oletusarvoisesti palvelimella säilytetään kymmenen viimeistä varmuuskopiota, mutta ohjelma antaa käyttäjälle mahdollisuuden itse asettaa haluttujen varmuuskopioiden määrän. Määrän vähentäminen saattaa olla järkevää, mikäli sivuston koko on suuri ja palvelintila on rajoitettu. Otetut varmuuskopiot on myös mahdollista lähettää sähköpostitse haluttuun osoitteeseen, mutta sivuston ollessa vähänkin suurempi, ei tätä mahdollisuutta kannata käyttää. Excludes-kohdan avulla on mahdollista määrittää halutut tiedostot tai hakemistot siten, että niitä ei sisällytetä lainkaan varmuuskopioihin. (Humanmade 2012.)

7.5.6 Kirjanmerkkien varmuuskopiointi ja synkronointi

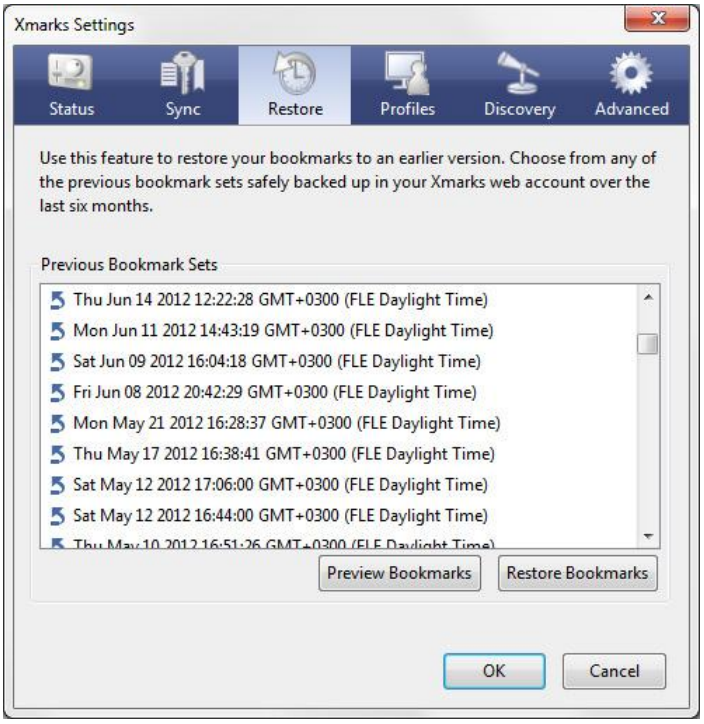
Kirjanmerkkien varmuuskopiointi saattaa vaikuttaa mitättömältä asialta, mutta ahkeran Internetin käyttäjän selaimen kirjanmerkkeihin on saattanut kertyä arvokkaita tietolähteitä useiden vuosien ajalta. Nämä kirjanmerkit on yleensä hieman selaimesta riippuen mahdollista tallentaa html-tiedostoksi, jonka avulla ne voidaan myös palauttaa tai siirtää toiseen selaimeen. Tätä tapaa ei kuitenkaan pysty helposti automatisoimaan. Koska kirjanmerkkeihin on kertynyt paljon hyödyllisiä linkkejä, haluttiin ne saada käyttöön myös muissa laitteissa sekä tarvittaessa myös käytettäessä vieraita koneita.

Kohdejärjestelmässä otettiin käyttöön Xmarks-niminen ilmaispalvelu, joka on käytännössä pilvitallennus- ja synkronointipalvelu kirjanmerkeille. Palveluun luodaan salasanasuojattu tili, johon Xmarksin selainlaajennus tallentaa kirjanmerkit. Laajennus tukee yleisimpiä selaimia, eli eri laitteiden välillä ei tarvitse välttämättä käyttää samaa selainta (kuvat 13-15).

Kuva 13. Xmarks-selainlaajennus.



Kuva 14. Xmarks-asetukset.



Kuva 15. Xmarks-varmuuskopiot.

Xmarks toimii automaattisena varmuuskopiointiohjelmana varmentaen kirjanmerkit aina, kun selain suljetaan. Sen avulla voidaan synkronoida myös avoimena olevat selaimen välilehdet sekä selainhistoria, joka tosin on käytettävissä ainoastaan Firefox-selainten välillä. Kaikki luodut varmuuskopiot säilytetään edellisen kuuden kuukauden ajalta ja restore-välilehdeltä voidaan tarkastella sekä palauttaa vanhoja kirjanmerkkejä päivämäärien sekä ajankohtien mukaan. Palveluun voidaan kirjautua myös selaimen kautta, jolloin omat kirjanmerkit saadaan käyttöön myös vierailla koneilla. (Xmarks 2012.)

8 POHDINTA

Opinnäytetyön toteutus oli monellakin tapaa mielenkiintoinen ja opettavainen prosessi. Aihevalintana tiedonvarmennusjärjestelmien käsittely oli omalta kohdaltani varsin onnistunut, sillä työ motivoi pohtimaan tietojen arvoa ja tärkeyttä paitsi yleisellä tasolla, myös omassa järjestelmässäni. Mietin mitä tapahtuisi mikäli nämä tiedot häviäisivät ja ennen kaikkea, miten voisin parhaani mukaan estää näitä tietoja koskaan häviämästä.

Tärkeiden tietojen häviäminen on aina vahingollista ja näiden tietojen häviämiseen johtavat riskit olivat hyvinkin tiedossa omien kokemusteni kautta jo ennen kirjoitusprosessin alkua. Tästäkin huolimatta huomasin, että laiskuus ja vääränlainen luottamus omiin laitteistoihin olivat ottaneet vallan omassa järjestelmässäni. Vaikka tiedonvarmennuksen konsepti olikin jollain tasolla ollut aina tiedossa, en ollut silti koskaan syventynyt tarkastelemaan aihetta suurempana kokonaisuutena. Ennen olin toteuttanut kokonaisuudesta vain pieniä, yksittäisiä osia varmuuskopioimalla vain tiettyjä tiedostoja ja usein melko vaihtelevin väliajoin.

Itse tutkimustyö oli melko haasteellista, koska kirjallista materiaalia löytyi aiheesta varsin vähän ja sekin oli pääasiassa englanninkielistä. Englanninkielisyys itsessään ei haitannut, mutta kirjojen saatavuus Suomesta oli melko rajoitettua. Ylivoimaisesti suurimman osan työn lähteistä muodostivatkin verkkolähteet, joiden valinnassa pyrin harjoittamaan lähdekritiikkiä tarkastamalla tiedot myös mahdollisista muista lähteistä ennen ko. lähteen hyväksymistä. Koska käsitellyt aiheet olivat suurimmaksi osaksi minulle tuttuja, nojasin lähdekritiikin osalta myös omiin tietoihini ja kokemuksiini.

Oman haasteensa toivat myös työn teoriaosuudessa käsiteltävät aihealueet. Koska ne ovat tiiviisti yhteyksissä toteutetun tiedonvarmennusjärjestelmän kanssa, piti kirjoitustyön edetessä miettiä etukäteen myös empiirisen osuuden vaikutusta aihevalintoihin ja käytännössä varmennusjärjestelmä piti hahmotella jo ennen kirjoitustyön aloittamista.

Toteutetun varmennusjärjestelmän punaisena lankana toimivat kustannustehokkuus ja yksinkertaisuus, mutta kuitenkin siten, että järjestelmän kattavuudesta ei tarvinnut tinkiä. Tarvittavia ohjelmistoja pyrittiin karsimaan määrittelemällä melko tarkasti niiltä halutut ominaisuudet, mutta empiirisen osuuden suurin työmäärä muodostui silti ohjelmistotestauksesta. Myös Linux-palvelimiin tutustuminen vei oman aikansa, koska lukuun ottamatta muutamaa Ubuntun työpöytäversion testiasennusta ei minulla ollut Linux-käyttökokemusta juuri lainkaan. Itse järjestelmän saattaminen käyttökuntoon oli melko yksinkertaista pitkälti hyvin toteutetun suunnitteluvaiheen ansiosta.

Varmennusjärjestelmä on tätä kirjoitettaessa toiminut ongelmattomasti noin puolen vuoden ajan. Puuta koputellen voidaan todeta, että lukuunottamatta kerran tehtyä käyttöjärjestelmän uudelleenasennusta levykuvista, ei varmennusjärjestelmää ole vielä tarvittu ongelmatilanteista palautumiseen. Pääasia onkin ollut mielenrauhan saavuttaminen ja tietoisuus siitä, että mahdollisiin ongelmatilanteisiin on varauduttu niin hyvin kuin käytössä olevien resurssien puitteissa on mahdollista.

LÄHTEET

Altaro 2012. Oops!Backup. Viitattu 5.8.2012 http://www.altaro.com/home-pc-backup/.

Ascomp 2012. Backup Maker overview. Viitattu 3.8.2012 https://www.ascomp.de/products/show/product/backupmaker/tab/details.

Bitreplica 2012. What is Bitreplica? Viitattu 4.8.2012 http://www.bitreplica.com/.

Cobiansoft 2012. Cobian Backup. Viitattu 4.8.2012 http://www.cobian.se/cobianbackup.htm.

Comodo 2012. Comodo Time Machine. Viitattu 5.8.2012 http://www.comodo.com/home/backup-online-storage/data-recovery.php.

Datpro Oy 2011. Mitä ”Master Data” on? Viitattu 23.7.2011 http://www.datpro.fi/yritys/mitae-master-data-on.

Duplicati 2012. Duplicati. Viitattu 4.8.2012 http://www.duplicati.com/.

FBackup 2012. FBackup 4.8. Viitattu 3.8.2012 http://www.fbackup.com/.

Genie9 2012. Genie Timeline Home 2012. Viitattu 5.8.2012 http://www.genie9.com/home/Genie_Timeline_Home/overview.aspx.

Gite, V. 2009. Software vs. hardware RAID. Viitattu 18.6.2012 http://www.cyberciti.biz/tips/raid-hardware-vs-raid-software.html.

Hard disk drive 2012. Wikipedia. Viitattu 20.6.2012 http://en.wikipedia.org/w/index.php?title=Hard_disk_drive&oldid=500087839.

Hayes, F. 2003. The history of RAID. Viitattu 19.5.2012 http://www.computerworld.com/s/article/87093/The_Story_So_Far.

Hewlett Packard 2012. QuickSpecs - HP Smart Array P822 Controller. Viitattu 3.6.2012 http://h18006.www1.hp.com/products/quickspecs/14341_div/14341_div.pdf.

Humanmade 2012. BackUpWordPress. Viitattu 4.7.2012 http://hmn.md/backupwordpress/.

Järvinen, P. 2002. Tietoturva & yksityisyys. Jyväskylä: Docendo.

Kay, R. 2010. Flash memory. Viitattu 28.5.2012 http://www.computerworld.com/s/article/349425/Flash_Memory.

Kayne, R. 2012. What is a disk image? Viitattu 22.4.2012 http://www.wisegeek.com/what-is-a-disk-image.htm.

Keriver 2011. Keriver 1-Click Restore Free 3.0. Viitattu 27.4.2012 http://www.keriver.com/.

Kyrnin, M. 2012. What is RAID. Viitattu 20.5.2012 http://compreviews.about.com/od/storage/l/aaRAIDPage1.htm.

Laakso, M. 2011. Jatkuvuus- ja toipumissuunnitelman laatiminen. Viitattu 18.1.2012 http://www.tietojesiturvaksi.fi/content/jatkuvuus-ja-toipumissuunnitelman-laatiminen.

Laaksonen, M.; Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja: ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita.

Leikomaa, M. 2005. Cibernarium-projekti Tietoturva 2. Viitattu 25.1.2012 http://www.cibernarium.tamk.fi/tietoturva2/varmuuskopiointi.htm.

Microsoft 2012. Windows deployment services. Viitattu 25.4.2012 http://www.microsoft.com/en-us/server-cloud/windows-server/windows-deployment-services-wds.aspx.

Mitchell, B. 2012. Introduction to NAS – Network Attached Storage. Viitattu 6.5.2012 http://compnetworking.about.com/od/itinformationtechnology/l/aa070101a.htm.

Moilanen, T. 2004. SAN – Storage Area Network. Viitattu 4.3.2012 http://www2.it.lut.fi/kurssit/03-04/010626000/palautukset/Seminaarit/SAN-SeminaariEsitys.pdf.

Ocster 2012. Ocster Backup freeware Windows edition. Viitattu 3.8.2012 http://www.ocster.com/ocster-backup-freeware/en.

Raggad, B. G. 2010. Information Security Management. Concepts and Practice. Boca Raton: CRC Press.

Redobackup 2012. Redo Backup and Recovery. Viitattu 28.4.2012 http://redobackup.org/.

Rhee, E. 2011. How to securely erase an SSD drive. Viitattu 18.6.2012 http://howto.cnet.com/8301-11310_39-20115106-285/how-to-securely-erase-an-ssd-drive/.

Secmeter 2008. Varmuuskopiointi. Viitattu 16.7.2011 http://www.secmeter.com/varmuuskopiointi.html.

Shultz, G. 2011. Use Windows 7 system image recovery to restore a hard disk. Viitattu 27.4.2012 http://www.techrepublic.com/blog/window-on-windows/use-windows-7-system-image-recovery-to-restore-a-hard-disk/4644.

Spector, L. 2008. Reinstall and restore your Windows PC in eight easy steps. Viitattu 18.4.2012 http://www.pcworld.com/businesscenter/article/155995/reinstall_and_restore_your_windows_pc_in_eight_easy_steps.html.

Spector, L. 2010. Move to a new hard drive. Viitattu 25.4.2012 http://www.pcworld.com/article/199279/move_to_a_new_hard_drive.html.

Stanek, W. R. 2001. Windows 2000 – Verkonhaltijan käsikirja. Helsinki: Edita.

Suutari, T. 2011. Pitkäaikaissäilytys. Viitattu 15.5.2012 http://www.digiwiki.fi/fi/index.php?title=Pitk%C3%A4aikaiss%C3%A4ilytys.

Symantec 2009. Hot imaging with Ghost solution suite 2.5. Viitattu 26.4.2012 http://www.symantec.com/docs/TECH110158.

Thomas, T. 2012. What is cold imaging backup? Viitattu 26.4.2012 http://data-backup-software-review.toptenreviews.com/what-is-cold-imaging-backup.html.

Tietosuojavaltuutetun toimisto 2010. Asiaa tietosuojasta 1/2005 – Henkilötietojen siirto ulkomaille henkilötietolain mukaan. Viitattu 22.4.2012 http://www.tietosuoja.fi/uploads/7nr20lwabx4vu.pdf.

Viitanen, A. 2004. RAID. Viitattu 16.6.2012 http://www.cs.uta.fi/tarkki/suoritus/luennot/raid.html.

Virmajoki, O. 2011. Tietoturvan peruskäsitteet. Viitattu 4.7.2011 http://gallia.kajak.fi/opmateriaalit/yleinen/ViOl/Tietoturva/Tietoturvan%20perusk%C3%A4sitteit%C3%A4.pdf.

Vähimaa, A. 2010. Nettijatko Tieto linjoille vaivatta 8/2010. Viitattu 19.4.2012 http://www.mbnet.fi/artikkeli/nettijatkot/nettijatko_tieto_linjoille_vaivatta_8_2010.

WordPress 2012. WordPress backups. Viitattu 4.7.2012 http://codex.wordpress.org/WordPress_Backups.

Xmarks 2012. Features overview. Viitattu 5.7.2012 http://www.xmarks.com/about/features.