Varmuuskopiointipalvelun suunnittelu ICT-yritykselle

Dmitry Sinyavskiy

Haaga-Helia ammattikorkeakoulu

Tradenomi (AMK), tietojenkäsittely

Amk-oppinäytetyö

2023

Tiivistelmä

Tekijä(t)
Dmitry Sinyavskiy

Tutkinto
Tradenomi (AMK), tietojenkäsittely

Raportin/Opinnäytetyön nimi
Varmuuskopiointipalvelun suunnittelu ICT-yritykselle

Sivu- ja liitesivumäärä
35 + 0

Varmuuskopioinnilla ja palautuksella viitataan prosesseihin ja toimenpiteisiin, jotka liittyvät digitaalisten tietojen, tiedostojen tai järjestelmien kopioiden luomiseen ja tallentamiseen, jotta ne voidaan suojata tietojen katoamiselta tai vioittumiselta ja palauttaa ne mahdollisen katastrofin tai vian sattuessa.

Varmuuskopioinnilla tarkoitetaan prosessia, jossa tiedoista tai järjestelmästä tehdään kopio joko manuaalisesti tai automaattisesti erilliseen tallennuslaitteeseen tai pilvipohjaiseen palveluun. Varmuuskopioinnilla suojataan tietojen katoamista vahingossa poistamiselta, järjestelmän kaatumiselta, laitteistovialta, kyberhyökkäyksiltä, luonnonkatastrofeilta tai muilta odottamattomilta tapahtumilta. Palauttamisella taas viitataan prosessiin, jossa varmuuskopiotiedot tai järjestelmä palautetaan alkuperäiseen tilaan, jos alkuperäiseen tietoon tai järjestelmään ei päästä käsiksi tai se vioittuu. Palautus voidaan toteuttaa useilla menetelmillä, mukaan lukien palauttaminen varmuuskopiotiedostoista, tietojen uudelleenrakentaminen ylimääräisistä kopioista tai erikoistuneen tietojen palautusohjelmiston avulla. Tehokkaat varmuuskopiointi- ja palautusstrategiat ovat ratkaisevan tärkeitä tärkeiden digitaalisten omaisuuserien ja järjestelmien eheyden ja saatavuuden ylläpitämisessä sekä liiketoiminnan jatkuvuuden varmistamisessa odottamattomien katastrofien tai häiriötilanteiden varalta.

IT-Futura Oy on ICT-alan suhteellisen nuori yritys, joka luotiin tätä oppinäytetyötä varten eikä ole olemassa oleva yritys. Oppinäytetyössä pyritään luoda IT-Futura Oy:lle varmuuskopiointipalvelu, joka olisi luotettava ja helppokäyttöinen sekä yrityksen ympäristöön ja tarpeisiin mukautuva. Lisäksi varmuuskopiointisuunnitelmaan on pystyttävä lisätä pilvitallennustilaa sekä ulkoista tallennustilaa. Oppinäytetyössä tutkitaan minkälaiset tallennusmediat sopivat IT-Futura Oy:n varmuuskopiointipalvelun tarpeisiin. Lisäksi tutkitaan sitä, miten erilaiset tallennusmenetelmät ja varmuuskopiointiohjelmat sopivat palveluun. IT-Futura Oy -yritys työllistää kolme henkilöä, joiden työhön kuuluu vanhemman sukupolven auttaminen heidän teknologisten laitteiden kanssa, kun he eivät itse osaa tai kykene siihen ja joilla ei ole mahdollisuutta matkustaa tai liikkua itse tullakseen toimistolle tai korjaamolle asti. Yritys käsittelee henkilökohtaisia tietoja, kuten nimiä, osoitteita ja yhteystietoja. IT-Futura varmuuskopioi siis asiakasrekisteriä ja omia sisäisiä asiakirjoja. Kyseinen varmuuskopiointisuunnitelma tehdään vain IT-Futura yritykselle ottaen huomioon sen tarpeet, eikä varmuuskopiointisuunnitelma koske yrityksen asiakkaita. IT-Futura Oy:lle valmistettu varmuuskopiointipalvelu sopii hyvin ICT-alan yritykselle ottaen huomioon sen tarpeet, datamäärä ja budjetti. Sitä voi tarvittaessa mukauttaa IT-Futura Oy:n tarpeiden mukaiseksi ja sen avulla pystyy täysin automatisoimaan varmuuskopiointi, jolloin eliminoituu mahdollisuus inhimillisiin virheisiin, kuten esimerkiksi vahingossa poistaminen. Lisäksi varmuuskopioinnin luotettavuus kasvaa, sillä se on ajastettu tehtäväksi päivittäin ja kopiot tallennetaan sekä pilvipalveluun että verkkolevylle.

Asiasanat
Varmuuskopiointi, tietojen palautus, tietoturva, tallennusmediat

Sisällys

1 Johdanto

Oppinäytetyön tavoitteena on suunnitella varmuuskopiointipalvelu ICT-alan yritykselle, IT-Futura Oy:lle, joka oli luotu tätä oppinäytetyötä varten, eikä ole olemassa oleva yritys. Kyseinen yritys työllistää kolme henkilöä, joiden työhön kuuluu vanhempien ihmisten auttaminen heidän teknologisten laitteiden kanssa, kun he itse eivät osaa tai kykene siihen. IT-Futuran henkilöstö käy paikan päällä esimerkiksi heidän kotonansa tekemään tarvittavat työt, jolloin asiakkaiden ei tarvitse itse matkustaa toimistolle asti. Työnä voi olla esimerkiksi puhelimen tai tietokoneen ohjelmien päivitysten teko, uusien ohjelmien asentaminen, virusten poistot ja vanhojen ohjelmien tai tiedostojen puhdistaminen/poistaminen.

Varmuskopiointi on prosessi, jonka avulla tarvitsemista tiedoista luodaan kopio, joka suojaa haitalliselta tai tahattomalta poistamiselta, laitteistovialta, kiristyshaittaohjelmilta sekä muilta tietojen katoamiselta. Tietojen varmuuskopiointi on mahdollista toteuttaa paikallisesti, ulkopuolelta tai käyttäen molempia tapoja samaan aikaan. Ulkopuolinen tietojen varmuuskopiointi on minkä tahansa liiketoiminnan jatkuvuuden/katastrofistrategian kriittinen osa. Varmuuskopioinnin ja tietoturvan avulla voidaan ehkäistä tapahtumasta yrityksen monia mahdollisia massiivisia vahinkoja. Näiden asioiden ollessa kunnossa, yrityksen toiminta voi keskittyä omaan kehittymiseen kyseisten ongelmien ratkaisemisen sijaan. Tietojen palautus/restaurointi (restoring) prosessi tunnetaan palautuksena (recovery), jonka avulla haetaan tarvittavia tietoja varmuuskopiosta. Tämä voi tarkoittaa tietojen kopioimista/siirtämistä varmuuskopiomedialta jo olemassa olevaan laitteeseen tai uuteen laitteeseen. Toisiaan se voi myös viitata tietojen kopioimista pilvestä paikalliseen koneeseen/laitteeseen tai yhdestä pilvestä toiseen (Burton 2020).

Oppinäytetyön tavoitteena on luoda IT-Futura Oy:lle varmuuskopiointipalvelu, joka olisi luotettava ja helppokäyttöinen sekä yrityksen ympäristöön ja tarpeisiin mukautuva. Lisäksi varmuuskopiointisuunnitelmaan on pystyttävä lisätä pilvitallennustilaa sekä ulkoista tallennustilaa. IT-Futura Oy on nuori yritys, jolla on pieni asiakaspohja ja suhteellisen pieni budjetti alkuun, minkä takia varmuuskopiointipalvelu on suunniteltava siten, että loppuaan lopuksi se ei maksaisi liikaa ja yritys pystyisi kustantamaan sen. Varmuuskopiointipalveluun tulee kuulumaan pilvipalvelun-, ohjelmiston- ja välineiden valinta sekä lyhyet ohjeet ohjelman asennukseen ja konfigurointiin.

Oppinäytetyössä tutkitaan minkälaiset tallennusmediat sopivat IT-Futura Oy:n varmuuskopiointipalvelun tarpeisiin. Lisäksi tutkitaan sitä, miten erilaiset tallennusmenetelmät ja varmuuskopiointiohjelmat sopivat palveluun. Oppinäytetyö koostuu kahdesta osasta, jossa ensimmäisessä käsitellään varmuuskopioinnin teoriaa ja toisessa itse varmuuskopiointisuunnitelman luominen näiden pohjatietojen avulla.

2 Varmuuskopiointi

2.1 Varmuuskopiointi käsitteenä

Varmuuskopiointi on prosessi, jonka avulla kopioidaan virtuaalisia tiedostoja tai tietokantoja varmuuskopiointipaikkaan, jos alkuperäiset tiedot katoavat tai vioittuvat (Acronis 2022). Varmuuskopiointi on siis suojamekanismi haitalliselta tai tahattomalta poistamiselta, laitteistovialta, kiristyshaittaohjelmilta sekä muilta tietojen katoamiselta (Burton 2020). Varmuuskopiointimenetelmällä tässä työssä tarkoitan kolmea eri tapaa järjestelmän tiedoista varmuuskopion ottamista. Jokaisella varmuuskopiointiohjelmalla on oma lähestymistapansa varmuuskopion suorittamiseen, mutta suurimmassa osassa ohjelmista on käytössä kolme yleistä varmuuskopiointimenetelmää: täysi (engl. full) varmistus, inkrementaalinen (engl. incremental) varmistus sekä differentiaalinen (engl. differential) varmistus. Varmuuskopiosta voidaan lisäksi käyttää termejä Online, Near-line ja Offline, jotka liittyvät varmuuskopioiden viiveeseen tai saatavuuteen (Rao&Nyak 2014, 264.).

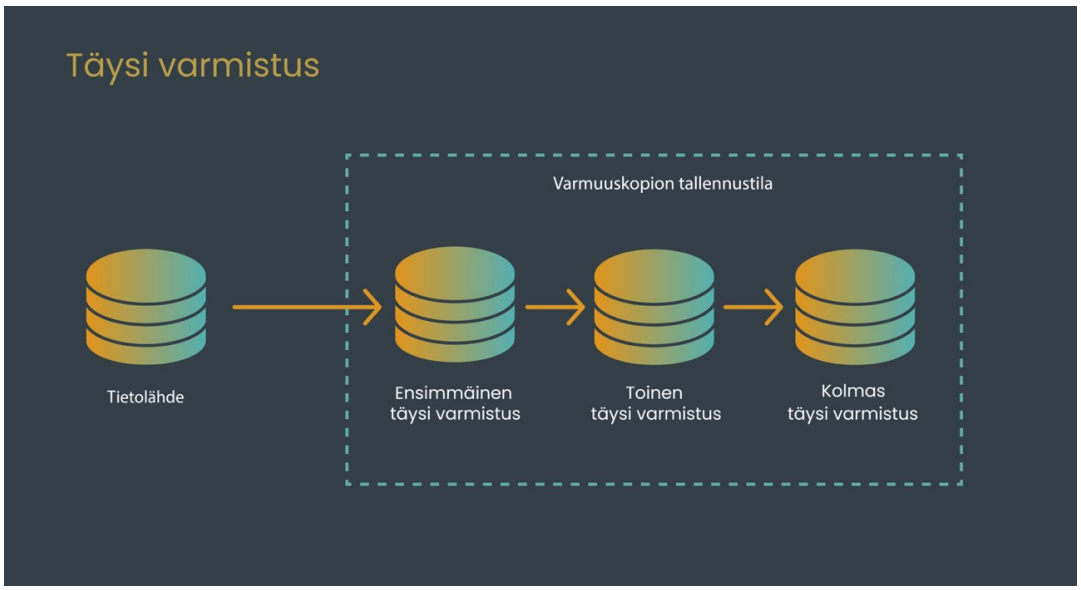
Tietojen varmuuskopiointi on mahdollista toteuttaa paikallisesti, ulkopuolelta tai käyttäen molempia tapoja samaan aikaan (Acronis 2022). Ulkopuolinen tietojen varmuuskopiointi on minkä tahansa liiketoiminnan jatkuvuuden/katastrofistrategian avainkomponeinteista, koska mikään ei kestä ikuisuuden, etenkin kun kyse on ajan myötä kuluvista laitteiston osista, kuten tietokoneista ja ulkoisista kiintolevyistä. Tästä syystä säännöllinen varmuuskopiointi on todella tärkeää ja sitä suunniteltaessa on otettava huomioon, minkälaista dataa on tarkoituksena varmistaa.

2.1.1 Täysi varmistus

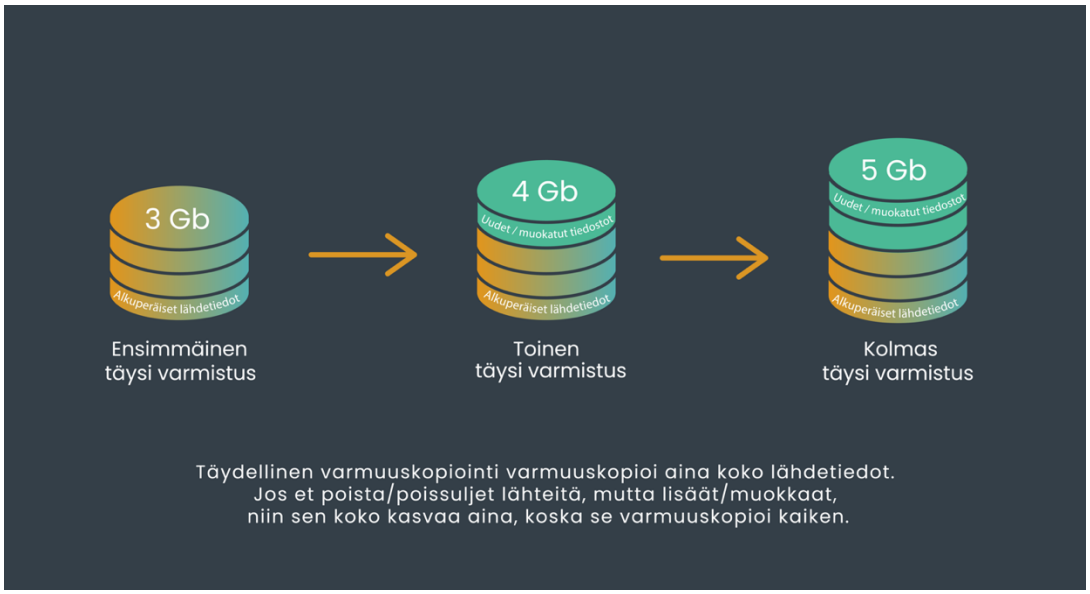
Nimensä mukaisesti, täysi varmistus koostuu identtisen kopion luomisesta kaikista valituista tiedostoista, kansioista ja muusta tiedosta Täysvarmistuksen tekeminen kestää kauemmin ja se vie enemmän resursseja sekä tallennustilaa verrattuna muihin varmuuskopiointimenetelmiin, mutta menetelmältään se on kattavin vaihtoehto, mikä tekee siitä yleisimmän varmuuskopiointimenetelmän. Täysvarmistuksen vahvuutena on siis se, että yhdessä paikassa sijaitsee kattava kopio kaikista tiedoista, jonka palauttaminen ei vie paljon aikaa. Lisäksi menetelmän hyvänä puolena on erilaisten varmuuskopioiden ylläpidon ja palauttamisen helppous (Drake 2022).

Täysvarmistuksen myöhemmät kopiot luodaan samassa koossa eli täyskopioina (Backup4all 2022a). Jos esimerkiksi lähdetietojen koko on 100 Gt niin seitsemän kokonaista kopiota/täyskopiota tekevät arkistoon yhteensä 700 Gt (Kuva 1). Mutta tämä pitää paikkansa vain jos mitään dataa ei poisteta/poissuljeta eikä lisätä uutta/muokattua dataa. Jos siis mitään ei

poisteta/poissuljeta, mutta dataa lisätään, niin täysvarmistuksen kopio tulee kasvamaan koossa, koska se varmuuskopioi kaiken (Kuva 2).



Kuva 1. Täysi varmistus



Kuva 2. Lisätietoa täydestä varmistuksesta

2.1.2 Inkrementaalinen varmistus

Inkrementaalinen varmuuskopiointi on nopeampi tapa varmuuskopioida tiedot kuin toistuvan täysvarmuuskopioinnin suorittaminen. Kyseisen varmuuskopiointimenetelmä sisältää vain tiedostot, joita on muokattu viimeisen varmuuskopioinnin jälkeen. Siitä se saakin nimensä, inkrementaalinen varmuuskopiointi, jossa jokainen varmuuskopio on edellisen varmuuskopion lisäys eli

inkrementaali (Backup4all 2022b). Kuvassa kolme näkyy, miltä näyttää neljä kertaa suoritettu varmuuskopiointi käytettäessä inkrementaalista varmuuskopiointia (Kuva 3).

Inkrementaalinen varmuuskopiointiprosessi voi olla erittäin nopea, ja tarvittava tallennuskapasiteetti on melko pieni verrattuna differentiaaliseen varmuuskopiointiin tai täydelliseen varmuuskopiointiin (Backup4all 2022b). Jos täysi varmuuskopio oli 50 gigatavua, asteittainen muutos päivästä toiseen saattaa olla esimerkiksi 1 gigatavu. Varmuuskopioinnista vastaavan johtajan on päätettävä, kuinka usein on tehtävä porraskopioita. Se voi olla päivittäin tai viikoittain tai jopa tunnin välein. Se riippuu siitä, kuinka paljon muutoksia tiedoissa tapahtuu ja kuinka kriittistä se on liiketoiminnan jatkamisen kannalta. Jos esimerkiksi yritys on huolissaan oman verkon kapasiteetista tai tallennustilasta, asteittainen varmuuskopiointi on paras valinta.

Inkrementaalisen varmuuskopiointiprosessin palautumisaika voi olla pidempi verrattuna differentiaaliseen prosessiin. Koska inkrementaalisen prosessin aikana luodaan enemmän varmuuskopioita, jokainen varmuuskopion kirjaus muuttuu edellisestä varmuuskopiosta, joten kaiken yhdistäminen takaisin yhteen vie aikaa. Joten nopean varmuuskopiointiajan etu kompensoituu pidemmällä palautusajalla (Backup4all 2022b).

Kaiken kaikkiaan lisävarmuuskopiot ovat hyviä organisaatioille, jotka tarvitsevat joustavuutta ja lyhyitä aikajaksoja varmuuskopioiden välillä. Inkrementaalisessa varmuuskopionnissa kopioidaan vähemmän tietoa, "Backup window" eli varmuuskopiointi-ikkuna on lyhyempi ja tiedostot ovat pienempiä. Varmuuskopiointiikkuna on siis määrätty ajanjakso, jonka aikana järjestelmässä tai verkossa suoritetaan varmuuskopiointitoimintoja.

Kuva 3. Inkrementaalinen varmistus

2.1.3 Differentiaalinen varmistus

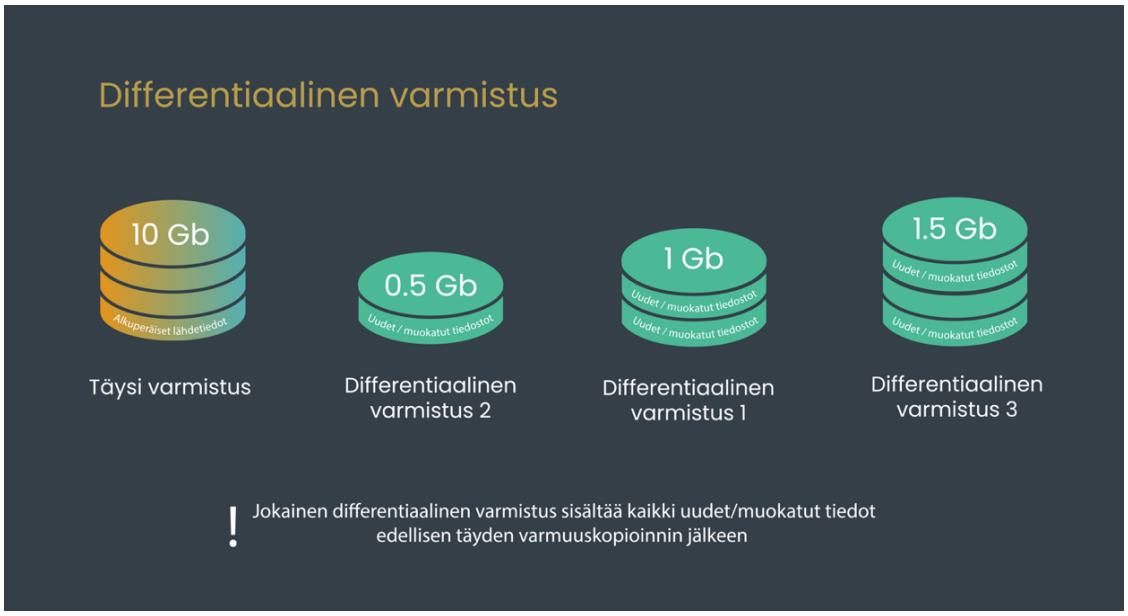
Differentiaalinen varmuuskopio sisältää kaikki edellisen täysvarmuuskopioinnin jälkeen muokatut tiedostot, ja sen etu täydellisiin ja inkrementaalisiin varmuuskopioihin verrattuna on palautusajan lyhentäminen. Jos differentiaalinen varmuuskopiointi tulee kuitenkin suoritettua liian monta kertaa, niin differentiaalivarmuuskopion koko saattaa kasvaa suuremmaksi kuin perustason täyden varmuuskopion koko (Backup4all 2018).

Differentiaalinen varmuuskopio on verrattavissa inkrementaaliseen varmuuskopiointiin, koska se on täyden varmuuskopion varmuuskopiolaajennus. Toisin kuin inkrementaalinen varmuuskopiointi, differentiaalinen varmuuskopio tiedot, jotka ovat muuttuneet edellisen täyden varmuuskopioinnin jälkeen (Kuva 4). Jos siis teet täyden varmuuskopion sunnuntaina, maanantaina tehty differentiaalinen varmuuskopio varmuuskopioi kaikki tiedot, jotka ovat muuttuneet sunnuntain jälkeen. Sitten tiistaina differentiaalivarmuuskopiointi varmuuskopioi myös kaiken, mikä on muuttunut sunnuntain jälkeen. Keskiviikon ja torstai-eron varmuuskopiot varmuuskopioivat samalla tavalla kaiken, mikä on muuttunut sunnuntain täyden varmuuskopioinnin jälkeen (Backup4all 2018).

Differentiaalinen varmuuskopiointiprosessi on pidempi, ja se tallentaa muutoksia tietoihin edellisen täyden varmuuskopioinnin jälkeen, mikä luo resurssi-intensiivisemmän prosessin, joka vaatii suurempaa tallennuskapasiteettia. Jos ehtona on rajalliset resurssit tai vaatimus nopeampaan varmuuskopiointiaikaan, inkrementaalinen lähestymistapa voi olla parempi vaihtoehto (Backup4all 2018).

Differentiaaliprosessia käytettäessä toipumisaika on paljon nopeampi verrattuna inkrementaaliseen prosessiin, koska se varmuuskopioi tietojen muutokset edellisen täyden varmuuskopioinnin jälkeen eli siinä on vain yksi suuri varmuuskopio, toisin kuin inkrementaalinen monikerta. Tietojen palauttaminen yhdestä suuresta lohkosta täyden varmuuskopion lisäksi on paljon nopeampaa kuin useiden lohkojen palauttaminen ja yhdistäminen (Backup4all 2018).

Jos yrityksellä on vaatimus nopeaan ja yksinkertaiseen tapaan palauttaa kadonneet tiedot, differentiaalinen varmuuskopiointi voi olla parempi vaihtoehto kuin asteittainen varmuuskopiointi. Varmuuskopiointinopeudessa ja tallennuskapasiteetissa on tehtävä uhraus, mutta niiden sijaan on palautusprosessi nopeaa.



Kuva 4. Differentiaalinen varmistus

2.1.4 Online, Near-line ja Offline -termit

Varmuuskopioiden viivettä tai saatavuutta kuvataan termeillä: Online, Near-line ja Offline. Online-varmuuskopiot otetaan reaaliajassa eli ne ovat jatkuvasti saatavilla verkossa, jonka ansiosta ne tarjoavat korkean vikasietoisuuden. Esimerkki online-varmuuskopioista on kahden levyn välillä tapahtuva RAID-1-tason peilaus (Rao&Nyak 2014, 264.).

Near-line varmuuskopio otetaan lähes reaaliajassa, kuten online-varmuuskopio, mutta oikean datan ja varmuuskopion välillä on ’pieni aukko’ eli lyhyt aikaviive (Rao&Nyak 2014, 264.).

Offline-varmuuskopiointi on yleisin käytetty verkosta kokonaan irrotettu varmuuskopiointimuoto. Kyseinen varmuuskopio otetaan paikalliseen mediaan, kuten nauha-asemille, DVD-levyille, CD-levyille, ulkoisille kovalevyille ja muihin asiaankuuluviin medioihin. Offline-varmuuskopiota voidaan myös tehdä samaan aikaan online-varmuuskopioinnin kanssa (Rao&Nyak 2014, 265.). Esimerkiksi yrityksen tärkein osa datasta varmuuskopioidaan joka päivä sekä toimiston verkkolevylle, että pilvipalveluun. Tämän ohella viikoittain yritys voi ottaa varmuuskopioita magneettinauhalle ja pitää ne paloturvallisessa kaapissa, jolloin tietojen turvallisuus kasvaa entisestään.

2.2 Varmuuskopiointimenetelmien hyvät ja huonot puolet

Kolmella suosituimmalla varmuuskopiointimenetelmällä on sekä hyvät että huonot puolensa, jotka on hyvä tietää suunniteltaessaan omaa varmuuskopiointi suunnitelmaa. Tietojen varmuuskopiointi on minkä tahansa liiketoiminnan jatkuvuuden/katastrofistrategian kriittinen osa.

Kuten ennen mainitsin, täysi varmistus on yleisin käytetty varmuuskopiointimenetelmä. Kattava kopio kaikista tiedoista sijaitsee yhdessä paikassa, eikä sen palauttaminen vie paljon aikaa. Lisäksi etuna on myös yksinkertainen tietojen tallennus ja hallinta, koska kaikki sijaitsee yhdessä kokonaisessa datasetissä (data set). Täysi varmistus antaa parhaan suojan tiedoille sekä nopeimman tavan palauttaa tiedot katastrofin jälkeen. Täyden varmistuksen tekeminen kuitenkin vie paljon aikaa ja tallennustilaa. Huonona puolena on myös mahdolliset turvallisuusongelmat sekä verkon rasitus, jos varmuuskopiointi tapahtuu verkossa (Navasardyan 2020). Kaikki tiedot on tallennettu yhteen paikkaan, jolloin on mahdollisuus menettää kaiken, jos varmuuskopiotietoihin päästään käsiksi tai ne vaarantuvat jollakin muulla tavalla.

Inkrementaalisen varmistuksen kohdalla taas hyvinä puolina on sen nopeus sekä alhaiset tallennustilanvaatimukset verrattuna täydelliseen varmistukseen, sillä jokainen varmuuskopioitu muutos on yksilöllinen palautuspiste (Mayer 2022). Varmuuskopiointityö toimii suurella nopeudella, koska vain inkrementaalit eli lisäykset varmuuskopioidaan. Tämä varmuuskopiointimenetelmä sopii hyvin yrityksille, joilla ei ole loputtomia resursseja tai jotka eivät vaadi tietojensa pitkäaikaista säilyttämistä, kuten esimerkiksi pankit ja muut rahalaitokset (DesignRush 2022). Se on myös hyvä vaihtoehto organisaatioille, jotka haluavat toipua nopeasti laitteisto- tai ohjelmistovian sattuessa, mutta joiden ei tarvitse palauttaa kaikkia tietojaan kerralla. Inkrementaalivarmuuskopioiden tarkoituksena on siis säästää tilaa ja aikaa. Tietojen palautus vie kuitenkin hieman enemmän aikaa kuin täydellisen varmuuskopion palautus, koska ensin on palautettava täydellinen varmuuskopio ja sitten myös jokainen seuraava lisäys eli inkrementaali. Jokainen lisäys on varmuuskopioitava onnistuneesti, jotta tietojoukko on täydellinen, muuten kaikkien myöhempien lisäysten palauttaminen voi epäonnistua (Vitanium 2020). Eli tietojen onnistunut palauttaminen riippuu ketjun kaikkien vaiheiden eheydestä. Lisäksi miinuksena on se, että tietyn tiedoston etsiminen useista varmuuskopiosarjoista voi olla työlästä.

Differentiaalisen varmistuksen hyvinä puolina on sen pienen tallennustilan vieminen verrattuna täydelliseen varmuuskopiointiin sekä kyseisen menetelmän tarjoamat eri versiot samoista tiedostoista. Differentiaalinen varmuuskopiointi on nopeampaa kuin täydellinen varmuuskopiointi, mutta kuitenkin hitaampaa kuin inkrementaalinen varmuuskopiointi. Verrattuna Inkrementaalisen varmuuskopion palauttamiseen, differentiaalisen varmuuskopion palauttaminen vaatii vähemmän aikaa, mutta kuitenkin kauemmin kuin täydellisen varmuuskopion palauttaminen.

Differentiaalivarmuuskopiot tarjoavat enemmän joustavuutta, koska niiden avulla voit valita kuhunkin varmuuskopiosarjaan sisällytettävien tiedostojen määrän ja päättää varmuuskopion monimutkaisuudesta tai yksinkertaisuudesta. (DesignRush 2022). Kyseisen menetelmän takia varmuuskopioit enemmän tietoja, jolloin ajan mittaan nämä varmuuskopiot voivat kuluttaa paljon enemmän tallennustilaa kuin inkrementaalinen varmuuskopiointi.

3 Tietojen palautus

3.1 Tietojen palautus (data recovery) käsitteenä

Tietojen palauttamisella tarkoitetaan prosessia, jossa haetaan laitteeseen tallennettuja tietoja, joihin ei ole pääsyä tavallisin keinoin aiemman poistamisen tai tietovälineen vaurioitumisen vuoksi. Tietojen palauttaminen voidaan kuitenkin tehdä vain, jos tiedoston sisältö on edelleen tallennuslaitteessa. Esimerkiksi se ei voi palauttaa asiakirjoja, jotka on luotu, mutta joita ei ole tallennettu sähkökatkon vuoksi. Tapauksissa, joissa tiedoston tallennustilan on vienyt jokin toinen tieto, palautusmenetelmät eivät pysty palauttamaan kadonneita tiedostoja. Kadonneet tiedostot voidaan palauttaa vain ulkoisen varmuuskopion avulla (UFS EXPLORER 2022).

Tietojen palautustekniikat voidaan jakaa kahteen tyyppiin: ohjelmistopohjaisiin (logical data recovery) ja laitteistopohjaisiin (physical data recovery). Useimmissa tapauksissa käytetään ohjelmistopohjaista lähestymistapaa, jossa käytetään erikoistuneita apuohjelmia tulkitsemaan tallennuslaitteen loogista rakennetta ja poimimaan tarvittavat tiedot käyttökelpoiseen muotoon. Vakavammissa tapauksissa fyysiset korjaukset voivat olla tarpeen, esimerkiksi silloin, kun laitteen mekaaniset tai sähköiset osat eivät toimi oikein. Tällaisissa tapauksissa keskitytään kriittisen sisällön poimimiseen laitteesta, jota asia koskee, ilman mahdollisuutta jatkaa laitteen käyttöä tulevaisuudessa (UFS EXPLORER 2022).

3.2 Fyysinen tietojen palautus (physical data recovery)

Virheilmoituksen saaminen laitteellesi voi olla hälyttävää, mutta monissa tapauksissa tiedostojen palauttaminen on kuitenkin mahdollista. Tätä varten on tärkeää määrittää tietojen häviämisen tarkka syy. Kun tarvittuihin tietoihin ei ole pääsyä, voi syynä olle kiintolevyn tai SSD-aseman fyysinen tai mekaaninen vika.

Fyysinen tai mekaaninen tietojen menetys tapahtuu, kun tallennusväline, kuten kiintolevy tai SSD, ei enää toimi kunnolla. Tämä voi johtua fyysisistä vaurioista, kuten esimerkiksi vesivahingoista, kiintolevypäiden kaatumisesta (HDD heads crash), piirilevyn hajoamiselta (printed circuit board corruption) tai karan jumiutumisesta (spindle seizure). Sähköongelmat, kuten väärä virransyöttö tai virtapiike, kuuluvat myös tähän luokkaan. Fyysisten vaurioiden merkkejä ovat ulkoisesta kiintolevystä tai USB-asemasta tulevat omituiset äänet, kuten outo surina tai naksahtava ääni (Platinium Data Recovery 2022).

Kun kiintolevyn tai muun laitteen sisällä olevat elektroniset mekanismit vaurioituvat niin, etteivät ne enää toimi tai ole luettavissa, kutsutaan tätä fyysiseksi vaurioksi. Tämäntyyppiset vauriot voivat aiheuttaa tiedostojen vioittumisen tai jopa pysyvän menetyksen, jos se vaikuttaa tiettyihin tiedostosektoreihin. Kadonneiden tietojen palauttamiseksi fyysisen vaurion jälkeen tarvitaan erikoistyökaluja ja ammattikokemusta aseman avaamiseen, sen komponenttien tarkastamiseen ja vaurioituneiden osien vaihtamiseen samalla, kun tarvittavia tietoja poimitaan oikein (Platinium Data Recovery 2022).

3.3 Looginen tietojen palautus (logical data recovery)

Looginen tietojen katoaminen tapahtuu, kun tiedostot eivät ole käytettävissä poistamisen, osion vioittumisen, osion poistamisen, alustamisen, uudelleenasennuksen, virusten ja muiden vastaavien syiden vuoksi. Tämäntyyppisessä tietojen katoamisessa tallennusväline on hyvässä toimintakunnossa, mutta tiedostojärjestelmä tai tiedot ovat vioittuneet tai vaurioituneet. Inhimillinen virhe on tärkein syy loogisiin ongelmiin, kuten vahingossa tapahtunut formatointi tai virheellisten tiedostojen poisto. Toisin kuin fyysiset vauriot, looginen vaurio aiheuttaa erilaisia oireita, kuten kadonneet tai vioittuneet tiedostot tai esimerkiksi tietokoneen kyvyttömyys käynnistyä jostain syistä. Sähkökatkot, järjestelmän kaatumiset, ohjainongelmat tai ohjainhäiriöt voivat myös aiheuttaa loogisia vaurioita (Platinium Data Recovery 2021).

Loogisen vaurion on mahdollista korjata omin käsin. Esimerkiksi tietojen palautusohjelmisto tai viruksenpoisto voi korjata ongelman. Tietojen palautusprosessiin kuuluu yleensä tiedostojärjestelmän korjaaminen, ohjelmien palauttaminen tai osittainen palauttaminen. On kuitenkin suositeltavaa välttää minkäänlaisia DIY-tietojen palautusmenetelmän käyttöä eli ’tee-se-itse’ palautusmenetelmän käyttöä, jos et ole alan asiantuntija. Vahinkotyypistä riippumatta, tietojen palautusprosessit on parasta luovuttaa palautusasiantuntijoille hoidettavaksi (Platinium Data Recovery 2021).

4 Tallennusmediat

4.1 NAS-palvelin eli verkkolevy

NAS-palvelin (Network-Attached Storage, verkkolevy) on tiedostojen tallennustyyppi, joka hakee tietoja keskitetetyistä HDD:stä eli kovalevyistä useille käyttäjille ja erilaisille asiakaslaitteille, kuten esimerkiksi älypuhelimelle. NAS-palvelimen avulla lähiverkkoon (LAN) liittyvät käyttäjät voivat käyttää jaettua tallennustilaa tavallisen Ethernet-yhteyden kautta (Bigelow ym. 2022).

NAS-yksiköitä hallitaan yleensä verkkopohjaisen apuohjelman kautta, eikä niissä ole näyttöä tai näppäimistöä. Jokainen NAS toimii itsenäisenä verkkosolmuna lähiverkossa ja sillä on oma ainutlaatuinen IP-osoite. Yksi verkkolevyn tärkeimmistä eduista on sen saavutettavuus, edullisuus ja suuri kapasiteetti. Nämä laitteet yhdistävät tallennustilan yhteen paikkaan ja tukevat pilvitallennusta sekä erilaisia tehtäviä, kuten arkistointia ja varmuuskopiointia (Bigelow ym. 2022).

4.2 HDD eli perinteinen kovalevy

Kovalevy (HDD) on tiedontallennuslaite, joka koostuu pyörivästä metallilevystä, jossa on magneettinen päällyste. Kiintolevylle tieto tallennetaan binäärimuodossa käyttämällä niin kutsuttuja bittejä. Nämä binäärinumerot ovat pienin digitaalisen tiedon yksikkö, ja niitä kutsutaan usein yksinkertaisesti "biteiksi" (ACS Data Recovery 2023).

Kovalevy (HDD) on eräänlainen ’haihtumaton/katoamaton’ tallennuslaite, joka voi säilyttää sille tallennetut tiedot myös ilman virtalähdettä. Kun ohjelmat vaativat pääsyn tietoihin, käyttöjärjestelmä (OS) kehottaa kiintolevyä lukemaan tai kirjoittamaan tarvittavat tiedot. Nopeus, jolla kovalevy pystyy suorittamaan nämä tehtävät, määräytyy täysin sen omien kykyjen mukaan. Alun perin kiintolevyt olivat tilaa vieviä laitteita tarjoen vain 3,75 megatavun tallennuskapasiteettia. Nykypäivän pöytätietokoneissa käytettävät kiintolevyt ovat kuitenkin paljon kompaktimpia ja voivat tarjota jopa 18 teratavua tallennustilaa, mikä tekee niistä paljon käytännöllisempiä ja tehokkaampia (IBM 2023).

4.3 SSD-levy eli puolijohdelevy

SSD-levy (Solid-State Drive) on tietokoneissa käytettävä tavanomaista kiintolevyä nopeampi tallennuslaite. Verrattuna kovalevyyn (HDD) SSD-levy tarjoaa nopeammin käynnistyvän

käyttöjärjestelmän, ohjelmien nopeamman latautumisen sekä tiedostojen nopeamman tallentumisen. SSD-levy sisältää kaksi avainkomponenttia, jotka ovat flash-ohjain ja NAND-flash-muistisirut. Tämä tarjoaa korkean luku-/kirjoitussuorituskyvyn peräkkäisissä ja satunnaisissa tietopyynnöissä (Gillis 2021).

Yritysten kasvava kysyntä nopeampaan siirräntäkykyyn (input/output, I/O) on vauhdittanut SSD-levyjen kehittymistä ja käyttöönottoa. SSD-levyt ovat erittäin tehokkaita raskaiden luku- ja satunnaisten työkuormien hallinnassa, koska niiden viive on pienempi kuin kovalevyillä (HDD). Tämä lyhyempi viive johtuu flash-SSD -levyjen kyvystä lukea tiedot tallennetuista tiedoista välittömästi ilman viivettä (Gillis 2021).

4.4 Magneettinauha

Magneettinauha on fyysinen tallennusväline erityyppisille tiedostoille, joka on suhteellisen vanha tekniikka verrattuna moniin muihin tallennusmedioihin. Magneettinauha on useiden vuosikymmenten ajan toiminut merkittävänä välineenä sekä ääni- että binaaridatan tallentamiseen, ja sitä käytetään edelleen joissakin järjestelmissä tiedon tallennusmuotona. Digitaalisen kuvantamisen ja audiovisuaalisen median tallennuksen yleisyys viime vuosina on johtanut magneettinauhalaitteiden käytön vähenemiseen (Rouse 2016).

Magneettinauhojen suosio perustuu siihen, että se on luotettava tallennusväline, sekä siihen, että sillä on hyvä hintakapasiteettisuhde. Magneettinauhat ovat hinnaltaan suhteellisen halpoja ja säilyvät pitkiä aikoja. Lisäksi ne kestävät hyvin rasitusta, joten niiden kuljettaminen paikasta toiseen on melko turvallista. Magneettinauhat ovat hyvä väline arkistointiin ja varmuuskopiointiin. Magneettinauhalla on myös huonot puolensa, kuten se, että tietojen luku- ja kirjoitusnopeus on hitaampi peräkkäisen käytön vuoksi. Tiedot siis tallentuu pitkälle magneettinauhalle, mikä takia joudut kelaamaan etsimään kohtaan (Crocetti 2018).

4.5 Optiset mediat

Optisella medialla tarkoitetaan mitä tahansa tiedontallennuslaitetta tai -laitteistoa, joka käyttää optista tiedontallennus- ja hakutekniikkaa tietojen lukemiseen ja kirjoittamiseen. Se tallentaa tiedot digitaalisesti medialaitteeseen ja käyttää laseria tietojen lukemiseen. Optiset mediat ovat usein

kannettavia/siirrettäviä, minkä ansiosta niitä on helppo kuljettaa eri järjestelmiin ja paikkoihin. Yleisimmät optisten medialaitteiden muodot ovat tällä hetkellä CD, DVD ja Blu-ray (Rouse 2015).

Magneettinauhaan, kiintolevyyn ja SSD-levyyn verrattuna, optinen tietoväline on kestävämpi ja vähemmän herkkä ympäristötekijöille. Optisten levyjen luku- ja kirjoitusnopeus on kuitenkin tyypillisesti hitaampi kuin perinteisillä kovalevyillä ja huomattavasti hitaampi suorituskyky verrattuna SSD-levyihin. Lisäksi ne tarjoavat pienemmän tallennuskapasiteetin kuin HDD- tai SSD-levyt. Vaikka Blu-ray-levyt tarjoavat tällä hetkellä nopeimman optisen median nopeuden ja suuremman tallennuskapasiteetin kuin CD- ja DVD-levyt, ne jäävät silti kiintolevyjen ja SSD-levyjen ominaisuuksista jälkeen. (Sheldon ym. 2021).

Optisia levyjä voidaan käyttää varmuuskopiointiin, mutta sen automatisointi on vaikeaa, koska itse levy on asetettava koneeseen, seuraavaksi on tehtävä itse varmuuskopiointi ja tämän jälkeen poistettava levy sille tarkoitettuun säilytyspaikkaan. Tämä koko varmuuskopiointiprosessi sitoo henkilökunnan tiettyyn paikkaan ja aikaan toteuttamaan kyseisen toiminnon.

5 Varmistusohjelmat

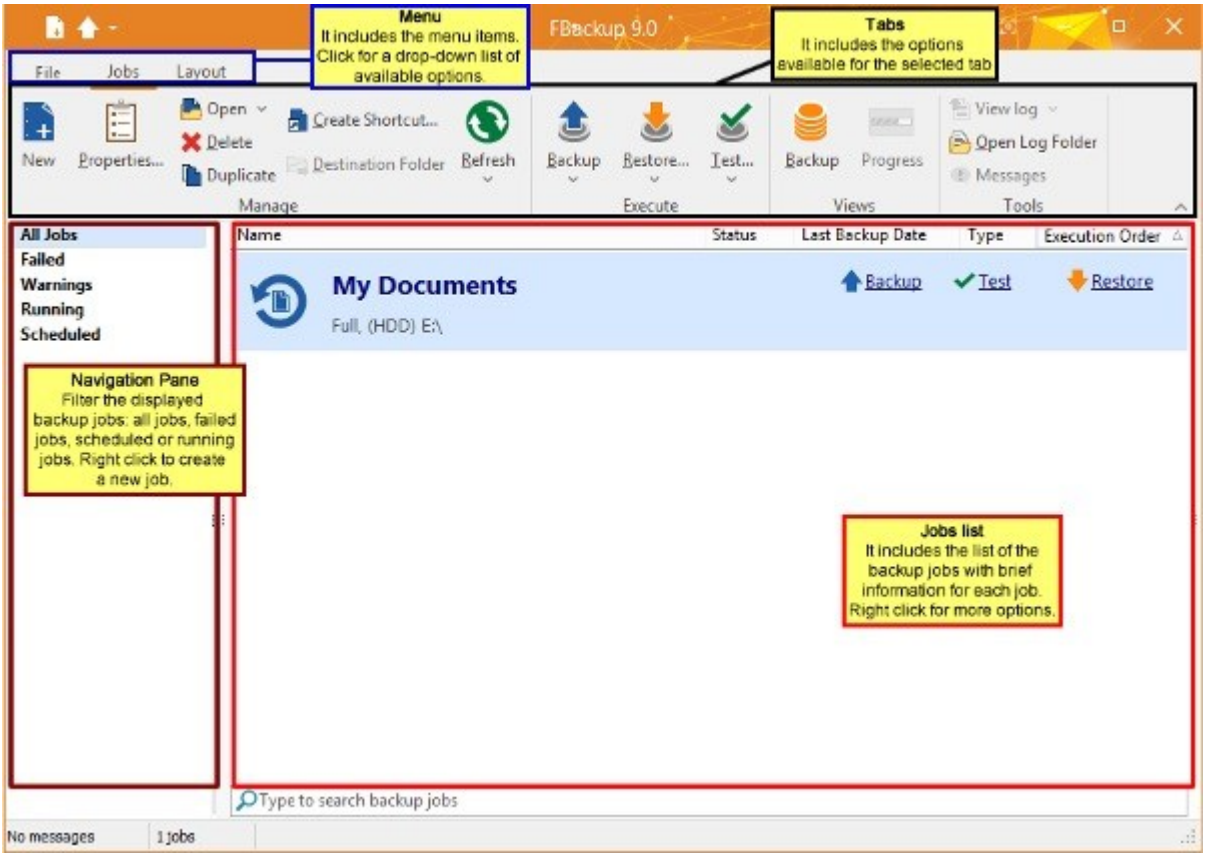
Vaikka tiedostoja voidaan kopioida käsin eli manuaalisesti yhdestä paikasta toiseen ilman mitään erillistä ohjelmistoa, periaatteessa varmuuskopiointi kuitenkin tarvitsee erillisen varmistusohjelman. Varmuuskopiointiin löytyy paljon erilaisia ohjelmia, joista tässä oppinäytetyössä varmuuskopiointipalvelua varten on tavoitteena etsiä ilmainen ja monipuolinen vaihtoehto, eli tässä työssä käsitellään vain ilmaisohjelmia. Ohjelmistot arvioidaan niiden ominaisuuksien avulla. Vuonna 2023 Techradar.comin mukaan yleisimpiä ilmaisia varmuuskopiointiohjelmia ovat Paragon Backup & Recovery, Cobian backup, EaseUS Todo Backup Free, FBackup ja Internxt. Muita esimerkkejä suosituista ilmaisohjelmista ovat Back4Sure, Syncback free ja Duplicati. Tästä listasta EaseUS Todo Backup Free, Internxt ja Paragon & Recovery eivät ole yrityskäyttöön ilmaisia, joten niitä ei tulla käsittelemään ehdokkaina.

5.1 FBackup

FBackup on Windowsille tarkoitettu varmuuskopiointiohjelmisto, jolla on käyttäjäystävällinen ja helppokäyttöinen käyttöliittymä (Kuva 5). Arvokkaiden tietojen suojaaminen osittaisilta tai täydelliseltä katoamiselta tapahtuu automatisoimalla varmuuskopiointitehtävät, suojaamalla salasanalla ja pakkaamalla ne tallennustilan säästämiseksi. FBackupin avulla varmuuskopiointi on mahdollista toteuttaa mihin tahansa paikalliseen verkkoasemaan, Dropboxiin (henkilökohtainen tai yritys), CD-, DVD- tai Blu-ray-levylle, Google Driveen tai muulle siirrettävälle tietovälineelle (kuten USB- tai Firewire-asemille). FBackup pystyy varmuuskopioimaan avoimet/lukitut tiedostot käyttämällä täydellistä- ja peilivarmuuskopiointia. Määritettäessä varmuuskopiota, on myös mahdollista asettaa erilaisia tiedostosuodattimia ja ajoittaa varmuuskopion suoritettavaksi automaattisesti. FBackupissa voit valita manuaalisesti, mitkä tiedostot ja kansiot varmuuskopioidaan. On myös mahdollisuus käyttää varmuuskopiolaajennuksia, jotka automaattisesti valitsevat tarvittavat tiedostot varmuuskopioita varten (FBackup User Manual 2021, 7-8).

FBackup tukee ZIP64:ää, mikä mahdollistaa yli 2 Gt:n kokoisten varmuuskopioiden luomisen. Se luo tavallisia zip-tiedostoja, joita voidaan käyttää millä tahansa zip-yhteensopivalla työkalulla. FBackup pitää kirjaa tiedostoversioista, jotka voidaan palauttaa vaivattomasti joko yksittäin tai kokonaisena kansiona. Palautusprosessi sisältää tiedostotyyppiin, päivämäärään, kokoon tai attribuutteihin perustuvia suodattimia. Varmuuskopion turvallisuuden ja tarkkuuden takaamiseksi FBackup testaa varmuuskopiotiedostot automaattisesti CRC32:lla. FBackup toimii Windows Server

2019/Server 2016/10/Server 2012/8.1/8/Server 2008/7/Server 2003/XP -käyttöjärjestelmissä ja tarjoaa tuen useilla kielillä (FBackup User Manual 2021, 7-8).



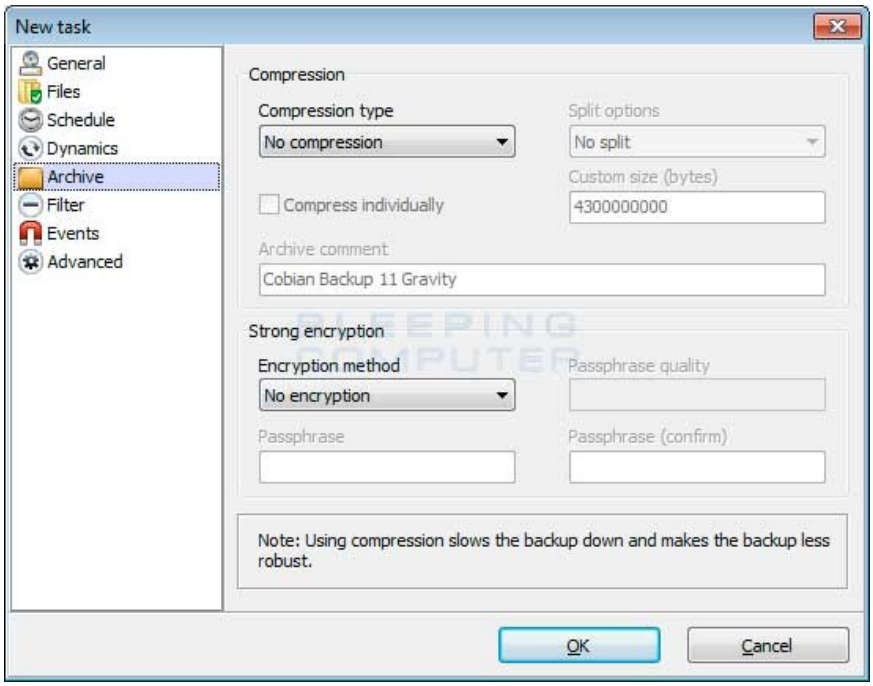
Kuva 5. FBackup:in käyttöliittymä käyttöohjeistustekstineen (FBackup UserManual 2023)

5.2 Cobian- backup ja Reflector

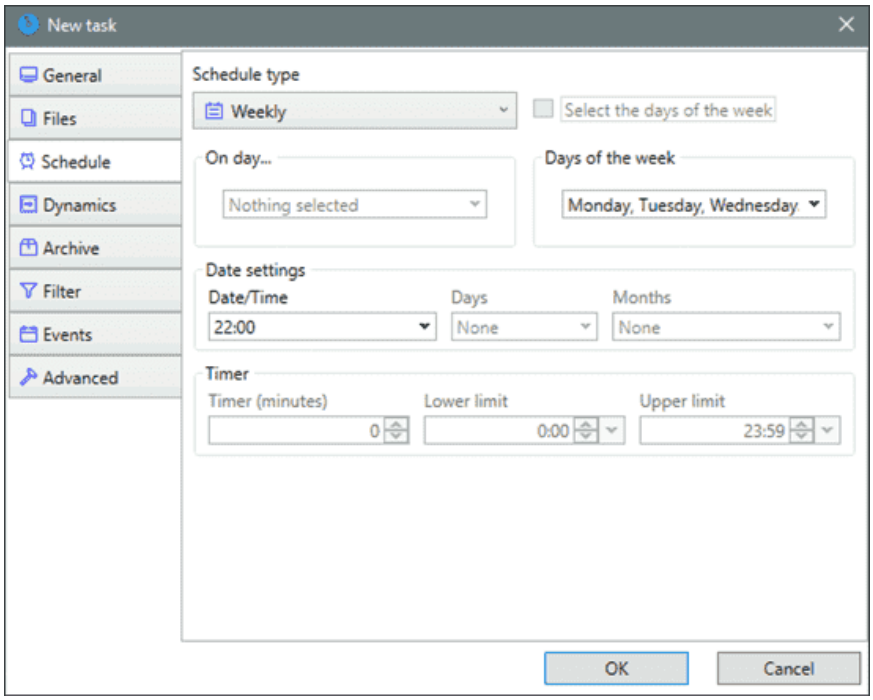
Cobian Backup on ilmainen varmuuskopiointiohjelma, jonka on luonut Kuubasta peräsin Luis Cobian. Ohjelma on täysin ilmainen sekä yksityiskäyttöön, että kaupalliseen käyttöön. Kyseistä varmuuskopiointiohjelmaa käytetään tiedostojen ja hakemistojen automaattisten varmuuskopioiden valmistamiseen, jotka se voi suorittaa samaan tietokoneeseen, verkon kautta tai FTP -palvelimen kautta (File Transfer Protocol). Cobian Backup voi suorittaa täydelliset-, differentiaaliset ja inkrementaaliset -varmuuskopiot (CobianSoft 2019). Kaikki varmuuskopiotiedostot voidaan pakata ja salata. Itse ohjelmisto on yksinkertainen, mutta tehokas varmuuskopiointiohjelma. Cobianin käyttöliittymää on todella helppo käyttää, sillä se näyttää hyvin samanlaiselta kuin klassiset Windows -sovellukset. Vaikka Cobian Backup on ollut olemassa jo vuosikymmenien ajan, se silti toimii luotettavasti ja johdonmukaisesti. Viimeisin versio, Cobian Backup 11 Gravity, oli viimeinen julkaistu versio, sillä omistaja ja alkuperäinen ohjelmoija Luis Cobian myi lähdekoodin vuonna 2014

(CobianSoft 2019). Cobian varmuuskopio on saatavana yksinomaan Windowsille, Windows XP:stä Windows 10:een.

Jos käytössä on Windows 10:n jälkeinen versio eli Windows 11, niin Cobian Backup 11 Gravity ei silloin sovi käytettäväksi, sillä uudemmille Windows versioille löytyy Cobian Reflector. Cobian Reflectorin käyttöliittymä näyttää melko samanlaiselta kuin Cobian Backup 11 Gravity:llä, mutta vähän uudemmalta (Kuvat 6 ja 7). Muuten kaikki toiminnot ovat samanlaisia ja sitä on helppo käyttää.



Kuva 6. Cobian Backup 11 Gravity ’Archive’ (BleepingComputer 2006)



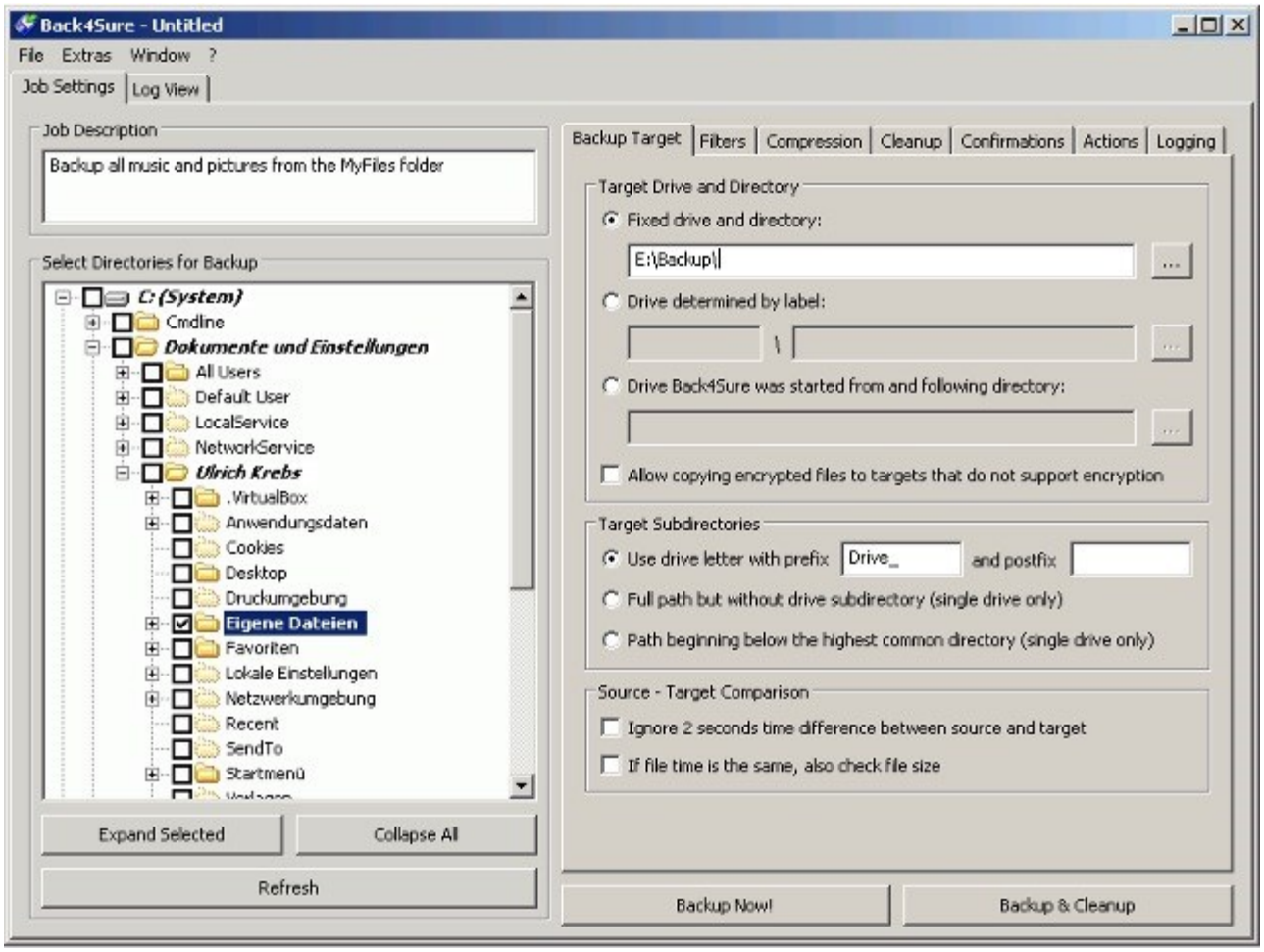
Kuva 7. Cobian Reflector ’Schedule’ -sivu

5.3 Back4Sure

Back4Sure ohjelman on luonut Ulrich Krebs. Se on ilmainen ja monipuolinen varmuuskopiointiohjelma henkilökohtaiseen- ja pienyrityksen käyttöön. Ohjelmalla on mahdollisemman yksinkertainen käyttöliittymä ja vaativimmille käyttäjille se sisältää pieniä lisäominaisuuksia (Kuva 8). Back4Sure pystyy keräämään varmuuskopioita varten valitut tiedostot tietokoneesi eri paikoista, mukaan lukien useista asemista. Tämän jälkeen se luo kopion näistä tiedostoista määritettyyn kohdehakemistoon. Kohdehakemistossa on automaattisesti kansio, jossa on lähdeaseman asemakirjain ja hakemistorakenne, mikä varmistaa, että kaikki tiedostot tallennetaan tarkasti ja ne ovat helposti saatavilla. Tämä varmuuskopiointiprosessi kopioi valikoivasti vain ne tiedostot, jotka ovat muuttuneet edellisen varmuuskopioinnin jälkeen, mikä mahdollistaa jopa suurten tiedostomäärien nopean varmuuskopioinnin. Varmuuskopiointia varten voi käyttää USB-muistitikkua, toissijaista kiintolevyä tai jaettua verkkoa varmuuskopion kohteena. Ainoa Back4Sure:n huono puoli on se, että sillä ei ole mahdollisuutta tehdä varmuuskopiointi suoraan pilvipalveluun. Lisäksi Back4Sure:lla ei ole sisäistä ajastusta, minkä takia käyttäjä joutuu itse tekemään ajastetun varmistuksen käyttämällä Windowsin oman tehtävien ajoitusta (Manual for Back4Sure 2023).

Sisäänrakennetun Back4Sure-pakkauksen avulla käyttäjä säästää tilaa ja erityisesti paljon aikaa flash-levyillä, tehdessä varmuuskopion tuhansista tiedostoistaBack4Sure välttää käyttämästä omaa tiedostomuotoa tietojen tallentamiseen. Sen sijaan se yksinkertaisesti kopioi tiedostot tai

tallentaa ne tavallisiin Zip- tai 7Zip-säiliöihin. Lisäksi Back4Sure sisältää kohdehakemiston puhdistusvaihtoehdon. Tämä vaihtoehto mahdollistaa orpotiedostojen poistamisen, jotka ovat olemassa vain kohdehakemistossa ilman vastaavia lähdetiedostoja. Orpotiedosto on tiedosto, joka on olemassa hakemistossa, mutta on menettänyt yhteyden emohakemistoon tai lähdetiedostoonsa. Vaikka Back4Sure tarjoaa useita varmuuskopiointivaihtoehtoja, se on todella kätevä ja mukautuva varmuuskopiointiohjelma. Se vie alle 10 Mt tallennustilaa, ja sitä voidaan käyttää helposti flash-asemalta ilman asennusta. Se ei jätä jälkiä isäntäjärjestelmään, eikä asenna laajennuksia tai palveluita. Back4Sure tarjoaa monia vaihtoehtoja varmuuskopiointiprosessiin, mutta se on myös kätevä ja joustava: se vie alle 10 Mt tallennustilaa ja sitä voidaan helposti käyttää flash-levyltä ilman asennusta. Se ei jätä jälkiä isäntäjärjestelmään eikä asenna minkäänlaisia laajennuksia tai palveluita (Manual for Back4Sure 2023).

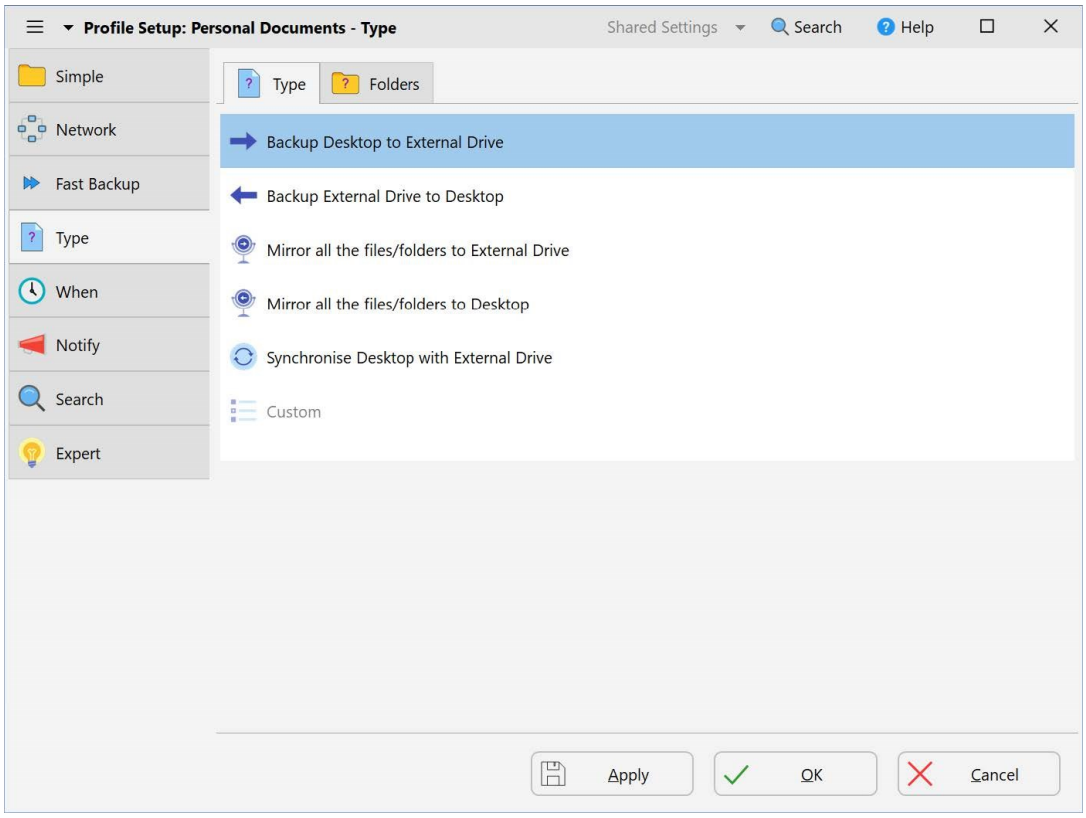


Kuva 8. Back4Sure -ohjelman käyttöliittymä (Back4Sure Manual version 3.7 2023)

5.4 SyncBackFree

Vuodesta 2003 alkaen käytössä ollut SyncBackFree on ilmainen varmuuskopiointiohjelma yksityis- ja kaupalliseen käyttöön, jonka on valmistanut 2BrightSpark. Ohjelma tarjoaa käyttäjilleen erinomaisen helppokäyttöisyyden ja toiminnallisuuden sekä joustavuuden valita, mitkä tiedostot ja kansiot sisällytetään varmuuskopioon (Kuva 9). Lisäksi ohjelmassa pystyy ajastamaan varmuuskopioinnin, pakata ja salata tiedostoja. Varmuuskopioinnin lisäksi SyncBackFree:n avulla pystyy tekemään synkronoinnin ja yksisuuntaista peilausta. SyncBackFree auttaa suojautumaan tietojen katoamiselta antamalla varmuuskopioida kaikki tärkeät tiedostot. Katastrofin iskettyä, palautusta varten on painettava vain yhtä painiketta, mikä tekee ohjelmasta vielä helppokäyttöisempää. Ohjelman huonona puolena on se, että sen avulla ei pysty tehdä varmistuksia suoraan pilvitallennuspalveluihin. Tämä on mahdollista vain SyncBackPro versiossa, mikä on maksullinen (SyncBackFree User Guide 2023, 3-4).

Varmuuskopiointiohjelma toimii Windows 11, 10, 8, 7 ja Vista:lla. Sekä 32-bittisiä että 64-bittisiä Windows versioita tuetaan. SyncBackFree ei kuitenkaan välttämättä sovi kaikille yrityksille käytettäväksi, koska Windows Serverin kanssa se ei toimi, mikä on monien yritysten vaatimus niiden työssään (SyncBackFree User Guide 2023, 3-4).

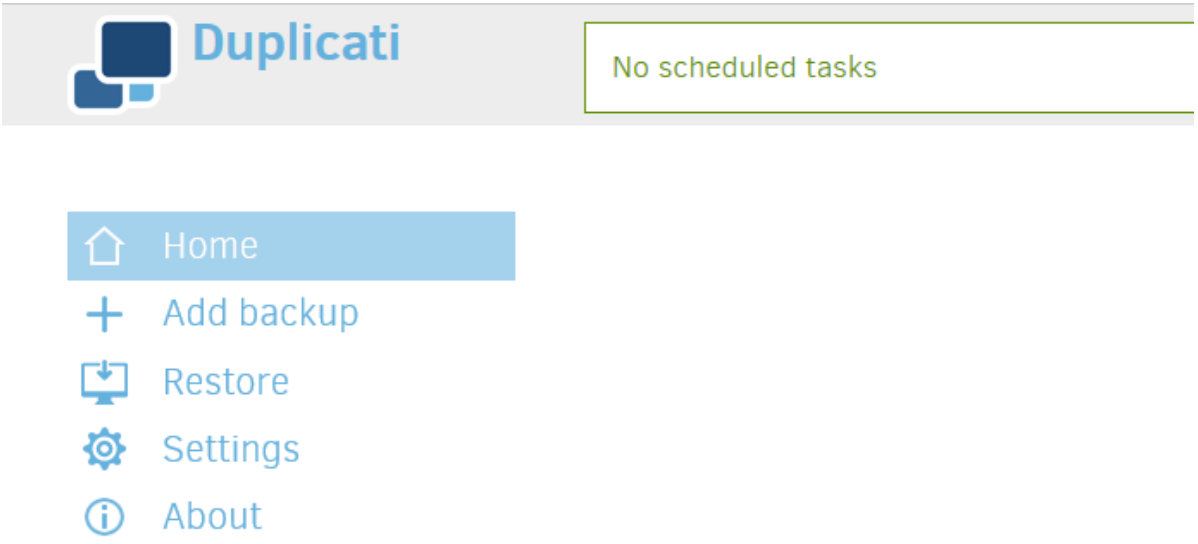


Kuva 9. SyncBackFree tyypin valinta (SyncBackFree V10 User Guide 2023)

5.5 Duplicati 2.0

Duplicati on ilmainen ja avoimen lähdekoodin varmuuskopiointisovellus yksityis- ja kaupalliseen käyttöön. Ohjelma tarjoaa erinomaisen pilvitallennuksen ja monia muita ominaisuuksia, joita tavallisesti löytyy vain maksullisista varmuuskopiointiohjelmista. Verkkopohjaisen käyttöliittymän ansiosta Duplicati tukee myös Windows-, MacOS- ja Linux-käyttöjärjestelmiä. Toimiakseen ohjelma kuitenkin vaatii .NET 4.5:n tai Monon. Ohjelma konfiguroidaan verkkokäyttöliittymmällä, joka toimii kaikissa selaimissa (jopa mobiililaitteissa) paikasta riippumatta ja joka on helppokäyttöinen ja käyttäjäystävällinen (Kuva 10). Tämä mahdollistaa myös ohjelman suorittamista verkkoon yhdistetyillä laitteilla, kuten NAS-palvelimella (verkkolevyllä). Duplicati toimii standardiprotokollien kanssa, kuten FTP, SSH, WebDAV, sekä suosittujen palveluiden, kuten Amazon S3, Microsoft OneDrive, Mega ja Google Drive:n kanssa (Duplicati 2 User's Manual 2023).

Duplicati oli alusta alkaen suunniteltu online-varmuuskopiointiin, minkä ansiosta se on tehokas datan kanssa ja käsittelee mainiosti verkko-ongelmia. Esimerkiksi keskeytettyjä varmuuskopioita voidaan jatkaa ja Duplicati testaa varmuuskopioiden sisällön säännöllisesti. Näin rikkoutuneiden tallennusjärjestelmien rikkinäiset varmuuskopiot voidaan havaita ennen kuin on liian myöhäistä. Duplicati varmuuskopioi tiedostot ja kansiot vahvalla AES-256-salauksella. Varmuuskopion salaamiseen voi myös käyttää GPG:tä (GNU Privacy Guard). Inkrementaalisella varmuuskopioinnilla ja tietojen duplikoinnilla tilaa säästyy, kun suoritat varmuuskopiot millä tahansa koneella verkkopohjaisen käyttöliittymän tai komentorivikäyttöliittymän kautta. Duplicatissa on sisäänrakennettu ajastin ja automaattinen päivitys (Duplicati 2 User's Manual 2023).



Kuva 10. Duplicatin pääsivun käyttöliittymä (Duplicati 2 User's Manual 2023)

6 Pilvitallennus

Pilvitallennuksessa dataa tallennetaan internet yhteyttä käyttäen jollekin ulkoiselle palvelimelle. Esimerkkejä tarjolla olevista palveluista ovat Microsoft OneDrive, Google Drive, Mega ja Dropbox.

Kaikilla pilvipalveluilla on sama toimintaperiaate, mutta tarjoamat palvelut voivat hieman erota ominaisuuksiltaan. Esimerkiksi Google Drive ja Microsoft OneDrive tarjoavat erilaisia hyödyllisiä toimisto-ohjelmia, jossa kaikki muutokset tallentuvat välittömästi pilveen. Pilvitallennus Megalla taas ei ole toimistotyökaluja, sillä se luottaa tallennustilaansa, joka on toimiva ja hyvin salattu systeemi.

6.1 Google Drive

Pilvitallennuspalvelun Google Drive on luonut Google, jossa uudelle asiakkaalle tarjotaan 15 gigatavua ilmaista tallennustilaa. Lisää tallennustilaa saa pientä maksua vastaan, 100 Gt/1,99€/kk, 200 Gt/2,99€/kk ja 2 Tt/9,99€/kk.

Google Drivella on sisäänrakennettu suojaus haittaohjelmia, roskapostia ja kiristysohjelmia vastaan. Drive tarjoaa myös salatun ja suojatun pääsyn tiedostoihisi. Kanssasi jaetut tiedostot voidaan skannata ja poistaa ennakoitavasti, jos haittaohjelmat, roskapostit, kiristysohjelmat tai tietojenkalastelua havaitaan. Lisäksi mukaan kuuluvat Docs-kirjoitusalusta, Sheets-taulukkolaskenta, Slides-esitysalusta sekä turvalliset Google Meet-videokonferenssit. Nämä kaikki ohjelmat toimivat suoraan Googlen pilvessä, jolloin Google Drive tallentaa kaikki reaaliajassa tehdyt muutokset. Googlen pilvessä on myös mahdollista tiedostojen muokkaaminen ja jakaminen useiden käyttäjien kesken jopa yhtä aikaa (Google Workspace 2023).

Google tarjoaa Backup&Sync -ohjelman, jonka avulla voidaan synkronoida tarvittavat tiedostot tietokoneelta Googlen pilveen ja pilvestä tietokoneelle. Ladattaessa Google Backup and Sync -sovelluksen, tietokoneelle ilmestyy uusi hakemisto, Google Drive, johon pystyy varmuuskopioida tarvittavat tiedot. Ohjelman avulla pystyy myös synkronoida tietoja tietokoneella olemassa olevista kansioista, kuten Documents tai Desktop, sekä USB-laitteista, SD-korteista ja Google Photographs -kuvista ja -videoista (Sappington 2022).

6.2 Dropbox

Inc -yhtiön luoma Dropbox on yksi vanhimmista ja suosituimmista pilvitallennuspalveluista, jota käytetään tiedostojen jakamiseen ja yhteistyöhön. Dropbox- sovellus toimii Windows-, Macintosh- ja Linux-työpöytäkäyttöjärjestelmillä. Löytyy myös sovelluksena iPhone, iPad, Android ja Blackberry-laitteille. Palvelu tarjoaa kaksi gigatavua maksutonta tallennustilaa (Dropbox 2023).

Dropbox sovelluksen asennuksen jälkeen näkyviin ilmestyy Dropbox-kansio, käyttäjän muiden kansioiden ohelle. Käyttäjänä voit tallentaa tiedostoja kansioon, luoda uusia kansioita sekä raahata ja pudottaa (’drag and drop’) tiedostoja kansioiden välillä, aivan kuin ne olisivat kaikki lokaaleja eli paikallisia. Dropboxin huonona puolena on kuitenkin se, ettei se anna valita synkronointia varten kansiota, joka on verkkolevyllä. Dropbox-kansiossa olevia tiedostoja voi käyttää mistä paikasta tahansa Internet-yhteyden kautta – käyttäjänä tarvitset vain kirjautua sisään tilillesi ladatakseen, lähettääkseen ja jakaakseen tiedostoja. Tiedostojen jakamista varten käyttäjä voi luoda sille URL-osoitteen Dropbox verkkosivulla ja lähettää sen, jotta muut voisivat avata ja lukea sen sisältöä (Dropbox 2023).

Yksityisille käyttäjille Dropbox tarjoaa Professional ja Professional+eSign -tilit, jotka molemmat tarjoavat 3 teratavua tallennustilaa. Tilit ovat hinnaltaan: Professional 19,99€/kk ja Professional+eSign 32,99€/kk. Yrityksille löytyy kolme erilaista tiliä, joista ensimmäinen on Standard tili, jossa 5 teratavua tilaa hintaan 14,50€/käyttäjä/kk. Toinen vaihtoehto on Standard+DocSend tili, jossa on myös 5 teratavua tilaa, mutta mukana myös turvallinen jakoalusta DocSend, joka auttaa tunnistamaan, kuka on kiinnostunut asioimaan kanssasi ja suojaa asiakirjojasi, hintaan 73€/käyttäjä/kk. Kolmantena vaihtoehtona on Advanced tili, joka tarjoaa rajoittamaton määrä tilaa hintaan 21.50€/käyttäjä/kk. Dropboxilla on myös Enterprise tili, joka on muokattava, suurille yrityksille tarkoitettu tili, joka on erikseen sovittava ja tilattava (Dropbox 2023).

6.3 MegaSync

MegaSync on pilvipalvelun MEGA.nz:n julkaisema sovellus tietojen synkronointia varten tietokoneesi ja MEGA Cloud Drive:n välillä. MEGA itsessään on yksi harvoista pilvipalveluista, joka tarjoaa päästä-päähän nollatietosalauksen (end-toend zero-knowledge encryption). Mega salaavat 128-bittisellä AES-salausjärjestelmällään (Advanced Encryption Standard) kaikki tiedot, minkä ansiosta käyttäjänä olet ainoa, joka pääsee tarkastelemaan tietojasi sekä ainoa, joka säilyttää salausavaimen. Tämä siis tarkoittaa, että jopa itse MEGA:n ylläpitäjillä ei ole pääsyä tietoihisi.

Tämän suojausprotokollan avulla salataan tiedot sekä lepotilassa, kun tiedot ovat MEGA-palvelimella, että siirron aikana eli kun tietoja siirretään tai ladataan niitä (MEGA 2023).

MEGA-tilin luomisen yhteydessä, käyttäjä saa ainutlaatuisen paikallisen yksityisen avaimen, joka on merkkijono kirjaimista ja numeroista. Avaimen voi tallentaa turvalliseen paikkaan, kuten luotettavaan salasananhallintaohjelmaan, ulkoiseen laitteeseen tai paperille. Avaimesta on kuitenkin pidettävä hyvää huolta, koska vain käyttäjällä on pääsy tähän avaimeen ja sen kadottua myös mahdollisuus päästä käyttäjän tietoihin katoaa. Lisäksi MEGA käyttää kaksivaiheista tunnistusta kirjautumisen yhteydessä, jonka ansiosta kukaan muu ei voi kirjautua tilillesi, vaikka heillä olisikin tilitietosi (MEGA 2023).

Mega tarjoaa 20 Gt ilmaista tallennustilaa. Maksua vastaan saat 400 Gt/4,99€/kk, 2 Tt/9,99€kk, 8Tt/19,99€/kk tai 17 Tt/29,99€/kk (MEGA 2023).

6.4 Microsoft OneDrive

Microsoftin luoma OneDrive on pilvipalvelu, joka tarjoaa 5 Gt ilmaista tallennustilaa ja rajoittamaton määrän tallennustilaa oppilaitosten opiskelijoille ja opettajille. OneDrive on integroitu Microsoft Officen kanssa, joten käyttäjät voivat käyttää Word-, Excel- ja PowerPoint-asiakirjoja OneDrivesta. Se ei vaadi latausta, ja sen pitäisi olla osana Windows 11:tä. One Driven käyttämiseen tarvitaan Microsoft-tili, ja käyttäjien on kirjauduttava sisään ennen sen käyttöä. OneDrive antaa käyttäjille mahdollisuuden tallentaa tiedostoja, valokuvia ja erilaisia asiakirjoja useille laitteille. Kun käyttäjä tallentaa tiedostonsa OneDriveen, se synkronoidaan automaattisesti muiden laitteiden välillä. Tämä ominaisuus helpottaa saman asiakirjan käyttöä ja käsittelyä useista paikoista. OneDrive tarjoaa vaivattoman pääsyn pilvitallennustilaan ja tarjoaa vaihtoehtoja sisällön jakamiseen muiden kanssa. Käyttäjät voivat valita tiedon tallennuspaikan joko OneDrivessa tai File Explorerissa. Niille, jotka aikovat käyttää OneDrivea varmuuskopioalustana, on suositeltavaa tallentaa tiedot molempiin paikkoihin. Muilla käyttäjillä on kuitenkin mahdollisuus tallentaa tiedostonsa joko OneDriveen tai File Exploreriin. (Provazza 2023).

Kotikäytön lisäksi OneDrive tarjoaa myös yrityksille suunnattuja palvelupakettiratkaisuja. Esimerkiksi palvelupaketti 1 tarjoaa yhden teratavun tallennustilaa käyttäjää kohden hintaan 50,4€/vuosi ja palvelupaketti 2 tarjoaa rajoittamattoman määrän tallennustilaa käyttäjää kohden hintaan 100,8€/vuosi. Samoin myös on tarjoilla käyttäjää kohden yksi teratavu tallennustilaa Office 365 -paketilla hintaan 126 €/vuosi (Microsoft. 2023).

6.5 Pilvipalveluiden vertailu

Microsoft OneDrive, MegaSync, Dropbox ja Google Drive ovat suosittuja pilvitallennuspalveluita, mutta niiden välillä on pieniä eroja, jotka on otettava huomioon suunniteltaessa pilvipalvelun hankintaa, etenkin yrityskäyttöön. Kaikki mainitsemat pilvipalvelut tarjoavat suhteellisen samanhintaisia yrityskäyttöön tarkoitettuja paketteja (Kuva 11). Google Drive (15Gt) ja Mega (20Gt) tarjoavat eniten ilmaista tallennustilaa verrattuna OneDriveen (5Gt) ja Dropboxiin (2Gt), joten tarkastellen vain tätä ilmaistallennustilan kriteeriä, niin ne ovat ’voittajia’.
Yhteistyöominaisuuksiltaan Google Drivella ja OneDrivella on paremmat yhteistyökalut, sillä niiden avulla useat käyttäjät voivat muokata tiedostoja samanaikaisesti tarjoten reaaliaikaista yhteistyötä. Yritykselle, jolla on käytössä Office 365, saattaa olla OneDrive todella hyvä ja helppo valinta. Siinä kaikki synkronoituu toimistosovelluksiin ja sopii mainiosti Windowsin kanssa. Googlella on suhteellisen samanlaiset toimistosovellukset, mutta vähemmällä valintavaihtoehdoilla. Jos ei ole kuitenkaan tarvetta monipuolisille Office 365 -toimistosovelluksille, niin sen sijalle hyvänä vaihtoehtona voisi olla myös Google Drive.
Dropbox on suosittu valinta henkilökohtaiseen käyttöön sen helppokäyttöisen käyttöliittymänsä ansiosta ja se on myös yksi vanhimmista pilvipalveluista. Dropboxin Paper-toiminto muistuttaa Googlen Docsia, sillä siinä voi tehdä muistiinpanoja jakamalla niitä muiden kanssa. Se ei kuitenkaan pysty kilpailemaan Microsoftin ja Googlen kanssa, jos kriteerinä on toimisto-ohjelmistojen laajuus ja monimuotoisuus.
Kaikki pilvipalvelut tarjoavat jonkin verran turvallisuutta, mutta MegaSync erottuu omalla päästä-päähän nollatietosalauksella (end-toend zero-knowledge encryption). Mega keskittyy tarjoamaan asiakkailleen luotettavaa tallennustilaa ja käyttökokemukseltaan se on monipuolinen ja helppokäyttöinen. Lisäksi MegaSync pitää tiedostosi koko ajan synkronoituina. Mega on todella hyvä vaihtoehto niille, joilla ainoana tarpeena on vain pilvitallennus.

Palvelu	Maksuton tallennustila	Tallennustilan hinta	Lisätietoja
Google Drive	15 Gt	10,40 € / 2Tt / kk	Sisäänrakennetut toimisto-ohjelmat
Dropbox	2 Gt	11,99 € / 2Tt / kk	Dropbox Paper tekstinkäsittelyyn
Mega	20 Gt	9,99 € / 2Tt / kk	Korostettu turvallisuus ja yksityisyys
OneDrive	5 Gt	4,20 € / 1Tt/ kk	Windows ja Office-sovellukset

Kuva 11. Pilvipalveluiden hintavertailu

7 Varmuuskopiointisuunnitelma

7.1 Yrityksen taustaa ja vaatimukset

IT-Futura Oy on ICT-alan suhteellisen nuori yritys, joka oli luotu tätä oppinäytetyötä varten eikä ole olemassa oleva yritys. Kyseinen yritys työllistää kolme henkilöä, joiden työhön kuuluu vanhemman sukupolven auttaminen heidän teknologisten laitteiden kanssa, kun he eivät itse osaa tai kykene siihen ja joilla ei ole mahdollisuutta matkustaa tai liikkua itse tullakseen toimistolle tai korjaamolle asti. IT-Futuran henkilöstö käy paikan päällä esimerkiksi heidän kotonansa tekemään tarvittavat työt, jolloin asiakkaiden ei tarvitse huolehtia matkustamisesta. Työnä voi olla esimerkiksi puhelimen tai tietokoneen ohjelmien päivitysten teko, uusien ohjelmien asentaminen, virusten poistot ja vanhojen ohjelmien tai tiedostojen puhdistaminen/poistaminen. IT-Futuralla ei ole minkäänlaista tämänhetkistä rahoitusta ja suhteellisen pieni budjetti alkuun. Yrityksen jäsenten tärkein tavoite on päästä auttamaan vanhempaa sukupolvea, joka aika usein jää yksin ilman ihmistä, joka pystyisi antaa apua teknologisten laitteiden kanssa kuten puhelin ja tietokone.

Toimistossa on kaksi pöytäkonetta ja kiinteä internetyhteys kaapelin kautta. Molemmilla pöytäkoneilla on asennettu Windows 10. Varmuuskopiointi halutaan toteuttaa ottamalla varmuuskopiot ’Tiedostot’- kansioista verkkolevylle (NAS-palvelimelle), josta ne siirtyvät pilvipalveluun. Yrityksen kaikki tärkeät varmuuskopiointiin kuuluvat tiedostot ovat aina tallennettu näiden kahden pöytätietokoneen Windows:in ’Tiedostot’-kansioon. Varmuuskopiointi tapahtuu tekemällä varmuuskopiot kyseisestä kansiosta verkkolevylle (NAS-palvelimelle), josta ne tämän jälkeen siirtyvät valittuun pilvipalveluun.

IT-Futura Oy on uusi ja vielä nuori yritys, jolla ei ole vielä isoa asiakaspohjaa, sillä yritys ei ole vielä ehtinyt kovin mainostaa itseään, minkä takia harvat tietää sen olemassaolosta. Tämän takia yrityksellä ei ole paljon dataa tallennettavaksi. Yrityksen vaatimuksena on varmuuskopiointisuunnitelman luominen ottaen huomioon pieni budjetti ja pieni työntekijämäärä, jolloin varmuuskopioinnin on oltava automatisoitu ja turvallinen. Suunnitelman pitää olla luotettava ja helppokäyttöinen sekä yrityksen ympäristöön ja tarpeisiin mukautuva. Lisäksi varmuuskopiointisuunnitelmaan on pystyttävä lisätä pilvitallennustilaa sekä ulkoista tallennustilaa tulevaisuutta varten. Varmuuskopiointipalveluun tulee kuulumaan pilvipalvelun-, ohjelmiston- ja välineiden valinta. Pilvipalvelulta vaatimuksena ovat sisäänrakennetut toimisto-ohjelmat tietojen ja finanssien ylläpitoa varten. Sisäänrakennetuilla toimisto-ohjelmilla tarkoitetaan esimerkiksi muistiinpanotyökaluja ja onlinevideo -kokoustyökalua.

7.2 Varmuuskopiointipalvelun suunnittelu

IT-Futura Oy on nuori yritys, jolla ei ole paljon dataa tallennettavaksi, joten varmuuskopiointisuunnitelman tulee olla suhteellisen yksinkertainen ja kustannustehokas. On kuitenkin tärkeää varmistaa, että varmuuskopiointisuunnitelma on luotettava ja että se voi palauttaa tiedot nopeasti katastrofin tai tietojen katoamisen sattuessa. Yritys käsittelee henkilökohtaisia tietoja, kuten nimiä, osoitteita ja yhteystietoja. IT-Futura varmuuskopioi siis asiakasrekisteriä ja omia sisäisiä asiakirjoja. Kyseinen varmuuskopiointisuunnitelma tehdään vain IT-Futura yritykselle ottaen huomioon sen tarpeet, eikä varmuuskopiointisuunnitelma koske yrityksen asiakkaita. Lisäksi on olennaista ottaa huomioon varmuuskopion suorittamisen "rajaehdot", kuten varmuuskopiointi-ikkuna. Tämä tarkoittaa sopivaa aikaa varmuuskopioinnin suorittamiseen tuotantoprosessia häiritsemättä. It-Futuralla ei ole 24/7-toimintaa, minkä takia varmuuskopiointi sopii parhaiten suoritettavaksi yöllä, esimerkiksi kello 21:00, jotta minimoitaisiin vaikutukset yrityksen päivittäiseen toimintaan. Tämä tapa sulkee pois myös kysymyksen verkkoyhteydestä. Koska yrityksellä on pieni budjetti ja rajallinen tietomäärä, niin ei välttämättä tarvitse investoida erilliseen verkkoyhteyteen yksinomaan varmuuskopiointia varten. Tekemällä varmuuskopiointi työajan ulkopuolella, yritys pystyy minimoimaan mahdolliset verkkoyhteysongelmat. Lisäksi yrityksellä tulee olemaan oma pilvipalvelu.

It-Futuran varmuuskopiointisuunnitelma tulisi sisältää säännölliset varmuuskopiot: täysi varmistus ja inkrementaalinen varmistus. Inkrementaalinen varmuuskopiointi tallentaa vain muutokset, jotka on tehty viimeisen täyden varmuuskopioinnin jälkeen, kun taas täydelliset varmuuskopiot tallentavat kaikki tiedot. Tämä varmuuskopioiden yhdistelmä tarjoaa tasapainon tallennettujen tietojen tiheyden ja täydellisyyden välillä ja auttaa minimoimaan tietojen menetyksen riskin. Täyden varmuuskopioinnin ja lisävarmuuskopioinnin yhdistelmän käyttäminen on yleinen käytäntö varmuuskopiointisuunnittelussa, erityisesti pienissä ja keskisuurissa yrityksissä, joilla on rajalliset resurssit. Inkrementaalinen varmuuskopiointi toteutetaan päivittäin maanantaista lauantaihin, jolloin sunnuntaille jää täysi varmistus tehtäväksi.

Täysi varmuuskopio on täydellinen varmuuskopio kaikista tiedoista ja tiedostoista. Se tehdään yleensä viikoittain tai kuukausittain, ja se luo perustan kaikille myöhemmille varmuuskopioille. Täysi varmuuskopiointi kestää kauemmin kuin asteittainen varmuuskopiointi ja vaatii enemmän tallennustilaa, mutta se varmistaa, että kaikki tiedot varmuuskopioidaan täydellisen tietojen katoamisen tapauksessa. IT-Futuralle tulee tehdä viikoittain täydellinen varmuuskopio kaikista tärkeistä tiedoista ja tiedostoista, mukaan lukien asiakasrekisteri ja sisäiset asiakirjat. Inkrementaalinen varmuuskopiointi varmuuskopioi vain tiedot, jotka ovat muuttuneet edellisen täyden varmuuskopioinnin tai porrastetun varmuuskopioinnin jälkeen. Se tehdään yleensä

päivittäin ja vaatii vähemmän tallennustilaa ja aikaa kuin täydellinen varmuuskopiointi. Inkrementaalinen varmuuskopiointi vähentää varmuuskopiointiikkunaa ja varmistaa, että vain uudet ja muuttuneet tiedot varmuuskopioidaan, mikä säästää tallennustilaa ja lyhentää varmuuskopiointiaikaa. IT-Futuralle kaikki tärkeät tiedot ja tiedostot tulee varmuuskopioida päivittäin.

Lopuksi on tärkeää testata ja tarkistaa säännöllisesti varmuuskopiointisuunnitelmaa sen varmistamiseksi, että tiedot voidaan palauttaa katastrofin tai muun tietojen katoamisen sattuessa. Tämä voidaan tehdä palauttamalla ajoittain varmuuskopiot tietojen eheyden ja täydellisyyden testaamiseksi sekä testaamalla palautusprosessia sen varmistamiseksi, että se toimii tarkoitetulla tavalla.

7.3 Pilvipalvelun valinta

IT-Futura Oy:n varmuuskopiointipalveluun pilvipalveluksi valitaan Google Drive. Yrityksen vaatimuksena oli sisäänrakennetut toimisto-ohjelmat tietojen ja finanssien ylläpitoa varten, minkä takia vaihtoehdoiksi jäi Google Drive ja OneDrive. Yritys tarjoaa myös asiakkaille mahdollisuuden ilmaiseen konsultointiverkkotapaamiseen, joten edellytyksenä olisi jonkinlainen verkkokokoustyökalu.

Google Driven saa hinnalla 10,40€ kuukaudessa käyttäjää kohden, jolloin tallennustilaa on käyttäjää kohden 2 Tt, käytössä yksilöity ja suojattu yrityssähköposti sekä paketin sisältämät sovellukset kuten, Google Meet, Docs, Sheets, Slides, Keep, Sites ja Forms. OneDrive olisi tarjonnut kaikki toimisto-ohjelmat (mukaan lukien yrityssähköpostin) käyttöön hinnalla 12,60 € kuukaudessa käyttäjää kohden, jolloin kokonaistallennustila olisi ollut vain 1 Tt. Lisäksi Google Drive tarjoaa ilmaiseksi 15 Gt tallennustilaa sillä välin, kun OneDrive tarjoaa vain 5 Gt ilmaista tallennustilaa. Täten valittiin yrityksen pilvipalveluksi Google Driven.

7.4 Ohjelmiston valinta

Varmuuskopiointipalveluun valittiin Cobian Backup sen helppokäyttöisyyden ja asetuksien monipuoleisuuden takia. Sen hyvinä puolina on se, että ohjelmisto pystyy pakkaamaan, salaamaan ja pilkkomaan tiedostoja itse. Käyttäjän ei tarvitse nimetä varmuuskopiot päivämäärän ja kellonajan mukaan, sillä ohjelma tekee sen käyttäjän puolesta. Käyttöliittymältään Cobian Backup on käyttäjäystävällinen ja sen avulla voi suorittaa täydelliset-, differentiaaliset ja inkrementaaliset -

varmuuskopiot. Täten kyseinen ohjelmisto sopii parhaiten, sillä jos tulevaisuudessa on tarvetta muulle varmuuskopiointityypille, niin ei tarvitse etsiä uutta varmuuskopiointiohjelmistoa.

7.5 Välineiden valinta

Laitteistoa valittaessa on otettava huomioon sen vikaherkkyys, tallennuskapasiteetti ja laitteen hinta. Tätä oppinäytetyötä varten hintavertailu suoritetaan Jimms.fi verkkosivun kautta, koska sillä on suurin tuotevalikoima, etenkin kun kyse on elektroniikasta. Pk-yritykselle magneettinauha on vähän lioteltu laitteisto, vaikka säilyvyydeltään ja hinnaltaan se on hyvä vaihtoehto. Magneettinauhan käyttöä varten tarvitaan aina ihminen, minkä takia tätä vaihtoehtoa ei oteta huomioon. Magneettinauhasta löytyy kalliitakin itsevaihtavia nauha-asemia, mutta suhteellisen pienen budjetin takia nekään ei sovi vaihtoehdoksi. Optiset mediat myös jätetään ehdokaslistan ulkopuolelle, koska löytyy edullisempia ja paljon helpompia varmennustapoja. Täten varmuuskopiointipalvelun laitteistoksi valitaan verkkolevy eli NAS-palvelin, koska kaikista tellennusmedioista se näyttäytyi parhaaksi vaihtoehdoksi. Lisäksi verkkolevyn nojalle otetaan tueksi ulkoinen kovalevy, johon tietyin väliajoin varmuuskopioidaan tiedostot. Kovalevy säilytetään yrityksen toimiston ulkopuolella turvallisuutta varten. Verkkolevyn käyttöönotto on helppoa, sillä on suuri kapasiteetti ja sen saa edullisella kustannuksella. Verkkolevy yhdistää tallennustilan yhteen paikkaan ja tukee pilvitasoa ja tehtäviä, kuten arkistointia ja varmuuskopiointia.

Jimms:ssä on suuri valikoima verkkolevyjä eri hintaluokissa. Halvimman verkkolevyn saa 100 euron tienoilla (Synagogy DiskStation DS120j ilman kovalevyjä) ja kalleimman saa yli 8 000 eurolla (QNAP TS-h1277XU-RP 128GB). Yrityskäyttöä varten olisi hyvä hankkia verkkolevyn minimissään kahdella kovalevyllä varustettuna ja joka tukee RAID-tekniikkaa. Koska yritys on nuori ja datamäärää on vähän, riittää käyttöön kahdella kovalevyllä varustettu verkkolevy, kuten Western Digital 6TB My Cloud Home Duo. Kyseinen NAS-palvelin on kapasiteetiltaan 2 x 3 Tt ja tukee RAID 1-tekniikkaa, mikä siis tarkoittaa sitä, että tallennettaessa tiedostoja kovalevylle, ne automaattisesti kopioidaan myös toiselle levylle. Sen hinta Jimms.fi sivulla on kirjoitushetkellä 362,00 € (Jimms.fi 2023). Jos yritys tavoittelee parempaa vikasietoisuutta niin voi myös harkita toisen verkkolevyn hankintaa, jonka asennetaan muualle ja johon tehdään tietojen peilaus yrityksen tiloissa olevalta verkkolevyltä. Jos yritys kuitenkin kokee, että datamäärä tulee paljon kasvamaan, niin voi harkita neljällä kovalevyllä varustettua verkkolevyä. Tässä oppinäytetyössä kuitenkin päädyttiin hankkimaan juuri kahden kovalevyn NAS-palvelin.

7.6 Ohjelman asentaminen

IT-Furua Oy hoitaa itse valmiin varmuuskopiointipalvelunsa asentamisen. Ennen varmuuskopiointipalvelun käyttöönottoa, NAS-palvelin on asennettava yrityksen omaan lähiverkkoon, jos sitä ei ole vielä tehty. Valitun palvelimen mukana tulevat kaikki tarvittavat asennusohjeet. Jos on tarvetta, niin ne on myös ladattavissa internetistä tuottajien omilta kotisivuilta. Aloitetaan varmuuskopiointisuunnitelman toteuttaminen lataamalla nettisivuilta kaikki vaadittavat tiedostot asennusta varten. Ne on helpompaa ja nopeampaa asentaa useammalle koneelle jos ne tallentaa esimerkiksi verkkolevylle tai USB-tikulle. Pilvipalvelun synkronointiohjelmaa on tarvetta asentaa vain yhdelle pöytäkoneelle. Asennustiedosto on löydettävissä Googlen omilta Google Drive nettisivuilta. Asennetaan Google Drive oletusasetuksin, minkä jälkeen ohjelman voi avata. Yritykselle on luotava omat tunnukset ja kirjauduttava sitten niillä sisään vaihtaen heti aluksi lähde- ja kohde kansiot varmuuskopiointia varten.

Cobian Backup varmuuskopiointiohjelma on asennettava kaikkiin yrityksen pöytäkoneisiin, joissa varmuuskopioitavia tiedostoja tullaan käsittelemään. Kun kaikki on asennettu, ohjelman käyttöliittymässä asetetaan uuden varmuuskopioinnin asetukset ja valitaan sille sopiva ajastus. Ohjelma jää toimimaan taustalle suorittaen halutut varmuuskopioit asetettuina ajankohtina.

8 Pohdinta

Yritykselle parhaan varmuuskopiointiohjelmiston selvittäminen ja itse varmuuskopiointisuunnitelman luominen voi olla erittäin monimutkaista useista syistä. Markkinat itsessään ovat valtavat, ja saatavilla olevien ratkaisujen määrä on kaikkien aikojen ennätys, ja ne tarjoavat runsaasti ominaisuuksia eri asiakastyypeille. Laaja tutkimus auttaa varmasti löytämään sopivan varmuuskopiointiratkaisun, mutta monet olosuhteet voivat rajoittaa varmuuskopiointiratkaisujen valintaa jollain tavalla. Esimerkiksi monet kattavammat varmuuskopiointiratkaisut tarjoavat monia ominaisuuksia, joille ei ehkä tule ikinä käyttöä, mikä tekee yhden näistä ratkaisuista itse kyseenalaisen päätöksen. Onneksi on olemassa monia varmuuskopiointiratkaisuja, jotka on suunnattu pienille yrityksille, joiden vaatimukset varmuuskopiointijärjestelmään ovat alhaisemmat. Osa näistä varmuuskopiointiratkaisuista on vielä jopa ilmaisiakin, mutta useimmiten ilmaisen varmuuskopioratkaisun valitseminen on vielä monimutkaisempaa kuin maksullisen ratkaisun valitseminen.

Tässä tutkimuksessa käsiteltiin kolme suosituinta varmuuskopiointimenetelmää (täysi-, inkrementaalinen- ja differentiaalinen varmistus) sekä tietojen palautusta. Jokaisella varmuuskopiointimenetelmällä on omat hyvät ja huonot puolensa ja menetelmän valinta riippuu hankkijan tarpeista ja tavoitteista. Aiheesta löytyy paljon tietoa ja tulevaisuudessa tiedon määrä tulee entisestään laajenemaan, sillä innovatiivisia varmuuskopiointi- ja palautusratkaisuja luodaan koko ajan lisää. Oppinäytetyön tavoitteena oli luoda IT-Futura Oy:lle varmuuskopiointipalvelu, johon kuului pilvipalvelun-, ohjelmiston- ja välineiden valinta. Kyseinen varmuuskopiointipalvelu sopii hyvin ICT-alan yritykselle ottaen huomioon sen tarpeet ja budjetti. Sitä voi tarvittaessa mukauttaa IT-Futura Oy:n tarpeiden mukaiseksi ja sen avulla pystyy täysin automatisoimaan varmuuskopiointi, jolloin eliminoituu mahdollisuus inhimillisiin virheisiin, kuten esimerkiksi vahingossa poistaminen. Lisäksi varmuuskopioinnin luotettavuus kasvaa, sillä se on ajastettu tehtäväksi päivittäin ja kopiot tallennetaan sekä pilvipalveluun että verkkolevylle.

Yksi tärkeimmistä huomioista varmuuskopiointisuunnitelman suunnittelussa oli tietotyypit, joita IT-Futura käsittelee, mukaan lukien henkilötiedot, kuten nimet, osoitteet ja yhteystiedot, sekä arkaluontoiset tiedot, kuten kirjautumistiedot tai taloudelliset tiedot. Varmuuskopiointisuunnitelma ottaa huomioon näiden tietojen turvallisuuden ja yksityisyyden ja varmistaa, että ne on suojattu tietojen katoamisen tai vioittumisen varalta. Toinen näkökohta oli yhtiön rajallinen budjetti ja pieni tietomäärä. Siksi valittiin pilvivarmuuskopioratkaisu, joka on kustannustehokas ja tehokas pienyrityksille. Lisäksi tarvitaan vain yksi Internet-verkkoyhteys, koska kaikki varmuuskopiot tehdään yöllä, mikä varmistaa, että työntekijät voivat jatkaa työskentelyä päivän aikana keskeytyksettä.

Itse palvelun käyttöönotto on helppoa. Se vaatii vain varmuuskopiointiohjelman ja pilvipalvelun asennuksen, mihin molempiin löytyy niiden nettisivuilta ladattava vaiheittainen ohje kuvineen. Lisäksi on asetettava varmuuskopiointi. Perustetaan pilvipalveluun yritykselle oman tilin, jos sellaista ei ole vielä entuudestaan olemassa. Tämän jälkeen varmuuskopiointi toimii automaattisesti ja vaatii vain ajoittaista valvontaa. Kyseinen varmuuskopiointipalvelu sopii mainiosti myös yksityiskäyttöön eli yhden ihmisen tiedostojen varmuuskopiointiin.

Tulevaisuuden tutkimukseen on olemassa useita kehitysehdotuksia, joita voidaan harkita IT-Futuran varasuunnitelman perusteella. Yksi mahdollinen tutkimusalue voisi olla vaihtoehtoisten varmuuskopiointiratkaisujen ja niiden kustannustehokkuuden tutkiminen pienyrityksille, kuten IT-Futuralle. Tämä voi esimerkiksi sisältää paikan päällä olevien varmuuskopiointiratkaisujen käyttökelpoisuuden arvioinnin. Toinen mahdollinen tutkimusalue on erilaisten varmuuskopiointitaajuuksien ja -tyyppien vaikutus varmuuskopiointisuunnitelman yleiseen turvallisuuteen ja luotettavuuteen. Tämä voi sisältää erilaisten varmuuskopiointiaikataulujen testaamisen tai vaiheittaisten varmuuskopioiden tehokkuuden vertaamista differentiaalisiin varmuuskopioihin. Lisäksi olisi hyödyllistä tarkastella ehdotetun varasuunnitelman tehokkuutta käytännössä ja arvioida, tarvitaanko muutoksia tai parannuksia. Tämä voi sisältää varmuuskopiointisuunnitelman seurantaa pidemmän aikaa ja varmuuskopiointi- ja palautusprosessien onnistumisen arvioimista.

Lopuksi on myös tärkeää ottaa huomioon varmuuskopiointisuunnittelun eettiset vaikutukset, erityisesti mitä tulee arkaluonteisten tietojen käsittelyyn. Tulevaisuuden tutkimuksessa voitaisiin selvittää oikeudellisia ja eettisiä näkökohtia, jotka on otettava huomioon suunniteltaessa varasuunnitelmaa IT-Futuran kaltaiselle pienyritykselle.

9 Johtopäätökset

Tietotekniikan jatkuvasti kasvava kysyntä sekä yhteiskunnan globaali tietokoneistuminen eivät ole tämänhetkistä sattumaa. Yhä useampi palvelu tarjotaan väestölle käyttämällä elektronisia laitteita, joista pääosa on henkilökohtaiset tietokoneet. Suurin osa tehtävistä, kuten tuotannon eri prosessien hallinta, työn organisointi, joukkoliikenteen ohjaaminen ja erilaisten kuljetusten organisoiminen, ovat annettu koneiden tehtäväksi laskea ja ohjata. Jos jokin näistä ketjuista epäonnistuu, seuraukset voivat olla arvaamattomia. Juuri tämän takia tietojen suojaaminen ja itse varmuuskopiointi ovat tällä hetkellä varsin akuutteja aiheita. Teknologian ja informatisoinnin jatkokehitys merkitsee tallennetun tiedon määrän voimakasta kasvua. Tämä johtaa tiedon tallennus- ja varmuuskopiointialan tutkimuksen voimakkaaseen kysyntään sekä sen edeltävään kehitykseen, jolloin ohjelmistotuotteita parannetaan ja mukautetaan yhteiskunnan tarpeisiin.

Valitettavasti tällä hetkellä ei ole olemassa täysin varmaa ja lopullista varmuuskopiointiratkaisua. Varmuuskopiointiin on paljon eri ohjelmia, välineitä ja valmiita palveluita. Halutessaan yritys voi organisoida varmuuskopioinnin omin käsin tai se on myös toteuttavissa yrityksen ulkopuolelta. Tärkeimpänä tavoitteena on kuitenkin suojata tarvittavat tiedot tavalla, joka takaa niiden säilymisen myös suurempien onnettomuuksien, vahinkojen ja varkauksien sattuessa.

Lähteet

About Luis Cobian. s.a. About Luis Cobian. WWW-dokumentti. Luettavissa: https://acsdata.com/how-hard-drives-work/. Luettu 07.01.2023.

Acronis 2022. What is Backup? (Data Backup) Comprehensive Guide. Luettavissa: https://www.acronis.com/en-eu/blog/posts/data-backup/. Luettu 14.09.2022.

ACS Data Recovery 2021. Hard Drive Design and Operation. Luettavissa: https://acsdata.com/how-hard-drives-work/. Luettu 19.02.2023.

Backup4all 2022a. Backup types. Luettavissa: https://www.backup4all.com/backup-types-kb.html. Luettu 15.09.2022.

Backup4all 2018. Differential backup. Luettavissa: https://www.backup4all.com/differential-backup-kb.html. Luettu 11.10.2022.

Backup4all 2022b. Incremental backup. Luettavissa: https://www.backup4all.com/incremental-backup-kb.html. Luettu 14.09.2022.

Burton, A. 2020. Data Backup and recovery Methods. Luettavissa: https://www.datto.com/blog/data-backup-and-recovery-methods-the-basics-you-need-to-know. Luettu 04.09.2022.

Bigelow, S., Lutkevich, B., Kran, G. 2022. TechTarget. Luettavissa: https://www.techtarget.com/searchstorage/definition/network-attached-storage. Luettu 20.12.2022.

CobianSoft 2019. Cobian backup/Cobian Reflector. Luettavissa: https://www.cobiansoft.com/cobianbackup.html. Luettu 15.02.2023.

Crocetti P. 2018. Magnetic tape storage. TechTarget. Luettavissa: https://www.techtarget.com/searchdatabackup/definition/magnetic-tape. Luettu 20.01.2023.

DesignRush 2023. Types of Backups. Luettavissa: https://www.designrush.com/agency/it-services/trends/types-of-backups. Luettu 07.02.2023.

Duplicati 2 User's Manual 2023. Introduction. Duplicati. Luettavissa: https://duplicati.readthedocs.io/en/latest/. Luettu 13.11.2022.

Drake, A. 2022. Your Data Is at Risk: Why Backup Is So Important. Luettavissa: https://www.g2.com/articles/what-is-backup. Luettu 14.09.2022.

Dropbox 2023. Products: Dropbox. Luettavissa: https://www.dropbox.com/dropbox. Luettu 05.02.2023.

FBackup User Manual 2021.Softland. s. 7-8 Luettavissa: https://docs.google.com/viewer?url=https%3A%2F%2Fwww.fbackup.com%2Fdownload%2Fpdf%2FUser-Manual.pdf. Luettu 13.01.2023.

Geeksforgeeks 2020. Magnetic Tape memory. Luettavissa: https://www.geeksforgeeks.org/magnetic-tape-memory/. Luettu 23.02.2023.

Gillis, A., SSD (solid-state drive). TechTarget. Luettavissa: https://www.techtarget.com/searchstorage/definition/SSD-solid-state-drive. Luettu 05.01.2023.

Google Workspace 2023. Hinnat. Google. Luettavissa: https://workspace.google.com/intl/fi/pricing.html. Luettu 03.02.2023.

IBM 2022. Hard Disk Drive (HDD) vs. Solid State Drive (SDD): What's the difference? Luettavissa: https://www.ibm.com/cloud/blog/hard-disk-drive-vs-solid-state-drive. Luettu 26.12.2022.

Maayan G. 2022. The future of Data Backup and Recovery. Luettavissa: https://www.computer.org/publications/tech-news/trends/the-future-of-data-backup-and-recovery. Luettu 21.10.2022.

Mayer A. 2022. Backup Types Explained: Full, Incremental, Differential. Luettavissa: https://www.nakivo.com/blog/backup-types-explained-full-incremental-differential-synthetic-and-forever-incremental/. Luettu 21.10.2022.

Mega 2023. Products: cloud storage. Luettavissa: https://mega.io/storage. Luettu 03.03.2023.

Navasardyan N. 2020. What is Incremental Backup and How Can I Benefit from It? Luettavissa: https://10web.io/blog/incremental-backup-and-how-to-benefit-from-it/. Luettu 21.10.2022.

Orphan file. 2020. Computer Hope. Luettavissa: https://www.computerhope.com/jargon/o/orphfile.htm#:~:text=An%20orphan%20file%20is%20a,space%20and%20are%20never%20used. Luettu 20.03.2023.

Platinium Data Recovery 2022. Data loss: How to Differentiate Between Logical and Physical Data Loss. Luettavissa: https://platinumdatarecovery.com/blog/data-loss-how-to-differentiate-between-logical-and-physical-data-loss. Luettu 11.10.2022.

Provazza, A. 2023. Microsoft OneDrive. TechTarget. Luettavissa: https://www.techtarget.com/searchmobilecomputing/definition/Microsoft-OneDrive. Luettu 17.02.2023.

Rao, U., Nayak, U. 2014. The InfoSec Handbook, s. 264-265. WWW-dokumentti. Luettavissa: http://link.springer.com/book/10.1007/978-1-4302-6383-8. Luettu 21.10.2022.

Rouse, M. 2016. Magnetic Tape. Techopedia. Luettavissa: https://www.techopedia.com/definition/8212/magnetic-tape. Luettu 23.02.2023.

Rouse, M. 2015. Optical Media. Techopedia. Luettavissa: https://www.techopedia.com/definition/5309/optical-media. Luettu 23.02.2023.

Sappington, J. 2022. Google Drive Backup and Sync: Everything you need to know. Luettavissa: https://www.promax.com/blog/google-drive-backup-and-sync. Luettu 08.03.2023.

Sheldon, R., Brown, R. 2021. Optical storage. Luettavissa: https://www.techtarget.com/searchstorage/definition/optical-storage. Luettu 15.02.2023.

SyncBackFree V10 PDF User Guide 2023. 2BrightSparks. Luettavissa: https://www.2brightsparks.com/assets/pdf/SyncBackFreeV10.pdf. Luettu 12.01.2023.

Sheldon R. ja Brown R. 2021. Optical disk. TechTarget. Luettavissa: https://www.techtarget.com/searchstorage/definition/optical-disc. Luettu 16.12.2022.

UFS EXPLORER 2022. What is data recovery? Luettavissa: https://www.ufsexplorer.com/articles/what-is-data-recovery/. Luettu 11.10.2022.

User Manual 2021. FBackup, Softland. Luettavissa: https://www.fbackup.com/download/pdf/User-Manual.pdf. Luettu 17.02.2023.

User Manual. Back4Sure. Luettavissa: https://www.ukrebs-software.de/download/back4sure/ManualBack4SureEnglish.pdf. Luettu 21.02.2023.

Vitanium 2020. The Pros and Cons of Different Data Backup Methods. Luettavissa: https://vitanium.com/the-pros-and-cons-of-different-data-backup-methods/. Luettu 21.10.2022.

What is Cobian Backup? 2020. CompareCamp. Luettavissa: https://comparecamp.com/cobian-backup-review-pricing-pros-cons-features/. Luettu 19.02.2023.