Kaisa Koskinen

TIETOJEN VARMISTAMINEN

Tietojenkäsittelyn koulutusohjelma

2017

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

TIETOJEN VARMISTAMINEN

Koskinen, Kaisa
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Toukokuu 2017
Ohjaaja: Nuutinen, Petri
Sivumäärä: 26
Liitteitä: -

Asiasanat: Liiketoiminnan jatkuvuussuunnitelma, katastrofista toipumissuunnitelma, varmistukset.

Tutkimuksessa käsitellään eri varmistusratkaisuja ja varmistusmenetelmiä. Varmistuspolitiikan luominen on osa liiketoiminnan jatkuvuussuunnitelmaa. Tutkimuksessa käydään läpi liiketoiminnan jatkuvuussuunnitelmaa varmistuksien ja katastrofista toipumisen osalta.

Toiminnallisessa osuudessa käydään läpi varmistusratkaisun käyttöönottoa ja sen eri vaiheita työn toimeksiantajan Saint-Gobain Technology Services Nordic & Baltic delegaation työasemille. Kohderyhmän rajauksessa todettiin, että varmistusratkaisu tullaan implementoimaan projektin aikana ainoastaan kannettaville tietokoneille. Tutkimuksessa käsitellään varmistusratkaisun ylläpitovaihetta sekä toimeksiantajan muuttuneita prosesseja liittyen käyttäjätunnusten luontiin. Tutkimuksessa perehdytään myös varmistusratkaisuun liittyvään raportointiin ja hallintaan.

Data backup

Koskinen, Kaisa
Satakunta University of Applied Sciences
Degree Programme in Information Technology
May 2017
Supervisor: Nuutinen, Petri
Number of pages: 26
Appendices: -

Keywords: Business continuity plan, disaster recovery plan, backup.

The purpose of this thesis was to present different backup solutions and backup procedures. Creating backup policy is part of business continuity plan. In this thesis examines business continuity plan from disaster recovery point of view.

In operational part goes through steps for implementing backup solution for the customer's Saint-Gobain Technology Services Nordic & Baltic workstations and different phases within the work. While limiting target group of the implementation of backup solution conclusion was came up to restrict workstations involved only for laptops. In this theses backup solution maintaining and changed processes in relation to creating new user accounts is also went through. In this thesis there is presented also reporting and management relating the implemented backup solution.

SISÄLLYS

1 JOHDANTO

Tuotettavan tiedon määrä kasvaa koko ajan. Vaikka käytössämme on yhä enemmän internetin pilvipalveluista jaettuja resursseja, ei tiedon varmistamisen tarve ole poistunut. Tässä työssä käsittelen varmistamista yleisesti sekä käyn tarkemmin teknisellä ja toiminnallisella tasolla läpi tietojen varmistamiseen käytössä olevia erilaisia varmistusmenetelmiä sekä niiden vahvuuksia ja heikkouksia.

Liiketoiminnan jatkuvuussuunnitelman tärkeimpiä osa-alueita on tiedon varmistaminen. Koska yrityksissä yhä tärkeämpi osa liiketoimintaa on tallennettu informaatio, on yhä enenevissä määrin yrityksen tärkeintä omaisuutta sen käyttäjien tietokoneilleen tallentama tieto. Luonnonkatastrofit, kuten tulipalot, vesivahingot tai varkaudet, tekniset toimintahäiriöt ja virusten tuomat uhat voivat aiheuttaa yrityksen liiketoiminnalle yllättävän suuria ja joskus jopa korvaamattomia menetyksiä. Tietojen varmistamista voidaan mielestäni pitää yrityksen ottamana vakuutuksena mahdollisten onnettomuuksien varalle. Onnettomuuksien riski on minimoitava ja varmistusratkaisuista huolehtimalla onnettomuuden sattuessa yritys ja sen liiketoiminta selviävät tilanteesta ilman kohtuuttomia menetyksiä. Varmistusratkaisun laajuuden tulisi olla suhteessa työn keskeytymisajasta muodostuviin kustannuksiin/tappioihin, mitä suuremmat kustannukset/tappiot työn keskeytymisestä muodostuvat sen suurempi pitäisi olla panostus valittavaan varmistusratkaisuun. Varmistamisessa on kyse tehdyn työn, ei tietokoneiden, tallentamisesta. Varmistetun tiedon tulee olla suojattu sekä palautettavissa vaadittavalla nopeudella.

Tiedon varmistamisen ohella on mielestäni hyvä suunnitella myös varmistettujen tietojen palautukseen liittyvät prosessit aina käyttäjän yksittäisten tiedostojen palauttamisesta, suurempien osakokonaisuuksien, kuten käytössä olevin tietojärjestelmien palauttamiseen katastrofista toipumisen yhteydessä.

2 VARMISTAMISESTA YLEISESTI

Säännölliset varmistukset ovat ensisijaisen tärkeitä tietojen katoamisesta tai vaurioitumisesta johtuvasta katastrofista toipumiseen. Kattavan ja vankan varmistuspolitiikan (Backup Policy) tekeminen vaatii sekä aikaa että rahaa. Käytetty aika ja raha eli resurssit tulee mitoittaa suhteessa varmistettavan tiedon arvoon. (Lo 2012.)

2.1 Liiketoiminnan jatkuvuussuunnitelma

Liiketoiminnan jatkuvuussuunnitelma (business continuity plan) metodologia, missä luodaan ja määritellään liiketoiminnan jatkuvuuden takaavat operaatiot ennen katastrofia, katastrofin aikana ja katastrofin jälkeen. Katastrofi on sellainen suunnittelematon tapahtuma, joka aiheuttaa keskeytyksen organisaation normaaleihin liiketoimintaprosesseihin. Liiketoiminnan jatkuvuussuunnitelma koostuu prosesseista, jotka varmistavat organisaation liiketoiminnan jatkuvuuden katastrofin sattuessa. Liiketoiminnan jatkuvuussuunnitelman yksi osa-alue on katastrofista toipumissuunnitelma (disaster recovery plan). Katastrofista toipumissuunnitelmassa käsitellään mahdolliset katastrofit ja miten katastrofeista toivutaan mahdollisimman nopeassa ajassa, minimoiden palautukseen ja liiketoimintakatkokseen liittyvät kustannukset. (Varghese 2002, 2)

2.2 Katastrofista toipumissuunnitelma

Katastrofista toipumissuunnitelma (disaster recovery plan) tarjoaa tehokkaan ratkaisun elintärkeiden liiketoimintaprosessien uudelleen käyttöönottoon tietyn aikaikkunan sisällä. Katastrofi voi olla tietomurto, tiedon katoaminen, tulipalo, tulva tai mikä tahansa tapahtuma mikä johtaa tietojen pääsyyn estymiseen. Katastrofista toipumissuunnitelman tarkoitus on minimoida suunnitteluun menevä aika katastrofin sattuessa. (Martin 2002, 2-3)

Katastrofista toipumissuunnitelma on osa liiketoiminnan jatkuvuussuunnitelmaa. Toipuminen palvelimen sähkökatkosta, tietoturvaloukkauksesta, tai hurrikaanista, kaikki menevät katastrofista toipumissuunnitelman piiriin. Katastrofista toipumisessa

on usein monia erillisiä kohtia suunnitteluvaiheessa, tosin nämä suunnitteluvaiheen kohdat harvoin vastaavat todellisuutta itse katastrofin sattuessa. Katastrofista toipumissuunnitelma tarjoaa keinoja pysäyttää katastrofin vaikutukset liiketoimintaan niin pian kuin mahdollista ja määrittää parhaan vaihtoehtoisen tavan jatkaa liiketoimintaa. (Rima 2013, 4)

2.3 Varmistuspolitiikka

Hyvästä suunnittelusta huolimatta katastrofeja tapahtuu aika-ajoin. Ihmiset tekevät virheitä, rikkeitä tapahtuu ja tekniikka hajoaa. Tällaisella hetkellä backupit ovat ainoa toipumisvaihtoehto. Data on kaikkein tärkein asia mikä tulee varmistaa. Varmistusten toistuvuus määritellään varmistuspolitiikassa (Backup Policy). Varmistuspolitiikassa määritellään myös se, minkälaiselle medialle varmistukset tehdään ja kuinka usein varmistettu tieto ylikirjoitetaan, eli varmistuksien kierto -politiikka. Varmistuksien kierron määrittely riippuu käytettävissä olevista resursseista, kuten esimerkiksi varmistusnauhojen määrästä. Varmistettavan datan palauttamiskelpoisuus tulee varmentaa säilyttämällä varmistukset uhkilta, kuten luonnonkatastrofeilta tai tietomurroilta, suojatussa tilassa. Varmistetun datan suojaaminen sekä säännöllinen datan eheyden varmistaminen ovat osa varmistuspolitiikkaa. (Varghese 2002, 125-127)

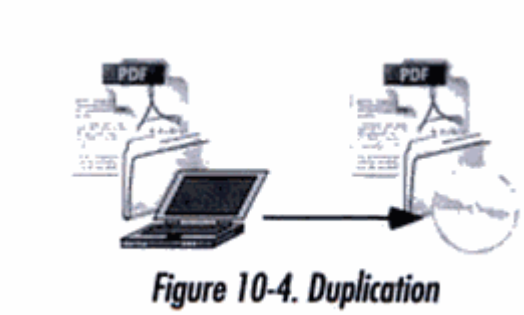
2.4 Tiedon varmistaminen

Tiedon varmistaminen yhdessä katastrofista toipumissuunnitelman kanssa kattavat sekä järjestelmien että tiedon suojaamisen. Tiedon ja järjestelmien suojaaminen voidaan jakaa kolmeen osa-alueeseen vikasietoisuuteen, peilaamiseen tai kahdentamiseen ja arkistoituihin varmistuksiin. (Cougias 2003, 5-7)

Vikasietoisuus ei ole osa varmistuksia. Vikasietoisuudella tarkoitetaan yleisesti sitä, että jollekin järjestelmälle on olemassa varaosa tai varajärjestelmä. Vikasietoisuudella voidaan tarkoittaa yksinkertaisimmillaan kahden verkkokortin asentamista, jos toinen verkkokortti rikkoutuu, otetaan toinen käyttöön tai monimutkaisen clusterin rakentamista palvelimesta, missä kahdennetaan kaikki. (Cougias 2003, 5-7)

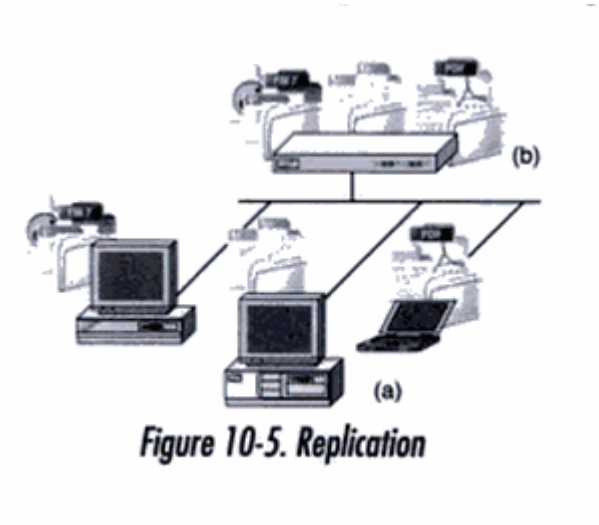
Peilaaminen on osa varmistusta. Peilaaminen koskee hardwarea. prosessissa asennetaan esimerkiksi useampi kiintolevy, joille tietoa tallennetaan siltä varalta, että joku levyistä vioittuu. (Cougias 2003, 5-7)

Kahdentamisessa eli replikointi prosessissa tiedostot kopioidaan lähdetietokoneelta toiseen sijaintiin. Tiedostojen tai kansioiden kahdentamisprosessissa lähdehakemistosta otetaan ne tiedostot tai tiedot, jotka halutaan kahdentaa ja siirretään eksakti kopio kohdehakemistoon, kuten kuvassa 1. Peilaaminen sekä kahdentaminen tähtäävät nopeaan tiedon palauttamiseen. (Cougias 2003, 277)



Kuva 1. Tiedostorakenteen kahdentaminen (Cougias 2003, 277)

Replikointi on prosessi, jossa tiedosto, kansio tai tietokanta tai jokin muu tieto jatkuvasti päivitetään lähdesijainnista toiseen kohdesijaintiin. Replikointi tehdään joko ajastetusti tai välittömästi tiedon muuttuessa. Tiedon replikointi on jatkuvasti päivittyvää ja yhteen sovitettavaa rinnastusta yhden tai useamman lähde- ja kohdehakemiston välillä. Kuvassa 2 prosessissa replikoidaan tiedostot useammalla asiakasohjelmistolla (a) palvelimelle (b) jossa replikointiprosessia ajetaan. (Cougias 2003, 277)



Kuva 2. Replikointi useammalta laitteelta palvelimelle. (Cougias 2003, 277)

Arkistoiduilla varmistuksilla tarkoitetaan tiedosta otettua kuvaa tietyltä ajanhetkeltä. Varmistettava tilanne tiedoista viedään turvalliseen ja suojattuun sijaintiin. Arkistoidut varmistukset koostuvat useasta eri ajanhetkellä otetusta tietojen tilanteesta. Arkistoitujen varmistusten avulla on mahdollista palata tiettyyn ajankohtaan historiassa.
(Cougias 2003, 277)

Tietojen varmistus kostuu seuraavista vaiheista:

1. lähdetiedon kopion ottaminen
2. kopion siirtäminen turvallisesti toiseen sijaintiin
3. kopion säilyttäminen varmistamiseen käytetyn ohjelmiston tarjoamassa formaatissa, sekä informaation historian säilyttäminen tiedon mahdollista palauttamista varten. (Cougias 2003, 288)

3 VARMISTUSMENETELMISTÄ

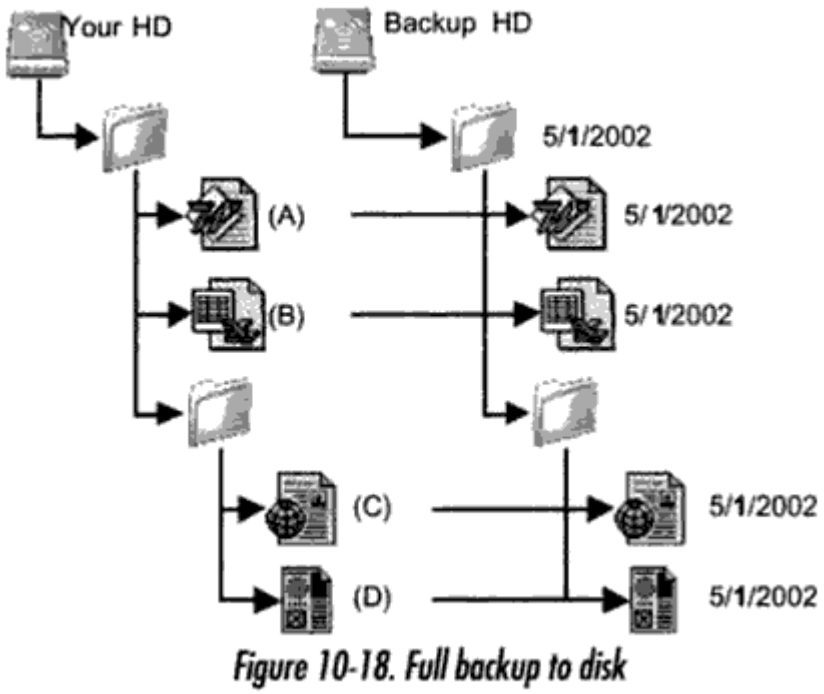
Varmistusratkaisusta riippumatta voidaan valita, varmistetaanko kaikki tiedot (full backup) vai vain osa tiedoista (incremental backup tai differential backup). Luvuissa 3.1.-3.5. on esitetty kuvaus erilaisista varmistusmenetelmistä.

3.1 Full backup

Full backup on kaikkein yleisin varmistustyyppi. Full backup on kokonaisvaltaisin varmistusmenetelmä. Full backup:in ottaminen vie varmistusmenetelmistä eniten aikaa ja vaatii kaikkein eniten levytilaa verrattua muihin varmistustyyppeihin, koska jokaisella varmistuskerralla kaikki tieto siirretään varmistuslaitteelle kohdehakemistoon. (Lo 2012)

Full backup varmistustyyppi ei tutki varmistettavaa tietoa, vaan yksinkertaisesti alkaa kopioida tietoja lähdehakemistosta kohdehakemistoon.

Tietojen palauttaminen full backupista onnistuu helposti, koska varmistettu tieto on täysin identtinen sisällöltään ja hierarkialtaan alkuperäisen tiedon kanssa. Full backup -varmistusmenetelmän ongelma on, että se ei tallenna historiatietoa, vaan palautettavissa on ainoastaan se, mitä viime kerralla on varmistettu. Jos tiedosto katoaa tai korruptoituu, palautettavissa on vain se versio, mikä on viimeksi varmistettu. Kuvassa 3 on esitetty Full backup to disk -rakennetta. (Cougias 2003, 293-295)



Kuva 3. Full backup to disk (Cougias 2003, 295)

3.2 Incremental backup

Incremental backup varmistusmenetelmässä varmistetaan vain muuttuneet tiedostot tai tiedostot, jotka on luotu viimeisen incremental backupin eli lisäävän varmistuskerran jälkeen. Incremental backup -varmistusmenetelmä on nopeampi tapa varmistaa tiedot kuin full backup ja vaatii vähemmän levytilaa. Yksittäisten tiedostojen palauttaminen on nopeaa, koska pystyt hakemaan muuttuneen tiedoston palautettavaksi tietyltä ajan hetkeltä. Tiedostojen täydellinen palauttaminen on full backup -varmistusmenetelmään verrattuna hitaampaa, koska incremental backup -varmistusmenetelmällä otettu varmistus tulee palauttaa jokainen lisätty osavarmistus kerrallaan. Löytääkseen jonkun tietyn version varmistetusta tiedostosta voidaan joutua palauttamaan useampi eri incremental backup -varmistusmenetelmällä otettu osavarmistus. (Lo 2012.)

3.3 Differential backup

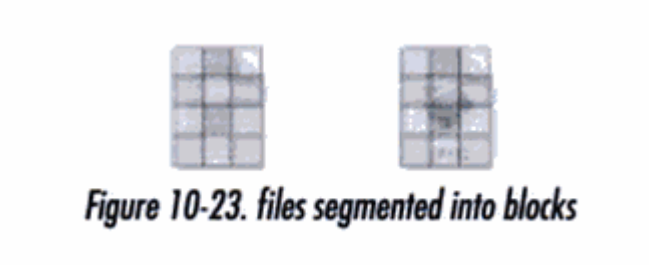
Differential backup -varmistusmenetelmällä varmistetaan myös osajoukko tiedoista, kuten incremental backup:ssakin. Differental backup varmistaa viimeisen Full backupin jälkeen luodut uudet tiedostot sekä muuttuneet tiedostot. (Lo 2012.)

Differential backup varmistusmenetelmä tutkii tietojen luonti ja muokkauspäivää. Jos tiedostoa on muokattu viime kertaisen full backupin jälkeen, lisätään se differential backupiin. Tietojen palauttaminen differential backup -varmistusmenetelmällä otetusta varmistuksesta on nopeampaa kuin incremental backup varmistusmenetelmällä otetusta varmistuksesta, koska jokainen varmistuskerta lisätään yhden ja saman varmistuskerran perään aina seuraavaan full backup -kertaan asti. (Cougias 2003, 301)

3.4 Delta block backup

Delta block -varmistusmenetelmällä evaluoidaan muuttunut tieto jakamalla jokainen tiedosto erillisiin lohkoihin. Varmistusohjelmisto tekee jaksollisen tarkistuksen erillisellä mekanismilla (Cyclical redudancy check, CRC) verratakseen jokaista lohkoa muokatusta tiedostosta jo varmistetun tiedoston lohkoihin. Kun varmistusohjelmisto

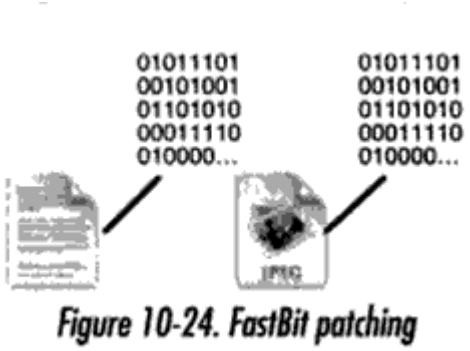
havaitsee eroavaisuuden lohkoissa, varmistaa se tiedoston niiden lohkojen osalta, jotka ovat muuttuneet sen sijaan, että varmistettaisiin koko muuttunut tiedosto. Delta block varmistusmenetelmä säästää aikaa ja vie vähemmän tilaa varmistuksien kohdehakemistosta. (Cougias 2003, 303)



Kuva 4. Tiedosto segmentoitu lohkoihin (Cougias 2003, 303)

3.5 FastBit patching

FastBit patching eroaa Delta block backupista vain siltä osin, että se käsittelee tietoja binääritasolla lohkotason sijaan. Tämä ansiosta muuttuneen tiedon määrä pystytään vielä tarkemmin rajaamaan ja varmistettavan tiedon määrää saattaa parhaimmillaan olla vain puolet Delta block backup -varmistusmenetelmällä varmistetun tiedon määrästä. (Cougias 2003, 304)



Kuva 5. Tiedosto muunnettuna binääritasolle (Cougias 2003, 304)

4 ERILAISISTA VARMISTUSRATKAISUISTA

4.1 Paikallinen varmistusratkaisu

Paikallisessa varmistusratkaisussa tiedot kopioidaan toiselle kiintolevylle, toiselle medialle tai jaetulle verkkolevylle. Tiedostojen varmistus voidaan käynnistää joko manuaalisesti tai automaattisesti tietyin väliajoin. Tässä varmistusratkaisussa kaikki tieto on koko ajan saatavilla, mikä on samaan aikaan tämän varmistusratkaisun etu sekä riski.

Paikallisesti varmistettuihin tietoihin on aina pääsy huolimatta siitä, onko internetyhteyttä käytössä vai ei. Varmistettujen tietojen palauttaminen on nopeaa. Paikallisessa varmistusratkaisussa varmistettu tieto on kuitenkin haavoittuvaisempaa kuin etävarmistusratkaisussa esimerkiksi varkauksien tai luonnonkatastrofien kuten tulipalon tai tulvan osalta. (Paul 2016.)

4.2 Etävarmistusratkaisu

Etävarmistusratkaisussa tietokone lähettää automaattisesti varmistettavat tiedot toiseen sijaintiin eli paikallisen verkon ulkopuolelle. Tiedot voidaan määritellä synkronoitumaan ajastetusti tai dynaamisesti aina, kun uusin versio tiedostosta on saatavilla. Etävarmistusratkaisun käyttöönotto vaatii minimissään asiakasohjelmiston asentamisen kaikille niille laitteille, joilta halutaan tietoja varmistettavan. Etävarmistusratkaisuissa pystytään keskitetysti määrittelemään kaikille laitteille yhteinen varmistusaikataulu sekä määritellä varmistuksen piiriin kuuluvat tiedostot ja kansiot. Asiakasohjelmisto ottaa varmistuksen automaattisesti hyödyntäen määriteltyä konfiguraatiota.

Käytettäessä etävarmistusratkaisua omien varmistuslaitteistojen hankinta ei ole pakollista, kriittisten tietojen palauttaminen onnistuu hätätilanteen sattuessa.

Etävarmistusratkaisun suurin riskitekijä on se, että varmistettavien tietojen siirtoon tarvitaan aina internetyhteys. Internetyhteys tarvitaan siis myös tiedostojen palauttamiseksi. Toinen merkittävä riskitekijä on tiedon tallentaminen kolmannen osapuolen järjestelmiin. Sopimusehdot ja lainsäädäntö palveluntarjoajan osalta on selvitettävä huolella. (Paul 2016.)

4.3 Cloud-varmistusratkaisut

Cloud-varmistusratkaisu on nopea ottaa käyttöön eikä vaadi erillisiä laitehankintoja. Cloud-varmistusratkaisu on etävarmistusratkaisu, eli varmistettavat tiedot tallennetaan toiseen sijaintiin. Cloud-varmistusratkaisussa varmistettavat tiedot tallennetaan jonkun Cloud-varmistusratkaisua tarjoavan palveluntuottajan online-tallennuspaikkaan. Varmistettuihin tietoihin päästään käsiksi tarvittaessa joko erillisen tietokoneelle asennettavan asiakasohjelmiston avulla tai autentikoimalla palveluun internetselaimen kautta. Asiakasohjelmiston avulla valitaan ne tiedostot ja kansiot, jotka halutaan varmistaa sekä määritellään varmistusaikataulu, jonka mukaan tiedostojen varmistaminen käynnistyy automaattisesti haluttuna ajankohtana. Katastrofin sattuessa varmistetut tiedostot päästään palauttamaan Cloud-varmistusratkaisupalvelua tuottavan palveluntarjoajan online-tallennuspaikkaan kirjautumalla. Cloud-varmistusratkaisun tiedostonsiirron tekevä asiakasohjelmisto siirtää tiedostot salattuna. Tiedostojen salaus puretaan, kun tiedostot on saatu siirrettyä palveluntarjoajan tallennuspaikkaan. Osa palveluntarjoajista tarjoaa mahdollisuutta käyttää omaa avainta tiedostojen salauksen hoitamiseksi. Omaa salausavainta käytettäessä varmistetaan, että tiedostot eivät ole kenenkään muun osapuolen luettavissa. Cloud-varmistusratkaisun ensimmäinen varmistuskerta saattaa kestää päiviä käytettävissä olevan yhteyden nopeuden mukaan sekä Cloud-varmistusratkaisun palvelun tarjoajan mahdollisten siirtorajoitusten mukaan.
(Paul 2016.)

5 VARMISTUSRATKAISUN VALINTA

Tehtävien varmistusratkaisujen valinta tulee tehdä kustannuksien suhteessa tietojen menettämisen riskiin.
Varmistussuunnitelmassa on määriteltävä

- mitä varmistetaan
- minne varmistetaan
- kuinka usein varmistukset ajetaan
- kenen vastuulla varmistusten ottaminen on

- ketä on vastuussa varmistusten toimivuuden valvonnasta. (Lo 2012.)

Tiedot tulee varmistaa pöytäkoneilta, kannettavilta tietokoneilta ja palvelimilta, mutta prioriteetti on asetettava bisnestoiminnan kannalta kriittiselle tiedolle. Jokaisen organisaation on määriteltävä, miten suuri riski pystytään ottamaan tietojen mahdolliseen menettämiseen liittyen ja muodostaa varmistussuunnitelma sen mukaisesti.
Kriittisen tiedon varmistamiseen on suositeltavaa muodostaa paikallisen varmistusratkaisun sekä etävarmistusratkaisun yhdistelmä. Liiketoiminnan jatkuvuuden kannalta kriittisin tieto tulee olla saatavilla, vaikka internetyhteys menetettäisiin.
(Lo 2012.)

6 TOIMEKSIANTAJAYRITYS SAINT-GOBAIN

6.1 Yrityksen esittely

Saint-Gobain on maailman laajuisesti markkinajohtaja teollisuus- ja asuinrakentamisen alalla. Saint-Gobain konserniin kuuluvat yritykset suunnittelevat, valmistavat ja toimittavat rakennusmateriaaleja sekä esittelevät innovatiivisia ratkaisuja erilaisiin haasteisiin, kuten kasvuun, energiatehokkuuteen ja ympäristönsuojeluun.
Saint-Gobainin perustivat vuonna 1665 ranskalainen ministeri Jean-Baptiste Colbert ja Ludvig XIV valmistaakseen ensimmäistä kertaa historiassa lasia teollisessa mittakaavassa. Saint-Gobainin ensimmäisiä lasitoimituksia on tehty muun muassa Versailles'n palatsin peilisaliin. Saint-Gobain työllistää maailmanlaajuisesti yli 170 000 työntekijää. Saint-Gobain on keskittynyt kolmeen toimialaan; innovatiivisiin materiaaleihin, rakennusmateriaaleihin ja rakennustuotteiden jälleenmyyntiin. (Saint-Gobain 2017.)

6.2 Saint-Gobain Technology Services Nordic & Baltic

Työn tilaaja on Saint-Gobain Technology Services Nordic & Baltic (SGTS N&B). Saint-Gobain konsernin jaetaan maantieteellisesti delegaatioihin. Nordic & Baltic delegaatio koostuu 7 eri maasta, Norjasta, Ruotsista, Tanskasta, Suomesta, Virosta, Latviasta ja Liettuasta. SGTS N&B on palveluorganisaatio, joka tuottaa ICT palveluja Nordic & Baltic alueen Saint-Gobain yrityksille. SGTS N&B hallinnoin noin 4 000 työasemaa ja sen palvelunpiiriin kuuluu 1 100 palvelinta ja 153 sijaintia.

7 KÄYTTÄJIEN TIETOJEN VARMISTAMINEN SGTS N&B DELEGAATIOSSA

7.1 Lähtötilanne

It-infrastruktuurin ja -käytäntöjen yhtenäistämiseksi on koko Saint-Gobain konsernissa tehty töitä jo useamman vuoden ajan. Tutkimuksessani tietojen varmistamiseen liittyen eteeni tuli toistuvasti käyttäjän tuottaman tiedon kriittisyys yritykselle.
Saint-Gobain konsernissa työasemavarmistuksien toteuttamiseen on standardoitu Druva inSync työasemavarmistusratkaisu. Druva inSync työasemavarmistusratkaisu oli otettu käyttöön jo osassa Saint-Gobainin Suomen ja Viron yritysten käyttäjien kannettavissa tietokoneissa.

Lähtötilanteessa käyttäjien tietoja oli tallennettu osassa yrityksistä verkkolevyille ohjaamalla käyttäjän default data profile suoraan käyttäjän omaan verkkokotihakemistoon. Osassa yrityksissä käyttäjien tietoja oli tallennettu sekä verkkokotihakemistolle että paikallisesti käyttäjän omalle tietokoneelle. Ongelmia tietojenvarmistukseen aiheuttivat erityisesti suuriksi kasvavat Outlookin arkistokansiot. Outlookin arkistokansioiden aikaleima muuttuu aina kun tiedosto avataan Outlookiin, jolloin palvelimien varmistamiseen Saint-Gobainilla käytössä ollut ohjelmisto käsittelee tiedostoa kokonaan uutena tiedostona ja lähtee siirtämään sitä ajastetun varmistuksen alkaessa. Outlookin arkistokansioiden käyttö verkkolevyltä etäyhteydellä on hidasta ja tästä syystä osa käyttäjistä oli omatoimisesti siirtänyt Outlookin arkistokansiot käytettä-

väksi omalta tietokoneelta. Edellä mainitut ongelmakohdat huomioon ottaen käyttäjien tietojen palauttaminen katastrofin sattuessa saattoi olla työlästä, eikä käyttäjien tietojen varmistusta pystytty kaikissa tilanteissa takaamaan. Lähtötilanteen toimintamalleista ei ollut mahdollista saada luotettavaa raporttia varmistuksien tilasta, jolloin varmistuksien hallinta ei ollut mahdollista.

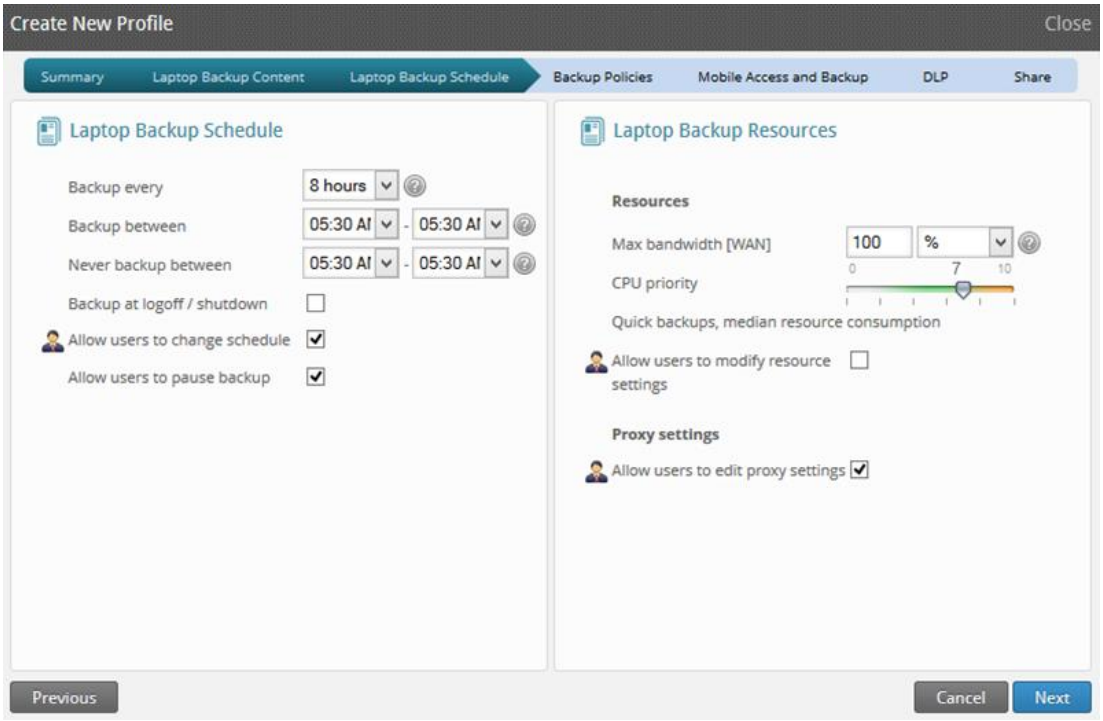
7.2 Druvasta inSync

Druva ympäristön hallintaan on tarjolla inSync's dashboard, jonka intuitiivisesta käyttöliittymästä pääsee helposti pureutumaan yksityiskohtaisempiin tietoihin pikalinkkien kautta. Yhdennetty konsoli tarjoaa kokonaisnäkymän ja kontrollin yrityksen varmistuksiin ja varmistuksien hallintaan. IT järjestelmänvalvoja voi helposti tarkastaa käyttäjien lukumäärän, data storage käyttöasteen, varmistus- sekä palautustapahtumat ja inaktiivisten tai epäonnistuneiden varmistuskertojen määrät ja virhekoodit. (Druva 2017.)

Kuva 6. inSync Dashboard (Druva 2017.)

Käyttäjän hallintaan inSync tarjoaa mahdollisuuden hallita varmistettavan tiedon sisältöä sekä tehdä määrityksiä myös käyttöjärjestelmäkohtaisesti. Varmistuksien aikatauluttaminen voidaan tehdä pakotetusti IT järjestelmänvalvoja toimesta tai jättää

käyttäjälle mahdollisuus muuttaa varmistuksien aikataulua, keskeyttää varmistuksen ottaminen ja muokata varmistukseen käytettäviä resursseja (kaista ja CPU prioriteetti) varmistuksen aikana. (Druva 2017.)



Kuva 7. inSync Backup scheduling (Druva 2017.)

IT järjestelmänvalvoja pystyy määrittelemään varmistuksien säilyttämiseen ja pääsyyn liittyvät politiikat ja sen, miten käyttäjät voivat autentikoitua järjestelmään (inSync salasana, Active Directory, SSO), estää inSync ikonia poistumasta tietokoneen ilmoitusalueelta ja kontrolloida milloin laite määrittyy inaktiiviseksi. (Druva 2017.)

7.3 Tavoite

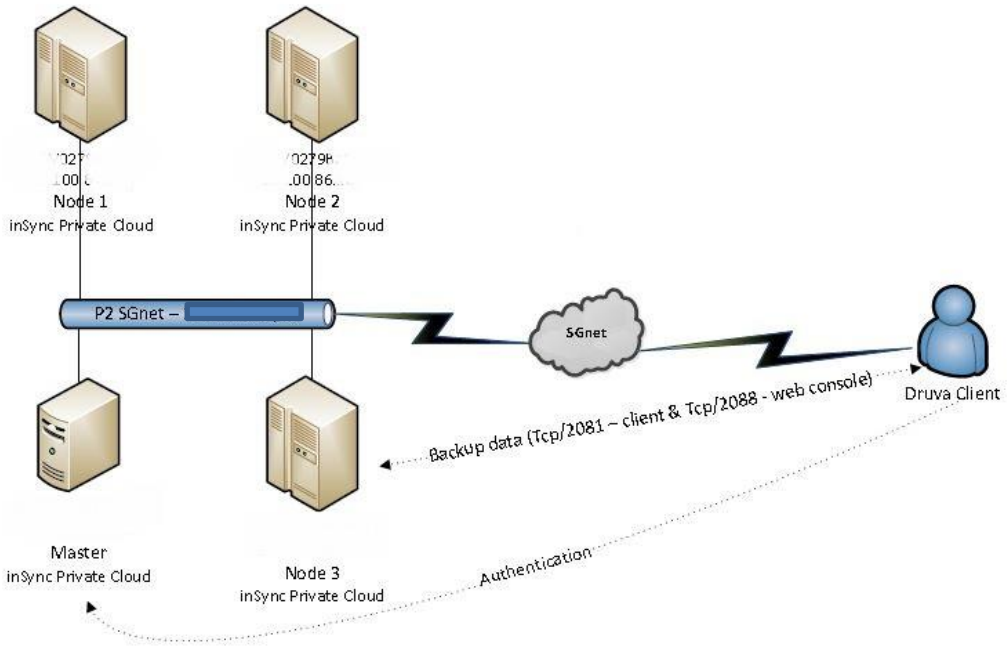
Tavoitteena toimeksiantajalla oli hallinnan automatisointi käyttäjien tietojen varmistamiseen ja palauttamiseen liittyen. Varmistusratkaisut tulisi yhtenäistää koko Nordic & Baltic -delegaation alueen yrityksissä. Työasemavarmistusratkaisun käyttöönoton myötä toimeksiantaja haluaa luopua käyttäjille tarjotuista verkkokotihakemistoista ja niiden ylläpidosta.

8 TOTEUTUS VAIHEITTAIN

Toimeksiantaja päätyi laajentamaan olemassa olevaa Druva inSync Private Cloud varmistusratkaisua. Druva inSync Private Cloud varmistusratkaisu on etävarmistusratkaisu, jossa tietokoneelle asennettava asiakasohjelmisto lähettää, joko varmistuspolitiikassa tehtyjen määritysten mukaisesti kerran päivässä tai manuaalisesti käynnistettäessä, uuden tai muuttuneen datan jollekin inSync Private Cloud palvelimista. Käyttäjän autentikointi tapahtuu Druva hallintajärjestelmään lisättyjen tunnuksien ja Active Director salasanan avulla. SGTS N&B varmistuspolitiikassa määriteltiin, että arkistoitavia varmistuskuvien eli tietyllä ajanhetkellä otetusta tietojen tilanteesta säilytetään maksimissaan 14 versiota, muodostuen seuraavan laisesti:

- 7 päivittäistä varmistuskuvaa
- 4 viikoittaista varmistuskuvaa
- 3 kuukausittaista varmistuskuvaa.

Kun varmistuskuvien maksimimäärä täyttyy, poistetaan vanhin versio automaattisesti ja se korvataan toiseksi vanhimmalla versiolla. Varmistuskuva siirretään automaattisesti varmistuspalvelimelle kerran päivässä (24h). Jos aikataulun mukainen varmistus ei ole käynnistynyt (esimerkiksi laite ollut offline), käynnistetään seuraava varmistuskerta heti kun mahdollista.



Kuva 8. SG Network overview

8.1 Kohderyhmän kartoitus

Projektin aloitusvaiheessa päädyttiin rajaamaan Druva inSync Private cloud varmistusratkaisun käyttöönotto koskemaan vain kannettavia tietokoneita. Druva inSync Private cloud varmistusratkaisun piiriin määriteltiin yhteensä 1425 asennettavaa asiakasohjelmistoa, jotka jakautuivat maakohtaiseesti seuraavan laisesti:

- Tanska 350 kannettavaa työasemaa
- Ruotsi 755 kannettavaa työasemaa
- Norja 318 kannettavaa työasemaa.

Kohderyhmän kartoituksen yhteydessä selvitettiin myös käyttäjien tietojen alkutilanteen sijainti ja dokumentoitiin prosessikuvaus default data profilen oletussijainnin palauttamiseksi, niiden käyttäjien kohdalta kenellä default data profile oli uudelleen ohjattu verkkokotihakemistoon. Kohderyhmän kartoituksessa dokumentoitiin myös prosessikuvaukset liittyen Offline folder -ominaisuuden purkuun sekä data kopiointien automatisointiin ja manuaaliseen toteutukseen.

8.2 Raportointi

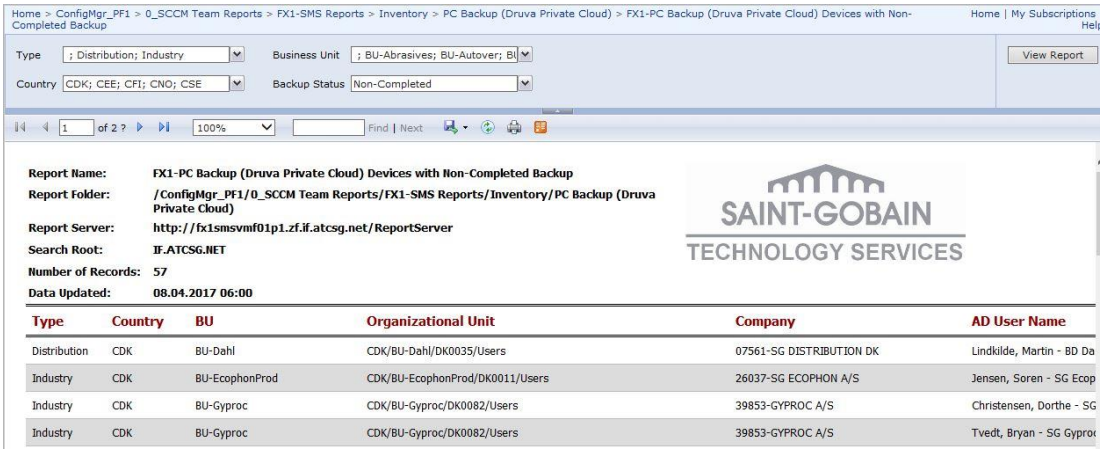
Druva inSync Private Cloud varmistusratkaisusta julkaistiin automaattisesti SGTS N&B Service Deskin työjonolle inaktiivisten laitteiden raportti käsiteltäväksi. Raporttia on tarkoitus verrata SGTS N&B:lle kuukausittain toimitettavaan päättyneiden työsuhteiden raporttiin ja tarvittaessa aloittaa toimenpiteet tarpeettomien Druva profiilin poistamiseksi.

Druva inSync Private Cloudin hallinnan avuksi aktivoitiin seuraavat raportit:

- FX1-PC Backup (Druva Private Cloud) Devices, joka sisältää kaikki SGTS N&B alueen varmistusratkaisun piiriin kuuluvien laitteiden tiedot
- FX1-PC Backup (Druva Private Cloud) Devices inactive for 45 Days or More, joka sisältää kaikki 45 tai kauemmin pois käytöstä olleet laitteet
- FX1-PC Backup (Druva Private Cloud) Devices of Orphaned Users, joka sisältää laitteet, joiden käyttäjän tietoja ei enää löydy Active Directorystä

- FX1-PC Backup (Druva Private Cloud) Devices with Non-Completed Backup, joka sisältää tiedon laitteista joiden ensimmäinen varmistus ei ole vielä valmis
- FX1-PC Backup (Druva Private Cloud) Monthly Invoicing, joka sisältää laskutukseen liittyvät tiedot
- FX1-PC Backup (Druva Private Cloud) Devices Users, joka sisältää tiedot varmistusratkaisun käyttäjistä.

Kaikkien raporttien tiedot päivittyvät päivittäin ja ne pystytän viemään esimerkiksi Exceliin edelleen käsiteltäväksi.



Kuva 9. Druva inSync Private Cloud FX1-PC Backup (Druva Private Cloud) Devices with Non-Completed Backup -report.

8.3 Asiakasohjelmiston jakelu

Asiakasohjelmiston jakelu suoritettiin keskitetysti maakohtaisesti jaksotettuna. Jakeluun käytettiin olemassa olevaa System Center Configuration Manager ratkaisua ja jo aiemmin Saint-Gobainille paketoitua ohjelmistopakettia. System Center Configuration Manager:iin oli määritelty software advertisement, mikä perustui Active Directoryn security groupiin, johon lisätään Druva inSync Private Cloud varmistusjärjestelmän käyttäjät. Jakelua seurattiin System Center Configuration Manager:iin luotujen raporttien avulla.

Druva inSync Private Cloud -asiakasohjelmiston asentumisen jälkeen ohjelma aktivoitui automaattisesti ja aloitti ensimmäisen varmistuksen.

8.4 Tiedostosiirrot

Tiedostosiirrot käyttäjien verkkohakemistoilta paikallisille levyille pyrittiin toteuttamaan ensisijaisesti ohjeistamalla käyttäjiä tekemään tiedostosiirrot itsenäisesti määräaikaan mennessä, jonka jälkeen yhteys verkkohakemistoon katkaistaan. Verkkohakemisto määrityksen poisto Active Directoryn user objectin takaa, tehtiin erillisellä Power Shell skriptillä.

Tiedostosiirtojen jälkeen, kun ensimmäinen varmistuskerta suoritettu, käynnistettiin prosessi Offline folder -toiminnon purkamiseksi. Offline folder -toiminto purettiin Group Policy objectin avulla. Offline folder -toiminnon purkamisen lisäksi luotiin toinen erillinen Group Policy object, jolla poistettiin paikalliset kopiot offline tiedostoista. Luomalla kaksi erillistä Group Policy objectia pystyttiin välttämään tiedostojen katoaminen Offline folder -toiminnon purkamisen yhteydessä. Sillä jos käyttäjällä oli tiedostoja Offline folder -toiminnon kautta vielä käytettävissä, ilmenisi tilanne pääsyn estyessä ja tiedostot pystyttäisiin edelleen palauttamaan aktivoimalla Offline folder -toiminto kyseessä olevalle tietokoneelle uudelleen ja siirtämään tiedostot tietokoneelle tallentuneesta Offline kopiosta käyttäjän profiiliin paikalliselle kiintolevylle.

8.5 Ylläpitovaihe

Druva inSync Private Cloud varmistusratkaisun käyttöönoton myötä muutettiin prosesseja koskien uuden käyttäjätunnuksen luontia ja käyttäjän tietokoneen käyttöönottoa tai vaihtoa, sellaiseksi että uusille käyttäjille ja käyttäjille tietokoneen käyttöönoton tai vaihdon yhteydessä otetaan Druva inSync Private Cloud varmistusratkaisu oletuksena käyttöön. Tietokoneen vaihdon yhteydessä, suoritetaan lisäksi seuraavat varmistusratkaisun käyttöönottoon liittyvät prosessit:

- Druva inSync Private Cloud käyttäjätunnuksen lisääminen
- ohjelmiston asennus System Center Configuration Manager ohjelmistonjakelun kautta
- tiedostosiirto

- Offline folder -toiminnon purku.

8.6 Druva inSync Private Cloud palvelukuvaus

Druva inSync Private Cloud varmistusratkaisun palvelukuvauksessa on määritelty Saint-Gobain N&B osalta käytettäväksi varmistusmenetelmäksi inceremental backup -varmistusmenetelmää, missä Full backup tehdään vain ensimmäisellä varmistuskerralla heti asiakasohjelmiston asentumisen jälkeen. Kaikki varmistuskerrat ensimmäisen Full backup varmistuskerran jälkeen ovat siis incremental backup -varmistusmenetelmällä toteutettavia. Edellä mainitun toimintamallin käyttäminen pienentää merkittävästi varmistuksen ottamiseen vaadittavaa aikaa, kun siirretään vain muuttunut ja uusi tieto varmistuspalvelimelle. Verkkoliikenteen minimoimiseksi varmistettavasta tiedosta poistetaan duplikaatit ja se pakataan automaattisesti Druva inSync Private Cloud asiakasohjelmiston toimesta ennen siirtämistä varmistuspalvelimelle. Varmistuspalvelimelle tallentunut tieto pakataan automaattisesti päivittäin ajastetulla maintenance taskilla tarvittavan tilantarpeen minimoimiseksi.

Standardi varmistusratkaisun profiili varmistaa kaikki tiedot käyttäjän oletus profiilista (%userprofile%), pois lukien audio-, video- ja jotkin erityistiedostot.

Included files/folders	Excluded files/folders
All files from %userprofile% path	~\$*.*;*.3gp;*.3gp;*.a52;*.aac;*.ac3;*.aif;*.aiff;*.ape;*.asf;*.au;*.avi;*.bak;*.bin;*.bwa;*.bwi;*.bws;*.bwt;*.cab;*.ccd;*.cda;*.cif;*.com;*.cpl;*.cso;*.daa;*.divx;*.dk;*.dll;*.dmg;*.drv;*.dts;*.dtx;*.dv;*.exe;*.fla;*.flac;*.flv;*.gho;*.gxf;*.ima;*.img;*.ipa;*.isc;*.iso;*.lcd;*.log;*.m1v;*.m2p;*.m2t;*.m2ts;*.m2v;*.m4a;*.m4b;*.m4p;*.m4v;*.mka;*.mks;*.mkv;*.mod;*.mov;*.mp1;*.mp2;*.mp3;*.mp4;*.mp4a;*.mp4v;*.mpa;*.mpc;*.mpe;*.mpeg;*.mpeg1;*.mpeg2;*.mpeg4;*.mpg;*.mpv;*.msi;*.msp;*.msu;*.mts;*.mxt;*.nds;*.nrg;*.ocx;*.oga;*.ogg;*.ogm;*.ogv;*.oma;*.ost;*.pcm;*.pqi;*.qt;*.qt3;*.qtr;*.qtx;*.ra;*.ram;*.redo_*;*.rf;*.rm;*.rmp4;*.rmvb;*.rpm;*.rv;*.spx;*.swf;*.sys;*.tmp;*.tp;*.trp;*.ts;*.uif;*.vhd;*.vhdx;*.vmdk;*.vmem;*.vmsn;*.vob;*.vsv;*.vud;*.wav;*.wim;*.wma;*.wmv;*.xn
All folders from %userprofile% path	$Extend;$RECYCLE.BIN;Cache;Cookies;I386;LocalService;MSOCache;Microsoft\InternetExplorer\Recovery;NetHood;NetworkService;PrintHood;Private;ProgramFiles(x86);ProgramFiles;ProgramData;RECYCLER;SafeBoot.rsv;Safeboot.fs;SystemVolumeInformation;Temp;TemporaryInternetFiles;Tmp;UsrClass.dat;WindowsRECYCLER;Windows;desktop.ini;hiberfil.sys;iPhotoLibrary\iPodPhotoCache;inSync4;ntuser.dat;pagefile.sys;
All PST files from all fixed drives	*.emlx;*.eml;*.msf;*.mbox;*.mbx;*.nsf;*.dbw;*.dbx;*.ost
All PST files in Outlook profile	

Kuva 10. varmistukseen piiriin standardi varmistusratkaisun profiilissa kuuluvat ja pois luetut tiedostotyypit

8.7 Palvelutasosopimus (Service level agreement SLA)

Käytetyt termit:

- Potential Restore Time (PRT) eli potentiaalinen palautusaika. Sisältää ajan WANin yli palautettaessa
- Recovery Time Objective (RTO) eli palautuksen aloittamisen kestoon sallittu aika
- Recovery Point Objective (RPO) eli viimeisimmästä varmistuskerrasta kulunut aika.

Palvelutasosopimus määrittyi seuraavasti:

- Järjestelmäkomponenttien kuukausittainen käytettävyys 95,00 %
- Käytettävyys 6 kuukauden tarkastelujaksolla 96,00 %
- Recovery Time Objective (RTO) 2 tuntia + PRT
- Recovery Point Objective (RPO) 24 tuntia.

9 LOPUKSI

Minulle on kertynyt työurani aikana omakohtaisia kokemuksia tiedostojen sekä kokonaisten järjestelmien onnistuneesta palautuksesta. Kokonaisen tietojärjestelmän palauttamista katastrofitilanteessa ei valitettavasti ehdi harjoitella, mutta palautuksien testausta tulisi tehdä säännöllisin väliajoin. Varmistukset ovat mielestäni yhtä kiitollisessa asemassa kuin koko IT-infrastruktuuria ylläpitävä henkilöstö, niiden olemassa oloa ei huomata, kun kaikki toimii eikä ongelmia ilmene.

Tärkeää varmistusratkaisua valittaessa on käytettävä aikaa ja selvitettävä tiedon omistajat, jotka voivat luokitella tiedon kriittisyyden. Ei kriittisen -tiedon varmistamiseen ei kannata käyttää monimutkaisia varmistusratkaisuja, vaan varmistaa tiedot matalamman saatavuuden tarjoamilla ratkaisuilla.

Kun liiketoimintaprosessien kriittiset tiedot on identifioitu yhteistyössä tiedon omistajien kanssa, pystytään resurssit ja valvonta keskittämään siihen osa-alueeseen tiedosta, jonka palauttaminen ja saatavuus on oltava korkeimmalla mahdollisella tasolla.

Perusasioiden hahmottaminen ja varmistussuunnitelman teettäminen yhteistyössä yrityksen liiketoiminnasta vastaavien tahojen kanssa luo turvallisen alusta toimia ja kehittää toimintaa myös ICT näkökulmasta.

En tutkimuksessani ottanut kantaa uusia haasteita tuovaan usean eri laitteen käyttöön liittyviin ongelmiin. Älypuhelimien tai tablettien varmistus rikkoutumisen, katoamisen tai varkauden varalta vaatii uudenlaista teknologiaa ja hallinta menetelmiä, joiden kehittymisen seuraamista jään innolla odottamaan.

LÄHTEET

Cougias, Dorian J., 2003. The Backup Book. Network Frontiers. Viitattu 28.2.2017. Saatavissa: https://books.google.fi/books?id=eLviiTag5A0C&printsec=frontcover&hl=fi&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=true

Druva 2017. Druva inSync Quick Tour. Viitattu 6.5.2017 Saatavissa: https://www.druva.com/products/insync/virtual-tour/

Lo, Kevin 2012. Your Organizations Backup Strategy. Viitattu 25.2.2017. Saatavissa: http://www.techsoup.org/support/articles-and-how-tos/your-organizations-backup-strategy

Martin, B.C. 2002. Disaster Recovery Plan Strategies and Processes. Viitattu 28.2.2017. Saatavissa: https://www.sans.org/reading-room/whitepapers/recovery/disaster-recovery-plan-strategies-processes-564

Paul, I. 2016. Why you need a cloud backup service, and how to use one. Viitattu 23.2.2017. Saatavissa: http://www.pcworld.com/article/3020270/security/why-you-need-a-cloud-backup-service-and-how-to-use-one.html

Rima, Chris 2013, Business Continuity and Disaster Recovery Planning for IT Professionals, Elsevier Science. Viitattu 5.4.2017. Saatavissa: http://ebookcentral.proquest.com/lib/samk/reader.action?docID=1115178

Saint-Gobain 2017. Tietoa Saint-Gobainista. Viitattu 9.4.2017. Saatavissa: http://www.saint-gobain.fi/tietoa-saint-gobainista/saint-gobain-maailmanlaajuisesti

Varghese, Mathew 2002, Disaster Recovery, Course Technology. Viitattu 5.4.2017. Saatavissa: http://ebookcentral.proquest.com/lib/samk/reader.action?docID=3135748#