Opinnäytetyö (AMK)

Tietojenkäsittely

Tietoliikenne

2010

Antero Riihimäki

PK-YRITYKSEN TIETOJEN VARMUUSKOPIOINTI

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

OPINNÄYTETYÖ (AMK) | TIIVISTELMÄ

TURUN AMMATTIKORKEAKOULU

Tietojenkäsittely | Tietoliikenne

Joulukuu 2010 | 30 sivua

Esko Vainikka

Antero Riihimäki

PK-YRITYKSEN TIETOJEN VARMUUSKOPIOINTI

Yrityksen tietojen varmuuskopiointi on erittäin tärkeää. Useissa yrityksissä sitä ei kuitenkaan hoideta kunnolla tai pahimmissa tapauksissa lainkaan.

Useimmat ihmiset eivät tiedä, että varmuuskopiointi on osa yrityksen tietoturvaa. Tietoturva voidaan yleisesti jakaa neljään eri osa-alueeseen: tiedon luottamuksellisuuteen, eheyteen, saatavuuteen ja alkuperän todennukseen. Varmuuskopiointi koskettaa näistä eritoten kahta keskimmäistä, eli eheyttä ja saatavuutta.

Varmuuskopioinnille on monta toteutustapaa, mutta ne voidaan jakaa kahteen kategoriaan, paikallinen ja etävarmuuskopiointi. Paikallisessa varmuuskopioinnissa tiedot kahdennetaan paikallisesti, joko toiselle tietokoneelle, CD/DVD-levylle tai vastaavalle muistille. Etävarmuuskopioinnissa tiedot siirretään yrityksen toimipisteen ulkopuolelle suojaan tulipalolta, vesivahingoilta sekä varkauksilta.

Varmuuskopiointitapa, josta tässä opinnäytetyössä puhumme on näiden kategorioiden yhdistelmä. Siinä tiedot varmuuskopioidaan ensin yrityksen paikalliselle palvelimelle, josta ne yö-aikaan varmuuskopioidaan yrityksen tilojen ulkopuoliselle palvelimelle, maksimaalisen tietoturvallisuuden takaamiseksi. Tiedot etävarmuuskopioidaan yö-aikaan siksi, että etävarmuuskopiointi on paljon verkkoa rasittava toimenpide eikä sen haluta häiritsevän työntekijöiden Internet-yhteyden käyttöä päiväsaikaan. Etävarmuuskopiointia suunniteltaessa on myös syytä muistaa siirrettävän tiedon suojaus esim. SSH-yhteydellä.

Paras tapa varmuuskopiointijärjestelmän luomiseen on 100-prosenttinen automaatio. Tämä poistaa inhimillisen elementin varmuuskopiointijärjestelmän toiminnasta ja näin luo lisää luotettavuutta. Koska inhimillistä tekijää ei kuitenkaan aina voi täysin eliminoida kuvioista, on hyvä asettaa järjestelmä lähettämään ylläpitäjälle seurantasähköposteja järjestelmän toimivuudesta, jolloin mahdolliset ongelmat havaitaan ennen kuin on liian myöhäistä.

ASIASANAT: yritys,varmuuskopiointi,linux,windows,mac,tietoturva,pk-yritys,tietojen,varmistus

BACHELOR´S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology | Data Communications

December 2010 | 30 pages

Esko Vainikka

Antero Riihimäki

DATA BACKUP FOR SMALL TO MEDIUM SIZED COMPANIES

Most companies do not back up their data at all, or not regularly enough. Losing data is a common issue for businesses. User Error, theft, program errors or hardware failures are unfortunately part of life but there are safeguards available with a functional backup system.

Most people do not know that backup is an essential part of a company's information security. Information security can be divided into four categories, confidentiality, availability, integrity and authenticity. By backing up your data, you can enhance the availability and integrity of your files and other data.

There are many ways in how to backup your data, but the two main categories are local and offsite backup. Local backup means copying the files to another computer, CD/DVD disc or other media, while off-site backup, or off-site file vaulting means to copy the data to another location. This means that your data will be safe in case an earth quake, fire or flood hits your office. When using off-site file vaulting, it is essential to make sure the file transfer is secured. This can be easily accomplished by using secure protocols such as SSH or VPN.

One of the most important things to consider while constructing a backup system, is to automate it 100%. By automating the process, your backups are not dependent on people remembering to do certain tasks. Of course, you should have a way to monitor the process in case something goes wrong, even though you have tested it thoroughly. For example, automatic emails to the administrator about server hard disk space, logs of all the backups and file transfers etc are quite handy.

Without these emails or other form of system monitoring, there is a good chance you'll notice there's something wrong, when the damage is already done.

KEYWORDS: backup,linux,windows,mac,security

SISÄLTÖ

KUVAT

1 Johdanto

Tässä opinnäytetyössä käsitellään pk-yrityksen varmuuskopiointia sekä toimivan varmuuskopiointijärjestelmän suunnittelua. Mitä tulee ottaa huomioon järjestelmää suunnitellessa ja mitkä ovat yleisimmät sudenkuopat. Opinnäytetyö vastaa myös kysymyksiin mitä, miten ja koska varmuuskopioida.

Pyrin myös selittämään varmuuskopioinnin tärkeyden sekä suosittelemani toimintamallit maanläheisin tavoin, esimerkiksi liikenneruuhkaa ja auto-vakuutusta esimerkkeinä käyttäen. Tarkoituksena on tuottaa dokumentti, jonka avulla ihmiset voisivat ymmärtää varmuuskopioinnin tärkeyden ennen kuin on liian myöhäistä. Tästä johtuen tulenkin vertaamaan varmuuskopiointia autovakuutukseen, sillä ne molemmat ovat täysin turhia, kunnes ne ovat välttämättömiä

Opinnäytetyössä kerron hieman myös siitä, miten Saferock IT Solutions Oy:n varmuuskopiointijärjestelmä on rakennettu sekä millaisia kehitysvaiheita ja ongelmia se on tähän mennessä nähnyt.

2 Teoriaa ja taustoja

Varmuuskopiointi on kaikessa yksinkertaisuudessaan tiedon kahdentamista. Varmuuskopioimalla yrityksen tiedot pyritään ehkäisemään tietojen häviäminen. Tietojen häviäminen on yleinen ongelma sekä yksityisille että yrityksille. Tietoa häviää usein vahingossa inhimillisen virheen sattuessa tai vahingon kuten tulipalon, vesivahingon tai ylijännitepiikin sattuessa, tai varkauden myötä.

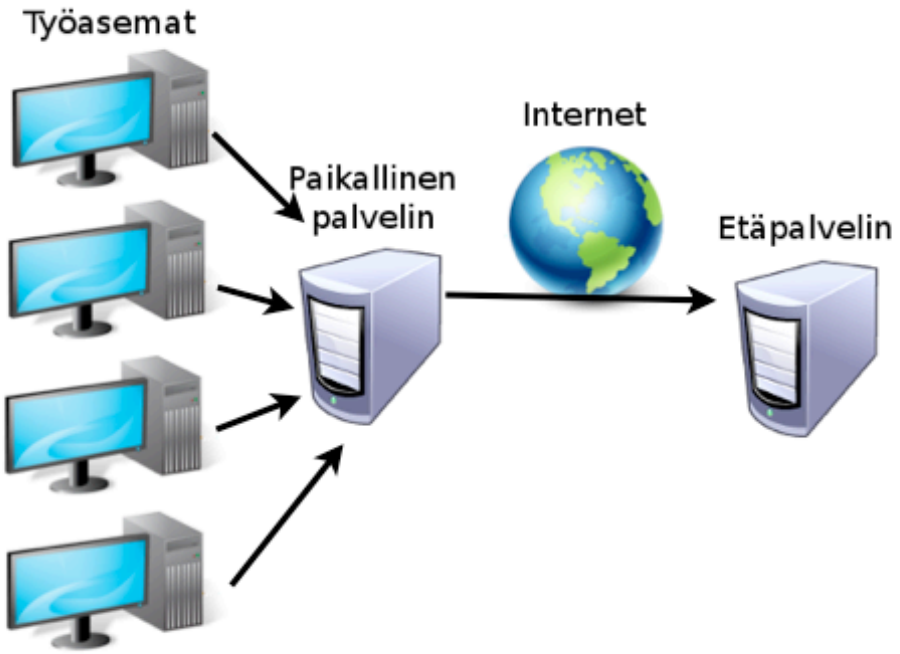
Olen itse usein verrannut tiedostojen varmuuskopiointia autovakuutukseen. Varmuuskopiointi, kuten kaikki muutkin yrityksen toiminnot, vievät resursseja, tavalla tai toisella. Jos varmuuskopiointi on ulkoistettu palvelu, se vie rahaa tietyn summan kuukaudessa, jos taas se tehdään itse, syö se yrityksen henkilöstö- sekä laiteresursseja ja rahaa. Näin ollen, kuten autovakuutus, myös varmuuskopiointi saattaa tuntua turhalta, niin kauan kuin mitään pahaa ei satu. Välillä ihmisille kuitenkin sattuu vahinkoja. Vahingon sattuessa, oli se itse aiheutettua tai jonkin ulkopuolisen ihmisen tai tapahtuman aiheuttamaa, on vakuutus hyvä olla olemassa. Samoin on varmuuskopioinnin laita. Suurena erona on se, että auton puskurilla on helposti määritettävä hinta, toisin kun yrityksen tiedostoilla.

Puskurin hinta on helposti selvitettävissä lähimmän autoliikkeen varaosalistasta, jonka jälkeen vakuutusyhtiö korvaa puskurin. Yrityksen tiedostoille taas ei löydy hinnastoa, tästä johtuen vakuutusyhtiöt eivät ole kovinkaan innoissaan korvaamassa yritykselle tietojen häviämisestä johtuneita kuluja.

Voi siis olla, että varmuuskopiointi on vain yksi rahareikä lisää, kuten autovakuutuskin. Huonossa tapauksessa, joka on oikeastaan aika positiivinen tapaus, ovat molemmat täysin tarpeettomia. Mutta aina on se pieni mahdollisuus, että ne saattavat pelastaa paljolta harmilta ja rahan menolta.

Varmuuskopiointi voidaan tehdä, paikallisena varmuuskopiointina, etävarmuuskopiointina tai näiden yhdistelmänä. Useimmiten käytetään näiden yhdistelmää maksimaalisen tiedostoturvallisuuden saavuttamiseksi. Paikallisessa varmuuskopioinnissa käyttäjän tiedot varmuuskopioidaan yrityksen fyysisessä

toimipaikassa olevalle ulkoiselle kiintolevylle, palvelimelle , muistitikulle tai muulle muistille. Etävarmuuskopiointi tarkoittaa sitä, että käyttäjän tiedot varmuuskopioidaan yrityksen varsinaisen toimipaikan ulkopuolella sijaitsevalle palvelimelle. Tämä lisää varmuuskopioiden turvallisuutta, sillä mikäli yrityksen toimipaikalla sattuu esimerkiksi tulipalo, varkaus, vesivahinko tai virtapiikki, ovat varmuuskopiot kuitenkin edelleen turvassa.



Kuva 1. Etävarmuuskopiointi.

Usein varmuuskopiointiin käytetäänkin eräänlaista sekä etä- että paikallisen varmuuskopioinnin yhteispeliä. Tällöin yrityksen työasemat varmuuskopioidaan päivisin paikalliselle, yrityksen toimitiloissa sijaitsevalle palvelimelle. Paikallisen palvelimen tiedostot puolestaan varmuuskopioidaan yön aikana etävarmuuskopiointipalvelimelle. Etävarmuuskopiointi kannattaa tehdä yön aikana, sillä päiväsaikaan se loisi ylimääräistä liikennettä yrityksen Internet-yhteyden taakaksi, joka taas näkyisi työntekijöille Internetin sekä sähköpostin hitautena. Nykyisenä Internet-aikakautena sähköpostin ja Internetin käytön tärkeyttä yritykselle on turha liikaa teroittaa, se on kaikille itsestään selvyys. Siksi var-

muuskopiointi tai muukaan tietoturva, vaikka ne tärkeitä yrityksen tulevaisuuden takaajia ovatkin, eivät saa aiheuttaa esteitä työntekijöiden päivittäisille rutiineille.

Etävarmuuskopioinnin suorittamista päivällä voisi verrata 45 ihmisen lähettämiseen, jokaisen omalla henkilöautollaan Kaarinasta vanhaa Helsingintietä Helsinkiin. Ruuhkahan siitä seuraisi, varsinkin kun otetaan huomioon ns. “normaalit” vanhan Helsingintien käyttäjät. Viimeistään Salon keskustan kohdalla olisi jonkinasteinen liikennekaaos valmis. Jos taas lähetämme samaisen 45 henkilön ryhmän linja-autolla samalle matkalle, ei vastaavaa liikennekaaosta tapahdu. Sama periaate pätee etävarmuus-kopiointiin yöllä, se on kuin tuo bussilastillinen ihmisiä, jotka eivät aiheuta ruuhkaa tai haittaa muille tienkäyttäjille.

3 Varmuuskopiointi ja tietoturva

Usein unohdetaan, että tietojen varmuuskopiointi on tärkeä osa tietoturvaa. Yleisesti ajatellaan, että tietoturva on sitä, että ei levitellä Visa-kortin tai verkkopankin tunnuslukuja ympäriinsä. Tämä on toki myös totta, mutta ei koko tarina tietoturvasta. Yleisesti tietoturva voidaan jakaa neljään eri osa-alueeseen, näitä ovat tiedon luottamuksellisuus, eheys, saatavuus sekä todennus. (Paananen 2003, 419-420.)

Varmuuskopiointi sopii edellä mainituista kategorioista kahteen, mutta kaikkia neljää kategoriaa tarvitaan, jotta toimiva varmuuskopiointijärjestelmä saadaan toteutettua.

Yrityksen tärkeät ja siksi varmuuskopiointia tarvitsevat tiedot ovat usein myös salaisia, tällaisia ovat esimerkiksi erilaiset asiakirjat kuten työ- sekä asiakkuussopimukset. On siis tärkeä rajata pääsy varmuuskopioihin yrityksen tietoverkkojen ylläpidosta vastaaviin henkilöihin.

Tietoturvan toinen kategoria eli tiedon eheys on myös otettava huomioon tietoja varmennettaessa. Tietoja siirrettäessä on mahdollista, että siirrettävä tiedosto sirpaloituu. Mikäli varmuuskopioitujen tiedostojen eheyttä ei varmisteta, saattaa

tiedoston sirpaloituminen aiheuttaa ikävän yllätyksen varmuuskopiota palautettaessa. Suurin sirpaloitumisen vaara on lisäävää (incremental) varmuuskopiointityyppiä käytettäessä.

Kolmas kategoria eli varmuuskopioiden saatavuus on toki itsestään selvää. Varmuuskopiointimedian, oli se sitten ulkoinen kiintolevy, palvelin tai muistitikun on tietenkin oltava saatavilla, jotta varmuuskopioiminen on edes mahdollista. Yhtä tärkeää on tietenkin myös varmuuskopioinnin palauttamisen mahdollisuus. Varmuuskopiointipalvelimen on oltava sellaisessa paikassa ja sellaisten yhteyksien päässä, että varmuuskopioiden palauttaminen lyhyelläkin varoitusajalla on mahdollista.

Neljäntenä asiana on tietenkin otettava huomioon se, etteivät ulkopuoliset tahot pääse käsiksi yrityksen varmuuskopioihin. Erilaiset kutsumattomat vieraat, tulivat he yrityksen palvelimelle mielenkiinnosta tai kilpailijan maksusta, saattavat tehdä paljonkin tuhoa. Tämän vuoksi etäpalvelimen verkko-osoitteista tai fyysisestä sijainnista ei saisi kertoa, kuin niille yrityksen työntekijöille, jotka tarvitsevat tietoa työtehtäviensä suorittamiseen. Näitä henkilöitä ovat yleensä vain yrityksen verkkoylläpidosta vastaavat henkilöt.

Yrityksen tietojen varmuuskopiointi voi äärimmäisessä tilanteessa pelastaa koko yritystoiminnan. Vähemmän traagisessa tilanteessa varmuuskopiointi voi pelastaa suurelta mielipahalta sekä uudelleen tehtävän työn tuomalta stressiltä.

4 Varmuuskopioinnin menetelmät

Useimmissa yrityksissä varmuuskopiointi suoritetaan silloin kun muistetaan. Manuaalisesti suoritettu varmuuskopiointi koetaan usein työläänä lisätyönä normaalin työn lisäksi. Tämän lisäksi varmuuskopiointi unohdetaan helposti.

Vastaus tähän ongelmaan on tietenkin varmuuskopioinnin automatisointi. Automaattisella varmuuskopioinnilla päästään kaikista edellä mainituista ongelmista. Kun tietokone kerran määritetään suorittamaan tietty tehtävä, tässä yhteydessä varmuuskopiointi, tietyin aikavälein, suorittaa se annetun tehtävän

kunnes toisin määrätään. Automaattisessakin varmuuskopioinnissa on kuitenkin ongelmansa. Kun kone kerran hoitaa varmuuskopioinnin yksinään, mitä jos jotakin tapahtuu, eikä varmuuskopiointi toimikkaan? Tämä voi olla todellinen ongelma, eikä vain tietotekniikkaan negatiivisesti suhtautuvan ihmisen epäilyä, siksi se on myös otettava tosissaan. Onneksi tähänkin ongelmaan on olemassa ratkaisu, nimittäin niin kutsutut log-tiedostot. Log-tiedosto tai suomeksi lokitiedosto, on nimensä mukaisesti tiedosto, johon ohjelma tai prosessi on tallentanut kaikki tapahtumat suorittamisensa ajalta. Näin ollen ylläpitäjä näkee lokitiedostosta, mikäli varmuuskopioinnin aikana on tapahtunut virheitä. Koska myös tämä varmuuskopiointijärjestelmän osa voi helposti unohtua, mikäli sitä ei automatisoida, on hyvä asettaa järjestelmä lähettämään automaattisesti lokitiedostot suoraan ylläpitäjän sähköpostiin.

Näin saadaan luotua täysin automatisoitu varmuuskopiointijärjestelmä. Loppu jää yrityksen ylläpitohenkilöiden huoleksi. He joko lukevat, tai eivät lue palvelimen lähettämiä sähköposteja. Näin saattaa helposti käydä, kun uusi hieno järjestelmä ja sen lähettämät sähköpostit menettävät uutuuden hohdettaan ja palvelimen lähettämät loki-tiedostot alkavat tuntua roskapostilta. Yrityksen ylläpitohenkilöiden on siis hyvä tiedostaa myös tämä ongelma ja toimia sen mukaisesti.

4.1 Paikallinen ja etävarmuuskopiointi

Paikallisen varmuuskopioinnin vahvuuksia ovat sen nopeus sekä varmuuskopioitaessa että palautettaessa. Paikallisen varmuuskopioinnin suurin heikkous taas on sen haavoittuvuus yrityksen toimitilaa kohtaavassa onnettomuudessa, kuten tulipalossa, vesivahingossa tai virtapiikin aikana.

Lisäturvaa paikalliselle varmuuskopioinnille saa, kun yrityksen palvelimia ei asenneta kellarikerrokseen, johon vesi ensimmäisenä virtaa, sekä huolehtii mahdollisesti varmistusnauhojen asianmukaisesta säilytyksestä paloturvallisessa kassakaapissa. Halvimmat paloturvalliset sekä normaalit kassakaapit eivät riitä, sillä niiden sisällä lämpötila nousee tulipalon syttyessä liian suureksi ja tuhoaa varmistusnauhat käyttökelvottomiksi. Virtapiikeiltä puolestaan pystyy suo-

jautumaan niin kutsutuilla UPS-laitteilla, jotka toimivat verkkovirran ja suojattavan palvelimen välissä poistaen virtapiikit palvelimelle johdettavasta sähkövirrasta.

Etävarmuuskopiointi eli niin sanottu “off-site filevaulting” on vastaus kahteen ensimmäiseen ongelmaan. Tämä tarkoitta siis sitä, että tiedostot varmuuskopioidaan yrityksen ulkopuolelle, ns. holviin (engl. vault). On erittäin epätodennäköistä, että kaksi rakennusta joutuu samanaikaisesti esimerkiksi tulipalon tai vesivahingon kohteeksi. Vainoharhaisimmat yritykset etävarmuuskopioivat myös etävarmuuskopionsa. (Little 2007, 7-11.)

Oikein toteutettuna etävarmuuskopiointi siis tuo lisävarmuutta yrityksen varmuuskopioille. Koska etävarmuuskopiointipalvelinta ei kannata sijoittaa sekä käytännön että tietoturvan takia työntekijöiden tai yrittäjän asuntoon, kannattaa yrityksen miettiä haluavatko he itse vuokrata palvelinhotellista laitetilaa vai ulkoistaa etävarmuuskopioinnista huolehtimisen.

Yksityishenkilön asunnossa ei palvelinta kannata pitää, sillä palvelimen vaatimukset Internet-yhteyden kaistanleveydelle ovat suuret. Normaalit yhden tai kahden megabitin ADSL-yhteydet hitaine yhteyksineen ulkomaailman suuntaan eivät riitä. Harvan yksityishenkilön asunnossa on tarpeeksi nopean ja kahdennetun Internet-yhteyden lisäksi kunnollista palvelinhuonetta, jossa on asianmukaiset kulunhallinta- sekä sammutusjärjestelmät.

Suurin syy etäpalvelimen sijoittamiselle täysin ulkopuolisen tahon tiloihin on, että silloin sen sijainti ei ole helposti arvattavissa. Tämä tietenkin lisää etäpalvelimen tietoturvaa.

Etäpalvelinta käytettäessä on tärkeä muistaa käyttää aina tiedostoja siirrettäessä salattua yhteyttä. Hyviä ja yleisimpiä tiedostojen siirron salausmenetelmiä ovat VPN:t sekä SSH. (Samuelle 2008. 188-190.)

4.2 Varmuuskopiointityypit

Varmuuskopiointityypit jaetaan kolmeen kategoriaan: täysi varmuuskopiointi (Full backup), differentiaalinen (Differential) sekä lisäävä (Incremental). Jokaisella varmuuskopiointityypillä on hyvät ja huonot puolensa. Kun varmuuskopiointi aloitetaan ensimmäisen kerran, tehdään tietenkin täysi varmuuskopiointi. Täysi varmuuskopiointi pitäisi tehdä uudelleen tietyin, ennalta sovituin väliajoin, sillä tiedostonsiirrossa tapahtuneen virheen vuoksi jokin täyden varmuuskopioinnin jälkeisistä lisäyksistä on saattanut tuhota tiedostot lukukelvottomaksi. Ilman testausta tämä ongelma havaitaan vasta siinä vaiheessa, kun hajonnutta tiedostoa yritetään palauttaa hajonneesta varmuskopiosta. (Habraken, J. 2003. 379-380.)

Ottamalla täysi varmuuskopio säännöllisin väliajoin, esimerkiksi kerran kuussa, ehkäistään tällaisen skenaarion mahdollisuutta huomattavasti. Uutta, täyttä varmuuskopiota otettaessa ei kuitenkaan kannata poistaa vanhoja varmuuskopioita, vaan ne tulee arkistoida. Vasta noin viisi tai kuusi kuukautta vanhat arkistoidut varmuuskopiot kannattaa poistaa. Tällä ehkäistään vahingossa poistettujen, mutta harvoin tarvittavien dokumenttien häviäminen.

Arkistointi on prosessi, jossa tieto, joko fyysinen (esim. edellisvuoden kirjanpitomappi) tai digitaalinen, esimerkiksi edellisvuoden toimintasuunnitelma Word dokumenttina, tallennetaan turvalliseen paikkaan sen varsinaisen käyttöiän jälkeen. Arkistointi tehdään, jotta informaatio olisi käytettävissä mahdollista tulevaisuuden tarvetta varten. (Olson, J. 2009. 3.)

Arkistoidut vanhat varmuuskopiot vievät toki jonkin verran tilaa palvelimelta tai muulta varmuuskopiointiin käytetyltä medialta, mutta kun se paha päivä sattuu kohdalle, ne nousevat arvoon arvaamattomaan. Jotta arkistot veisivät mahdollisimman vähän tilaa, kannattaa ne pakata jollakin tiedostonpakkaus-ohjelmalla. Mikäli haluaa lisäturvaa arkistolleen, on nämä pakatut tiedostot hyvä suojata salasanalla.

Jotkin varmuuskopiointiohjelmat tekevät varmuuskopiosta yhden tiedoston palvelimelle, jolloin puhutaan niin kutsutuista varmuuskopioseteistä (backup

set). Nämä setit on helppo arkistoida, mutta ne ovat etävarmuuskopioinnin kannalta hankalia suuren kokonsa tähden.

Toiset varmuuskopiointiohjelmat taas kopioivat tiedostot yksitellen varmuuskopiointimedialle. Tämä helpottaa yksittäisten tiedostojen palauttamista sekä etävarmuuskopiointia, mutta hankaloittaa varmuuskopioiden arkistoimista.

4.2.1 Täysi varmuuskopio

Täydessä varmuuskopiossa siirretään kaikki valitut tiedostot, uudet ja vanhat, varmuuskopiointimedialle. Täysi varmuuskopio vie eniten tilaa palvelimelta. Koska siirrettävä tiedostomäärä on suurempi kuin muissa varmuuskopiointityypeissä, vie täysi varmuuskopiointi myös eniten aikaa. Varsinkin etävarmuuskopiointina tehtäessä täysi varmuuskopio kannattaa sijoittaa viikonlopulle, jolloin yrityksen toimistolla on pidemmän aikaa hiljaista, eikä varmuuskopioinnin viemä kaistanleveys häiritse työntekijöitä.

Täyden varmuuskopion hyvät puolet:

- Se on nopein palauttaa.
- Kaikki varmuuskopioitavaksi valitut tiedostot ovat yhdessä varmuuskopiointi setissä.

Täyden varmuuskopion huonot puolet:

- Se on hitain toteuttaa.
- Se vie paljon tilaa varmuuskopiointimedialta.

4.2.2 Differentiaalinen varmuuskopiointi

Differentiaalisessa varmuuskopioinnissa siirretään varmuuskopiointimedialle kaikki ne tiedostot, jotka ovat muuttuneet viimeisen täyden varmuuskopion jälkeen. Vaikka kyseistä tiedosta ei olisi viime varmuuskopiointikerran jälkeen muokattukaan, mutta sitä on kuitenkin muokattu viimeisen täyden varmuuskopioinnin jälkeen, kopioidaan tiedosto varmuuskopiointimedialle.

Tämä lisää varmuuskopiointiprosessin kestoa sekä verkon ylitse suoritettaessa se myös vie enemmän kaistaa kuin lisäävä varmuuskopiointi. Lisäksi sama tiedosto saatetaan siirtää montakin kertaa ns. turhaan. Mikäli tiedoston siirrossa tapahtuu virhe, saattaa varmuuskopioitava tiedosto tuhoutua lukukelvottomaksi. Tiedoston tuhoutumisen riskin nousu on suoraan verrannollinen tehtävien tiedostokopioiden määrään.

Differentiaalisen varmuuskopion hyvät puolet:

- Se on nopeampi palauttaa kuin lisäävä (incremental)
- Se on nopeampi toteuttaa kuin täysi varmuuskopio
- Se vie vähemmän tilaa kuin täysi varmuuskopio

Differentiaalisen varmuuskopion huonot puolet:

- Palauttaminen varmuuskopiointisetistä on hidasta sillä uusimman differentiaalisen varmuuskopion lisäksi on palautettava myös täysi varmuuskopio.
- Yksittäisen tiedoston palauttaminen varmuuskopiosetistä hankalaa.

4.2.3 Lisäävä varmuuskopiointi

Lisäävässä varmuuskopioinnissa siirretään vain ne tiedostot, jotka ovat muuttuneet viimeisen varmuuskopiointi kerran jälkeen. Lisäävä varmuuskopiointityyppi on suosituin tapa suorittaa päivittäiset tiedostojen varmuuskopiot.

Lisäävässä varmuuskopioinnissa siirrettävien tiedostojen määrä on vähäisin, mikä laskee varmuuskopiointiin tarvittavaa aikaa. Koska lisäävässä varmuuskopioinnissa ei myöskään siirretä tiedostoja “turhaan”, kuten differentiaalisessa varmuuskopioinnissa, on tietojen pirstaloitumisen mahdollisuus pienempi.

Lisäävän varmuuskopion hyvät puolet:

- Nopein toteuttaa
- Vie vähiten tilaa

Lisäävän varmuuskopion huonot puolet:

- Jotta tiedostot voidaan palauttaa varmuuskopiointisetistä, on kaikkien lisäävien varmuuskopioiden oltava saatavilla.
- Tietyn tiedoston palauttaminen varmuuskopiointisetistä on hitaampaa, sillä se pitää etsiä uusimmasta lisäävästä varmuuskopioversiosta.

Varmuuskopiotyyppejä vertaillessa on kuitenkin hyvä muistaa, että niiden muokkailtavuus sekä toimintavarmuus ovat viime kädessä riippuvaisia käytettävästä varmuuskopiointiohjelmasta tai skriptistä.

Paras toimintavarmuus sekä tiedostojen säilyvyys saavutetaan, kun täyden varmuuskopion lisäksi käytetään joko differentiaalista tai lisäävää varmuuskopiointityyppiä. Valittava varmuuskopiointityyppi sekä se kopioidaanko tiedostot varmuuskopiointiseteissä vai yksittäin riippuu hyvin suuresti yrityksen tarpeista, sekä siitä käytetäänkö paikallisen palvelimen etävarmuuskopiointia. (Microsoft Oy 2006.)

4.3 Varmuuskopioitavat dokumentit

Se, mitä halutaan varmuuskopioida on erittäin tapauskohtaista. Nyrkkisääntönä voidaan kuitenkin sanoa, että varmuuskopioida kannattaa kaikki työtiedostot, sähköpostit, yhteystiedot, valokuvat sekä selaimen kirjanmerkit ja asetukset, sekä verkkolaitteiden, kuten kytkinten, modeemien tukiasemien sekä tulostinten asetukset.

Suurimmasta osasta verkkolaitteita saa asetukset helposti ulos joko tekstitiedostoksi, tai laitekohtaiseksi asetustiedostoksi. Tekstitiedostot voi myöhemmin palauttaa esimerkiksi kytkimen asetuksiksi helposti etäyhteyden, useimmiten Telnet, avulla. Asetustiedostot taas ladataan yleensä laitteen selainpohjaisen ohjausjärjestelmän kautta.

Tämän lisäksi työntekijöillä saattaa olla joitakin erityisiä ohjelmia ja tiedostoja, jotka tarvitsevat varmuuskopiointia. Tällaisia ovat esimerkiksi kirjanpito sekä pankkiohjelmat. Nämä tarpeet toki vaihtelevat yrityksen verkkomallin mukaan,

riippuen siitä, onko esimerkiksi kirjanpito-ohjelma asennettuna paikallisesti kirjanpitäjän työasemalle, vai käytetäänkö sitä verkkoyhteyden avulla palvelimelta.

Mediatiedostoja, kuten musiikkia, harvemmin kannattaa varmuuskopioida, sillä ne vievät suhteessa paljon tilaa varmuuskopiointi medialta ja ovat usein helposti uudelleen ladattavissa musiikkikaupasta tai CD:ltä.

Selaimen kirjanmerkkien sekä salasanojen varmuuskopiointi taas helpottaa esimerkiksi uuden työaseman käyttöönottoa. Nykyään ihmisillä on monia salasanoja, sekä työ- että yksityiselämässä ja usein selain muistaa ne heidän puolestaan. Vanhojen salasanojen palautteluun menee helposti paljon aikaa, varsinkin kun ihmisellä ei välttämättä ole enää edes käytössään sitä sähköpostiosoitetta, jolla hän kirjautui esimerkiksi tavarantoimittajan sivuille kymmenen vuotta sitten.

Sähköpostit, kalenterimerkinnät sekä yhteystiedot ovat puolestaan itsestäänselvyys työtiedostojen sekä valokuvien ohella. Useissa yrityksissä on käytössä Microsoft Office -paketin mukana tuleva Outlook -ohjelmisto, joka sisältää sekä sähköpostin, kalenterin että yhteystiedot. Outlookia varmuuskopioitaessa pitää ottaa huomioon, että käynnissä ollessaan Outlook lukitsee kaikki tiedostonsa, eikä niitä näin ollen voida varmuuskopioida Outlookin ollessa käytössä. (Mann 2003, 402.)

Varmuuskopiointijärjestelmän on siis syytä osata kertoa käyttäjälle Outlookin sammuttamisesta ennen kuin varmuuskopiointi voi alkaa. Outlookin huonoja puolia varmuuskopioinnin kannalta on myös sen tapa varastoida kaikki käyttäjän sähköpostit kiintolevylle yhteen tiedostoon. Nykyajan sähköisessä kaupankäynnissä, jossa sähköposti toimii myös arkistona sekä ristiriita-tilanteissa todistusaineistona, eivät työntekijät juuri poistele sähköpostejaan. Käytännössä se tarkoittaa sitä, että käyttäjän sähköpostit saattavat olla yhdessä yli 4 gigatavua kiintolevyltä vievässä tiedostossa. Aina, kun käyttäjä saa uuden sähköpostin, muuttuu tiedosto, joka varmuuskopiointityypistä huolimatta tarkoittaa sitä, että parhaimmillaan muutamia kilotavua kooltaan oleva sähköposti tarkoittaa monen gigatavun siirtomäärää tiedostoja varmuuskopioitaessa.

Tästä hyvänä vastakohtana mainittakoon Applen Mail.app, joka varastoi jokaisen sähköpostin uniikkina tiedostona palvelimelle. Näin ollen mikäli käyttäjä on saanut ja lähettänyt 50 kilotavun edestä uusia sähköposteja viime varmuuskopioinnin jälkeen, ei varmuuskopiointijärjestelmä siirrä kaikkea 4 gigatavua, vaan vain uudet saapuneet ja lähetetyt eli 50 kilotavua.

5 Varmuuskopiointijärjestelmän kehitys

Ensimmäisen Saferock IT Solutions Oy varmuuskopiointijärjestelmän kehitys aloitettiin jo vuonna 2007. Järjestelmän kehitystyö kesti noin puolivuotta, jonka aikana hioimme järjestelmää valmiiksi tuotteeksi, sekä eliminoimme järjestelmässä havaittuja lastentauteja. Kun ensimmäinen varmuuskopiointijärjestelmä oli ollut käytössä noin vuoden, aloimme markkinoida varmuuskopiointijärjestelmiä myös muille yrityksille sekä yhteisöille.

5.1 Etävarmistus Rsyncillä

Alusta asti käytimme Rsync -nimistä varmuuskopiointiohjelmistoa tiedostojen etävarmistukseen paikalliselta palvelimelta etäpalvelimelle. Rsync on avoimen lähdekoodin ilmainen ohjelmisto Linux alustalle (Davison 2010). Rsyncistä on nykyään saatavissa myös Windows versio, CwRsync, joka on eräänlainen Cygwinin ja Rsyncin yhteispaketti. Cygwin on ohjelma, jonka avulla on mahdollista ajaa Windows koneessa Linux ohjelmistoja. (ITeF!x Consulting 2010.)

Rsyncin ehdottomia vahvuuksia on myös SSH-tuki, joka mahdollistaa tiedostojen siirron etäpalvelimelle salattua SSH-yhteyttä käyttäen.

5.2 Varmuuskopioinnin ajoittaminen

Aluksi varmuuskopiointi ajoitettiin Windowsin alas ajon yhteyteen ns. logout skriptinä. Tässä törmäsimme kuitenkin heti testiympäristössämme olleiden Windows XP koneiden kanssa suureen ongelmaan. Windows sulkee alas ajettaessaan verkkoyhteydet, ennen kuin se ajaa logout skriptit. Toisin sanoen varmuuskopiointia ei pystynyt ajoittamaan koneen sammuttamisen yhteyteen.

Koneen käynnistämisen yhteyteen ajoitettuna varmuuskopiointi taas olisi lisännyt koneen käynnistysaikaa, ja näin ollen ollut erittäin epämukava yrityksen työntekijöille.

5.3 Varmuuskopiointiohjelmat

Järjestelmää kehittäessämme testasimme muutamia erilaisia vaihtoehtoja työasemien varmuuskopiointiin paikalliselle palvelimelle. Tämä osoittautui koko järjestelmän laatimisen vaikeimmaksi osa-alueeksi. Tuntui, ettei juuri meidän tarkoitukseemme sopivaa, luotettavaa ja ennen kaikkea ilmaista ohjelmistoa löydy mistään.

5.4 Microsoft backup

Järjestelmän ensimmäinen versio varmuuskopioi Windows työasemat Microsoftin omalla varmuuskopiointityökalulla, joka löytyy Windows XP:n asennusmedialta. Tämän työkalun käytöstä luovuttiin muutama viikko etävarmuuskopioinnin aloittamisen jälkeen, koska ohjelma toimi varmuuskopiointisettien avulla. Ohjelman luoman tiedoston sisälle ei Rsync tietenkään pääse, ja siitä syystä se lähetti koko varmuuskopiointitiedoston aina etäpalvelimelle, eikä vain muuttuneita ja uusia tiedostoja. Tämä puolestaan kuormittaa verkkoa huomattavasti. Pahimmillaan ylimääräistä dataa siirtyi tästä syystä reilun 10 Gigatavun verran.

Esimerkiksi erään testikäyttäjän varmuuskopioitavat tiedostot veivät työasemassa noin 770 Mt tilaa kiintolevyltä, mutta samaisen käyttäjän varmuuskopio palvelimella oli lähes 8 Gt suuruinen. Tämä johtuu siitä, että Windowsin backup ilmeisesti teki muutakin kuin vain lisäsi uudet ja ylikirjoitti muuttuneet tiedostot, mitä sen ei olisi pitänyt asetusten mukaan tehdä.

5.5 Xcopy sekä Robocopy

Tämän jälkeen varmuuskopiointia ryhdyttiin suorittamaan bat-skriptin avulla. Skriptin kehitysvaiheessa käytettiin aluksi xcopyä. Windows ohjelma ei kuitenkaan ymmärtänyt Linuxin tiedostojärjestelmien tapaa hallita tiedostojen muokkausaikoja (timestamp). Näin siirryimme eteenpäin ja Microsoft 2003

Server Resource-kitin mukana tulevan Robocopyn käyttöön. Robocopy on eräänlainen xcopyn paranneltu versio ja sen piti olla paremmin yhteensopiva Linuxin kanssa. Mutta sekään ei kyennyt lukemaan palvelimella jo olleiden tiedostojen tallennusaikaa oikein, ja siirsi kaikki tiedostot aina palvelimelle. (Mueller 2007, 45-53.)

Windows backup siis kuormitti etävarmistusta ja Robocopy lähiverkkoa. Robocopyn ongelma onnistuttiin kiertämään lisäämällä skriptiin osio, joka kirjoittaa palvelimella olevaan tekstitiedostoon päiväyksen aina varmuuskopioinnin päätteeksi ja tietenkin lukee päiväyksen aina samaisesta tiedostosta varmuuskopioinnin aluksi. Ongelma johtui NTFS- sekä EXT2 & 3 -tiedostojärjestelmien erosta käsitellä tiedostojen tallennusaikoja, joten päädyimme luomaan skriptiin edellä mainitun ohituskikan.

Ongelman olisi voinut myös ohittaa lisäämällä Robocopy-skriptin loppuun attribuutin /FFT. Tämä asettaa Robocopyn käyttämään FAT-tiedostojärjestelmän tapaa käsitellä tiedostojen tallennusaikoja, joka on lähempänä EXT-tiedostojärjestelmien tapaa kuin NTFS:n tapa. (Hanscom 2008.)

Robocopyä testatessamme huomasimme, että vaikka Robocopy tukee tiedostonimen sekä hakemiston pituutta yhteensä 256 merkkiin asti, joissakin tapauksissa pitkän tiedostonimen omaavat tiedostot jäivät varmuuskopioimatta. Tämä johtui pitkän hakemistopuun sekä pitkän tiedostonimen aiheuttamasta tiedostopolun pituudesta, eikä suinkaan ainoastaan tiedostonimen pituudesta.

5.6 Cobian Backup 9

Seuraavaksi kokeilimme Cobian Backup 9 -nimistä ohjelmistoa. Cobian oli ilmaiseksi ohjelmaksi erittäin pystyväinen ja omasi hyvät toiminnot, kuten esimerkiksi automaattisen sähköpostin lähetyksen varmuuskopioinnin onnistumisesta. Käytännössä kuitenkaan yksikään sähköposti ei testipostin jälkeen ilmestynyt sähköpostilaatikkooni. Myöskään varmuuskopioinnin ajastus ei Cobianin avulla onnistunut ongelmitta. (Cobian 2010.)

5.7 CwRsync

Koska aikaisemmat järjestelmämme olivat olleet epävarmoja, päätimme yrittää CwRsyncillä työasemien varmuuskopiointia. CwRsync osoittautui testaamistamme ohjelmistoista kaikkein varmatoimisimmaksi, joten päätimme käyttää sitä siirtäessämme tiedostoja Windows koneelta Linux-koneelle. Windows - Windows siirroissa käytämme kuitenkin edelleen Robocopy:ä. (ITeF!x Consulting 2010.)

6 Varmuuskopiointijärjestelmä pähkinänkuoressa

6.1 Työnkulku

Kaikessa yksinkertaisuudessaan järjestelmä toimii seuraavasti. Käyttäjän työasemaan on räätälöity varmuuskopiointiskripti, joka varmuuskopioi käyttäjän tärkeät tiedostot. Skriptin ajaminen on ajoitettu tiettyihin kellonaikoihin tiettyinä päivinä. Ensisijaisesti skriptien ajoittaminen yritetään sovittaa yksiin esimerkiksi yrityksen erilaisten viikkopalaverien kanssa, jolloin varmuuskopiointi ei häiritse käyttäjän työskentelyä lainkaan.

Mikäli käyttäjällä on käytössään Microsoft Outlook -sähköpostiohjelma, tarkastaa skripti ensitöikseen onko Outlook käynnissä. Tämä johtuu siitä, että Outlook lukitsee käyttämänsä tiedostot muilta ohjelmilta ollessaan käynnissä, eikä sähköposteja siitä johtuen voi varmuuskopioida Outlookin ollessa päällä .(Mann 2003, 402). Skriptin Linux/Mac-variantti ei tätä tietenkään kysy, sillä Outlookista ei ole Linux/Mac versiota.

Seuraavaksi skripti kopioi käyttäjänkoneelta kaikki viime varmuuskopiointikerran jälkeen muuttuneet tiedot lähiverkon palvelimelle ja lopuksi kirjoittaa palvelimen tietokantaan tiedon onnistuneesta varmuuskopioinnista. Tällä seurataan varmuuskopiointien onnistumista sekä toteutumista. Mikäli käyttäjän tietokone ei ole onnistunut varmuuskopioimaan tietojaan 5 vrk sisällä kertaakaan, lähettää järjestelmämme käyttäjälle sähköpostitse automaattisen kehotuksen var-

muuskopioinnin suorittamisesta manuaalisesti. Manuaalinen varmuuskopioinnin suorittaminen onnistuu helposti käyttäjän työpöydälle lisätyn pikakuvakkeen avulla.

Yleisesti ottaen varmuuskopioinnin suorittamatta jääminen on erittäin harvinaista. Yleisin syy tähän on työntekijän poissaolo sairauden tai loman takia. Liikkuvammille yrityksen työntekijöille ja heidän kannettavilleen asetetaan joko etäyhteys palvelimelle tai skriptin ajaminen ohjelmoidaan toimimaan vain käyttäjän ollessa toimistolla. Tämä onnistuu helposti tarkistamalla esimerkiksi mihin WLAN-verkkoon käyttäjän kone on kirjautuneena.

Seuraavana yönä tiedostot siirretään paikalliselta palvelimelta etäpalvelimelle suojattua etäyhteyttä käyttäen. Loki-tiedosto tiedostojen siirrosta lähetetään automaattisesti ylläpitäjän sähköpostiin, josta hän voi tarkistaa esimerkiksi varmuuskopioinnin onnistumisen, sekä siirrettyjen tiedostojen ja datan määrän.

6.2 Palvelin

Varmuuskopiointijärjestelmän toimivuus perustuu pitkälti automaatioon sekä automaattisesti tapahtuvan työnkulun seurantaan sähköpostilla. Suurin syy siihen, miksi suosimme Linux-palvelimia, on niiden monikäyttöisyys sekä asetusten muokkauksen helppous. Linux-palvelin taipuu helpommin ja huokeammalla useampaan käyttötarkoitukseen.

Esimerkiksi automatisoitujen pienten ohjelmien, eli skriptien luominen, ajoittamien sekä palvelimen etähallinta ovat huomattavasti helpompia Linux-palvelinta käytettäessä (Koski & Kajala 2005, 90). Toki Windows-palvelimiakin voi automatisoida skriptein sekä etähallita, mutta niiden etähallinta on kankeaa ja vaatii usein etätyöpöytäyhteyden. Linux-palvelimia taas hallitaan käyttäen suojattua SSH-komentokehoteyhteyttä. SSH-palvelun saa nykyään asennettua myös Windows-koneisiin, mutta koska se ei ole integroitu järjestelmään kuten Linuxissa, ei SSH ole Windows-maailmassa läheskään yhtä tehokas työkalu. Tämä selittyy osaksi myös sillä, että Windows-koneita hallitaan ensiarvoisesti graafisen käyttöliittymän, eli GUI:n avulla, kun taas Linuxia hallitaan oletuksena

komentoriviltä. Linux-käyttöjärjestelmissä GUI on lähinnä pieni, käyttöä helpottava palikka varsinaisen järjestelmän päällä. (Rantala 2003, 17.)

6.3 Sähköpostinlähetys

Linux-palvelimille on olemassa monta erilaista sähköpostipalvelin-ohjelmaa. Itse käytämme Postfix -nimistä palvelinohjelmistoa (Wietse Venema 2010). Postifixiä käytämme helpon asennuksen sekä käyttäjäystävällisyyden vuoksi. Palvelimemme eivät itse varsinaisesti lähetä sähköpostia, vaan välittävät sen palveluntarjoajan (esim. Sonera tai DNA) sähköpostipalvelimelle, joka lähettää viestin käyttäjälle. Tätä kutsutaan relay-palvelinjärjestelmäksi.

Jotta järjestelmä toimisi halutulla tavalla, pitää jokaisen asiakkaan kohdalla tietää, minkä palveluntarjoajan Internet-yhteys heillä on, sillä esimerkiksi Soneran Internet-yhteydellä ei pysty lähettämään sähköpostia DNA:n palvelimen kautta. Palveluntarjoajat rajaavat näin sähköpostipalvelimen käytön vain omille asiakkailleen, estäen samalla niiden käytön sähköpostin spämmäämiseen sekä muihin väärinkäytöksiin.

6.4 Etäpalvelin

Etäpalvelimella tiedostot ovat suojattu RAID-levyjärjestelmällä. Näin ollen kiintolevyn hajotessa emme menetä tietoja. (Flyktman 2002, 741.)

RAID-järjestelmää valvotaan automatisoidun skriptin avulla, joka ilmoittaa ylläpitäjälle sähköpostitse, mikäli järjestelmässä havaitaan häiriöitä tai palvelimen kiintolevytilasta on käytetty yli 80%. Tämän lisäksi palvelin tarkistaa sille tallennetut tiedostot virusten varalta päivittäin. Myös virustutkan tietokannan päivitys on automatisoitu päivittäiseksi työksi. Ylläpitäjä saa tiedot kaikista palvelimelle tapahtuvista skriptien ajoista sähköpostiinsa.

Tämän lisäksi palvelimen etäyhteyden portti on muutettu oletusarvosta generoimalla porttinumero tietokoneen avulla. Tämä tehtiin, koska sen on huomattu vähentävän niin sanotut hammerointi-hyökkäykset palvelinta kohtaan käytännössä katsoen täysin nollaan. Hammerointi tarkoittaa yritystä murtautua

palvelimelle käyttäen käyttäjänimi- sekä salasanalistaa. Tältä listalta hyökkääjän hyökkäysohjelma valitsee yksitellen käyttäjänimen ja vastaavan salasanan sekä yrittää päästä niiden avulla kirjautumaan hyökkäyksen kohteena olevaan järjestelmään.

Koska etäpalvelin ei vastaa etäyhteyden oletusportissa minkäänlaisiin paketteihin, ei hyökkäysohjelma edes aloita hammerointi-yritystään palvelinta kohtaan.

Edellä mainitut skriptit saattavat vaikuttaa monimutkaisilta, mutta ovat itseasiassa erittäin yksinkertaisia. Palvelimen ylläpidosta vastaavat skriptit ovat erittäin lyhyitä eikä niiden automatisoimiseen tarvita erillisiä työkaluja, sillä Linux-järjestelmissä kaiken tehtävien ajoittamisen hoitaa cron -niminen ohjelma.

Jokaisella järjestelmän käyttäjällä on oma ns. crontab, johon käyttäjä voi halutessaan lisätä ajoitettuja toimintoja aina yhdestä komennosta monimutkaisiin skripteihin asti. Palvelimen crontab voi näyttää esimerkiksi seuraavanlaiselta:

20 10 * * * /home/scriptit/komento.sh

Ylläoleva crontab -rivi tarkoittaa, että joka päivä klo 10:20 ajetaan komento.sh -niminen tiedosto, joka löytyy /home/scriptit/ -kansiosta. Rivillä on siis viisi aikamääremuuttujaa, sekä ajettava komento tai skripti. Kuten esimerkistä on helppo huomata, aikamääremuuttujina voi käyttää myös tähtiä niin kutsuttuina villeinä kortteina (engl. wild card). Tämä tarkoittaa sitä, että tähti tarkoittaa mitä tahansa mahdollista arvoa. Kuten esimerkissämme on helppo havaita, ilman villejä kortteja pitäisi joka päivä ajettava skripti laittaa crontabiin 365 kertaa, mikäli villit kortit eivät olisi käytössä.

Crontab rivin aikamääremuuttujat ovat seuraavanlaisessa järjestyksessä: Minuutti, Tunti Kuukauden päivä, Kuukausi ja Viikonpäivä. Crontab antaa siis erittäin laajat sekä moninaiset mahdollisuudet skriptin ajoittamiselle. (Blum 2008, 353.)

Kun skriptit ajavan käyttäjän kotikansiossa olevaan piilotiedostoon .forward annetaan haluttu sähköpostiosoite, järjestelmä lähettää automaattisesti ajettujen skriptien lokit yms. varoitukset suoraan haluttuun sähköposti-osoitteeseen.

Mikäli palvelimen sähköpostipalvelut on määritetty oikein ja ne toimivat, ei .forward-tiedostoon tarvitse lisätä mitään muuta kuin haluttu sähkö-postiosoite.

Palvelimen palomuuri ei vastaa ulkopuolelta tuleviin ping-paketteihin. Palomuurin toimivuus tarkistettiin skannaamalla palvelimen portit Zenmap ohjelmalla ennen palvelimen viemistä yhteistyökumppanin laitetilaan. Tämä tehtiin jo ennalta valmiiksi, sillä palvelinten palomuurin asetusten muuttaminen etäyhteyden avulla ei ole järkevää. Yksi pieni virhe katkaisee etäyhteyden ja ylläpitäjän pitää lähteä laitetilaan, josta yhteistyökumppani laskuttaa aina ekstraa. Toinen syy on porttiskannauksen laittomuus. Toki omaa konettaan saa skannailla, mutta mikäli sen tekee Internetin ylitse, saattaa joutua selittelemään viranomaisille tekemisiään.

6.5 Paikallinen palvelin

Paikallisella palvelimella pyörivät samat skriptit ja järjestelmät, kuin etäpalvelimellakin. Niiden lisäksi paikallinen palvelin ajaa kahta lisäskriptiä. Ensimmäinen on tietenkin tietojen varmuuskopiointi etäpalvelimelle ja toinen ulkoisen IP-osoitteen varmistus-skripti. Skripti tarkistaa, mikä on palvelimen ulkoinen IP-osoite. Mikäli osoite on muuttunut viime tarkistuksesta, uusi IP-osoite lähetetään ylläpitäjälle sähköpostitse. Tämän jälkeen ylläpitäjä tekee tarvittavat DNS-päivitykset, jotta käyttäjät pääsevät edelleen palvelimelle ongelmitta.

NAT:n takana olevan palvelimen lähiverkon IP-osoite ei tietenkään ikinä muutu, sillä se on staattinen. Skripti siis tarkistaa ADSL-modeemin ulkoisen IP-osoitteen.

Erittäin harvassa pienessä yrityksessä on yritysliittymä Internet-yhteytenä, sillä ne ovat hyötyynsä nähden erittäin arvokkaita. Yksi suuri ero yritysliittymässä on, että niissä on usein staattinen, eli pysyvä ulkoinen IP-osoite. Staattiselle yrityksen ulkoiselle IP-osoitteelle ei tietenkään olisi mitään tarvetta, ellei yrityksen paikalliselle palvelimelle otettaisi yhteyttä ulkomaailmasta.

Normaalillakin yksityiskäyttöön tarkoitetulla ADSL-yhteydellä IP-osoitteen muuttuminen on erittäin harvinaista, vaikka ADSL-modeemin joutuisikin käynnistämään uudelleen, sillä osoitteita jakavat DHCP-palvelimet jakavat usein samoille laitteille samat osoitteet kuin aina ennenkin. DHCP-palvelimet yhdistävät asiakaslaitteen MAC-osoitteen tiettyyn IP-osoitteeseen, jolloin sama laite saa periaatteessa aina saman IP-osoitteen.

Paikallisen palvelimen ulkoiselle IP-osoitteelle määritetään oma DNS-nimi, jotta käyttäjien olisi helpompi ottaa yhteys palvelimeen. DNS-nimen käyttö helpottaa myös IP-osoitteen vaihtuessa, sillä tällöin ylläpitäjän ei tarvitse kertoa jokaiselle käyttäjälle erikseen, että he vaihtaisivat ohjelmistaan IP-osoitteen, johon he ottavat yhteyttä. Ottaen huomioon myös yrityksissä työskentelevien ihmisten tietotaitotason vaihtelut tietokoneita käytettäessä, tehtävä söisi huomattavan määrän ylläpidon resursseja.

Jotta kaikki paikallisen palvelimen palvelut toimisivat moitteetta, on ADSL-modeemiin asetettava niin kutsutut port forwardit halutuille palveluille. Port forwardit tarkoittavat sitä, että ADSL-modeemin tiettyyn ulkoiseen porttiin tuleva kysely ohjataan tietyn lähiverkon IP-osoitteen tiettyyn haluttuun porttiin.

7 CASE: PK-yrityksen tietojen varmuuskopiointi

Projektin tarkoituksena oli luoda varmuuskopiointijärjestelmä alle 10 henkilöä työllistävälle pk-yritykselle. Asennusta helpotti se, että yrityksen toimitiloissa oli jo valmis parikaapeliverkko, joten erillistä kaapelointityötä ei tarvinnut tehdä.

7.1 Paikallinen palvelin

Koska yrityksessä ei ollut ennestään yhtäkään paikallista palvelinta ja yrityksen sihteeri tarvitsi uuden työaseman, tehtiin sihteerin vanhasta työasemasta paikallinen varmuuskopiointipalvelin.

Tämä lisäsi hieman työtaakkaa, sillä varmuuskopiointijärjestelmän asentamisen lisäksi piti myös siirtää sihteerin vanhan koneen tiedot, asetukset sekä ohjelmat uudelle koneelle.

Paikallisena palvelimena tässä projektissa käytettiin ajan säästämiseksi Windows käyttöjärjestelmän omaavaa tietokonetta. Jälkeenpäin katsottuna, vaikka koneen kiintolevyn olisi kokonaan formatoinut ja asentanut siihen Linux-käyttöjärjestelmän olisin saattanut päästä vähemmällä. Windowsin taipuminen esim. automatisoituun SSH-tiedonsiirtoon, puhumattakaan tarvittavista komentorivi-skripteistä, on lähes olematonta. Mahdollista, mutta olematonta.

7.2 Etäpalvelin

Etäpalvelimena käytettiin Saferock IT Solutions Oy:n omaa varmuuskopiointipalvelinta, joka sijaitsee erään palvelinhotellipalveluja tuottavan yrityksen tiloissa.

8 CASE: Valokuvaajan tiedostojen varmuuskopiointi

Projektin tarkoituksena oli luoda valokuvaajalle varmuuskopiointijärjestelmä, joka kattaisi valokuvaajantyön erityistarpeet, kuten suurien tiedostokokojen nopean siirtelyn sekä muokkauksen.

8.1 Paikallinen palvelin

Järjestelmän luonti aloitettiin uuden palvelimen rakentamisella. Palvelin rakennettiin monella tavalla, kuten etäpalvelinkin on rakennettu. Tiedostoja turvaamaan asennettiin RAID-järjestelmä ja palvelimeen asennettiin kaksi verkkokorttia. Toinen yhdistettiin suoraan valokuvaajan tietokoneeseen käännetyllä verkkokaapelilla ja toinen ADSL-modeemiin etävarmuuskopioinnin suorittamiseksi.

Tämä tehtiin, jotta tiedostojen siirto olisi mahdollisimman nopeaa. Testeissä kuitenkin osoittautui, ettei kuvia voinut editoida verkon ylitse, vaikka käytössä olikin 1000 Mbps:n verkkoyhteys koneiden välillä. Näin ollen järjestelmää paranneltiin siten, että kuvapankin lisäksi palvelimella on oma kansionsa työstettäville kuville, jotka editoidaan suoraan työaseman kiintolevyltä, mutta varmuuskopioidaan päivittäin palvelimelle.

8.2 Etäpalvelin

Etäpalvelimena käytettiin Saferock IT Solutions Oy:n etäpalvelinta. Etäpalvelimelle varmuuskopioidaan vain työstämisvaiheessa olevat sekä valmiit kuvat. Etävarmistus suoritetaan vain näille kuville, sillä niiden säilyminen on kaikkein tärkeintä.

9 Yhteenveto

Koko projekti varmuuskopiointijärjestelmän kehittämisestä käytännön toteutuksiin on ollut erittäin kiehtova. Matkalla on ollut erilaisia ylä- ja alamäkiä, ja järjestelmä on kokenut monia kasvojen kohotuksia erilaisten ohjelmisto sekä toimintatapa, muutosten muodossa.

Molemmat CASE-projektit olivat haastavia, joskin kumpainenkin eri tavoilla. PK-yrityksen kohdalla haasteet olivat suurimmaksi osaksi aikataulullisia. Valokuvaajalle tekemässämme varmuuskopiointijärjestelmässä taas harmaita hiuksia aiheutti lähinnä siirrettävien tiedostojen koko.

Näkemäni ja kokemani perusteella voin sanoa, että tietojen varmuuskopioinnin kannattaa olla kunnossa, olitpa sitten yrittäjä, yrityspäättäjä tai yksityinen henkilö. Yritykselle tietojen menettäminen saattaa pahimmassa tapauksessa tietää konkurssia, ja vähemmän pahassa vähintäänkin suurta työmäärää. Yksityiselle taas esim. digikuvien menetys tarkoittaa paljoa mielipahaa ja harmia.

Itse olen omakohtaisten digikuvien sekä koulutöiden menetysten takia kiinnostunut asiasta, ja nykyään pidänkin huolen siitä, että kaikki tietoni ovat vähintään kahdessa paikassa.

Kokonaisuutena katsottuna projekti on kuitenkin ollut kaikin puolin onnistunut. Matkalla tuli vastaan ongelmia, joita ei osannut odottaa lainkaan. Tällaisia olivat mm. erilaisten tiedostojärjestelmien tapa käsitellä tiedostojen aikamääreitä, Outlookin tapa käsitellä tiedostoja sekä varmuuskopiointisettien etävarmuuskopiointi.

LÄHTEET

Blum, R. 2008. Linux® Command Line and Shell Scripting Bible. 1. painos. Indianapolis: Wiley Publishing Inc.

Davison Wayne 2010. rsync. Viitattu 6.11.2010 http://samba.anu.edu.au/rsync/. Flyktman, R. 2002. Inside PC-laitetekniikka. 3. painos. Helsinki: Edita.

Habraken, T. 2008. Absolute beginner's guide to networking. 4. painos. Indianapolis: Que Publishing.

Hanscom, K. 2008. Fixed! ROBOCOPY Usage on Linux EXT2 / EXT 3 File Systems. Viitattu 21.11.2010 http://www.somelifeblog.com/2008/05/robocopy-usage-ext2-ext-3-linux- systems.html.

ITeF!x Consulting 2010. cwrsync - Rsync for Windows | ITeF!x. Viitattu 03.11.2010 http://www.itefix.no/i2/node/10650.

Koski, R.; Kajala, T. 2005. Linux ylläpitäjän käsikirja. 1. painos. Helsinki: Edita.

Little, D.; Farmer, S. & El-Hilali, O. 2007. Digital data integrity:the evolution from passive protection to active management. 1. painos. Indianapolis: John Wiley and Sons.

Lucius Cobian 2010. Cobian Backup. Viitattu 03.11.2010 http://www.educ.umu.se/~cobian/ cobianbackup.htm.

Mann, B. 2003. How to do everything with Microsoft Office Outlook 2003. 1. painos. California: McGraw-Hill Professional.

Microsoft Oy 2006. Description of Full, Incremental, and Differential Backups. Viitattu 25.10.2010 http://support.microsoft.com/kb/136621/fi.

Mueller, J. 2007. Windows Administration at the Command Line for Windows Vista, Windows 2003, Windows XP, and Windows 2000. 1. painos. Indianapolis: John Wiley and Sons.

Olson, J. 2009. Database archiving: How to keep lots of data for a very long time. 1. painos. Burlingtoni: Morgan Kaufmann Publishers.

Paananen, J. 2003. Tietotekniikan peruskirja. 1. painos. Jyväskylä: Docendo. Rantala, A. 2003. Linux. 1. painos. Jyväskylä: Docendo.

Samuelle, J. 2003. Mike Meyers' CompTIA Security+ Certification Passport, Second Edition. 1. painos. California: McGraw-Hill Professional.

Venema, W. 2010. The Posftix Home Page. Viitattu 6.11.2010 http://www.postfix.org/.