VIDEOTIEDOSTOJEN VARMUUSKOPIOINTI JA TIEDONSIIRTO PK-MULTIMEDIATOIMISTOSSA

HAMK
HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Ammattikorkeakoulututkinnon opinnäytetyö

Hämeen ammattikorkeakoulu, Tietojenkäsittelyn koulutusohjelma, Tradenomi

Kevät 2018

Roope Aramo

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Tietojenkäsittelyn koulutusohjelma, Tradenomi
Hämeen ammattikorkeakoulu, Visamäki

Tekijä Roope Aramo **Vuosi** 2018

Työn nimi Videotiedostojen varmuuskopiointi ja tiedonsiirto PK-multimediatoimistossa

Työn ohjaaja Erkki Laine

TIIVISTELMÄ

Opinnäytetyön tavoitteena oli tutkia varmuuskopiointia, tietoturvaa ja niihin kuuluvia asioita yleisellä tasolla ja tarjota kyseisistä aiheista helposti ymmärrettävä kokonaisuus lukijalle. Työn toimeksiantajana toimi Hämeen ammattikorkeakoulun yhteydessä toimiva pieni multimediatoimisto Studio C3. Toimeksiantajayrityksen vanha varmuuskopiointijärjestelmä oli hajonnut, ja sen tilalle luotiin suunnitelma uuden järjestelmän toteuttamista varten. Suunnitelma luotiin työhön kerätyn teorian pohjalta ja yhteistyössä yrityksen työntekijöiden kanssa.

Opinnäytetyön toimeksiantajayritykselle tehdyssä suunnitelmassa keskityttiin ratkaisemaan yrityksen työntekijöiden kanssa yhdessä kartoitetut keskeisimmät ongelmat, kuten tiedostojen varmuuskopiointi sekä lähiverkon hitaat yhteydet työasemien ja verkkolevypalvelimen välillä. Taloudellisen kannattavuuden vuoksi suunnitelmassa haettiin hyödyllisiä käyttötarkoituksia myös uusien laitehankintojen tieltä siirtyville vanhoille laitteille, roskalavalle päätymisen sijaan.

Suunnitelmalla pystyttiin korjaamaan toimeksiantajayrityksen suurin ongelma, eli tietojen varmuuskopioinnin puuttuminen. Varmuuskopioinnin kannalta tärkein laitehankinta oli uusi verkkolevypalvelin, jonka ympärille loput suunnitelmasta pystyttiin rakentamaan. Varmuuskopioinnin automatisointi poisti inhimillisen virheen riskin, lisäsi luotettavuutta ja vähensi työntekijöiden työtaakkaa. Lisäksi verkkolevypalvelimen mahdollistaman nopeamman yhteyden käyttäminen vähensi pullonkauloja yrityksen lähiverkossa tiedostoja siirrettäessä.

Avainsanat Varmuuskopiointi, palvelin, tallennusmedia, verkkolevypalvelin (NAS), pilvipalvelu, lähiverkko (LAN), tietoturva

Sivut 36 sivua

HÄMEEN AMMATTIKORKEAKOULU
HÄME UNIVERSITY OF APPLIED SCIENCES

Degree Programme in Business Information Technology
Häme University of Applied Sciences, Visamäki

Author	Roope Aramo	**Year** 2018
Subject	Backing up video files and data transfer in a small / medium sized multimedia office	
Supervisor	Erkki Laine	

ABSTRACT

The purpose of the thesis was to investigate backup, information security and related issues on a general level while providing a readily understandable set of information for the reader. The task was commissioned by the small multimedia company Studio C3 which operates in the premises of Häme University of Applied Sciences. Because the old backup system of the assignee company had broken down, the thesis introduced a plan for implementing a replacement system for file backup. The plan was created based on the theory gathered for the thesis and in co-operation with the company's employees.

The made plan for the assignee company focused on solving the most common problems that were identified together with the company's employees. The problems consisted of subjects such as file backups and slow connections between the workstations and the network access storage. Due to the economic viability of the plan, new useful uses were also sought for old appliances that would be replaced with new equipment purchases.

The plan was able to fix the lack of data backup that was the largest problem of the assignee company. The most important device purchase from the point of view of data backup was a new network access storage server, around which the rest of the plan could be built. By automating the data backup the risk of human error was removed and reliability increased while the workload of employees decreased. Additionally, using a faster connection, enabled by the new network access storage server, reduced bottlenecks while transferring files in the company's local network.

Keywords Backup, Server, Storage Medium, Network Access Storage (NAS), Cloud Service, Local Area Network (LAN), Information Security

Pages 36 pages

SISÄLLYS

1 JOHDANTO

Opinnäytetyön aiheena on varmuuskopiointi ja tiedonsiirto pienessä / keskisuuressa multimediatoimistossa. Opinnäytetyö käsittelee yrityskäytössä olevaa varmuuskopiointiin liittyvää laitteistoa ja tapoja, joilla varmuuskopiointi voidaan suorittaa luotettavasti niin, ettei se resursseja syömällä vaikuta päivittäiseen työskentelyyn yrityksessä.

Työ käsittelee teoriaa varmuuskopioinnin periaatteista, tietoturvasta ja tallennusmedioista (esimerkiksi palvelimet, Network Access Storage (NAS) ja pilvipalvelut). Lisäksi työssä käydään lyhyesti läpi historiaa varmuuskopioinnissa käytetyistä ratkaisuista. Pääasiassa teoriaosuus koostuu opinnäytetyössä tehtävän varmuuskopiointi- ja tiedonsiirtojärjestelmän sisältävistä aiheista, kuten varmuuskopioinnin menetelmistä, siihen liittyvistä laitteista, tietoturvallisuudesta ja varmuuskopioinnin kytkeytymisestä siihen.

Käytännössä työ suoritettiin HAMKin Visamäen kampuksella toimivalle Studio C3:lle. Siirrettävien tiedostojen koot mediatoimistolla voivat olla poikkeuksellisen suuria, joten oikean laitteiston valinta ja hyvin optimoitu kokonaisuus olivat tärkeitä asioita järjestelmän toimivuuden kannalta. Lisäksi työssä piti ottaa huomioon sujuva tiedostojen siirto yrityksen sisällä ja asiakkaiden välillä.

Opinnäytetyössä luodaan Studio C3:lle toimiva suunnitelma yrityksen käyttämien tärkeiden tiedostojen varmuuskopiointia varten. Varmuuskopiointi pyritään toteuttamaan useampaan kuin yhteen paikkaan alkuperäisen tallennuspaikan lisäksi. Mahdollisia sijainteja varmuuskopioille ovat yrityksen palvelin, paikallinen levyjärjestelmä ja NAS-verkkolevypalvelin. Suunnitteilla on ottaa käyttöön myös One Drive -tili, johon varmuuskopiot tallennettaan automatisoidusti tietyin aikavälein. Pilvipalvelu tarjoaa turvallisen paikan tallentaa tiedostoja yrityksen tilojen ulkopuolelle, missä tiedot ovat paikallisen tallennuspaikan lisäksi turvassa rikollisuudelta, vesivahingolta, tulipalolta ja useilta muilta tietoteknisiltä ja fyysisisiltä riskeiltä.

Turvallisen varmuuskopioinnin lisäksi työssä huomioidaan asiakkaan ja yrityksen välisten tiedostojen siirron sujuvuus. Asiakkaiden kanssa käytössä on HAMKin sisäinen verkko ja Google Drive, joka mahdollistaa tiedostojen jaon myös HAMKin sisäisen verkon ulkopuolella toimiville asiakkaille.

Suunnitelman valmistuttua ja asiakkaan hyväksyttyä sen tarkoituksena oli aloittaa käytännön työ järjestelmän parissa. Riippuen asiakkaan budjetista, uusien ohjelmien ja laitteiden kuten verkkolevypalvelimen ja verkkokorttien asennus, piti liittyä osaksi opinnäytetyötä. Ohjelmistojen osalta tehtävät olisivat koostuneet pääasiassa tarvittavien asetusten asettamisesta

työn tilaajan käytössä oleville tietokoneille uusien laitteiden asennusten jälkeen. Uusien laitteiden kuten verkkolevypalvelimen tilauksen toimitusaika venyi yllättäen opinnäytetyön suoritusajan ulkopuolelle, minkä takia opinnäytetyön käytännön osuuteen ei varsinaista fyysistä asennustyötä ehditty ottamaan mukaan.

Opinnäytetyössä pyritään vastaamaan tutkimuskysymyksiin:

- Mitä asioita pitää ottaa huomioon varmuuskopiointijärjestelmää suunniteltaessa?
- Millaista varmuuskopiointia pieni multimediatoimisto tarvitsee, kun data koostuu pienistä määristä suuria tiedostoja?
- Millä tavoilla varmuuskopiointia ja tiedonsiirtoa voidaan optimoida?

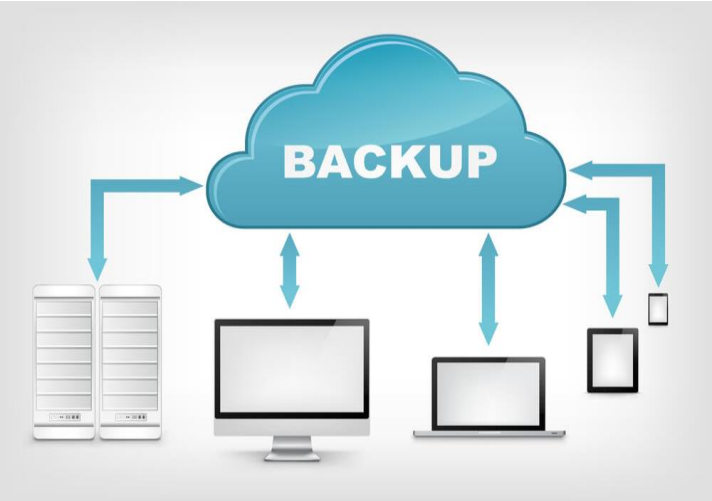
2 VARMUUSKOPIOINTI

Tässä luvussa kerrotaan yleisesti varmuuskopioinnista ja siihen liittyvistä riskeistä. Luku esittelee myös varmuuskopiointijärjestelmään liittyviä laitteita ja niiden toimintaa. Lisäksi käydään läpi varmuuskopioinnin historiaa ja sen kehitystä vuosien varrella sekä erilaisia menetelmiä, joilla yksityishenkilö tai yritys voi oman varmuuskopiointinsa suorittaa.

2.1 Varmuuskopioinnista lyhyesti

Varmuuskopiointi tarkoittaa prosessia, jossa tietokoneen tiedostot kopioidaan ja arkistoidaan yhteen tai useampaan paikkaan alkuperäisen tallennuspaikan lisäksi. Yksityiskäytössä hyvä paikka varmuuskopioille voi olla USB-muistitikku (Universal Serial Bus). Yrityskäytössä suuremmat tiedostot voidaan kopioida esimerkiksi yrityksen paikallisen palvelimen kiintolevyille.

Tietokoneiden kanssa työskennellessä tietojen häviäminen ja korruptoituminen ovat harmillisen yleinen ongelma. Yleensä syynä on inhimillinen virhe. Muita tietojen menetykseen liittyviä riskejä voivat olla esimerkiksi tulipalo, vesivahinko, maanjäristys, virtapiikki tai rikollisuus hakkeroinnin ja fyysisen varkauden muodossa. Varmuuskopiointi on tehokas tapa ehkäistä tiedostojen menetykseen liittyviä riskejä, koska se mahdollistaa menetettyjen tiedostojen palauttamisen. Sen varmuutta voidaan parantaa ajamalla varmuuskopiot lyhyin aikavälein ja luomalla tiedostokopiot useampaan kuin yhteen paikkaan, esimerkiksi kopioimalla tiedostot automatisoidulla komentosarjalla palvelimelta tai muilta laitteilta pilveen (Kuva 1). Varmuuskopiointia voidaan pitää yhtenä tärkeimmistä tekijöistä yrityksen jatkuvuuden ja tietoturvallisuuden kannalta, sekä tehokkaana ratkaisuna haittaohjelmien ja virusten aiheuttamiin ongelmiin.



Kuva 1. Varmuuskopiointi pilvipalveluun (Prinzlau 2017).

Varmuuskopiointi voidaan jakaa paikalliseen ja etävarmuuskopiointiin. Yleinen toimintatapa varmuuskopiointijärjestelmän toteutuksessa on, että tiedostokopiot tallennetaan ensisijaisesti paikallisesti esimerkiksi yrityksen palvelimen kovalevyille, joka sijaitsee yrityksen toimitiloissa. Palvelimelta tiedot kahdennetaan maantieteellisesti eri paikassa sijaitsevaan paikkaan, esimerkiksi pilvipalveluun tai toisessa rakennuksessa sijaitsevalle palvelimelle. Etävarmuuskopioinnissa kannattaa ottaa huomioon, että tiedostojen siirto tapahtuu internetin välityksellä, joten siirtonopeudet ovat huomattavasti hitaampia kuin paikallisessa tiedostonsiirrossa. Tiedostojen siirtäminen vaatii myös ison osan verkkokapasiteetista. Lisäksi kolmannen osapuolen palveluntarjoajia käytettäessä tiedon varmuuskopiointiin tulee tarkistaa palveluntarjoajan luotettavuus, kun tärkeät tiedostot luovutetaan täysin ulkoisen toimijan säilytettäväksi. Mikäli etävarmuuskopiointia tehdään usein, kannattaa se suorittaa sellaiseen aikaan, ettei se vaikuta työntekijöiden työhön syömällä resursseja yrityksen internetyhteydestä. Tällä tavalla voidaan eliminoida vesivahingon tai tulipalon aiheuttamat riskit, koska on hyvin epätodennäköistä, että esimerkiksi tulipalo sattuu kahdessa yritykselle tärkeässä rakennuksessa yhtä aikaa.

Valitettavan useissa yrityksissä varmuuskopioinnin tärkeys aliarvioidaan tai siihen ei panosteta tarpeeksi siitä aiheutuvien kustannusten vuoksi. Yrityksen tietojen arvoa voi olla vaikea suoraan rahallisesti määrittää ja siksi varmuuskopiointijärjestelmän hankkiminen voi olla vastahakoista. Paljon tietokoneiden kanssa tekemisissä olevissa yrityksissä varmuuskopiointi toimii kuin kattava vakuutus. Ulkoistettuna palveluna siitä aiheutuu yritykselle rahallisia kuluja ja yrityksen sisäinen varmuuskopiointijärjestelmäkin vaatii uusien laitteiden hankintoja sekä tietyn määrän henkilökuntaa ylläpitämään järjestelmää. Optimitilanteessa varmuuskopioita ei tulla ikinä tarvitsemaan, minkä takia tietyt yritykset suhtautuvat varmuuskopiointijärjestelmän hankkimiseen nihkeästi. Katastrofin sattuessa, kun kaikki tiedot on menetetty, varmuuskopiointi osoittautuu kuitenkin korvaamattomaksi pelastautumissuunnitelmaksi.

2.2 **Varmuuskopiointimenetelmiä**

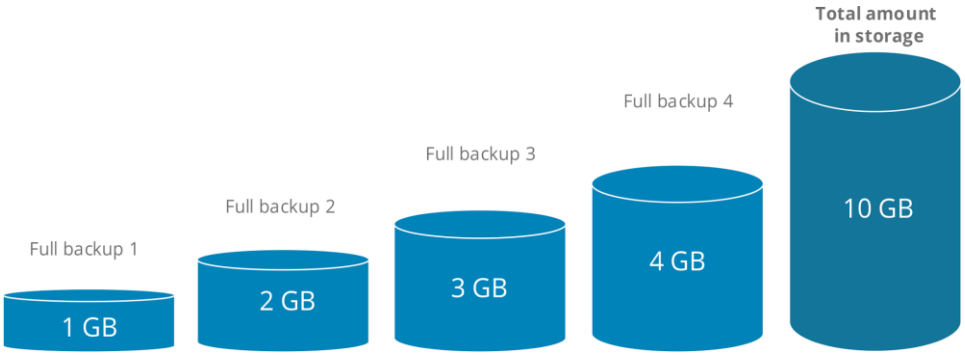
Kaikki varmuuskopiointisuunnitelmat alkavat kysymyksellä: Miten tieto varmuuskopioidaan? Varmuuskopiointi voidaan suorittaa manuaalisesti käsin kopioimalla tiedostot alkuperäisestä tallennuspaikasta toiseen sijaintiin tai automatisoimalla prosessi varmuuskopiointiohjelman avulla. Yksityiskäytössä manuaalinen tapa voi olla hyvinkin riittävä, mutta yritysten laajemmissa tietoympäristöissä varmuuskopioinnin ainakin osittainen automatisointi on suositeltavaa. Varmuuskopiotiedoista ja niiden päivämääristä on suositeltavaa pitää kirjaa esimerkiksi luettelon tai tietokannan avulla. Näin pysytään selvillä siitä, mitä tietoa mihinkin paikkaan on tallennettu ja vältytään turhalta sekaannukselta, kun varmuuskopiotietoja tarvitaan. Eri varmuuskopiointiohjelmat käyttävät erilaisia tapoja tietojen kopi-

oimiseen ja tapoja on olemassa lukuisia, mutta jo jonkin aikaa yleisesti käytössä on ollut kolme perusmenetelmää tiedon varmuuskopioimiseksi. Nämä ovat nimeltään täysi, inkrementaalinen ja differentiaalinen varmuuskopiointi. Kolmen varmuuskopioinnin perusmenetelmän ominaisuuksien hyviä ja huonoja puolia taulukossa 1. (Posey 2010.)

Taulukko 1. Varmuuskopiointimenetelmät (Backup4All 2012).

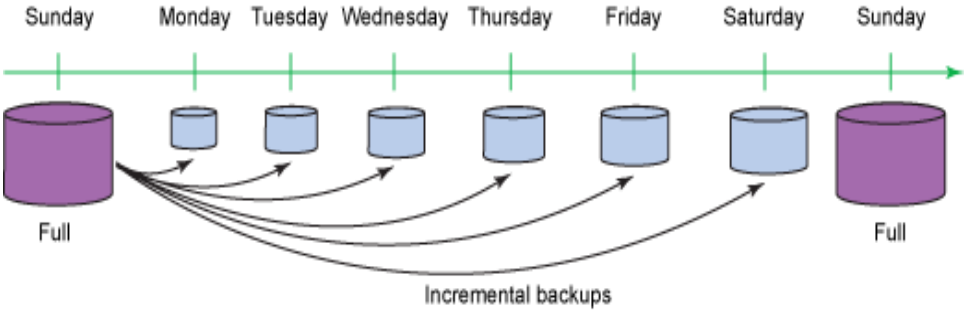
Varmuuskopiointimenetelmä	**Varmuuskopioitu tieto**	**Varmuuskopiointiaika**	**Palautumisaika**	**Vaadittu tallennustila**
Täysi	Kaikki tieto	Hitain	Nopea	Korkea
Inkrementaalinen	Vain uudet /muokatut tiedostot/kansiot	Nopea	Keskiverto	Matala
Differentiaalinen	Kaikki tieto viimeksi tehdyn täyden varmuuskopioinnin jälkeen	Keskiverto	Nopea	Keskiverto

Ensimmäinen kolmesta läpikäytävästä varmuuskopioinnin perusmenetelmästä on täysi varmuuskopiointi. Nimensä mukaisesti tämä tallennusmenetelmä sisältää kaiken tiedon järjestelmästä ja siksi toimii perustana myös muille varmistusmenetelmille. Vaikka täysi varmuuskopiointi takaa parhaan tietoturvallisen suojan tiedoille, käytetään sitä yrityksissä varsin pitkin aikavälein ja työajan ulkopuolella, koska menetelmänä se vaatii paljon aikaa ja laiteresursseja. Täysi varmuuskopiointi voidaan vielä jakaa kiintolevyn kloonaamiseen ja järjestelmäkuvan luomiseen. Kloonatessa kiintolevyltä kopioidaan kaikki sen sisältämä tieto toiselle kiintolevylle. Järjestelmän hajotessa kloonaaminen on nopea tapa palata työn ääreen yksinkertaisesti vaihtamalla kloonin sisältävä kiintolevy tietokoneeseen. Järjestelmäkuvan tekeminen on kuin ison pakatun tiedoston luominen. Järjestelmäkuva on kooltaan paljon pienempi kuin suora klooni kiintolevystä ja siksi menetelmänä monipuolisempi käyttötarkoituksiltaan. Esimerkiksi useista tietokoneista voidaan luoda järjestelmäkuva yhdelle kiintolevylle. (Spector 2013.)



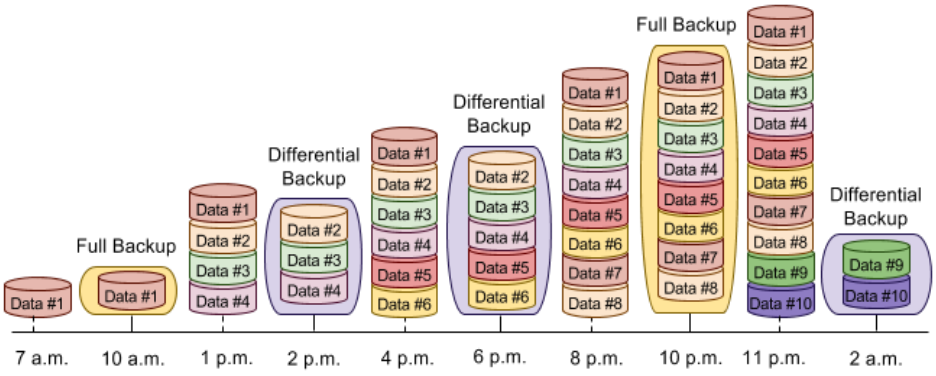
Kuva 2. Täysi varmuuskopiointi (CloudBerry Lab n.d.).

Koska täysi varmuuskopiointimenetelmä vie paljon aikaa, kehiteltiin inkrementaalinen eli kasvava varmuuskopiointi, joka vaatii vähemmän aikaa ja tallennuskapasiteettia. Pääperiaate inkrementaalisessa menetelmässä on varmuuskopioiden luominen vain tiedosta, joka on muuttunut edellisestä varmuuskopioinnista, riippumatta siitä mitä menetelmää on käytetty. Esimerkiksi työviikon alussa maanantaina tehdään täysi varmuuskopio yrityksen tiedoista ja muina viikonpäivinä suoritetaan inkrementaalinen varmistus. Tällöin tiistaina suoritettu varmistus sisältää vain maanantaista muuttuneet tiedot ja keskiviikkona suoritettu varmistus vain tiistaista muuttuneet tiedot ja niin edelleen. Kuvassa 3 on selkeämmin kuvattu inkrementaalisen varmuuskopioinnin toiminta. Inkrementaalisen varmuuskopioinnin heikkous on tietojen palauttamisen hitaus. Palauttaminen täytyy tehdä yksi varmistus kerrallaan, ja jos välistä puuttuu varmistus tai varmistus on vahingoittunut, kaikkea tietoa ei pystytä palauttamaan. (Posey 2010.)



Kuva 3. Inkrementaalinen varmuuskopiointi (Brook, A. 2017).

Kolmas varmuuskopioinnin perusmenetelmistä on differentiaalinen varmuuskopiointi. Menetelmänä siinä on varsin paljon yhteneväisyyksiä inkrementaaliseen varmistukseen. Molemmat menetelmät alkavat täydestä varmuuskopiosta, ja sitä seuraavat varmistukset sisältävät vain muuttuneen tiedon. Ero inkrementaaliseen varmistukseen on, että differentiaalinen menetelmä sisältää aina kaiken muuttuneen tiedon edellisestä täydestä varmuuskopioinnista. Esimerkiksi työviikon alussa maanantaina tehdään täysi varmuuskopiointi tiedoista ja differentiaaliset varmistukset joka päivä loppuviikon ajan. Tiistaina differentiaalinen varmistuksen sisältö olisi täysin identtinen inkrementaaliseen varmistuksen sisällön kanssa. Keskiviikkona taas muutaman lisätiedoston muuttuessa differentiaalinen varmistus sisältäisi kaiken tiedon, joka on muuttunut tiistain ja keskiviikon aikana maanantaina tehdystä täydestä varmuuskopioinnista. Differentiaalisen varmuuskopioinnin sykli jatkuu aina siihen asti, kunnes tehdään uusi täysi varmuuskopiointi, jolloin sykli alkaa uudestaan alusta. Differentiaalisen varmuuskopioinnin toiminta havainnollistettu kuvassa 4. Differentiaalisen menetelmän heikkous inkrementaaliseen varmistukseen verrattuna on, että se vaatii enemmän tallennuskapasiteettia. Etuna ovat kuitenkin nopeammat ja helpommat tiedon palautusajat, sillä differentiaalisen varmuuskopion palauttaminen ei koskaan vaadi enempää kuin kaksi varmistusta. (Posey 2010.)



Kuva 4. Differentiaalinen varmuuskopiointi (Omelchenko 2015).

2.3 Tallennusmediat ja varmuuskopioinnin laitteet

Riippumatta varmuuskopiointimenetelmästä tieto pitää pystyä tallentamaan johonkin. Tietotekniikassa tallennusmedialla tarkoitetaan laitteita tai materiaaleja, joihin tietoa tallennetaan, säilytetään ja joista sitä voidaan myös palauttaa. Yleensä kyseessä on toissijainen paikka säilyttää tietoa, kuten varmuuskopioita. Tekniikan kehittyessä ja kilpailun kiihtyessä markkinoille on ilmaantunut uusia tallennusmedioita, jo olemassa olevat ratkaisut kehittyvät hyvää vauhtia ja hinnat ovat laskeneet. Yleisimpiä ja tunnetuimpia tallennusmedioita nykypäivänä ovat CD- (Compact Disc), DVD- (Digital Versatile Disc), ja Blu-ray-levyt, Flash-muistit, kuten USB-tikut (Universal Serial Bus), muistikortit ja SSD-muistit (Solid State Drive) sekä magneettiset tallennusvälineet, kuten kiintolevyt ja magneettinauhaan perustuvat tallennusvälineet. Lisäksi nykyään on tarjolla myös laaja valikoima etätallennusvaihtoehtoja, kuten pilvipalveluita. (Computer Hope 2017.)

Tallennusmedioita on lukuisia, mutta vain kourallinen vaihtoehdoista on päätynyt yleiseen käyttöön varmuuskopiointijärjestelmissä. Käytettävää tallennusmediaa valittaessa täytyy olla selkeä tieto siitä, minkälaista ja miten paljon tietoa halutaan tallentaa. Erityisesti suuria tietomääriä käsittelevissä varmuuskopiointijärjestelmissä suosiota ovat niittäneet NAS-verkkolevyt (Network Attached Storage), HDD-kiintolevyt (Hard Disk Drive), pilvipalvelut ja magneettinauhat. Esimerkiksi optisten tallennusmedioiden käyttö varmuuskopioinnissa ei ole kannattavaa, koska niiden kapasiteetti tiedon tallentamisessa on pieni ja ne ovat herkkiä vaurioitumaan. DVD- ja CD-levyille tallennetun tiedon lukemisen voi estää jo pienikin naarmu tai tahra levyn pinnassa. Toisaalta viime vuosina on kehitetty uudenlaisia optisia levyjä, kuten M-DISC (Millennial Disc), jonka patentoidun teknologian väitetään pitävän tiedon levylle kirjoitettuna jopa 1000 vuoden ajan oikein säilytettynä. (M-DISC n.d.)

Tekniikan kehityksen myötä kiintolevyjen tallennuskapasiteetit ovat kasvaneet paljon ja samalla niiden hinta on pudonnut. Kiintolevyjen kirjoitus- ja lukunopeudet ovat hyvät, ja ne ovat helposti asennettavissa ja vaihdettavissa tallennusjärjestelmään. Kiintolevy voi olla tietokoneen sisäinen tai ulkoinen esimerkiksi USB-yhteydellä. Yleensä sisäisillä liittimillä kiinnitetyn kiintolevyn kirjoitus- ja lukunopeudet ovat paremmat kuin ulkoisesti esimerkiksi USB-liittimellä kiinnitetyn kiintolevyn. Kiintolevyjen heikkoutena on niiden herkkyys fyysiselle rasitukselle kuten kolhuille, koska kiintolevyt toimivat liikkuvien mekaanisten osien avulla. Tämä tuo mukanaan riskin tiedon säilyvyyden vakaudessa riippuen siitä, miten raskaassa käytössä kiintolevy on. (Computer Hope 2017.)

SSD-massamuistien käyttö varmuuskopioinnin tallennusmediana on pikkuhiljaa nostamassa päätään myös yrityskäytössä. Etuja SSD-teknologiassa verrattuna perinteisiin HDD-kiintolevyihin ovat nopeampi tiedonsiirto, pienempi virrankulutus, äänettömyys ja vähäinen lämmöntuotto. Lisäksi SSD-levyt ovat kiintolevyjä pienempiä ja kevyempiä eikä niissä ole liikkuvia osia, joten ne kestävät paljon paremmin fyysistä rasitusta. SSD on tallennusmediana varsin uusi, jonka vuoksi SSD-levyjen hinnan suhde tallennuskapasiteettiin on vielä huono. SSD on kuitenkin nopeasti kehittyvä teknologia, jonka tiedonsiirtonopeus ja tallennuskapasiteetti kasvavat jatkuvasti samalla kun tarjonta markkinoilla monipuolistuu ja hinnat laskevat. (Z-DBackup n.d.)

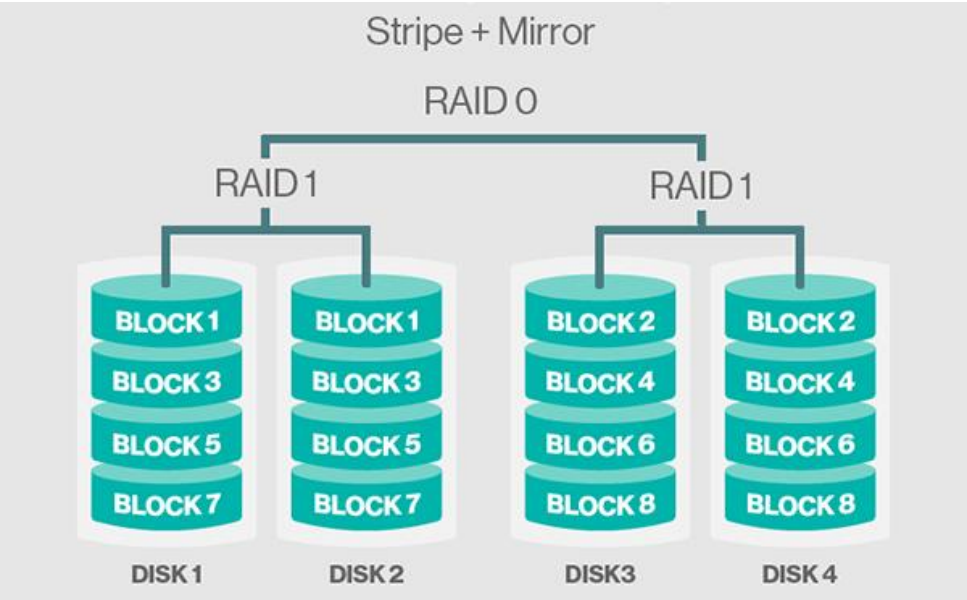
Magneettinauhoja sekä nauhoja lukevia ja niille kirjoittavia nauha-asemia on etenkin varmuuskopioinnissa käytetty jo 60-luvulta lähtien. Magneettinauhat ovat tallennusmediana vielä nykyäänkin hyvin varteenotettava vaihtoehto, koska niille voidaan tallentaa ja arkistoida tietoa pitkäaikaista säilytystä varten. Magneettinauhojen vahvuus on siis niiden luotettavuus. Heikkouksia ovat nauhojen hinnan ja tallennuskapasiteetin suhde, sillä kehityksen ja markkinoiden kilpailutuksen myötä tavallisten kiintolevyjen käyttö saattaa olla edullisempi ratkaisu. Lisäksi magneettinauhoille kirjoittamiseen ja niiden lukemiseen tarvitaan erillinen nauha-asema, joka lisää järjestelmäkustannuksia. (Encyclopædia Britannica n.d.) Vaikka magneettinauha on hyvin vanha tiedon tallennusteknologia, sitä kehitetään edelleen. Esimerkiksi vuonna 2017 IBM ja Sony kehittivät yhteistyössä uuden magneettinauhajärjestelmän, joka kykenee tallentamaan jopa 201 gigabittiä tietoa yhdelle neliötuumalle magneettinauhaa. Teoriassa tällä tekniikalla olisi mahdollista tallettaa jopa 330 teratavua tietoa yhdelle kämmenelle mahtuvalle kasetille. (Sebastian 2017.)

Jo 90-luvun puolivälistä lähtien erilaiset verkkolevyjärjestelmät (NAS) ovat kasvattaneet suosiotaan etenkin pienien ja keskisuurten yritysten varmuuskopiointijärjestelmien toteutuksessa. Periaatteessa NAS ei itsessään ole tallennusmedia, mutta sen tarjoama tekniikka mahdollistaa luotettavamman tallennusympäristön. NAS-verkkolevyt muodostavat tallennuskapasiteettinsa käyttämällä useita kiintolevyjä samaan tapaan kuin useita kiintolevyjä käyttävä tietokone. (Synology n.d.)

2.4 **RAID**

Useamman kuin yhden kiintolevyn käyttäminen mahdollistaa RAID-tekniikan (Redundant Array of Independent Disks) hyödyntämisen tietojen tallennuksessa. Käyttämällä RAID-tekniikkaa kiintolevyjen lukunopeuksia ja luotettavuutta voidaan parantaa häiriötilanteen sattuessa. Yleisimmät kuluttajatason käyttämät RAID-tasot ovat RAID 0 eli lomitus (striping), RAID 1 eli peilaus (mirroring), RAID 10-hybriditaso, RAID 5 ja RAID 6. (Synology n.d.)

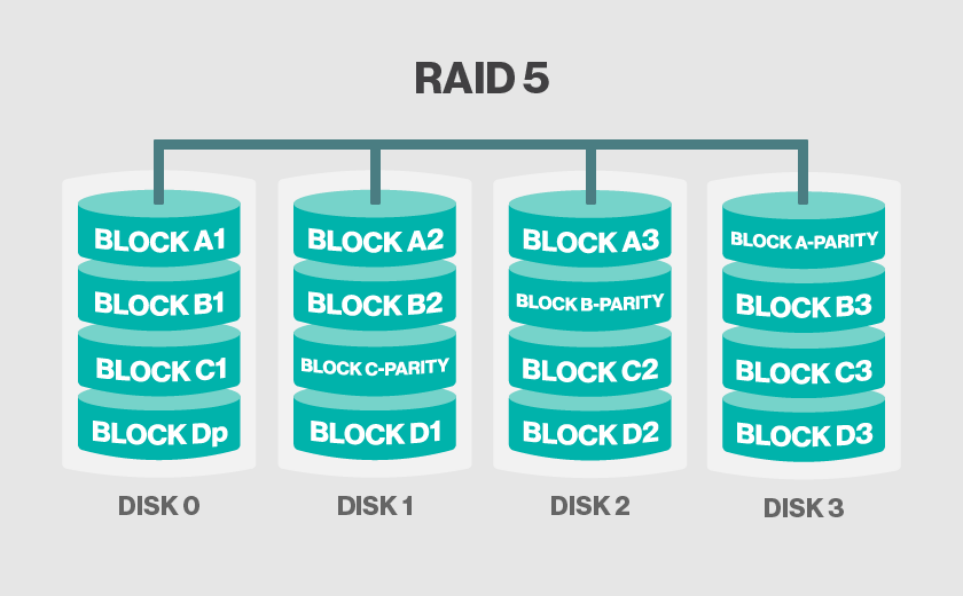
Käytännössä RAID 0-tasolla useita erillisiä kiintolevyjä voidaan lomittamalla yhdistää yhdeksi loogiseksi levyksi. Tekniikkaa voidaan soveltaa usealla eri tavalla ja riippuen käytetystä RAID-tyypistä tietojen menettämisen riski voidaan eliminoida. RAID 1-tasolla eli peilaamisella sama tieto tallennetaan kahdelle tai useammalle erilliselle levylle. Näin tieto ei katoa, vaikka yksi järjestelmän levyistä hajoaisi ja samalla voidaan moninkertaistaa peilatun tiedon lukunopeus. Hybridissä RAID 10-tasossa levyistä luodaan lomitettu kokonaisuus kahdesta tai useammista peilatuista levyistä. Tällä tekniikalla levykokoelma voi pysyä toimintakuntoisena, vaikka useampia levyjä vaurioituisi niin kauan, kun peilattu kokonaisuus ei menetä kaikkia levyjään. RAID 10-hybriditason kiintolevyjen lomittaminen ja peilaaminen on havainnollistettu kuvassa 5. (Synology n.d.)



Kuva 5. RAID-tekniikan lomittaminen ja peilaaminen (Sullivan & Poelker 2017).

RAID 5-taso toimii periaatteessa samalla tavalla kuin RAID 0, jossa levyt on yhdistetty yhdeksi loogiseksi levyksi ja niille tallennettu tieto levitetään tasaisesti kaikille pakassa toimiville levyille. RAID 5-tason varmistus perustuu pariteettidataan, joka tallennetaan tasaisesti kaikille RAID-pakassa toimiville levyille niin, että minkä tahansa yhden levyn hajotessa pariteettidatan

avulla voidaan rekonstruktoida kaikki kyseisen levyn sisältämä tieto. Kyseisessä tekniikassa tallennustila on aina levyjen kokonaismäärä kertaa levyjen tallennuskapasiteetti, miinus yhden levyn tallennuskapasiteetti, joka käytetään hajautetun pariteettidatan tallentamiseen. Esimerkiksi kuvassa 6, levy nollan hajotessa menetetään lohkojen A1, B1, C1-osioiden sisältämä tieto sekä D-lohkon pariteettidata. Menetetyt tiedot pystytään kuitenkin palauttamaan muilla pakassa olevilta levyiltä. Esimerkiksi levyillä 2 ja 3 on vielä tallessa C-lohkon C2 ja C3-osiot sekä levyllä 1 C-lohkon pariteettidata. Laskemalla C2 ja C3-osioiden sisältämät tiedot suhteessa C-lohkon pariteetin sisältämään tietoon, voidaan määrittää menetetty tieto ja rakentaa se uudestaan pariteettidatan pohjalta. Kun käytetään RAID 5-tasoa, useamman kuin yhden levyn hajotessa kaikki tieto kuitenkin menetetään, koska tiedon palauttamista varten tehtävää laskutoimitusta ei voida enää suorittaa. RAID 6-tyyppi toimii muuten samalla tavalla kuin RAID 5, mutta se sisältää enemmän pariteettidataa. RAID 6:ssa toimivasta levypakasta voidaan menettää yhtäaikaisesti kaksi levyä ilman, että tietoa menetetään. (Rouse 2014b.)



Kuva 6. RAID 5-tason toiminta (Rouse 2014b).

Vaikka RAID-tekniikkaa voidaan käyttää tavallisen työaseman käyttöjärjestelmän levyajureissa, tekniikan käyttäminen vaatii suhteellisen paljon suoritintehoa, joten yleensä se tehdään erityisesti kyseiseen tarkoitukseen varatulla RAID-ohjaimella. Kehittyneemmissä palvelimissa ja verkkolevyjärjestelmissä on mahdollista vaihtaa vaurioituneita levyjä ja rekonstruktoida RAID-järjestelmä ilman, että laitetta sammutetaan käyttämällä hot swap -tekniikkaa. Lisäksi kehittyneemmissä laitteissa levyjä voidaan varata hot spare -tekniikkaa varten. Tässä järjestelmän ylimääräiseksi varattuja levyjä voidaan ottaa lennosta käyttöön vaurioituneen levyn tilalle vikatilanteen sattuessa. (Synology n.d.)

2.5 **Pilvipalvelut**

Tiedon tallentaminen niin sanottuun pilveen on yleistynyt nykypäivänä. Esimerkiksi yrityksen varmuuskopioinnin ulkoistaminen pilvipalveluun on mahdollista sen sijaan, että itse tehtäisiin laitehankintoja ja ylläpidettäisiin varmuuskopiointiin liittyvää järjestelmää. Pilvipalveluiden käyttö on helppoa ja tarjoaa kätevän ratkaisun useille yrityksen tietoteknisille tarpeille. Eri pilvipalvelumalleissa palveluntarjoajan ja kuluttajan vastuualueet ovat erilaisia ja siksi palvelua hankittaessa on tärkeää ymmärtää, kuka on vastuussa mistäkin osasta ostettavaa tuotetta. Suurimmat riskit pilvipalvelua käytettäessä ovat tietoturvauhat. Siksi palveluntarjoajaa valittaessa on tärkeää vertailla, minkälaista tietoturvaa tarjotaan ja missä tietoja maantieteellisesti säilytetään. (Laaksonen 2015.)

Pilvipalvelu on resurssi, joka tarjotaan kuluttajalle internetin välityksellä. Käytännössä pilvipalvelu tarkoittaa tietotekniikan palvelullistamista pilvilaskennan avulla. National Institute of Standards and Technology (NIST) määrittelee pilvilaskennan toimintamalliksi, jonka perusajatuksena ovat helposti käyttöön ja pois käytöstä otettavat, muokattavat ja skaalautuvat tietotekniikkapalvelut, joita tarjotaan niin että asiakkaalle aiheutuu mahdollisimman vähän vaivaa ylläpidosta ja vuorovaikutuksesta palveluntarjoajan kanssa. Tarjottuja palveluita voivat olla esimerkiksi verkot, palvelimet, tallennustila, sovellukset ja palvelut. Lisäksi NIST-määritelmä pitää sisällään viisi ominaispiirrettä, kolme palvelumallia ja neljä pilvityyppiä. Tärkeät ominaispiirteet ovat käytön tasainen valvonta, dynaaminen skaalautuvuus, resurssien jakaminen, laaja käytettävyys verkon yli ja vaadittaessa itsepalvelu. (NIST 2010.)

Yleisimmän pilvipalvelutyypit ovat julkinen pilvi (public cloud), yhteisöpilvi (community cloud), yksityinen pilvi (private cloud) ja hybridipilvi (hybrid cloud). Julkisessa tyypissä pilvipalvelu ja infrastruktuuri ovat julkisesti jaettu Internetissä. Palvelu on palveluntarjoajan ylläpitämä ja useiden käyttäjien jakama ympäristö, jonka kuka tahansa voi verkosta ottaa käyttöönsä. Suurimmat ja tunnetuimmat julkisten pilvipalveluiden tarjoajat ovat Google, Microsoft ja Amazon. Yhteisöpilvi toimii muuten samanlaisesti kuin julkinen pilvi, mutta sen käyttö on rajattu vain tietyille kuluttajayhteisöille (esimerkiksi ammattikorkeakoulun henkilökunta ja oppilaat). Yksityisen pilven palvelut ja laitteistot ylläpidetään yksityisessä verkossa, esimerkiksi yrityksen sisäinen pilvipalvelu, jonka laitteisto sijaitsee yrityksen tiloissa. Tämä tyyppi on hyvä tietoturvallisuuden ja vapaan hallinnan kannalta, mutta vaatii yritykseltä paljon osaamista sekä ohjelmisto- ja laitteistohankintoja. Neljäs tyyppi on hybridipilvi, jossa käytetään kontrolloidusti yrityksen yksityistä pilveä, mutta tarvittaessa esimerkiksi ruuhka-aikaan toimintoja delegoidaan julkiseen pilveen sujuvan toiminnan takaamiseksi. (Laaksonen 2015.)

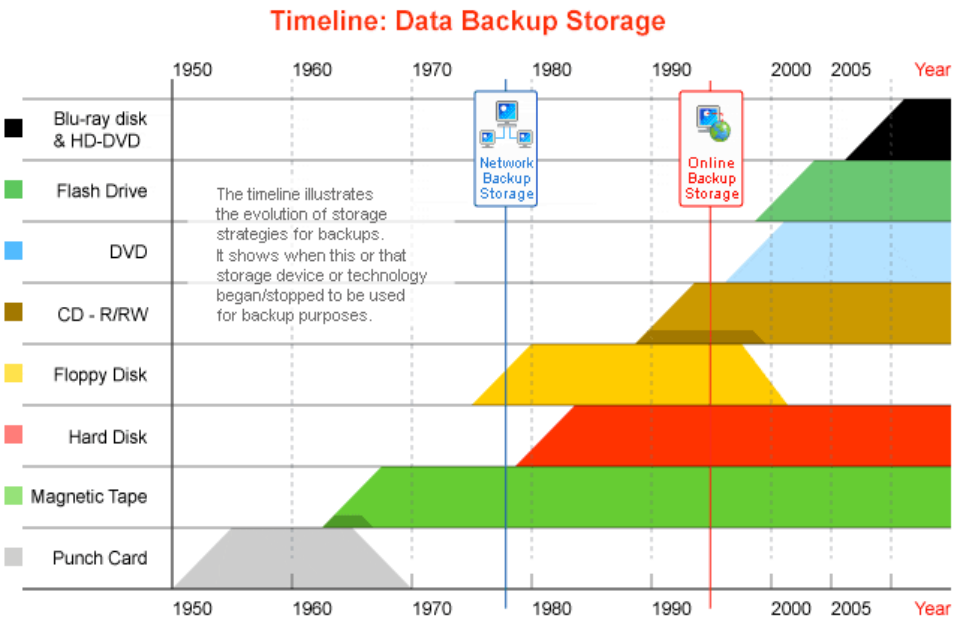
Kolme perinteistä palvelumallia pilvipalveluissa ja pilvilaskennassa ovat IaaS (Infrastructure as a Service), PaaS (Platform as a Service) ja SaaS (Software as a Service). IaaS-mallissa ulkoistetaan kokonaisia palvelinympäristöjä. Käytännössä palvelun tilaajalla on käytössä virtuaalinen laitteisto, joissa hän voi ajaa tarvitsemiansa käyttöjärjestelmiä ja ohjelmia. Malli vaatii käyttäjältä paljon osaamista, sillä palvelimien hallinnointi ja konfigurointi jäävät täysin käyttäjän vastuulle. PaaS-mallilla tarkoitetaan helposti käyttöön otettavan palvelualustan ulkoistamista pilvipalveluun. Malli laajentaa palveluntarjoajan vastuuta käyttöjärjestelmän ja ohjelmistojen hallinnointiin. Itse käyttäjän huolehdittavaksi jäävät ohjelmien päivitys ja niiden tietoturva. Esimerkiksi PaaS-alustalle luoduilla verkkosivuilla käytettävien julkaisujärjestelmiin liittyvät päivityksen ja tietoturvan ylläpito ovat käyttäjän vastuulla. SaaS-palveluissa palveluntarjoaja vastaa kokonaisvaltaisesti kuluttajalle tuotetusta ohjelmistosta, esimerkiksi sähköpostipalvelusta. Kyseisessä mallissa palvelun käyttäjälle jää vastuuta hyvin vähän, kun palvelun ylläpito ja siihen kuuluvat päivitykset ja lisenssit sisältyvät palvelun hintaan. Yritykselle ohjelmistojen ostaminen palveluna on helppoa ja edullista ottaen huomioon säästöt, jotka syntyvät palveluntarjoajan huolehtiessa ohjelmiston ylläpidosta. Pilvipalveluiden kolmen perusmallin ominaisuudet ja käyttötarkoitukset on koottu taulukossa 2. (Eronen 2016.)

Taulukko 2. Pilvipalveluiden kolme perusmallia (Lepistö 2016, 32).

	IaaS	**PaaS**	**SaaS**
Kenelle malli on suunnattu.	Ammattilaisille, kehittäjille.	Palvelunkehittäjille, ammattilaisille, ohjelmistokehittäjille.	Kenelle tahansa.
Käytön osaamistaso.	Vaatii paljon osaamista.	Suuri osaamistaso hyödyllinen.	Pieni, ei vaadi suurta osaamista.
Mitä malli tarjoaa.	Tarjoaa virtuaalisen laitteiston, jonka päälle käyttäjä voi rakentaa alustansa.	Palveluiden kehitysympäristön, palvelualustan ulkoistaminen.	Sovelluspalveluita, ilman kiinteää lisenssiä.
Kuka hallitsee resursseja.	Fyysisiä resursseja hallitsee palveluntarjoaja, muita resursseja käyttäjä.	Palveluntarjoaja, käyttäjä ei pysty vaikuttamaan laitteiston infrastruktuuriin. Käyttäjä hallitsee käytettäviä ohjelmistoja.	Palveluntarjoaja, käyttäjä ei pysty vaikuttamaan laitteiston infrastruktuuriin.
Järjestelmän ja resurssien muokattavuus.	Hyvä muokattavuus palveluntarjoajan ehdoin.	Muokattavuus palveluntarjoajan ehdoin.	Huono, infrastruktuuriin ei käyttäjä pysty vaikuttamaan.
Kenen vastuulla on tietoturva.	Käyttäjällä on vastuu tietoturvasta ja tarvittavasta yksityisyyden suojasta.	Tietoturva pääosin käyttäjän vastuulla.	Tietoturva pääosin palveluntarjoajan vastuulla.

2.6 Varmuuskopioinnin historia

Varmuuskopiointi on nykyään nopeasti kasvava aihealue, jonka varmistusmenetelmät ja -tekniikat muuttuvat koko ajan monimutkaisemmiksi. Perustason tieto varmuuskopioinnin historiasta on hyvä apuväline, jos haluaa kunnolla ymmärtää varmuuskopiointimenetelmiä, sen kehitystä ja siihen liittyvää laitteistoa ja ratkaisuja. (Yurin n.d.) Kuvassa 7 näkyvät käytetyt tallennusmediat aikajanalle sijoitettuna.



Kuva 7. Varmuuskopioinnin historia (Yurin n.d.).

Varmuuskopioinnin historian voidaan katsoa alkaneen noin 70 vuotta sitten, kun ensimmäinen kaupallisesti valmistettu tietokone UNIVAC I rakennettiin vuonna 1951. Tietokone käytti reikäkortteja tiedon tuomiseen ja ulkoiseen säilytykseen. Reikäkortti on neliskulmainen, yleensä kartongista valmistettu palanen, jossa on satoja lävistyskohtia tiedon ilmaisua varten. Tieto tallennetaan kortille tekemällä reiät sellaisiin kohtiin niin, että tietokoneen sitä lukiessa välittyy koneelle haluttu tieto. Toki kyseinen menetelmä oli hyvin alkeellinen, mutta se täytti varmuuskopioinnin kriteerit, koska ylimääräisiä kopioita reikäkorteista tehtiin ja säilytettiin alkuperäisen kortin katoamista varten. Reikäkortit olivat kuitenkin hitaita käyttää, niihin mahtui vain vähän tietoa ja tiedon lukeminen niistä vaati paljon työtä ja laitteita. (Yurin n.d.)

60-luvulla reikäkortit paikattiin magneettinauhalla, joka tarjosi paljon tehokkaamman tavan tallentaa tietoa. Yksi rulla magneettinauhaa saattoi sisältää jopa 10 000 reikäkortin verran tietoa ja siitä tuli suosituin tallennusmedia 80-luvun puoliväliin asti. Magneettinauhojen kehitys on jatkunut nykypäivään asti, ja erilaiset nauhaa käyttävät varmuuskopiointijärjestelmät ovat nykyäänkin suhteellisen yleisiä. (Yurin n.d.)

80-luvulla kuvaan astuivat kiintolevyt, jotka olivat jo 50-luvulta asti olleet kehityksen alla. Kiintolevy otettiin yleisesti käyttöön tietokoneissa sen helppokäyttöisyyden ja suuren tallennuskapasiteetin takia 90-luvulla, kun tekniikka oli kehittynyt kilpailukykyiseksi magneettinauhaa vastaan. Myös 90-luvun alussa kehitetyn RAID-tekniikan tuomat hyödyt auttoivat kiintolevyjä pysymään käytetyimpänä tallennusmediana. (Yurin n.d.)

80-luvun loppupuoliskolla levyke (Floppy Disk) nousi keskeiseksi tallennusmediaksi pienyritysten ja yksityiskäyttäjien käytössä. Tallennusvälineen levyke oli mullistava keksintö tietokoneiden välisessä tiedonsiirrossa. 90-luvulla CD-R/RW-levyjen hintojen laskeminen ja DVD-levyjen keksiminen aiheutti levykkeiden syrjäytymisen. Yksinkertainen syy tähän oli CD- ja DVD-levyjen paljon suuremmat tallennuskapasiteetit levykkeisiin verrattuna. Myöhemmin vuonna 2006 Blu-ray levyjen tuleminen markkinoille on auttanut optisten tallennusmedioiden olemassaoloa nykypäivään asti. (Yurin n.d.)

2000-luvun alussa markkinoille ilmestyivät Flash-muistiin perustuvat USB-muistitikut. Pienikokoisiin ja helppokäyttöisiin tikkuihin mahtui jo yhtä paljon tai enemmän tietoa, kuin optiselle tallennusvälineelle. Flash-muisti on kehittynyt hurjaa vauhtia ja nykyään erilaiset muistitikut ovatkin syrjäyttäneet lähes kokonaan optiset tallennusmediat etenkin yksityiskäytössä. Lisäksi Flash-muistiin perustuvat SSD-massamuistit valtaavat nykyään markkinoilta alaa pienen kokonsa, kestävyytensä ja suurien kirjoitus- ja lukunopeuksiensa ansiosta. Vaikka SSD-muistit tarjoavat useita etuja perinteiseen kiintolevyyn verrattuna, ovat ne varmuuskopiointiympäristöissä vielä varsin harvinaisia niiden pienemmän tallennuskapasiteetin ja siihen nähden suhteellisen korkean hinnan vuoksi. (Yurin n.d.)

3 TIETOTURVA

Luvussa käydään yleisellä tasolla läpi, mitä tietoturva on ja mitä se pitää sisällään. Lukijalle annetaan yleiskuva tietoturvan periaatteista ja siitä, miten varmuuskopiointi liittyy toimivan tietoturvajärjestelmän luontiin. Lisäksi luvussa esitellään tietoturvan osa-alueita, yleisimpiä tietoturvauhkia ja muutamia ajatuksia siitä, miten yksityishenkilö tai yritys voisi parantaa omaa tietoturvaansa.

3.1 Tietoturvasta lyhyesti

Tietoturva on nykypäivänä paljon keskusteltu aihe, kun yhä useammilla on käytössä internetyhteys, tietokoneita ja älylaitteita. Mediassa uutisoidaan tietomurroista tuon tuosta, mikä nostaa puheen tietoturvan puutteista ja tarpeellisuudesta ihmisten huulille.

Kaikissa tietokoneiden kanssa työskentelevissä yrityksissä tietoturva on tärkeässä roolissa. Nykyään tietoturvan olemassaoloa yritysmaailmassa voidaan pitää jo lähes itsestäänselvyytenä, koska melkein kiistatta kaikki liiketoimintaan liittyvä tieto tallennetaan ja kuljetetaan tavalla tai toisella tietokoneiden ja internetin avulla. Tietoturvalla tarkoitetaan järjestelmien, palveluiden ja tietoliikenteen suojaamista, riskien kartoittamista ja niihin varautumista sekä käytännön menetelmiä, joilla estetään luvatonta pääsyä käsiksi tietoon sen ollessa tallennettuna tai sitä siirrettäessä. Sillä pyritään poistamaan riski muun muassa tärkeiden tietojen väärinkäytöstä, kuten lukemisesta, muuttamisesta, paljastamisesta, tallentamisesta, häirinnästä ja tuhoamisesta. Lyhyesti sanottuna tietoturvalla suojataan paha-aikeisilta ulkopuolisilta tekijöiltä itse tietoa, laitteita ja järjestelmiä, jotka käsittelevät tietoa. (Rouse 2014a.)

Nykyään etenkin suuremmissa yrityksissä on yleistä, että organisaatiossa tehtävistä toimenpiteistä palkataan vastaamaan joukko asiantuntevia ja ammattitaitoisia tietoturvaihmisiä. Tyypillisesti tämä ryhmä on vastuussa riskienhallinnasta, jollaa järjestelmän heikkouksia ja uhkia kartoitetaan jatkuvasti sekä tarvittavien suojien päättämisestä ja toimeenpanosta. (Rouse 2014a.) Tietoturvan luontiprosessiin ja käytäntöön kuuluu yleisesti hallinnollisia, fyysisiä ja teknisiä toimenpiteitä, joilla tietoja pyritään suojaamaan aiemmin mainituilta riskitekijöiltä. Hallinnollisilla toimia käytetään organisaation tietoturvatoiminnan hallintaan ja määrittämään ihmisten osaa tietoturvasta. Esimerkiksi tietojen käsittelyyn asetetut standardit, toimintatavat ja henkilökunnan koulutukset tietoturvalliseen toimintaan ovat hallinnollisia toimia tietoturvassa. Fyysiset toimet on tarkoitettu hallitsemaan fyysistä pääsyä käsiksi tietoon. Näitä voivat olla esimerkiksi palvelimen sijoittaminen useiden lukittujen ovien taakse, hälytysjärjestelmät ja kameravalvonta. Ikävä fakta on, ettei ole mitään väliä miten hyvin tietoturva on tekniseltä puoleltaan rakennettu, jos joku voi helposti varastaa fyysisen

palvelintietokoneen. Yleinen käsitys on, että tietoturva koostuu kokonaan tai ainakin suurimmaksi osaksi tietoteknisistä asioista, vaikka todellisuudessa tekninen hallinta on vain osa suurta kokonaisuutta. Tietoturvan tekninen osuus koostuu esimerkiksi palomuureista, virustorjuntaohjelmista, tiedon salausmenetelmistä sekä salasanoista ja tietojen luku- ja kirjoitusoikeuksia määrittävistä ryhmäkäytännöistä eli käyttöoikeuksista. Lisäksi kokonaisuuden ylläpitämiseksi voidaan tehdä yrityksen sisäisiä turvallisuustarkastuksia, joilla voidaan arvioida organisaation kykyä pitää järjestelmät turvallisina vakiintuneita riskejä vastaan. (Francen 2015.) Tietoturvan osa-alueista kerrotaan lisää myöhemmin Tietoturvan osa-alueet -luvussa.

3.2 Tietoturvan periaatteet

Tietoturvallisuus voidaan jakaa kolmeen periaatteeseen: tiedon luottamuksellisuus (Confidentiality), eheyden säilyttäminen (Integrity) ja käytettävyys (Availability). Nämä yhdessä muodostavat niin sanotun CIA-kolmion (Kuva 8), jota tietoturvallisuudessa pyritään toteuttamaan tasapainoisesti niin, että se vaikuttaisi mahdollisimman vähän yritysorganisaation tuottavuuteen ja toimintakykyyn. Optimitilanteessa kaikki kolme periaatetta toteutuvat. Toteutuksen onnistuminen vaatii kuitenkin paljon suunnittelua ja yleensä sen eteen joudutaan tekemään kompromisseja tietoverkossa. (Rouse 2014a.)

Kuva 8. CIA-kolmio (OpenText n.d.).

Luottamuksellisuus tarkoittaa sitä, että tietoa voivat käsitellä vai sellaiset tahot, joille siihen on annettu oikeus. Toisin sanottuna tärkeiden tietojen saatavuutta rajoitetaan. Luottamuksellisuutta voidaan parantaa tekemällä

organisaation sisäiset selkeät jaot, kenelle ja mitä oikeuksia mihinkin tietoon annetaan. Tietojen hallinnoitsijoiden määrä tulisi pitää pienenä, ja näiden työntekijöiden olla ammattitaitoisia ja luotettavia. Tallennettavan tiedon luottamuksellisuutta voidaan edistää myös salaamalla eli kryptaamalla, jotta tärkeitä tietoja pystyvät lukemaan vain valtuutetut osapuolet. Lisäksi organisaatiossa työskentelevien olisi suositeltavaa käyttää yhä monimutkaisempia salasanoja. Tämän on tarkoitus vähentää tietoon kohdistuvia riskejä, jotka voivat vaarantaa tietoturvan, kuten tiedon joutuminen vääriin käsiin. Tietomurtojen yleistyessä luottamuksellisuuden merkitys tietoturvassa on noussut hyvin tärkeäksi. (Rouse 2014a.)

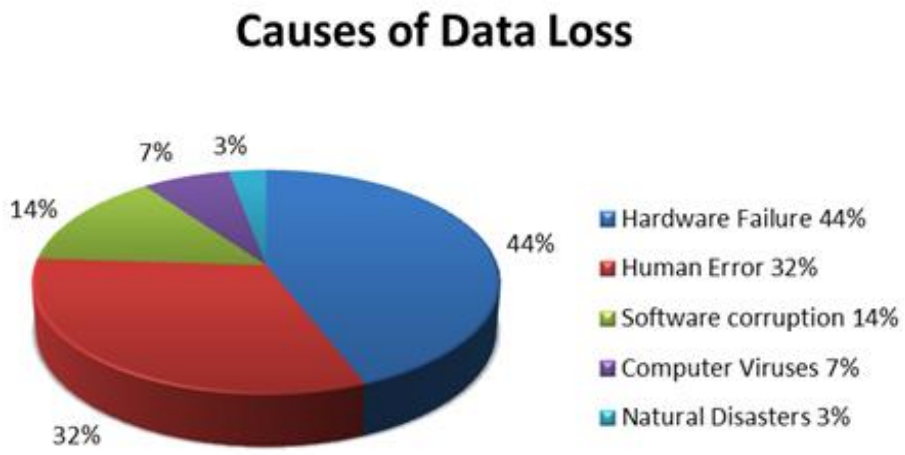
Tiedon eheydellä tarkoitetaan, että suojattavien tietojen ja järjestelmien pitää olla luotettavia, vioittumattomia ja ajan tasalla. Ne eivät saa muuttua laitteisto- tai ohjelmistovian tapahtuessa, eikä inhimillinen ilkivalta tai virhe pysty niihin vaikuttamaan. Esimerkiksi tietokonevirukset ja vioittuneiden tallennusmedioiden käyttö ovat yleisiä riskejä tiedon eheyden säilyvyyden kannalta. Tiedon eheyden säilyvyyteen voidaan vaikuttaa päivittämällä käytössä olevia ohjelmistoja ja laitteita usein, varmuuskopioimalla tiedot ajantasaisesti ja automatisoimalla tiedon kirjoittamista ja tallentamista mahdollisimman paljon, mikä vähentää inhimillisen virheen riskiä. Toki automatisoidessakin koneessa voi tapahtua virhe ja tiedot jäävät kirjoittamatta kokonaan. Joskus on kuitenkin parempi, että tietoa ei ole ollenkaan kuin että tallennettuna olisi väärää tietoa. Kukaan ei halua tehdä liike-elämän tärkeitä valintoja väärien tietojen pohjalta. (Affirma Consulting 2018.)

Käytettävyys voidaan kiteyttää yhteen lauseeseen: tieto on saatavilla, kun sitä tarvitaan. Tiedon käytettävyyden voi varmistaa huolellisesti ylläpitämällä laitteistoa ja käyttöjärjestelmiä, sekä varmistamalla että tiedon siirtoa ja tallentamista varten on käytössä tarpeeksi kaistaa. Käytännössä kaikki korjaustoimenpiteet laitteistolle suoritetaan välittömästi, käyttöjärjestelmät pidetään päivitettyinä, eikä niissä tapahdu ohjelmistovirheitä ja tieto kulkee yrityksen tietoverkossa sujuvaa vauhtia. Tiedon käytettävyyteen liittyvät riskit koostuvat tietoteknisistä ja fyysisistä tapaturmista, kuten ohjelmistovirhe, tietokonevirus, ilkivalta, tulipalo, vesivahinko ja virtapiikki. Tämän vuoksi ehdottomasti tärkein asia tiedon käytettävyyden takaamisen kannalta on luotettava varmuuskopiointijärjestelmä. (Rouse 2014a.)

3.3 **Varmuuskopiointi osana tietoturvaa**

Kuten aiemmin todettiin, voidaan tietoturva jakaa kolmeen periaatteeseen: tiedon eheyden säilyttämiseen, käytettävyyteen ja luottamuksellisuuteen. Jotta riittävän hyvä tietoturva voidaan toteuttaa, tarvitaan toimiva ja luotettava varmuuskopiointijärjestelmä. Varmuuskopiointi liittyy kaikkiin edellä mainittuihin tietoturvan periaatteisiin. Vahvimmin var-

muuskopioinnin tärkeys tulee esiin tiedon eheyden säilyttämisen ja käytettävyyden kohdalla. Hyvin toimivalla ja ylläpidetyllä varmuuskopiointijärjestelmällä voidaan luottaa siihen, että tiedot ovat aina vioittumattomia ja tarvittaessa saatavilla, vaikka sattuisikin tietotekninen tai fyysinen vahinko. Toki tietojen menettäminen vahingon myötä aiheuttaa vaivaa, kun tietoja joudutaan alkamaan siirtämään takaisin varmuuskopiointisijainnista, mutta haittavaikutus ei ole läheskään niin suuri, kuin mitä se voisi olla kunnollisen varmuuskopiointijärjestelmän puuttuessa. Äärimmäistapauksessa toimiva varmuuskopiointijärjestelmä voi pelastaa koko yritystoiminnan. Kuvassa 9 näkyy ympyrädiagrammina yleisimmät syyt tiedon menetykseen. Niin kauan, kun laite johon varmuuskopiotiedostot ja tallennusmediamedia, johon ne ovat tallennettuna, pysyvät vioittumattomina, voi tietojen varmuuskopiointi pelastaa yrityksen kaikilta näiltä syiltä. (Devery 2015.)



Kuva 9. Tiedon katoamisen syyt (Devery 2015).

Varmuuskopioitaessa tieto saattaa sirpaloitua, mikä voi pahimmassa tapauksessa estää kokonaan tiedon palauttamisen ja on iso uhka tietojen eheydelle. Järjestelmällinen tietojen eheyden tarkistaminen esimerkiksi varmuuskopioinnin ohella luoduista lokitiedostoista, on tehokas tapa vähentää tiedon sirpaloitumiseen liittyvää riskiä. Mitä aikaisemmassa vaiheessa vioittunut tai kokonaan puuttuva varmuuskopioitu tieto huomataan, sitä paremmalla todennäköisyydellä ja pienemmällä vaivalla tilanne pystytään korjaamaan. (Riihimäki 2010.)

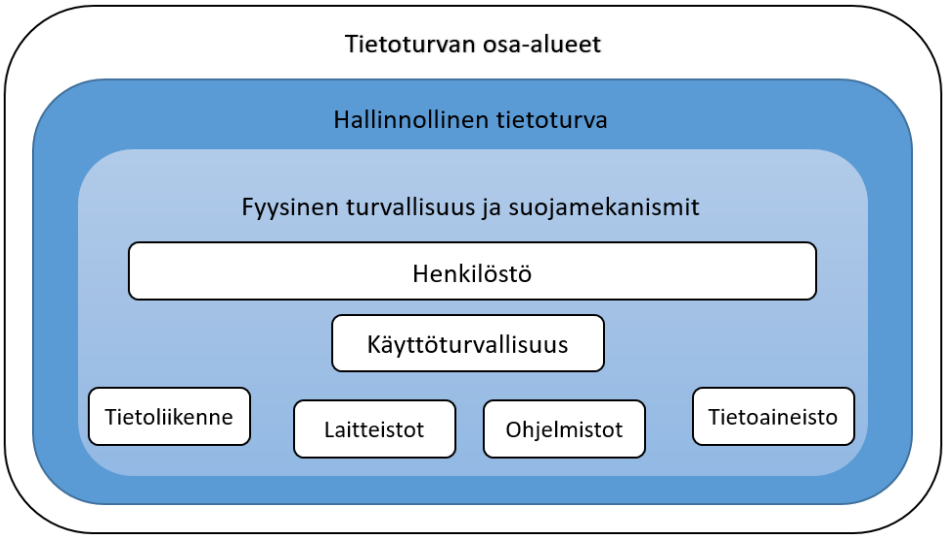
Tietojen saatavuus on varmuuskopioinnin toimivuuden kannalta itsestäänselvyys. Tieto voidaan tallentaa useille erilaisille laitteille, kuten USB-muistitikulle, paikalliselle tai etäpalvelimelle, NAS-verkkolevylle, nauha-asemalle tai ulkoiselle kiintolevylle. Tallennusmediasta riippumatta tiedon on oltava tarvittaessa saatavilla, jotta varmuuskopioinnista ylipää-

tänsä on käyttäjälle hyötyä. Varmuuskopioituja tietoja palautettaessa varmuuskopioita säilyttävän laitteen on oltava saatavilla tarpeeksi suurien tiedonsiirtonopeuksien päässä, jotta tiedon palauttaminen voidaan tarvittaessa tehdä lyhyellä varoitusajalla ja nopeasti. (Bourgeois 2014.)

Varmuuskopiointijärjestelmää mietittäessä täytyy ottaa huomioon myös tiedon luottamuksellisuus. On tärkeää, että vain tarkoin valitulla henkilöstöllä on pääsy paikkaan, missä varmuuskopioita säilytetään niin digitaalisesti kuin fyysisesti. Esimerkiksi etäpalvelimen verkko-osoitteet ja mahdollisesti fyysinen sijainti olisi tiedossa vain niillä työntekijöillä, jotka tarvitsevat varmuuskopioitua tietoa työnsä puolesta. Näin pystytään karsimaan suuri määrä varmuuskopioihin kohdistuvista ilkivallan riskeistä. Automatisoidun varmuuskopioinnin valvontaan voidaan määrätä luotettavia ja ammattitaitoisia työntekijöitä, jotka käyvät läpi varmuuskopioita tehtäessä syntyneet lokitiedostot ja varmistavat, ettei tietojen kopioinnissa ole tapahtunut virheitä. (Bourgeois 2014.)

3.4 Tietoturvan osa-alueet

Tietoturva on laaja alue, joka voidaan jakaa useaan pienempään osa-alueeseen. Yleisesti tietoturvan osa-alueita katsotaan olevan hallinnollinen ja fyysinen tietoturva, henkilöstöturvallisuus, käyttöturvallisuus, tietoliikenneturvallisuus, laitteistoturvallisuus, ohjelmistoturvallisuus ja tietoaineistoturvallisuus. Perinteisen jaottelun mukaan hallinnolliset ja fyysiset toimenpiteet luovat pohjan muiden osa-alueiden toteuttamiselle. Laitteistojen, tietoliikenteen, ohjelmistojen ja tietoaineiston turvallisesta käytöstä ovat vastuussa itse yrityksen työntekijät. Kuvassa 10 tietoturvan osa-alueet on esitetty perinteisellä tavalla. (Laakso 2010.)



Kuva 10. Tietoturvan perinteinen jaottelu.

Tietoturvaan liittyvät toimintatavat vaativat kehittämistä ja johtamista yhtä lailla, kuin muutkin yritystoimintaan liittyvät metodit. Hallinnolliseen tietoturvaan kuuluvat menettelytavat, joilla ohjataan muita tietoturvan osa-alueita ja varmistetaan että ne ovat riittävän hyvällä tasolla. Käytännössä hallinnollisia toimia voivat olla henkilöstön organisointi ja koulutus tietoturvalliseen toimintaan sekä tietoturvapolitiikkaan liittyvät linjaukset ja dokumentit. Tietoturvan hallinnollisen osan onnistuminen vaatii yrityksen johdolta osallistumista ja vastuualueiden järjestelmällistä jakamista. (Laakso 2010.)

Fyysisellä turvallisuudella tarkoitetaan yrityksen tiloja ja niissä olevien laitteiden suojaamista. Se on tarkoitettu hallitsemaan fyysistä tietoihin käsiksi pääsyä esimerkiksi sijoittamalla yrityksen palvelintietokone lukittuun tilaan ja asentamalla kamera- ja hälytysjärjestelmiä. Minkään tiedon turvallisuutta ei voida varmistaa, jos sen säilytyspaikkaa ei ole fyysisesti turvattu. Fyysisiä turvallisuusriskejä voivat olla palo-, vesi- ja sähkövahingot sekä inhimilliset uhat, kuten ilkivalta ja varkaus. Yrityksen koosta ja tietotekniikasta riippuvaisuuden mukaan fyysistä turvaa sovelletaan joko kokonaisvaltaisesti tai enemmän keskitetysti, vaikka palvelinhuoneen turvaamisessa. (Laakso 2010.)

Työntekijöiden toimintatavat ja käytännöt ovat suuri osa kokonaisvaltaista tietoturvallisuutta. Henkilöstön tulee olla tietoinen siitä, miten työskennellä tietoturvallisesti esimerkiksi tunnistamalla ja välttämällä haittaohjelman sellaiseen törmätessä. Tietoturvaosaamisen vaatimustasot vaihtelevat työtehtävistä riippuen, joten toimiva henkilöstöturvallisuus on vahvasti riippuvainen hyvin toteutetusta hallinnollisesta tietoturvasta ja etenkin siihen kuuluvista henkilöstökoulutuksista tietoturvallisuuteen liittyen. Erityisen kriittisiä hetkiä yritystoiminnassa henkilöstöturvallisuuden kannalta ovat työntekijän palkkaaminen ja irtisanominen. Johdon on suositeltavaa käydä läpi työtä hakevan henkilön taustat tarkasti riippuen siitä, millaiseen työtehtävään häntä ollaan palkkaamassa. Myös henkilöstön irtisanomistilanteessa on pidettävä huoli, että kyseinen työntekijä suljetaan täysin ulos yrityksen tietojärjestelmistä. Näin suljetaan pois riski siitä, että irtisanottu voisi työssä ollessaan saaduilla tiedoilla, esimerkiksi yrityksen käyttämillä salasanoilla, aiheuttaa katkeruuksissaan vahinkoa yritykselle. (Laakso 2010.)

Yleensä eritellään omaksi osa-alueeksi vielä käyttöturvallisuus, joka pitää sisällään organisaation rutiinien ja jokapäiväisten toimintojen turvaamisen. Tietojenkäsittelyn manuaaliset ja automaattiset suojatoimenpiteet, kuten salasanakäytäntöjen hallinnointi ja järjestelmien valvonta ovat osa käyttöturvallisuutta. Lisäksi käyttöturvallisuuteen voi kuulua turvallinen etätyöskentely, esimerkiksi käyttämällä VPN-yhteyksiä (Virtual Private Network). Joissain tapauksissa käyttöturvallisuus yhdistetään osaksi muita tietoturvan osa-alueita, niiden samanlaisten luonteiden vuoksi. (Laakso 2010.)

Tietoliikenneturvallisuudella tarkoitetaan laitteita ja käytäntöjä, joilla suojataan yrityksen tietoverkossa liikkuvan datan luottamuksellisuus, eheys ja käytettävyys. Aihealue on erittäin suuri ja siksi tietoliikenteen turvaamiseksi on olemassa paljon fyysisiä ja teknisiä tapoja. Yksi yleisimmistä tietoliikenneyhteyksistä yrityskäytössä on internet. Internetyhteyden käyttömenetelmät vaihtelevat yrityksen koon ja siten tarpeiden mukaan matkapuhelinyhteyksistä aina valokuituyhteyksien välillä. Tietoliikenneverkon rakenteen mukaan niiden tietoturvaa voidaan salasanasuojauksien lisäksi parantaa erilaisilla laitteilla, kuten reitittimillä, kytkimillä ja palomuureilla. Yleinen käytäntö yrityksissä on nimetä, kouluttaa tai palkata tietoliikenneturvallisuudesta vastaavat työntekijät, joilla on tarvittava asiantuntemus aiheeseen liittyen. (Laakso 2010.)

Nykyään lähes jokaisella yrityksellä on käytössä enemmän tai vähemmän teknisiä laitteita, kuten tietokoneita, matkapuhelimia, tulostimia ja palvelimia. Näiden laitteiden suojaamista kutsutaan laitteistoturvallisuudeksi. Kuten kaikissa muissakin tietoturvan osa-alueissa, suojattavien laitteiden, niiden komponenttien ja niihin kohdistuvien suojaustoimien tarkka dokumentointi on tärkeää, jotta vikatilanteessa ongelman selvittäminen olisi mahdollisimman nopeaa ja selkeää. Inventaario käytettävistä laitteista on hyvä lähtökohta laitteistoturvallisuuden suunnittelulle. Esimerkiksi työn kannalta tarpeeton työntekijöiden omien laitteiden käyttäminen yrityksen verkossa luo tietoturvariskin, koska henkilökohtaisia laitteita ei valvota ja suojata samalla tavalla kuin yrityksen omia ja ne saattavat sisältää haittaohjelmia. Laitteiden huoltaminen ja ohjelmistojen säännöllinen päivittäminen ovat tehokas tapa välttyä suurelta määrältä turvallisuusriskejä. (Laakso 2010.)

Myös yrityksen käytössä olevien ohjelmistojen turvallisuus täytyy suojata. Työkoneissa ja palvelimissa käytettävien ohjelmistojen ja lisenssien hallinta muodostavat ohjelmistoturvallisuuden. Työntekijöille on hyvä luoda selkeät ohjeet, mitä ohjelmia työympäristössä on sallittua käyttää, joten käyttöturvallisuus kulkee tiukasti käsi kädessä ohjelmistoturvallisuuden kanssa. Ohjelmistoihin liittyviltä turvallisuusuhilta, kuten viruksilta ja haittaohjelmilta voidaan välttyä pitämällä ohjelmistolisenssit voimassaolevina. Esimerkiksi virustorjuntaohjelman lisenssin loppuminen aiheuttaa vaarallisen tietoturva-aukon yrityksen tietojärjestelmään. On myös tärkeää valita käytettävät ohjelmat huolella ja varmistaa, että ne ovat laadukkaita ja tietoturvallisia. Useista ilmaisohjelmista voi kokonaan puuttua käyttäjän todennus, jolloin ohjelmia voi päästä käyttämään käytännössä kuka tahansa. Vikatilanteiden välttämiseksi ja niiden varalta ohjelmistot tulee päivittää järjestelmällisesti ja esimerkiksi niissä käytettävät projektitiedostot varmuuskopioida säännöllisin aikavälein. (Laakso 2010.)

Tietoaineiston turvallisuuden tarkoitus on suojata itse tietojen suojaaminen. Toimenpiteitä tämän tavoitteen saavuttamiseksi ovat esimerkiksi tietojen varmuuskopiointi ja palauttaminen sekä turvallinen säilyttäminen ja tuhoaminen. Tietoaineiston turvallisuuden rakentaminen alkumetreillä on

suositeltavaa luokitella yrityksen käyttämät tiedot. Yleinen tapa on jakaa tiedot kolmeen tai neljään luokkaan. Näitä voivat olla julkiset, sisäiset, luottamukselliset ja salaiset tiedot. Näin pystytään paremmin priorisoimaan turvallisuutta tärkeisiin tietoihin, kuten henkilötietoihin ja liiketoimintaan liittyviin tietoihin. Työntekijöiden oikeaoppinen tiedon käsittely ja säilyttäminen tarvitsevat yrityksen johdolta ohjeistusta. Esimerkiksi valtiovarainministeriö on koonnut verkkosivuilleen kattavat VAHTI-tietoturvaohjeet, joita yrityksessä voidaan soveltaa. Tietoaineiston turvallisuus tulee pitää mielessä tietoja hävitettäessäkin, jotta arkaluontoista materiaalia ei jää vahingossa jäljelle ulkopuolisten luettavaksi. Turvallinen hävittäminen pätee sekä sähköisiin että fyysisiin tietoihin, kuten paperidokumentteihin. Fyysiset dokumentit on suositeltavaa tuhota käyttämällä paperisilppuria. Sähköisten dokumenttien tuhoamisessa pelkkä tiedoston poistaminen tallennusmediasta ei riitä. Sen sijaan itse tallennusmedian tuhoaminen fyysisesti niin, ettei siitä voida tietoa enää lukea tai tiedon ylikirjoittamiseen kehitettyjen sovellusten käyttö ovat turvallisempia keinoja sähköisen tiedon hävittämiseen. (Laakso 2010.)

3.5 **Tietoturvan uhat**

Tekniikka on kehittynyt ja sen käyttäminen yleistynyt valtavasti niin yrityskuin yksityiskäytössä. Tietokoneiden, älylaitteiden ja niillä käsiteltävän tiedon määrän kasvaessa myös niihin kohdistuvia uhkia kehitellään enemmän. Tämän johdosta tietoturvan merkitys nousee tuon tuosta jopa valtamedian otsikoihin. Osion on tarkoitus avata lukijalle yleisimpiä tietoturvauhkia ja keinoja, joilla niiden luomaa riskiä voidaan vähentää tai suojautua kokonaan.

Tietoturvauhka on tekijä, joka aiheuttaa vaaran yhdelle tai useammalle tietoturvan osa-alueelle. Muita aiheeseen liittyviä termejä ovat haavoittuvuus, joka tarkoittaa esimerkiksi tietoturvaan liittyvien laitteiden ja järjestelmien alttiutta tietoturvauhille, ja tietoturvariski, jolla tarkoitetaan tietoturvauhkien toteutumisen todennäköisyyttä. Tietoturvallisen haavoittuvuuden voi aiheuttaa heikkolaatuisten ilmaisohjelmien käyttäminen tai ohjelmistojen päivittämättä jättäminen. Suuri riski tietoturvalle on itse tietokoneen tai älylaitteen käyttäjän inhimilliset virheet. Tiedon tahaton muuttaminen tai poistaminen ja esimerkiksi salasanojen huoleton säilyttäminen tai jakaminen ovat yleisiä käyttäjän aiheuttamia tietoturvariskejä. Siksi erityisen tärkeää on huolehtia työntekijöiden kouluttamisesta tietoturvalliseen käyttäytymiseen ja työskentelyyn yrityksen tietoympäristössä. (Jyväskylän Yliopisto 2010.)

Nykyään on olemassa lukuisia tietoturvauhkia, joista tyypillisimpiä ovat haittaohjelmat, kuten virukset, madot, troijalaiset, kiristysohjelmat ja näppäilyn tallentajalaitteet tai -ohjelmat. Haittaohjelma on yleensä rikolliseen tarkoitukseen rakennettu ohjelma, jolla pyritään aiheuttamaan vahinkoa tietojärjestelmille, ohjelmistoille ja laitteistoille. Yleensä niiden tavoitteena

on saada suoraan rahallista hyötyä esimerkiksi kiristämällä tai kerätä haltuun salaisia tietoja, kuten salasanaoja tai käyttäjätunnuksia. Klassisia haittaohjelmien levittämistapoja on kolme. Ne voivat levitä tietokoneelle internetistä tehtyjen tiedostolatausten yhteydessä, sähköpostin mukana tulevien liitteiden kanssa tai irrotettavassa tallennuslaitteessa, kuten muistitikussa. Lisäksi kaikki tietoverkkoon kytkettynä olevat tietokoneet ovat alttiina haittaohjelmalle, jos yksi koneista on sellaiselle altistunut. Tehokas keino haittaohjelmien torjumiseen on ajan tasalla oleva virustorjuntaohjelmisto, joka mahdollistaa tietokonevirustartunnan torjumisen kokonaan tai ainakin huomaa tartunnan aikaisessa vaiheessa, jolloin suuremmilta vahingoilta pystytään välttymään. (AllBusiness n.d.)

Mitä aikaisemmassa vaiheessa uhka huomataan ja pystytään paikantamaan, sitä pienempi riski suuriin vahinkoihin on. ”Esimerkiksi haittaohjelma pääsee yrityksen järjestelmään ja työasemalle. Tämä työasema synkronoidaan tiedostopalvelimen kanssa, joten kyseinen haittaohjelma pääsee leviämään myös palvelimelle. Tämä tiedostopalvelin varmuuskopioidaan ja nyt haittaohjelma leviää myös varmuuskopioon. Vaikka haittaohjelma saataisiin poistettua yrityksen järjestelmästä, on se tässä tapauksessa myös varmuuskopioissa ja voi täten levitä tiedostonpalautuksen yhteydessä uudestaan yrityksen järjestelmään.” (Lepistö 2016, 12).

Haittaohjelmien lisäksi myös tietomurrot ovat todellinen uhka tietoturvalle. Tietomurrolla tarkoitetaan toimenpidettä, jossa ulkopuolinen tekijä murtautuu tietokoneelle joko paikallisesti tai yleisemmin verkon yli. Yleistä on, että suojauksen murtamisessa käytetään apuna erilaisia haittaohjelmia. Tietomurrolla on yleensä tarkoitus saada haltuun suojattuja arkaluontoisia ja luottamuksellisia tiedostoja tai henkilökohtaisia tietoja, kuten salasanoja ja luottokorttitietoja, ja niiden väärinkäyttäminen. Yleinen mielikuva tietomurrosta on hakkeri, joka murtautuu yrityksen tietoverkkoon ja varastaa sieltä haltuunsa salaista tietoa. Käsitteenä tietomurto ei ole kuitenkaan aivan näin mustavalkoinen. Esimerkiksi jos sairaalan työntekijä vilkuilee luvatta potilaan terveystietoja tietokoneen näytöltä valtuutetun työntekijän olan yli, voidaan katsoa tietomurron kriteerien täyttyneen. (Rouse 2017.)

Alttiutta tietomurrolle edistävät esimerkiksi heikot salasanat, puuttuvat ohjelmistopäivitykset ja varastetut tietokoneet ja mobiililaitteet. Jos käyttäjän yhdistää laitteen väärennettyyn verkkoon, joka tallentaa verkossa käytetyt kirjautumistiedot ja muut arkaluontoiset tiedot, hän voi myös altistaa tiedot luvattomalle ulkopuoliselle taholle. Yhtä tiettyä tuotetta tai toimea tietomurtojen estämiselle ei ole olemassa. Maalaisjärjen käyttö tietokonetta tai älylaitetta käytettäessä sekä henkilökunnan kouluttaminen tietoturvan perusteisiin ovat parhaita tapoja vähentää tietomurron riskiä. Yrityksessä voidaan suorittaa myös säännöllisin ajoin järjestelmän haavoittuvuustestejä, käyttää tehokasta ja luotettavaa virustorjuntaohjelmistoa, käyttää vahvoja salasanoja ja vaihtaa niitä jatkuvasti, salata luottamukselliset tiedot sekä pitää järjestelmissä käytettävät ohjelmistot päivitettyinä.

(Rouse 2017.) Ohessa Toni Lepistön kandidaatintyöstä lainattu taulukko hyvistä keinoista, joilla tietoturvariskejä voidaan vähentää.

Taulukko 3. Keinoja tietoturvan parantamiseksi (Lepistö 2016, 20).

Parantamiskeino	**Selite ja lisätietoa**
Käytä vahvaa salasanaa.	Vahva salasana sisältää vähintään 8 merkkiä ja siinä käytetään suuria ja pieniä kirjaimia, numeroita sekä erikoismerkkejä sekaisin.
Vaihda salasana määräajoin.	Salasanan vaihto määräajoin estää ja vaikeuttaa salasanan vakoilua. Vaihto voi tapahtua esimerkiksi kerran kuukaudessa.
Käytä tietojen salausta.	Tietokoneen kovalevyn salauksen käyttö suojaa tietoja mahdollisten tietomurtojen tapahtuessa sekä oikein käytettynä estää arkaluontoisten ja yksityisten tietojen joutumisen ulkopuolisille.
Tiedostojen allekirjoitus.	Tiedostojen allekirjoitus tapahtuu usein avainparilla eli julkisella ja yksityisellä avaimella, jolloin tiedoston alkuperä voidaan todentaa.
Käytä salattua tietoliikenneyhteyttä aina kun mahdollista.	Salatulla tietoliikenneyhteydellä, kuten SSH (Secure Shell) ja SSL (Secure Sockets Layer) avulla voidaan suojata tietoliikennettä vakoilua vastaan. SSH mahdollistaa salatun yhteyden esimerkiksi kotikoneelta yrityksen koneelle. SSL on internet sovellusten salausprotokolla.
Pidä ohjelmistot päivitettyinä.	Ohjelmistojen päivitys ja pitäminen ajan tasalla estää ohjelmien haavoittuvuuksien käyttämistä, sillä päivityksillä pyritään korjaamaan mahdollisia haavoittuvuuksia.
Käytä virustentorjuntaohjelmaa ja pidä se päivitettynä.	Virustorjuntaohjelman käyttö estää haittaohjelmien leviämistä.
Käytä palomuuria.	Palomuurin käyttäminen auttaa estämään haittaohjelmien leviämisen ja estää epätoivottuja verkon murtautumisyrityksiä.
Älä avaa tuntemattomia sähköpostiliitteitä.	Tuntemattomien sähköpostiliitteiden avaaminen mahdollistaa erilaisten huijauksien sekä haittaohjelmien leviämisen.

4 STUDIO C3

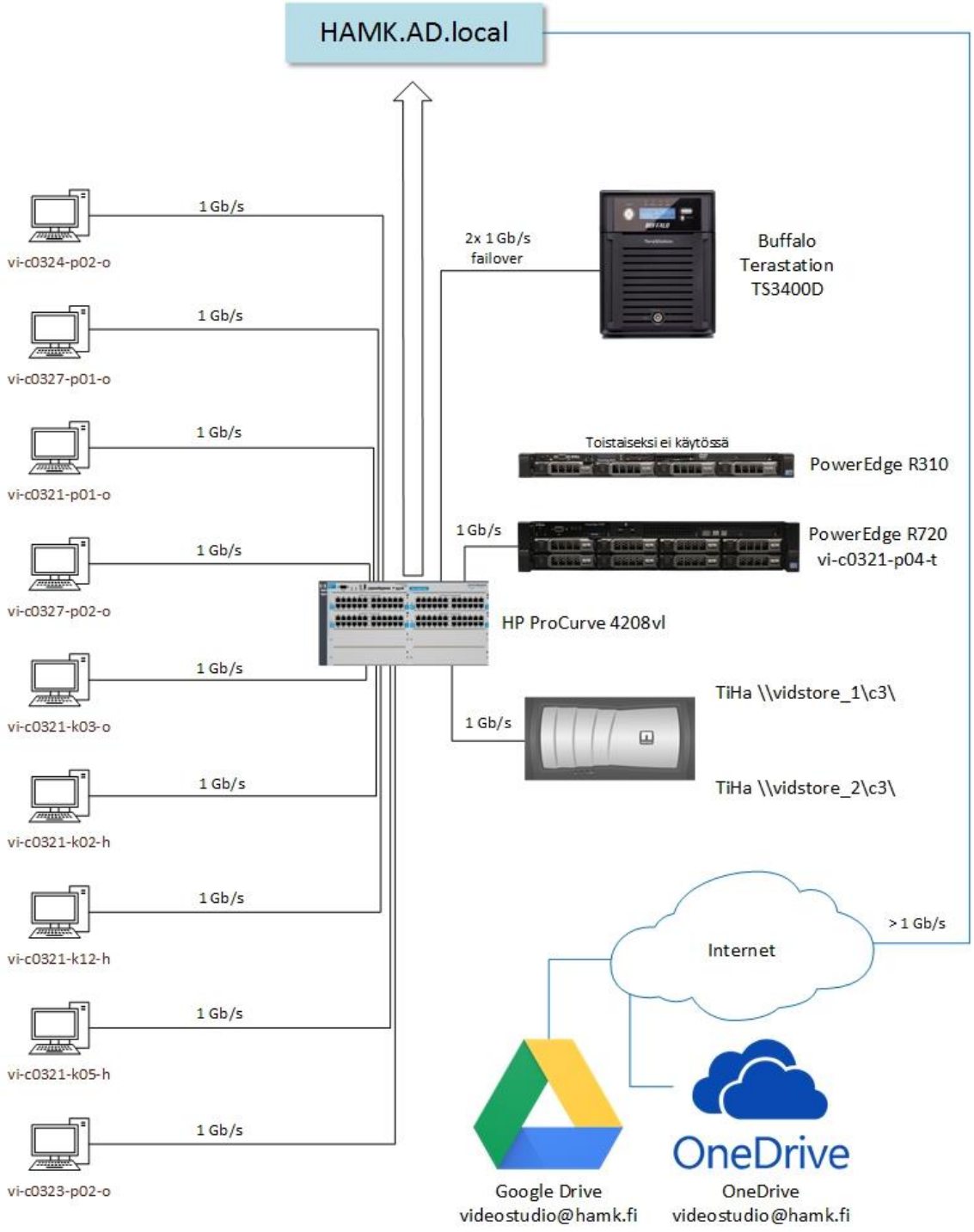
Tässä luvussa käsitellään opinnäytetyön toimeksiantajan Studio C3:n jo olemassa olevaa lähiverkkoa. Yrityksen toimitilat sijaitsevat Hämeen ammattikorkeakoulun Visamäen kampuksen C-rakennuksessa. Aiheen tiimoilta käydään läpi tiedon siirtoon ja tallentamiseen liittyviä ohjelmistoja ja laitteistoja. Laitteita ja niiden välisiä yhteyksiä avataan Microsoft Visio -vuokaaviolla. Tarkoituksena on kartoittaa lähtökohdat, joiden pohjalle opinnäytetyön varsinaista varmuuskopiointia ja tiedonsiirtojärjestelmää aletaan suunnitella.

Studio C3:n toimitiloissa sijaitsevat tietokoneet ja muut laitteet ovat yhteydessä yhteen Hewlett-Packard ProCurve 4208vl -kytkimeen ja ovat sitä kautta osa Hämeen ammattikorkeakoulun lähiverkkoa. Yrityksen lähiverkko koostuu yhdeksästä työasemasta, joista neljä ovat kannettavia tietokoneita ja viisi pöytäkoneita. Kaikkiin työasemiin on asennettu Microsoft Windows 10 –käyttöjärjestelmä ja lähes kaikkiin Adoben Creative Cloud -paketti, jonka sisältämät sovellukset, kuten Adobe Photoshop, Audition ja Premiere ovat keskeinen osa multimediatoimiston työtä.

Toimitiloissa lukitun oven takana olevassa palvelinhuoneessa sijaitsevat Dell PowerEdge R310 ja R720 -räkkipalvelimet, joista vain jälkimmäinen on toistaiseksi aktiivisesti käytössä. R720 -palvelinkoneeseen on asennettu Windows 10 käyttöjärjestelmä sekä kuusi 4 Tt kiintolevyä, jotka toimivat RAID 0:ssa ja yhdessä lomitettuina muodostavat noin 22 teratavun tallennuskapasiteetin. Kaikki työasemat ja palvelin ovat yhteydessä lähiverkkoon 1 Gb/s nopeuksisilla Ethernet kaapeleilla. Palvelinhuoneessa toimii myös Buffalo Terastation TS3400D -verkkolevypalvelin. Verkkolevy on yhdistetty lähiverkkoon kahdella 1 Gb/s Ethernet-kaapelilla, joista toinen kaapeli toimii ”failoverina”. Käytännössä siis yhteyden nopeus on 1 Gb/s, mutta toisen kaapelin vaurioituessa tiedon siirtäminen voi jatkua normaalisti käyttäen toista kaapelia. Yrityksen toimitiloissa sijaitsevien laitteiden lisäksi Studio C3:lla on käytössä HAMKin tietohallinnon palvelintiloissa toimiva NetApp-levyjärjestelmä, josta Studio C3:n käyttöön on hajautettu kaksi 10 Tt osiota tiedon tallennusta varten.

Pilvipalveluista yrityksen aktiivisessa käytössä ovat Microsoft OneDrive ja Google Drive. Pilvipalveluiden pääasiallinen tehtävä on varmuuskopioiden säilytys sekä helpon ja käytännöllisen tiedostojen siirron mahdollistaminen yrityksen ja HAMKin ulkopuolisten asiakkaiden välillä. Aikaisemmin yrityksen Buffalo Terastation verkkolevy on ollut synkronoituna Google Driveen ja siten tiedostot on pystytty jakamaan asiakkaille helposti linkin avulla. Vuoden 2017 loppupuolella verkkolevyn Google Drive synkronointi vioittui, minkä jälkeen pilvipalveluiden käyttö on vähentynyt. Nykyinen käyttö koostuu lähinnä manuaalisesta tiedostojen siirrosta pilveen ja niiden linkityksestä asiakkaalle tarpeen vaatiessa. Verkkolevyn synkronoinnin vioittu-

misen jälkeen Studio C3:n tiedostoja ei ole varmuuskopioitu ollenkaan. Kuvassa 11 on havainnollistettu Studio C3:n lähiverkon rakenne Microsoft Visio vuokaavion avulla.



Kuva 11. Studio C3:n lähiverkon rakenne (Aldershoff 2017; Amazon n.d.; Data-Systems n.d.; Intelligent Servers n.d.; Stallion Technology n.d.; VisioCafe 2017; Wikimedia Commons 2012).

5 VARMUUSKOPIOINTI- JA TIEDONSIIRTOJÄRJESTELMÄN SUUNNITTELU

Osiossa esitellään opinnäytetyön tilaajayritykselle luotua suunnitelmaa, jonka tarkoitus on parantaa yrityksen sisäistä ja asiakkaiden välistä tiedonsiirtoa sekä paikata yritykseltä kokonaan puuttuva tiedostojen varmuuskopiointijärjestelmä. Nykyistä lähiverkkoa tutkittaessa ilmenneitä ongelmakohtia esitellään ja niihin tarjotaan ratkaisuja. Lisäksi käydään läpi uusia laitehankintoja ja laitteiden sekä ohjelmien toimintaa suunnitelmassa tehtävässä järjestelmässä. Osiossa myös pohditaan, miten pystyttäisiin hyötykäyttämään yrityksellä jo olemassa olevia käyttämättömiä ja uusien hankintojen tieltä pois käytöstä siirtyviä laitteita, esimerkiksi paikallisena tallennuspaikkana varmuuskopioille.

5.1 Ongelmakohdat yrityksen lähiverkossa

Vuoden 2017 loppupuolella Studio C3:n verkkolevypalvelimen Google Drive synkronoinnin hajoamisen jälkeen yrityksen tiedostoja ei ole varmuuskopioitu ollenkaan. Pilvisynkronoinnin hajoaminen johtui kolmannen osapuolen sovelluksen yllättävistä yhteensopivuusongelmista, uusien Google Drive -päivitysten myötä. Tietojen varmuuskopioinnin puuttuminen on selvästi suurin ongelma, joka oli tiedossa opinnäytetyön alkumetreiltä asti. Tämä aiheuttaa tilaajayrityksen tietoturvaan merkittävän aukon, koska laitteiden fyysisten vaurioiden, tiedon korruptoitumisen tai inhimillisen virheen sattuessa tilaajayrityksellä ei ole varasuunnitelmaa menetettyjen tietojen palauttamiseksi.

Hitaat tiedonsiirtonopeudet työasemien, palvelimen ja verkkolevyn välillä voivat olla työskentelytehokkuutta ja työtä hidastavia tekijöitä. Myös työasemien puutteelliset komponentit, kuten parhaat päivänsä nähneet näytönohjaimet pistävät työskentelytehokkuudelle kapuloita rattaisiin, kun raakavideomateriaaleja editoitaessa laskentateho ei riitä ja työskentely ei ole sulavaa. Studio C3:lla kyseiseen ongelmaan alettiin puuttua jo opinnäytetyön tekovaiheen aikana korvaamalla kahdessa työasemassa vanhat NVIDIA GTX750 -näytönohjaimet uusilla GTX 1060 -ohjaimilla. Kuten edellisessä luvussa esitellystä Studio C3:n lähiverkon havainnollistavasta vuokaaviosta näkyy, ovat kaikki työasemat, palvelinkone, paikallinen NetApp -levyjärjestelmä ja verkkolevypalvelin kytketty Gigabit Ethernet (1GbE) -yhteydellä yrityksen tiloissa sijaitsevan kytkimen kautta toisiinsa. Esimerkiksi tapahtumatallenteista syntyvien useiden satojen gigatavujen kokoisten raakavideotiedostojen siirtämiseen 1Gb/s -yhteys on liian hidas. Koska yrityksessä videotiedostot ovat tallennettuna verkkolevylle tai levyjärjestelmille ja editoinnissa videotiedostoja käytetään sieltä käsin, kaista menee harmillisen helposti tukkoon. Useamman kuin yhden työntekijän renderoidessa projektitiedostoa tai siirtäessä tiedostoja syntyy helposti ongelmia, koska 1Gb/s -yhteyden tiedonsiirtonopeus ei riitä.

5.2 **Synology RackStation RS3617RPxs**

Koska Studio C3:lla raakavideoiden editointi tapahtuu suoraan verkkolevyltä, ilmenee 1Gb/s -yhteyden aiheuttama pullonkaula siinä eniten. Nykyisen Buffalo Terastation verkkolevypalvelimen tilalle hankitaan uusi, paljon suorituskykyisempi NAS-palvelin, jolla pystytään tiedossa olevien puutteiden paikkaamisen lisäksi tarjoamaan lukuisia yritykselle hyödyllisiä ominaisuuksia, kuten tiedostojen automatisoidun pilvivarmuuskopioinnin ja paikallisen varmuuskopioinnin. Laitehankintaa oli tilaajayrityksessä haudutteltu jo ennen opinnäytetyöprosessin alkamista, mikä helpotti laitteen valintaa. Koska suuri osa yrityksen toiminnasta tapahtuu tavalla tai toisella NAS-palvelimen kautta, päädyttiin yrityskäyttöön valmistettuun Synology Rackstation RS3617RPxs verkkolevypalvelimeen (kuva 12). Synologyn NAS-palvelimen asentaminen ja konfigurointi pitivät liittyä osaksi opinnäytetyön käytännön osuutta, mutta NAS-palvelimen toimituksen viivästymisen takia tämä ei ollut mahdollista.

Kuva 12. Synology Rackstation RS3617RPxs (Synology n.d.).

Tekniset tiedot ja laajentamismahdollisuudet valitussa NAS-palvelimessa ovat hyvin lupaavia. Prosessorina verkkolevypalvelimessa toimii tehokas Xeon D-1521 neliydinprosessori 2.4GHz peruskellotaajuudella ja 2.7GHz turbolla, joka tukee laitteistopohjaista tiedostojen salaamista. NAS-palvelin toimitetaan 8Gt DDR4 keskusmuistia asennettuna ja yhteensä laitteessa on neljä muistipaikkaa, joihin on mahdollista asentaa maksimissaan 4 x 16Gt muistikampoja. Laitteen saapuessa Studio C3:lle, siihen on suunnitteilla asentaa jo heti toinen 8Gt RAM-kampa, koska tiedossa on, ettei 8Gt yksin riitä yrityksen tarpeisiin. Synology NAS-palvelimen tallennuskapasiteettia varten laitteessa on 12 paikkaa kiintolevyille, joihin sopivat 3.5” SATA HDD, 2.5” SATA HDD ja 2.5” SATA SSD-kovalevyt. Yhteensä tallennuskapasiteettia laitteen sisäisillä levypaikoilla voidaan saada jopa 144Tt asentamalla 12 x 12Tt kiintolevyjä. Laite tukee kiintolevyjen hot swap -tekniikkaa, eli järjestelmästä voidaan poistaa tai vaihtaa esimerkiksi vaurioitunut levy uuteen ilman, että laitetta sammutetaan. NAS-palvelimeen on lisäksi mahdollista hankkia laajennusyksikkö, jonka avulla laitteeseen voidaan kytkeä yhteensä 36 kiintolevyä, joiden teoreettinen maksimitallennuskapasiteetti on 432Tt. Maksimaalinen tallennuskapasiteetti voi vaihdella riippuen siitä, missä RAID-tyypissä levyjä ajetaan. Tuetut RAID-tyypit ovat RAID F1, JBOD, RAID 0, 1, 5, 6 ja 10.

5.3 **Suunnitelma**

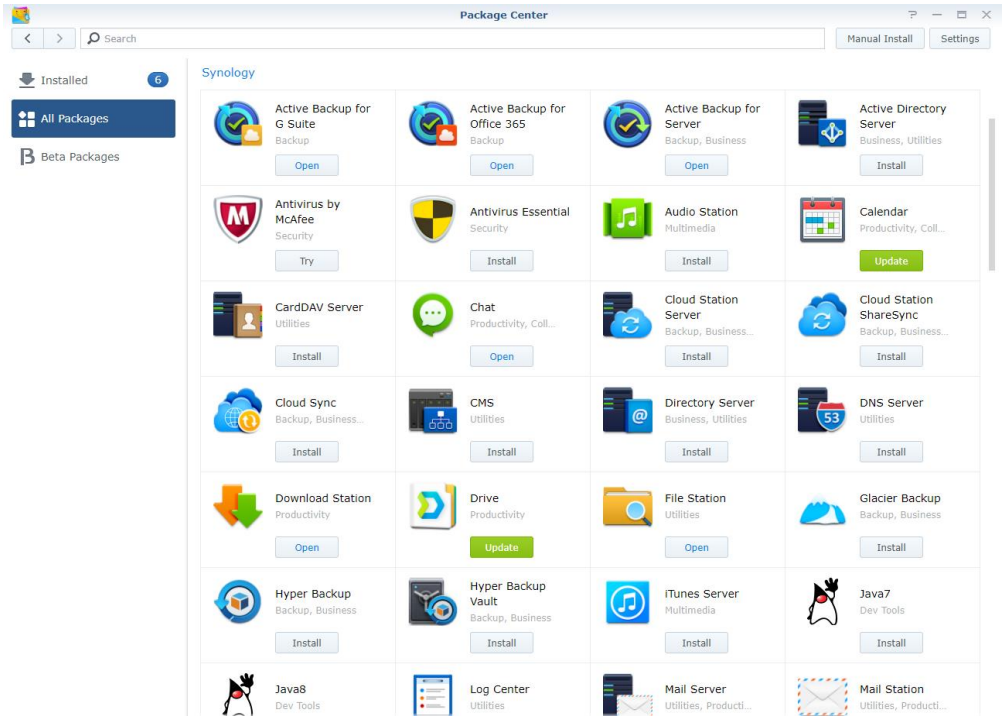
Suunnitelmana on, että kun Synologyn NAS-palvelimen toimitus saapuu Studio C3:lle, siirretään yrityksen paikallisesta palvelinkoneesta kuusi kappaletta 4Tt HDD-kiintolevyjä verkkolevypalvelimeen. Tähän ratkaisuun päädyttiin, koska yrityksen paikallisella palvelinkoneella ei tällä hetkellä ole ollut oikeastaan muuta käyttöä kuin toimia varakoneena, jolla on voitu suorittaa paljon aikaa vaativia toimenpiteitä. Esimerkiksi pitkien videoiden renderointi tai suurien tiedostojen pakkaaminen on voitu jättää palvelinkoneen tehtäväksi niin, ettei yksi tai useampi varsinaisista työasemista joudu olemaan pois käytöstä niiden aikana. Kiintolevyt asennetaan verkkolevypalvelimeen yhdistämällä ne yhdeksi loogiseksi levyksi RAID 5-tekniikalla.

NAS-palvelinta varten on tilattu neljä 1Tt Samsung EVO 850 SSD-kovalevyä, jotka asennetaan laitteeseen. SSD-levyistä tullaan tarpeen mukaan tekemään oma RAID-pakkansa, jota käytetään ajankohtaisimpien ja eniten käytettyjen tietojen tallentamiseen ja lukemiseen tai vaihtoehtoisesti niitä käytetään verkkolevypalvelimella välimuistina. Ensimmäisessä vaihtoehdossa, jossa SSD-levyt asennetaan omaan RAID:iin, suunnitelmana on valita käytettäväksi Synologyn NAS-palvelimen tukema RAID F1-tyyppi. Tämä tyyppi toimii muuten samalla tavalla kuin RAID 5-tyyppi, mutta se on optimoitu erityisesti sellaisille RAID-pakoille, joissa on käytössä ainoastaan Flash-muistia käyttäviä levyjä. Tästä RAID-pakasta voidaan tarpeen mukaan luoda oma varmuuskopio laitteessa toimivan HDD-kiintolevyistä koostuvan RAID-pakan lisäksi. SSD-levyt ovat myös paljon kestävämpiä, kuin liikkuvia osia sisältävät HDD-kiintolevyt, joka pienentää vaurioitumisen riskiä huomattavasti. Vasta laitteen ollessa yrityksessä varsinaisessa käytössä pystytään paremmin määrittelemään, onko SSD-levyjen käyttäminen NAS-palvelimen välimuistina kannattavaa tai RAID F1:n käyttö tarpeellista, vai olisiko järkevämpää ajaa SSD-levyjä mieluummin RAID 0:ssa suuremman tallennuskapasiteetin saavuttamiseksi. HDD- ja SSD-levyjen asentamisen jälkeen NAS-palvelimen omista levypaikoista jää vielä kaksi tyhjäksi, joihin voidaan yrityksen tarpeiden mukaisesti hankkia uudet levyt tallennuskapasiteetin kasvattamiseksi.

Yhdet tärkeimmistä Synologyn NAS-palvelimen tarjoamista ominaisuuksista, jotka vaikuttavat Studio C3:n jokapäiväiseen työskentelyyn, ovat neljä 1GbE porttia, joihin liitetty yhteys voidaan yhdistää yhdeksi 4Gb/s -nopeuksiseksi loogiseksi yhteydeksi sekä tuki PCIe 3.0-väylään asennettavia 10Gbit-verkkokortteja varten. Lisäksi useita yhteyksiä käytettäessä voidaan tarpeen vaatiessa yksi tai useampi kaapeleista varata failoveria varten, jotta tiedonsiirto ei keskeytyisi, vaikka kaapeli vaurioituisi. Käyttämällä 10Gb/s yhteyttä tai trunkkaamalla eli yhdistämällä 1Gb/s yhteyksiä yhdeksi loogiseksi yhteydeksi voidaan välttyä tiedonsiirrossa syntyvältä pullonkaulalta, kun esimerkiksi useampi työntekijä renderoi projektitiedostoja yhtä aikaa. Näin työnteko säilyy sulavana, eivätkä ohjelmat

kaadu paikallaan jumittavan tiedoston muuntamisen aikana. 10Gb/s yhteyden käyttäminen olisi optimaalinen ratkaisu mediastudion käyttämien suurien videotiedostojen käsittelyn vaatimiin tarpeisiin, muttei valitettavasti yrityksen nykyisen kytkimen kanssa ole mahdollista. 10Gb/s yhteyden täydellinen hyödyntäminen vaatisi uusia laitehankintoja, kuten 10Gbit-kytkimen, 10Gbit-verkkokortteja työasemiin ja verkkolevypalvelimeen sekä SSD-levyjä työasemiin, jotta tietokoneiden omista kiintolevyistä ei synny pullonkaulaa tiedonsiirrossa.

Synology NAS tarjoaa oman DSM (Synology DiskStation Manager) -käyttöliittymän, jonka avulla laitteen toimintaa ja ohjelmistopuolta on helppo hallinnoida. Käyttöliittymää käytetään tietokoneen selaimen avulla etänä. DSM:n Package Centerin kautta NAS-palvelimeen voidaan asentaa työkaluja, jotka mahdollistavat laitteen eri ominaisuuksien käytön. Tarjolla olevat ohjelmat koostuvat Synologyn omista sekä kolmannen osapuolen luomista sovelluksista. DSM:n Package Center näkymä kuvassa 13. Käytännössä DSM:llä on mahdollista esimerkiksi hallita useita Synology NAS-palvelimia yrityksen sisällä, luoda ja hallita virtuaalikoneita, luoda tietoturvallinen ja yksityinen sähköpostiratkaisu tai keskustelualusta, hallita valvontakamerajärjestelmää, holvata tiedostoja ja automatisoida tiedostojen synkronointi pilvipalveluun tai varmuuskopiointi paikalliseen levyjärjestelmään. Pienen multimediatoimiston kuten Studio C3:n käytössä joidenkin ominaisuuksien, kuten tietojen holvaamisen, virtuaalikoneiden pyörittäminen ja valvontakamerajärjestelmän hallinta olisivat lähinnä resurssien tuhlaamista. DSM:llä helposti käyttöön otettavat tai käytöstä poistettavat työkalut tarjoavat käyttäjälle mahdollisuuden kustomoida laitteen suorittamat toiminnot omien tarpeidensa mukaisiksi.



Kuva 13. Synology DSM Package Center -näkymä.

Synologyn DiskStation Managerin Package Centerin tarjoamista sovelluksista opinnäytetyön kannalta tärkeimmiksi nousivat Cloud Sync -pilvisynkronointisovellus sekä Hyper Backup, jolla varmuuskopiointi paikalliseen levyjärjestelmään voidaan automatisoida. Käytännössä Cloud Sync -ohjelmalla NAS-palvelimella sijaitsevat tiedostot synkronoidaan One Drive -pilvipalveluun kerran vuorokaudessa yöaikaan, jotta toiminto ei syö laitteen ja verkon resursseja silloin, kun työntekijät niitä aktiivisesti käyttävät. Google Drive -palvelua käytetään valikoitujen videotiedostojen tallentamiseen ja asiakkaille jakamiseen. Kaiken tiedon tallentamisen sijaan pienempien ja asiakkaiden kannalta olennaisten kokonaisuuksien synkronointi Google Drive -pilvipalveluun mahdollistaa paljon tiheämmän tahdin synkronointien välillä, jotta ajankohtaisimmat tiedostot ovat asiakkaiden saatavilla.

Paikallinen tiedostojen varmuuskopiointi suoritetaan käyttämällä Hyper Backup -ohjelmaa. Kopioiden tallennuspaikaksi suunniteltiin paikallinen NetApp -levyjärjestelmä, joka on aikaisemmin ollut Studio C3:n käytössä jaettuna kahteen 10 teratavun osioon. Tarkoituksena on yhdistää kyseiset kaksi osiota niin, että ne ovat käytettävissä yhtenä 20 teratavun kokonaisuutena varmuuskopioiden tallennusta varten. Alustavana suunnitelmana varmuuskopiointi paikalliseen levyjärjestelmään suoritetaan samoin aikavälein kuin pilvisynkronointi, eli kerran vuorokaudessa yöaikaan, varsinaisen työajan ulkopuolella. Järjestelmän käyttöönoton jälkeen ensimmäinen varmuuskopiointi levyjärjestelmään tehdään täytenä varmistuksena. Tämän jälkeen tiedostokopioiden varmistus suoritetaan inkrementaalisena, eli vain edellisestä varmistuskerrasta muuttuneet tiedostot varmuuskopioidaan.

Vaikka vanhan Buffalo Terastation TS3400D-verkkolevypalvelimen pilvisynkronointi ei enää kolmannen osapuolen varmuuskopiointiohjelman Google Drive -yhteensopivuusongelmien vuoksi ole käyttökelpoinen, laitteelle suunniteltiin eri käyttötarkoitus Studio C3:n hyödyksi. Vanhaa verkkolevypalvelinta käytetään tiedostojen tallentamiseen ja jakamiseen HAMKin lähiverkossa toimiville sisäisille asiakkaille. Aikaisemmin kyseistä tehtävää palvellut NetApp -levyjärjestelmä siirtyi uuden suunnitelman myötä paikallisten varmuuskopioiden tallennuspaikaksi, joten vanhan Terastation -verkkolevypalvelimen siirtäminen kyseiseen tehtävään tuntui luonnolliselta ratkaisulta. Mahdollisuus jakaa tiedostoja lähiverkon yli 1Gb/s -yhteyksien avulla HAMKin sisäisille asiakkaille, tarjoaa huomattavasti nopeamman tiedoston siirtonopeuden verrattuna pilvipalvelun käyttöön. Lisäksi ratkaisu tarjoaa laitteelle oikeasti hyödyllistä ja kustannustehokasta tehtävää vanhan NAS-palvelimen siirtyessä pois käytöstä sen sijaan, että se hyllytettäisiin kokonaan.

6 YHTEENVETO

Tietoturva ja varmuuskopiointi tuntuvat olevan asioita, jotka helposti laiminlyödään, eikä niiden tärkeyttä yrityksen oman toiminnan turvaamisen kannalta ymmärretä. Yleisimpiä syitä ovat niistä aiheutuvat kulut, osaamisen puute tietotekniikan parissa sekä rajoitetut resurssit etenkin pienissä yrityksissä. Opinnäytetyön tilaajayrityksen kohdalla varmuuskopiointi oli vioittunut sen suorittavan ohjelman ja varmuuskopioiden tallennuspaikkana toimivan pilvipalvelun yhteensopivuusongelman vuoksi. Opinnäytetyön tekijällä ei ollut aiempaa kokemusta varmuuskopioinnista yrityskäytössä, joten työ tarjosi mainion tilaisuuden päästä ratkaisemaan oikeaa ongelmaa yrityksessä sekä oppia uutta käsiteltävistä aiheista.

Opinnäytetyön tavoitteena oli luoda realistinen ja toimeksiantajayrityksen Studio C3:n toteutettavissa oleva suunnitelma uudesta järjestelmästä, jolla tiedostojen varmuuskopiointi voidaan suorittaa ja yrityksen lähiverkon tiedonsiirtonopeuksia parantaa. Työssä tutkittiin varmuuskopiointia, tietoturvaa ja yleisimpiä tietoturvauhkia yleisellä tasolla, sekä miten varmuuskopiointi liittyy osaksi yrityksen tietoturvaa. Suunnitelma laadittiin tutkitun teorian pohjalta. Tärkein osa laadittua suunnitelmaa oli uuden NAS-verkkolevypalvelimen hankinta, siihen tutustuminen ja sen sisällyttäminen osaksi Studio C3:n lähiverkkoa. Uuden verkkolevypalvelimen kanssa yrityksen paikallista tallennuskapasiteettia pystyttiin kasvattamaan huomattavasti siirtämällä periaatteessa käyttämättöminä olleet kiintolevyt Windows palvelinkoneesta verkkolevypalvelimeen. Lisäksi uusina hankittujen SSD-levyjen, sekä 4Gb/s nopeuksisen trunkatun yhteyden käyttö NAS-palvelimella paransivat työntekijöiden työskentelyn sulavuutta, kun pullonkauloja tiedonsiirrossa pystyttiin karsimaan. Osaksi suunnitelmaa liittyi myös uusien laitehankintojen tieltä siirtyvien laitteiden, kuten vanhan NAS-verkkolevypalvelimen hyödyntäminen eri tehtävissä sen sijaan, että laite poistuisi kokonaan käytöstä. Suunnitelmassa jätettiin myös ajatuksia jatkokehitystä varten, kuten lähiverkon laitteiden välisten yhteyksien päivittäminen 10Gbit-yhteyteen.

Työssä huomattiin, miten tärkeää varmuuskopiointi yrityksessä on tietoturvan ja liiketoiminnan jatkuvuuden kannalta. Varmuuskopioinnin puuttuessa tärkeiden tietojen menettäminen voi johtaa suureen määrän ylimääräistä työtä tai pahimmassa tapauksessa konkurssin. Työ tarjoaa yleistietoa varmuuskopioinnista ja tietoturvasta, joiden pohjalta niitä voidaan kehittää yrityksessä.

Synologyn NAS-verkkolevypalvelimen asentaminen ja konfigurointi Studio C3:n käyttöön oli tarkoitus liittyä osaksi opinnäytetyön käytännön osuutta. Valitettavasti laitteen toimitusaika viivästyi opinnäytetyöajan ulkopuolelle, minkä vuoksi varsinaista käytännön asennusta ei työhön voitu ottaa mukaan ja käytännön osuus jouduttiin suorittamaan täysin suunnitelman muodossa.

LÄHTEET

Affirma Consulting (2018). Improve your Enterprise Data Integrity. Haettu 17.1.2018 osoitteesta
http://www.affirmaconsulting.com/5-tips-to-improve-your-enterprise-data-integrity/

Aldershoff, J. (2017). OneDrive. Haettu 5.3.2018 osoitteesta
https://www.myce.com/news/microsoft-ends-onedrive-unlimited-storage-plans-81568/

AllBusiness (n.d.). How do computer viruses spread? Haettu 7.2.2018 osoitteesta
https://www.allbusiness.com/how-do-computer-viruses-spread-1329-1.html

Amazon (n.d.). Buffalo Terastation TS3400D. Haettu 5.3.2018 osoitteesta
https://www.amazon.com/Buffalo-TeraStation-Network-Attached-Storage/dp/B004QO8XVY

Backup4All (2012) Backup types, (Varmuuskopiointimenetelmät). Haettu 19.1.2018 osoitteesta
http://www.backup4all.com/kb/backup-types-115.html

Bourgeois, D. (2014). Information Systems Security. *Pressbooks* 2014. Haettu 1.2.2018 osoitteesta
https://bus206.pressbooks.com/chapter/chapter-6-information-systems-security/

Brook, A. (2017). Inkrementaalinen varmuuskopiointi. Haettu 22.1.2018 osoitteesta
https://www.reneelab.com/free-windows-7-incremental-backup-software.html

CloudBerry Lab (n.d.). Täysi varmuuskopiointi. Haettu 31.1.2018 osoitteesta
https://www.cloudberrylab.com/images/articles/diff-backup-1.png

Computer Hope (2017). Storage device. Haettu 23.1.2018 osoitteesta
https://www.computerhope.com/jargon/s/stordevi.htm

Data-Systems (n.d.). HP ProCurve 4208vl. Haettu 5.3.2018 osoitteesta
https://www.data-systems.fi/tuotteet/tuote/hp-procurve-switch-4208vl-96-36331/kategoria/verkkotuotteet-kytkimet-kytkimet-laajennettu-valikoima-modulaariset-kytkimet-3108/

Devery, D. (2015). Tiedon katoamisen syyt. Haettu 30.1.2018 osoitteesta https://www.netsupport.ie/blog/data-loss-itll-never-happen-to-me-right/

Encyclopædia Britannica (n.d.). Magnetic recording. Haettu 23.1.2018 osoitteesta https://www.britannica.com/topic/magnetic-recording#ref75462

Eronen, H. (2016). *IaaS, PaaS, SaaS? Mikä pilvipalvelu sopii yrityksellesi. Planeetta* 3/2016. Haettu 14.2.2018 osoitteesta https://blog.planeetta.net/iaas-paas-saas

Francen, E. (2015). *Information security and compliance explained. FRSecure* 7/2015. Haettu 25.1.2018 osoitteesta https://frsecure.com/blog/information-security-and-compliance-explained/

Intelligent Servers (n.d.). PowerEdge R310. Haettu 5.3.2018 osoitteesta http://www.intelligentservers.co.uk/servers/dell-poweredge-r310-lff-hotplug-cto-1u-rack-server-x6vt9/

Jyväskylän Yliopisto (2010). Tietoturvauhat. *Koppa* 12/2010. Haettu 1.2.2018 osoitteesta https://koppa.jyu.fi/avoimet/mit/virtuaaliset-oppimisympaeristoet/oppimisympaeristoejen-tietoturva/tietoturvariskit

Laakso, M. (2010). Tietoturvasuunnitelman laatiminen. *Tietojesiturvaksi.fi* 12/2010. Haettu 30.1.2018 osoitteesta https://tietojesiturvaksi.fi/tietoturvasuunnitelma

Laaksonen, A. (2015). Pilvipalvelut pähkinänkuoressa. *Pilveen.net* 9/2015. Haettu 22.2.2018 osoitteesta http://www.pilveen.net/2015/09/pilvipalvelut-pahkinankuoressa.html

Lepistö, T. (2016). *Varmuuskopiointi ja tietoturva mikroyrityksessä*. Kandidaatintyö. Tietotekniikan koulutusohjelma. Lappeenrannan teknillinen yliopisto. Haettu 16.1.2018 osoitteesta http://www.doria.fi/bitstream/handle/10024/124116/Kandidaatinty%C3%B6_Lepist%C3%B6_Toni_2016.pdf?sequence=2&isAllowed=y

M-DISC (n.d.). What is M-DISC? Haettu 24.1.2018 osoitteesta http://www.mdisc.com/corporate/

NIST (2010). NIST Cloud Computing Program – NCCP. National Institute of Standards and Technology 11/2010. Haettu 14.2.2018 osoitteesta https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp

Omelchenko, A. (2015). Differentiaalinen varmuuskopiointi. Haettu 22.1.2018 osoitteesta https://sqlbak.com/academy/differential-backup/

OpenText (n.d.). CIA-kolmio. Haettu 17.1.2018 osoitteesta https://www.opentext.com/what-we-do/business-needs/information-governance/ensure-compliance/information-security-and-privacy

Posey, B. (2010). Data backup types explained: Full, incremental, differential and incremental-forever backup. *TechTarget* 7/2010. Haettu 19.1.2018 osoitteesta http://searchdatabackup.techtarget.com/tip/Data-backup-types-explained-Full-incremental-differential-and-incremental-forever-backup

Prinzlau, M. (2017). Varmuuskopiointi pilvipalveluun. Haettu 22.1.2018 osoitteesta https://www.cloudwards.net/best-windows-server-backup/

Pukki, J. (2012). *Yrityksen offsite-varmuuskopiointi.* Opinnäytetyö. Tietojenkäsittelyn koulutusohjelma. Oulun seudun ammattikorkeakoulu. Haettu 19.1.2018 osoitteesta https://www.theseus.fi/bitstream/handle/10024/44475/Pukki_Jari.pdf?sequence=1

Riihimäki, A. (2010). *PK-yrityksen tietojen varmuuskopiointi.* Opinnäytetyö. Tietojenkäsittelyn koulutusohjelma. Turun ammattikorkeakoulu. Haettu 15.1.2018 osoitteesta http://www.theseus.fi/handle/10024/25465

Rouse, M. (2014a). Confidentiality, Integrity and Availability (CIA triad). *TechTarget* 11/2014. Haettu 17.1.2018 osoitteesta http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA

Rouse, M. (2014b). RAID 5 tason toiminta. RAID 5 (Redundant Array of Independent Disks). *TechTarget* 12/2014. Haettu 2.3.2018 osoitteesta http://searchstorage.techtarget.com/definition/RAID-5-redundant-array-of-independent-disks

Rouse, M. (2017). Data breach. *TechTarget* 12/2017. Haettu 7.2.2018 osoitteesta http://searchsecurity.techtarget.com/definition/data-breach

Sebastian, A. (2017). IBM and Sony cram up to 330 terabytes into tiny tape cartridge. *Ars Technica* 2/2017. Haettu 23.1.2018 osoitteesta https://arstechnica.com/information-technology/2017/08/ibm-and-sony-cram-up-to-330tb-into-tiny-tape-cartridge/

Spector, L. (2013). Backing up your entire drive: Cloning vs. imaging. *PCWorld* 11/2013. Haettu 19.1.2018 osoitteesta https://www.pcworld.com/article/2029832/backing-up-your-entire-drive-cloning-vs-imaging.html

Stallion Technology (n.d.). PowerEdge R720. Haettu 5.3.2018 osoitteesta https://www.stalliontek.com/refurbished-dell-poweredge-r720-3-5-8-bay-configure-to-order

Sullivan, E. & Poelker, C. (2017). RAID-tekniikan lomittaminen ja peilaaminen. Haettu 24.1.2018 osoitteesta http://searchstorage.techtarget.com/answer/RAID-types-and-benefits-explained

Synology (n.d.). Choose a RAID Type. Haettu 24.1.2018 osoitteesta https://www.synology.com/en-global/knowledge-base/DSM/help/DSM/StorageManager/volume_diskgroup_what_is_raid

Synology (n.d.). RackStation RS3617RPxs. Haettu 28.2.2018 osoitteesta https://www.synology.com/en-us/products/RS3617RPxs

VisioCafe (2017). NetApp-levyjärjestelmä. Haettu 5.3.2018 osoitteesta http://www.visiocafe.com/netapp.htm

Wikimedia Commons (2012). Google Drive. Haettu 5.3.2018 osoitteesta https://commons.wikimedia.org/wiki/File:Google_Drive_Logo.svg

Yurin, M. (n.d.). Varmuuskopioinnin historia. The history of backup. Haettu 23.1.2018 osoitteesta http://www.backuphistory.com/

Z-DBackup (n.d.). Backup to SSD. Haettu 24.1.2018 osoitteesta https://www.z-dbackup.com/backup-ssd.html