

Opinnäytetyö (AMK)

Tietojenkäsittely

2019

Toni Lindroos

LINUX-PALVELIN OSANA PIENYRITYKSEN TIETOJÄRJESTELMÄÄ

– Tapaus yritys X

Toni Lindroos

LINUX-PALVELIN OSANA PIENYRITYKSEN TIETOJÄRJESTELMÄÄ

- Tapaus yritys X

Tietotekniikan merkitys yhä pienempien yritysten toiminnassa on lisääntynyt, minkä myötä myös laitteiden ja palveluiden hankinta- ja ylläpitokulut ovat kasvaneet. Opinnäytetyön tavoitteena oli suunnitella ja toteuttaa toimeksiantona pienyrityksen X tarpeisiin soveltuva kustannustehokas, mutta silti monipuolinen tietojärjestelmä, joka rakentuu edullisen Linux-palvelintietokoneen ja sen mahdollistamien toimintojen ympärille.

Opinnäytetyön teoriaosuudessa esitellään Linux-käyttöjärjestelmä sekä sen jakelupaketin valinnassa huomioitavat tekijät ja kerrotaan, mitä toimintoja Linux-palvelimen avulla voidaan toteuttaa. Lisäksi tutkitaan, millainen laitteisto soveltuu pienyrityksen palvelinkoneen perustaksi ja mitä tyyppilinen yrityksen tietoverkko pitää sisällään.

Toiminnallisessa osuudessa suunnitellaan ja toteutetaan toimeksiantajan tarpeita vastaava tietojärjestelmä soveltaen aiemmin esiteltyä teoriaa käytännössä. Asiakasyritykselle rakennettiin uusi palvelintietokone, minkä lisäksi uudistettiin lähiverkkoa ja otettiin käyttöön uusi langaton verkko. Myös uuden järjestelmän hallittuun käyttöönottoon, vikatilanteisiin varautumiseen ja ylläpitoon kiinnitettiin erityistä huomiota.

Projektin lopputuloksena toimeksiantajan käyttöön syntyi edullinen tietojärjestelmä, joka täytti sille ennalta asetetut vaatimukset. Lisäksi järjestelmä mahdollistaa uusien toimintojen lisäämisen tulevaisuudessa yrityksen tarpeiden muuttuessa. Huolellisen suunnittelun ansiosta sekä järjestelmän rakentaminen että käyttöönotto sujuivat ongelmitta aikataulun mukaisesti.

Opinnäytetyössä esitelty tietojärjestelmäratkaisu on helposti muunneltavissa myös muiden yritysten tarpeita vastaavaksi ja toimii hyvänä esimerkkinä siitä, että Linuxiin ja edulliseen palvelintietokoneeseen perustuvat ratkaisut voivat olla varteenotettava vaihtoehto kalliimmille ratkaisuille, kuten Windows-palvelinkäyttöjärjestelmälle ja varsinaiselle palvelinkäyttöön tarkoitettulle tietokoneelle.

ASIASANAT:

Linux, palomuuri, palvelin, yritys, reititin, tietojärjestelmä, tietoverkko

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Business Information Technology

2019 | 66 pages, 4 pages in appendices

Toni Lindroos

LINUX SERVER AS PART OF THE INFORMATION SYSTEM OF A SMALL BUSINESS

- Case: Company X

Information technology plays an increasingly significant role in business activities of even smaller companies which has also led to the growing acquisition costs and maintenance expenses of the devices and the services. The objective of this thesis was to design and implement a cost-effective yet versatile information system for the small business company X which commissioned this thesis. The information system is based on a reasonably priced Linux server computer and the functions enabled by it.

The theoretical part of this thesis covers the introduction of the Linux operating system and the choice of a suitable Linux distribution. Furthermore, it describes what kind of functions can be implemented with a Linux-based server, how to choose hardware components for the server computer and what is a typical design of a local area network in a small business.

The practical part explains how the theory described earlier was applied to practice in designing and realizing an information system which corresponds to the commissioner's needs. A new server computer was built and the client's internal network was improved including the deployment of the new wireless local area network. Special attention was paid to the controlled deployment of the new system, preparing for error recovery situations, and the easily underestimated maintenance.

The result of the project was an affordable Linux-based information system which fully met the demands set for it by the commissioning company. In addition, new features can be added to the flexible system in the future according to the changing needs of the commissioner. Due to the thorough planning both the building and implementation stages of the system went without problems and according to the schedule.

The information system demonstrated in this thesis can be easily adapted to meet the needs of many different companies. It also functions as a good example of the fact that a system based on the Linux operating system and an affordable server computer can be a worthy alternative to the solutions based on the Windows server operating system and an actual server computer.

KEYWORDS:

Business, data network, firewall, information system, Linux, router, server

SISÄLTÖ

KÄYTETYT LYHENTEET JA SANASTO	5
1 JOHDANTO	8
2 OHJELMISTO JA LAITTEISTO	10
2.1 Linux-käyttöjärjestelmä	10
2.2 Palvelimen mahdollistamat toiminnot	14
2.3 Palvelinkone	19
2.4 Vaihtoehtona Windows-palvelin	20
2.5 Palvelimen virtualisointi	24
2.6 UPS-varavirtajärjestelmä	26
2.7 Tietoverkko	27
3 SUUNNITTELU	32
3.1 Tapaus yritys X	32
3.2 Vanha tietojärjestelmä	32
3.3 Vaatimusten määrittely	34
3.4 Uusi tietojärjestelmä	36
4 TOTEUTUS	46
4.1 Palvelimen asennus ja käyttöönotto	47
4.2 Tietoverkon muutokset	50
4.3 Toiminnan tarkistaminen	53
4.4 Ylläpito	54
5 PÄÄTELMÄT	60
LÄHTEET	63

LIITTEET

- Liite 1. Linux-palvelinkoneen hankintakustannukset.
- Liite 2. Windows-palvelinkoneen hankintakustannukset.
- Liite 3. Käyttöjärjestelmän versiopäivitys Zypper-ohjelmalla.

KÄYTETYT LYHENTEET JA SANASTO

Active Directory	Microsoftin kehittämä verkossa toimiva hakemistopalvelu, josta haetaan sinne tallennettuja käyttäjiin ja laitteisiin liittyviä tietoja, kuten esimerkiksi käyttäjätunnuksia ja salasanoja sekä tietoja käyttöoikeuksista (Microsoft 2017).
Avoin lähdekoodi	Avoimen lähdekoodin ohjelmiston lähdekoodi on vapaasti saatavilla ja sitä saa muokata, kopioida ja jakaa eteenpäin ilman lisenssimaksujen maksamista, mutta kuitenkin lisenssiehtoja noudattaen. (Blum & Bresnahan 2015, 28–29.)
CAL	Client Access License. Käyttöoikeuslisenssi, joka vaaditaan joidenkin Microsoftin tuotteiden käyttämiseksi. Esimerkiksi Windows Server -käyttöjärjestelmällä varustettu palvelin vaatii jokaiselta sitä käyttävältä käyttäjältä tai laitteelta oman CAL-lisenssin. (Microsoft 2019d.)
DHCP	Dynamic Host Configuration Protocol. Verkkoprotokolla, jota käyttäen DHCP-palvelin jakaa IP-osoitteita verkkoon kytketyille laitteille. (Internet Systems Consortium 2019.)
Ethernet	Yleisin käytössä oleva lähiverkkotekniikka. Termi Ethernet käsittää myös standardissa IEEE 802.3 määritellyt lähiverkkojen toteutuksessa käytetyt tekniikat. (Kaario 2002, 33–34.)
IMAP	Internet Message Access Protocol. Sähköpostien lukemiseen ja hallinnoimiseen käytetty protokolla, jota käytettäessä sähköposteja säilytetään yleensä palvelimella, josta niihin pääsee käsiksi useammalla eri laitteella tai ohjelmalla. (IBM 2014.)
IP-osoite	Jokaiselle IP-verkkoon liitetyle laitteelle määriteltävä yksilöivä tunniste, joka mahdollistaa yhteydenpidon verkon muiden laitteiden kanssa. IPv4-osoitteet ovat pituudeltaan 32-bittisiä numerosarjoja (esim. 192.168.0.1). (Kaario 2002, 53.) Uudemmat IPv6-osoitteet ovat 128-bittisiä heksadesimaalisia numerosarjoja (esim. 2001:DB8:7654:3210:FEDC:BA98:7654:3210) (Kaario 2002, 109).
Jakelupaketti	Engl. distribution. Linuxin ytimeistä, sovellusohjelmista ja asetustiedostoista koostuva käyttöjärjestelmän jakeluun käytettävä ohjelmistopaketti, joita on julkaistu monien eri tahojen toimesta. (Blum & Bresnahan 2015, 13.)
Kernel	Käyttöjärjestelmän ydin on ohjelma, joka huolehtii käyttöjärjestelmän perustoiminnoista ja mahdollistaa ohjelmistojen ja laitteiston välisen kommunikoinnin. Se huolehtii myös mm. käyttöoikeuksista sekä keskusmuistin ja prosessoritehon jakamisesta eri prosessien kesken. (Negus 2010, 25–27.)

Komentosarja	Engl. script. Tietyllä komentokielellä kirjoitettu, suoritettavista komennoista muodostuva ohjelma, joka voi olla tallennettu esimerkiksi tekstitiedostoon. (Blum & Bresnahan 2015, 211–212.)
Lähdekoodi	Tekstimuodossa oleva selväkielinen listaus, joka sisältää tietyn tietokoneohjelman tai sen osan jollakin ohjelmointikielellä kuvattuna. Lähdekoodi käännetään ennen sen suorittamista konekielelle, jota tietokone osa tulkita. (Paananen 2005, 467.)
MAC-osoite	Media Access Control. Verkkosovittimen yksilöllinen 48 bittiä pitkä osoite, joka yleensä merkitään kuutena heksadesimaalisena lukuna (esim. 0B:10:FC:22:1A:6D). (Paananen 2005, 467.)
Palomuri	Palomuri on järjestelmä, joka valvoo ja hallinnoi verkkoliikennettä tiettyjen ennalta asetettujen määritysten perusteella joko estäen tai sallien liikennöinnin (Blum & Bresnahan 2015, 304).
POE	Power Over Ethernet. PoE-tekniikan avulla laitteelle syötetään sen tarvitsema käyttösähkö samaa verkkokaapelia pitkin, jota se käyttää tietoliikenteeseensä. (Oliviero & Woodward 2014, 98.)
POP3	Post Office Protocol. Sähköpostien lukemiseen ja hallinnoimiseen käytetty protokolla, jota käytettäessä sähköpostit yleensä poistetaan palvelimelta sen jälkeen, kun sähköpostiohjelma on hakenut ne käyttäjän koneelle. (IBM 2014.)
RAID	Redundant Array of Inexpensive Disks. Tietokoneiden tallennusjärjestelmien vikasietoisuuden ja suorituskyvyn kasvattamiseen käytetty tekniikka, jossa useita erillisiä kiintolevyjä yhdistetään yhdeksi loogiseksi levyksi. (Kim & Solomon 2016, 1123–1124.)
RDP	Remote Desktop Protocol. Microsoftin kehittämä protokolla, jonka avulla voidaan etäkäyttää toista, yleensä Windows-tietokonetta verkkoyhteyden välityksellä. Etäkoneen työpöytä näkyy asiakasohjelmaa käyttävän koneen ruudulla ja hiiri- ja näppäinkomennot välittyvät etäkoneelle. (Microsoft 2018a.)
Reititin	Tietoverkoissa käytettävä laite, joka yhdistää useita eri verkkoja toisiinsa välittäen tietopaketteja niiden välillä sille määriteltyjen sääntöjen mukaisesti. Reitittimen avulla yhdistetään esimerkiksi sisäverkon laitteet Internetiin. (Cisco 2019.)
SMTP	Simple Mail Transfer Protocol. Protokolla, jota käytetään sähköpostiviestien lähettämiseen käyttäjän tietokoneelta palvelimelle ja viestien välittämiseen sähköpostipalvelimien välillä. (IBM 2017.)

SSH	Secure Shell. Protokolla, jossa käytetään salausmenetelmää asiakastietokoneen ja palvelimen välisen tietoliikenteen turvaamiseksi. (SSH Communications Security Oyj 2019a.)
UPS	Uninterruptible Power Supply. Akun sisältävä laite, jolla varmistetaan esimerkiksi tietokoneen katkoton virransyöttö sähköverkon lyhyiden katkosten aikana. (Paananen 2005, 479.)
Verkkokytkin	Tietoverkoissa käytettävä laite, joka yhdistää laitteet, kuten tietokoneet ja muut verkkokytkimet, samaan verkkoon, jossa ne voivat viestiä keskenään (Cisco 2019).
Virtuaalikone	Ohjelmallisesti virtualisointialustalle toteutettu tietokone, joka käyttää virtualisointialustan sille tarjoamia resursseja. Virtuaalikone näkee vain sille tarjotut abstraktit resurssit, joten virtualisointialustan laitteiston resurssit ovat sen näkymättömissä. Yhdellä virtualisointialustalla voidaan ajaa useita virtuaalikoneita samanaikaisesti. (Portnoy 2016, 37–38.)
Virtualisointi	Tekniikka, jossa luodaan ja hyödynnetään virtuaalisia (abstrakteja) resursseja todellisten (fyysisten) resurssien sijaan. Esimerkiksi laitteistovirtualisoinnissa virtualisointialusta (hypervisor) käyttää laitteiston fyysisiä resursseja, kuten prosessoria, keskusmuistia ja tallennustilaa, joita se jakaa virtualisointiympäristön käyttäjille, jotka ovat virtuaalikoneita. (Portnoy 2016, 1–2.)
VLAN	Virtual LAN. Tekniikka, joka mahdollistaa useamman virtuaalisen lähiverkon luomisen yhden fyysisen verkon sisälle. Vaikka laitteet ovat fyysisesti samassa verkossa, voidaan ne erotella erillisiin virtuaalisiin verkkoihin lisäämällä tietopaketeihin erityinen VLAN-tunnus. (Kaario 2002, 234.)
VOIP	Voice Over IP. Tekniikka, jossa äänipuheluita siirretään pakettikytkentäisessä IP-verkossa. (Kaario 2002, 224.)
VPN	Virtual Private Network. Tekniikka, jossa julkisen Internetin läpi muodostetaan salattu yhteys. (Kaario 2002, 304.)
WLAN	Wireless Local Area Network. Langaton lähiverkkotekniikka, jossa tietoa siirretään laitteiden välillä käyttäen radiotaajuuksia kiinteän verkkokaapeloinnin sijasta. (Paananen 2005, 481–482.)

1 JOHDANTO

Yritysten tietojärjestelmilleen asettamat tehtävät ja vaatimukset vaihtelevat yrityksen koon, toimialan ja työskentelytapojen mukaisesti. Yhä pienemmät yritykset joutuvat miettimään, miten ne voisivat tietotekniikkaa hyödyntämällä tehostaa toimintaansa ja saavuttaa näin taloudellista etua sekä parantaa työntekijöidensä viihtyvyyttä. Suuremmista yrityksistä tutut toimintatavat ja palvelut, kuten etätyöskentely ja erilaiset tietokantoja käyttävät palvelut, yleistyvät siten myös pienemmissä yrityksissä. Tietotekniikan kasvaneesta merkityksestä liiketoiminnassa seuraa myös se, että yrityksen pitää tiedostaa ja minimoida tietojärjestelmiensä riskit, joita ovat esimerkiksi tietojärjestelmän palveluiden vikaantuminen ja tietojen katoaminen. Tässä yhteydessä tietojärjestelmällä tarkoitetaan tietoliikenneverkosta, tietojenkäsittelylaitteista ja ohjelmistoista sekä niiden tiedoista, palveluista ja käyttäjistä muodostuvaa kokonaisuutta.

Lukuisten liiketoiminnan kannalta tärkeiden tietoteknisten palveluiden hankkiminen saattaa olla monelle pienyritykselle suhteellisen suuri kuluerä liiketoiminnan muihin kuluihin verrattuna. Tämän opinnäytetyön tarkoituksena onkin suunnitella ja toteuttaa pienyritykselle X toimeksiantona kustannustehokas, mutta silti ominaisuuksiltaan monipuolinen tietojärjestelmä ilmaisen Linux-käyttöjärjestelmän ja siinä toimivien muiden avoimen lähdekoodin sovellusten avulla. Opinnäytetyössä käsitellyn tietojärjestelmän perustana on edullinen palvelinkone, ja muut kustannukset muodostuvat pääasiassa järjestelmän määrittämis- ja asennustöistä, koska ilmaisia avoimen lähdekoodin sovelluksia käytettäessä vältetään ohjelmistojen hankintakustannuksilta.

Työn tavoitteena on myös lisätä tietoisuutta Linuxiin ja edulliseen tietokoneeseen perustuvista ratkaisuista vaihtoehtona hankintahinnaltaan kalliimmille ratkaisuille, kuten Windowsin palvelinversioille ja varsinaiseen palvelinkäyttöön tarkoitettuille laitteille. Vertailun vuoksi opinnäytetyössä esitellään yleisellä tasolla myös tyypillinen Windows-palvelinratkaisu, joka koostuu yrityskäyttöön suunnitellusta palvelintietokoneesta ja maksullisesta Windows Server -käyttöjärjestelmästä.

Linux valikoitui opinnäytetyössä toteutetun palvelimen käyttöjärjestelmäksi maksuttomuutensa vuoksi ja sekä oman että toimeksiantajan aiempien hyvien kokemusten perusteella. Itselläni on kokemusta Linux- ja Windows-käyttöjärjestelmien hyödyntämisestä työasema- ja palvelinkäytössä yli 20 vuoden ajalta ja olen suunnitellut sekä toteuttanut useita palvelimia pienyritysten käyttöön. Tätä käytännön kokemusten kautta hankit-

tua osaamista hyödynnetään opinnäytetyön toteutuksessa. Muina lähteinä käytetään sekä kirjallisia lähteitä että tarkoin valittuja verkkolähteitä, joiden esittämiin tietoihin suhtaudutaan vaadittavalla kriittisyydellä.

Tämä konstruktivinen tapaustutkimus on tarkoitettu yrityksen IT-asioista vastaaville henkilöille, joilta odotetaan tietotekniikan ja tietoverkkojen yleisimpien käsitteiden tuntemusta. Asioita pyritään kuitenkin käsittelemään melko yleisellä tasolla kuvailematta yksityiskohtaisesti esimerkiksi käyttöjärjestelmän asennusta tai sen asetusten määrittelyä vaihe vaiheelta. Tutkimuksen ulkopuolelle on rajattu myös Linux- ja Windows-käyttöjärjestelmien keskinäinen vertailu, joista löytyy runsaasti jo aiempaa tietoa esimerkiksi alan kirjallisuudesta ja muiden tekemistä opinnäytetöistä.

Opinnäytetyössä esitellään ensin yleisellä tasolla Linux-käyttöjärjestelmä sekä sen jakelupaketin valintaan vaikuttavat tekijät ja selvitetään, millaisia toimintoja yritys voi Linux-palvelimen avulla toteuttaa. Lisäksi kerrotaan, millainen laitteisto soveltuu yleisimpiin käyttötarkoituksiin pienyritykselle. Seuraavissa luvuissa käsitellään tarkemmin toimeksiantajan järjestelmän suunnittelua ja toteutusta soveltaen viitekehysessä esitettyä teoriaa käytännössä. Tärkeää, mutta usein unohdettua järjestelmän ylläpitoa käsitellään omassa alaluvussaan. Loppuluvussa arvioidaan, miten toimeksiannon toteutuksessa onnistuttiin, miten järjestelmää voitaisiin jatkossa kehittää ja mitä asioita olisi kiinnostavaa tutkia tarkemmin.

2 OHJELMISTO JA LAITTEISTO

2.1 Linux-käyttöjärjestelmä

Linux on avoimeen lähdekoodiin perustuva Unix-tyyppinen käyttöjärjestelmä, joka rakentuu kernelin eli Linux-ytimen ympärille (Blum & Bresnahan 2015, 8). Lukemattomat eri tahot ovat koonneet Linuxin ja siinä toimivia sovellusohjelmia sekä asetustiedostoja kokonaisuuksiksi, joita kutsutaan jakelupaketeiksi (Blum & Bresnahan 2015, 13). Erilaisia jakelupaketteja on useita satoja, mutta niistä kaikkia ei enää aktiivisesti kehitetä (LWN 2019).

Tyypillinen jakelupaketti koostuu Linuxin ytimen lisäksi oheisohjelmista, ohjelmakirjastoista, ikkunointijärjestelmän päällä toimivasta työpöytäympäristöstä ja ohjeista (Blum & Bresnahan 2015, 13). Ilmaisista ohjelmista toimitetaan yleensä käyttövalmiiden binääritiedostojen lisäksi myös lähdekoodi, jota voidaan tarvittaessa muokata vastaamaan uusia käyttötarpeita. Yleensä jakelupakettien mukana tulee myös joitakin ohjelmistoja, joiden lähdekoodia ei ole julkaistu, mutta joiden käyttö ilmaiseksi on kuitenkin sallittua. Esimerkiksi osa laitevalmistajista saattaa julkaista laitteidensa ajurit Linuxille vain suoritettavina binääritiedostoina, joiden lähdekoodi ei ole vapaasti tarkasteltavissa.

Suurin osa jakelupaketeista on ilmaisia, mutta joukkoon mahtuu myös maksullisia erityisesti yrityskäyttöön tarkoitettuja vaihtoehtoja, jotka vastineeksi hankintahinnalle tarjoavat esimerkiksi parempia tukipalveluita niitä tarvitseville. Jakelupaketit eroavat usein toisistaan käyttöjärjestelmän asennusohjelman sekä oheisohjelmapakettien hallintaan käytetyn paketinhallintajärjestelmänsä osalta ja niiden mukana tulevat ohjelmat on saatettu valita erityisesti joltain tiettyä käyttötarkoitusta varten. Yleistä on suuntautuminen joko työasema- tai palvelinkäyttöön ja osa jakelupaketeista on erikoistunut viihdekäyttöön. (Blum & Bresnahan 2015, 13–15.) Mobiililaitteikäytössä suosittu Android-käyttöjärjestelmäkin voidaan joidenkin lähteiden mukaan määritellä Linux-jakeluksi, vaikka se ei täytäkään kaikkia Linux-jakelupaketin tunnusmerkkejä (Wikipedia 2019a).

Jakelupaketin valintakriteerit

Käyttötarkoitukseen soveltuvan Linux-jakelupaketin valintaan kannattaa käyttää riittävästi aikaa, sillä valinnan vaikutukset näkyvät niin käyttöönoton ja ylläpidon sujuvuus-

dessa kuin ohjelmisto- ja käyttötuen kestossakin. On huomattavasti helpompaa etukäteen perehtyä eri jakelupakettien ominaispiirteisiin kuin vaihtaa vaihtoehdosta toiseen kesken käyttöönoton tai pahimmassa tapauksessa vasta sen jälkeen, kun järjestelmä on jo tuotantokäytössä.

Työpöytäkäyttöön tarkoitetun Linux-jakelupaketin valinnassa huomio saattaa usein kiinnittyä siihen, mitä ikkunointiympäristöjä siihen on saatavilla, millaisia graafisen käyttöliittymän omaavia ohjelmia sen mukana tulee ja kuinka helppoa asetusten muuttaminen ja päivittäinen käyttö on. Oman kokemukseni mukaan palvelinkäytössä edellä mainituilla seikoilla ei ole niinkään paljon merkitystä, vaan huomiota tulee kiinnittää erityisesti seuraaviin asioihin: laitteistotuki, ohjelmistovalikoima, ohjelmistojen ja niiden toiminnan muuttumattomuus, ohjelmistotuen kesto, ohjelmien asentamisen ja päivittämisen vaivattomuus, käyttötuen saatavuus ja laatu sekä ylläpitäjän kokemus ja miellymykset. Näitä asioita käydään tarkemmin läpi seuraavaksi.

Käyttöjärjestelmän laitteistotuki ratkaisee, millaisista komponenteista muodostuvassa laitteistossa se toimii. Linuxin mukana tulevat laiteajurit yleisimmille laitteille. Palvelinkäytössä huomiota tulee kiinnittää lähinnä siihen, että tietokoneen emolevyn piirisarja ja kiintolevyohjain sekä verkkokortti toimivat Linuxin kanssa. Suurin osa laiteajureista on avointa lähdekoodia, mutta joidenkin laitteiden käyttäminen edellyttää laitevalmistajan toimittamien suljettujen ajurien asentamista (Blum & Bresnahan 2015, 32). Lisäksi esimerkiksi näytönohjaimille on olemassa usein sekä avointa lähdekoodia olevat ajurit että suljetut ajurit, joiden toimivuudessa ja ominaisuuksissa eri käyttötarkoituksissa on eroja (Blum & Bresnahan 2015, 91). Valmistajien toimittamien ajurien kohdalla on varmistettava, että ne toimivat juuri tietyn Linux-jakelun kanssa.

Useimpien jakeluiden mukana tulee palvelinkäyttöön soveltuva ohjelmistovalikoima, mutta on silti hyvä varmistaa toimittajan sivustolta, että juuri omaan käyttöön valituista ohjelmista on mukana riittävän uudet versiot. Linux-jakeluiden omien asennuslähteiden (engl. repository) lisäksi voidaan käyttää myös epävirallisia asennuslähteitä, ohjelmistot voidaan asentaa yksittäisestä paketista tai kääntää itse ohjelmakoodista. On kuitenkin vaivattomampaa niin ohjelman asentamisen kuin säännöllisen päivittämisenkin kannalta, jos ohjelma toimitetaan ja se päivittyy jakelupaketin mukana.

E erityisen tärkeää järjestelmän vakauden ja ylläpidon kannalta on ohjelmistojen ja niiden toiminnan muuttumattomuus. Jos toimittajalla on usein tapana vaihtaa järjestelmän tärkeimpiä ohjelmistoja toisiin vastaaviin, aiheutuu siitä ylimääräistä ylläpitotyötä. Tär-

keää on myös, että järjestelmän pääversioiden välissä julkaistavat välipäivitykset eivät ratkaisevasti muuta järjestelmän toimintaa. Edellä mainitun kaltaisia päivityksiä tulisi tulla vain uuden pääversion mukana, jolloin ylläpitäjä voi huolellisesti valmistautua muutoksiin ja valita päivitykselle sopivan ajankohdan.

Yrityskäytössä yksi tärkeimmistä jakelupaketin valintakriteereistä on ohjelmistotuen kesto eli se, kuinka kauan käyttöjärjestelmään ja sen ohjelmistoihin on saatavilla yksittäisiä päivityksiä ennen kuin se pitää päivittää uuteen pääversioon (Blum & Bresnahan 2015, 17). Tuotantokäytössä olevan palvelimen käyttöjärjestelmän pääversion päivittäminen aiheuttaa usein toimintaan keskeytyksiä ja lisäkustannuksia varsinkin, jos päivitystyö pyritään tekemään yrityksen työajan ulkopuolella. Jos erityisesti Internetiin avoimena olevan palvelimen säännöllisestä ylläpidosta ei olla sovittu, saattaa käyttöjärjestelmä jäädä päivittämättä pitkäksi aikaa, mikä muodostaa merkittävän tietoturvariskin. Keskeistä on myös se, että tietoturva-aukkoja paikkaavat päivitykset julkaistaan riittävän nopeasti. Ohjelmistotuen kesto ja päivitysvälit selviävät helpoiten toimittajien www-sivustoilta. Kääntöpuolena jakelupaketin pitkällä ohjelmistotuella voi olla se, että ohjelmistokomponentteja ei enää tietyn ajan jälkeen välttämättä päivitetä uusia ominaisuuksia lisääviin seuraaviin pääversioihin, vaan niihin julkaistaan vain pienempiä päivityksiä.

Tavanomaisessa ylläpitotyössä korostuu ohjelmien asentamisen ja päivittämisen vaikeus. Helpoin tapa asentaa ja päivittää ohjelmistot on käyttää paketinhallintajärjestelmää. Yleisimmät Linux-jakeluissa käytetyt paketinhallintajärjestelmät perustuvat joko RPM- tai DEB-tyyppisten ohjelmapakettien käsittelyyn (Blum & Bresnahan 2015, 15). Käytännössä ei ole väliä, kumpaa pakettityyppiä Linux-jakelussa käytetään, vaan tärkeintä on valita sellainen paketinhallintajärjestelmä, joka on helppokäyttöinen ja jonka toiminnan voi tarvittaessa myös automatisoida. Tarjolla on sekä komentorivipohjaisia että graafisella käyttöliittymällä toimivia paketinhallintaohjelmia. Yksittäisten ohjelmistopakettien päivittämisen lisäksi on syytä varmistaa, että Linuxin päivitys uuteen pääversioon onnistuu mahdollisimman vähällä vaivalla ja luotettavasti.

Tärkeitä Linux-jakelupaketin valintakriteereitä ovat myös käyttötuen saatavuus ja laatu. Kokeneinkin alan ammattilainen voi kohdata ongelmia jo Linuxin käyttöönoton alkuvaiheessa, jos esimerkiksi asentaminen keskeytyy johonkin yllättävään ongelmaan tai asetusten määrittelyssä tarvitaan apua. Tällöin korostuu toimittajan tuottaman ohjeistuksen määrän, laadun ja ajantasaisuuden merkitys.

Mikäli ratkaisua ongelmaan ei löydy ohjeista, voi sitä etsiä toimittajan tai kolmansien osapuolien keskustelufoorumeilta. Mitä yleisempi Linux-jakelu on kyseessä, sitä enemmän on saatavilla siihen liittyvää käyttäjien jakamaa tietoa. Joillakin toimittajilla on tarjolla myös ilmaisia tai maksullisia tukipalveluita. (Blum & Bresnahan 2015, 123–124). Yrityksen kannalta on tärkeää valita sellainen Linux-jakelupaketti, johon löytyy osamista myös muilta kuin yrityksen omalta ylläpitäjältä.

Linux-jakelupaketin valintaan vaikuttavat usein ratkaisevasti myös ylläpitäjän oma kokemuksen kautta hankittu tietotaito ja henkilökohtaiset mieltymykset. Eri jakeluissa tiedyt asiat, kuten ohjelmistojen asentaminen ja päivittäminen sekä varsinkin järjestelmän asetusten määrittely, tehdään toisistaan poikkeavasti. Tällöin ylläpitoa helpottaa, kun järjestelmä on ylläpitäjälle valmiiksi tuttu ja entuudestaan toimivaksi havaittu.

Muita valintakriteereitä saattavat olla käyttöjärjestelmän ja sen ohjeistuksen kieli. Yleensä käyttöjärjestelmän kielenä on kuitenkin syytä pitää englantia, sillä se on ylläpidon kannalta luontevin valinta ja lisäksi ongelmatilanteissa helpointa on löytää apua englanniksi. Myös kattavin ohjeistus eri toimenpiteisiin löytyy englanniksi eikä suomeksi.

Joillekin saattaa olla periaatteen vuoksi tärkeää, käytetäänkö käyttöjärjestelmässä ja sen oheisohjelmissa vain avoimen lähdekoodin ohjelmistoja vai myös suljettuja binääritiedostoja. Samoin jakelupaketin toimittajan omistussuhteet ja kaupalliset yhteistyökumppanit voivat vaikuttaa valintapäätökseen. Jotkut voivat nähdä esimerkiksi Red Hatin päättymisen IBM:n omistukseen negatiivisena asiana, kun taas toisille se voi olla merkki siitä, että kyseisen jakelupaketin tulevaisuus on entistä varmempi (Red Hat 2018).

Jakelupakettivaihtoehdot

Linux-jakelupaketteja on useita satoja, mutta ne perustuvat usein tiettyihin perusjakeluihin, joista on johdettu useita muita jakelupaketteja. Esimerkiksi ilmaiseen Fedoraan pohjautuu maksullinen Red Hat Enterprise Linux, josta on johdettu ilmainen CentOS sekä monia muita jakeluita. Debian-nimiseen jakeluun pohjautuu puolestaan ilmainen Ubuntu, johon perustuu muuan muassa työasemakäytössä suosittu ilmainen Linux Mint. Myös ilmaisen Opensusen ja kaupallisen Suse Linux Enterprisen eri versioiden kehitystyöt on sidottu toisiinsa. (Wikipedia 2019b.)

Jakelupakettien suosiota voidaan arvioida monella tavalla ja Internetistä löytyykin useita sivustoja, jotka listaavat eri käyttötarkoituksiin soveltuvia vaihtoehtoja (Distrowatch 2019; LWN 2019; Techradar Pro 2018). Käytännössä suosituksissa toistuvat usein samat vaihtoehdot, joista erityisesti yritysten palvelinkäyttöön soveltuvat seuraavat jakelupaketit:

- CentOS (ilmainen)
- Debian (ilmainen)
- Fedora Server (ilmainen)
- Opensuse (ilmainen)
- Red Hat Enterprise Linux (maksullinen)
- Suse Linux Enterprise Server (maksullinen)
- Ubuntu Server (ilmainen).

2.2 Palvelimen mahdollistamat toiminnot

Linux-käyttöjärjestelmällä varustettua palvelinkonetta voidaan käyttää lukuisiin eri käyttötarkoituksiin. Tavanomaisin käyttötarkoitus pienyrityksissä lienee tiedostojen jakaminen ja varmuuskopiointi lähiverkossa, mutta palvelinta voidaan käyttää myös tietoliikenneyhteyksien toteuttamiseen, jolloin sillä voidaan korvata myös reititin- ja palomuurilaitteet ja mahdollistaa etäyhteydet. Lisäksi palvelin voi huolehtia yrityksen sähköpostitileistä ja sen avulla on mahdollista toteuttaa erilaisia verkossa toimivia palveluita, kuten www-sivusto ja työaikaseurantajärjestelmä. Verrattuna ulkopuoliselta palveluntarjoajalta ostettuihin palveluihin ovat yrityksen omalle palvelimelle sijoitettujen palveluiden etuina yleensä räätälöitävyys yrityksen tarpeisiin ja tallennustilan edullisuus. Haittapuolena puolestaan on se, että omaa palvelinta ja sen ohjelmistoja täytyy ylläpitää säännöllisesti erityisesti riittävän tietoturvan takaamiseksi.

Tietoliikenneyhteydet

Linux-palvelimella voidaan korvata erillinen reitittimenä toimiva laite, kuten verkkopääte-laite, WLAN-reititin tai palomuurilaite. Silloin yksi sen verkkoliitännöistä määritellään toimimaan verkkokyttimeen liitettynä sisäverkon verkkoliitännänä ja toinen verkkoliitännä yhdistetään Internet-yhteyttä varten verkkopäätelaitteeseen, minkä jälkeen palvelin

pystyy välittämään tietoa verkon eri osien välillä. Palvelinta on tällöin mahdollista käyttää myös palomuurilaitteena, jolla pyritään estämään Internetin suunnasta tulevat asiattomat yhteydenotot yrityksen sisäverkkoon kytkettyihin laitteisiin ja jolla toisaalta voidaan valvoa myös sisäverkosta Internetiin suuntautuvaa liikennettä esimerkiksi mahdollisten haittaohjelmien havaitsemiseksi. Palvelin voi toimia myös IP-osoitteita lähiverkkoon liitetyille laitteille jakavana DHCP-palvelimena. Näistä toiminnoista kerrotaan tarkemmin luvussa 3.4.

Linux-palvelinta voidaan käyttää myös langattomana tukiasemana Hostapd-ohjelmiston avulla, jos siihen lisätään esimerkiksi USB- tai PCI Express -väyläisiä langattomia verkkosovittimia (Archlinux 2019). Kuitenkin yleisempi ratkaisu on käyttää erillisiä WLAN-tukiasemia, jolloin palvelimelle voidaan asentaa myös pelkkä tukiasemien hallintaohjelmisto. Silloin palvelin toimii vain tukiasemien kontrollerina. Yksi esimerkki tällaisesta ratkaisusta on Ubiquiti Networksin Unifi-tukiasemajärjestelmä, jota voidaan hallita omalle palvelimelle asennettavan Unifi Controller -ohjelmiston kautta (Ubiquiti Networks 2019a). Luvussa 4.2 kerrotaan asiakkaalle Unifi-järjestelmän avulla toteutetusta langattomasta verkosta.

Linux-palvelimelle voidaan myös asentaa ohjelmistoja, joiden avulla on mahdollista tarkkailla verkossa olevien laitteiden toimintaa. Suosittuja ilmaisia verkonvalvontaohjelmistoja ovat Cacti, Nagios ja Zabbix (Psychz Networks 2018). Valvontaohjelmisto voi lähettää sähköpostitse hälytyksen, mikäli johonkin laitteeseen ei enää saada yhteyttä tai jos esimerkiksi palvelintietokoneen levytila on loppumaisillaan tai sen kuormitus on kasvanut liian suureksi. Valvontaohjelmiston hallintasivuston kautta voidaan myös tarkkailla yrityksen sisäverkon ja Internet-yhteyden kuormitusta havainnollisten kuvaajien avulla. (Network Admin Tools 2018.)

Etäkäyttö

Linux-palvelin tarjoaa monia vaihtoehtoja yrityksen tiedostojen ja sen verkkoon liitettyjen laitteiden etäkäyttöön. Yksinkertaisimmillaan palvelimella säilytettävät tiedostot voidaan jakaa käyttäen esimerkiksi Linuxin mukana toimitettavaa SSHD-palvelinohjelmistoa (OpenSSH SSH Daemon), jolloin työasemat voivat ottaa siihen yhteyttä käyttäen asiakasohjelmistoa ja siirtää tiedostoja palvelimen ja työaseman välillä. OpenSSH:n avulla voidaan myös luoda salattu SSH-yhteystunneli työaseman ja yrityksen sisäverkon välille, jolloin työasemalta voidaan muodostaa yhteys sisäverkos-

sa olevaan laitteeseen (SSH Communications Security Oyj 2019b). Tämä toiminta mahdollistaa esimerkiksi yrityksen sisäverkossa olevan työaseman käyttämisen RDP-etätyöpöytäyhteyden avulla. SSH:n avulla toteutettavia etäkäyttömahdollisuuksia käsitellään tarkemmin luvussa 3.4.

SSH:n lisäksi etäyhteys työaseman ja yrityksen sisäverkon välille voidaan muodostaa käyttäen VPN-yhteyttä (Virtual Private Network), joka on julkisen Internetin läpi kulkeva salattu yhteys (Kaario 2002, 304). Linux-käyttöjärjestelmälle on saatavilla esimerkiksi OpenVPN-palvelinohjelmistosta ilmainen avoimen lähdekoodin Community-versio ja sitä tukevia työasemille asennettavia yhteysohjelmia on monille eri käyttöjärjestelmille (OpenVPN 2019). Kun työasemalta on muodostettu VPN-yhteys yrityksen sisäverkkoon, voidaan esimerkiksi siellä sijaitsevia verkkolevyjä ja tulostimia käyttää samaan tapaan kuin yrityksen sisäverkostakin. Sekä etäkoneen että palvelimen Internet-yhteyden nopeus kuitenkin käytännössä määrittelee, kuinka sujuvaa tiedostojen etäkäyttö Internetin välityksellä on.

Tiedostojen jakaminen ja tulostaminen

Palvelimen avulla voidaan jakaa sen kiintolevyillä sijaitsevat tiedostot lähiverkkoon liitettyjen työasemien käyttöön. Toiminnallisuus saadaan toteutettua Linuxissa käyttämällä Samba-ohjelmistoa, jolla jaetut hakemistot voidaan liittää Windows-työasemiin verkkolevyiksi (Samba.org 2019). Samban avulla palvelin voi toimia myös Active Directory -hakemistopalvelun Domain Controller -palvelimena verkkoon liitetyille Windows-työasemille, mikä mahdollistaa keskitetyn käyttäjä- ja laitehallinnan vastaavalla tavalla kuin Windows Server -käyttöjärjestelmää käyttävä palvelinkin (Tecmint 2019). Palvelinta voidaan käyttää myös tulostuspalvelimena ja jakaa siihen liitetyt sekä muut verkossa toimivat tulostimet työasemille käyttämällä Samban lisäksi CUPS-ohjelmistoa (Ubuntu 2019b).

Varmuuskopiointi

Työasemien tärkeitä tiedostoja voidaan kopioida palvelimelle myös käsin, mutta järkevintä on automatisoida ja ajastaa varmuuskopiointi tapahtuvaksi esimerkiksi kerran vuorokaudessa. Varmuuskopiointi voidaan toteuttaa esimerkiksi palvelinkoneella suoritettavalla yksinkertaisella komentosarjatiedostolla tai tähän tarkoitukseen tehdyllä oh-

jelmalla niin, että se ottaa yhteyttä työasemasta jaetuiksi määriteltyihin hakemistoihin ja kopioi niiden sisältämät tiedostot palvelimelle. Levyjakoja käyttävän ratkaisun etuna on se, ettei se vaadi työasemalle asennettavaa erillistä ohjelmistoa, minkä vuoksi se toimii käytännössä useimpien eri käyttöjärjestelmien kanssa. Lisäksi komentosarjatiedostoa voidaan räätälöidä vastaamaan juuri tietyn yrityksen vaatimuksia ja se voi hyödyntää apunaan muita Linux-palvelimelle asennettuja ohjelmia.

Varmuuskopiointi voidaan toteuttaa myös asentamalla työasemille erillinen asiakasohjelma, joka toimii yhteistyössä palvelimelle asennetun varmuuskopiointiohjelman kanssa. Näin toimii esimerkiksi suosittu avoimen lähdekoodin ohjelmisto Bacula, joka tarjoaa yksinkertaista komentosarjatiedostoa monipuolisemmat ominaisuudet varmuuskopiointiin ja erityisesti niiden hallinnointiin (Bacula.org 2019). Ohjelmistosta on saatavilla myös maksullinen versio Bacula Enterprise, joka tarjoaa ilmaisversiota monipuolisemmat ominaisuudet ja ennen kaikkea kattavat tukipalvelut (Bacula Systems 2019).

Myös palvelimella säilytettävien varmuuskopioiden ja työtiedostojen varmuuskopiointi yrityksen toimitilojen ulkopuolella sijaitsevalle tallennusvälineelle on erittäin tärkeää, jotta esimerkiksi toimitiloihin kohdistuneen murtautumisen tai tulipalon yhteydessä tiedot säilyvät tallessa. Varmuuskopiointi toimitilojen ulkopuolelle voidaan toteuttaa joko Internetin välityksellä tai käyttäen siirrettävää massamuistia, kuten USB-väyläistä kiintolevyä.

Sähköpostipalvelut

Linux-palvelinta voidaan käyttää yrityksen sähköpostien lähettämiseen, vastaanottamiseen ja säilyttämiseen sekä niiden roskapostisuodatuksen, virustorjunnan ja selainsähköpostin toteuttamiseen. Sähköpostien lähettämiseen ja vastaanottamiseen tarvitaan palvelimelle Mail transfer agent (MTA), joka ottaa sähköpostit vastaan käyttäjältä tai toiselta MTA:lta sekä välittää käyttäjän lähettämät sähköpostiviestit vastaanottajan sähköpostipalvelimelle SMTP-protokollaa käyttäen (IBM 2017). Yleisesti Linuxissa käytettyjä MTA-ohjelmia ovat Exim, Postfix ja Sendmail. MTA toimii usein myös MDA:na (Mail Delivery Agent), joka tallentaa palvelimella sijaitsevien sähköpostitilien viestit sähköpostilaatikoihin (Red Hat 2019a). Näiden sähköpostitilien viestejä käyttäjät voivat lukea ja poistaa käyttäen joko POP3- tai IMAP-protokollaa. Esimerkiksi Dovecot-ohjelma toimii POP3- ja IMAP-sähköpostipalvelimena, johon käyttäjät ottavat yhteyttä sähköpostiohjelmallaan eli MUA:lla (Mail User Agent) (Dovecot 2019). Sähköpostioh-

jelman lisäksi viestien hallinnoimiseen voidaan käyttää palvelimelle asennettavaa selainsähköpostia, joka on mahdollista toteuttaa esimerkiksi ohjelmilla Horde, Roundcube tai SquirrelMail.

Palvelimen välittämät sähköpostit voidaan myös suodattaa niin, että niistä erotellaan ja ohjelmistojen määryksistä riippuen myös poistetaan roskapostit ja viruksia sisältävät viestit ennen kuin ne tallennetaan käyttäjien sähköpostilaatikoihin. Nämä toiminnot voidaan toteuttaa esimerkiksi ohjelmien Amavis, Spamassassin ja Clamav avulla. (Ubuntu 2019a.)

Sähköpostipalveluiden toteuttaminen ja ylläpitäminen vaatii paljon osaamista, mutta etuna niiden hoitamisessa yrityksen omalla palvelimella on kuitenkin se, että käytössä on käytännössä rajattomasti tallennustilaa sähköposteille. Ulkopuolista palveluntarjoajaa käytettäessä riittävästä tallennustilasta pitää maksaa lisähintaa, jos sähköpostit halutaan säilyttää palvelimella. Sähköpostilaatikat kasvavat helposti useiden gigatavujen kokoisiksi varsinkin, jos isoja liitetiedostoja sisältäviä viestejä on paljon. Palveluntarjoajalta ostetut sähköpostipalvelut ovat kuitenkin monille yrityksille selvästi vaivattomin vaihtoehto ja luotettavasti toimivista palveluista maksettava hinta voi muodostua lisälevyttilan tarpeesta huolimatta kohtuulliseksi.

Esimerkiksi Sigmatic Oy:n arvonlisäverottomana 15 e/kk maksavaan Professional-webhotellipalveluun sisältyy 20 Gt tallennustilaa, joka on jaettu sähköpostilaatikoiden ja kotisivutilan kesken. Tallennustilan laajentaminen maksaa kuukaudessa 1,50 e/5 Gt. Jos yrityksellä on 20 sähköpostilaatikkoa, joista jokaiselle halutaan varata tilaa 10 Gt/kpl, tulee peruspakettiin sisältyvän tilan lisäksi tarvittavan 175 Gt:n lisäkustannukseksi 35 e/kk, jos huomioidaan vain sähköpostilaatikoiden viemä tallennustila. (Sigmatic 2019.)

WWW-sivusto ja muut verkossa toimivat palvelut

Palvelimelle voidaan sijoittaa myös yrityksen oma www-sivusto, joka muuten sijaitisi ulkopuolisen palveluntarjoajan palvelimella. Lisäksi sivustolla voi olla asiakkaiden ja yhteistyökumppaneiden palvelemista varten oma kirjautumista vaativa extranet-osio sekä vain yrityksen työntekijöitä palveleva intranet. Kaksi Linuxissa toimivaa suosittua www-palvelinohjelmistoa ovat Apache ja Nginx, jotka kumpikin ovat ilmaisia avoimen lähdekoodin ohjelmistoja (Blum & Bresnahan 2015, 66).

Yrityksen omassa käytössä oleva palvelinkone mahdollistaa myös monien muiden verkossa toimivien palveluiden toteuttamisen. Niitä voivat olla esimerkiksi asiakastietokanta, työaikaseuranta, laskutus, projektinhallinta ja kalenteri. Nämä palvelut voivat rakentua esimerkiksi www-palvelimen ja MySQL- tai MariaDB-tietokannan ympärille ja niiden toteuttamiseen voidaan käyttää saatavilla olevia valmiita ilmaisia tai maksullisia ohjelmistoja tai vaihtoehtoisesti juuri oman yrityksen käyttöön ohjelmoitua ratkaisua. Lisäksi palvelinta voidaan käyttää valvontakamerajärjestelmän hallintapalvelimena ja tallennustilana.

2.3 Palvelinkone

Linux-käyttöjärjestelmä itsessään ei vaadi paljoa laitteistolta, vaan laitteistovaatimukset määräytyvät pitkälti palvelimen käyttötarkoituksen ja sille asetettujen suorituskykyvaatimusten perusteella. Suositeltavaa on, että käytössä on 64-bittinen prosessori, vähintään 2 Gt keskusmuistia ja vähintään 5 Gt levytilaa käyttöjärjestelmälle ohjelmineen (Opensuse 2019a).

Peruskäyttöön, kuten tiedostopalvelimeksi ja reitittimeksi, riittää hieman vanhempikin tietokone, joka voi olla esimerkiksi yrityksen muutaman vuoden ikäinen työasema, joka halutaan uusida, koska työntekijä tarvitsee käyttöönsä suorituskykyisemmän uuden tietokoneen. Muuten käytöstä poistuvaa tietokonetta voidaan hyödyntää palvelintietokoneena, kunhan se varustetaan käyttötarkoituksen mahdollisesti vaatimilla laitteistokomponenteilla. Tällaisia komponentteja voivat olla esimerkiksi toinen verkkokortti ja kaksi suurikapasiteettista kiintolevyä vikasietoisuuden kasvattamiseksi RAID-järjestelmän avulla. Kuten luvussa 2.1 on kerrottu, laiteajurien saatavuus on syytä varmistaa ennen laitteiston osien hankintaa.

Vaativaankaan palvelinkäyttöön tulevan uuden koneen hankkiminen ei tule kalliiksi (liite 1). Tällaiseen käyttöön tarkoitettulta palvelinkoneelta vaaditaan erityisesti seuraavia ominaisuuksia:

- hyvän ilmanvaihdon omaava kotelo, jossa on riittävästi laajennustilaa kiintolevyille
- suorituskykyinen moniydinprosessori (vähintään neljä ydintä)
- keskusmuistia vähintään 8 Gt

- levyjärjestelmän vikasietoisuuden toteuttamiseksi vähintään kaksi kiintolevyä käytettäessä RAID-tasoa 1
- kaksi Ethernet-verkkoliitintä (esimerkiksi emolevylle integroitu verkkosovitin ja lisäkortti).

Omaa näyttöä palvelinkone ei välttämättä asennuksen jälkeen tarvitse, koska sitä voidaan hallita muiden verkkoon kytkettyjen tietokoneiden avulla. Tarvittaessa palvelimeen voidaan mahdollisten ongelmatilanteiden selvittämistä varten kytkeä väliaikaisesti jonkin toisen koneen näyttö.

Palvelimen vikasietoisuutta voidaan kasvattaa esimerkiksi kahdentamalla sen virtalähde. Eri palvelut voidaan myös hajauttaa useammalle palvelimelle, jolloin vikaantuneen palvelimen tehtävistä riippuen kaikki verkon palvelut eivät välttämättä keskeydy. Kahta palvelinta käytettäessä voi toinen niistä toimia varapalvelimena, joka voidaan ottaa käyttöön ensisijaisen palvelimen vikaannuttua.

Laitteet kannattaa sijoittaa metalliseen laitekaappiin, jossa ne ovat paremmin suojassa ulkoisilta vahingoilta. Lukittavissa oleva laitekaappi parantaa myös tietoturvaa, kun laitteisiin ei pääse fyysisesti käsiksi ilman lupaa. Samaan laitekaappiin voidaan palvelinkoneen ja varavirtalähteen lisäksi sijoittaa toimitilojen sisäverkkokaapeloinnin kytkentäpaneeli ja verkkolaitteet.

2.4 Vaihtoehtona Windows-palvelin

Opinnäytetyön lähtökohtana on monipuolisen tietojärjestelmän toteuttaminen pienellä budjetilla, mikä esimerkiksi toimeksiantajana toimivan pienyrityksen tapauksessa määrittelee käyttöjärjestelmävaihtoehdoksi ilmaisen Linuxin ja palvelimeksi edullisen, yleisesti saatavilla olevista osista kootun tietokoneen (liite 1). Vertailun vuoksi on kuitenkin hyvä tarkastella, millaisen vaihtoehdon Microsoftin maksullinen Windows Server 2019 -käyttöjärjestelmä ja yrityskäyttöön tarkoitettu valmis palvelinkone tarjoavat.

Jos yritys päättää käyttää palvelinratkaisunsa toteuttamiseen selvästi enemmän rahaa, voi vaihtoehtona olla Windows Server 2019 -käyttöjärjestelmällä varustettu valmis palvelinkone, kuten liitteessä 2 esitelty Dell EMC -merkkinen laite. Windows Server 2019:n hankintahintaan vaikuttavat mm. sen tukemat toiminnot ja tuettujen prosessoriytimien määrä.

Windows Server -käyttöjärjestelmä

Edullisin vaihtoehto Windows Server 2019 -käyttöjärjestelmästä on arvonlisäverottomana 354,76 e maksava Essentials-versio (liite 2), joka soveltuu käyttäjämäärältään riittävän pienelle yritykselle yksinkertaiseksi tiedosto- ja tulostuspalvelimeksi. Sen ominaisuuksia on kuitenkin karsittu kalliimpiin versioihin nähden, joten sen saa asentaa vain yhteen fyysiseen tai virtuaaliseen palvelimeen ja se tukee vain kahta prosessoria sekä enintään 64 Gt:n keskusmuistia. Lisäksi sen lisenssi edellyttää, että palvelinta käyttää enintään 25 käyttäjää tai 50 laitetta, mutta se ei vaadi kalliimmista versioista poiketen lisähintaan ostettavia CAL-käyttöoikeuslisenssejä. (Microsoft 2019a; 2019b.) Nämä rajoitukset eivät välttämättä ole esteenä pienimpien yritysten tapauksessa, mutta moni kalliimpien versioiden mahdollistama toiminto jää hyödyntämättä. Microsoftin mukaan Essentials -versiosta ei todennäköisesti enää tulevaisuudessa julkaista uudem-paa versiota, vaan käyttäjiä yritetään ohjata ostamaan kalliimpia versioita ja Microsoftin tarjoamia pilvipalveluita (Microsoft 2018b). Siitä johtuen edessä voi kuitenkin olla siirtyminen kalliimpaan vaihtoehtoon viimeistään nykyisen 2019-version tuen loppuessa.

Ominaisuuksiltaan Essentials-versiota monipuolisempi ja siten paremmin pienyrityksen käyttöön soveltuva Standard-versio 16 prosessoriytimen tuella maksaa arvonlisäverottomana 717,66 e (liite 2). Standard-version lisenssi mahdollistaa sen käyttämisen joko yhdessä fyysisessä palvelinkoneessa tai kahdessa virtuaalikoneessa. Sen avulla on siis sallittua asentaa kaksi virtuaalista Windows Server 2019 -palvelinta toimimaan yhdellä fyysisellä palvelimella, jonka käyttöjärjestelmänä voi olla saman lisenssin kattama Windows Server 2019 tai esimerkiksi ilmainen, mutta ominaisuuksiltaan yksinkertaisempi Microsoft Hyper-V Server 2019. (Microsoft 2019c.) Toimintojen jakaminen kahdelle eri virtuaalikoneelle parantaa järjestelmän vikasietoisuutta. Windows Server 2019 -käyttöjärjestelmävaihtoehdoista monipuolisin Datacenter maksaa 16 prosessoriydintä tukevana versiona arvonlisäverottomana 4 838,63 e (liite 2). Harva pienyritys kuitenkaan tarvitsee sen mahdollistamia lisätoimintoja, kuten rajoittamatonta määrää virtuaalikoneita (Microsoft 2019c).

Windows Server 2019 -versioiden Standard ja Datacenter tapauksessa on hankintakustannuksissa huomioitava myös niitä käyttävien käyttäjien ja laitteiden määrä, koska jokaista käyttäjää tai konetta varten on hankittava CAL-käyttöoikeuslisenssi. Käyttäjäperusteinen User CAL -lisenssi antaa käyttöoikeuden yhdelle käyttäjätunnukselle, jota voidaan käyttää useammalla laitteella. Laitteperustainen Device CAL -lisenssi puoles-

taan antaa käyttöoikeuden yhdelle laitteelle, jota voi käyttää useampi eri käyttäjä. (Microsoft 2019d.) Useimmissa tapauksissa sopivin valinta on hankkia jokaista käyttäjätun- nusta varten oma käyttäjäperusteinen lisenssi, joita myydään esimerkiksi viiden kappa- leen paketeissa arvonlisäverottomaan hintaan 179,76 e (liite 2).

16 prosessoriydintä tukevan Windows Server 2019 Standard -käyttöjärjestelmän ja 15 käyttäjäperustaisen CAL-lisenssin yhteishinta arvonlisäverottomana on 1 256,44 e (liite 2). Se on jo merkittävä lisäkustannus verrattuna ilmaiseen jakelupakettiin Linux- käyttöjärjestelmästä ja mitä enemmän palvelimella on käyttäjiä, sitä kalliimmaksi Win- dows Server -käyttöjärjestelmän hankinta tulee.

Windows-palvelimen toiminnot

Käyttöjärjestelmävalintana Windows Server ei rajaa pois kaikkia luvussa 2.2 esiteltyjä Linux-palvelimelle yleisimpiä toimintoja, vaan useimmat niistä voidaan toteuttaa myös Windowsissa. Tavanomaisten tiedosto- ja tulostinpalvelutoimintojen lisäksi Windows Server -palvelinta voidaan hyödyntää myös esimerkiksi Domain Controller -palvelimena Active Directory -hakemistopalvelussa, DNS-palvelimena ja DHCP-palvelimena (Microsoft 2019c). Windows-palvelin voi toimia myös yrityksen lähiverkon reitittimenä ja palomuurina, mutta sen käyttäminen siihen tarkoitukseen lienee melko harvinaista (Ex- perienicing IT 2019). Yrityksen työntekijöiden VPN-etäyhteydet voidaan toteuttaa Win- dowsin sisältämän Remote Access -ominaisuuden avulla (Microsoft 2019e).

Windows-palvelimella voidaan myös ajaa WWW-palvelinohjelmistoa, kuten Windowsiin sisältyvää Internet Information Services -ohjelmistoa tai samoja ilmaisia Apache- ja Nginx-ohjelmistoja kuin Linuxissakin (The Apache Software Foundation 2019; Microsoft 2019c; Nginx 2019). Myös Linuxista tutut ilmaiset tietokantaohjelmistot MySQL ja Ma- riaDB ovat käytettävissä maksullisen Microsoft SQL Serverin lisäksi (MariaDB 2019; Microsoft 2019f; MySQL 2019). Sähköpostipalvelut voidaan toteuttaa Microsoft Ex- change Server 2019:n avulla, mutta se on laitteistovaatimustensa ja hinnoittelunsa puolesta tarkoitettu lähinnä suuryrityksille, minkä vuoksi jollekin palveluntarjoajalle ul- koistetut sähköpostipalvelut ovat varsinkin pienyrityksille parempi vaihtoehto (BWW Media Group 2018).

Lähiverkkoon liitettyjen Windows-työasemien varmuuskopiointiin Windows Server 2019 -käyttöjärjestelmässä ei ole valmiita toimintoja, vaan varmuuskopiointi pitää to-

teuttaa jollakin erikseen hankittavalla maksullisella ohjelmistolla, joita on runsaasti saatavilla. Itse palvelin tiedostoiheen voidaan varmuuskopioida joko palvelimen omalle levyille tai verkkolevyille käyttäen esimerkiksi käyttöjärjestelmän mukana toimitettavaa Windows Server Backup -toimintoa, mutta se ei ole ominaisuuksiltaan kovin monipuolinen (Rootusers 2016). Suositeltavampaa onkin käyttää jotakin maksullista palvelinkäyttöjärjestelmän varmistukseen tarkoitettua ohjelmistoa.

Dell EMC -palvelinkone

Liitteessä 2 on esitelty palvelinkone Dell EMC PowerEdge T440, joka on varustettu vastaavalla kiintolevykapasiteetilla kuin liitteessä 1 esitelty Linux-palvelinkone. Tornimalliseen koteloon kootussa koneessa on prosessorina huomattavasti Linux-palvelinkoneen prosessoria tehokkaampi 8-ytiminen 2,1–3 GHz:n Intel Xeon Silver 4110, jonka tuomasta lisätehosta tosin ei ole merkittävää hyötyä tavanomaisessa tiedosto- ja tulostuspalvelinkäytössä, vaan sen edut tulevat esille vasta mahdollisia raskaampia sovellusohjelmia ajettaessa. Koneessa on myös vapaa paikka toiselle prosessorille, joten prosessoritehon lisääminen on tarvittaessa helppoa. Keskusmuistia koneessa on 8 Gt ja sen emolevyille on integroitu kaksi verkkoliitäntää.

Palvelimen kaksi pienempää kiintolevyä muodostavat 1 Tt:n RAID 1 -tason vikasietoisien levyjen käyttöjärjestelmäosiota varten ja työtiedosto-osiota varten suunniteltu 4 Tt:n RAID 1-tason levyjen muodostuu kolmesta kiintolevystä, joista yksi on varalla. Kiintolevyjä varten on koneen etuosassa kahdeksan paikkaa ja kiintolevyt ovat hot-plug-tyyppisiä eli ne voidaan vaihtaa yksitellen ilman palvelinkoneen sammuttamista. Kone mahdollistaa myös kahden virtalähteen käytön samassa kotelossa, joten vikasietoisuutta on parannettu Linux-palvelinkoneeseen verrattuna valitsemalla koneeseen kaksi virtalähdettä. Yhden virtalähteen vikaantuessa koneen toiminta jatkuu ennallaan toisen virtalähteen avulla ja vikaantunut virtalähde on vaihdettavissa uuteen koneen käydessä.

Palvelinkoneen esimerkkikokoonpanon arvonlisäveroton hinta on 3 156,55 e (liite 2). Hinta sisältää kolmen vuoden huoltolaajennuksen, joka tarjoaa perustakuuta kattavat huoltopalvelut ja nopeamman vasteajan, minkä myötä korjaustyöt suoritetaan asiakkaan tiloissa seuraavana arkipäivänä. Huoltolaajennuksen hankinta on perusteltua, koska koneessa käytettäviä laitteistokomponentteja ei ole saatavilla mistä tahansa alan liikkeestä toisin kuin yleisiä PC-tietokoneiden osia. Myös vikatilanteiden selvittä-

minen saattaa olla hidasta ja vaikeaa, jos ylläpitäjällä ei ole kokemusta nimenomaan saman valmistajan palvelimista.

Dell EMC -palvelinkoneen, Windows Server 2019 Standard -käyttöjärjestelmän sekä 15 käyttäjän CAL-käyttöoikeuslisenssien yhteishinta on 4 412,99 e arvonlisäverottomana (liite 2). Vastineeksi korkeammalle hinnalle ratkaisu tarjoaa laitteiston osalta edullista Linux-palvelinta paremman vikasietoisuuden, mahdollisesti laadukkaammat ja testatus- ti keskenään yhteensopivat laitteistokomponentit sekä tunnetun laitetoimittajan maksul- liset tukipalvelut. Windows Server -käyttöjärjestelmä puolestaan saattaa olla osalle IT- ylläpitopalveluja tarjoavista tahoista Linux-käyttöjärjestelmää tutumpi vaihtoehto, joka voi helpottaa tukipalveluiden hankkimista.

Eräs ratkaisu voi myös olla käyttää laitteistona edullista palvelinkonetta, mutta hankkia siihen maksullinen Windows Server -käyttöjärjestelmä. Kalliimpi vaihtoehtoinen ratkai- su puolestaan on hankkia valmis palvelinkäyttöön suunniteltu tietokone, mutta asentaa siihen Linux-käyttöjärjestelmästä joko ilmainen tai maksullinen jakelupaketti. Vaihtoeht- oja on joka tapauksessa monia ja lopulta hankintaan käytettävissä oleva rahamäärä ja halutut toiminnot ratkaisevat, millaisista osista kokonaisuus koostuu.

2.5 Palvelimen virtualisointi

Virtualisointi mahdollistaa yhden tai useamman ohjelmallisesti toteutetun tietokoneen eli virtuaalikoneen samanaikaisen toimimisen virtualisointialustalla, joka puolestaan toimii fyysisellä palvelinkoneella. Virtualisointialusta (engl. hypervisor) asennetaan siis fyysiselle isännäksi (engl. host) kutsutulle palvelinkoneelle ja alustalle luodaan vieraksi (engl. guest) kutsuttuja virtuaalikoneita. Virtuaalikoneet eivät näe fyysisen palvelimen laitteistoresursseja, kuten prosessoria, keskusmuistia, tallennustilaa ja verkkosovitti- mia, vaan ainoastaan alustan sille tarjoamat virtuaaliset resurssit. Virtuaalikoneelle asennetaan esimerkiksi Linux- tai Windows -käyttöjärjestelmä, jolle virtuaalikone näkyy tietokoneena samalla tavalla kuin fyysisenkin tietokone näkyisi. Käyttöjärjestelmän kannalta on siis sama asia, onko se asennettu todelliselle tietokoneelle vai virtuaaliko- neelle. (Portnoy 2016, 1–2, 37–38.)

Fyysiseen palvelimeen nähden virtualisoinnin etuina ovat mm. pienemmät laitteistoku- lut, pienempi laitetilän tarve ja alhaisempi sähkönkulutus ajettaessa yhdellä fyysisellä palvelinkoneella useampia virtuaalisia palvelimia. Fyysisen palvelimen laitteistoresurs-

sit saadaan hyödynnettyä huomattavasti paremmin virtuaalikoneiden avulla verrattuna siihen, että jokainen palvelin toimisi omalla fyysisellä palvelimellaan, jonka resursseja hyödynnettäisiin vain osittain. Virtuaalikoneille voidaan määritellä juuri sen verran prosessoritehoa, keskusmuistia ja tallennustilaa kuin ne tarvitsevat toimiakseen tehokkaasti (Portnoy 2016, 10–11.) Lisäksi uuden virtuaalipalvelimen käyttöönotto jo valmiiksi toiminnassa olevalle virtualisointialustalle on huomattavasti nopeampaa kuin uuden fyysisen palvelin, koska pois jäävät mm. uuden laitteiston tilaaminen, toimituksen odottaminen ja asentaminen laitetilaan. Myös jo olemassa olevasta virtuaalikoneesta voidaan luoda kopio uuden virtuaalikoneen pohjaksi, jolloin säästytään aikaa vievältä käyttöjärjestelmän asennusvaiheelta. (Portnoy 2016, 197.)

Palveluiden hajauttaminen useammalle virtuaalikoneelle lisää myös vikasietoisuutta, koska yhden virtuaalisen palvelimen vikaantuminen esimerkiksi ohjelmistovirheen seurauksena ei vaikuta muilla virtuaalikoneilla toimivien palveluiden toimintaan (Savill 2017, 9). Tällä tavalla menettelemällä voidaan esimerkiksi tiedostopalvelin pitää erillään tietokanta- tai varmuuskopiointipalvelimesta, jolloin myös tietoturva paranee, kun yhden palvelimen joutuminen tietomurron kohteeksi ei välttämättä altista muita palvelimia samalle uhalle. Hajauttaminen helpottaa myös ylläpitotoimia siltä osin, että yhden virtuaalipalvelimen käynnistäminen uudelleen ei mahdollisesti vaikuta kuin sille määriteltyihin toimintoihin.

Koska virtuaalikone on käytännössä vain kokoelma levyille tallennettuja tiedostoja, voidaan se varmistaa helposti kopioimalla kyseiset tiedostot esimerkiksi muualla sijaitsevaan tallennustilaan (Portnoy 2016, 198). Lisäksi snapshot-pikavarmuuskopioiden avulla virtuaalikoneen sen hetkinen tila voidaan tallentaa ja virtuaalikone voidaan helposti palauttaa kyseiseen tilaan myöhemmin (Portnoy 2016, 50–51). Toiminnosta on hyötyä esimerkiksi silloin, kun palvelimelle on tehty muutoksia, jotka aiheuttavat ongelmia sen toiminnassa.

Vikatilanteissa palvelin saadaan otettua nopeammin uudelleen käyttöön, kun virtuaalikone tai siitä otettu varmuuskopio voidaan palauttaa toimintaan nopeasti myös toisella fyysisellä palvelimella, jolle on asennettu yhteensopiva virtualisointialusta. Toisen fyysisen palvelimen ei siis tarvitse olla laitteistoltaan identtinen, vaan riittää, että virtualisointialusta toimii myös siinä. (Savill 2017, 6.) Virtualisointi mahdollistaa myös virtuaalikoneen siirtämisen jonkin palveluntarjoajan pilvipalveluun, mutta se vaatii riittävän nopean ja luotettavan Internet-yhteyden (Savill 2017, 10).

Markkinoilla on tarjolla useita ilmaisia ja maksullisia virtualisointialustoja. Suositusta Vmware Esxistä on olemassa kolme eri versiota, joista yksi on maksullinen, toinen 60 päivän kokeiluversio ja kolmas täysin ilmainen versio. Ilmaisversiossa on kuitenkin joi-takin toiminnallisia rajoituksia verrattuna muihin versioihin. (Altaro 2017.) Ilmaiseen, avoimen lähdekoodin Xen Projectiin puolestaan pohjautuu kaupallinen Citrix Xen -virtualisointialusta (Portnoy 2016, 31). Microsoft tarjoaa alustaksi sekä maksulli-sen Windows Server -käyttöjärjestelmänsä Hyper-V-ominaisuutta että ilmaista Hyper-V Server -nimistä vaihtoehtoa, joka ei vaadi erillisen Windows Server -lisenssin ostamis-ta, vaan sisältää itsessään pelkistetyn Core-version Windows Ser- ver -käyttöjärjestelmästä (Savill 2017, 29). Varteenotettava vaihtoehto virtualisointialus-taksi on myös ilmainen KVM (Kernel-based Virtual Machine), joka on osa Linuxia toi-mien sen ytimen kanssa ladattavien moduulien avulla. KVM:stä on olemassa myös maksullinen Red Hat -yrityksen myymä versio. (Red Hat 2019b.)

Laitteistovirtualisoinnilla on siis useita etuja, joiden perimmäisenä hyötynä yritykselle on laite- ja ylläpitokuluissa säästäminen. Saavutettava hyöty on sitä suurempi, mitä use-ampi fyysinen palvelin korvataan virtuaalikoneella. Jos tarkoituksena ei ole ajaa virtu-alisointialustalla kuin yhtä virtuaalikonetta, jäävät virtualisoinnin suurimmiksi eduiksi vikasietoisuuden parantuminen vikatilanteista palautumisen nopeutumisen myötä ja helpompi siirrettävyys laitteistolta tai palveluntarjoajalta toiselle. Virtualisointialusta vie myös oman osansa fyysisen palvelimen laitteistoresursseista, mutta sen vaatimukset vaihtelevat valitusta alustasta riippuen (Portnoy 2016, 23–25). Ylläpitäjältä vaaditaan riittävästi osaamista virtualisointialustan luomisessa ja hallinnassa, mutta virtuaaliko-neissa toimivien palvelimien ylläpito ei eroa fyysisten palvelimien ylläpitämisestä.

2.6 UPS-varavirtajärjestelmä

Sähköverkon häiriöt voivat aiheuttaa monenlaista haittaa yrityksen toiminnalle ja siksi niihin varautuminen on tärkeä osa yrityksen tietojärjestelmän toiminnan turvaamista. Ylijännite saattaa rikkoa laitteita ja äkillinen sähkökatkos voi aiheuttaa tärkeiden työtie-dostojen menetyksiä tai aiheuttaa virheitä tietojärjestelmän toiminnoissa. Joka tapauk-sessa sähkökatkos aiheuttaa ainakin katkoksen niihin yrityksen toimintoihin, joiden sähkönsyöttöä ei ole suojattu ja varmistettu.

Tietojärjestelmän keskeytymätön, sähköverkon häiriöistä riippumaton sähkönsyöttö voidaan järjestää UPS-varavirtajärjestelmällä, joka voidaan toteuttaa joko hajautetusti

tai keskitetysti. Keskitetyssä järjestelmässä UPS-laite on usein yhdistetty kiinteistön sähkökeskukseen ja virta laitteille tuodaan seinäpistorasioita hyödyntäen. (Eaton 2012.) Pienyrityksen palvelinkoneen ja sen yhteydessä olevien laitteiden, kuten verkkokytkimen ja Internet-yhteyden verkkopäätelaitteen, varmistamiseen kustannuksiltaan edullisin ratkaisu on kuitenkin hajautettu järjestelmä. Käytännössä se tarkoittaa esimerkiksi yhtä tai useampaa torni- tai rakkimallista UPS-laitetta, johon varmistettavat laitteet on liitetty suoraan laitteiden omilla virtajohdoilla.

UPS-laitteet jaetaan toteutustapansa perusteella kolmeen pääluokkaan, jotka ovat standby (off-line), line-interactive ja on-line (Wikipedia 2019c). Toteutustapa vaikuttaa myös laitteen hintaan. Halvimmat UPS-laitteet on toteutettu standby-tekniikalla. Ominaisuuksiltaan niitä parempien laitteiden tyyppi on line-interactive ja parhaimmat sekä samalla kalleimmat UPS-laitteet puolestaan käyttävät on-line-tekniikkaa. Line-interactive-tekniikalla toteutettu UPS on usein edullinen ja ominaisuuksiltaan riittävä valinta yksittäisen palvelinkoneen ja verkon aktiivilaitteiden varavirtajärjestelmäksi.

Vaadittavan varakäyntiajan ja UPS-laitteeseen liitettyjen laitteiden yhteenlasketun kuorman perusteella voidaan laskea, minkä kokoinen UPS-laite tarvitaan. Laittevalmistajien www-sivustoilla on laskureita, joiden avulla valinta helpottuu. (Eaton 2019.)

2.7 Tietoverkko

Kaapeloitu lähiverkko

Lähiverkon perustan muodostaa verkkokaapelointi. Useimmiten siirtomediana käytetään parikaapelia tai valokuitukaapelia, mutta myös radioaaltoja voidaan hyödyntää langattomissa WLAN-verkoissa. Suurimmassa osassa yritysten lähiverkkoja käytetään Ethernet-tekniikkaa ja verkon fyysinen toteutus on tähtimäinen, jossa jokainen laite on yhdistetty omalla verkkokaapelillaan verkon aktiivilaitteeseen, kuten verkkokytkimeen. (Paananen 2005, 223–226).

Verkkokaapelina hieman vanhemmissa verkoissa on kategoria 5e:n tai 6:n mukainen suojaamaton tai suojattu parikaapeli, joka käytännössä mahdollistaa siirtonopeuden 1 Gb/s. Vanhemmissa verkoissa siirtonopeus voi rajoittua arvoon 100 Mb/s johtuen kaapeloinnista, verkon aktiivilaitteista tai esimerkiksi tietokoneen verkkokortista. Myös valokuitukaapelia käytetään etenkin pitkillä etäisyyksillä yhdistämään verkon aktiivilait-

teita toisiinsa. (Paananen 2005, 229). Uudemmat verkot voi olla toteutettu myös jollakin uudemmalla parikaapelityypillä. Riittävän nykyaikainen kaapelointi ja uusinta tekniikkaa käyttävät laitteet mahdollistavat siirtonopeuden 10 Gb/s (Oliviero & Woodward 2014, 121).

Nykyään lähiverkon miniminopeutena voidaan pitää arvoa 1 Gb/s, jolloin verkon siirtokapasiteetti ei vielä muodostu pullonkaulaksi esimerkiksi varmuuskopiointia suoritettaessa tai suuria tiedostoja siirrettäessä.

Langaton lähiverkko

Langattomassa lähiverkossa eli WLAN:ssa laitteet siirtävät tietoa verkkokaapelin sijasta korkeataajuuksisia radioaaltoja eli mikroaaltoja käyttäen. Suurin osa langattomista lähiverkoista perustuu IEEE 802.11 -standardeihin, joista käytetään myös markkinointinimeä Wi-Fi. Ad-Hoc-tyyppisessä verkossa päätelaitteet keskustelevat suoraan keskenään ilman tukiasemaa, mutta yleisempi toimintatapa on infrastruktuuritila, jossa liikenne kulkee tukiaseman kautta. Tukiaseman tehtävänä on yhdistää langattoman ja langallisen verkon laitteet keskenään. (Al Agha ym. 2016, 154–156.)

Yritykselle langattoman lähiverkon käyttö tuo sekä etuja että haittoja. Merkittävin etu on se, ettei laitteen yhdistäminen verkkoon vaadi kaapelointia. Tällöin laitteet on mahdollista sijoittaa toimitiloissa vapaammin ja työntekijä voi helpommin työskennellä muualakin kuin oman työpöytänsä äärellä. Langattomuus mahdollistaa myös liikuteltavien laitteiden, kuten matkapuhelimien sekä tablettitietokoneiden, yhdistämisen lähiverkoon ja yleensä sitä kautta myös Internetiin. Lisäksi langattomuus tarjoaa uusia mahdollisuuksia myös erilaisten liikkuvien tuotanto- ja kuljetuskoneiden verkottamiseen. Myös yrityksen työntekijöiden, asiakkaiden ja yhteistyökumppaneiden omille laitteille voidaan luoda erillinen langaton vierasverkko, jonka kautta ne voivat olla yhteydessä Internetiin, mutta jonka kautta ne eivät pääse yrityksen sisäverkkoon. WLAN-verkon välityksellä voidaan hoitaa mobiililaitteiden yhteydet myös sellaisissa paikoissa rakennusten sisällä ja maan alla, jonne operaattorien matkapuhelinverkot eivät kuulu.

Langattomalla verkolla on myös haittapuolia, joista vaarallisim on langattomuuden aiheuttama tietoturvariski. Vaikka tietoliikenne hyvin toteutetussa langattomassa verkossa onkin suojattu riittävän vahvaa suojausmenetelmää ja hyvin muodostettua salasanaa käyttäen, saattaa ulkopuolinen taho saada selville verkon salasanan, jonka jälkeen hän

pääsee liittymään verkkoon. On myös mahdollista, että parhaimmastakin langattoman verkon suojausmenetelmästä löytyy tietoturva-aukko, jota yrityksen tietojärjestelmään tunkeutuja voi hyödyntää. Myös tietokoneiden jatkuva laskentatehon kasvu nopeuttaa verkon salasanan selvittämistä kokeilemalla.

WLAN-verkoissa käytetään usein yhtä tai useampaa tukiasemaa, jotka ominaisuuksistaan riippuen tukevat esimerkiksi 2,4 GHz:n ja 5 GHz:n taajuuksia. Taajuusalueet on jaettu kapeampiin osiin eli kanaviin, joita laitteet käyttävät. 2,4 GHz:n taajuusalueen ongelmana on kanavien vähäisestä määrästä ja kapeudesta johtuen sen ruuhkaisuus erityisesti käyttöpaikoissa, joissa on paljon langattomia verkkoja ja niiden käyttäjiä. (Al Agha ym. 2016, 175–179.) Ruuhkaisuus näkyy hitaampina siirtonopeuksina ja kasvaneina vasteaikoina. Myös erilaiset muista kuin verkkolaitteista johtuvat häiriöt ovat yleisiä 2,4 GHz:n taajuusalueella. Esimerkiksi mikroaaltouunit sekä langattomat puhelimet ja valaistusjärjestelmät saattavat aiheuttaa häiriöitä yhteyteen.

5 GHz:n taajuusalue mahdollistaa suuremmat siirtonopeudet ja koska käytettävissä olevia kanavia on enemmän, myös ruuhkaisuudesta johtuvat ongelmat vähenevät. Ongelmana korkeampaa taajuutta käytettäessä on kuitenkin se, että verkon kuuluvuus heikkenee, koska erilaiset esteet, kuten seinät, vaimentavat signaalia enemmän verrattuna 2,4 GHz:n taajuuteen. Siirtonopeuden ja kuuluvuuden ongelmia pystytään kuitenkin hallitsemaan käyttämällä useita oikein sijoiteltuja ja määriteltyjä tukiasemia. (Wikipedia 2019d.)

Verkon aktiivilaitteet

Yrityksen verkon aktiivilaitteita voivat olla esimerkiksi verkkokytkin, langattoman verkon tukiasema, reititin, palomuurilaite ja Internet-yhteyden muodostava verkkopäätelaite. Osa näiden laitteiden toiminnoista voi olla integroituna myös samaan laitteeseen.

Lähiverkossa verkkokaapelilla kiinni olevat laitteet yhdistetään toisiinsa yhden tai useamman verkkokytkimen kautta. Kytkin voi olla erillinen laite tai se voi olla pienimmissä toteutuksissa sisäänrakennettu esimerkiksi WLAN-reitittimeen tai palomuurilaitteeseen. Osa verkkokytkimistä on hallittavia, jolloin niiden asetuksia pääsee muuttamaan ja liikennettä valvomaan pääteyhteydellä tai hallintasivuston kautta www-selaimella. Hallintaominaisuudet mahdollistavat sellaisten tietoturvaa parantavien ratkaisujen kuin virtuaalilähiverkkojen (VLAN) käyttämisen. Lisäksi kytkin voi tukea liikenteen priorisointia

sen luokittelun perusteella, jolloin esimerkiksi VoIP-puheluiden paketeille voidaan määrittellä ensisijaisuus muuhun vähemmän kriittiseen liikenteeseen nähden. Myös vikatilanteiden selvittäminen helpottuu, kun laitteen hallintasivustolta voidaan tarkistaa yksittäisen kytkinportin tila ja siihen kytketyn laitteen MAC-osoite.

Verkkokytkin voi myös tukea Power over Ethernet -ominaisuutta (PoE), jossa laitteelle syötetään sen tarvitsema käyttö sähkö samaa verkkokaapelia pitkin, jota se käyttää tietoliikenteeseensä (Oliviero & Woodward 2014, 98). Tällöin PoE-ominaisuutta tukevan laitteen, kuten langattoman verkon tukiaseman, IP-puhelimen tai valvontakameran, asennus yksinkertaistuu, koska se ei tarvitse erillistä virtajohtoa, vaan pelkän verkkokaapelin vetäminen käyttöpaikkaan riittää. Mikäli yrityksen on tarkoitus käyttää vain yhtä tai kahta PoE-laitetta, ei sen välttämättä kannata maksaa kytkimen PoE-ominaisuudesta ylimääräistä. Laitteiden virransyöttö voidaan nimittäin hoitaa myös sähköpistorasiaan kytkettävän PoE-injektorin avulla, jonka kautta laitteen verkkoyhteys kytketään. Lisäksi on tarjolla hieman edullisempia kytkinmalleja, joiden verkkoporteista vain osa tukee PoE-ominaisuutta.

Reititin on laite, joka yhdistää verkkoja välittäen tietoa verkon eri osien, kuten lähiverkon ja Internetin, välillä (Cisco 2019). Tällöin reitittimen yhteen porttiin on yhdistetty yrityksen lähiverkko ja toiseen porttiin Internet-yhteyden verkkopäätelaite. Varsinkin pienemmissä yrityksissä reitittimen tehtävät kuitenkin usein hoitaa esimerkiksi palomuurilaite. Palomuurin tehtävänä on tarkkailla sen kautta kulkevaa tietoliikennettä ja tarvittaessa estää datapakettien kulku verkosta toiseen ennalta määriteltujen sääntöjen ja asetusten perusteella. Sääntöjen avulla voidaan esimerkiksi sallia pääsy Internetistä vain tiettyihin yrityksen sisäverkon palvelimella käytössä oleviin palveluihin, kuten www-sivustolle. Myös lähiverkosta Internetiin suuntautuvaa liikennettä on syytä tarkkailla ja hallita, jotta esimerkiksi lähiverkon koneille päässeiden haittaohjelmien toimintaa voitaisiin rajoittaa. Palomuurilaite toimii usein myös DHCP-palvelimena jakaen IP-osoitteita lähiverkkoon liitetyille laitteille ja sen avulla voidaan toteuttaa myös VPN-etyhteydet yrityksen lähiverkkoon.

WLAN-tukiasema yhdistää langattoman lähiverkon laitteet osaksi muuta verkkoa. Tukiasema on liitetty verkkoon joko verkkokaapelilla tai langattomasti toisen WLAN-tukiaseman tai esimerkiksi mobiiliverkon välityksellä. WLAN-tukiasemat toimivat esimerkiksi taajuuksilla 2,4, 5 ja 60 GHz riippuen siitä, mitä IEEE 802.11 -standardia ne tukevat (Al Agha ym. 2016, 185). Tukiaseman valinnassa kannattaa kiinnittää huomiota sen tukemiin langattoman verkon standardeihin sekä radioiden että antennien mää-

rään, jotka vaikuttavat verkossa saavutettavaan tiedonsiirtonopeuteen. Tukiaseman asennusta helpottaa, mikäli sen käyttösähkö voidaan syöttää verkkokaapelia käyttäen PoE-ominaisuuden avulla. Monen tukiaseman ratkaisussa voi olla joskus myös tarpeen käyttää niin sanottua Mesh-ominaisuutta, jossa osa tukiasemista voi olla liitetty lähiverkkoon langattomasti toisen tukiaseman kautta.

Mikäli langattoman verkon suunniteltu toimialue on laaja ja sisältää paljon radiosignaalia vaimentavia rakenteita, voi olla tarpeen käyttää useampia tukiasemia. Tällöin itsenäisesti toimivien tukiasemien sijasta järkevämpi valinta ovat osana yhtenäistä järjestelmää toimivat tukiasemat, jolloin erillisiin tukiasemiin verrattuna voidaan paremmin hallita muun muassa päätelaitteen siirtymistä tukiasemalta toiselle kuuluvuuden heikentyessä. Yhtenäisen langattoman verkon järjestelmän etuihin lukeutuvat myös keskitetty asetusten määrittely sekä mahdollisuus tarkkailla ja rajoittaa liikennettä kätevästi järjestelmän hallintasivuston tai mobiililaitteessa toimivan ohjelman välityksellä. Esimerkiksi langattoman verkon nimi, salasana tai kanava voidaan muuttaa hallintasivuston kautta, josta asetukset siirtyvät järjestelmään liitettyihin tukiasemiin.

Lähiverkko yhdistetään Internetiin verkkopäätelaitteella, joita voivat olla esimerkiksi lankapuhelinverkon kaapelointia hyödyntävä DSL-modeemi, kaksisuuntaisen kaapelitelevisioverkon kaapelimodeemi, valokuituyhteyden kuitupäätelaite tai mobiililaajakaistareititin. Verkkopäätelaite voi sisältää myös muita toimintoja, kuten WLAN-tukiaseman, reitittimen ja palomuurin. Pienyrityksessä ei siis välttämättä tarvita kuin esimerkiksi kuitupäätelaite tai mobiililaajakaistareititin, jonka Ethernet-verkkoliitäntöihin lähiverkon laitteet kytketään. On kuitenkin syytä tiedostaa, että edullinen kuluttajakäyttöön tarkoitettu yhdistelmälaite ei ole yhtä monipuolinen ja luotettava kuin yrityskäyttöön tarkoitettut erillislaitteet.

3 SUUNNITTELU

3.1 Tapaus yritys X

Opinnäytetyössä toteutettiin Varsinais-Suomessa toimivalle reilun kymmenen työntekijän pienyritykselle hanke, joka sisälsi yrityksen vanhan tietojärjestelmän uudistamisen. Yritys kuuluu kansainväliseen konserniin ja toimii meriteollisuuden alalla sekä valmistaen itse tuotteita että tarjoten suunnittelu- ja huoltopalveluita kansainvälisillä markkinoilla. Asiakasyritys halusi pysyä nimettömänä, koska sen tietojärjestelmän yksityiskoh- taisten tietojen paljastaminen aiheuttaisi tietoturvariskin.

Kokonaisvaltaisen tietojärjestelmä uudistuksen sijasta toimeksianto keskittyi pitkälti vanhan tiedostopalvelimen korvaamiseen uudella palvelimella, joka mahdollisti myös monia muita toimintoja tiedostojen jakamisen lisäksi. Lisäksi käytössä olleet kaksi verkkokytkintä korvattiin yhdellä uudella verkkokytkimellä ja langaton reititin vaihdettiin kahdesta erillisestä tukiasemasta koostuvaan järjestelmään, jonka toiminnan tarkkailu ja hallintatoimenpiteet voidaan hoitaa keskitetysti.

3.2 Vanha tietojärjestelmä

Palvelinkone

Toimeksiantajayrityksellä oli käytössään vuonna 2011 käyttöönotettu palvelinkone, jonka Linux-käyttöjärjestelmänä toimi Opensuse 12.1. Kyseisen käyttöjärjestelmäversi- on päivityspakettien jakelu oli loppunut jo vuonna 2013, mikä muodosti merkittävän tietoturvauhan, koska se merkitsi samalla sitä, ettei sen jälkeen havaittuja tietoturva- aukkoja ollut korjattu (Opensuse 2019b).

Palvelin oli rakennettu vain yrityksen sisäverkon tiedostopalvelimeksi ja vaikka sen osia oli vuosien varrella vaihdettu uusiin rikkoutumisen vuoksi ja levytilan kasvattamiseksi, oli laitteiston pohjana edelleen vanha työasematietokone vuodelta 2008. Lähes kym- menen vuoden iästä johtuen koneen laitteistokomponentteja olisi todennäköisesti jou- duttu uusimaan lisää lähitulevaisuudessa. Koneen korjauksesta aiheutuneet toiminta-

katkokset olisivat puolestaan haitanneet merkittävästi yrityksen toimintaa aiheuttaen myös taloudellista tappiota.

Työasemat ja muut laitteet

Yrityksen työntekijöillä oli käytössään 12 työasemaa, joista neljä oli kannettavia tietokoneita. Koneiden käyttöjärjestelmänä oli Windows 10. Vaikka osa koneista oli jo yli viisi vuotta vanhoja, työntekijät olivat pääosin tyytyväisiä niiden toimintaan ja suorituskykyyn.

Lähiverkkoon oli kytketty verkkokaapelilla myös kaksi monitoimilaitetta ja niiden lisäksi kaksi pienempää tulostinta. Lisäksi osa työntekijöiden puhelimista käytti yrityksen langatonta sisäverkkoa.

Lähiverkko ja Internet-yhteys

Käytössä ollut Ethernet-lähiverkko oli verkkotopologialtaan tähtimäinen ja se oli toteutettu kategorian 5e mukaisella suojaamattomalla parikaapelilla, joka käytännössä mahdollisti siirtonopeuden 1 Gb/s. Verkon osia yhdistivät kaksi 8-porttista hallitsematonta verkkokytintä, jotka oli sijoitettu lukittavaan laitekaappiin, jossa olevaan kytkentäpaneeliin myös lähiverkon kaapeloinnit ja puhelinliittymä oli päätetty. Toinen kytkimistä tuki vain nopeutta 100 Mb/s, mikä hidasti varsinkin siihen liitettyjen työasemien varmuuskopiointia palvelinkoneelle. Kaikkien laitekaapissa olevien laitteiden virransyöttö oli varmistettu UPS-laitteella APC Back-UPS RS Pro 1500 VA.

Verkon reitittimenä ja langattomana tukiasemana toimi WLAN-reititin Asus RT-N66U, joka jakoi verkkoon liitetuille laitteille DHCP-menetelmää käyttäen sisäverkon IP-osoitteet. Erillistä vierasverkkoa ei ollut, vaan langattomasta verkosta oli suora pääsy yrityksen sisäverkkoon, mikä muodosti merkittävän tietoturvariskin.

Yrityksen Internet-yhteys oli toteutettu yritystason ADSL-yhteydellä, jonka nopeus oli 8/1 Mb/s ja jossa oli kiinteä julkinen IP-osoite. ADSL-päätelaite oli teleoperaattorin toimittama vuokralaite.

3.3 Vaatimusten määrittely

Hanke aloitettiin selvittämällä, millaisia tarpeita, vaatimuksia ja toiveita toimeksiantajalla oli uuden tietojärjestelmän osalta. Lähtökohtana pidettiin vanhaa palvelinta ja sen avulla toteutettuja toimintoja.

Toimeksiantaja oli tyytyväinen vanhan palvelimen Linux-käyttöjärjestelmän toimintavarmuuteen ja itse valituista osista kootun palvelinkoneen luotettavuuteen sekä kokonaisratkaisun edullisiin hankinta- ja ylläpitokuluihin. Sen vuoksi käyttöjärjestelmäksi haluttiin edelleen ensisijaisena vaihtoehtona Linux, vaikka käyttöjärjestelmävaihtoehtona tarkasteltiin myös luvussa 2.4 tarkemmin käsitellyä Windows Server 2019 Standard -käyttöjärjestelmää. Windowsin tapauksessa käyttöjärjestelmän ja tarvittavien käyttöoikeuslisenssien hinnaksi olisi kuitenkin muodostunut arvonlisäverottomana 1 256,44 e (liite 2) ja toisaalta Windowsin valitseminen olisi käytännössä rajannut pois uuden palvelinkoneen käyttämisen palomuurina ja reitittimenä. Windowsiin päätyminen olisi myös merkinnyt työasemien varmuuskopiointin järjestämistä jollakin maksullisella Windowsissa toimivalla varmuuskopiointiohjelmalla.

Vanhasta palvelinkoneesta oli koko sen käyttöaikana uusittu vain virtalähde. Sekin saatiin vaihdettua saman työpäivän aikana uuteen, koska kyse oli standardin mukaisesta osasta, jonka pystyi hankkimaan mistä tahansa alan liikkeestä tai kiireellisessä tapauksessa vaihtamaan esimerkiksi vähemmän tärkeästä työasematietokoneesta. Asiakkaan toiveena kuitenkin oli, että esimerkiksi tavanomaisten osien hajoamisesta johtuvat käyttökätköt saataisiin pysymään mahdollisimman lyhyinä. Siksi yhtenä vaihtoehtona harkittiin myös nimenomaan palvelinkäyttöön suunniteltua tietokonetta, joka on esitelty luvussa 2.4. Dell EMC PowerEdge T440 -palvelinkone olisi tarjonnut enemmän suorituskykyä ja vikasietoisuutta, mutta hankinnan esteeksi muodostui laitteiston korkea hankintahinta, joka olisi ollut arvonlisäverottomana 3 156,55 e (liite 2). Kustannussyistä laitteistoksi valittiin siis itse koottu tietokone valmiin palvelinkoneen sijasta.

Yritys halusi pitää tiedostot toimipaikkansa vartioiduissa tiloissa sijaitsevilla omissa laitteillaan, mikä sulki pois fyysisesti muualle sijoitetun etä- tai virtuaalipalvelimen käytön. Lisäksi rajoittavana tekijänä pilvipalveluiden käytölle oli Internet-yhteyden nopeus, koska yrityksen toimipaikkaan ei ollut saatavilla valokuituliittymää.

Palvelimen tärkeimmiksi tehtäviksi määriteltiin edelleen työtiedostojen jakaminen lähiverkossa ja työasemien ajastettu varmuuskopiointi. Vanhan palvelimen työtiedostojen

tallentamiseen ja työasemien varmuuskopiointiin käytetty levytila oli kuitenkin käynyt vähiin, joten sen määrää haluttiin lisätä vastaamaan muuttuneita tarpeita. Myös vanha palvelinkone haluttiin säilyttää toiminnassa, mikä vaati sen osittaista uudistamista. Etäkäytön osalta riitti, että tiedostoihin pääsi käsiksi Internetin kautta ja että tarvittaessa työasemille voitiin muodostaa myös etätyöpöytäyhteys.

Edullisen kuluttajakäyttöön tarkoitetun WLAN-reitittimen käyttäminen reitittimenä koettiin riskiksi sekä tietoturvalle että verkon toiminnalle. Siitä johtuen Linux-palvelimen haluttiin toimivan myös reitittimenä ja lähiverkon laitteille IP-osoitteita jakavana DHCP-palvelimena. Lisäksi Linuxin palomuurin todettiin mahdollistavan aiempaa laitetta monipuolisemmat palomuurisäännöt sekä etäyhteyksien toteuttamisen monella eri tavalla.

Vanhan WLAN-reitittimen avulla toteutetun langattoman verkon nopeutta ja tietoturvaa sekä erityisesti kantamaa isoissa toimitiloissa haluttiin parantaa sekä luoda vierailijoita ja työntekijöiden omia laitteita varten erillinen vierasverkko, josta ei olisi pääsyä yrityksen lähiverkon laitteisiin ja palveluihin. Vaikka useita vuosia vanhaan langattoman verkon reitittimeen olikin vielä säännöllisesti julkaistu uusia tietoturvapäivityksiä, oletettiin niiden julkaisun kuitenkin vähitellen harvenevan ja lopulta loppuvan kokonaan lähivuosina tuotteen vanhenemisen myötä. Lisäksi laitteen päivitysten asentaminen käsin laitteen hallintasivuston kautta ilman automaattista toimintoa koettiin käytännössä liian hankalaksi, minkä vuoksi päivityksiä ei aiemminkaan ollut asennettu riittävän säännöllisesti.

Laitteiston toimintavarmuudesta ja tietoturvallisuudesta haluttiin huolehtia aiempaa paremmin, joten erilaisia vikatilanteita sekä esimerkiksi tietoturvapäivitysten ja käyttöjärjestelmän versiopäivitysten asentamista varten haluttiin luoda säännöllinen ylläpitosuunnitelma. Kuten aiemmin tässä alaluvussa todettiin, myös yleisimpien laitteistovikojen korjaaminen mahdollisimman nopeasti määriteltiin yhdeksi tavoitteeksi. Lisäksi sekä toimeksiantajan että sen IT-järjestelmän toiminnasta huolehtivan tahon toiveena oli, että ohjelmistopäivitykset ja järjestelmän asetuksiin tehtävät muutostyöt voitaisiin mahdollisimman usein tehdä etäyhteyden avulla, jolloin säästyisi sekä aikaa että rahaa.

Uuden järjestelmän käyttöönotto haluttiin tehdä siten, että siitä käyttökatkojen muodossa yrityksen liiketoiminnalle aiheutuvat haitat olisivat mahdollisimman pieniä. Tärkeänä toimeksiantaja piti myös sitä, että käyttöönottovaiheessa yrityksen työntekijät voisivat tarvittaessa pyytää apua toimeksiannon toteuttajalta. Käyttöönoton jälkeen käyttäjien tueksi toivottiin riittävää ohjeistusta ainakin yleisimpiin ongelmatilanteisiin.

Alustavien laskelmien jälkeen laitehankintoihin budjetoitiin rahaa yhteensä 2000 e arvonlisäverottomana, josta uuden palvelinkoneen osiin varattiin puolet. Loput rahamäärästä suunniteltiin käytettäväksi lähiverkon parantamiseen, uuden langattoman verkon laitteisiin sekä vanhan palvelinkoneen uudistamiseen. Myös järjestelmän asennus- ja määrittelytöiden kustannukset arvioitiin.

3.4 Uusi tietojärjestelmä

Uuden tietojärjestelmän keskeisenä osana oli uusi palvelinkone, joka suunnittelultaan ja toiminnoiltaan pohjautui pitkälti vanhaan palvelinkoneeseen, jonka toimintaan toimeksiantaja oli ollut tyytyväinen. Työtiedostojen ja varmuuskopioiden tallentamiseen käytettävän levytilan määrää oli kuitenkin tarpeen kasvattaa ja toimintavarmuutta lisätä tilanteissa, joissa osa kiintolevyistä vioittuisi. Ikääntyneen laitteiston uusimisella pyrittiin muutenkin pienentämään laitteistovioista aiheutuvaa riskiä toiminnalle. Palvelimen uusiksi toiminnoiksi määriteltiin tietoliikenteen reitittäminen sekä DHCP-palvelimena ja palomuurina toimiminen.

Yrityksen langaton lähiverkko päätettiin uusida ottamalla käyttöön uudet tukiasemat, joiden avulla toteutetussa ratkaisussa olisi korjattu aiemmin havaitut puutteet ja ongelmat. Myös langallista lähiverkkoa uudistettiin ottamalla käyttöön uusi verkkokytkin. Käyttäjien työasemia, monitoimilaitteita tai tulostimia ei tämän toimeksiannon yhteydessä uusittu. Työasemiin tehtävät muutokset rajoittuivat Windows-käyttöjärjestelmän verkkolevyjen määrittelyjen uusimiseen uuden palvelimen käyttöönoton jälkeen.

Varsinaista kattavaa riskienhallintasuunnitelmaa ei laadittu, mutta eri laitteiden ja toimintojen yhteydessä pyrittiin huomioimaan mahdolliset riskit ja pohdittiin, miten ne voitaisiin minimoida hyväksyttävälle tasolle. Suunnitelluissa ratkaisuissa huomioitiin myös tietoturva kiinnittäen erityistä huomiota salasanojen vahvuuteen sekä eri toimintojen ja laitteiden käytön rajaamiseen vain niille käyttäjille, jotka niitä tarvitsivat.

Uusi palvelin

Toimeksiantajan esittämänä vaatimuksena oli, että palvelinkoneen osien mahdollisesta rikkoutumisesta johtuvien vikatapausten aiheuttamat käyttökatkot jäisivät mahdollisimman lyhyiksi. Erityisesti palvelinkäyttöön suunniteltu ja siten tavallista tietokonetta vi-

kasietoisempi valmis palvelinkone oli kuitenkin tässä tapauksessa liian kallis vaihtoehto. Eräs ratkaisu järjestelmän vikasietoisuuden lisäämiseksi olisi ollut kahden uuden rinnakkaisen fyysisen palvelinkoneen hankkiminen, mutta se olisi lisännyt kustannuksia tuntuvasti ja aiheuttanut myös lisätyötä järjestelmän toiminnan määrittelyssä.

Myös luvussa 2.5 käsiteltyä palvelimen toteuttamista virtuaalipalvelimena harkittiin, mutta se päätettiin kuitenkin lopulta jättää tekemättä. Virtualisoinnin avulla olisi ollut mahdollista parantaa vikasietoisuutta, nopeuttaa järjestelmän ottamista uudelleen käyttöön vikatilanteen jälkeen ja helpottaa esimerkiksi palvelimen varmuuskopiointia. Laitteiston hankintakuluissa olisi kuitenkin säästetty vasta, jos nyt yhdelle palvelimelle määritellyt toiminnot olisi hajautettu useammalle palvelimelle, mikä puolestaan olisi lisännyt asennuksen ja ylläpidon vaatimaa työmäärää. Lisäksi itselläni ei ollut riittävästi käytännön kokemusta virtualisoinnin toteuttamisesta käytettävissä olevilla ilmaisilla virtualisointialustoilla, joten yrityksen tuotantokäyttöön tulevaa järjestelmää ei haluttu käyttää uusien menetelmien toimivuuden testaamiseen.

Laitteistovikatilanteista toipumista päätettiin nopeuttaa hankkimalla varalle toinen virtualähde. Myös kiintolevyjen määrää lisättiin niin, että työtiedostojen tallennukseen käytetty RAID-levypakka sietäisi kahden kiintolevyn hajoamisen ilman toiminnan keskeytystä ja tietojen menettämistä.

Edullisen Linux-palvelimen pohjana voidaan usein hyödyntää myös vanhaa työasemakäytössä ollutta tietokonetta, mutta toimeksiantajan tapauksessa laitteisto päädyttiin kokoamaan uusista osista, jotta laitteiston oletettu käyttöikä olisi mahdollisimman pitkä ja koska kokoonpanon hinta muodostui edulliseksi. Liitteessä 1 esitellyn laitteistokokoonpanon osien arvonlisäveroton hinta oli 1 044,91 e ilman varalle hankittua toista virtualhdettä. Kevyeen palvelinkäyttöön sopivat osat valittiin harkiten ja tarkistaen, ettei esimerkiksi emolevylle integroitujen toimintojen ja erillisen verkkokortin osalta ollut tiedossa olevia yhteensopivuusongelmia käyttöjärjestelmän kanssa.

Kaksi 1 Tt:n kiintolevyä muodostavat käyttöjärjestelmän tiedostojen käyttöön varatun RAID 1 -tason levypakan eli loogisen tallennustilan, joka näkyy käyttöjärjestelmälle yhtenä 1 Tt:n kokoisena kiintolevynä. RAID 1 -tason järjestelmässä tiedostot tallennetaan kahdelle tai useammalle kiintolevylle, jolloin tiedostot säilyvät niin kauan kuin levypakassa on yksikin ehjä kiintolevy (Linux Raid Wiki 2019). Kolme 4 Tt:n kiintolevyä hankittiin yrityksen työtiedostojen säilyttämistä varten. Kiintolevyt muodostavat 4 Tt:n RAID 1 -levypakan, jossa kolmas levy on varalla, jolloin se voidaan ottaa käyttöön vi-

kaantuneen kiintolevyn tilalle joko automaattisesti tai ylläpitäjän toimesta. Kiintolevyiksi valittiin edulliset, omakohtaisen kokemuksen perusteella aiemmissä käyttökohteissa luotettaviksi havaitut ja hyvin myös testeissä pärjänneet Western Digitalin mallit. Ne eivät tarjoa aivan parhaita suorituskykyä, vaan ne on suunniteltu luotettaviksi levyiksi tallennusjärjestelmien käyttöön (Storagereview 2013).

Intelin Z370-piirisarjaa käyttävälle Asuksen emolevylle on integroitu kuutta levyä tukeva Serial ATA -kiintolevyohjain, joka voi tarvittaessa toimia myös RAID-ohjaimena. Tässä tapauksessa päädyttiin sen sijaan hyödyntämään Linuxin ohjelmistopohjaista RAID-ratkaisua. Sen etuna emolevyn piirisarjaan integroituun tai erillisellä lisäkortilla toteutettuun ohjaimen verrattuna on muun muassa se, että tarvittaessa kiintolevyt RAID-pakkoineen voidaan helposti ottaa käyttöön toisessa Linux-tietokoneessa ilman, että siinä pitäisi olla käytössä samanlainen kokonaan tai osittain laitteistolla toteutettu RAID-ohjain (Gentoo Linux 2019).

Proessoriksi valikoitui Intelin Core i3 -sarjan neliydinprossessori, joka edullisesta hinnasta huolimatta tarjoaa palvelimelle määriteltyn käyttöön riittävästi suorituskykyä. Näytönohjaimena hyödynnetään emolevyn ja sen piirisarjan tukemaa prosessoriin integroitua Intel UHD Graphics 630 -grafiikkasuoritinta. Emolevylle integroidun verkko-ohjaimen lisäksi kokoonpanoon valittiin Intelin piirisarjaan perustuva PCI Express -väyläinen verkkokortti, jotta palvelinta voitaisiin käyttää reitittimenä erottaen sisä- ja ulkoverkkojen tietoliikenne omiin verkko-ohjaimiinsa. DDR4-keskusmuistia kokoonpanoon laitettiin 8 Gt ja siihen asennettiin varmuuden vuoksi myös DVD-asema, vaikka käyttöjärjestelmän asennus yleensä onnistuukin kätevämmiin USB-muistitikulta.

Palvelimen koteloksi valikoitui Fractal Desing -merkkinen erittäin tilava kotelo, jossa on hyvin tilaa komponenteille ja jonka suunnittelussa on kiinnitetty huomiota ilmanvaihtoon. Virtalähteenä toimii Silverstonen 550-wattinen ATX-virtalähde, jonka voi hintansa ja ominaisuuksien perusteella olettaa olevan aivan halvimpia virtalähteitä laadukkaampi ja joka ominaisuuksiensa soveltuu hyvin käyttötarkoitukseensa (Silverstone Technology 2019). Tarvittaessa koneen näyttönä toimii vanha 19-tuumainen LCD-näyttö, jota voi pienen kokonsa ansiosta säilyttää samassa laitekaapissa muiden laitteiden kanssa. Hiiri ja näppäimistö ovat Logitechin edullisia perusmalleja.

Vanha palvelin

Toimeksiantaja halusi säilyttää myös vanhan palvelinkoneen toiminnassa uuden rinnalla. Koneessa oli 2,2 GHz:n Intel Core 2 E4500 -prosessori ja 2 Gt DDR2-keskusmuistia, jotka mahdollistivat käyttötarkoitukseen riittävän suorituskyvyn. Vanhalle palvelimelle oli alkuvaiheessa tarkoitus varmuuskopioida ajastetusti uuden palvelimen sisältö ja jatkossa se olisi mahdollista myös määritellä varapalvelimeksi siltä varalta, että varsinainen palvelinkone hajoaisi niin, ettei sen korjaaminen riittävän nopeasti olisi mahdollista.

Palvelimen työtiedostojen ja varmuuskopioiden tallentamiseen käytetyt 2 Tt:n kiintolevyt olivat kuitenkin jo noin seitsemän vuotta vanhoja, joten ne päätettiin uusiksi ennen kuin ne hajoaisivat. Uusiksi kiintolevyiksi valittiin kolme samanlaista 4 Tt:n Western Digitalin mallia kuin uuteenkin palvelinkoneeseen ja niistä muodostettiin 4 Tt:n RAID 1 -levypakka, jossa kolmas levy on varalla. Käyttöjärjestelmäosion RAID 1 -tason levypakan muodostavia 160 Gt:n kiintolevyjä ei vielä haluttu uusiksi.

Vanhan palvelimen luotettavuudelle suurimman riskin aiheutti kymmenisen vuotta vanha emolevy. Sen rikkoutuessa palvelin jouduttaisiin rakentamaan uuden emolevyn, prosessorin ja muistien ympärille, koska alkuperäistä vastaavia laitteistokomponentteja ei enää saisi hankittua uutena. Toinen ongelmakohta oli käyttöjärjestelmäosion vanhoissa kiintolevyissä, jotka todennäköisesti hajoaisivat joidenkin vuosien sisällä. Palvelimen tärkein sisältö eli uudelta palvelimelta ajastetusti otetut varmuuskopiot olisivat kuitenkin tallessa uusilla kiintolevyillä, jotka voitaisiin ottaa helposti käyttöön toisessakin tietokoneessa. Uutta palvelinta varten varalle hankittu virtalähde soveltui käytettäväksi myös vanhassa palvelimessa.

Käyttöjärjestelmä

Kummankin palvelimen Linux-jakelupaketiksi valittiin ilmainen Opensuse Leap 42.3, koska saman toimittajan vanhempi jakelupakettiversio oli havaittu erinomaisesti toimivaksi toimeksiantajan vanhassa palvelinkoneessa. Valintaan vaikutti ratkaisevasti myös monen vuoden omakohtainen kokemukseni Opensusen tuotteista ja se, että tulisin toimimaan myös toimeksiantajan palvelimen ylläpitäjänä. Edellä mainitun kokemuksen perusteella Opensusen vahvuuksina muihin vaihtoehtoihin verrattuna voidaan pitää

erityisesti asennuksen ja ylläpidon vaivattomuutta. Jakelupaketti tarjoaa ylläpitäjän käyttöön Yast-ohjelman, jonka avulla käyttöjärjestelmän asennus sujuu helposti. Samalla ohjelmalla voidaan hallita lähes kaikkia käyttöjärjestelmän asetuksia ja erityisen kätevä se on ohjelmistopakettien asentamisessa ja hallinnassa. Yast-ohjelma toimii sekä graafisessa työpöytäympäristössä että komentorivipohjaisella pääteyhteydellä, joten se soveltuu hyvin myös etähallintaan. Opensusen RPM-tyyppisiä ohjelmistopaketteja voidaan hallita Yastin lisäksi esimerkiksi komentorivipohjaisella Zypper-ohjelmalla (Opensuse 2019c). Valmistaja tarjoaa käyttöjärjestelmälle kattavasti ohjeita eri tilanteisiin ja apua ongelmiin voi kysyä kehittäjäyhteisön omien tukikanavien lisäksi monilla muilla keskustelufoorumeilla (Opensuse 2019d).

Vapaaehtoisvoimin kehitettävästä Opensusesta on saatavilla myös maksullinen versio Suse Linux Enterprise Server (SLES). Sen valmistaja Suse tukee ilmaisen jakelupaketin kehitystyötä, jota puolestaan käytetään maksullisen version kehitystyön pohjana. SLES tarjoaa ilmaista Opensusea vakaamman ja viimeistellymmän käyttöjärjestelmän, joka on ominaisuuksiltaan suunnattu yrityskäyttöön ja johon on saatavilla maksullisia tukipalveluita. (Opensuse 2019e.) Ilmainen käyttöjärjestelmäversio voidaan myös päivittää maksulliseen SLES-versioon seuraamalla valmistajan tuottamaa ohjeistusta, mutta silloin on otettava huomioon, että SLES:n mukana tulee pienempi valikoima oheisohjelmia kuin Opensusessa (Suse 2019).

Ilmaisista jakelupaketeista erityisen varteenotettava vaihtoehto olisi ollut myös Ubuntu Server, jolla on laaja käyttäjäpohja ja jolle siten löytyy helposti tukea esimerkiksi keskustelufoorumeilta. Tässä tapauksessa valinnan kuitenkin ratkaisivat Opensusen eduksi sekä omat että toimeksiantajan hyvät kokemukset ja henkilökohtaiset mieltymykset. Linux-käyttöjärjestelmästä ja jakelupaketin valinnassa huomioitavista asioista kerrotaan yleisesti luvussa 2.1.

Toiminnot

Palvelimen tärkeimmäksi tehtäväksi määritelty tiedostojen jakaminen suunniteltiin toteutettavaksi käyttäen Linuxin Samba-ohjelmistoa, jonka avulla Linux-palvelimelle tallennetut tiedostot saadaan jaettua Windows-työasemille. Samba käyttää tiedostojen jakamiseen SMB-protokollaa, jota Microsoft on jo vuosia käyttänyt Windows-käyttöjärjestelmiensä yhteydessä (Samba.org 2019). Palvelimen työtiedoille varatulle levyosiolle luotiin hakemisto, joka näkyi Windows-työasemilla verkkolevynä, jonne

käyttäjät voivat tallentaa tiedostojaan. Tiedostojen jakaminen Samba-ohjelmiston vanhemmalla versiolla oli käytössä jo yrityksen vanhalla palvelinkoneella, joten Samban vaatimat asetukset voitiin kopioida siitä.

Palvelimen haluttiin toimivan myös tietoliikennepaketteja verkon eri osien, kuten sisäverkon ja Internetin, välillä reitittävänä laitteena aiemman WLAN-reitittimen sijasta. Kyseinen toiminnallisuus voidaan toteuttaa Linuxissa vakiona olevien ominaisuuksien avulla. Tämä toiminnallisuus määriteltiin palvelimelle Opensuse Leap 42.3:n yksityiskohtaista ohjeistusta noudattaen (Opensuse 2019f).

Palvelin tuli toimimaan myös palomuurina, jonka tarkoituksena on estää esimerkiksi Internetin suunnasta tulevat asiattomat yhteydenotot yrityksen sisäverkkoon. Opensuse Leap 42.3:n palomuuuri on toteutettu Susefirewall2-komentosarjatieidoston avulla, joka käytännössä luo käyttäjän määrittelyitä vastaavia palomuurisääntöjä iptables-ohjelman avulla (Opensuse 2019g). Palomuurin toimintaa varten sille pitää määritellä erilaisia vyöhykkeitä eli IP-osoitteiden ryhmiä, joille puolestaan määritellään palomuurisääntöjä keskitetysti.

Palvelimen ulko-verkon verkkoliitäntä yhdistettiin ADSL-päätelaitteen siltaavassa tilassa olevaan verkkoliitäntään, jolloin se käytti julkista IP-osoitetta. Kyseiselle verkkoliitäntälle määriteltiin Internet-palveluntarjoajalta saatu kiinteä IP-osoite, aliverkonpeite ja yhdyskäytävä. Tämä verkkoliitäntä määriteltiin palomuurin asetuksista external zoneksi eli ulkoiseksi, turvattomaksi vyöhykkeeksi, josta sisäverkkoon päin aloitetut yhteydet oletusarvoisesti estetään.

Palvelimen sisäverkon verkkoliitäntä yhdistettiin verkkokytkimeen ja sille määriteltiin kiinteä sisäverkon IP-osoite 192.168.0.1. Tämä verkkoliitäntä määriteltiin palomuurin asetuksista internal zoneksi eli luotetuksi sisäverkon vyöhykkeeksi, jolla sijaitsevista IP-osoitteista tulevaa liikennettä ei rajoiteta yhtä tiukasti kuin turvattoman vyöhykkeen tapauksessa, vaikka siitä saatetaankin suodattaa osa pois tietoturvan parantamiseksi.

Palomuurin asetuksista määriteltiin avoinna oleviksi vain ne portit, joissa toimiviin palveluihin piti päästä ottamaan yhteyttä Internetin suunnasta. Asiakkaan palvelimen tapauksessa Internetin suunnasta sisäverkkoon päin tulevien yhteydenottojen osalta avoimeksi asetettiin vain SSH-palvelun käyttämä portti, joka oli oletuksena 22. SSH-palvelun portti muutettiin tietoturvan parantamiseksi joksikin muuksi kuin oletusportiksi. Susefirewall2-palomuurin asetuksia voidaan hallita asetustiedostoja suoraan tekstiedi-

torilla muokkaamalla tai Yast-ohjelmalla joko komentorivipohjaisesti tai graafisessa ympäristössä.

Aiemmin sisäverkon DHCP-palvelimena toimi vanha WLAN-reititin, mutta sekin toiminto haluttiin siirtää uuden palvelimen hoidettavaksi. Linuxin mukana toimitetaan DHCPD-ohjelma (Dynamic Host Configuration Protocol Server), joka jakaa lähiverkkoon liitetyille laitteille IP-osoitteita DHCP-protokollaa käyttäen (Internet Systems Consortium 2019). Uudet verkkoon liitetyt laitteet saavat siis sattumanvaraisesti valitun vapaana olevan IP-osoitteen palvelimen asetuksiin määritellyltä osoitealueelta. Työasemille, monitoimilaitteille ja verkkokytkimille määriteltiin DHCP-palvelimen asetustiedostoon kuitenkin kiinteät IP-osoitteet, jotka jaetaan niille laitteiden MAC-osoitteiden perusteella.

Palvelimelle asennettiin myös selainpohjainen Webmin-ohjelma, jolla voidaan kattavasti määritellä palvelimen asetuksia (Webmin 2019). Opensuseen Webmin suositellaan asennettavaksi Git-asennuslähteen kautta, eikä sille ole saatavissa virallista RPM-asennuspakettia (Opensuse 2019h).

Etäkäytön osalta yritykselle riitti, että tarvittaessa tiedostoihin pääsisi käsiksi Internetin kautta esimerkiksi etätyötä tehtäessä. Lisäksi toivottiin mahdollisuutta muodostaa etätyöpöytäyhteys yrityksen sisäverkkoon liitetyille työasemille. Suunniteltujen etäkäyttömahdollisuuksien mahdollistamiseksi palvelimella käytettiin Linux-jakelupaketin mukana tulevaa SSHD-ohjelmaa (OpenSSH SSH Daemon).

Windows-työasemalta avataan salauksella suojattu SSH-yhteys palvelimelle esimerkiksi Putty-ohjelmalla, johon voidaan määritellä tarvittavat SSH-tunnelit eli yksittäisten porttien ohjaukset (Tatham 2019). SSH:n porttiohjauksen avulla ohjataan jokin työaseman paikallinen portti osoittamaan etäkoneen tiettyyn porttiin (SSH Communications Security Oyj 2019b). Etäkone voi olla joko palvelinkone tai esimerkiksi palvelimen kanssa samassa sisäverkossa oleva työasema, johon halutaan muodostaa yhteys. Tunneloinnin avulla paikallisen koneen ja etäkoneen porttien välinen liikenne kulkee palvelimelle muodostetun SSH-yhteyden kautta. Tämä toiminto mahdollistaa esimerkiksi RDP-etätyöpöytäyhteyden muodostamisen työntekijän kotikoneelta yrityksen palomuurilla suojatussa sisäverkossa olevaan työkoneeseen.

Tiedostojen siirtämiseen voidaan käyttää SSH:n SFTP-protokollaa (SSH File Transfer Protocol) hyödyntävää Winscp-ohjelmaa. Se mahdollistaa tiedostojen salatun siirtämisen SSH-yhteyden välityksellä Windows-työaseman ja palvelimen välillä. (Winscp 2019.)

Yrityksen Windows-työasemat oli jo aiemman tietojärjestelmän aikana varmuuskopioitu palvelimelle ajastetusti kerran vuorokaudessa. Samaa hyvin toiminutta menetelmää haluttiin käyttää myös uuden palvelimen kanssa. Varmuuskopioinnista vastaa palvelimella ajastetusti toimiva, jo aiemmin itse tehty komentosarja (engl. script) eli tiedosto, jossa olevia komentoja suoritetaan Linuxin Bash-komentotulkin avulla (Blum & Bresnahan 2015, 211–212). Komentosarjatiedosto sisältää yksinkertaista ohjelmointia ja sen kautta voidaan ajaa myös muita Linuxin ohjelmia.

Windows-työasemien varmuuskopioitaviksi valitut hakemistot jaettiin Windowsin tiedostojenjako-ominaisuutta käyttäen. Jotta varmuuskopioiden koko ei olisi kasvanut tarpeettoman suureksi, varmuuskopioitaviksi valittiin vain esimerkiksi käyttäjien työtiedostoja ja järjestelmän asetuksia sisältäviä hakemistoja. Palvelimella toimiva komentosarjatiedosto varmuuskopioi verkossa olevien koneiden jaetut hakemistot Smbclient-ohjelman avulla ja pakkaa ne tar.gz-tiedostoihin, jotka nimetään tietyn logiikan mukaan sisältäen muun muassa varmuuskopiointiajankohdan, työaseman tunnuksen ja kopioitavan jaon nimen. Jokaiselle viikonpäivälle luodaan oma työasema- ja tiedostojakokohtainen tiedostonsa. Komentosarjatiedosto osaa myös tarkistaa, onko varmuuskopioitava kone tavoitettavissa ja jollei ole, se yrittää herättää sen Wake-on-Lan-toiminnon avulla. Lisäksi työasemat ajastettiin käynnistymään ennen varmuuskopiointia.

Varmuuskopiointi asetettiin toimimaan niin, että jokaisen työaseman tiedostoista säilytetään kerran vuorokaudessa otetut varmuuskopiot kahden viikon ajalta. Komentosarjassa on toiminto, jonka avulla se siivoaa vanhat versiot varmuuskopioista pois säilyttäen kuitenkin halutun määrän verran uusimpia versioita. Siivoustoiminto suoritetaan vasta, kun uusin varmuuskopiointi on suoritettu. Lisäksi varmuuskopioinnin yhteydessä tarkistetaan tiedostokokoa tarkastelemalla, onko tuloksena syntynyt tiedosto kelvollinen. Siis esimerkiksi tyhjät ja joidenkin ongelmien seurauksena syntyneet liian pienet tiedostot (tiedostokokoa alle 100 tavua) poistetaan heti. Järjestelmä tallentaa tiedot varmuuskopioinnin vaiheista lokitiedostoonsa, jonka avulla varmuuskopioinnin toimivuutta voidaan tarkkailla.

Varmuuskopioihin ei normaaliolosuhteissa pääse käsiksi suoraan Windows-työasemilta, vaan niiden käyttäminen vaatii, että palvelimella oleva varmuuskopiot sisältävä hakemisto yhdistetään erilliseksi verkkolevyksi työasemalle käyttäen sellaista käyttäjätunnusta ja salasanaa, jota ei ole tallennettu Windowsin asetuksiin. Verkkolevyn tiedostoihin on silloinkin vain lukuoikeus eli niitä ei pääse poistamaan työaseman kautta palvelimelta. Näin menettelemällä parannettiin tietoturvaa ja varmistettiin, ettei

esimerkiksi yksittäiselle työasemalle asentunut haittaohjelma pääsisi tuhoamaan varmuuskopioita tai salakirjoittamaan niitä käyttökeltottomiksi.

Lisäksi uudella palvelimella sijaitsevat työtiedostot, järjestelmän asetustiedostot ja työasemien varmuuskopiot määriteltiin kopioitumaan ajastetusti vanhalle palvelinkoneelle toisen komentosarjatiedoston ja Rsync-ohjelman avulla. Tiedostot voidaan myös kopioida palvelinkoneen USB-liitäntään yhdistetylle ulkoiselle kiintolevyille, jota varmuuskopioinnin jälkeen säilytetään muualla kuin yrityksen toimitiloissa. Tätä toimintoa ei kuitenkaan vielä automatisoitu, joten ulkoiselle kiintolevyille kopioinnin säännöllisyys on riippuvainen niistä yrityksen työntekijöistä, joiden vastuulle asia on annettu. Tiedostot voitaisiin jatkossa varmuuskopioida myös Internetin ylitse muualla sijaitsevalle palvelimelle, mutta se vaatisi yrityksen nykyisen Internet-yhteyden päivittämistä huomattavasti nopeammaksi.

Lähiverkko ja Internet-yhteys

Kaksi vanhaa 8-porttista verkkokytöntä päätettiin korvata yhdellä nykyaikaisella hallittavalla verkkokytöntimellä, jossa olisi vähintään 24 porttia, mikä mahdollistaisi kaikkien laitteiden yhdistämisen samaan fyysiseen kytkimeen. Laitteen vaihdon myötä siirtonopeus 1 Gb/s olisi käytettävissä koko lähiverkossa, kun toinen vanhoista kytkimistä ei enää rajoittaisi nopeutta arvoon 100 Mb/s osassa verkkoa. Myös verkkokaapelointia haluttiin parantaa vetämällä joitakin uusia verkkokaapeleita kytkentäpaneelistä uusille käyttöpaikoille.

Langattoman lähiverkon toiminnan parantamiseksi nykyisen WLAN-reitittimen tilalle päätettiin hankkia kaksi tukiasemaa, jolloin verkon käyttöalue saataisiin katettua paremmin, mikä yhdessä teknisiltä ominaisuuksiltaan parempien tukiasemien kanssa mahdollistaisi myös suuremmat nopeudet. Tietoturvan parantamiseksi suunniteltiin tehtäväksi kaksi toisistaan erillistä langatonta verkkoa, joista yksi olisi yrityksen sisäiseen käyttöön ja toinen vierailijoita sekä työntekijöiden omia laitteita varten. Vieraverkon salasanaa voitaisiin näin jakaa vapaammin yrityksen ulkopuolisille käyttäjille. Yrityksen sisäiseen käyttöön tarkoitetun verkon salasana puolestaan voisi olla tarkemmin varjeltu salaisuus ja myös selvästi aiempaa monimutkaisempi, koska siinä ei tarvitsisi enää huomioida vierailijoiden käyttökokemusta, jonka vuoksi salasana usein määritellään liian helpoksi.

Yrityksen nopeuden 8/1 Mb/s ADSL-yhteys oli toimeksiantajan henkilökunnan kokemusten perusteella havaittu liian hitaaksi vastaamaan nykyajan tiedonsiirtovaatimuksia varsinkin sen jälkeen, kun yrityksen henkilöstömäärä oli kasvanut nykyiselle tasolle. Lisäksi suunniteltu tiedostojen varmuuskopiointi Internetin välityksellä etäpalvelimelle vaatisi selvästi nykyistä suurempaa lähetysnopeutta. Yrityksen nykyisen ja samalla alueen lankapuhelinverkon omistavan Internet-operaattorin toimintaan oltiin tyytyväisiä, joten siltä pyydettiin tarjousta sekä mahdollisesta valokuituyhteydestä että nykyistä lankapuhelinverkkoa hyödyntävästä nopeammasta DSL-pohjaisesta yhteydestä. Lisäksi haluttiin vertailun vuoksi selvittää mobiililaajakaistan nopeus- ja hintavaihtoehdot.

Operaattorilta tarjouspyyntöön saadun vastauksen mukaan valokuituliittymää ei ollut saatavilla, mutta lankapuhelinverkkoa hyödyntävät nopeusvaihtoehdot 10/10 Mb/s ja 24/2 Mb/s olivat mahdollisia, eivätkä ne kohtuuttomasti nostaisi yhteyskuluja käytössä olevaan liittymään verrattuna. Mobiililaajakaistaliittymälle ominaiseen tapaan sen nopeudelle ilmoitetut vaihteluvälit olivat suuret eli vastaanottonopeuden minimiarvoksi taattiin vain 5 Mb/s maksimiarvon ollessa jopa 100 Mb/s. Vastaavasti lähetysnopeuden vaihteluväliksi ilmoitettiin 4–50 Mb/s. Nopeuden 10/10 Mb/s DSL-liittymälle ilmoitettu vaihteluväli oli 7–10/7–10 Mb/s ja nopeuden 24/2 Mb/s liittymälle 10,5–15/1–1,5 Mb/s. Kaikki vaihtoehdot sisälsivät toimeksiantajan tarvitseman kiinteän julkisen IP-osoitteen. Kolmesta vaihtoehdosta kallein oli mobiililaajakaistaliittymä ja halvin nopeuden 24/2 Mb/s DSL-yhteys. Hint erot liittymien välillä olivat noin 20 e ilman arvonlisäveroa. Internet-yhteyden päivittäminen nopeampaan päätettiin kuitenkin jättää myöhemmäksi.

4 TOTEUTUS

Yrityksen edustajien kanssa käytyjen alustavien keskustelujen jälkeen tehtiin toimeksiantosopimus. Projekti aloitettiin selvittämällä uudelle tietojärjestelmälle asetetut vaatimukset yhdessä asiakasyrityksen kanssa ja kartoittamalla nykyisen järjestelmän osat mahdollisimman tarkasti. Sen jälkeen uudesta järjestelmästä tehtiin suunnitelma ja kustannusarvio, jotka hyväksyttiin asiakkaalla.

Tarvittavien laitteistohankintojen jälkeen koottiin uusi palvelinkone, johon tehtiin valmiiksi käyttöjärjestelmän ja muiden ohjelmistojen asennus- ja määrittelytyöt ennen sen toimittamista asiakkaalle. Käyttöönoton ensimmäisessä vaiheessa vanha palvelin korvattiin uudella palvelimella. Toisessa vaiheessa tehtiin suunnitellut muutokset asiakkaan tietoverkkoon ja tietoliikenneyhteydet reititettiin kulkemaan uuden palvelimen kautta vanhan WLAN-reitittimen sijasta. Kolmannessa vaiheessa vanha palvelinkone uudistettiin ja liitettiin takaisin osaksi yrityksen tietojärjestelmää toimimaan uudessa tehtävässään osana tiedostojen varmuuskopiointijärjestelmää ja mahdollisena varapalvelimena. Neljännessä vaiheessa oli vuorossa uuden langattoman verkon käyttöönotto. Myöhemmin päivitettiin vielä kummankin palvelimen Linux-käyttöjärjestelmä uusimpaan versioon.

Toteutuksen eri vaiheissa pyrittiin välttämään yrityksen toiminnalle haittaa aiheuttavat katkokset tietojärjestelmän toiminnassa suorittamalla työt suurimmaksi ajaksi yrityksen työajan ulkopuolella ja tekemällä käyttöönotto vaiheittain. Eri toimintojen toimivuus myös varmistettiin huolellisesti jokaisen työvaiheen jälkeen, millä vältettiin mahdolliset ikävät yllätykset.

Uuden järjestelmän käyttöönoton eri vaiheista tiedotettiin toimeksiantajalle sekä ennen yksittäisen vaiheen toteutusta että sen jälkeen. Käyttäjille kerrottiin, miten uusi järjestelmä eroaa vanhasta ja millaisia toimenpiteitä heiltä mahdollisesti vaadittaisiin muutostilanteessa. Käyttäjille järjestettiin mahdollisuus olla yhteydessä suoraan toimeksiannon toteuttajaan, jos he havaitsisivat ongelmia toiminnassa tai tarvitsisivat apua. Lopuksi toimeksiantajalle selostettiin riittävän tarkasti, miten järjestelmä toimii ja sovittiin, että myöhemmin voidaan tarvittaessa toimittaa järjestelmän tarkka toimintakuvaus.

4.1 Palvelimen asennus ja käyttöönotto

Palvelimen rakentaminen ja käyttöjärjestelmän asentaminen

Uuden palvelinkoneen osat hankittiin luvussa 3.4 esitellyn suunnitelman mukaisesti eikä koneen kokoamisessa ilmennyt ongelmia. Emolevyn BIOS-ohjelmisto päivitettiin uusimpaan saatavilla olevaan versioon ja lopuksi varmistettiin, että koneen ja kotelon eri osat toimivat odotetusti. Keskusmuistin toiminta varmistettiin käyttämällä muistites-tiohjelmaa Memtest86+ (Memtest86+ 2013) ja kiintolevyt tarkistettiin niiden valmistajan toimittamalla testiohjelmalla siitä huolimatta, että ne olivat uusia.

Käyttöjärjestelmän asennusta varten jakelupakettitoimittaja Opensusen sivustolta ladattiin käyttöjärjestelmän levykuvatiedosto, joka tallennettiin USB-muistitikulle. Tietokone käynnistettiin muistitikulta, joka käynnisti käyttöjärjestelmän asennukseen käytettävän Yast-ohjelman. Koska tietokone oli liitetty Internetiin, tunnisti asennusohjelma automaattisesti tarvittavat verkkoyhteyden asetukset. Mikäli Internet-yhteyttä ei voida muodostaa automaattisesti, pitää tarvittavat asetukset määritellä itse. Internet-yhteyden avulla asennusohjelma voi päivittää itsensä ja tarvittaessa hakea erikseen määritellyistä asennuslähteistä sellaisia asennuspaketteja, joita ei toimiteta levykuvatiedoston mukana.

Seuraavassa vaiheessa valittiin järjestelmän tyyppi, joka määrittelee, mitä ohjelmapaketteja järjestelmän lisäksi asennetaan. Valinta server sopii palvelinkäyttöön, jossa ei tarvita graafista käyttöliittymää. Tässä tapauksessa päädyttiin valintaan custom, joka mahdollistaa haluttujen asennuspakettien yksityiskohtaisen valinnan. Näin menetelmällä voitiin heti valita kaikki tarvittavat ohjelmat sen sijaan, että ne olisi asennettu erikseen vasta käyttöjärjestelmän asennuksen jälkeen. (Opensuse 2019i.)

Vaikka asennusohjelma ehdotti mielestään sopivaa tapaa kiintolevyjen osioimiseksi, piti RAID-levyjärjestelmää varten osioiden asetukset määritellä käsin Expert Partitioner -toiminnon avulla. RAID 1 -levypakkojen luomisen jälkeen niille määriteltiin käyttöjärjestelmän vaatimat ja työtiedostojen tallentamiseen käytetyt osiot sekä valittiin niillä käytettävät tiedostojärjestelmät. (Opensuse 2019j.)

Seuraavaksi luotiin tarvittavat käyttäjätunnukset. Aluksi tehtiin tavallisen käyttäjän oikeuksilla varustettu tunnus ja määriteltiin sen jälkeen järjestelmässä vakiona olevalle root-pääkäyttäjätunnukselle eri salasana. Tarkoituksena on, että pääkäyttäjätunnusta käytet-

tään vain sellaisiin ylläpitotoimiin, jotka vaativat ylläpitäjän oikeuksia, koska muuten root-tunnusta käytettäessä on vaarana, että käyttäjän tekemä yksittäinenkin virhe voi johtaa esimerkiksi järjestelmän tiedostojen tuhoutumiseen. (Opensuse 2019i.)

Lopuksi tarkistettiin vielä asennusohjelman ilmoittamasta yhteenvedosta valitut asetukset ja tehtiin niihin tarvittavat muutokset. Esimerkiksi käyttöjärjestelmän käynnistäminen RAID 1 -levyjärjestelmällä sijaitsevalta /boot-osiolta vaati, että käyttöjärjestelmän laatusohjelma (engl. boot loader) asennettiin kiintolevyn ensimmäiselle sektorille (engl. master boot record, MBR). Lisäksi avattiin palomuuriasetuksista SSH-pääteyhteyden käyttämä portti, joka on vakioasetuksena 22. (Opensuse 2019i.)

Asetusten hyväksymisen jälkeen asennusohjelma aloitti käyttöjärjestelmän ja sen mukana toimitettavien ohjelmien asentamisen. Tämän palvelimen tapauksessa asennusvaihe kesti vajaan tunnin verran. Asennuksen jälkeen tietokone käynnistyi uudelleen, minkä jälkeen koneelle voitiin kirjautua joko paikallisesti tai SSH-pääteyhteyden kautta muiden asetusten määrittelyä varten.

Mahdollisten ongelmatilanteiden selvittelyyn kannattaa varata runsaasti aikaa. Asennusohjelman suoritus voi keskeytyä esimerkiksi tiedostojen lukuvirheeseen varsinkin, jos asennus suoritetaan DVD-levyltä. Mikäli asennusohjelma hakee osan asennuspaketeista Internetissä sijaitsevasta asennuslähteestä, saattaa välillä tulla eteen tilanteita, joissa asennusohjelma pyytää käyttäjää vahvistamaan asennuspaketin uudelleen lataamisen yrittämisen. Jos kiintolevyjen ja levyosoiden määrittelyssä on tehty virheitä, saattaa koko käyttöjärjestelmän käynnistyminen keskeytyä virheeseen. Ongelmatilanteissa apua löytyy yleensä parhaiten Internetin keskustelufoorumeilta ja Linux-jakelupakettivalmistajan tukikanavien kautta.

Käyttöjärjestelmän asennuksen jälkeen asennettiin vielä muutamia puuttuvia ohjelmia Yast-ohjelman avulla ja samalla ohjelmalla määriteltiin myös suurin osa järjestelmän asetuksista. Osa asetuksista määriteltiin kuitenkin tekstieditorilla suoraan ohjelmien asetustiedostoja muokaten. Muutettavat asetukset liittyivät muun muassa sähköpostien välilyöntiin (Postfix-ohjelma), DHCP-palvelimeen, tiedostojen jakamiseen SMB-palvelun avulla sekä kiintolevyjen ja RAID-levyjärjestelmän toiminnan tarkkailuun. Lisäksi luotiin yrityksen työntekijöille tarvittavat käyttäjätunnukset salasanoineen ja määriteltiin tiedostojen jakamiseen liittyvät asetukset ja käyttöoikeudet.

Palvelimen käyttöönotto

Palvelin käytiin asentamassa yrityksen tiloihin ennalta sovittuna aikana yrityksen työajan ulkopuolella. Se asennettiin vanhan palvelimen tilalle samaan lukittavaan laitekaappiin, jossa muun muassa tietoverkon aktiivilaitteet sijaitivat. Laitteen virransyöttö varmistettiin laitekaapissa sijaitsevalla UPS-laitteella.

Uudelle palvelinkoneelle määriteltiin aluksi väliaikainen IP-osoite ja se kytkettiin tiedostojen siirtämistä varten samaan verkkoon vanhan palvelinkoneen rinnalle. Palvelimelle tallennetut työtiedostot ja muut säilytettäväksi tarkoitetut tiedostot kopioitiin vanhalta palvelimelta uudelle palvelimelle verkon ylitse sellaisena ajankohta, jolloin niitä ei yrityksessä käytetty. Tiedostojen kopiointiin käytettiin Rsync-ohjelmaa varmistaen, että tiedostojen alkuperäiset päiväykset, omistussuhteet ja käyttöoikeudet säilyivät muuttomattomina. Tiedostojen siirtämisen jälkeen vanha palvelin kytkettiin irti verkosta ja uuden palvelimen IP-osoite muutettiin samaksi kuin vanhalla palvelimella oli ollut.

Vanhan palvelimen uudistaminen

Kun uusi palvelin oli otettu kokonaan käyttöön, myös vanha palvelinkone uudistettiin suunnitelman mukaisesti vaihtamalla sen ikääntyneistä kiintolevyistä uusiin ne, joita käytetään toisesta palvelimesta otettavien varmuuskopioiden tallentamiseen. Sekä uudet että vanhat kiintolevyt tarkistettiin niiden valmistajien sivustoilta haetuilla testiohjelmilla ja keskusmuistin toiminta varmistettiin muistitestiohjelmalla Memtest86+ (Memtest86+ 2013).

Palvelimen toimintavarmuutta olisi voitu parantaa uusimalla myös käyttöjärjestelmäosion kaksi vanhaa kiintolevyä. Sen sijaan päätettiin hyväksyä niiden palvelimen toiminnalle aiheuttama riski ja luottaa siihen, että RAID-levyjärjestelmä ilmoittaa kiintolevyjen vikaantumisesta riittävän ajoissa ja että vikaantunut kiintolevy tai tässä tapauksessa mieluummin kummatkin levyt ehditään uusimaan ennen toisenkin levyn hajoamista. Käyttöjärjestelmälevyjen vikaantuminen aiheuttaa käytännössä kuitenkin vain sen, ettei yrityksen tietojärjestelmän uudesta palvelimesta oteta uusia varmuuskopioita. Jo aiemmin otetut varmuuskopiot säilyvät tallessa palvelimen toisilla kiintolevyillä.

Vanhan palvelimen käyttöjärjestelmäksi asennettiin ensin sama Opensuse Leap 42.3 kuin toiseenkin koneeseen ja myöhemmin käyttöjärjestelmä päivitettiin uusimpaan ver-

sioon. Lisäksi palvelinkone puhdistettiin paineilman avulla sen sisälle vuosien mittaan kertyneestä pölystä. Vanha palvelin sijoitettiin yrityksen laajojen toimitilojen toiseen osastoon kauas uudesta palvelinkoneesta, jotta esimerkiksi tulipalon sattuessa todennäköisyys kummankin koneen ja siten myös varmuuskopioiden tuhoutumiselle olisi pienempi. Laitteen toiminta sähkökatkojen varalta varmistettiin sen yhteyteen sijoitetulla UPS-laitteella.

Käyttöjärjestelmän versiopäivitys

Opinnäytetyön tekemisen aikana asiakkaan palvelimien käyttöjärjestelmän jakelupaketista ilmestyi uusi versio. Sekä uuden että vanhan palvelimen Opensuse Leap 42.3 päivitettiin versioon 15.0, joka on pienemmästä versionumerosta huolimatta aiempaa uudempi johtuen valmistajan käyttöönottamasta uudesta nimeämiskäytännöstä (Opensuse 2019k).

Päivitys tehtiin SSH-päätelytehtävien kautta etänä käyttäen komentorivipohjaista Zyperohjelmaa ja se kesti neljä tuntia, kun huomioidaan myös noin 3,5 Gt:n suuruisen päivitystiedostojen lataamiseen kulunut aika hitaan ADSL-yhteyden välityksellä. Käyttöjärjestelmän versiopäivitystä käsitellään tarkemmin luvussa 4.5.

4.2 Tietoverkon muutokset

Lähiverkkoon tehdyt muutostyöt

Lähiverkon kaksi vanhaa 8-porttista hallitsematonta verkkokytkintä korvattiin 24-porttisella hallittavissa olevalla verkkokytkimellä HP Pro Curve 1810G-24, joka sijoitettiin samaan lukittavaan laitekaappiin, jonka kytkentäpaneeliin myös lähiverkon kaapeloinnit ja puhelinliittymä oli päätetty. Uusi kytkin mahdollisti useamman laitteen yhdistämisen lähiverkkoon entistä suuremman porttimääränsä vuoksi. Lisäksi kytkimen hallintaominaisuudet mahdollistivat sellaisten tietoturvaa parantavien ratkaisujen kuin virtuaalilähiverkkojen (VLAN) käyttämisen. Myös vikatilanteiden selvittäminen tulisi helpottamaan, kun laitteen hallintasivustolta voitaisiin tarkistaa yksittäisen kytkinportin tila ja siihen kytketyn laitteen MAC-osoite.

ADSL-päätelaite oli aiemmin sijoitettu epäkäytännöllisesti suuren toimitilarakennuksen toisessa päädyssä sijaitsevan puhelinpistorasian yhteyteen, joten se siirrettiin saman laitekaapin sisälle, jossa oli myös puhelinverkkokaapeloinnin kytkentärima. Oikeiden kytkentöjen selvittäminen vaati runsaasti aikaa ja vaivaa, koska rakennuksen sisäistä puhelinkaapelointia ei ollut dokumentoitu riittävän hyvin. Laitekaapissa sijaitsevan lähiverkon kytkentäpaneelin ja verkkokytkimen väliset verkkokaapelit vaihdettiin uusiin, koska osa vanhoista kaapeleista oli huonokuntoisia ja pituudeltaan vaihtelevia. Näin menettelemällä saatiin myös laitekaapin yleisilme siistimmäksi.

Yrityksen lähiverkko myös dokumentoitiin eli aiemmin virheellisesti merkityt tai merkitsemättä jätetyt kytkentäpaneelin ja käyttöpaikkojen rasioiden väliset kaapeloinnit selvitettiin, minkä jälkeen kaapeloinnit merkittiin selvästi liitäntöjen yhteyteen. Merkintöjen ja ohjeistuksen ansiosta jatkossa muutosten tekeminen kytkentöihin on oleellisesti aiempaa helpompaa. Kaapeloinnin selvittämisen yhteydessä testattiin myös kytkentäpaneelin ja rasioiden välisten yhteyksien toimivuus, minkä yhteydessä löydettiin kolme rasiaa, joiden välityksellä saavutettiin vain yhteysnopeus 100 Mb/s, vaikka laitteet, liittimet ja kaapelit tukivat nopeutta 1 Gb/s. Ongelma syyksi epäiltiin joko viallisia kaapeleita tai puutteellisesti tai virheellisesti tehtyjä kytkentöjä, mutta asian tarkempi tutkiminen päätettiin jättää myöhemmäksi, koska kyseisille yhteyksille ei sillä hetkellä ollut käyttötarvetta.

Tietoliikenneyhteyksien reititys uuden palvelimen kautta

Tietoliikenne reititettiin kulkemaan Linux-palvelimen kautta vasta sen jälkeen, kun uusi palvelin oli ensin vähän aikaa toiminut tiedostopalvelimena entisen palvelimen tilalla. Siihen asti reitittimenä oli toiminut vanha WLAN-reititin, joka nyt poistettiin käytöstä lopullisesti. Linux-palvelimen sisäverkon verkkoliitäntä yhdistettiin verkkokytkimeen ja ulkoverkon verkkoliitäntä ADSL-päätelaitteeseen.

Linux-palvelin määriteltiin toimimaan sisäverkon DHCP-palvelimena eli jakamaan verkkoon liitetyille laitteille IP-osoitteet. Muutostöiden jälkeen varmistettiin, että yhteydet toimivat edelleen kuten pitikin.

Uuden langattoman verkon käyttöönotto

Osana yrityksen tietojärjestelmän uudistamista otettiin käyttöön myös uusi langaton verkko. Luvussa 3.4 esitellyn suunnitelman mukaisesti yrityksen vanha WLAN-reititin korvattiin kahdella erillisellä Ubiquiti Networksin valmistamalla Unifi AC Pro -tukiasemalla. Itselleni oli työni kautta kertynyt myönteisiä kokemuksia kyseisen valmistajan tukiasemajärjestelmästä sekä siihen perustuvien laajojenkin langattomien verkkojen toteutuksesta ja ylläpidosta. Unifi-laitteiden ominaisuudet sopivat yrityksen tarpeisiin hyvin ja myös järjestelmän kokonaishinta oli erittäin kilpailukykyinen muihin vastaviin ratkaisuihin verrattuna.

Unifi AC Pro -tukiasemat tukevat IEEE 802.11ac -standardia ja siten sekä 2,4 GHz:n että 5 GHz:n taajuuksia. Ne toimivat osana yhtenäistä järjestelmää, joka mahdollistaa järjestelmään määriteltyjen langattomien verkkojen keskitetyn hallinnan ja toiminnan tarkkailun. Tukiasemien kontrollerina eli niiden toimintaa ohjaavana palvelimena voi toimia joko paikallisesti yrityksen tiloihin sijoitettu palvelin tai ulkopuoliselta taholta hankittu pilvipalvelu ja verkkoa voidaan hallita joko mobiilisovelluksen tai hallintasivuston kautta (Ubiquiti Networks 2019a). Asiakasyrityksen tapauksessa päädyttiin ohjaamaan tukiasemia jälleenmyyjältä hankitun verkossa toimivan palvelun kautta, vaikka kontrolleriohjelmistoa olisi voitu ajaa myös yrityksen omalla palvelimella tai käyttää siihen tarkoitukseen Unifi Cloud Key -palvelinlaitetta.

Langattomaan verkkoon liitetyt laitteet saavat IP-osoitteensa yrityksen uuden palvelimen DHCP-palvelimelta samalla tavalla kuin kaapeloidun lähiverkon laitteet. Langattoman verkon liikenne ei kulje kontrollerin kautta, vaan sen tehtävänä on ainoastaan järjestelmän ominaisuuksien sekä siihen liitettyjen laitteiden hallinta ja tarkkailu. Langaton verkko toimii siis normaalisti myös ilman jatkuvaa yhteyttä kontrolleriin. (Ubiquiti Networks 2019b.)

Ongelmatilanteiden ratkaisua helpottaa, kun hallintajärjestelmän kautta nähdään, mihin tukiasemaan päätelaite on yhdistettynä ja mikä on sen yhteysnopeus ja signaalivoimakkuus. Järjestelmä tarjoaa myös monipuolista tilastotietoa verkon tietoliikenteestä ja sen avulla voidaan myös jälkikäteen selvittää, mitä laitteita verkkoon on ollut liitettynä tiettyinä ajankohtana. Lisäksi langattoman verkon nimi sekä salasana voidaan helposti muuttaa kaikkiin tukiasemiin samalla kertaa ja langattoman verkon käyttämät kanavat ja lähetysteho voidaan määritellä tukiasemakohtaisesti. Hallintajärjestelmän kautta voi-

daan havaita myös muut alueen langattomat verkot sekä niiden voimakkuudet ja kanavat.

Yrityksen vanhan, yhteen tukiasemaan perustuneen langattoman verkon ongelmaksi oli muodostunut heikko kuuluvuus laajan toimitilarakennuksen eri osissa. Ongelma ratkaistiin sijoittamalla kaksi erillistä tukiasemaa sellaisiin paikkoihin, joista niiden luoma langaton verkko kykeni kattamaan koko kiinteistön alan. Asennusta helpotti se, että tukiasemien käyttösähkö voitiin syöttää niille verkkokaapelia käyttäen PoE-ominaisuuden avulla. Valkoiset, seinään ja kattoon asennetut pyöreät AC Pro -tukiasemat sulautuivat huomaamattomasti toimitilojen sisustukseen. Unifi-järjestelmän etuihin lukeutuu myös mahdollisuus laajentaa langatonta verkkoa Mesh-ominaisuuden avulla, jolloin osa tukiasemista voi olla liitettynä verkkoon toisen tukiaseman kautta ilman lähiverkkokaapelointia (Ubiquiti Networks 2019c).

Järjestelmään määriteltiin kaksi toisistaan erillistä langatonta verkkoa. Yrityksen työntekijöiden ja laitteiden käyttöön tarkoitettusta verkosta sallittiin pääsy samoihin verkon palveluihin ja laitteisiin kuin kaapeloidustakin lähiverkosta. Vierasperkosta puolestaan mahdollistettiin pääsy vain Internetiin. Kummatkin verkot suojattiin erillisillä riittävän pitkillä ja vahvoilla salasanoilla, mutta vierasperkon salasanasta tehtiin hieman lyhyempi ja siten helpommin vierailijoiden laitteille syötettävissä oleva, jotta verkkoon liittymistä ei tehtäisi tarpeettoman hankalaksi. Vierasperkkoon liitettiin myös sellaiset työntekijöiden käytössä olevat laitteet, joista ei tarvitse olla pääsyä yrityksen sisäverkon palveluihin. Näin toimimalla esimerkiksi haittaohjelman saastuttama mobiililaitte ei pääse tunkeutumaan yrityksen sisäverkkoon.

4.3 Toiminnan tarkistaminen

Palvelinlaitteistojen toiminta tarkistettiin luvussa 4.1 kuvatulla tavalla erilaisten testiohjelmien avulla. Lisäksi järjestelmän toiminta varmistettiin käyttöjärjestelmän asentamisen jälkeen katsomalla sen lokitiedostoista, että kaikki halutut palvelut käynnistyivät suunnitellusti ja ettei lokimerkintöjen joukossa ollut virheilmoituksia, jotka olisivat antaneet viitteitä mahdollisista laitteisto- tai ohjelmisto-ongelmista tai virheistä asetusten määrittelyssä.

RAID-levyjärjestelmää käytettäessä on tärkeää varmistaa, että järjestelmä käynnistyy ja toimii, vaikka osa levypakan kiintolevyistä olisi vioittunut. Tämä tarkistettiin kytkemäl-

lä irti vuorotellen toinen levykasan aktiivisessa käytössä olevista kiintolevyistä ja toteamalla, että järjestelmä toimi kuten pitikin ja palvelimelle määritelty valvontajärjestelmä ilmoitti virhetilanteista odotetulla tavalla sekä lokimerkinnöillä että sähköposti-ilmoituksella. Yrityksen verkkoon liitetyiltä työasemilta varmistettiin, että levyjaot toimivat kuten aiemminkin ja käyttäjien luku- ja kirjoitusoikeudet verkkolevyjen eri hakemistoihin olivat kunnossa.

Uuden tietojärjestelmän käyttöönoton toisessa vaiheessa tietoliikenneyhteydet reititettiin kulkemaan uuden palvelimen kautta vanhan WLAN-reitittimen sijasta. Sen jälkeen varmistettiin, että verkkoon liitetyt laitteet saivat palvelimen DHCP-palvelimelta oikeat IP-osoitteet ja että yhteydet Internetiin sekä sisäverkon palveluille, kuten verkkolevyihin ja monitoimilaitteisiin, toimivat suunnitellusti. Palomuurin toiminta testattiin varmistamalla, että Internetin suunnasta sai yhteyden vain palvelimen SSH-palvelun porttiin ja että etäkäyttö toimi SSH-yhteyden sekä RDP-protokollaa käyttävän Remote Desktop Connection -ohjelman avulla.

Uuden langattoman verkon käyttöönoton yhteydessä tehtiin vastaavat tarkistukset kuin kaapelilla verkkoon liitettyjen laitteidenkin tapauksessa. Lisäksi varmistettiin, että langattoman verkon kuuluvuus riitti kattamaan yrityksen toimitilat kokonaisuudessaan ja että nopeus oli riittävä. Lisäksi kokeiltiin, ettei langattomasta vierasverkosta päässyt käsiksi yrityksen sisäverkon palveluihin, vaan ainoastaan Internetiin.

Palvelimen ja erityisesti varmuuskopiointijärjestelmän toimivuuden tarkkailua jatkettiin myös käyttöönoton jälkeen lokimerkintöjä seuraamalla ja tiedustelemalla käyttäjiltä kokemuksia järjestelmän toiminnasta.

4.4 Ylläpito

Yrityksen tietojärjestelmää suunniteltaessa on otettava huomioon myös järjestelmän ylläpidon toteutus ja kustannukset. Varsinkin tietoturva-aukkoja paikkaavien päivitysten säännöllinen asentaminen on tärkeää. Palvelimen käyttöjärjestelmän ja sen ohjelmistojen päivityksistä useimmat voidaan määritellä asentumaan automaattisesti, mutta osa päivityksistä voi vaatia niiden asentamisen ylläpitäjän toimesta ja myös Linuxin ytimeen kohdistuvat päivitykset vaativat koneen käynnistämisen uudelleen.

Etänä muutos- ja päivitystöitä tehtäessä on syytä varautua käymään myös paikan päällä palvelimen luona, sillä yhteys siihen voi katketa esimerkiksi asetusmuutoksen, järjes-

telmän virhetilanteen tai tietoliikenneyhteyden teknisen vian vuoksi. Osa edellä mainituista ongelmatilanteista voidaan ratkaista käynnistämällä laitteisto uudelleen etäohjattavan pistorasian avulla. Yleisimpiä vikatilanteita varten kannattaa laatia toimintasuunnitelma ja ohjeistaa myös yrityksen työntekijöitä suoriutumaan tietyistä vianselvitysprosessiin liittyvistä tehtävistä, kuten laitteiston käynnistämisestä uudelleen.

Tietojärjestelmän ylläpitotyöt sisältävät usein myös paljon muuta kuin ohjelmistopäivitysten asennuksia ja laitevikojen korjaamista. Yritykseen saatetaan hankkia uusia laitteita, jotka pitää määritellä käyttökuntoon ja myös muutokset henkilökunnassa vaativat usein käyttäjätunnusten, tiedostojen ja sähköpostitilien hallintaa. Näiden ylläpitotoimien hoitamista helpottaa oleellisesti yrityksen tietojärjestelmästä tehty ajan tasalla oleva dokumentaatio. Ongelmatilanteiden ratkaisussa puolestaan auttaa tietojärjestelmän hyvin toimiva etähallinta, joka kattaa niin verkon aktiivilaitteet kuin palvelimet ja työasematkin.

Ohjelmistopäivitykset

Linux-jakelupakettitoimittaja Opensusella on tarjolla kaksi erilaista jakelupakettia käyttöjärjestelmästänsä. Opensuse Leap on tavanomainen Linux-jakelu, jota päivitetään säännöllisin, ennalta määritellyin väliajoin uudempaan versionumeroon. Sen päivitykset on pyritty testaamaan mahdollisimman huolellisesti ja sen mukana toimitettavat ohjelmistot eivät välttämättä ole aivan uusimpia, vaan toiminnaltaan vakaiksi havaittuja versioita. (Opensuse 2019l.)

Opensuse Tumbleweedillä ei puolestaan ole versionumeroa, vaan se saa yksittäisten ohjelmapakettien päivityksiä sitä mukaa kuin niitä julkaistaan eli mahdollisesti vaikka viikoittain. Tumbleweed onkin tarkoitettu niille käyttäjille, jotka haluavat mahdollisimman nopeasti käyttöönsä uusimmat versiot ohjelmapaketeista ja niiden mukanaan tuomat uudet ominaisuudet. Sen haittapuolena on, että käyttöjärjestelmä saattaa kokea hyvinkin nopeasti merkittäviä muutoksia ja että sille julkaistuja ohjelmistoja ei ole välttämättä ehditty testata riittävästi ennen julkaisua. Jatkuvasti muuttuvan Tumbleweedin sijasta onkin suositeltavaa valita Leap sellaisiin käyttökohteisiin, joissa vaaditaan vakautta ja ennakoitavuutta järjestelmässä tapahtuvien muutosten osalta. (Opensuse 2019m.)

Jakelupakettitoimittaja pyrkii ylläpitämään Opensuse Leapin pääversiojulkaisuja (esimerkiksi Opensuse 15) vähintään 36 kuukautta, jonka jälkeen julkaistaan uusi pääver-

sio. Pienempiä versiopäivityksiä (15.1, 15.2. jne.) julkaistaan yleensä vuosittain ja toimittaja olettaa, että käyttäjät päivittävät niihin kuuden kuukauden sisällä niiden ilmestymisestä, jolloin niiden eliniäksi muodostuu 18 kuukautta. Leapin tapauksessa jakeluversion eliniän aikana siihen julkaistaan tietoturvapäivityksiä ja ohjelmistovirheiden korjauksia, mutta ei uusia ominaisuuksia. (Opensuse 2019b.)

Järkevintä on päivittää käyttöjärjestelmä säännöllisesti uusimpaan versioon, mikä takaa päivityspakettien saatavuuden ja helpon päivitystien seuraavaan versioon. Tukiajan loputtua ohjelmistotoimittaja ei enää julkaise tuotteelleen edes tietoturvapäivityksiä, minkä vuoksi siitä muodostuu ennen kaikkea merkittävä tietoturvariski, joka toteutessaan voi johtaa yrityksen tietojen tuhoutumiseen tai päätymiseen väriin käsiin. Lisäksi erittäin vanhan jakeluversion päivittäminen voi muodostua hankalaksi, koska se vaatii päivittämistä asteittain versio kerrallaan kohti uusinta versiota tai vaihtoehtoisesti koko käyttöjärjestelmän asentamista uudelleen. Liitteessä 3 on esitelty käyttöjärjestelmän versiopäivityksen tekemisen vaiheet komentorivipohjaisen Zypper-ohjelman avulla.

Opinnäytetyön toimeksiantajan kanssa sovittiin, että käyttöjärjestelmän tarjoamat päivityspaketit asennetaan pääsääntöisesti joka kuukauden ensimmäisenä maanantaina. Kriittiset tietoturva-aukot korjaavat päivitykset asennetaan kuitenkin niin pian kuin mahdollista, vaikka silloin ei vielä olisikaan sovittu kuukausittainen päivitysajankohta. Aikaa päivitysten asentamiseen varataan yksi tunti kuukautta kohden.

Opensuse Leap -Linux-käyttöjärjestelmän versiopäivitykset sovittiin hoidettavaksi valmistajan suositteleman kuuden kuukauden sisällä niiden ilmestymisestä, joka takaa sen, että järjestelmään on aina saatavilla uusimmat päivityspaketit (Opensuse 2019b). Aikaa järjestelmän versiopäivitysten asentamiseen varattiin kuusi tuntia päivitystä kohden.

Laitteistovikoihin varautuminen

Tietojärjestelmässä olevat laitteet eivät kestä ikuisesti. Järjestelmän osista ja toteutuksesta riippuen sen toiminta lakkaa joko kokonaan tai osittain, kun yksi sen osista viikaantuu. Laitteistoviat voivat ilmetä vielä niiden ollessa melko uusiakin, mutta useimmiten todennäköisyys rikkoutumiselle kasvaa sitä mukaa kuin laitteita käytetään ja niille kertyy ikää. Laitteiden hajoamisesta aiheutuvat riskit on siis tiedostettava ja niihin on myös varauduttava. Harva yritys pystyy nykyään jatkamaan toimintaansa ilman tietojär-

jestelmänsä ainakaan kovin pitkään. Yrityksen onkin päätettävä, onko sillä varaa menettää tärkeitä järjestelmänsä tallennettuja tietoja ja kuinka kauan se pystyy odottamaan järjestelmän korjaamista.

Laitteiden hajoamista voidaan yrittää ennaltaehkäistä hankkimalla mahdollisimman laadukkaita laitteita, mutta usein rajallinen hankintabudjetti pakottaa tekemään kompromisseja laadun ja kustannusten välillä. Myös laitteiden oikealla sijoituksella niille sopiviin olosuhteisiin ja oikeilla käyttötavoilla voidaan vaikuttaa niiden elinikään. Ulkokäyttöön tai pölyisiin tehdasolosuhteisiin ei siis kannata hankkia siistiin toimistoympäristöön tarkoitettuja laitteita ainakaan, jollei niiden kestävyyttä paranneta esimerkiksi olosuhteisiin sopivalla lisäkoteloinnilla. Vaativaan käyttöön suunniteltu laite saattaa olla hankintahinnaltaan kalliimpi, mutta todennäköisesti se myös kestää pidempään kuin tavanomaiseen käyttöön suunnitellut laitteet. Esimerkiksi palvelimen levyjärjestelmän kiintolevyiksi ei kannata valita kaikkein halvimpia työasemakäyttöön tarkoitettuja kiintolevyjä, vaan mieluummin nimenomaan palvelinkäyttöön suunniteltuja levyjä, joille korkeamman hankintahinnan vastineeksi luvataan myös pidempää käyttöikää.

Tärkeää on myös tarkkailla laitteiden toimintaa niin, että niiden viat voitaisiin havaita jo ennen laitteiden lopullista hajoamista. Esimerkiksi tietojen tallennukseen käytetyistä kiintolevyistä on mahdollista kerätä SMART-järjestelmän avulla useita erilaisia tietoja, joiden perusteella voidaan päätellä, milloin levyn kunto alkaa heiketä ja siten voidaan varautua vaihtamaan levy ennen sen hajoamista ja mahdollista tietojen menettämistä (Acronis 2019).

Jos järjestelmä on yrityksen toiminnalle tärkeä, kannattaa laitteita uusia jo ennen niiden hajoamista. Tällöin laitteiden vaihto voidaan tehdä suunnitellusti ja siten minimoida siitä aiheutuvan toimintakatkoksen pituus. On vaikea tarkalleen arvioida, kuinka kauan mikäkin laite tulee kestävänsä. Kiintolevyvalmistajat ilmoittavat tuotteilleen keskimääräisen vikaantumisvälin (engl. mean time between failure, MTBF), mutta sekään ei takaa, että juuri tietty laiteyksilö kestäisi odotetun ajan. Omien kokemusteni mukaan laadukkaatkin perinteiset liikkuvia osia sisältävät kiintolevyt saattavat yhtäjaksoisessa mutta kevyessä palvelinkäytössä kestää vain viidestä kahdeksaan vuotta. Toisaalta huonompi levy-yksilö saattaa osoittaa merkkejä sen kunnan heikkenemisestä jo muutaman kuukaudenkin käytön jälkeen, joten minkään kiintolevyn todellista elinikää ei voida taata. Varminta onkin tarkkailla levyjen kuntoa aktiivisesti, huolehtia säännöllisestä varmuuskopioinnista ja uusia levyt esimerkiksi viiden vuoden välein tai viimeistään, kun niistä ensimmäinen alkaa vikaantua.

Vaikka vikoja yritettäisiin ehkäistä ennalta mahdollisimman hyvin, tulee niitä kuitenkin vastaan ennemmin tai myöhemmin. Siksi onkin tärkeä, että yrityksellä on valmiit toimintasuunnitelmat eri ongelmatilanteiden varalta, jotta niistä voitaisiin toipua nopeasti aiheuttaen yrityksen toiminnalle mahdollisimman vähän haittaa. Huolellisen suunnittelun lisäksi ongelmiin voidaan varautua rakentamalla vikasietoisia järjestelmiä ja hankkimalla todennäköisimmin rikkoutuvien laitteiden varalle korvaavia laitteita, jotka voidaan ottaa käyttöön mahdollisimman nopeasti.

Palvelimen levyjärjestelmään saattaa olla viisasta hankkia varalle vähintään yksi kiintolevy. Se voidaan joko vaihtaa nopeasti RAID-levypakkaan rikkoutuneen levyn tilalle järjestelmän antaman hälytyksen perusteella tai ottaa automaattisesti käyttöön vikatilanteessa ennen kuin riski tietojen menettämisestä kasvaa entisestään sen myötä, että muutkin levyt mahdollisesti vikaantuvat. Paraskaan levyjärjestelmä ei kuitenkaan korvaa ajan tasalla olevia varmuuskopioita.

Palvelimen toimintaedellytyksiä voidaan vahvistaa myös hankkimalla sen perustaksi sellainen tietokone, jossa on kaksi virtalähdettä, joista rikkoutunut voidaan vaihtaa aiheuttamatta katkosta koneen toimintaan. Halvempi vaihtoehto kahdennetulle virtalähteelle on hankkia toinen virtalähde varalle odottamaan käyttöä. Sen vaihdosta aiheutuva toimintakatkos on joka tapauksessa lyhyempi kuin silloin, jos uusi osa pitäisi hankkia vasta vahingon tapahduttua.

Palvelinkoneen toiminnan kannalta keskeinen osa on myös sen emolevy. Sille voi olla vaikea löytää vastaavaa yhteensopivaa osaa kaupasta niinkin lyhyen ajan kuin vuoden tai kahden kuluttua sen hankinnasta, koska myynnissä olevien tuotteiden tekniikka uusiutuu niin nopeasti. Silloin emolevyn rikkoutuessa voidaan koko palvelin joutua rakentamaan käyttäen uuden tekniikan mukaisia muistimoduuleita, prosessoria ja emolevyä. Useita vuosia vanha palvelinkone onkin järkevää korvata kokonaan uudella laitteistolla jo ennen sen hajoamista, jollei vikojen varalle ole hankittu riittävästi yhteensopivia varaosia.

Vikasietoisuutta voidaan kasvattaa myös kahdentamalla järjestelmän toiminnan kannalta keskeisimmät laitteet. Ensisijaisen palvelinkoneen rinnalle voidaan rakentaa toinen palvelinkone, jonka ei välttämättä tarvitse olla yhtä tehokas sekä toimintavarma kuin pääasiallisen palvelimen. Tämä halvempi palvelin voi normaalitilanteessa toimia muissa tehtävissä, kuten varmuuskopiointilaitteena, mutta tarvittaessa se voidaan kuitenkin määrittellä hoitamaan vikaantuneen ensisijaisen palvelimen tehtäviä väliaikaisesti. Mi-

käli yrityksen Internet-yhteys on erillisen palomuurilaitteen ja verkkopäätelaitteen varassa, voidaan niille hankkia vastaavat varalaitteet, jotka on määritelty käyttövalmiiksi.

Järjestelmän parempi vikasietoisuus voidaan saavuttaa myös virtualisoinnin avulla sijoittamalla palvelut useammalle virtuaalikoneelle sen sijaan, että käytettäisiin fyysisiä palvelinkoneita. Virtualisoinnin myötä laitteistokomponenttien rikkoutumisesta aiheutuvista vikatilanteista voidaan selvittää oleellisesti nopeammin ja helpommin, kun virtuaalikoneet voidaan palauttaa toimintaan virtualisointialustalle, joka voi toimia aivan erilaisista osista kootulla fyysisellä palvelimella kuin alkuperäinen alusta. Virtualisoinnista on kerrottu tarkemmin luvussa 2.5. Tietojärjestelmän keskeytymättömän toiminnan tärkeys yritykselle ja sen toimintavarmuuden parantamiseen käytettävissä olevat rahavarat kuitenkin määräävät sen, millaisiin varotoimenpiteisiin on aiheellista ja mahdollista ryhtyä.

Järjestelmän toiminnan tarkkailu ja vikatilanteisiin reagoiminen

Asiakkaan kanssa sovittiin, että kuukausittaisen päivitysajankohdan yhteydessä varmistetaan lokitiedostoja seuraamalla, että järjestelmä toimii oikein. Mikäli toimenpiteitä aiheuttavia vikoja havaitaan, ilmoitetaan asiasta yrityksen edustajalle ja sen jälkeen korjaukset suoritetaan mahdollisimman pian ottaen huomioon vikojen vakavuusaste.

RAID-levyjärjestelmä määriteltiin ilmoittamaan vikatilanteista automaattisesti sekä asiakkaan että ylläpitäjän sähköpostiosoitteisiin. Lisäksi toiminta tarkistetaan kuukausittain myös käyttäen levyjärjestelmän tilan näyttävää komentoa `cat /proc/mdstat` ja varmistaamalla komennolla `smartctl`, ettei kiintolevyjen sisäisen SMART-valvontajärjestelmän lokitiedostomerkintöjen perusteella ole syytä epäillä levyn olevan rikki tai menossa rikki.

Varmuuskopioinnin toimivuus tarkistetaan kuukausittain lokitiedostomerkintöjen lisäksi tarkistamalla jokaisen varmuuskopioitavan koneen kohdalta sekä tiedostokokoja että päivämäärämerkintöjä tutkien, että kopiointi on suoritettu onnistuneesti.

Asiakkaan vastuulle jäi ilmoittaa ylläpitäjälle välittömästi, mikäli järjestelmän toiminnassa havaittaisiin ongelmia. Mahdollisten ohjelmisto- ja laitteistovikojen korjaaminen sovittiin aloitettavaksi viimeistään seuraavana arkipäivänä.

5 PÄÄTELMÄT

Opinnäytetyön tavoitteena oli suunnitella ja toteuttaa toimeksiantajan tarpeita vastaava edullinen, mutta silti monipuolinen tietojärjestelmä. Asetetussa tavoitteessa onnistuttiin erinomaisesti sekä toimeksiantajan että oman arvioni mukaan. Toimeksiannon lopputuloksena oli Linux-käyttöjärjestelmää ja edullista palvelinkonetta hyödyntävä tietojärjestelmä, jota voidaan tulevaisuudessa päivittää vastaamaan uusia käyttötarpeita. Ominaisuuksiltaan odotusten mukaisesti toimivan tietojärjestelmän lisäksi erityisen tyytyväinen toimeksiantaja oli siihen, että uusi palvelin saatiin otettua käyttöön aiheuttamatta häiriötä liiketoiminnalle. Lisäksi samalla toteutettua lähiverkon uudistamista ja uuden langattoman verkon käyttöönottoa pidettiin onnistuneena. Ero uuden ja vanhan langattoman verkon toiminnan välillä oli helposti havaittavissa varsinkin siinä, että uusi verkko kuului hyvin kaikissa toimitilojen osissa. Myös verkon tietoturva parantui oleellisesti.

Toimeksiannon suunnittelussa ja toteuttamisessa kohdattiin myös joitakin haasteita. Projekti aikataulua ei sovittu riittävän yksityiskohtaisesti, mistä aiheutui välillä epätietoisuutta eri työvaiheiden toteutusaikatauluista, vaikka kaikki sujuikin melko tarkasti kokonaisuutena mukaisesti. Myöskään kirjallista projektisuunnitelmaa ei tehty, vaikka se olisi auttanut sekä töiden aikatauluttamisessa että toteutuksen eri vaiheiden esittelyssä asiakkaalle. Toisaalta asiakas kiitti siitä, että kaikista muutoksista tiedotettiin etukäteen ja samalla kerrottiin, mitä yrityksen työntekijöiden mahdollisesti pitäisi huomioida omassa toiminnassaan eri työvaiheiden jälkeen.

Uuden tietojärjestelmän suunnittelun haasteena oli pitää kustannukset tavoitteen mukaisesti alhaisina samaan aikaan, kun kokonaisuudesta haluttiin tehdä myös riittävän vikasietoinen. Palvelinkoneen osalta tämä tarkoitti esimerkiksi sitä, että sen virtalähteeksi valittiin tavallinen edullinen virtalähde ja varalle hyllyyn vikatilannetta odottamaan hankittiin toinen vastaava osa, kun taas palvelimen täysin katkeamattoman toiminnan takaava kahdennettu virtalähde olisi maksanut nelinkertaisesti. Vastaavasti tietojen tallennukseen käytettyjen kiintolevyjen koossa ja niiden määrässä piti huomioida niiden hankinnan kokonaishinta. Kuhunkin käyttötarkoitukseen soveltuva ratkaisu onkin aina jonkinlainen kompromissi ominaisuuksien, vikasietoisuuden ja kustannusten välillä.

Projektin lopputuloksena asiakasyrityksessä käyttöön otettu ratkaisu osoittaa, että Linux-käyttöjärjestelmällä ja muilla ilmaisilla avoimen lähdekoodin sovelluksilla voidaan toteuttaa pienyritykselle monipuolinen tietojärjestelmä, jonka hankinta- ja ylläpitokus-

tannukset eivät nouse kohtuuttoman suuriksi. Laitteistokustannukset jäävät pieniksi ja suurin osa kustannuksista muodostuukin palvelimen ja sen ohjelmistojen asennus- ja määrittelytyöstä sekä ylläpidosta. Haasteena saattaakin usein olla työn osuuden arvioiminen kustannuksista etukäteen. Koska tietojärjestelmä on toteutettu käyttäen yleisesti saatavilla olevia laitteistokomponentteja ja avoimen lähdekoodin ohjelmistoja, voi tarvittavan järjestelmätyön ostaa melkein miltä tahansa alan koti- tai ulkomaiselta yritykseltä kilpailutuksen perusteella. Myös tietotekniikka-alan opiskelijoiden joukosta löytyy runsaasti Linux-osaajia.

Opinnäytetyössä esitelty tietojärjestelmäratkaisu on myös helposti muunneltavissa yrityksen kulloistenkin tarpeiden mukaiseksi. Sitä voidaan tarvittaessa päivittää asteittain ja se voidaan tarvittaessa myös korvata toiminto kerrallaan toisenlaisilla ratkaisuilla. Esimerkiksi reitittimen ja palomuurin tehtävät voidaan siirtää erilliselle laitteelle palvelimen jatkaessa silti tehtäviään tiedostojen jakamisessa ja varmuuskopioinnissa.

Yrityksien tietojärjestelmistä vastaavat henkilöt voivat käyttää opinnäytetyötä yhtenä tietolähteenään vertaillessaan eri vaihtoehtoja yrityksensä palvelinkoneen toteuttamiseksi. Muina päätöksen teossa auttavina tietolähteinä voivat toimia vastaavat Windows-palvelinkäyttöjärjestelmää ja kalliimpia palvelinlaitteistoja sekä ulkoistettuja pilvipalveluita koskevat tutkimukset. Opinnäytetyötä ei ole tarkoitettu käytettäväksi yksityiskohtaisena ohjeena palvelimen toteuttamisessa, mutta silti erityisesti Linux-palvelinratkaisuun päätyvät suunnittelusta ja toteutuksesta vastaavat tahot voivat käyttää opinnäytetyössä esitettyjä ratkaisuja ja toimintatapoja hyödykseen omissa projekteissaan.

Vaikka opinnäytetyön lopputuloksena toteutunut yrityksen tietojärjestelmä täytti sille asetetut vaatimukset, tuli opinnäytetyöprosessin aikana esille useita asioita, joiden avulla tietojärjestelmästä olisi saatu tehtyä vieläkin parempi ja monipuolisempi. Osa näistä asioista oli tiedossa jo työtä suunniteltaessa, mutta niitä ei toteutettu aikataulu- ja kustannussyistä.

Suurin osa kehitysajatuksista liittyi tietojärjestelmän vikasietoisuuden kasvattamiseen ja vikatilanteista toipumisen nopeuttamiseen. Kustannusten säästämiseksi kaikkia laitteistokomponentteja ei ollut mahdollista hankkia varalle, mutta vanhasta palvelinkoneesta olisi voinut tehdä varapalvelimen, joka pystyisi hoitamaan varsinaisen palvelinkoneen tehtäviä sen vikaantuessa. Linux-palvelimen olisi voinut toteuttaa myös virtualisointialustan päälle luotuna virtuaalipalvelimenä, joka olisi vikatilanteessa mahdollista pa-

lauttaa toimintaan varmuuskopiosta tarvittaessa myös toiselle fyysiselle palvelimelle. Tietojärjestelmästä ja sen uudistamisprojektista olisi myös ollut syytä tehdä kattava riskienhallintasuunnitelma. Lisäksi yleisimpien vikatilanteiden varalle luodut toimintasuunnitelmat nopeuttaisivat ongelmatilanteiden ratkaisua.

Palvelimen avulla voitaisiin toteuttaa myös etäkäyttö VPN-yhteytenä, joka olisi osalle yrityksen työntekijöistä helppokäyttöisempi vaihtoehto kuin käyttöön otettu SSH-yhteyteen perustuva ratkaisu, jossa on käytettävä useita eri ohjelmia riippuen siitä, mitä etäyhteyden avulla halutaan tehdä. Tiedostoja voisi olla hyödyllistä jakaa Internetiin myös omalla palvelimella toimivan palvelun kautta, mutta tämä vaatisi myös Internet-yhteyden nopeuden kasvattamista nykyisestä.

Yrityksen nykyistä varmuuskopiointijärjestelmää tulisi kehittää niin, että varmuuskopioita otettaisiin automaattisesti myös ulkopuoliselle palvelimelle Internetin välityksellä. Lisäksi ulkoiselle kiintolevyille tapahtuva kopiointi pitäisi tehdä niin helpoksi, että yrityksen työntekijöiden ei tarvitsisi kuin vaihtaa palvelimeen liitettyjä kiintolevyjä ennalta tehdyn suunnitelman mukaisesti. Palvelimessa olisi tällöin kiinni kerrallaan yksi ulkoinen kiintolevy ja yhtä tai useampaa muuta varmuuskopioita sisältävää levyä säilytettäisiin yrityksen toimitilojen ulkopuolella. Varmuuskopiointijärjestelmän tulisi myös tunnistaa paremmin yleisimmät varmuuskopioinnissa tapahtuvat virhetilanteet ja ilmoittaa niistä sähköpostitse.

Monet opinnäytetyössä melko pintapuolisesti käsitellyistä asioista voisivat sopia riittävän laajasti ja yksityiskohtaisesti käsiteltyinä omiksi tutkimusaiheikseen, mutta erityisen kiinnostavaa voisi olla selvittää virtuaalipalvelinten ja sekä maksullisten että ilmaisten virtualisointialustojen soveltuvuutta pienyritysten käyttöön. Myös kattavan kustannusvertailun tekeminen Windows- ja Linux-pohjaisten palvelintoteutusten välillä sekä hankinta- että ylläpitokulujen osalta saattaisi kiinnostaa monia yrityksiä.

Opinnäytetyön aiheen huolellisen rajaamisen jälkeenkin oli kirjallisen osuuden tuottamisessa suurena haasteena pitää teoriaa ja toteutusta koskeva asiasisältö riittävän yleisellä tasolla, jotta kokonaisuus ei kasvaisi sivumäärältään liian suureksi. Samalla oli silti kyettävä kertomaan asioista tarvittavassa laajuudessaan, jotta lopputuloksesta olisi hyötyä muille vastaavia toimeksiantoja tekeville. Tämän haasteen vuoksi opinnäytetyössä ei myöskään esitetä esimerkiksi eri ohjelmistojen asennustyövaiheita yksityiskohtaisesti tai kerrota niiden toiminnasta enempää kuin asian ymmärtämiseksi on välttämätöntä.

LÄHTEET

Acronis 2019. Knowledge base. 9636: S.M.A.R.T. monitoring. Viitattu 1.4.2019
<https://kb.acronis.com/content/9636>.

Al Agha, K.; Pujolle, G. & Ali Yahiya, T. 2016. Mobile and Wireless Networks. Hoboken: John Wiley & Sons, Inc.

Altaro 2017. Is ESXi Really Free? Let's put it to the Test. Viitattu 4.6.2019
<https://www.altaro.com/vmware/esxi-free/>.

The Apache Software Foundation 2019. Using Apache HTTP Server on Microsoft Windows. Viitattu 6.4.2019 <http://httpd.apache.org/docs/current/platform/windows.html>.

Archlinux 2019. Software access point. Viitattu 20.4.2019
https://wiki.archlinux.org/index.php/Software_access_point.

Bacula.org 2019. What is Bacula? Viitattu 11.4.2019 <https://www.bacula.org/what-is-bacula/>.

Bacula Systems 2019. Bacula Enterprise. Viitattu 11.4.2019 <https://www.baculasystems.com/>.

Blum, R. & Bresnahan, C. 2015. Linux Essentials. 2. painos. Indianapolis: John Wiley & Sons, Inc.

BWW Media Group 2018. Petri IT Knowledgebase. The Tenth Version of Exchange Shows There's Life in this On-Premises Server. Viitattu 6.4.2019 <https://www.petri.com/exchange2019-email-server>.

Cisco 2019. Networking basics: What you need to know. Viitattu 21.4.2019
<https://www.cisco.com/c/en/us/solutions/small-business/resource-center/networking/networking-basics.html>.

Distrowatch 2019. Top ten distributions. Viitattu 23.3.2019
<https://distrowatch.com/dwres.php?resource=major>.

Dovecot 2019. Mail server overview. Viitattu 14.4.2019
<https://wiki2.dovecot.org/MailServerOverview>.

Eaton Corporation 2012. UPS-käsikirja, Euroopan versio. Viitattu 23.3.2019
http://pqlit.eaton.com/ll_download_bylitcode.asp?doc_id=24030.

Eaton Corporation 2019. How to size a UPS. Viitattu 23.3.2019
<https://powerquality.eaton.com/thoughtleadership/choosing-ups/size-a-ups.asp>.

Experiencing IT 2019. LAN Routing and NAT with Windows Server 2016. Viitattu 4.6.2019
<https://www.experiencingit.net/windows/windows-server/lan-routing-nat-windows-server-2016/>.

Gentoo Linux 2019. Complete handbook. Software RAID. Viitattu 23.3.2019
https://wiki.gentoo.org/wiki/complete_handbook/software RAID.

IBM 2014. Overview of advantages of IMAP and POP3 protocols. Viitattu 21.4.2019
<https://www-01.ibm.com/support/docview.wss?uid=swg21414623>.

IBM 2017. Learn Linux, 101: Mail transfer agent (MTA) basics. Viitattu 14.4.2019
<https://developer.ibm.com/tutorials/l-lpic1-108-3/>.

Internet Systems Consortium 2019. ISC DHCP. Viitattu 8.4.2019
<https://www.isc.org/downloads/dhcp/>.

Kaario, K. 2002. TCP/IP-verkot. Jyväskylä: Docendo Finland Oy.

Kim, D. & Solomon, M. 2016. Fundamentals of Information Systems Security. 3. painos. Burlington: Jones & Bartlett Learning, LLC.

Linux Raid Wiki 2019. What is RAID and why should you want it. Viitattu 23.3.2019 https://raid.wiki.kernel.org/index.php/What_is_RAID_and_why_should_you_want_it%3F.

LWN 2019. The LWN.net Linux distribution list. Viitattu 23.3.2019 <https://lwn.net/distributions/#lead>.

MariaDB 2019. Installing MariaDB MSI Packages on Windows. Viitattu 6.4.2019 <https://mariadb.com/kb/en/library/installing-mariadb-msi-packages-on-windows/>.

Memtest86+ 2013. Memtest86+ - Advanced memory diagnostic tool. Viitattu 23.3.2019 <https://www.memtest.org/>.

Microsoft 2017. Active Directory domain services overview. Viitattu 21.4.2019 <https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/get-started/virtual-dc/active-directory-domain-services-overview>.

Microsoft 2018a. Remote desktop protocol. Viitattu 21.4.2019 <https://docs.microsoft.com/en-us/windows/desktop/TermServ/remote-desktop-protocol>.

Microsoft 2018b. Windows Server Blog. Windows Server 2019 Essentials update. Viitattu 4.6.2019 <https://cloudblogs.microsoft.com/windowsserver/2018/09/05/windows-server-2019-essentials-update>.

Microsoft 2019a. What's New in Windows Server 2019 Essentials. Viitattu 4.6.2019 <https://docs.microsoft.com/en-us/windows-server-essentials/get-started/what-s-new-19>.

Microsoft 2019b. System Requirements for Windows Server Essentials. Viitattu 4.6.2019 <https://docs.microsoft.com/en-us/windows-server-essentials/get-started/system-requirements>.

Microsoft 2019c. Comparison of Standard and Datacenter editions of Windows Server 2019. Viitattu 4.6.2019 <https://docs.microsoft.com/en-us/windows-server/get-started-19/editions-comparison-19>.

Microsoft 2019d. Client Access Licenses and Management Licenses. Viitattu 4.6.2019 <https://www.microsoft.com/en-us/licensing/product-licensing/client-access-license>.

Microsoft 2019e. Remote Access. Viitattu 4.6.2019 <https://docs.microsoft.com/en-us/windows-server/remote/remote-access/remote-access>.

Microsoft 2019f. SQL Server 2019. Viitattu 4.6.2019 <https://www.microsoft.com/en-us/sql-server/sql-server-2019>.

MySQL 2019. Download MySQL Community Server. Viitattu 6.4.2019 <https://dev.mysql.com/downloads/mysql/>.

Negus, C. 2010. Linux Bible 2010 Edition. Indianapolis: Wiley Publishing, Inc.

Network Admin Tools 2018. Zabbix vs. Nagios comparison for network and bandwidth monitoring. Viitattu 16.4.2019 <https://www.netadmintools.com/zabbix-vs-nagios-comparison>.

Nginx 2019. Nginx for Windows. Viitattu 6.4.2019 <http://nginx.org/en/docs/windows.html>.

Oliviero, A. & Woodward, B. 2014. Cabling: The Complete Guide to Copper and Fiber-Optic Networking. 5. painos. Indianapolis: John Wiley & Sons, Inc.

- Opensuse 2019a. Hardware requirements. Viitattu 23.3.2019
https://en.opensuse.org/hardware_requirements.
- Opensuse 2019b. Lifetime. Viitattu 23.3.2019 <https://en.opensuse.org/Lifetime>.
- Opensuse 2019c. Package management. Viitattu 23.3.2019
https://en.opensuse.org/Package_management.
- Opensuse 2019d. Support portal. Viitattu 23.3.2019 <https://en.opensuse.org/Portal:Support>.
- Opensuse 2019e. Opensuse FAQ. Viitattu 23.3.2019 <https://en.opensuse.org/openSUSE:FAQ>.
- Opensuse 2019f. Opensuse reference. Basic networking. Viitattu 8.4.2019
<https://doc.opensuse.org/documentation/leap/archive/42.3/reference/html/book.opensuse.reference/cha.basicnet.html>.
- Opensuse 2019g. Susefirewall2. Viitattu 8.4.2019 <https://en.opensuse.org/SuSEfirewall2>.
- Opensuse 2019h. Opensuse support database. Webmin. Viitattu 8.4.2019
<https://en.opensuse.org/SDB:Webmin>.
- Opensuse 2019i. Opensuse start-up. Installation. Installation steps. Viitattu 23.3.2019
<https://doc.opensuse.org/documentation/leap/startup/html/book.opensuse.startup/cha.install.html>.
- Opensuse 2019j. Opensuse reference. Using the expert partitioner. Viitattu 23.3.2019
https://doc.opensuse.org/documentation/leap/reference/html/book.opensuse.reference/cha.expert_partitioner.html.
- Opensuse 2019k. Mailinglist archive: opensuse-factory. Viitattu 23.3.2019
<https://lists.opensuse.org/opensuse-factory/2017-04/msg00584.html>.
- Opensuse 2019l. Leap portal. Viitattu 31.3.2019 <https://en.opensuse.org/Portal:Leap>.
- Opensuse 2019m. Tumbleweed portal. Viitattu 31.3.2019
<https://en.opensuse.org/Portal:Tumbleweed>.
- OpenVPN 2019. Community wiki and tracker. Viitattu 16.4.2019
<https://community.openvpn.net/openvpn>.
- Paananen, J. 2005. Tietotekniikan peruskirja. 6. painos. Jyväskylä: Docendo Finland Oy.
- Portnoy, M. 2016. Virtualization Essentials. 2. painos. Indianapolis: John Wiley & Sons, Inc.
- Psychz Networks 2019. Zabbix vs. Nagios vs. Cacti. Viitattu 16.4.2019
<https://www.psychz.net/client/question/en/zabbix-vs-nagios-vs-cacti.html>.
- Red Hat 2018. IBM to acquire Red Hat, completely changing the cloud landscape and becoming world's #1 hybrid cloud provider. Viitattu 23.3.2019
<https://www.redhat.com/en/about/press-releases/ibm-acquire-red-hat-completely-changing-cloud-landscape-and-becoming-worlds-1-hybrid-cloud-provider>.
- Red Hat 2019a. Mail delivery agent. Viitattu 14.4.2019
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/6/html/deployment_guide/s2-email-types-mda.
- Red Hat 2019b. What is KVM? Viitattu 4.6.2019
<https://www.redhat.com/en/topics/virtualization/what-is-KVM>.
- Rootusers 2016. How To Backup Windows Server 2016. Viitattu 4.6.2019
<https://www.rootusers.com/how-to-backup-windows-server-2016/>.

Samba.org 2019. What is Samba? Viitattu 8.4.2019
https://www.samba.org/samba/what_is_samba.html.

Savill, J. 2017. Mastering Windows Server 2016 Hyper-V. Indianapolis: John Wiley & Sons, Inc.

Sigmatic 2019. Varmatoimiset webhotellipalvelut. Viitattu 14.4.2019
<https://www.sigmatic.fi/palvelut/webhotellit>.

Silverstone Technology 2019. Home. Power supplies. Essential series. ET550-G. Viitattu 23.3.2019
<https://www.silverstonetek.com/product.php?area=en&pid=766>.

SSH Communications Security Oyj 2019a. SSH (Secure Shell). Viitattu 1.4.2019
<https://www.ssh.com/ssh/>.

SSH Communications Security Oyj 2019b. SSH port forwarding example. Viitattu 8.4.2019
<https://www.ssh.com/ssh/tunneling/example>.

Storagereview 2013. WD Red 4TB HDD review (WD40EFRX). Viitattu 23.3.2019
https://www.storagereview.com/wd_red_4tb_hdd_review_wd40efrx.

Suse 2019. SUSE Linux Enterprise Server 15 upgrade guide. 5.9 Migrate from openSUSE Leap to SUSE Linux Enterprise Server. Viitattu 23.3.2019
https://www.suse.com/documentation/sles-15/singlehtml/book_sle_upgrade/book_sle_upgrade.html.

Tatham, S. 2019. Putty. Viitattu 8.4.2019
<https://www.chiark.greenend.org.uk/~sgtatham/putty/>.

Techradar Pro 2018. Best Linux server distro of 2018. Viitattu 23.3.2019
<https://www.techradar.com/news/best-linux-server-distro>.

Tecmint 2019. Create an Active Directory infrastructure with Samba4 on Ubuntu. Viitattu 19.4.2019
<https://www.tecmint.com/install-samba4-active-directory-ubuntu/>.

Ubiquiti Networks 2019a. Unifi - Getting started FAQ. Viitattu 27.3.2019
<https://help.ubnt.com/hc/en-us/articles/360008150173-UniFi-Getting-Started-FAQ>.

Ubiquiti Networks 2019b. Unifi - Controller FAQ. Viitattu 27.3.2019
<https://help.ubnt.com/hc/en-us/articles/360008240754-UniFi-Controller-FAQ>.

Ubiquiti Networks 2019c. Unifi - Feature guide: Wireless uplink. Viitattu 27.3.2019
<https://help.ubnt.com/hc/en-us/articles/115002262328-UniFi-Feature-Guide-Wireless-Uplink>.

Ubuntu 2019a. Ubuntu 18.04. Ubuntu server guide. Email services. Mail filtering. Viitattu 14.4.2019
<https://help.ubuntu.com/lts/serverguide/mail-filtering.html.en>.

Ubuntu 2019b. Ubuntu 18.04. Ubuntu server guide. Samba. Print server. Viitattu 19.4.2019
<https://help.ubuntu.com/lts/serverguide/samba-printserver.html.en>.

Webmin 2019. What is Webmin? Viitattu 8.4.2019
<http://www.webmin.com/>.

Wikipedia 2019a. Linux distribution. Viitattu 23.3.2019
https://en.wikipedia.org/wiki/linux_distribution.

Wikipedia 2019b. List of Linux distributions. Viitattu 23.3.2019
https://en.wikipedia.org/wiki/list_of_linux_distributions.

Wikipedia 2019c. UPS. Viitattu 23.3.2019
http://en.wikipedia.org/wiki/uninterruptible_power_supply.

Wikipedia 2019d. IEEE 802.11. Viitattu 23.3.2019
https://en.wikipedia.org/wiki/ieee_802.11.

Winscp 2019. Introducing Winscp. Viitattu 8.4.2019
<https://winscp.net/eng/docs/introduction>.

Liite 1. Linux-palvelinkoneen hankintakustannukset

Tuotteiden hinnat 24.11.2017 Jimm's PC-Store Oy:ssä.

Komponentti	Merkki ja malli	Hinta e (ALV 0 %)
Proessori	Intel Core i3-8100 3,60 GHz LGA1151 6 MB Cache Boxed CPU (Coffee Lake)	99,84
Emolevy	Asus TUF Z370-PLUS GAMING, ATX	136,29
Keskusmuisti	Kingston 8 Gt (2x4 Gt) HyperX Fury DDR4 2666 MHz, CL15	79,84
Kiintolevyt (käyttöjärjestelmä)	2 kpl Western Digital 1 Tt, WD10EFRX, WD Red	117,5
Kiintolevyt (tiedostopalvelin)	3 kpl Western Digital 4 Tt, WD40EFRX, WD Red	384,68
DVD-asema	Asus DRW Super-Multi Black, Bulk, SATA	16,05
Kotelo	Fractal Design Define R5 Black, ATX	63,71
Virtalähde	Silverstone 550 W Essential Series ET550-G, ATX	60,40
Verkkokortti	Intel EXPI9301CT PCIe	34,19
Näppäimistö	Logitech Keyboard K120, USB, Nordic	15,32
Hiiri	Logitech B100 Optical Mouse, Black	8,06
Muut tarvikkeet (mm. kaapelit)	6 kpl SATA-kaapeli	29,03
Yhteensä e (ALV 0 %)		1 044,91

Liite 2. Windows-palvelinkoneen hankintakustannukset

Tuotteiden hinnat 30.5.2019 Verkkokauppa.com Oyj:ssä.

Komponentti	Merkki ja malli	Hinta e (ALV 0 %)
Palvelinkone	Dell EMC PowerEdge T440 - Intel Xeon Silver 4110 2,1–3,0 GHz - 8 Gt DDR4 2666 MHz RDIMM ECC - Kiintolevy 1 Tt (3,5" SATA, 7200 rpm, hot-plug) - DVD-RW -asema - Tornikotelo (5U) - 2 kpl verkkoliitännöitä - Virtalähde 495 W (hot-plug)	1 753,15
Kiintolevyt (käyttöjärjestelmä)	1 kpl Dell EMC 1 Tt (3,5" SATA, 7200 rpm, hot-plug)	170,89
Kiintolevyt (tiedostopalvelin)	3 kpl Dell EMC 4 Tt (3,5" SATA, 7200 rpm, hot-plug)	744,93
Lisävirtalähde	Dell EMC 495 W (hot-plug)	147,50
Takuulaajennus	Dell EMC Service ProSupport NBD Onsite (3 vuotta)	317,66
Näppäimistö	Logitech Keyboard K120, USB, Nordic	12,02
Hiiri	Logitech B100 Optical Mouse, Black	10,40
Yhteensä e (ALV 0 %)		3 156,55
Käyttöjärjestelmä	Microsoft Windows Server 2019 Essentials (OEM)	354,76
Käyttöjärjestelmä	Microsoft Windows Server 2019 Standard, 16 ydintä (OEM)	717,66
Käyttöjärjestelmä	Microsoft Windows Server 2019 Datacenter, 16 ydintä (OEM)	4 838,63
Käyttöjärjestelmän CAL-lisenssi (5 käyttäjää)	Microsoft Windows Server 5 User CAL 2019 (OEM)	179,76

Liite 3. Käyttöjärjestelmän versiopäivitys Zypper-ohjelmalla

1. Asenna kaikki päivitykset nykyiseen versioon:
`zypper refresh; zypper update`
2. Varmuuskopioi nykyisen käyttöjärjestelmän tiedostot (esim. hakemistot `/etc`, `/boot`, `/root` ja `/home`).
3. Päivitä aina versio kerrallaan kohti uusinta versiota (esim. 42.1 -> 42.2 -> 42.3).
4. Tarkista, mitkä asennuslähteet (repositoryt) ovat käytössä:
`zypper repos --uri`
5. Lisää sen version update-repository, johon olet päivittämässä:
`zypper addrepo --check --refresh --name 'openSUSE-Leap-42.3-Update' http://download.opensuse.org/update/leap/42.3/oss/ repo-update`
6. Jos asennuslähde `repo-update` löytyy jo, poista se ensin ja lisää sen jälkeen uudempi versio:
`zypper removerepo repo-update`
7. Päivitä järjestelmän paketit uusimpiin versioihin komennoilla `zypper-refresh` ja `zypper update`:
`zypper refresh; zypper update`
8. Tarkista komennolla `zypper repos --uri`, mitkä asennuslähteet ovat käytössä:
`zypper repos --uri`
9. Poista käytöstä mahdolliset kolmansien osapuolien asennuslähteet (esimerkiksi Libdvdcss Repository ja Packman Repository):
`zypper modifyrepo -d 7`
10. Varmuuskopioi kaikki käyttöön jäävät asennuslähteet ja muuta niiden URL:it uuden version mukaisiksi:
`cp -Rv /etc/zypp/repos.d /etc/zypp/repos.d.Old`
`sed -i 's/42.2/42.3/g' /etc/zypp/repos.d/*`
11. Päivitä uusien asennuslähteiden tiedot:
`zypper refresh`
12. Päivitä koko jakelupaketti hakien paketit etukäteen ennen asennusta (parametri `--download-in-advance`):
`zypper dup --download-in-advance`
13. Etsi mahdollisista aiemmin poistetuista kolmansien osapuolien asennuslähteistä uudet versiot ja lisää ne jommallakummalla komennolla:

```
zypper addrepo --name <name> <url> <alias>
```

```
zypper ar <url.repo>
```

14. Käynnistä kone uudelleen:

```
reboot
```

15. Lisäksi komennolla `zypper update` voidaan välillä varmistaa, että kaikki käytössä olevat paketit ovat uusimpia versioita.