Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

VESA VÄLITALO

Pienyrityksen tietotekninen konsultointi ja suunnittelu

SÄHKÖ- JA AUTOMAATIOTEKNIIKAN TUTKINTO-OHJELMA
2021

Tekijä(t) Välitalo Vesa	Julkaisun laji Opinnäytetyö, AMK	Päivämäärä huhtikuu 2021
	Sivumäärä 27	Julkaisun kieli Suomi
Julkaisun nimi **Pienyrityksen tietotekninen konsultointi ja suunnittelu**		
Tutkinto-ohjelma Sähkö- ja automaatiotekniikka		

Opinnäytetyön tarkoituksena oli tuottaa aloittavalle yritykselle suunnitelma tietoturvasta ja valita heidän käyttöönsä sopivat laitteet ja hankintatapa. Tarkoituksena oli myös tuottaa yritykselle suunnitelma laitteiden ylläpidosta ja huoltamisesta sekä niiden hallitusta vaihtamisesta laitteiden palvelusiän päättyessä. Lisäksi liitteinä yritykselle toimitettiin esimerkki dokumentit vikatilannepankista ja laiterekisteristä.

Opinnäytetyön tavoitteena oli aloittavan yrityksen tietoteknisen toiminnan alkuun saattaminen sekä laitteiden turvallisen käytön varmistaminen. Lisäksi tavoitteena oli varmistaa yrityksen laitteiden sujuva toiminta, koko niiden palvelusiän ajan sekä sujuva laitevaihto laitteiden käyttöiän päässä.

Opinnäytetyön lähtökohtana oli työn tilaajan lakiasiaintoimisto Lindholm & Gustafssonin tarve laitehankinnoille ja tietotekniselle konsultaatiolle yrityksen perustamisen alkuvaiheessa.

Teoriaosuudessa käsiteltiin tietoturvaan, laitehankintoihin ja ylläpitoon sekä tiedon tallentamiseen ja jakamiseen liittyviä kohtia. Opinnäytetyö tulee toimimaan pienyrityksen tietoteknisenä oppaana. Opinnäytetyö toteutettiin toiminnallisena opinnäytetyönä.

Asiasanat
Tietotekninen konsultointi, laitehankinnat, tietoturva

Author(s) Välitalo Vesa	Type of Publication Bachelor's thesis	Date April 2021
	Number of pages 27	Language of publication: Finnish

Title of publication
Small business IT consulting and planning

Degree program
Electrical and automation engineering

The purpose of this thesis was to make an information security plan and choose proper devices and the way of purchase for starting small business. In addition, the purpose was to make a maintenance plan and controlled replace plan for the company's devices. Malfunction document and device register documents are given to the company as an attachment.

The aim of this thesis was to help with the beginning of the IT operations in the starting company and ensuring the safe use of the devices. The other aim of this thesis was to ensure smooth function of the company´s devices throughout its planned operation life, and the fluent replacement of the device's.

The starting point of the thesis was the law firm Lindholm & Gustafsson's need for equipment purchases and IT consulting in the early stages of founding their company.

The theory part includes information security, device purchases and maintenance and file saving and sharing. The thesis will serve as an IT guide for law firm. The thesis was made as a functional thesis.

Key words
IT consulting, equipment purchases, security

SISÄLLYS

1 JOHDANTO

Opinnäytetyön lähtökohtana oli lakiasiaintoimiston tarve laitehankinnoille ja konsultaatiolle yrityksen perustamisen alkuvaiheessa. Toimeksiantona oli myös yrityksen käyttöön suunnatun oppaan tekeminen, jossa käsiteltäisiin aiheita, joita pienyritys tulee kohtaamaan omissa IT-hankinnoissaan ja ylläpidossa. Opinnäytetyö tulee toimimaan yrityksen tilaamana oppaana.

Työssä käsitellään tietoturvaa yleisellä tasolla esitellen hyviä tietoturvaan liittyviä tapoja. Lisäksi käsitellään yrityksen toiminnan alkuvaiheen hankintoja, jotta toiminnan aloittaminen olisi sujuvaa. Työssä annetaan perustelut erilaisille hankinnoille ja toimintatavoille. Työssä käsiteltävät perustelut tulevat omista hyviksi todetuista tavoista ja yleisistä suosituksista. Perustelujen ja esimerkkien on tarkoitus ohjata yritystä soveltamaan esiteltyjä aiheita ja tapoja omaan toimintaansa sopivaksi.

Opinnäytetyö toteutettiin projektimaisesti ja se täytti projektin tunnusmerkit. Projektilla tarkoitetaan johonkin tiettyyn asetettuun tavoitteeseen pyrkivää ja harkittua hanketta, jolla on oma aikataulunsa, omat resurssinsa ja oma organisaationsa. Jokainen projekti on ainutlaatuinen ja jokaisella projektilla on alku ja loppu. (Rissanen 2002, 14). Projekti-sanalle suomen kielessä käytetään sanaa hanke. Hanke kuitenkin usein viittaa yksitäistä projektia suurempaan kokonaisuuteen sillä hankkeessa voi olla useita pienempiä projekteja (Ruuska 2007, 18).

Työn tarkoituksena on tuottaa aloittavalle yritykselle suunnitelma tietoturvasta ja valita yrityksen käyttöön sopivat laitteet ja hankintatapa. Tarkoituksena on myös tuottaa suunnitelma laitteiden ylläpidosta ja huoltamisesta sekä niiden hallitusta vaihtamisesta laitteiden palvelusiän päättyessä. Lisäksi liitteinä yritykselle toimitetaan esimerkki dokumentit vikatilannepankista ja laiterekisteristä.

Projektin tavoitteena on aloittavan yrityksen tietoteknisen toiminnan alkuun saattaminen sekä laitteiden turvallisen käytön varmistaminen. Lisäksi tavoitteena on varmistaa yrityksen laitteiden sujuva toiminta koko niiden palvelusiän ajan sekä sujuva laitevaihto laitteiden käyttöiän päässä.

2 TIETOTURVA

Tietoturvallisuus on osa yrityksen jokapäiväistä toimintaa. Tietoturvalla pyritään turvaamaan yrityksen hallussa olevan tiedon perusominaisuuksia eli eheyttä, luottamuksellisuutta ja käytettävyyttä (Laaksonen, Nevasalo & Tomula 2006, 17). Tietoturvalla tarkoitetaan suojausta, joka kohdistuu suoraan tietoihin ja järjestelmiin. Tietoturvan toteutumisen kannalta käyttäjällä on suuri vastuu. Käyttäjän vastuulla on omien käyttäjätunnusten ja salasanojen turvallinen säilyttäminen ja käyttäminen. Huolimattomalla tunnusten käytöllä tai säilyttämisellä hyväkin järjestelmä on uhattuna (Järvinen 2012, 24).

Tietoturvan suojaan kuuluvat myös kaikki laitteet, jotka ovat jollain tavalla yhteydessä internettiin. Tietokoneet ja järjestelmät ovat yleisesti hyvin suojattuja mutta tietoturvan kannalta turvattomampia laitteita ovat IoT-laitteet. IoT-laitteilla tarkoitetaan kaikkia laitteita, jotka ovat yhteydessä internettiin, esimerkiksi älyvalojärjestelmät, autot, kodinkoneet ja viihde-elektroniikka. IoT-laitteita suunnitellaan helpoiksi käyttää ja ne ovat kuluttajaystävällisiä, mikä toisaalta laskee niiden tietoturvaa (Gilchrist, A. 2017, 6 & 29).

Oikeanlaisella laitteiden valinnalla yritys pystyy lisäämään tietoturvaa. Hankkimalla laitteita, joiden valmistajat panostavat tietoturvaan jo laitetasolla, lisää yrityksen tietoturvallisuutta. Android-puhelimista turvallisimpia ovat laitteet, jotka toimitetaan puhtaalla Android-käyttöjärjestelmällä. Puhtaalla käyttöjärjestelmällä tarkoitetaan käyttöjärjestelmää, johon laitteen valmistaja ei ole esiasentanut mitään ylimääräistä, vaan käyttäjä saa itse asentaa mitä tarvitsee. Nokia ja Google tarjoavat puhtaita käyttöjärjestelmiä puhelimissaan. Turvattomimpia laitteita ovat halvat Android

käyttöjärjestelmällä varustetut laitteet. Nämä puhelimet ovat yleisesti kevyeen käyttöön tarkoitettuja, eikä niissä ole tarpeeksi tehoa ajamaan erillistä torjuntaohjelmistoa. Torjuntaohjelmiston ajaminen näissä kevyissä puhelimissa aiheuttaa puhelimen hidastumista. Yrityksen on syytä valita tarpeeksi tehokkaat puhelimet käyttöönsä. Yrityksen käytössä oleviin puhelimiin ja tietokoneisiin on hyvä hankkia omat tietoturvaohjelmistot. Laitteiden valinnassa tulee huomioida torjuntaohjelmiston vaatimukset, sillä yleensä älypuhelimista keskusmuisti loppuu kesken. Älypuhelimissa tulisi olla vähintään 6gb keskusmuistia, mutta mielellään 8gb**.** Keskusmuistin loppuminen on myös kannettavien tietokoneiden ongelma. Kannettavissa tietokoneissa tulisi olla vähintään 8gb keskusmuistia, joka riittää kevyeen käyttöön. Suositeltavaa on kuitenkin hankkia kannettava tietokone, jossa keskusmuistia on 16gb. Laitevakioinnin ansiosta voidaan varmistua siitä, että laitteiden ominaisuudet ja tietoturvan taso säilyvät myös seuraavan hankintakierroksen laitteilla. Laitevakioinnilla tarkoitetaan yrityksen käyttöön soveltuvien laitemallien valintaa. Laitevakiointia tehdessä otetaan huomioon laitevalmistajan suunnitelmat mallisarjan jatkamiselle, jotta lähes samanlaisia laitteita voidaan käyttää jatkossa.

Yrityksen hyvään tietoturvaan kuuluu tietoturvaohjelmiston käyttö. Erillisellä torjuntaohjelmistolla saavutetaan parempi ja laajempi suojaus kuin käyttöjärjestelmään sisäänrakennetulla ohjelmistolla. Torjuntaohjelmisto tulee pitää päivitettynä, jotta saavutetaan tuoreimmat viruskuvaukset ja säilytetään tuvallisuus omilla laitteilla.

Työpaikalla tietoturvan toteuttaminen ei ole pelkästään ohjelmistojen hankintaa ja käyttöä. Turvallisuuteen tulee kiinnittää huomiota muutenkin kuin pelkästään torjuntaohjelmistojen kautta. Yrityksen tulisi määritellä omaan käyttöön ja ympäristöön tiettyjä sääntöjä, joilla luodaan lisää turvaa omaan toimintaan. Esimerkkinä voidaan mainita tietokoneiden ja puhelimien lukittuminen tietyn ajan kuluessa. Tällä estetään väärinkäyttö, jos käyttäjä jättää laitteensa huomiotta. Huomiota tulee myös kiinnittää USB- muistien käyttöön. Yritys voi hankkia omat muistit jokaiselle työntekijälle, jolla varmistetaan vain tietynlaisten ja omien muistien käyttö.

2.1 Tietosuoja

Tietosuojalla tarkoitetaan myös tiedon suojaamista kuten tietoturvalla, mutta suojaus kohdistuu ihmisten henkilötietoihin ja niiden yksityisyyden suojaamiseen. Tavoitteena on estää henkilötietojen tarpeeton ja epäasiallinen käyttö (Järvinen 2012, 12). Hyvin toteutetulla tietosuojalla pystytään estämään henkilötietoihin kohdistuvat tietoturvaloukkaukset. Henkilötietoihin kohdistuvilla loukkauksilla voi olla vakavia seurauksia, esimerkiksi henkilötietojen valvomiskyvyn menettäminen ja pahimmissa tapauksissa jopa identiteettivarkaus tai petos (Tietosuojavaltuutetun toimiston www-sivut 2020).

GDPR eli General Data Protection Regulation on vuonna 2018 voimaan tullut laki, jota sovelletaan kaikissa EU-maissa. Lainsäädännön tavoitteena on parantaa henkilötietojen suojaa ja yhtenäistää tietosuojasääntelyä EU-maissa. Tietosuoja-asetuksella suojataan henkilötietoja riippumatta niiden säilytystekniikasta. Henkilötietoja ovat tiedot, jotka liittyvät tunnistettuun tai tunnistettavissa olevaan henkilöön. Henkilötiedot voivat olla säilytyksessä omassa järjestelmässään tai paperiarkistossa (Tietosuojavaltuutetun toimiston www-sivut 2021).

2.2 Salasanat

Salasana on tällä hetkellä yleisimpiä todentamisen menetelmiä. Salasana on itsessään huono todentamisen väline, koska salasanat sisältävät lukuisia ongelmia, mitkä tekevät niistä yksinään heikkoja (Järvinen 2012, 112). Yleisimpiä ongelmia on käyttäjällä olevien salasanojen määrä, joita voi helposti olla jopa useita kymmeniä. Tämä taas houkuttaa käyttäjiä käyttämään samaa salasanaa monessa paikassa tai kirjoittamaan käyttäjätunnus-salasana pareja muistiin (Järvinen 2012, 112; Laaksonen, Nevasalo & Tomula 2006, 166). Vapaa-ajan ja työpaikan salasanat tulisi erotella toisistaan ja samaa salasanaa ei tulisi käyttää useammassa palvelussa. Tällä vähennetään tietojen menettämisen riskiä mahdollisen salasanamurron tai -vuotamisen tapahtuessa (Laaksonen, Nevasalo & Tomula 2006, 166)

Biometrinen tunnistautuminen on yleistynyt mm. älypuhelimien myötä. Biometrisellä tunnistautumisella tarkoitetaan automaattista tunnistamista sopivaa järjestelmää, joka

perustuu henkilön käyttäytymiseen tai biologisiin ominaisuuksiin kuten sormenjälkeen (Suomen Standardisoimisliiton www-sivut). Monista puhelimista löytyy nykyään ainakin sormenjälkitunnistus ja ainakin uusimmista puhelimista löytyy myös kasvojentunnistus. Biometrinen tunnistus yhdistettynä salasanatunnistautumiseen luo vahvan tunnistautumisen, vaikka salasana olisikin heikko (Järvinen & Rousku 2017, 57).

Biometrinen tunnistautuminen on myös käytössä tietokoneisiin kirjautuessa, yleisimmin kuitenkin kannettavissa tietokoneissa. Myös pöytäkoneille on saatavana erilaisia sormenjälki- ja kämmenlukijoita, joiden avulla biometrinen tunnistautuminen on mahdollista. Laitehankintoja tehdessä kannattaa perehtyä siihen, onko haluamallaan valmistajalla tuotteita, joissa olisi mahdollisuus joko sormenjäljen tai kämmenen tunnistamiselle. Esimerkiksi Fujitsu tarjoaa pöytäkoneisiin erillistä kämmentunnistinta, jonka voi sijoittaa haluamallaan tavalla. Lisäksi Fujitsu tarjoaa myös näyttöihin integroituja tunnistimia.

Vaikka salasanojen kirjoittamista muistiin ei suositella, niin turvallisempi vaihtoehto tietoturvan kannalta on luoda vahva salasana ja kirjoittaa se muistiin esimerkiksi omaan henkilökohtaiseen vihkoon. Vahva salasana estää ja hidastaa salasanojen murtoon käytettävien työkalujen toimintaa. Muistiin kirjoittamisessa kannattaa pitää huoli, että käyttäjätunnus-salasanapari ei olisi helposti ymmärrettävissä. Salasana voi olla esimerkiksi lause tai lauseen osa, joka on kirjoitettu muistiin paperille. Tätä tapaa voidaan pitää turvallisena, sillä käsin kirjoitettuihin salasanoihin hakkerit tai ohjelmat eivät voi päästä käsiksi. Jos salasanapaperia käsittelee turvallisesti ja säilyttää asiallisesti, se ei päädy vääriin käsiin muuten kuin fyysisen murron yhteydessä.

Salasanat kannattaa vaihtaa säännöllisesti, vaikka yrityksen omat järjestelmät eivät sitä vaatisi. Tällä estetään tilin väärinkäyttö, jos salasana päätyy vääriin käsiin. Sopivana vaihtovälinä voi pitää yhdestä kolmeen kuukautta.

2.3 Kaksivaiheinen tunnistautuminen

Kaksivaiheisella tunnistautumisella tarkoitetaan tunnistautumista kahdella toisistaan riippumattomalla tavalla. Yleisimmin kaksivaiheista tunnistautumista käytetään vahvistamaan kirjoitettua salasanaa. Kaksivaiheisessa tunnistautumisessa tunnistaudutaan salasanan lisäksi esimerkiksi tekstiviestillä tulevalla koodilla, sormenjäljellä, kasvontunnistuksella tai käytetään erillistä autentikointisovellusta kuten Google Authenticator. Kaksivaiheinen tunnistautuminen vahvistaa oman käyttäjätilin suojausta ja vähentää väärinkäyttöä, vaikka salasana vaarantuisi (Hernandes, L, 2020).

Kaksivaiheiseen tunnistautumiseen voidaan käyttää myös fyysisiä avaimia, jotka liitetään tietokoneen USB-liitäntään tai erilliseen kortinlukijaan. NFC ja bluetooth- teknologia mahdollistaa myös näiden fyysisten avaimien käytön langattomasti esimerkiksi mobiililaitteiden kanssa. Vastaavia laitteita on käytetty myös yrityksen sisäverkossa laitteella, joka näyttää pienellä näytöllä numerokoodin, jota käytetään kirjautumiseen (Vähimaa, A, 2019).

Kaksivaiheinen tunnistautuminen on ollut käytössä maksamisessa jo kauan. Käyttäjä tarvitsee sirukortin lisäksi kortin PIN-koodin, jotta maksaminen onnistuu. Kaksivaiheisen tunnistautumisen käytöllä vähennetään mahdollisia tunnusten väärinkäyttöjä (Nieminen, J, 2017).

Kaksivaiheinen tunnistautuminen kannattaa ottaa käyttöön, jos se vain on mahdollista. Tällä lisätään huomattavasti palvelun turvallista käyttöä. Monet sovellukset on mahdollista varustaa kaksivaiheisella tunnistautumisella, kuten esimerkiksi googlen palvelut.

2.4 Palomuuri

Palomuurilla tarkoitetaan ohjelmistoa tai laitteistoa, joka vastaa tietoliikenteen tarkistamisesta ja suodattamisesta. Palomuuri voi olla ohjelmistollinen, millä tarkoitetaan esimerkiksi käyttöjärjestelmiin rakennettuja palomuureja (Järvinen, P. 2012. 189).

Palomuuri voi olla myös oma laitteensa eli laitepalomuuri, joita käytetään yleensä isoissa yritysten verkoissa. Laitepalomuuria pidetään turvallisempana vaihtoehtona, koska laitepalomuuria ei käyttäjä pysty itse ottamaan pois käytöstä eikä myöskään laitepalomuuria pysty sammuttamaan ohjelmistollisesti. Laitepalomuuri suojaa myös kaikkia verkon laitteita. Päätelaitteissa voidaan vielä käyttää ohjelmistollista palomuuria lisävarmuutena, mutta väärin konfiguroituna sisäkkäiset palomuurit aiheuttavat ongelmia verkkoliikenteessä. Useimpiin reitittimiin, joita myydään niin kotikäyttöön kuin yrityskäyttöön, on sisäänrakennettuna laitepalomuuri. Reitittimiin sisäänrakennetuissa laitepalomuureissa ei ole yhtä paljon ominaisuuksia kuin erillisessä palomuurilaitteessa (Järvinen, P. 2012. 190).

Palomuurille voidaan tarvittaessa määritellä rajoituksia tulevalle ja lähtevälle liikenteelle. Palomuuria ei tule missään tilanteessa ottaa pois käytöstä, sillä se aiheuttaa yrityksen verkon ja koneiden saastumisen. Jos palomuuri aiheuttaa yrityksen verkon ja ohjelmien käyttöön ongelmia, tulee ongelma ratkaista palomuurin konfiguroinnilla eli asetusten muuttamisella.

2.5 NAT

NAT on lyhenne sanoista Network Address Translation eli osoitteenmuunnos. Se tarkoittaa oman verkon laitteiden IP-osoitteiden muuttamista yhdeksi julkiseksi osoitteeksi ja toisinpäin. Osoitteenmuunnoksen suorittaa joko reititin tai palomuuri. NAT voidaan konfiguroida siten, että ulkoverkosta ei pysty IP-osoitteiden perusteella päättelemään, montako laitetta verkossa on (Järvinen, P. 2012. 194).

NAT kehitettiin alun perin säästämään julkisia IP-osoitteita. NAT voidaan jakaa kahteen tyyppiin, staattiseen ja dynaamiseen. Staattisessa osoitteenmuutoksessa on varattu jokaiselle sisäverkon osoitteelle oma julkinen osoite. Dynaamisessa osoitteenmuutoksessa on varattu tietty määrä julkisia IP-osoitteita, joita otetaan käyttöön sitä mukaa kun tarvetta tulee (Lammle, T. 2005. 95).

Saapuvan liikenteen osoitteen muutoksella voidaan lisätä yrityksen tietoturvaa tietoliikenteen osalta. Yrityksen laitteisiin ei saada suoraa yhteyttä, kun NAT on käytössä. Tämä aiheuttaa toisaalta ongelmia erilaisille sovelluksille, jotka vaativat suoraa yhteyttä ja yhteyden pysymistä auki toimiakseen. Yleisesti osoitteenmuutoksen hoitaa yrityksen reititin, ellei sitä ole erikseen määritelty esimerkiksi palomuurille. Reitittimissä osoitteenmuunnos on oletuksena päällä, mutta reitittimestä riippuen on mahdollista valita NAT:in tyyppi.

Esimerkiksi Huawei 5G cpe pro reitittimestä löytyy NAT:in valinnalle kaksi eri vaihtoehtoa. Valittavana on symmetrinen NAT, jota käytetään, kun on korkeat turvallisuusvaatimukset. Valittavana on myös kartiomainen NAT, jolla suojaustaso ei ole niin korkea, mutta se mahdollistaa paremman sopivuuden laitteisiin ja sovelluksiin, jotka vaativat suoran yhteyden laitteisiin. Omalta internetpalveluntarjoajalta on mahdollista myös tilata oma julkinen IP-osoite.

2.6 VPN

VPN eli Virtual Private Network tarkoittaa virtuaalista erillisverkkoa, jota käytetään luomaan suojattu yhteys julkiseen verkkoon. VPN:in avulla voidaan päästä käsiksi yrityksen sisäverkossa toimiviin ympäristöihin yrityksen oman verkon ulkopuolelta (Henmi, Lucas, Singh & Cantrell, 2006. 212).

VPN:in ollessa käytössä verkkoliikenne ohjataan erillisen VPN-palvelimen kautta, jolloin käyttäjän oma IP-osoite ja sijainti pysyvät salattuna (F-Secure www-sivut 2021). VPN-yhteyttä voidaan käyttää palveluntarjoajan tarjoamalla sovelluksella tai Windows 10- käyttöjärjestelmään rakennetulla VPN-profiililla. Käyttämällä käyttöjärjestelmän VPN-profiilia, tulee käyttäjän tietää oman VPN-palvelun palvelimen osoite, kirjautumistiedot ja mahdollisia lisäasetuksia (Microsoft tuki www-sivut).

VPN:in käyttöönotossa kannattaa tarkastella millainen tapa on itselle soveltuva. Suosittelen kokeilemaan palveluntarjoajan tarjoamaa sovellusta, mutta kannattaa myös

kokeilla VPN-profiilin luomista Windows 10- käyttöjärjestelmän asetuksista. Kokeilemalla selviää, kumpi edellä mainituista tavoista sopii paremmin omaan käyttöön.

VPN tulee ottaa käyttöön aina, kun tehdään töitä yrityksen oman verkon ulkopuolelta. Palveluntarjoaja kannattaa valita huolella, sillä erityisesti ilmaiset VPN-palvelut ovat vaarallisia. Nämä palvelut eivät piilota käyttäjänsä IP-osoitetta ja sijaintia, ja ne tarkastelevat ja jopa poistavat tietoja käyttäjän laitteelta. Edellä mainittujen syiden vuoksi kannattaa valita luotettava palveluntarjoaja.

3 LAITEHANKINNAT JA YLLÄPITO

3.1 Laitehankinnat

Yrityksen laitteiden hankinta on oleellisena osana yrityksen perustamista. Laitteiden oikeanlaisen valinnan avulla mahdollistetaan yritykselle toimiva kokonaisuus, joka kestää laitteille suunnitellun käyttöiän loppuun asti. Laitteiden hankinta aloitetaan määrittelemällä omat tarpeet, eli mitä esimerkiksi tietokoneilta ja lisälaitteilta kuten näytöiltä vaaditaan. Laitehankinnoissa tulee ottaa huomioon työpisteen ergonomia ja mahdollisuuksien mukaan työntekijän vaatimukset. Samaa prosessia voidaan käyttää verkkolaitteiden hankinnassa, kuten myös tulostimien valinnassa (Kurki 2010, 47).

Laitehankinnat voidaan hankkia hajautetusti tai keskitetysti. Keskitetyllä hankinnalla yrityksen kaikki laitteet hankitaan samalta toimittajalta. Hankintatapa tulee suunnitella omaan käyttöön sopivaksi. Pääsääntöisesti laitteet hankitaan joko omistuslaitteiksi tai leasingperiaatteella. Yrityksen tulee miettiä omaan tarkoitukseen sopiva hankintamuoto, joka palvelee parhaalla mahdollisella tavalla yritystä ja sen toimintaa (Kurki 2010, 45).

Laitehankinnoissa kannattaa ottaa huomioon laitevakiointi. Laitevakioinnilla tarkoitetaan laitteita, joita valmistaja valmistaa useamman vuoden lähes muuttumattomana.

Tällä saavutetaan käyttöönotossa etuja, sillä yleensä vanhojen laitteiden tarvikkeet sopivat myös uusiin, kuten esimerkiksi kannettavien tietokoneiden telakat. Uudelle laitehankintakierrokselle lähdettäessä tulee selvittää uusien laitteiden yhteensopivuus vanhoihin. Jos yrityksen kaikki laitteet ovat hankittu leasingperiaatteella ja uudet hankittavat tietokoneet sopivat vanhoihin telakoihin, on kannattavaa lunastaa kaikki muut laitteet itselle, paitsi kannettavat tietokoneet. Näyttöjä, näppäimistöjä ja hiiriä ei tarvitse uusia leasingsopimuksen loputtua, sillä ne ovat yleensä pitkäikäisiä ja niiden saatavuus on hyvä, eikä käyttöönotto ei vaadi kuin laitteen kytkemisen tietokoneeseen.
Laitehankintoja tehdessä tulee jokainen hankittu laite tietoineen täydentää laiterekisteriin (Liite 1). Laiterekisteri on yrityksen laitteiden dokumentaatioon tarkoitettu dokumentti, josta näkee kaikki yrityksen hankkimat laitteet ja niiden tiedot. Laiterekisteriin tulisi merkitä laitteen valmistaja ja malli. Tämän lisäksi on tärkeää merkitä myös laitteen sarjanumero. Sarjanumeroa voi tarvita takuukysymyksissä tai mahdollisesti laitteen rekisteröintitilanteissa. Syytä olisi myös merkitä laitteen hankintapäivä, hankintatapa eli omistus tai leasing ja laitteen takuuajan pituus. Takuutietojen lisääminen helposti luettavaan taulukkoon helpottaa ja nopeuttaa takuun selvittämistä tarvittaessa.

Taulukkoon voi halutessaan lisätä laitteen käyttäjän. Laiterekisteriä tulee päivittää aina kun laitteita tulee yrityksen käyttöön. Kun laitteiden määrä on pieni, riittää yksi dokumentti, johon lisätään laitteita niiden saapuessa. Laiterekisteriin on hyvä merkitä laitteiden poistuminen yrityksen käytöstä joko poistamalla ne kokonaan taulukosta tai korostamalla poistuneet koneet esimerkiksi punaisella värillä.

Halutessaan yritys voi tehdä esimerkiksi tietokoneille, tulostimille ja näytöille oman dokumentin ja lisälaitteille kuten hiiret, näppäimistöt ym. oman dokumentin. Laiterekisterin käyttö helpottaa laitteiden hallintaa ja takuutilanteissa se on erityisen tärkeä. Rekisteristä näkee nopeasti omat laitteet ja niiden sarjanumerot, joita tarvitaan takuuasioiden etenemiseen. Rekisteristä löytyy myös takuuajan pituus ja laitteen toimittaja.

3.2 Leasing

Leasing on terminä laaja ja käsittää käytännössä erilaisia vuokrasopimuksia. Leasingsopimuksella yksityiset ja yritykset voivat hankkia käyttöönsä esimerkiksi IT-laitteita (Tepora 2013, 116). IT- ja konttorilaitteet hankitaan yleensä käyttöoikeusleasingilla, joka on verrattavissa tavalliseen esineen vuokraan mutta eroaa siten, että vuokraaja sitoutuu huolehtimaan esineen huollosta ja ylläpidosta (Tepora 2013, 128).

Leasingsopimuksen päättyessä yritys voi lunastaa laitteet itselleen tai yritys palauttaa laitteet takaisin vuokraajalle. Laitteiden eri hankintatavoilla on omat etunsa. Omaksi ostamalla saadaan yleensä kustannussäästöjä, kun ei tule maksuja rahoitus- ja korkokuluista. Omistuslaitteiden kohdalla yrityksen on helpompi ajoittaa laitteiden vaihdot uusiin oman työtilanteen siihen soveltuessa, tai laitteita voidaan vaihtaa porrastetusti. Leasingin etuina ovat tasaiset kulut, jotka on helpompi budjetoida koko sopimuskaudeksi**.** Yritys voi vähentää leasingmaksut vähennyskelpoisina kuluina verotettavasta liikevaihdosta. Leasingmaksut eivät rasita yrityksen tasetta, koska laitteet ovat vuokralla eivätkä yrityksen omaisuutta. Leasing mahdollistaa laitteiden säännöllisen vaihtamisen uusiin sopimuskauden päätyttyä. Tällöin yrityksellä on käytössään jatkuvasti uusia laitteita ja laitteet tulee vaihdettua säännöllisesti ja laitevakiointi pysyy samana (Itaito www-sivut).

Leasingsopimuksia on eri pituisia. Yrityskäytössä oleville kannettaville tietokoneille hyvä leasingsopimuksen pituus on 36 kk. Tämä on hyvä vaihtoikä yrityskäytössä oleville kannettaville tietokoneille. Leasingsopimuksesta kannattaa tarkastaa mahdolliset ehdot leasingajan ylitykselle ja ehdot laitteiden omaksi lunastamiselle. Leasingsopimuksen lähestyessä loppuaan kannattaa olla yhteydessä toimittajaan uusien laitteiden valintaa varten hyvissä ajoin.

3.3 Laitteiden ylläpito

Yrityksen toiminnan kannalta toimivat ja luotettavat laitteet ovat tärkeitä. Pienellä vaivalla voidaan mahdollistaa laitteiden moitteeton toiminta niiden vaihtoiän päähän. Laitteiden hallitulla ja suunnitellulla vaihdolla pyritään saavuttamaan mahdollisimman nopea ja mahdollisimman vähän töitä häiritsevä laitteiden uusiminen. Laitteiden

hallitulla vaihdolla pystytään aloittamaan valmistautuminen laitteen vaihtoon jo ennakkoon. Mahdollisesti määritellään uudelleen omat tarpeet, jos edellinen hankinta ei ole ollut täysin onnistunut tai työnkuva ja laitteen käyttö on muuttunut tai on muuttumassa. Valmistautumisella myös minimoidaan menetettävän datan määrä ja keskeneräisten töiden häviäminen tai lykkääntyminen laitevaihdon takia (Pratt, M. 2014).

Samaa laitteidenvaihtosysteemiä kannattaa soveltaa myös yrityksen muihin laitteisiin. Esimerkiksi tulostimissa tulee helposti ongelmia, kun ne ikääntyvät ja niitä on hankalampaa korjata ja huoltaa kuin muita laitteita. Verkkolaitteet ja näytöt kestävät yleensä pitkään, mutta rikkoutuessaan ne saattavat estää työnteon. Tällaisiin tilanteisiin olisi hyvä varautua.

Laitevaihtoon kannattaa varautua ennakkoon. Kannattaa aloittaa omien tarpeiden tarkastelusta ja omasta tyytyväisyydestä edelliseen laitehankintakierrokseen. Tämän jälkeen tulee tarkastaa mitä laitteita ollaan hankkimassa vanhojen tilalle ja vaatiiko uusien laitteiden käyttöönotto muita laitevaihtoja. Onnistuneen laitevakioinnin avulla mahdollistetaan seuraavan hankintakierroksen laitteiden sopivuus jo olemassa oleviin lisälaitteisiin. Käyttäjän on hyvä käydä vanha kone läpi ja tarkistaa, että kaikki tärkeät tiedot on kopioitu jo muualle. Kannattaa myös tehdä itselle listaus omista ohjelmistoista ja selaimista, joita on tottunut käyttämään.

Selaimista kannattaa ottaa kirjanmerkit ja kansiot talteen. Jokainen selain on hieman erilainen, mutta kaikista pystyy tallettamaan kirjanmerkit omaan tiedostoonsa ja palauttamaan ne tiedostosta. Tietenkin pitää muistaa tallettaa tiedostot ulkoiseen sijaintiin vaihtuvasta koneesta. Uuden koneen käyttöönoton yhteydessä päivitetään laiterekisteriin (LIITE 1) koneen tiedot.

Laitteiden kovalevyjen tyhjentäminen ennen koneiden hävittämistä tulee tehdä, jos laitteet ovat yrityksen omistuksessa. Leasinglaitteiden toimittajat hoitavat yleensä kovalevyjen tyhjentämiset koneiden luovuttamisen jälkeen, mutta tämä pitää kuitenkin tarkistaa sopimuksesta.

Omistuslaitteiden kohdalla vaihdot kannattaa suorittaa säännöllisesti. Kannettaville tietokoneille yrityskäytössä sopiva vaihtoväli on 36 kuukautta. Pöytäkoneiden sopiva

vaihtoväli yrityskäytössä on 48 kuukautta. Näillä vaihtoväleillä varmistetaan koneiden toimivuus koko niiden käyttöiän ajan. Omistuskoneiden kohdalla vaihdot on helpompi sovittaa omaan aikatauluun sopivaksi ja mahdollistaa vaihtoajan tarkastelun ja pidentämisen. Jos koneet ovat toimineet 36 kuukautta moitteettomasti, niin voisi ehkä olla kannattavaa siirtää vaihtoa vielä 6 tai 12 kuukautta. Kuitenkaan koneiden vaihtamista ei kannata jatkuvasti siirtää. Koneiden yllättävästä hajoamisesta toipumiseen voi mennä useita päiviä ja mahdollisesti vielä menetetään tietoja, ellei niitä ole juuri varmuuskopioitu.

Säännöllisillä vaihdoilla vähennetään koneiden yllättäviä hajoamisia ja töiden menettämistä ja näistä palautumiseen kuluvaa aikaa merkittävästi. Esimerkiksi hallittu koneiden vaihto vie yhden työpäivän ja tiedostoja ei menetetä. Yllättävällä koneen hajoamisella kuluu helposti viikko ennen kuin on palattu lähtötasolle, joka oli ennen koneen hajoamista. Lisäksi koneen hajoamispäivän työt voidaan menettää.

3.4 Takuu

Takuun antamisella tarkoitetaan sitä, että yritys sitoutuu vastaamaan tuottamansa tavaran käyttökelpoisuudesta ja ominaisuuksista määrätyn ajan. Takuunantaja vastaa takuuaikana aiheutuvista ja ilmenevistä vioista. (Kilpailu- ja kuluttajaviraston www-sivut).

Laitehankinnoissa takuu kannattaa ottaa huomioon. Takuun pituus ja taso tulee olla tarpeeksi kattava. Yleisesti laitteiden perustakuu kattaa rikkoutuneen laitteen varaosat, mutta laite pitää erikseen toimittaa korjattavaksi, mikä aiheuttaa useiden päivien keskeytyksen töihin. Laitteita voi hankkia myös takuupaketilla, johon kuuluvat tarvittavat varaosat ja korjaustyö asiakkaan omissa tiloissa. Myös takuun käsittelyajat vaihtelevat takuun tason mukaan muutamista tunneista useisiin päiviin (Itaito www-sivut).

3.5 Vikasietoisuus ja toipuminen

Vikasietoisuudella tarkoitetaan laitteiden ja järjestelmien kykyä ja mahdollisuuksia toimia ilman ongelmia. Vikasietoisuutta pitää ylläpitää laitteiden koko käyttöiän ajan. Vikasietoisuuden ylläpitämisellä mahdollistetaan vikatilanteiden syntyminen niiltä osin kuin niihin pystyy itse vaikuttamaan. Varautuminen erilaisiin ongelmiin lisää vikasietoisuutta. Tietokoneiden ja puhelimien akkujen pitäminen ladattuina mahdollistaa työskentelyn myös sähkökatkon aikana. Sähkökatkoihin voi myös varautua hankkimalla UPS-laitteet kriittisimpien laitteiden yhteyteen. Tämä mahdollistaa työskentelyn sähkökatkon ajan. UPS eli Uninterruptible power supply on itsenäisesti verkkovirrasta latautuva varavirtalaite, jonka tehtävänä on sähkökatkon aikana antaa virtaa siihen kytkettyihin laitteisiin. Varavirtalaitteen käyttäminen mahdollistaa töiden tallentamisen ja koneiden hallitun sammuttamisen sähkökatkon aikana (Ylä-Jääski, V. 2012).

Mahdollisten selainten toimintavirheille voi varautua pitämällä asennettuna ja päivitettynä useamman selaimen. Hyvä olisi myös jakaa selainten välillä samat kirjainmerkit ja kansiot, jotta työskentelyn jatkaminen toisella selaimella olisi sujuvaa ja nopeaa. Näillä pienillä panostuksilla voidaan vähentää turhautumista. Jos käytössä on esimerkiksi langattomia hiiriä ja näppäimistöjä, kannattaa pitää niihin varaparistoja tallessa.

Vikatilasta toipumisella tarkoitetaan kulunutta aikaa ja tehtäviä töitä, joita vaaditaan päästäkseen samaan tilaan mitä oli ennen virheen tapahtumista. Pienessä yrityksessä virheestä toipuminen tapahtuu yleensä nopeasti, kun laitteita on vähän ja ympäristö on pieni. Vian etsintä aloitetaan ja vika pyritään paikantamaan ja korjaamaan mahdollisimman nopeasti ja tehokkaasti.

Vikatilanteen syntyessä on hyvä kirjata dokumenttiin, minkälainen toiminta aiheutti vian ja miten vika huomattiin sekä vian kuvaus. Dokumenttia on hyvä päivittää samalla kun tekee vian etsintää ja korjaustoimenpiteitä. Jatkossa kun vikatilanteista on tehty dokumentteja, on samanlaisista vikatiloista nopeampi toipua. Tällä nopeutetaan toipumista, jos vika on hankala korjata tai se vaatii aikaa. Dokumentteja on myös hyvä päivittää, kun vika ilmenee uudestaan. Jos dokumentaatio on tehty hyvin ja selkeästi,

niin kokematonkin työntekijä pystyy dokumentin avulla toipumaan vikatilanteesta, jota ei ole ennen kohdannut (Dines, R. 2012).

Vikatilanteita varten löytyy vikatilanneraportti (Liite 2) jota tulisi käyttää aina kun kohdataan jokin ongelma. Vikatilanneraporttien avulla luodaan yrityksen omaan käyttöön vikatilannepankki, johon raportoidaan kaikki kohdatut vikatilanteet. Raportin ja pankin tarkoituksena on toimia tulevaisuudessa apuna, kun vastaavanlainen vikatilanne kohdataan uudestaan. Kaikkein pienimmistä ongelmista ei ole välttämätöntä kirjoittaa raporttia, mutta vähänkään suuremmista se olisi hyvä kirjoittaa, sillä dokumentti nopeuttaa vastaavanlaisen ongelman ratkaisemista. Hyvin tehty raportti voi mahdollistaa vian korjaamisen täysin itse ilman ulkopuolista apua. Raporttiin kirjataan vikatilanteen nimi, päivämäärä ja kirjaaja. Raportissa tulee myös kuvailla vikatilanne tarkemmin, mitä tehtiin tilanteen ratkaisemiseksi, missä järjestyksessä korjaavat toimet tehtiin ja tarvittiinko ongelman ratkaisemiseksi ulkopuolista apua. Mahdollisuuksien mukaan kannattaa pyytää ulkopuoliselta ratkaisijalta pienimuotoinen selvitys mitä tehtiin. Selvitys kannattaa liittää raportin yhteyteen.

3.6 Varmuuskopiointi

Varmuuskopioinnilla tarkoitetaan tietokoneen tiedostojen kopiointia varsinaisesta tallennusmediasta erilliseen tallennusmediaan, josta ne ovat tarpeen tullen palautettavissa (Nielsen, S. 2019.). Varmuuskopioinnissa suositellaan käytettäväksi 3-2-1 sääntöä, joka tarkoittaa 3 kopiota omasta datasta, joista 2 on paikallisia varmuuskopioita ja 1 on ulkoinen pilvessä oleva varmuuskopio (Klosowski, T. 2019).

Varmuuskopioinnin suorittamiseen on olemassa automaattisia työkaluja, jotka hoitavat varmuuskopioinnin taustalla ilman käyttäjän toimia. Automaattisten ohjelmien käyttö poistaa mahdollisuuden varmuuskopioinnin unohtamiselle, sillä yksinkertaisesti varmuuskopioinnin voi suorittaa kopioimalla itse tiedostot toiseen ulkoiseen tiedostosijaintiin (Klosowski, T.2019; Nielsen, S. 2019).

Tekemällä varmuuskopiot omille ulkoisille laitteille kuten esimerkiksi riittävän suurelle muistitikulle, varmuuskopioita pystytään käyttämään ilman verkkoyhteyttä. Tällä tavoin myös varmuuskopioinnin kustannukset ovat alhaiset (Rasmussen, H. 2020).

Windows 10- käyttöjärjestelmään on rakennettu oma varmuuskopiointiominaisuus, jolla pystyy luomaan varmuuskopion ja ohjelma toimii automaattisesti taustalla ja päivittää varmuuskopiota, kun tiedostoissa tapahtuu muutoksia. Ohjelmisto pystyy myös palauttamaan tekemänsä varmuuskopion (Microsoft tuki www-sivut 2021.).

Varmuuskopioinnit tulee suorittaa säännöllisesti omaan sopivaan sijaintiin. Varmuuskopiot voidaan tehdä esimerkiksi pilveen, tai mahdollisesti voidaan hankkia oma verkkokiintolevy niitä varten. Pääasia on kuitenkin tehdä varmuuskopioita ja välillä harjoitella tietojen palauttamista, jolloin ei tositilanteessa tule yllätyksiä. Harjoitusten avulla pystytään helposti todentamaan oman varmuuskopioinnin toimivuus ja palautettavuus. Varmuuskopioiden hallitsemista helpottaa, jos kaikilla yrityksen tietokoneilla pidetään samat tiedostosijainnit ja kansiorakenteet, sekä huolehditaan tiedostojen oikeanlaisesta tallentamisesta. Tiedostot voivat olla omassa sovitussa kansiossaan ja kansioista voidaan luoda pikakuvake käyttäjän työpöydälle käyttöä helpottamaan. Näin käyttäjä löytää oikeat sijainnit nopeasti.

Varmuuskopiointi on hyvä suorittaa myös yrityksen puhelimille, jotta asiakkaiden kontakti- ja viestitiedot pysyisivät tallessa. Puhelimien varmuuskopiot tallentuvat yleensä Android-puhelimissa Googlen tarjoamaan Google Drive-palveluun. Applen laitteilla varmuuskopiot tallennetaan iCloudiin tai iTunesiin kytkemällä puhelin tietokoneeseen. Puhelimien varmuuskopioita tehdessä kannattaa rajata, mitä haluaa varmuuskopioida. Suositukseni on puhelimien osalta tallentaa yhteystiedot, sovelluskirjasto ja laitteen asetukset. Näin uuden puhelimen käyttöönotto sujuu nopeasti ja helposti.

3.6.1 Varmistuspolitiikka

Varmistuspolitiikalla tarkoitetaan koko varmuuskopioinnin prosessia tiedostojen kopioinnista niiden palauttamiseen. Varmistuspolitiikalla määritellään varmistettavat tiedostot ja niiden varmistustiheys. Varmistuspolitiikassa määritellään myös mihin varmuuskopiot tallennetaan ja miten ne eri sijainneista saadaan palautettua. Varmistuspolitiikka määrittelee ja ottaa huomioon myös tilanteet, joissa mahdollisesti menetetään yrityksen omat laitteet ja toimitilat ja miten tällaisissa tilanteissa varmuuskopioiden palauttaminen tapahtuu (Keskuskauppakamari 2016).

Varmuuskopioinnit voidaan suorittaa usealla eri tavalla. Täysi varmuuskopio tarkoittaa yrityksen kaiken datan kopioimista. Osittainen varmuuskopio tarkoittaa vain muuttuneiden tiedostojen kopiointia. Varmuuskopioinneissa kannattaa ottaa käyttöön molempien kopiointitapojen hyvät puolet. Täyden varmuuskopion luomiseen menee kauan aikaa, joten täysi kopiointi kannattaa suorittaa esimerkiksi viikonloppuisin. Osittainen kopiointi on nopea ja ei vie paljon levytilaa. Näitä voi suorittaa muuttuneiden tiedostojen kohdalla esimerkiksi öisin. Näiden tapojen yhdistelmällä saadaan tehokas ja nopea varmuuskopiointi ja minimoidaan menetetyt tiedostot (Collins, T, 2020).

Viikoittaisia täysiä varmuuskopioita otettaessa tulisi miettiä monenko viikon varmuuskopiot säästetään. Lyhyt säästöaika säästää levytilaa mutta ei mahdollista vanhojen tiedostojen palauttamista. Vaatimuksia erilaisten tiedostojen ja dokumenttien säilyttämisestä tulee lainsäädännöstä. Esimerkkeinä kirjanpitoon liittyvät dokumentit ja materiaali tulee säilyttää vähintään kuusi vuotta ja asianajotoimintaan liittyvät toimeksiantoa koskeva materiaali tulee säilyttää vähintään 10 vuotta. Nämä erityisehtoja sisältävät dokumentit tulisi säilyttää omaan sijaintiinsa, jotta niitä ei tule poistettua esimerkiksi päälle kirjoitettaessa (Kauppi, J, 2019; Asianajajaliiton www-sivut).

3.7 Päivitykset

Käyttöjärjestelmän päivittäminen on osa laitteiden ylläpitoa ja tietoturvaa. Käyttöjärjestelmän päivitysten mukana toimitetaan päivityksiä ja korjauksia toimivuuteen ja

suojaukseen. Windows 10-käyttöjärjestelmässä päivitysten toimittaminen voidaan hoitaa automaattisesti. Käyttäjälle jää vain tietokoneen uudelleen käynnistäminen sopivana ajankohtana, mutta uudelleen käynnistyminenkin voidaan esimerkiksi ajastaa käyttämällä Windowsin aktiivinen aika ominaisuutta. Määrittelemällä aktiivisen ajan käyttöjärjestelmä pyrkii välttämään uudelleen käynnistymistä kyseisenä ajankohtana. Windows 10-päivitykset tulevat joko ominaisuuspäivityksinä tai laatupäivityksinä. Ominaisuuspäivitykset Microsoft julkaisee yleisesti kaksi kertaa vuodessa. Ominaisuuspäivitykset sisältävät päivityksiä käyttöjärjestelmän ominaisuuksiin ja toimintoihin. Ominaisuuspäivitysten mukana toimitetaan myös tarvittaessa suojauspäivityksiä. Laatupäivityksiä julkaistaan useammin korjaamaan käyttöjärjestelmän virheitä ja suojausta (Microsoft tuki www-sivut).

Ohjelmien säännöllisellä päivittämisellä varmistetaan niiden pysyminen ajan tasalla. Etenkin selainten päivittäminen on tärkeää, koska monia eri ohjelmia voidaan ohjata selaimen välityksellä. Selainten päivittäminen tapahtuu niihin rakennetusta asetusvalikosta. Kaikkien selainten päivitykset on hyvä tarkistaa säännöllisesti. Tällä varmistetaan kaikkien selainten toimivuus.

Älypuhelimien päivitykset on tarkistettava säännöllisesti. Laitevalmistajat tarjoavat päivityksiä käyttöjärjestelmiin ja tietoturvaan. Älypuhelimen asetuksista valitaan käyttöjärjestelmän päivitysten automaattinen lataaminen ja asentaminen. Sovellusten päivittäminen kannattaa automatisoida. Päivitykset löytyvät sovelluskaupasta. Älypuhelinta valittaessa tulee kiinnittää huomiota laitevalmistajan tarjoamaan käyttöjärjestelmän ja tietoturvan päivitysten tuen pituuteen. Tuen päättyessä älypuhelimet pitää vaihtaa uusiin. Näin varmistetaan laitteiden pysyminen turvallisina.

4 TIEDON TALLENNUS JA JAKO

Yritykselle tulee väistämättä tarve jakaa tiedostoja työntekijöiden kesken. Perinteisesti tämä on hoidettu muistitikuilla, mutta on olemassa paljon nopeampia ja helpompia tapoja jakaa tiedostoja ja dokumentteja työntekijöiden kesken.

Windows 10-käyttöjärjestelmässä on tiedostojen ja kansioiden jakamiselle rakennettu ominaisuus. Tiedostojen jakamisen voi tehdä lähijakona, joka toimii joko wifi- tai bluetooth-tekniikalla. Jollekin yrityksen käytössä olevalle tietokoneelle voidaan luoda kansio jaettaville tiedostoille, joka jaetaan kaikkien käyttäjien kesken. Jaettava kansio voidaan yhdistää omaksi verkkoasemakseen, joka näkyy tietokoneen kiintolevyjen puurakenteessa omana verkkolevynään. Tiedostojen käsittely on nopeaa ja helppoa. Jaettu kansio vaatii isäntäkoneen pitämisen käynnissä ja samassa verkossa niiden koneiden kanssa, joille tiedostoja halutaan jakaa (Microsoft tuki www-sivut). Tämä ei ole paras eikä turvallisin tapa luoda tiedostojako, mutta kyseinen jakokansio voidaan myös salata ja pääsyyn vaaditaan isäntäkoneen käyttäjätunnus ja salasana.

4.1 NAS

Varmempi tapa luoda verkkojako on hankkia NAS-asema, eli network attached storage, eli ulkoinen verkkokiintolevy. Ulkoinen verkkokiintolevy liitetään yrityksen omaan lähiverkkoon, josta se on kaikkien laitteiden tavoitettavissa. Ulkoisen verkkokiintolevyn tavoittaminen on myös mahdollista etänä käytettäessä VPN-yhteyttä. Verkkokiintolevy on oma laitteensa, joka mahdollistaa tiedostojen tavoittamisen kellon ympäri. Verkkokiintolevyä käytetään yleensä laitevalmistajan sovelluksella. Myös selainpohjaista ohjelmistoa on mahdollista käyttää. Verkkokiintolevy on laajennettavissa isommilla kovalevyillä tarpeen vaatiessa.

Verkkokiintolevyt käyttävät RAID-kokoonpanoja tiedostojen tallentamiseen. RAID eli Redundant Array of Independent Disks on tietojen tallennuksessa käytettävä virtualisointitekniikka, jolla yhdistetään useita levyjä yhdeksi yksiköksi. RAID- kokoonpanoilla voidaan tavoitella suorituskyvyn parantamista tai luotettavuutta ja vikasietoisuutta (Dell tuki www-sivut 2021).

Isommissa ja edistyneemmissä laitteissa on mahdollista käyttää myös kehittyneempiä RAID kokoonpanoja. Yleisimmin käytössä ovat RAID 1 ja RAID 5. RAID 1 eli peilaus vaatii kaksi kiintolevyä, joista molemmilla on identtiset tiedot. Yhden levyn

vikaantuminen ei vaikuta toimintaan. RAID 5 kokoonpano vaatii useamman kiintolevyn. RAID 5 kirjoittaa hajautetusti kaikille levyille erillisen pariteettidatan kanssa. Yhden levyn vikaantumisella ei ole vaikutusta toimintaan sillä tiedostot ovat palautettavissa täydellisesti muilta levyiltä. Tallennustila on RAID 5 tilassa kaikkien levyjen yhteiskapasiteetti vähennettynä yhden levyn kapasiteetilla (Vähimaa, A. 2020).

Verkkokiintolevyt voidaan myös lisätä tietokoneen kiintolevyjen puurakenteeseen tai luoda oma pikakuvake työpöydälle käyttämällä verkkokiintolevyn yhdistäminen ominaisuutta. Konfiguroinnissa kysytään käyttäjän haluama verkkolevyn tunnuskirjain ja verkkokiintolevyn osoite (Microsoft tuki www-sivut 2021).

Verkkokiintolevy on hyvä ja kohtuu edullinen vaihtoehto lisätallennustilalle, johon kaikki työntekijät pääsevät käsiksi. Verkkokiintolevyjärjestelmää kannattaa harkita pilvipalvelun sijasta, jos tarvittavan tallennustilan määrä kasvaa suureksi tai tallennettavia tiedostoja ei haluta tallentaa oman ympäristön ulkopuolelle. Verkkokiintolevyjärjestelmä vaatii ylläpitoa siinä missä muutkin yrityksen laitteet. Verkkokiintolevyjärjestelmässä tulee jossakin vaiheessa vastaan kiintolevyjen uusiminen ja itse laitteen vaihtaminen. Kevyessä käytössä hyvä verkkokiintolevylaite voi kestää kauan ja ainoana huoltona on säännöllinen päivittäminen, pölyjen puhaltaminen ja kovalevyjen vaihtaminen niiden rikkoutuessa.

4.2 Pilvitallennus

Pilvitallennuksella tarkoitetaan tiedostojen tallentamista palveluntarjoajan konesaliin. Pilvitallentamista voidaan pitää turvallisena ja varmana tapana hoitaa yrityksen datan tallentamisen ja varmistamisen tarpeet. Esimerkiksi Microsoft tarjoaa yrityksille paketteja OneDrive-palvelun käyttöön. Microsoft tarjoaa maksullisissa palveluissa 1Tb tallennustilaa käyttäjää kohden, jota on mahdollista laajentaa tarvittaessa. Pilvestä löytyvät tiedostot ovat aina saatavilla ja mahdollista käyttää myös mobiililaitteilla. OneDrive-palvelussa on mahdollista luoda jaettavia kansioita, joihin yrityksen muut työntekijät pääsevät käsiksi (Microsoft www-sivut).

Pienyrityksen on kannattavaa ottaa käyttöön jokin pilvipalvelu silloin kun ympäristö on pieni ja käyttäjiä on vähän. Pilvipalvelun käytöllä vähennetään omien hallittavien laitteiden määrää ja ongelmia ei juurikaan tule. Pilvipalvelu on myös kokemattomille käyttäjille helpompi omaksua ja hallita kun ei tarvitse huolehtia laitepuolesta. Mahdollisuuksien ja omien käyttötottumusten mukaan kannattaa valita omaan käyttöön sopiva palvelu. Usein esimerkiksi Microsoftin tarjoamat yrityspaketit sisältävät OneDrive-palvelun. Keskittämällä nämäkin hankinnat yrityksen on helpompi hallita omia kulujaan ja käytössä olevia palveluita.

5 YHTEENVETO

Opinnäytetyön toimeksiannon sain elokuussa 2020. Tilaajana toimi Lakiasiaintoimisto Lindholm & Gustafsson. Aloittaneella lakiasiaintoimistolla oli tarve tietokoneiden ja muiden tarvikkeiden hankinnalle. Yrityksen laitteet hankittiin leasingperiaatteella kustannusten ja helppouden takia. Jatkossa yritys itse määrittelee, miten se laitteensa hankkii. Laitteiksi yritykselle valittiin Dellin yrityskäyttöön tarkoitetut koneet. Koneiden valinnassa kiinnitettiin huomiota niiden komponentteihin ja muihin ominaisuuksiin, jotta koneet kestäisivät moitteitta koko niiden käyttöiän ja palvelisivat parhaalla mahdollisella tavalla aloittavaa yritystä. Kannettavien tietokoneiden lisäksi hankittiin niihin sopivat USB-C-telakat, joihin on kytkettynä langattomat näppäimistöt, hiiret ja erillinen 27-tuumainen näyttö. Telakat hankittiin, koska töitä tehdään myös toimiston ulkopuolella ja liittimien jatkuva irrottelu on aikaa vievää ja saattaa aiheuttaa turhaa kulumista koneen liitännöille. Erillisen näytön, näppäimistön ja hiiren hankintaa perusteltiin mukavuus- ja ergonomisista syistä. Puhelimiksi yritys valitsi Samsung Galaxy A20e älypuhelimet. Yritykselle valittiin vain kevyeen käyttöön tarkoitetut puhelimet, sillä niitä käytetään vain puheluiden soittamiseen. Yrityksellä oli jo leasingsopimuksella hankittu monitoimilaite tulostusta varten. Laite toimii verkkotulostimena, mikä helpottaa tulostamista.

Yritykselle valittiin yritystason internetliittymä ja palomuuripalvelu. Palomuurin mukana toimitettiin kymmenelle käyttäjälle soveltuva VPN-palvelu.

Työssä esittelin myös tietokoneiden vaihtoon liittyvät toimenpiteet, ja mitä tulee ottaa huomioon laitevaihtoja valmisteltaessa ja tehdessä. Huomioon otettavat asiat liittyivät uusien laitteiden yhteensopivuuteen vanhojen laitteiden kanssa ja vanhojen laitteiden tietojen siirtämiseen. Laitevaihdoista käsiteltiin myös mitä laitteita kannattaa lunastaa omaksi ja mitkä laitteet kannattaa jatkossakin hankkia leasingsopimuksella.

Erilaisia tiedostojen jakamis- ja tallennustekniikoita käsiteltiin myös kattavasti ja monipuolisesti. Työssä esiteltiin ja vertailtiin eri tapojen eroja ja turvallisuutta, joista päädyttiin ottamaan käyttöön aluksi Microsoftin OneDrive-palvelu. OneDrive-palvelun helppous ja aiemmat käyttökokemukset tukivat tätä päätöstä.

Koneiden ja laitteiden sujuvaa käyttöä ajatellen työssä käsiteltiin myös päivitysten tärkeys ja miten päivitykset tulisi asentaa. Yrityksellä on käytössään pääasiassa selaimella käytettäviä sovelluksia ja ohjelmia, joten oli tärkeää käsitellä myös selainten päivittämiseen liittyvät toimenpiteet ja selainten kirjainmerkkien ja kansioiden tallentaminen. Useamman selaimen pitämistä käyttökuntoisena suositeltiin, jotta mahdollisista ongelmista palauduttaisiin nopeasti.

Yrityksen on tärkeää pitää omat varmuuskopiot ajan tasalla ja opetella palauttamaan varmuuskopiot. Työssä esiteltiin varmistuspolitiikka, jonka pohjalta voi yritys luoda itselleen sopivan tavan luoda omat varmuuskopiot. Varmuuskopioiden tekemisessä otetaan myös huomioon puhelimien varmuuskopioinnit, jotka helposti pääsevät unohtumaan.

Edelliset kohdat toteuttavat tietoturvaa, mutta oli myös tärkeää käsitellä tietoturvaa lisää tarkemmin ja monipuolisemmin. Esittelin huomioita salasanojen käyttöön ja muistiin kirjoittamiseen liittyen. Näillä huomioilla pyritään muistuttamaan miten salasanoja tulisi säilyttää turvallisesti. Esittelin myös huomioita omiin vapaa-ajalla käytettäviin salasanoihin, joiden tulisi olla selkeästi erilaisia kuin työssä käytettävät salasanat. Tietoturvaosiossa käsitelin tietokoneiden ja oman verkon suojauksen lisäksi myös puhelimien suojaukseen liittyviä asioita.

Opinnäytetyön avulla pystyin tutustumaan yrityksen laitehankintoihin. Opas osuudessa pyrittiin tuomaan esiin tärkeitä ja helposti unohtuvia huomioita erilaisiin asioihin. Opinnäytetyön tekeminen oli mielenkiintoista ja toi minulle uutta tietoa, jota voin hyödyntää tulevaisuudessa.

LÄHTEET

Asianajotoimintaa koskevia säädöksiä ja ohjeita. B10 Asiakirjojen säilyttämistä koskeva ohje 2019. Viitattu 10.2.2021 https://asianajajaliitto.fi/asianajajaksi/suorita-asianajajatutkinto/asianajotoimintaa-koskevia-saadoksia-ja-ohjeita/

Collins, T. 2020. Full backup vs. Incremental backup vs. differential backup: Which is best? Viitattu 10.2.2021 https://www.atlantech.net/blog/full-backup-vs.-incremental-backup-vs.-differential-backup-which-is-best

Dell tuki www-sivut 2021. Viitattu 15.4.2021 https://www.dell.com/support/home/fi-fi

Dines, R. 2012. CIO, varmista firman toipuminen it-kriisistä. Viitattu 20.11.2020 https://www-tivi-fi.lillukka.samk.fi/uutiset/cio-varmista-firman-toipuminen-it-kriisista/983b9e5a-8116-3f12-8202-1567535748f8

F-secure www-sivut 2021. Viitattu 9.2.2021. https://www.f-secure.com/fi

Gilchrist, A. 2017. IoT Security Issues. Boston: Walter de Gruyter Inc.

Henmi, A., Lucas, M., Singh, A. & Cantrell, C. 2006. Firewall policies and vpn configurations. Syngress publishing inc.

Hernandez, L. 2020. Kaksivaiheinen tunnistautuminen suojaa käyttäjätilejäsi. Viitattu 2.2.2021 https://blog.f-secure.com/fi/kaksivaiheinen-tunnistautuminen/

Itaito www-sivut 2021. Viitattu 2.2.2021. https://www.itaito.fi/

Järvinen, P. & Rousku, K. 2017. Työpaikan tietoturvaopas Helsinki: Alma Talent.

Järvinen, P. 2012. Arjen tietoturva. Saarjärven Offset Oy

Kauppi, J. 2019. Backupit kuntoon – hoida varmuuskopiointi kunnialla. Viitattu 10.2.2021 https://www.leijonasecurity.fi/2019/10/17/varmuuskopiointi/

Keskuskauppakamari 2016. Tietoturvaopas yrityksille 2016. Viitattu 4.2.2021 https://kauppakamari.fi/wp-content/uploads/2020/06/tietoturvaopas-yrityksille.pdf

Kilpailu- ja kuluttajaviraston www-sivut 2021. Viitattu 2.2.2021. https://www.kkv.fi/

Klosowski, T. 2019. How to back up your computer. Viitattu 22.1.2021 https://www.nytimes.com/wirecutter/guides/how-to-back-up-your-comp

Kurki, M. 2010. Pk-yrityksen tietotekniikka käytännönläheisesti. Jyväskylä: WS Bookwell oy.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja Helsinki: Oy Nordprint Ab

Lammle, T. 2005. CCNA: Cisco certified network associate study guide. Alameda: Sybex Inc.

Microsoft tuki www-sivut 2021. Viitattu 21.1.2021. https://support.microsoft.com/

Microsoft www-sivut 2021. Viitattu 2.3.2021. https://www.microsoft.com/fi-fi/

Nielsen, S. 2019. Kuinka usein pitää varmuuskopioida? Viitattu 21.1.2021 https://kotimikro.fi/ohjelmat/varmistus/kuinka-usein-pitaa-varmuuskopioida

Nieminen, J. 2017. Digitreenit: Kaksivaiheinen tunnistautuminen. Viitattu 2.2.2021 https://yle.fi/aihe/artikkeli/2017/11/30/digitreenit-kaksivaiheinen-tunnistautuminen-eiko-yksi-kerta-riita

Pratt, M. 2014. A computer maintenance checklist for your company´s computers Viitattu 18.11.2020 https://www.business.org/it/hardware/computer-maintenance-checklist-companys-computers/

Rasmussen, H. 2020. Minne varmuuskopiot pitäisi tallentaa? Viitattu 22.1.2021 https://kotimikro.fi/tietoturva/minne-varmuuskopiot-pitaisi-tallentaa

Rissanen, T. 2002. Projektilla tulokseen. Jyväskylä: Gummerrus.

Rousku, K. 2014. Kyberturvaopas. Talentum Media Oy

Ruuska, K. 2007. Pidä projekti hallinnassa. 6. painos. Helsinki: Talentum Media Oy.

Suomen Standardisoimisliiton www-sivut. Viitattu 15.4.2021. https://sfs.fi/

Tepora, J. 2013. Rahoitusmuodot ja vakuudet. Vantaa: Hansaprint Oy

Tietosuojavaltuutetun toimiston www-sivut 2020. Viitattu 6.11.2020 https://tietosuoja.fi/etusiv .

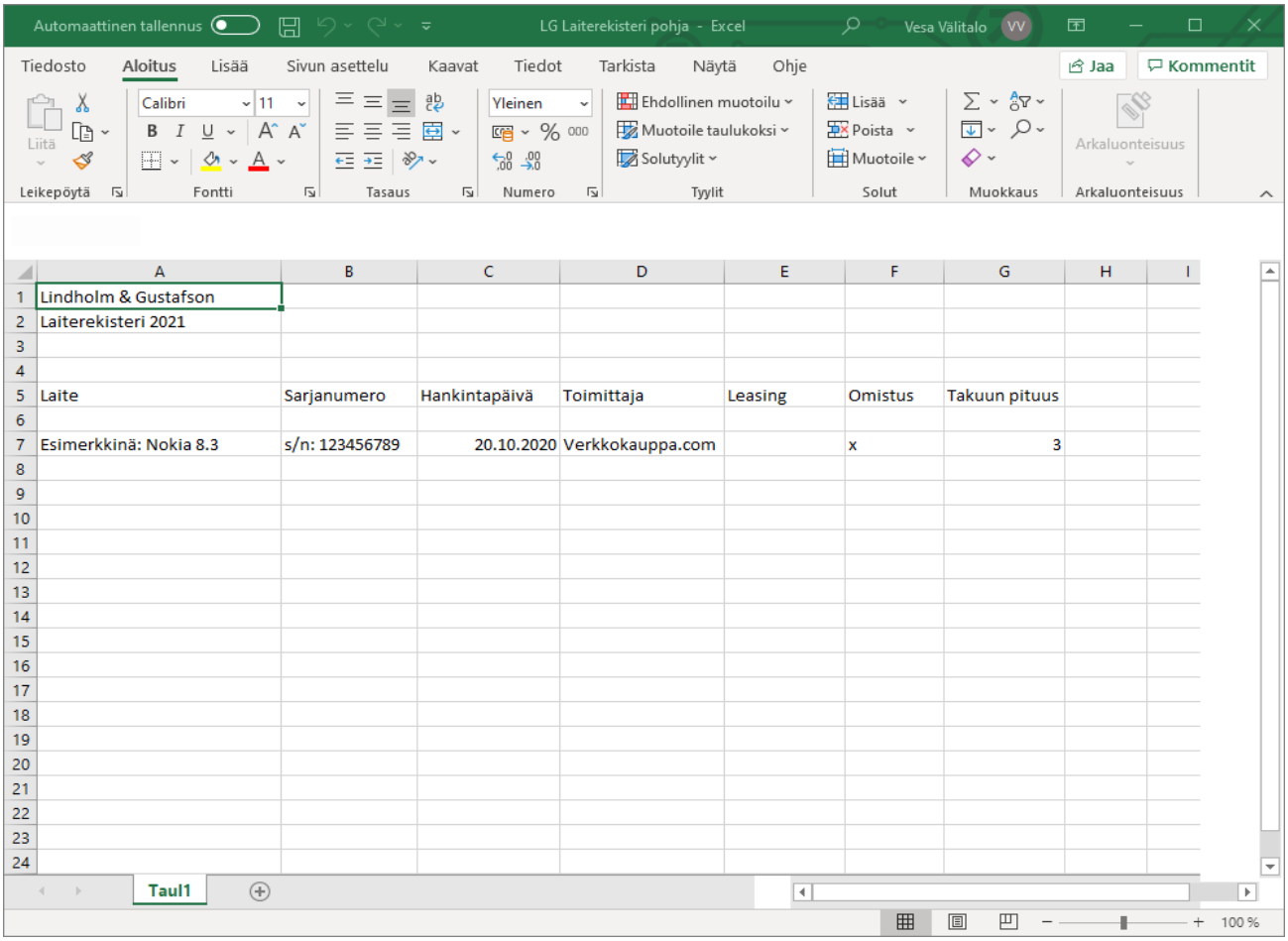
Vähimaa, A. 2020. Testissä edulliset verkkokiintolevyt: 4 tapaa varmuuskopioida ja tallentaa tiedot turvallisesti verkkoon. Viitattu 18.2.2021. https://www-mikrobitti-fi.lillukka.samk.fi/testit/testissa-edulliset-verkkokiintolevyt-4-tapaa-varmuuskopioida-ja-tallentaa-tiedot-turvallisesti-verkkoon/7084fc28-a985-4996-84f0-a7f8bf883534

Vähimaa, A. 2017. Tietokoneen data turvaan helposti – 3 tapaa varmuuskopioida tiedot pilveen. Viitattu 20.1.2021. https://www.mikrobitti.fi/testit/tietokoneen-data-turvaan-helposti-3-tapaa-varmuuskopioida-tiedot-pilveen/e8648bc9-b745-3db9-9922-7dc773f5b4a0

Vähimaa, A. 2019. Romauta tietomurron todennäköisyys. Tässä 7 tapaa kaksivaiheiseen tunnistautumiseen. Viitattu 2.2.2021. https://www-mikrobitti-fi.lillukka.samk.fi/neuvot/romauta-tietomurron-todennakoisyys-tassa-7-tapaa-kaksivaiheiseen-tunnistautumiseen/80bbaaa9-c299-42e7-a7aa-f266888f6f9a

Ylä-Jääski, V. 2012. TM-vertailu: Ups-laitteet. Viitattu 15.4.2021 https://tekniikan-maailma.fi/tm-vertailu-ups-laitteet/

LIITE 1



	A	B	C	D	E	F	G	H	I
1	Lindholm & Gustafson								
2	Laiterekisteri 2021								
3									
4									
5	Laite	Sarjanumero	Hankintapäivä	Toimittaja	Leasing	Omistus	Takuun pituus		
6									
7	Esimerkkinä: Nokia 8.3	s/n: 123456789	20.10.2020	Verkkokauppa.com		x	3		
8									
9									
10									
11									
12									
13									
14									
15									
16									
17									
18									
19									
20									
21									
22									
23									
24									

LIITE 2

Lindholm & Gustafsson

Vikatilanne raportti

Päivämäärä:

Tekijä:

Vikatilanne:

Vikatilanteen tarkempi kuvaus:

Ratkaisu: