Microsoft Intunen käyttöönotto — Case Swan IT

Olli Onnela

2020 Laurea

Laurea-ammattikorkeakoulu

Microsoft Intunen käyttöönotto – Case Swan IT

Olli Onnela
Tietojenkäsittelyn koulutusohjelma
Opinnäytetyö
Joulukuu, 2020

Laurea-ammattikorkeakoulu **Tiivistelmä**

Tietojenkäsittely

Tietojenkäsittely (AMK)

Olli Onnela

Microsoft Intunen käyttöönotto – Case Swan IT

Vuosi 2020 Sivumäärä 29

Tämän opinnäytetyön tavoitteena oli tutkia ja testata Swan IT:lle käyttöönotettavaa uutta laitehallintaohjelmistoa, Microsoft Intunea. Projektissa keskitytään Windows 10 -käyttöjärjestelmällisiin tietokoneisiin. Tavoitteisiin liittyi ottaa selvää laitteenhallintajärjestelmän mahdollisuuksista ja miten ne voidaan toteuttaa. Työ tehtiin toimeksiantona suomalaiselle IT-konsultointiyritykselle, Swan IT:lle.

Työssä käydään läpi projektiin liittyvät tavoitteet, teoriaa projektiin liittyen ja Intuneen tehdyt toimenpiteet sekä lopuksi pohdintaa aiheesta. Tavoitteisiin päästiin perehtymällä käyttöönotettavan laitehallintaohjelman sekä NIST-kyberturvallisuuskehyksen sähköisiin materiaaleihin. Projektissa onnistuttiin luomaan Intune-ympäristö, jonka pohjalta voidaan kehittää Intunea toimeksiantoyrityksen käyttöön. Intuneen määriteltiin erilaisia ryhmiä, sovelluksia, asetuksia ja tietoturva-asetuksia.

Tulosten merkitystä arvioitaessa pohditaan, miten saadut tulokset vastasivat asetettuja tavoitteita ja mitä projektissa tehtiin sekä miten projektia tehtiin. Projektin haasteena oli tarkan päämäärän puuttuminen määrittelyn osalta, jossa laitehallintaohjelman tarpeet olisi kuvattu tarkalla tasolla. Pohdinnassa myös tutkitaan miten tulokset vastaavat NIST-kyberturvallisuuskehystä.

Asiasanat: Microsoft, Intune, laitehallinta, MDM

Laurea University of Applied Sciences **Abstract**

Degree Programme in Business Information Technology

Bachelor's Thesis

Olli Onnela

Deployment of Microsoft Intune – A Case Study of Swan IT

Year 2020 Pages 29

The purpose of this thesis was to research and test Swan IT's new device management tool, Microsoft Intune. The project will focus on computers running Windows 10 operating system. The objectives were to find out about the possibilities of the device management tool and how they can be achieved. This project was commissioned by a Finnish IT consulting company, Swan IT.

The work reviews the objectives related to the project, the theory related to the project, the procedures made to Intune and finally the reflection on the topic. The goals were achieved by getting acquainted with device management tool's and NIST cybersecurity framework's electric materials. The project succeeded in creating an Intune environment on the basis of which Intune can be developed for the use of the company.
Different groups, applications, settings, and security settings were defined for Intune.

When assessing the significance of the results, it is considered how the results obtained corresponded to the set objectives and what was done in the project, as well as how the project was done. The challenge of the project was the lack of a precise goal in terms of definition, where the needs of the device management tool would be described at a precise level. The reflection also examines how the results fit into the NIST cybersecurity framework.

Keywords: Microsoft, Intune, device management, MDM

Sisällys

1 Johdanto

Tämän projektin tavoitteena oli saada Microsoft Intune -laitehallintaohjelma käyttövalmiiksi suomalaiselle IT-konsultointiyritykselle Swan IT:lle siten, että tulevaisuudessa loppukäyttäjälle tulevat tietokoneet olisivat hallinnoitavissa Intunen kautta. Projektissa on rajoituttu tutkimaan Windows-tietokoneiden hallintaa. Intune on myös tavoitteena yhdistää Azure AD:seen ja tätä kautta yrityksen paikalliseen omaan AD:seen. Intunen pariin tulisi saada sekä yrityksen omat että tulevien uusien asiakkaiden tietokoneet. Intunen avulla laitteisiin pitäisi voida myös upottaa kaikki tarvittavat ohjelmat, turvallisuusasetukset ja muut tarvittavat asetukset automaattisesti. Tavoitteena on ollut, että loppukäyttäjän ei tarvitsisi nähdä vaivaa, jos hän haluaa tietyn asian koneelleen. Käyttöönoton tulisi olla niin pitkälle automatisoitua kuin vain mahdollista. Optimitavoitteena projektin automaatiossa on ollut, että tietokoneen ei tarvitsisi käydä yrityksen IT-osaston kautta, vaan laite tulee voida suoraan lähettää loppukäyttäjälle.

Tavoitteeseen liittyy myös laitteiden käyttöönoton lisäksi tarve kehittää loppukäyttäjän tukipalvelua. Tämä saadaan tehdyksi tietokoneissa ja yritysportaalin kautta. yritysportaalin kautta loppukäyttäjä näkee tarvittavat tiedot IT-tuesta, että voi itse ladata tarvittaessa yrityksen omia sovelluksia.

Projektin tavoitteena oli myös integroida laitteiden etäyhteys -työkalu TeamViewer Intunen piiriin. TeamViewerillä on tarkoitus pystyä ottamaan erilaisia etäyhteyksiä Intunessa oleviin koneisiin riippuen laitteen tarkoituksesta. Tietokoneissa tulee olla kahdenlaisia tapoja ottaa etäyhteys. Ensimmäisen tavan pitäisi olla sellainen, jossa loppukäyttäjän täytyy itse hyväksyä etäyhteys. Toisen tavan kuuluisi olla sellainen, että tietokoneeseen voidaan ottaa suoraan etäyhteys, ilman että kukaan olisi koneen toisessa päässä hyväksymässä pyyntöä.

Tämän kaiken täytyisi olla mahdollisimman tietoturvallista, ja tähän onkin pyritty vertaamalla tuloksia NIST:n, eli National Institute of Standards and Technology:n, kyberturvallisuuden viitekehystä.

1.1 Työn lähtökohdat

Tämän opinnäytetyön aihe tulee toimeksiantajayrityksen, Swan IT:n, käytännöntarpeesta. Swan IT toimii IT-konsultointiyrityksenä, ja hoitaa paljon asiakkaidensa IT-infrastruktuuri ja -ylläpitoratkaisuja (SwanIT 2020.) Nykyaikana lisääntyvien pilvipalvelujen kasvu on tuonut uusia tarpeita tälle liikealalle, mutta Swan IT:llä ei ollut vielä omaa ratkaisua asiakkailleen tähän ongelmaan. Osoitin Swan IT:n palvelupäällikölle kiinnostusta osallistua uuden laitahallintajärjestelmän Intunen käyttöönottoon opinnäytetyön muodossa.

Laitehallintajärjestelmä oli tarkoitus ottaa lokakuu – marraskuu 2020 välisenä aikana käyttöön, joten projekti oli todella nopea.

1.2 Keskeiset käsitteet

Pilvipalvelu = Tietoteknisten palveluiden toimittamista internetin välityksellä.

Tenantti = Microsoftin käyttämä termi, joka kuvaa organisaation ympäristöä.

Agentti = Ohjelmisto, joka toimii tietyssä ympäristössä ja pystyy toimimaan itsenäisesti suunnittelutavoitteiden saavuttamiseksi.

Pilvi = Palveluiden verkosto.

Kyberturvallisuuskehys = Tarkoittaa kattavaa joukkoa ohjeita siitä, miten organisaatiot voivat estää, havaita ja reagoida erilaisiin kyberhyökkäyksiin.

MSP = Tulee sanoista Managed Service Provider, joka tarkoittaa palveluntarjoajaa.

AAD = Azure AD on Microsoftin pilvipohjainen hakemisto- ja identiteetinhallintapalvelu.

Bugi = Tarkoittaa tietokoneohjelman lähdekoodissa olevaa virhettä.

MDM = Tulee sanoista Mobile Device Management ja se tarkoittaa hallintatyökalua, jolla IT-osastot pystyvät etähallitsemaan työntekijöiden matkapuhelimia, tabletteja ja kannettavia tietokoneita.

OOBE = Out of Box Experience. Tarkoitetaan kokemusta, kun käyttäjä ottaa ensimmäisen kerran laitteen käyttöönsä.

2 NIST-kyberturvallisuuskehys

NIST tulee sanoista National Institute of Standards and Technology ja sillä tarkoitetaan yhdysvaltalaista kauppaministeriön alaista virastoa, jonka tarkoituksena on kehittää ja edistää erilaisia mittaustekniikoita, tekniikoita ja standardeja liittyen kyberturvallisuuteen (Horan 2019.)

NIST-kyberturvallisuuskehys tarkoittaa kattavaa joukkoa ohjeita siitä, miten organisaatiot voivat estää, havaita ja reagoida erilaisiin kyberhyökkäyksiin. NIST-kyberturvallisuuskehyksen ei ole tarkoitus toimia absoluuttisena valmiina mallina yrityksille, vaan sen tarkoitus on auttaa organisaatioita kehittämään omaa lähestymistapaansa kyberturvallisuuteensa. Seuraamalla tätä kehystä yritykset pystyvät huomioimaan omat vaatimukset, riskit,

haavoittuvuudet, uhat ja sietokyvyt mahdollisimman tehokkaasti. (SolarWinds 2019). Tässä opinnäytetyössä onkin tarkoitus verrata, miten projektin aikana on päästy näihin tavoitteisiin.

NIST-kyberturvallisuuskehys luokittelee turvallisuusperiaatteet viiteen eri toimintoon, jotka tunnetaan nimellä ”Framework Core Functions”, eli viitekehyksen ydintoiminnot. Näistä viidestä osasta rakentuu yleiskatsaus organisaation kyberturvallisuusriskien hallintaohjelmasta, jossa eri osat edustavat keskeistä kronologista vaihetta organisaation turvallisuuden parantamisessa. Nämä viisi toimintoa jakaantuvat vielä 23:een alakategoriaan. (SolarWinds 2019.)

Function	Category	ID
Identify	Asset Management	ID.AM
	Business Environment	ID.BE
	Governance	ID.GV
	Risk Assessment	ID.RA
	Risk Management Strategy	ID.RM
	Supply Chain Risk Management	ID.SC
Protect	Identity Management and Access Control	PR.AC
	Awareness and Training	PR.AT
	Data Security	PR.DS
	Information Protection Processes & Procedures	PR.IP
	Maintenance	PR.MA
	Protective Technology	PR.PT
Detect	Anomalies and Events	DE.AE
	Security Continuous Monitoring	DE.CM
	Detection Processes	DE.DP
Respond	Response Planning	RS.RP
	Communications	RS.CO
	Analysis	RS.AN
	Mitigation	RS.MI
	Improvements	RS.IM
Recover	Recovery Planning	RC.RP
	Improvements	RC.IM
	Communications	RC.CO

Kuvio 1: Viitekehys ydin (NIST 2018)

NIST:in ensimäinen osa on ”Identify”, eli tunnista. Tällä tarkoitetaan sitä, että organisaation täytyy kehittää ymmärrystä ympäristöstään hallitakseen kyberturvallisuusriskejä järjestelmille, varoille, tiedoille ja ominaisuuksille. Tämän osan noudattamiseksi on välttämätöntä, että organisaatiolla on täydellinen näkyvyys digitaalisiin ja fyysisiin omaisuuksiin. Yrityksellä täytyy olla myös näkyvyys määriteltyihin rooleihin ja vastuisiin, sekä

ymmärtää nykyiset riskit ja otettava käyttöön käytäntöjä ja menettelyjä näiden riskien hallitsemiseksi. (Anderson 2020.)

NIST:in toinen osa on ”Protect”, eli suojaa. Tällä tarkoitetaan sitä, että MSP:n on kehitettävä laitettava täytäntöön tarvittavat suojatoimenpiteet mahdollisen kyberhyökkäyksen ehkäisemiseksi tai vähentämiseksi. Tätä varten MSP:n ja heidän asiakkaidensa on vaadittava hallittua pääsyä digitaaliseen ja fyysiseen omaisuuteen, otettava käyttöön käytäntö identiteettien todentamiseksi ja tietojen suojaamiseksi sekä kouluttamalla käyttäjiä kyberturvallisuustietoisuudesta. (Anderson 2020.)

Kolmannella osalla, ”Detect”, tarkoitetaan havaitsemista. MSP:llä ja heidän asiakkaillaan tulisi olla asianmukaiset toimenpiteet kyberhyökkäysten ja muiden tapahtumien tunnistamiseksi nopeasti. Tämä vaihe koostuu todennäköisesti seurantaratkaisuista ja uhkien metsästämisestä epätavallisen toiminnan havaitsemiseksi. (NIST 2019.)

Kehyksen neljännellä osalla, ”Respond, eli vastaa, tarkoitetaan toimintasuunnitelman luomista kyberhyökkäyksen sattuessa. MSP:llä ja asiakkaalla täytyy olla verkkohyökkäysten tai rikkomusten tapahtuessa selkeä toimintasuunnitelma niiden tapahtuman vaikutusten rajoittamiseksi. (NIST 2019.)

Viimeisellä osalla,”Recover”, tarkoitetaan palautusta. MSP:t ja heidän asiakkaansa tarvitsevat suunnitelman järjestelmien ja ohjelmien palauttamiseksi järjestykseen kyberturvallisuustapaturman jälkeen. Tällainen asianmukainen suunnitelma heikentyneiden palveluiden palauttamiseksi tulisi toteuttaa kauan ennen tällaista tapahtumaa esimerkiksi elvytyssuunnittelulla. (Anderson 2020.) Edellä mainittujen viiden ydintoiminnon voi vielä jakaa 23 erilaiseen alakategoriaan (Kuvio 1), joita verrataankin opinnäytetyön lopussa saatuihin tuloksiin.

3 Pilvipalvelu

Pilvipalvelulla tarkoitetaan sitä, että tiedot ja ohjelmat eivät ole omalla tietokoneella tai yrityksen palvelimella, vaan pilvipalvelun tarjoavan palvelun yrityksen palvelimella. Niihin pääsee käsiksi tietokoneella tai mobiililaitteella, kunhan näistä löytyy internetyhteys. (Elisa 2017.)

Nykyaikana pilvipalveluiden käyttö on kasvanut yritysmaailmassa, sillä siitä on paljon hyötyjä suhteessa perinteiseen IT-infraan, jossa työpaikan ohjelmistoihin ja tiedostoihin pääsee käsiksi vain toimiston verkossa lokaalisti. Hyötyihin kuuluvat muun muassa kustannustehokkuus, infran skaalautuvuus, liikkuvuus, tietoturva, varmuuskopiointi ja uusien palveluiden käyttöönotto. (Nousiainen 2020.)

3.1 Pilvipalvelun hyödyt

Kustannustehokkuuden hyöty ilmenee sillä, että yrityksen ei tarvitse kuluttaa järjettömiä summia it-infraan ja sen ylläpitoon, sillä mitään laitteistoa tai datakeskusta ei tarvita. Palvelun laskutus tapahtuukin yleensä tuntitasolla ja perustuu usein siihen, että kuinka paljon resursseja tarvitaan käyttöön. Myöskään yritykset eivät välttämättä tarvitse omaa IT-osastoa, jos pilvipalvelut on otettu palveluntarjoajalta, jolloin palveluntarjoaja hoitaa asiantuntemuksen IT-asioissa. Skaalaavuus on tästä samasta syystä hyöty, sillä on paljon helpompi pienentää tai suurentaa omia tarpeitaan pilvessä, kuin fyysisen laitteiston avulla. (Nousiainen 2020.)

Liikkuvuuden hyöty tulee näkyviin siinä, että työntekijöiden ei tarvitse olla yrityksen omilla konttoreilla, vaan tekee kotikonttorilla etätöitä. Kun palvelut ovat pilvessä ja työntekijät kotikonttoreilla, niin on paljon helpompi myös ottaa uusia palveluita ja ohjelmia käyttöön. Esimerkiksi Microsoftin työkaluilla yritykset voivat työskennellä reaaliaikaisesti tietokoneilla, kuin myös puhelimilla, sillä tieto päivittyy automaattisesti pilveen. (Wallenius 2020.)

Tietoturva ja varmuuskopiointi on myös todella suuri osa pilvipalveluita. Tietojen ollessa pilvessä, ei haittaa, vaikka läppäri tai puhelin vaurioituisi. Pilvipalvelut tarjoavat nopean tietojen palautumisen tällaisissa tapauksissa. Tietoturva taas on yksi yritysten isoimmista huolenaiheista, oli yritys sitten pieni tai suuri. Pilvipalvelut ovat hyviä yritykselle sen takia, että ne tarjoavat monia suojaominaisuuksia, jotka takaavat arkaluontoisen tiedon turvallisen käsittelyn ja tallentamisen. Näitä suojaominaisuuksia ovat muun muassa tekoälyn hyödyntäminen suojauksessa ja kaksivaiheinen tunnistautuminen. (Nousiainen 2020.)

3.2 Palvelumallit

Pilvipalvelut jaetaan perinteisesti kolmeen eri palvelumalliin, joita ovat SaaS (Software as a Service), PaaS (Platform as a Service) ja IaaS (Infrastucture as a service). Palvelun ostajana ei ole niin suuri vastuukynnys tietää näiden merkitystä, sillä palveluntarjoajat osaavat kertoa, että mikä on näistä paras vaihtoehto yritykselle. (Eronen 2016.)

Koska projektin tavoitteena halutaan ottaa käyttöön Swan IT:lle pilvipalvelu, ja alkaa tarjota sitä myöhemmin asiakkaille, on todella tärkeä erottaa eri palvelumallit toisistaan.

SaaS on yhtä kuin ohjelmisto palveluna. SaaS palveluissa palveluntarjoaja vastaa kokonaisvaltaisesti koko ohjelmistosta. Tämä on palvelun ostajalle hyvä ratkaisu, sillä heidän ei tarvitse kuin käyttää ohjelmistoa ja MSP hoitaa loput. SaaS palveluita käytetään usein selaimen kautta, ja tästä on hyvänä esimerkkinä Office 365:n palvelut. (Eronen 2016.)

IaaS tarkoittaa infrastruktuuria palveluna. Tässä tapauksessa asiakkaalle tarjotaan käyttöön yleensä web-pohjainen hallintaliittymä, jonka kautta asiakas voi itse perustaa tarvittavia

palvelimia sekä hallinnoida näitä ja niiden asetuksia. IaaS-mallissa MSP:n vastuu on vain alustojen kohdalla, joten asiakkaalla pitää olla tarpeeksi osaamista, että he voivat hyödyntää tätä mahdollisimman hyvin. IaaS onkin täten hyvä palvelu organisaatiolla, jolla on jo oma IT-osasto tai vastaava osaaminen jotain muuta kautta. (Eronen 2016.)

PaaSista puhutaan, kun MSP tarjoaa palveluna sovellusalustoja, joista on tehty valmiiksi helposti käyttöön otettavia. Sovellusalustat tarjotaan yleisesti ottaen ohjelmistokehityksen käyttöön ja tarpeisiin. Käytännössä voi mennä niin, että palvelunkäyttäjä tilaa sopivan alustan ja siirtää omat sovellukset alustaan. Tässä tapauksessa palvelunkäyttäjälle jää vastuu oman sovelluksen tietoturvasta, joten palvelunkäyttäjän täytyy itse hoitaa päivitykset sekä tietoturva kuntoon omissa sovelluksissaan. PaaS tuo palvelunkäyttäjälle tehokkuutta, sillä heidän ei pidä pitää huolta alustasta ja sen kunnossapidosta. (Eronen 2016.)

4 TeamViewer

TeamViewerillä tarkoitetaan yleensä TeamViewer-yrityksen lippulaivatuotetta: TeamVieweriä. TeamViewer on käytännössä kaikenkattava ratkaisu erilaisiin etätukiin, etäyhteyksiin ja verkkokokouksiin (TeamViewer 2020). Tämän työprojektin aikana on tarkoitus saada TeamViewerissä toimimaan etäyhteystyökalu, että tulevaisuudessa käyttäjien tukeminen etänä olisi helpompaa ja tehokkaampaa.

4.1 Etäyhteydet

TeamViewerin liittäminen Intuneen mahdollistaa myös erilaisten etäyhteyksien hallinnoinnin, mikä oli projektin yhtenä tavoitteena. Tavoitteena oli mahdollistaa kahdenlaisia etäyhteyksiä. Ensimmäinen etäyhteys oli tarkoitus olla sellainen, jossa loppukäyttäjän täytyy itse hyväksyä etäyhteyden otto. Tämän etäyhteyden on tarkoitus luoda tietoturvallisuutta siten, että yhteyden muodostamiseen tarvitaan aina kaksi henkilöä. Myös on tärkeää, että loppukäyttäjä tietää, että hänen tietokoneeseensa ei voi ottaa etäyhteyttä ilman hänen hyväksyntäänsä.

Toisenlainen etäyhteys, jota tarvittiin, piti olla sellainen, että laitteeseen pääsi ottamaan etäyhteyden tietyltä koneelta ilman mitään salasanoja tai loppukäyttäjiä. Tämän pystyi mahdollistamaan TeamViewerin ominaisuudella ”Easy access”.

Easy access on TeamViewerin oma termi, jolla tarkoitetaan yhteyttä, joka ei tarvitse mitään salasanoja. Easy accessin tietoturvallisuus on taattu sillä, että tämän toiminnon voi toteuttaa vain koneilla, jotka ovat yhteydessä yhteen TeamViewer-käyttäjään. Tämä käyttäjä voi omata vaikka kaksivaiheisen tunnistautumisen salasanan lisäksi tuomaan turvallisuutta. (TeamViewer 2019.) Easy access -yhteyttä tarvitaan yrityksessä siihen, että voidaan tarvittaessa ottaa yhteys firman omiin serverikoneisiin etänä. Korona-aikana tätä mahdollisuutta tarvittiin

enemmän, kun koskaan, sillä työskentely oli suurilta osin siirtynyt pois firman omalta toimistolta kotikonttoreille.

4.2 TeamViewer agentti

TeamViewerin agentti, jonka kautta etäyhteyttä on tarkoitus käyttää, on tarkoitus upottaa laitteisiin käyttöönottoprosessin aikana. Prosessin tulisi olla mahdollisimman helppoa loppukäyttäjälle, jotta tuen antaminen veisi mahdollisimman vähän aikaa ja resursseja.

Loppukäyttäjien ei tarvitse etäyhteyttä halutessa kuin napsauttaa TeamViewerin agentti auki tietokoneen työpöydältä ja kertoa IT-tuelle agentissa näkyvä ID.

5 Microsoft Intune

Tässä luvussa käydään läpi Microsoft Intune -järjestelmää, sekä siihen liittyviä ominaisuuksia, mahdollisuuksia ja vaatimuksia käyttöönottoon. Luvussa on myös tarkoitus käydä läpi Microsoft Azuren merkitystä prosessissa ja sen tuomia lisäominaisuuksia laite- ja käyttäjähallintaan. Kappaleessa on tarkoitus myös käydä läpi, että miten Intune saatiin käyttövalmiiksi Swan IT:lle.

Microsoft Azure on Microsoftin julkinen pilvipalvelu, joka tarjoaa sekä PaaS-, että IaaS-tyyppisiä palveluja sovellusten alustaksi. Näitä palveluja ovat esimerkiksi Microsoftin Office 365 -työkalut sekä laitehallintatyökalu Microsoft Intune. Microsoft Azure mahdollistaa myös monivaiheisen tunnistautumisen, joka on tosi iso osa projektin kyberturvallisuustavoitteita. Monivaiheinen tunnistautuminen tarkoittaa sitä, että palvelun käyttäjä käyttää kahta tai useampaa keinoa tunnistaa itsensä kirjautuessaan tiettyyn järjestelmään tai palveluun. (Sulava 2014.)

Microsoft Intune on Microsoft Azure pilvialustalle integroitu järjestelmä. Microsoft Intune on MDM-järjestelmä (Mobile Device Management), eli laitehallintajärjestelmä, jonka tarkoituksena on mobiililaitteiden, tietokoneiden sekä applikaatioiden hallinnointi kokonaan pilvessä. Intunessa yritys pystyy tekemään omanlaisia profiileita, jolla yritys päättää sille sopivat asetukset, ominaisuudet ja suojausasetukset laitteillensa. (Microsoft Docs 2020.)

5.1 Testaus

Microsoft Intunen testaamisessa käytettiin projektin aikana yrityksen yhtä varalla ollutta kannettavaa Windows 10 -tietokonetta. Projektin alussa kaikkia Intunen toimintoja testattiin aluksi vain tälle laitteelle siksi, että palvelusta saataisiin järkevästi käytettävä, ennen kuin sitä alettaisiin tuotteistamaan ja käyttämään oikeissa työympäristöissä. Testauksen

tarkoituksenahan onkin varmistaa, että käyttöönotettava ohjelmisto toimii kuten pitääkin (Iivonen 2020).

5.2 Vaatimukset

Tässä osiossa käydään läpi Microsoft Intunen käyttöönottoon tarvittavat lisenssit sekä vaatimukset. Näihin sisältyvät erilaiset käyttöjärjestelmät, tuetut selaimet sekä Microsoft tilaukset. Myös ”Intune Service Adminstrator role” -rooli on vaatimus Azure-käyttäjällä, jotta käyttäjä voi tehdä muutoksia Intunessa.

Microsoft Intune on sisälletty seuraaviin lisensseihin: Microsoft 365 E3 ja E5, Enterprise Mobility + Security E3 ja E5, Microsoft 365 Business Premium, Microsoft 365 F1 ja F3 sekä Microsoft 365 Government G3 ja G5. (Microsoft Docs 2019.) Projektissa käytettiin E3-lisenssiä.

Jotta Intunen ottaa käyttöön tai haluaa tuotteistaa, tarvitsee tietää mitä käyttöjärjestelmiä ja selaimia Intune pystyy tukemaan. Microsoftin käyttöjärjestelmät, jotka tukevat Intunea ovat: Windows 10 (Home, S, Pro, Education, ja Enterprise versiot), Windows 10 Enterprise 2019 LTSC, Windows 10 IoT Enterprise (x86, x64), Windows 10 Teams (Surface Hub), Windows 10 1709 (RS3) ja myöhemmät, Windows 8.1 RT, PC:t joissa on käytössä Windows 8.1 ylläpito-tila sekä Windows Holographic for Business (Microsoft Docs 2019).

Applen käyttöjärjestelmät, jotka tukevat Intunea: Apple iOS 11.0 ja myöhemmät, Apple iPadOS 13.0 ja myöhemmät sekä Mac OS X 10.12 ja myöhemmät (Microsoft Docs 2019).

Googlen käyttöjärjestelmät, jotka tukevat Intunea ovat: Android 5.0 ja myöhemmät versiot sekä Android enterprise (Microsoft Docs 2019).

Microsoft Intunea tukevat selaimet ovat Google Chromen, Firefoxin, Microsoft Edgen ja Safarin viimeiset versiot. Myös Internet Explorer 11 -versio tukee Intunea. (Microsoft Docs 2019.)

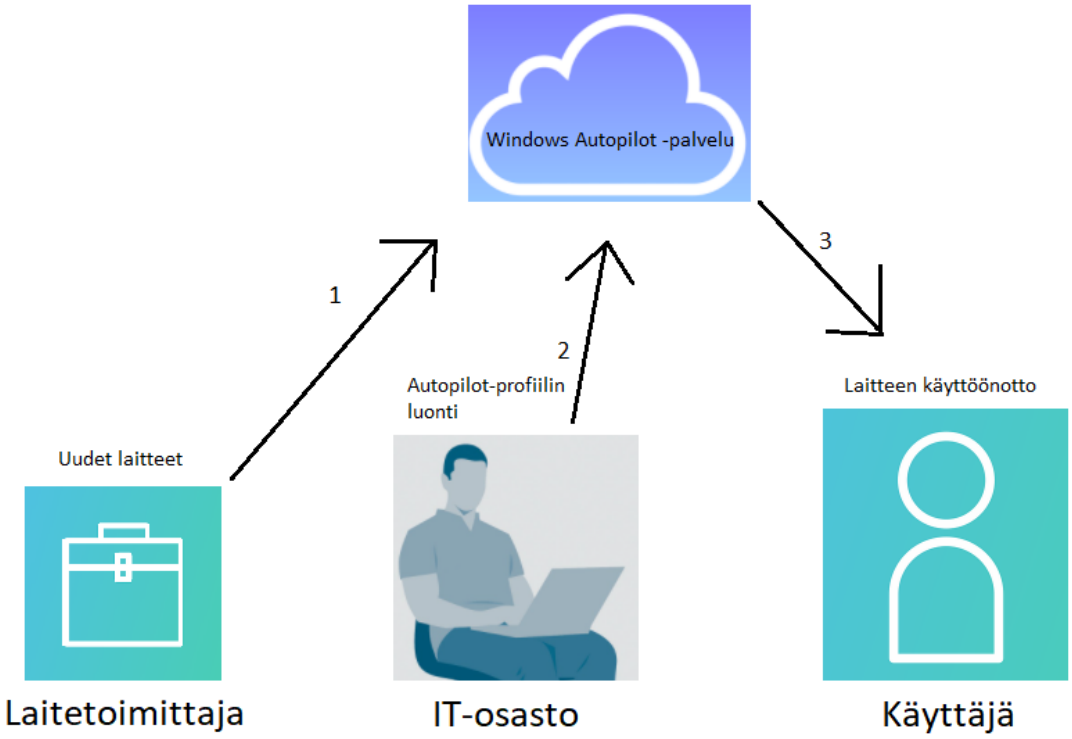
5.3 Asetuksien määrittäminen Intuneen

Tämän osion tarkoituksena on käydä läpi, että millaisia erilaisia määrityksiä Intuneen tehdään ennen laitteiden kirjausta järjestelmään. Osio sisältää ryhmien ja käyttäjien luonnin, sovellusten määrittämisen ja niiden lisäämisen, erilaiset tietoturva-asetukset, ehdollisen pääsyn, päivitykset ja muita satunnaisia määrityksiä, joita tehtiin.

5.3.1 Laitteiden kirjaus Intuneen

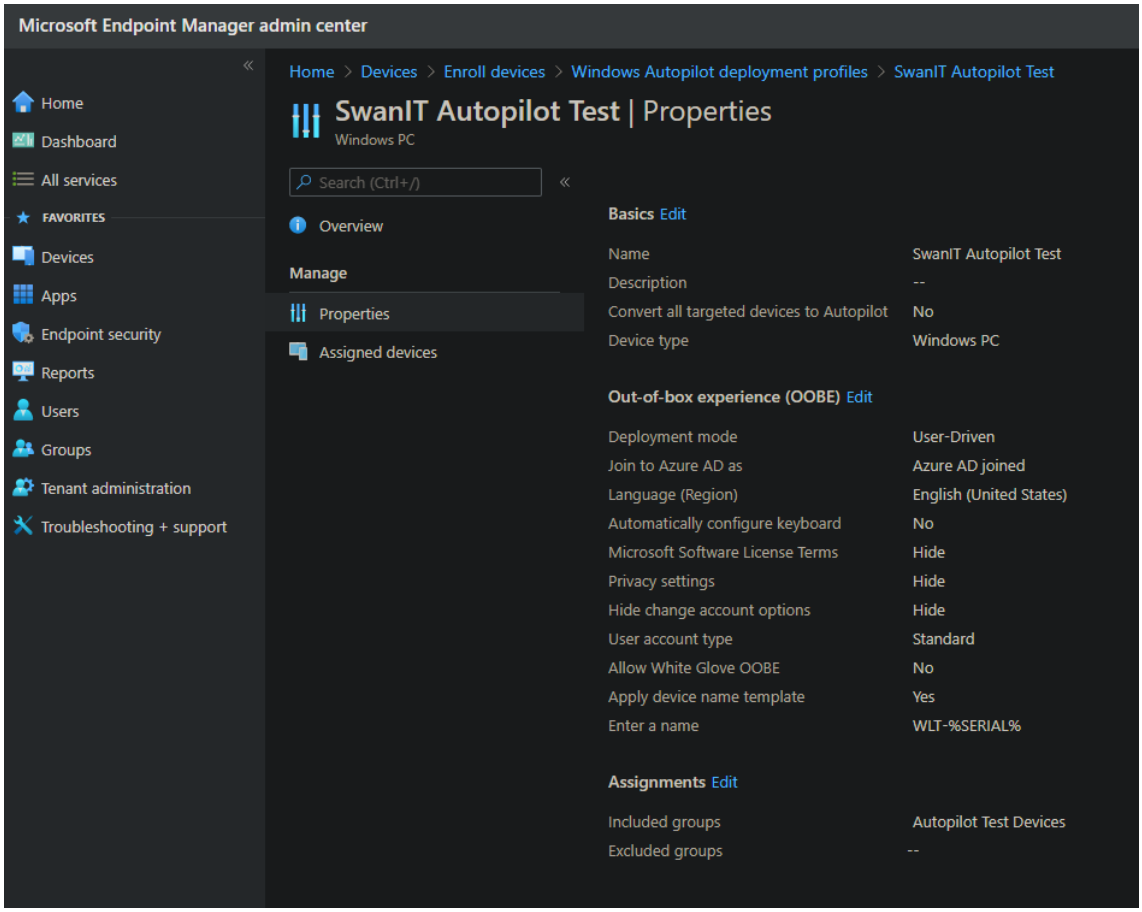
Laitteiden kirjaamiseen käytetään Windows Autopilottia. Windows Autopilotilla on tarkoitus yksinkertaistaa ja automatisoida tapa, jolla laite otetaan käyttöön, nollataan tai kohdistetaan

uudelleen ilman yrityksen IT-tuen apua. Käyttäjän perspektiivistä ainoat asiat mitä pitää tehdä, on liittää laitteeseen nettiyhteys ja kirjautua sisään omilla tunnuksillaan. Yrityksen IT-osaston perspektiivistä aikaa säästyy siten, että jokaiselle koneelle ei tarvitse tehdä omia profiileita ja asetuksia, vaan samanlaiset asetukset voidaan upottaa Autopilotin kautta monelle koneelle. (Microsoft Docs 2020.) IT-osaston ei tarvitse edes lisätä laitteita itse Autopilot-käyttöönottopalveluun, sillä laitteistomyyjä tekee tämän heidän puolestaan (Microsoft 2020).



Kuvio 2: Autopilot-palvelun prosessin havainnointi

Kuviossa 2 selitetään laitteen Autopilot-palvelun prosessi. Kohdassa 1 laitetoimittaja lisää laitteet Autopilot-käyttöönottopalveluun ja lähettää laitteen käyttäjälle. Kohdassa 2 käyttäjän IT-osasto luo Autopilot-profiilin, joka määritetään käyttäjälle. Kohdassa 3 käyttäjä saa tietokoneen ja käynnistää OOBE-prosessin (Out of Box Experience), millä tarkoitetaan prosessia, kun käyttäjä ottaa laitteen ensimmäisen kerran käyttöönsä (Microsoft Docs 2018). Käyttäjän täytyy yhdistää laite internettiin ja kirjautua sisään omalla työtunnuksellaan, ja Windows Autopilot asentaa profiilin mukaiset asetukset koneelle.



Kuvio 3: Windows Autopilot profiili

Testauksessa luotu profiili Windowseja varten. Profiilissa on määritetty, että:

- käyttäjä itse kirjaa koneensa Azure AD:seen omilla tunnuksillaan.
- Tietokoneen kieleksi tulee englanti, sillä se on yritysystävällisempi
- Käyttäjästä tulee ”Standard” käyttäjä, eli hänellä ei tule olemaan ylläpitäjän oikeuksia
- Asennuksessa piilotettu asetusten muuttaminen.
- Tietokoneen nimeksi tulee Intunessa WLT-%SERIAL%, mikä tarkoittaa, että tietokoneen nimeksi tulee Intuneen sen sarjanumero.
- Tietokone kuuluu ”Autopilot Test Devices” -ryhmään, jota käytettiin Windows Autopilot -testiryhmänä.

Intuneen on myös mahdollista kirjata käyttäjien jo valmiiksi omaamat laitteet. Näitä laitteita kutustaan BYOD-laitteiksi (Bring your own device). Tämä voidaan tehdä esimerkiksi siitä syystä, että yritys vaatii käyttäjiltä laitteen kirjaamisen Intuneen ennen kuin laitteella pääsee käsiksi yrityksen resursseihin. Laitteet voidaan kirjata lataamalla käyttäjän laitteeseen yritysportaali. Yritysportaali ladataan Windows-koneilla Microsoft Storesta, Android-laitteilla

Play Kaupasta ja Applen tuotteilla App Storesta. Latauksen jälkeen käyttäjä kirjautuu yritysportaaliin omalla työsähköpostilla ja hyväksyy laitteen kirjauksen Intuneen yritysportaalista. (Microsoft Docs 2020.)

5.3.2 Ryhmät ja käyttäjät

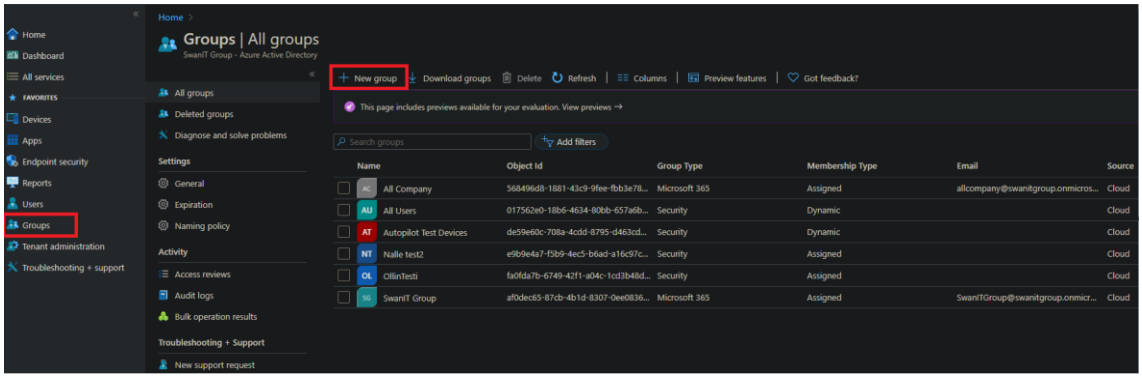
Microsoft Intune käyttää Azure Active Directoryn ryhmiä hallinoidakseen laitteita ja käyttäjiä. Ryhmät tehdään yrityksen tarpeiden mukaiseksi. Yritykset voivat esimerkiksi tehdä omanlaiset ryhmät maantieteellisen sijainnin, osaston tai laitteiden käyttöjärjestelmän mukaisesti.

Ryhmiä pystyy tekemään kahdenlaisia:

- ”Assigned group”, eli määrätyt ryhmät. Näihin ryhmiin voi lisätä laitteita ja käyttäjiä manuaalisesti.
- ”Dynamic group”, eli dynaaminen ryhmä. Tämä tarkoittaa sitä, että käyttäjät tai laitteet menevät automaattisesti näihin ryhmiin, riippuen ryhmän asetuksista. Esimerkiksi ryhmäksi voi laittaa ”Esimiehet”, jolloin kaikki käyttäjät, joilla on tittelinä esimies, siirtyy automaattisesti tähän ryhmään. Toinen hyvä esimerkki on tehdä dynaaminen ryhmä eri käyttöjärjestelmille. (Microsoft Docs 2019).

Projektissa luotiin Swan IT:lle jo omia ryhmiä valmiiksi, sekä erilaisia testiryhmiä Intunen testaamiseen. Ryhmät, jotka projektissa luotiin:

- All Company – Testiryhmä. Tämä ryhmä on tyypiltään ”Microsoft 365” -ryhmä, eli se antaa kaikille ryhmässä oleville yhteisen resurssikokoelman.
- All Users – Dynaaminen ryhmä, joka määräytyy jokaiselle käyttäjälle Intunessa.
- Autopilot Test Devices – Dynaaminen ryhmä, jonka avulla kirjattiin Windows Autopilotin avulla testikoneet Intunen ympäristöön.
- SwanIT Group – Ryhmä, joka lisätään jokaiselle Swan IT:n käyttäjälle. Tämä ryhmä on tyypiltään ”Microsoft 365” -ryhmä.
- Erilaiset ”Security” testiryhmät – Käytettiin erilaisten testien toteuttamisessa.



Kuvio 4: Intune -ryhmät

Kuviossa 3 näkyy projektissa luodut ryhmät. Ryhmät voi luoda Intunen portaalista kohdasta Groups -> New Group. Ryhmää tehdessä voi valita, että onko ryhmän tyyppi joko ”Security” vai ”Microsoft 365”. ”Security” tyyppiset ryhmät määrittelevät, että kuka voi käyttää mitäkin resursseja (Microsoft Docs 2019).

Microsoft 365 -ryhmällä luodaan resurssikokoelma eri käyttäjien välille. Tähän resurssikokoelmaan kuuluu jaettu sähköpostilaatikko, kalenteri ja jaettu SharePoint-sivusto. (Microsoft 2020.)

5.3.3 Sovellukset

Microsoft Intunessa on mahdollista hallinnoida yrityksen käyttämiä sovelluksia. Yksi IT ylläpitäjien prioriteeteistä onkin pitää huolta, että työntekijöillä on tarvittavat sovellukset työntekoon. Sovelluksia voi konfiguroida, lisätä, lisätä tietyille käyttäjille/ryhmille, suojata, valvoa, päivittää ja poistaa. (Microsoft Docs 2020.)

Projektissa testattiin asentaa sovelluksia kaikilla mahdollisilla tavoilla Windows-koneelle, jotta saataisiin omakohtaista kokemusta sovellusten asentamisesta ja että mitkä tavat sopisivat mihinkin tarkoitukseen. Eri sovelluksien jakotapoja kutsutaan Intunessa sovellustyypeiksi.

Ensimmäinen sovellustyyppi, jota testattiin, oli nettisivussa oleva lataus eli ”Web app”. Tässä tapauksessa luotiin yrityksen yritysportaaliin kuvake, joka käyttää nettisivun osoitetta ladatakseen sovelluksen. Loppukäyttäjän näkökulmasta asennus on helppoa, sillä käyttäjän täytyy vain painaa sovellusta yritysportaalista ja painaa ”Lataa”. Huono asia tässä kuitenkin on se, että usein netistä ladatut sovellukset lataavat asennustiedostoja, jotka voivat vaatia ylläpitäjän oikeuksia, että ne voidaan laittaa käyntiin. Ylläpitäjän näkökulmasta tämä sovellustyyppi jaetaan seuraavasti: Intunen portaalista valitse Apps -> Windows -> Add -> Valitse Web link. Web link -sovellukseen tarvitsee laittaa vain sovelluksen nimi, julkaisijan nimi, sovelluksen kuvaus sekä URL-osoite, josta lataus käynnistyy.

Kuvio 5: Microsoft Store - SwanIT Group -välilehti

Toinen tyyppi, jolla ladattiin sovelluksia testikoneelle, oli tyypiltään Microsoft store app. Tässä tapauksessa erilaisia sovelluksia voidaan laittaa yrityksen omalle Microsoft Storen sivulle ladattavaksi (SwanIT Group -välilehti kuviossa 4). Tämä tapa jakaa sovelluksia oli muuten hyvä, paitsi että se rajoittui pelkkiin Microsoft Storen sovelluksiin. Nämä Microsoft Store -sovellukset tulivat myös näkyviin yrityksen omaan yritysportaaliin. Loppukäyttäjän näkökulmasta tämä tapa on helppo saada sovelluksia, sillä niitä täytyy vain etsiä Microsoft Storesta ja painaa ”Lataa”. Hyviä asioita Microsoft Store -sovelluksissa ylläpitäjän kannalta oli se, että niitä on todella helppo laittaa jakoon. Ylläpitäjän täytyy kirjautua selaimella Microsoft Storen portaaliin -> etsiä sieltä sovellusta -> ladata sovellus. Kun ylläpitäjä on ladannut sovelluksen, voi sovelluksen asetuksista laittaa sovelluksen näkyviin yrityksen omalle Microsoft Store -sivulle. Tämän sovelluksentyypin voi laittaa käyttäjille vapaaehtoisena latauksena tai pakottaa ”hiljaisena” latauksena koneelle. Hiljainen lataus tässä tapauksessa tarkoittaa sitä, että lataus tapahtuu automaattisesti ja huomaamattomasti loppukäyttäjälle.

Kolmas sovellustyyppi, jolla jaettiin sovelluksia, oli nimeltään ”Line-of-business- app” tai LOB-applikaatio. Tällä tarkoitetaan usein yrityksen omia, eli ”in-house”, sovelluksia. Käytännössä tämä tapa toimii Windowsissa siten, että Intuneen upotetaan joko .msi, .appx, .appxbundle, .msix, tai .msixbundle -tiedostomuodossa oleva lataustiedosto. Tämä lataustiedosto jaetaan yritysportaalin kautta tietokoneisiin. Sovellus voidaan laittaa vapaaehtoiseksi lataukseksi tai pakotetuksi lataukseksi. (Microsoft Docs 2020). Projektissa tätä testattiin TeamViewerin lisenssissä mukana tulevalla MSI-tiedostolla. Käyttäjien näkökulmasta tämä on omasta mielestä paras vaihtoehto, sillä tämä ei vaadi mitään ylläpitäjätunnuksia ladatessa ja lataus on vain parin klikkauksen päässä yritysportaalissa. Ylläpitäjän puolesta tämä ei välttämättä ole helpoin vaihtoehto, sillä MSI-tiedostojen (tai vastaavien tiedostomuotojen) tekeminen sovelluksista ei ole helppoa, eikä niiden tekemiseen perehdytty tämän projektin aikana.

Neljäs testattu sovellustyyppi oli ”Microsoft 365 Apps”. Tällä sovellustyypillä pystytään lisäämään yritysportaaliin Microsoftin 365 -sovelluksia joko pakotettuna latauksena tai vaihtoehtoisena latauksena. Projektissa jaettiin tämän sovellustyypin kautta seuraavat sovellukset: Excel, OneDrive Desktop, OneNote, Outlook, PowerPoint, Publisher, Skype for Business, Teams ja Word.

Intune mahdollistaa myös sovelluksen datan suojaamisen erilaisilla sovellussääntöpolitiikoilla. Sovelluksille voi tehdä kolme erilaista sääntöä Intunen portaalista kohdasta Apps -> App Protection Policies > Create Policy. Nämä säännöt ovat ”Block”, ”Allow Overrides” ja ”Silent”. Blockilla tarkoitetaan yrityksen datan siirron estämistä sovelluksesta. ”Allow Overrides” tarkoittaa sitä, että sovellus huomauttaa, kun yrityksen dataa ollaan siirtämässä ei-suojattuun sovellukseen. ”Silent” tarkoittaa sitä, että sovelluksesta voi siirtää yrityksen dataa vapaasti. Projektissa ei laitettu millekään sovellukselle näitä sääntöjä, sillä näitä ei koettu hyödylliseksi. Kuitenkin tulevaisuutta varten on hyvä olla selvillä, että tällainen mahdollisuus on olemassa.

5.3.4 Päivitykset

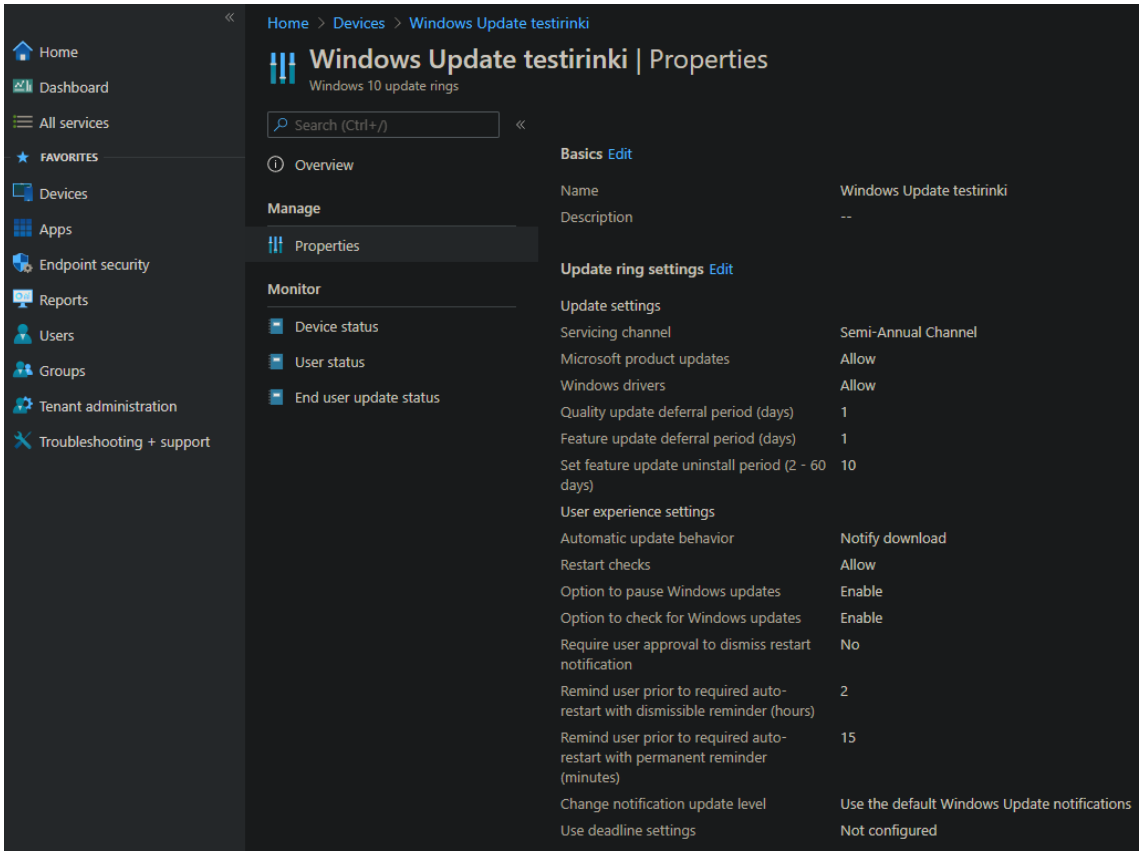
Windows-päivitykset tulevat Intunen ”Windows update ring” -toiminnon avulla. Windows update ring on kokoelma erilaisia päivitysasetuksia, joita voidaan säädellä Intunen ryhmien avulla. Windows update ring -profiilissa voi valita kolmea erilaista ”Servicing Channelia”, eli huoltokanavaa. Näitä ovat Semi-Annual Channel, Windows Insider – Fast, ja Windows Insider - Slow. Näillä kanavilla määritellään, että millaiset ja milloin päivitykset tulevat laitteille. (Windows Docs 2020.)

Semi-Annual channeleissa käyttöjärjestelmäpäivitykset tulevat kahdesti vuodessa, ja näitä päivityksiä tuetaan 18 kuukautta. Päivitykset ovat vakaita ja bugittomia, sillä niitä testattu ennen julkaisua.

Windows Insider -kanavat ovat tarkoitettu niille, jotka haluavat päivitykset ennen kuin Semi-Annual kanava voi tarjota niitä. Insider–Fast -kanava on tarkoitettu niille, jotka haluavat uusimmat päivitykset ensimmäisenä esimerkiksi testausmielessä (Microsoft Docs 2020.) Fast-kanavalla olevat päivitykset eivät ole vakaita ja voivat sisältää pieniä vikoja. Insider – Slow -kanava on tarkoitettu niille, jotka haluavat nopeasti vakaita päivityksiä. Slow-kanavan päivitykset eivät ole aivan yhtä nopeita kuin Fast-kanavan. (Langowski 2020.)

Projektissa luotu Windows update ring -profiili sisältää seuraavat määritykset:

- Käytetään Microsoftin Semi-annual channelia.
- Windows update ring pystyy päivittämään tietokoneen ajureita ja Microsoftin tuotteita.
- Päivitykset tulevat Windows-ilmoituksena käyttäjälle
- Ilmoitus päivityksistä tulee kaksi tuntia ennen päivitystä.
- Loppukäyttäjä voi lykätä 3. päivällä päivityksiä.

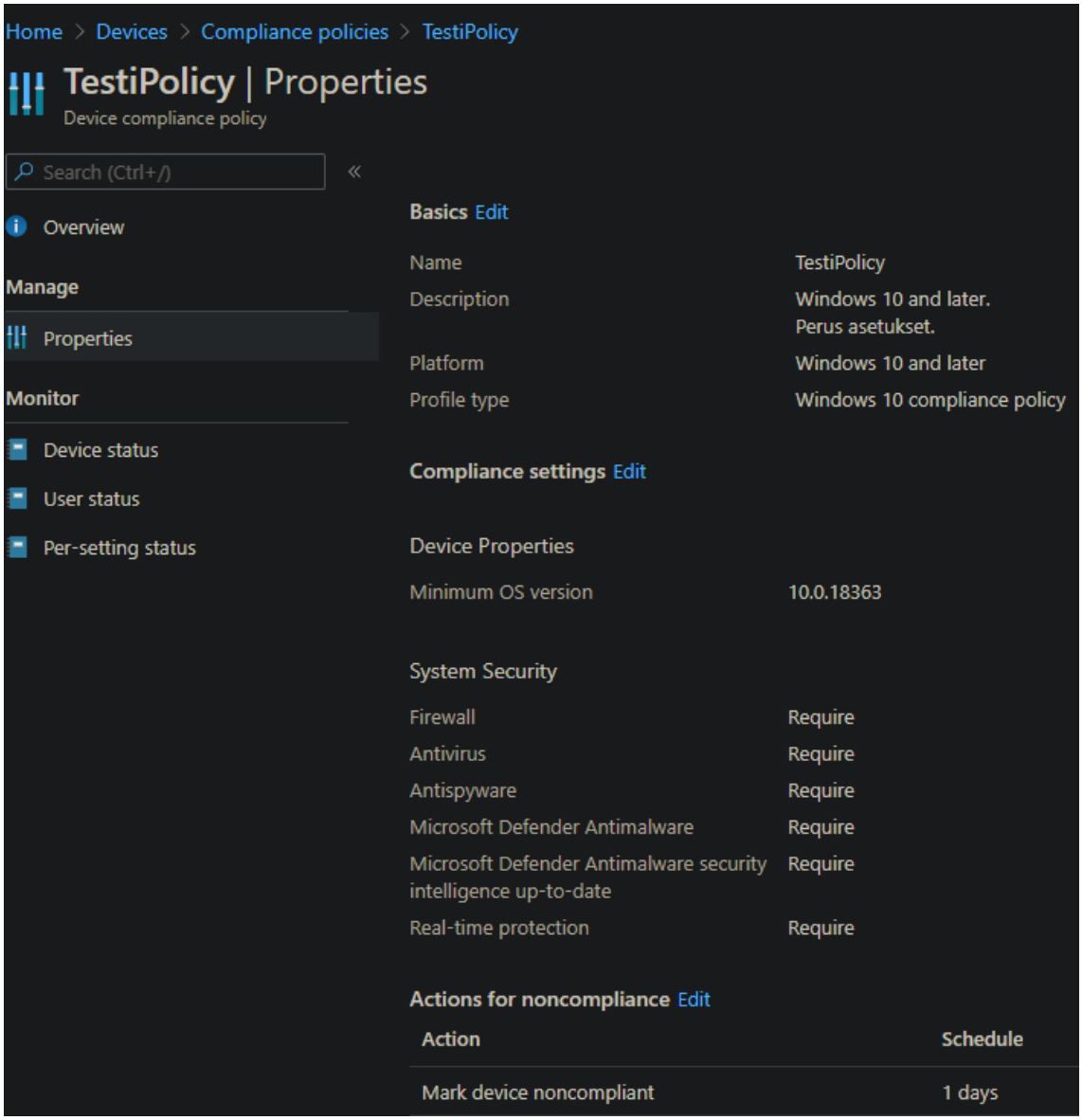


Kuvio 6: Windows Update Ring -profiili

Kuviossa 3 on projektissa luotu Update Ring -profiili. Profiilit luodaan Intunen portaalista kohdasta Devices -> Windows 10 update rings -> Create profile. Semi-annual channel valittiin projektissa sen takia, koska se on hyvin testattu, eikä siinä pitäisi olla paljon bugeja. Päivitykset määriteltiin lykättäväksi, koska käyttäjällä ei välttämättä ole aina aikaa asennella päivityksiä.

5.3.5 Compliance policy

”Compliance policylla” tarkoitetaan Intunessa sitä, että onko laite säädösten mukainen ja voiko sen päästää yrityksen resursseihin. Laitteiden on läpäistävä määritellyt säännöt ja asetukset, jotka käyttäjille ja laitteille on asetettu, jotta laitteet ovat yhteensopivia Intunen kanssa. Jos laite noudattaa sääntöjä, se on ”Compliant”, eli noudattava laite. Jos laite ei noudata sille annettuja sääntöjä, se on ”Not compliant”. Erilaisia toimenpiteitä voidaan määritellä laitteille, jotka ovat Non compliant -tilassa. Näitä ovat sähköpostin lähettäminen laitteen käyttäjälle, että laite ei noudata sääntöjä ja asetukset pitää korjata tietyn ajan kuluessa. Toinen on, että laite lukitaan tietyn ajan kuluttua siitä, kun laite on mennyt Non compliant -tilaan. Kolmas on, että jos laite on liian kauan Non compliant, se poistetaan Intunesta ja yrityksen data pyyhitään pois. (Microsoft Docs 2020.)



Kuvio 7: Compliance policy -profiili

Kuviossa 7 on projektissa luotu Compliance policy -profiili, eli sääntöprofiili laitteille. Profiili on määritelty Windows 10 -laitteille ja profiilissa on määritelty seuraavat asiat:

- Windows-versio oltava vähintään 10.0.18363.
- Palomuuri tulee olla päällä.
- Pitää olla jonkunlainen viruksentorjuntaohjelma
- Pitää olla päällä Microsoft Defender Antimalware ja sen päivitykset täytyy olla ajan tasalla.
    - Myös Real-time protection, eli Microsoft Defenderin kyky skannata reaaliajassa haittaohjelmia, täytyy olla päällä.

- Jos nämä säännöt eivät täyty yhden päivän sisällä, tulee laitteesta ”Not compliant”. Laitteen haltijalle on laitettu lähtemään sähköposti, kun jokin laitteen asetus ei vastaa sääntöjä. Adminit pystyvät myös näkemään Intunen portaalista, että minkä takia käyttäjän laite on ”Not compliant”.

Compliance policyillä on tarkoitus tuoda kyberturvallisuutta erilaisin tavoin. Suhteutettuna NIST-kyberturvallisuuskehykseen, compliance policyt täyttävät kategorioita kohdista ”Suojaa” ja ”Havaitse”. Suojaa-osasta compliance policyt täyttävät kategorian ”Data Security”. Data securityllä tarkoitetaan datan suojaamista erilaisin tavoin, kuten toimintasuunnitelmilla tai yrityspolitiikoilla (NIST 2018). Projektissa luodussa Compliance policy -profiilissa on määritelty, että käyttäjien on pakko pitää erilaisia suojausmenetelmiä päällä koneessa, mikä suojaa tietokoneen dataa.

Havaitse-osasta täyttyy kohta ”Security Continuous Monitoring”. Tällä tarkoitetaan jatkuvaa turvallisuuden valvontaa (NIST 2011). Tähän on päästy pakottamalla käyttäjiä pitämään Microsoft Defenderin ”Real-time protectionia” päällä compliance policyn avulla.

5.3.6 BitLocker

BitLockerilla tarkoitetaan kiintolevyn tai ulkoisen muistilaitteen salausohjelmaa Windowseissa. Käytännössä BitLocker sekoittaa tietokoneen datan, minkä takia dataa ei pysty lukemaan ilman todennusta. BitLocker salaa kiintolevyn tiedostot salasanan avulla. (ZumBrunnen 2019.)

BitLockerin salauksen ansiosta koneiden tiedot ovat turvassa, vaikka kiintolevyt otettaisiin irti koneesta. Tämän BitLocker tekee siten, että se ottaa muistiin tietokoneen sisäisten osien sarjanumeroita, joiden avulla BitLocker tunnistaa onko muisti siihen kuuluvassa tietokoneessa. (ZumBrunnen 2019.)

Työprojektissa luodussa profiilissa määriteltiin seuraavat asiat:

- BitLocker täytyy olla aktivoitu
- BitLocker ei salaa ulkoisia muistilaitteita
- BitLockerin salausavain tulee näkyviin myös Azure AD:seen, eikä BitLockeria saa päälle, ennen kuin Azure AD on vastaanottanut salausavaimen.
    - Tämä varmuudeksi, jos loppukäyttäjä hävittää oman salausavaimensa.
- Muuten Intunen vakioasetukset BitLockerille.

BitLocker tuo monella tapaa kyberturvallisuutta. BitLocker täyttää NIST-kyberturvallisuuskehyksen kategoriasta ”Suojaa” kohdat Data Security ja Protective Technology. Näillä tarkoitetaan datan suojausta ja suojaavaa teknologiaa. BitLocker myös

täyttää ”Vastaa”-kategoriasta kohdan ”Mitigation”, jolla tarkoitetaan riskien lieventämistä. Käytännön esimerkkinä tästä on esimerkiksi se, jos työntekijä hävittää laitteensa työmatkalla ulkomailla. Tässä tapauksessa laitteen tiedot on suojattu teknologialla ja täten riskiä tiedon joutumista kolmannen osapuolen käsiin on lievennetty.

5.3.7 SSPR

SSPR tulee sanoista Self-service password reset. Tällä tarkoitetaan käyttäjien kykyä resetoida itse heidän salasanansa, ilman ylläpitäjiä tai IT-osastoa. Tämä nopeuttaa loppukäyttäjän työskentelyä, jos jostain syystä salasana on unohtunut tai käyttäjä on lukittautunut. Tällä toiminolla palvelunkäyttäjän help deskilläkin säästyy paljon aikaa.

SSPR toimii Azure AD:n kautta. Kun käyttäjä yrittää vaihtaa salasanaansa, Azure AD tekee seuraavaksi mainitut toimenpiteet verifioidakseen käyttäjän. Ensimmäisenä AAD tarkistaa onko käyttäjällä SSPR päällä ja onko se yhdistetty AAD-lisenssiin. Toiseksi AAD tarkistaa, että onko käyttäjän todennusmenetelmät määritelty. Kolmanneksi AAD tarkistaa, että käyttäjän salasana on hallinnoitu myös ”on-premises” AD:ssa, eli perinteisessä AD:ssa. Jos kaikki nämä kolme tarkistusta menee läpi, voi käyttäjä jatkaa salasanan vaihtoa. Jos jokin näistä ei mene läpi, tulee käyttäjälle viesti, että hänen täytyy ottaa omaan IT-tukeen yhteyttä. (Microsoft Docs 2020).

Että loppukäyttäjillä toimii SSPR, on palveluntarjoajan valittava todennusmenetelmä, jolla käyttäjät todentavat itsensä. Näihin todennusmenetelmiin kuuluvat puhelimen todennusapplikaatio, sähköposti, puhelimen tekstiviesti, turvallisuuskysymykset ja perinteiset toimistopuhelimet. Näistä menetelmistä on pakko valita ainakin yksi, mutta mahdollisuutena on myös valita kaksi. (Microsoft Docs 2020).

Tässä projektissa valittiin testiryhmälle todennusmenetelmäksi puhelimen applikaatio, sillä se on omasta kokemuksesta kaikkein nopein ja helppokäyttöisin. Muita asetuksia, joita valittiin SSPR -käytössä, oli päivien määrä, kunnes todennustapa pitää varmentaa uudestaan. Tämä asetettiin 180 päivään. Myös salasanan vaihdosta asetettiin tulemaan sähköposti, että käyttäjä huomaa, jos hänen salasanansa vaihdetaan ilman hänen tietämättä.

5.3.8 Konfiguraatioprofiilit

Microsoft Intune sisältää erilaisia asetus- ja toimintoprofiileja, joita kutsutaan konfiguraatioprofiileiksi. Konfiguraatioprofiileita voidaan määrätä joko laitteelle, henkilölle tai ryhmille. Erilaisille käyttöjärjestelmille on yhteisiä, mutta myös yksityisiä profiileja (tämä siitä syystä, koska eri käyttöjärjestelmillä on erilaiset asetukset). (Microsoft Docs 2020.)

Projektissa keskityttiin Windows-käyttöjärjestelmään liittyviin konfiguraatioprofiileihin. Profiilit pystyvät muuttamaan koneen asennuksia ja toimintoja todella monella tapaa. Näitä

ovat muun muassa profiilit, jotka vaihtavat koneen turvallisuusasetuksia, muuttavat sovelluksien asetuksia tai automatisoi koneen käyttöä. (Microsoft Docs 2020.)

Projektissa luotiin muutamia profiileja, jotka koettiin hyödylliseksi. Näitä olivat jo aiemmin mainitut Bitlocker- ja SSPR-profiilit. Muita olivat WiFi-, tulostin-, OneDrive- sekä aikavyöhykeprofiilit. Profiilit pystyivät luoda Intunen portaalista -> Devices -> Configuration Profiles -> Add ja täältä valitsemalla Windows ja profiilin kategoria.

Tulostinprofiilissa laitettiin toimiston tulostin asentumaan automaattisesti, kunhan käyttäjä on toimiston verkossa. Jos yrityksellä olisi ollut oma tulostinpalvelin, niin yrityksen verkkoa ei olisi tarvittu. Profiilissa määriteltiin myös printterin olevan oletustulostin. Profiilissa tarvitsi määritellä printterin nimi ja printterin IP-osoite.

WiFi-profiilissa määriteltiin toimiston henkilökunnan verkko yhdistämään työntekijöiden Windows-koneille. Verkolle täytyi määritellä nimi sekä verkon salasana, jotta tietokoneet pystyivät ottamaan verkkoon yhteyden. Wifi-profiilissa myös määriteltiin, että laitteet yhdistävät verkkoon automaattisesti, vaikka verkko olisi piilotettu, kunhan verkko on tavoitettavissa.

OneDrive-profiili määritettiin sen takia, että se automatisoi käyttöönottoa. Profiilissa määriteltiin, että OneDrive kirjautuu hiljaisesti sisään Windows-käyttäjätunnuksilla. Profiilissa määriteltiin myös, että OneDrive kehottaa käyttäjää synkronoimaan ”Windows known folders” OneDriveen. Nämä tunnetut kansiot ovat työpöytä-, dokumentti-, lataus- sekä kuvakansiot. OneDrive täyttää myös NIST-kyberturvallisuuskehyksen ”Recovery Planning” -kategoriaa, jolla tarkoitetaan suunnitelmia kyberhyökkäyksistä palautumisesta (NIST 2018). Tästä esimerkiksi, jos käyttäjän koneille tulee virus ja koneen joutuu palauttamaan tehdasasetuksille, niin tiedostot eivät katoa, vaan löytyvät pilvestä.

Viimeinen profiili, joka projektissa luotiin oli aikavyöhykeprofiili. Tämä tehtiin siksi, koska testikoneen kellonaika oli pielessä. Profiilia luodessa täytyi merkitä Suomen aikavyöhykkeen nimi, eli ”FLE Standard Time”.

6 Pohdinta

Projekti oli siltä kannalta onnistunut, että siitä saatiin hyvä pohja ja hyvää informaatiota Intunen käyttöönottoon. Projekti toi Swan IT:lle tietoja ja käytännöntaitoja, joita ennen ei ollut. Projektista saadun tiedon ja taidon ansiosta yrityksessä voidaan ottaa Intune käyttöön ja parannella sitä ajan myötä käyttötarpeiden mukaan. Intunen käyttö tulee viemään tulevaisuudessa aikaa, sillä uusiin ominaisuuksiin tutustuminen ottaa oman aikansa. Aikaa

tulee menemään myös siihen, että työntekijöille täytyy opettaa Intunen käyttöä, sillä tämän kokoisella sovelluksella ei voi olla vain yhtä ylläpitäjää.

Intune myös tuo todella paljon tietoturvallisuutta yritykselle. Verrattuna NIST-kyberturvallisuuskehykseen, Intune täyttää jo monta kategoriaa. Näitä kategorioita ovat Recovery Planning, Data Security, Protective Technology, Security Continuous Monitoring ja Mitigation. Käytännössä tämä tarkoittaa sitä, että Intune antaa tietoturvaa ennen ja jälkeen tietoturvahyökkäyksen. Muutenkaan Intunen ei olekaan tarkoitus täyttää koko kehystä, eikä se ole edes mahdollista, sillä kehykseen kuuluu kategorioita, joita Intune ei pysty täyttämään. Intune kuitenkin tekee hyvää työtä siinä missä pitääkin, eli laitehallintaan liittyvässä tietoturvallisuudessa.

Haasteena oli perehtyä Intuneen siinä mielessä, että millainen ympäristöstä tulee, kun siihen lisätään asiakkaiden laitteet. Tavallaan tällä tavalla ajattelu onkin ollut mahdotonta. Tämä siitä syystä, että jokaisella yrityksellä on omanlaiset tavoitteet laitteenhallinnassa ja sovellustenhallinnassa, ja näistä tavoitteista pitää sopia palveluntarjoajan/asiakkaan kanssa. Intunen käytöstä alkaakin saamaan kunnolla dataa vasta, kun työkalun käyttö normalisoituu ja se saadaan asiakkaillekin käyttöön. Pitkän ajan käytöstä esiintyviä ongelmia ja muita vikatilanteitakin voidaan havainnoida vasta tietyn ajan jälkeen.

Olen itse oppinut valtavasti itse järjestelmästä ja sen käytöstä projektin aikana. Jouduin projektin aikana tekemään siinä käytetyn ympäristön alusta alkaen, käyttäen Microsoftin omaa dokumentaatiota, joka ei aina ollut aivan ajan tasalla, sillä Intune on niin nopeasti muuttuva järjestelmä. Vielä on kuitenkin todella paljon opittavaa laitehallintajärjestelmistä, sillä tulevaisuudessa täytyy opetella, miten Intune toimii eri käyttöjärjestelmien kuin pelkästään Windowsin kanssa yhteen. Projektista tulleen tiedon kautta minun on myös helpompi tulevaisuudessa laajentaa osaamista muihin Microsoftin järjestelmiin, sillä niistä on varmasti apua tulevaisuudessa.

Lähteet

Sähköiset

Anderson, E. 2020. How to comply in 2020 with the 5 functions of the NIST cybersecurity framework. Viitattu 8.11.2020. https://www.forescout.com/company/blog/how-to-comply-with-the-5-functions-of-the-nist-cybersecurity-framework/

Elisa 2017. Mikä on pilvipalvelu? Viitattu 10.11.2020. https://elisa.fi/ideat/mika-on-pilvipalvelu/

Eronen, H. 2016. IaaS, PaaS, SaaS? Mikä pilvipalvelu sopii yrityksellesi. Viitattu 11.11.2020. https://www.planeetta.fi/2016/03/15/iaas-paas-saas-mika-pilvipalvelu-sopii-yrityksellesi/

Haas, K. 2020. Understanding Office 365 Update Channels. Viitattu 17.11.2020. https://www.mirazon.com/understanding-office-365-update-channels/

Horan, M. 2019. What is NIST? Understanding Why You Need to Comply. Viitattu 8.11.2020. https://www.ftptoday.com/blog/what-is-nist

Iivonen, J. 2020. Testaussanasto – ohjelmistotestauksen tärkeimmät termit selitettynä. Viitattu 14.11.2020. https://projecttop.com/testaussanasto/

Langowski, A. 2020. Introducing Windows Insider Channels. Viitattu 21.11.2020. https://blogs.windows.com/windows-insider/2020/06/15/introducing-windows-insider-channels/

Microsoft 2020. Windows Autopilot. Viitattu 29.11.2020. https://www.microsoft.com/fi-fi/microsoft-365/windows/windows-autopilot

Microsoft Support 2020. Lisätietoja Microsoft 365 -ryhmistä. Viitattu 23.11.2020. https://support.microsoft.com/fi-fi/office/lis%c3%a4tietoja-microsoft-365-ryhmist%c3%a4-b565caa1-5c40-40ef-9915-60fdb2d97fa2?ui=fi-fi&rs=fi-fi&ad=fi

Microsoft Docs 2018. Customize the Out of Box Experience (OOBE). Viitattu 29.11.2020. https://docs.microsoft.com/en-us/windows-hardware/customize/desktop/customize-oobe

Microsoft Docs 2019. Add groups to organize users and devices. Viitattu 22.11.2020. https://docs.microsoft.com/en-us/mem/intune/fundamentals/groups-add

Microsoft Docs 2019. Microsoft Intune licensing. Viitattu 14.11.2020. https://docs.microsoft.com/en-us/mem/intune/fundamentals/licenses

Microsoft Docs 2020. Add a Windows line-of-business app to Microsoft Intune. Viitattu 27.11.2020. https://docs.microsoft.com/en-us/mem/intune/apps/lob-apps-windows

Microsoft Docs 2020. Apply features and settings on your devices using device profiles in Microsoft Intune. Viitattu 28.11.2020. https://docs.microsoft.com/en-us/mem/intune/configuration/device-profiles

Microsoft Docs 2020. Overview of Windows as a service. Viitattu 21.11.2020. https://docs.microsoft.com/en-us/windows/deployment/update/waas-overview

Microsoft Docs 2020. Overview of Windows Autopilot. Viitattu 16.11.2020. https://docs.microsoft.com/en-us/mem/autopilot/windows-autopilot

Microsoft Docs 2020. Tutorial: Enable users to unlock their account or reset passwords using Azure Active Directory self-service password reset. Viitattu 13.11.2020. https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr

Microsoft Docs 2020. Use compliance policies to set rules for devices you manage with Intune. Viitattu 23.10.2020. https://docs.microsoft.com/en-us/mem/intune/protect/device-compliance-get-started

Microsoft Docs 2020. What is Microsoft Intune app management? Viitattu 26.11.2020. https://docs.microsoft.com/en-us/mem/intune/apps/app-management

NIST 2011. Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations. Viitattu 25.11.2020.

NIST 2018. An Introduction to the Components of the Framework. Viitattu 8.11.2020. https://www.nist.gov/cyberframework/online-learning/components-framework

Nousiainen, M. 2020. Pilvipalvelut 2020 – miten liiketoimintani hyötyy pilvipalveluista? Viitattu 10.11.2020. https://www.voicelink.fi/blogi/pilvipalvelut-2020-miten-liiketoimintani-hyotyy-pilvipalveluista/

SolarWinds 2019. NIST Cybersecurity Framework Overview. Viitattu 8.11.2020. https://www.solarwindsmsp.com/blog/nist-framework-cybersecurity

Sulava 2014. Mikä se Azure oikein on? Viitattu 14.11.2020. https://sulava.com/pilvi-infrastruktuuri/mika-se-azure-oikein/

SwanIT 2020. IT-alan hurjin palvelulupaus? Viitattu 11.10.2020. https://www.swanit.fi/

TeamViewer 2019. All about passwords. Viitattu 7.11.2020. https://community.teamviewer.com/t5/Knowledge-Base-EN/All-about-passwords/ta-p/28442#toc-hId-585378451

TeamViewer 2020. What is TeamViewer. Viitattu 7.11.2020. https://community.teamviewer.com/t5/Knowledge-Base-EN/What-is-TeamViewer-incl-video/ta-p/33184

Traficom 2020. Kyberturvallisuus ja yrityksen hallituksen vastuu. Viitattu 8.11.2020. https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/T_KyberHV_digiAUK_220120.pdf

Wallenius, N. 2020. Pilvipalvelut – 7 syytä miksi pilvestä on hyötyä liiketoiminnalle vuonna 2020. Viitattu 11.11.2020. https://niklaswallenius.fi/pilvi-hyoty-liiketoiminta/

ZumBrunnen, J. 2019. BitLocker and Windows 10 Pro protect your data. Viitattu 21.11.2020. https://community.windows.com/en-us/stories/what-is-bitlocker-windows-10

Kuviot