Mikko Kärkkäinen

YRITYKSEN KÄYTTÄJÄHALLINTA JA TIETOTURVA PILVIPALVELUNA

Tietojenkäsittelyn koulutusohjelma

2017

samk
Satakunnan ammattikorkeakoulu
Satakunta University of Applied Sciences

YRITYKSEN KÄYTTÄJÄHALLINTA JA TIETOTURVA PILVIPALVELUNA

Kärkkäinen, Mikko
Satakunnan ammattikorkeakoulu
Tietojenkäsittelyn koulutusohjelma
Joulukuu 2017
Ohjaaja: Nieminen, Hans
Sivumäärä: 32
Liitteitä: 0

Asiasanat: tiedonhallintajärjestelmät, pilvipalvelut, tietoturva

---

Opinnäytetyö suoritettiin Nuventur Oy:n toimeksiantona. Tämän opinnäytetyön tavoitteena oli selvittää pienille ja keskisuurille yrityksille sopivaa käyttäjähallintaa ja sen tekniseen ympäristöön liittyvää tietoturvaa pilvipalveluina. Työssä tutkittiin Microsoftin Office 365, Azure Active Directory ja Intune -palveluiden tarjoamia mahdollisuuksia. Kyseiset palvelut valittiin, koska ne ovat yleisesti käytössä monissa pk-yrityksissä ja pilvipalveluiden käytön määrä on lisääntynyt yrityksissä.

Työssä on ensin käsitelty tietoturvan ja pilvipalveluiden teoriaa, sekä lopuksi käytännön ratkaisujen ohjeistusta palveluiden toteutukseen. Opinnäytetyöni tarjoaa ratkaisuja Office 365 -ympäristön käyttöönottoon, käyttäjien lisäämisen aktiivihakemistoon sekä tietoturvallisen kokonaisuuden luomiseen ja ylläpitoon.

USER MANAGEMENT AND SECURITY AS A CLOUD SERVICE FOR ENTERPRISES

Kärkkäinen, Mikko
Satakunta University of Applied Sciences
Degree Programme in Business Information Systems
December 2017
Supervisor: Nieminen, Hans
Number of pages: 32
Appendices: 0

Keywords: user management, cloud computing, data protection

This thesis was made for Nuventur Oy. The purpose of this thesis was to investigate a cloud based user management and security solutions for small and middle-sized businesses. The study examined the possibilities offered by Microsoft Office 365, Azure Active Directory and Intune. These services were chosen because they are commonly used by many SMBs and the number of cloud services has increased in companies.

The thesis deals with the theory of information security and cloud services and finally guidelines for practical solutions for service implementation. My thesis offers solutions for Office 365 environments, adding users to the active directory and creating and maintaining security in this environment.

SISÄLLYS

1 JOHDANTO 5
2 YRITYSTEN ESITTELY 6
2.1 Nuventur Oy 6
2.2 Omafirma Oy 6
3 PILVIPALVELUT 7
3.1 Mitä käsitteellä tarkoitetaan? 7
3.2 Luokittelu 8
3.3 Jakelumallit 8
3.4 Hyödyt 9
3.5 Riskit ja huolenaiheet 10
4 TIETOTURVA 12
5 TYÖN TEKNINEN TOTEUTUS 13
5.1 Microsoft Office 365 13
5.2 Hinnoittelu 14
5.3 Palvelun käyttöönotto 14
5.3.1 Rekisteröinti ja toimialueeseen liittäminen 14
5.3.2 Käyttäjät ja ryhmät 16
5.3.3 Palveluiden lisääminen 18
5.4 Tietoturvaominaisuudet 19
5.4.1 Enterprise Mobility +Security 19
5.4.2 Intunen hallinta 20
5.4.3 Laitteiden hallinta 21
5.4.4 Sovellusten jakaminen 26
5.4.5 Office 365 Secure score 27
5.4.6 Cloud App Security 29
6 JOHTOPÄÄTÖKSET 30
LÄHTEET 32

1 JOHDANTO

Opinnäytetyön aiheena oli käyttäjähallinta ja tietoturva pilvipohjaisena palveluna pienille ja keskisuurille yrityksille. Opinnäytetyö toteutettiin Nuventur Oy:n toimeksiantona. Lähestyin Nuventur Oy:tä etsiessäni aihetta opinnäytetyölle ja heillä oli kiinnostusta ja tarvetta ottaa selvää erityisesti Microsoftin Office 365 ja Intune -palveluihin liittyvistä käyttäjähallinta- ja tietoturva-asetuksista.

Työtä varten luotiin kuvitteellinen yritys, Omafirma Oy, joka vastaa mahdollista Nuventur Oy:n asiakasta. Omafirma Oy:lle luotiin tarpeet, jotka toteutettiin Microsoftin Office 365 -pilvipalvelua hyväksi käyttäen. Erityistä huomiota käytettiin käyttäjähallintaan ja tietoturvaan, joissa käytettiin Microsoftin Enterprice Mobility +Security -pakettiin sisältyvää Intune-palvelua.

Työn tarkoituksena oli tehdä Omafirma Oy:lle käyttäjäystävällinen ja helposti lähestyttävä palvelu, joka kuitenkin takaa tietoturvallisen ympäristön. Tärkeää oli myös käyttää nykyaikaisia tekniikoita, jotka on toteutettu pilvipohjaisina ratkaisuina.

Työssä otettiin myös yleisesti kantaa pilvipalveluilla toteutettavan ratkaisun hyötyihin ja haittoihin sekä ratkaisujen tietoturvaan. Ratkaisussa oli tärkeää ottaa huomioon myös BYOD (Bring Your Own Device) -periaatteen, eli laitteistosta riippumattoman periaatteen mukainen lähestyminen.

Aluksi työssä käydään läpi pilvipalveluihin ja tietoturvaan liittyvää teoriaa ja sen jälkeen esitetään käytännön ratkaisuja ja asetusten määrittelyjä Microsoftin tuotteita käyttäen. Työn lopusta löytyy yhteenvetoa palveluista opittujen asioiden perusteella.

2 YRITYSTEN ESITTELY

2.1 Nuventur Oy

Lähestyin Nuventur Oy:tä, koska halusin tehdä nykyaikaiseen järjestelmänhallintaratkaisuun perustuvan opinnäytetyön. Nuventur Oy on vuonna 2007 perustettu laaja-alaisia ICT-palveluita tarjoava yritys. Yritys tarjoaa esimerkiksi asiakkailleen nimetyn vastuuhenkilön, joka voi johtaa asiakasyrityksen päivittäistä tietohallintoa. Hallintaan ja valvontaan yritys käyttää nykyaikaisia tietotekniikan työkaluja. Yrityksen asiakkaita ovat lähinnä pienet ja keskisuuret yritykset. Nuventur -nimi tulee sanoista ”New Venture” ja yrityksen toiminta-ajatuksena on turvata asiakkaan tulevaisuus turvaamalla heidän toimintansa. Opinnäytetyön kirjoitushetkellä yrityksessä työskenteli kuusi työntekijää. (Nuventurin www-sivut 2017.)

Nuventur Oy:llä oli tarpeena saada enemmän tietoa Microsoftin 365 ja Intune -tuotteiden sisältämistä ominaisuuksista ja niiden käyttämisestä palveluratkaisuissa omille asiakkailleen. Nykypäivänä asiakkaiden vaatimuksiin kuuluvat usein luotettava tietoturva ja erilaisten päätelaitteiden, kuten kannettavien, älypuhelimien ja tablettien yhteensopivuus. Nuventur Oy:llä minua ohjasi ja ohjeisti yrityksen varatoimitusjohtaja Otso Väisänen.

2.2 Omafirma Oy

Opinnäytetyö aloitettiin luomalla kuvitteellinen yritys, joka vastaa mahdollista Nuventur Oy:n asiakasta. Omafirma Oy:llä on kolmetoista työntekijää ja se toimii kansainvälisesti sekä Suomessa että Yhdysvalloissa. Yrityksen pääpaikkana toimii Suomessa Oulun toimipiste ja sillä on etätoimipisteet Helsingissä sekä Yhdysvalloissa New Yorkissa. Omafirma Oy on kodin turvalaitteisiin erikoistunut yritys, jolla on työntekijöinään myyjiä, laitteiston testaajia sekä johtajia. Heidän työntekijöillään on tarve käyttää tietoteknisiä ratkaisuja keskinäiseen kommunikointiin, asiakas- ja tuotetiedon tallentamiseen ja käsittelemiseen, sekä johtajilla työntekijöiden johtamiseen.

Työntekijöiden liikkumisen kannalta on tärkeää, että he pääsevät yrityksen järjestelmiin helposti paikasta ja laitteista riippumatta. Ratkaisussa painotettiin tietoturvaa, jotta yrityksen tiedot eivät pääsisi leviämään vääriin käsiin ja toiminta olisi mahdollisimman luotettavaa. Myös yrityksen laajenemismahdollisuudet oli otettava huomioon. Työntekijöiden ja palveluiden lisääminen ja poistaminen järjestelmästä tulisi olla helposti lähestyttävää.

3 PILVIPALVELUT

3.1 Mitä käsitteellä tarkoitetaan?

Käsitteelle pilvipalvelu (cloud computing) ei ole olemassa mitään yleistä määritelmää. Pilvi (cloud) käsitettä on käytetty internettiin viittaavana kielikuvana ja pilvipalveluilla on tarkoitettu eri tietotekniikkaresurssien muodostamia malleja, jotka tarjotaan käyttäjille verkon kautta. Tietotekniikkaresursseja ovat esimerkiksi sovellukset, palvelut, tallennuskapasiteetti ja tietoliikenneyhteydet. Käyttäjien ei välttämättä tarvitse tietää resurssien sijaintia tai vastata niiden ylläpidosta ja toiminnasta. (Salo 2012, 16.)

Pilvipalvelut voidaan usein ostaa internetistä luottokortilla. Pilvipalveluiden ominaisuutena on elastinen provisiointi, joka mahdollistaa joustavan ja usein myös automaattisen uusien asiakkaiden liittämisen sekä uusien palveluiden tarjoamisen. Myös käytön lopettaminen on tehty joustavaksi, koska palvelut tarjotaan yleensä kuukausi- tai vuosihinnoittelulla. Kaikki asiakkaat käyttävät mahdollisuuksien mukaan samaa multitenant -ympäristöä, jossa tietojenkäsittelykapasiteetti on yhteiskäytössä kaikkien käyttäjien/käyttäjäryhmien (tenants) kesken ja jossa data on käyttäjä/käyttäjäryhmä kohtainen. (Heino 2010, 40-42.)

Ominaista pilvipalveluille on myös riippumattomuus päätelaitteesta ja käyttöpaikasta. Käyttäjät tarvitsevat laitteeseensa usein vain verkkoyhteyden, jonka avulla pilvipalveluihin kirjaudutaan joko selaimen tai palvelua varten tehdyn sovelluksen avulla. Paikkariippumattomuus mahdollistaa työn tekemisen missä päin tahansa, kunhan otetaan huomioon maakohtaiset tietoliikenneyhteydet. (Heino 2010, 45-47.)

3.2 Luokittelu

Pilvipalvelumallit voidaan luokitella erilaisiin ryhmiin niiden ominaispiirteidensä mukaan. Tunnetuimmat ja yleisimmät ryhmistä ovat infrastruktuuri palveluna (IaaS), sovellusalusta palveluna (PaaS) ja sovellukset palveluna (SaaS). (Salo 2012, 20.)

Infrastructure as a service (IaaS) tarkoittaa sitä, että asiakas ostaa palveluna käyttöönsä palveluntarjoajan laitteiston resurssit, jotka käsittävät esimerkiksi tallennustilan, laskentatehon ja eri palveluita. Näissä palveluissa palveluntarjoajan ylläpito ja skaalautuminen ovat mahdollisimman automatisoituja ja resurssit pitkälti virtualisoituja. Kapasiteetin lisääminen ja vähentäminen on tehty joustavaksi aina tarpeen mukaan. Laskutus perustuu usein siihen, kuinka paljon resursseja käytetään. IaaS -palveluita voivat olla esimerkiksi virtuaalikoneet, virtuaaliset palomuurit tai virtuaalinen sisäverkko. (Salo 2012, 22-23.)

Platform as a service (PaaS) on palvelualusta, jonka päällä sovelluksia voidaan testata, kehittää ja ylläpitää. PaaS -ratkaisussa voidaan ottaa käyttöön esimerkiksi verkkosivuille tai tietokannalle luotu alusta. PaaS -palveluina voivat olla esimerkiksi tietokannat tai käyttöjärjestelmät. (Salo 2012, 24.)

Software as a service (SaaS) tarkoittaa sitä, että yritys tai yksityinen asiakas käyttää palveluntarjoajan sovelluksia tarpeensa mukaan. Asiakkaan ei tarvitse omistaa, asentaa tai ylläpitää sovellusta, vaan hän ostaa käyttöoikeuden sovelluksiin. SaaS -palveluna voi olla esimerkiksi tässä työssä käsitelty Microsoftin Office 365 -palvelu, jonka sovelluksia käytetään verkkoselaimen avulla. (Salo 2012, 26.)

3.3 Jakelumallit

Pilvipalvelut voidaan luokitella myös sen mukaan, kuka palvelua käyttää tai kuka sen omistaa. Kolme yleisintä mallia ovat yksityinen pilvipalvelu, julkinen pilvipalvelu ja hybridi pilvipalvelu. (Heino 2010, 54-57.)

Private cloud eli yksityinen pilvipalvelu on yrityksen tai julkisyhteisön omaan LAN-lähiverkkoon tai muulla tavalla toteutettuun, luotettavaan verkkoon käytetty pilvipalvelumalli. Tässä mallissa asiakas itse omistaa ja ylläpitää palvelukoneistoaan, sekä maksaa siihen liittyvät kustannukset. (Heino 2010, 55.)

Public cloud eli julkinen pilvipalvelu toteutetaan internet-yhteyden kautta. Asiakas saa jaetun ympäristön kapasiteettia, eikä asiakas välttämättä tarvitse omaan käyttöönsä pyhitettyä eli dedikoitua kapasiteettia tai laitteistoa. Julkisen pilvipalvelun tarjoaja vastaa koneistossa olevan laitteiston omistamiseen liittyvistä kustannuksista ja ylläpidosta. Asiakas maksaa itse palvelusta. (Heino 2010, 54-55.)

Hybrid cloud on toteutettu yhdistämällä julkinen ja yksityinen pilvipalvelu. Yrityksen yksityinen pilviympäristö yhdistetään palveluntarjoajan julkiseen pilvipalveluun internet-yhteyden kautta. Esimerkkinä hybridiratkaisusta voi olla pilviympäristö, johon on liitetty yrityksen omissa laitteissa toimiva aktiivihakemisto, pilvipohjainen aktiivihakemisto ja kolmannen osapuolen julkinen pilvipalvelu. (Heino 2010, 56.)

3.4 Hyödyt

Kuluttajakäyttäjillä monet pilviratkaisut ovat olleet käytössä jo pitkään ennen yrityskäyttäjiä. Esimerkiksi tiedostojen jako verkkopohjaisena, selainpohjaiset sähköpostipalvelut ja pilvipalveluna tarjottu tallennuskapasiteetti ovat olleet jo vuosia käytössä kuluttajilla. Myös yritysmaailmassa pilvipalveluiden käyttö on koko ajan lisääntynyt ja varsinkin useat pienet ja keskisuuret yritykset luopuvat konesaleistaan ja siirtyvät käyttämään pilvipalveluina tarjottavia vaihtoehtoja. Tällä säästetään kustannuksissa huomattavastikin, kun laitteet eivät vie yrityksen tiloissa sähköä ja samalla lisää ilmastoinnin, palvelinraudan ja tilan tarpeesta syntyviä kustannuksia. Pilvipalveluiden etuna on myös nopea käyttöönotto monissa palveluissa, sekä joustavuus yritysten tarpeisiin. Palveluista on tehty mahdollisimman helposti lähestyttäviä ja hallittavia. Myös väliaikaistarve tiettyyn palveluun tai sovellukseen on helpompi toteuttaa pilvipalvelun kautta, kuin lisäämällä kapasiteettia konesaliin. Myös henkilöstöresurssien pula ajaa yritykset usein käyttämään pilviratkaisuja. (Salo 2012, 34-35; Heino 2010, 189-190.)

IT:n teollistuminen on johtanut standardointiin ja tuotteistamiseen. Useat yritysten tarvitsemat sovellusratkaisut on koottu saman paketin alle ja yritys voi räätälöidä siitä itselleen sopivan kokonaisuuden. Pakettien hintakin perustuu usein sen mukaan, mitä sovelluksia yritys tarvitsee. Virtualisointi, automaatio ja rinnakkaislaskenta ovat myös lisänneet pilvipalveluiden kehittymistä ja tätä kautta suosiota. (Salo 2012, 35; Heino 2010, 202.)

Pilvipalveluiden suurena etuna on niiden saavutettavuus melkeinpä mistä päin maailmaa tahansa, mihin aikaan tahansa, mistä löytyy verkkoyhteys. Pilvipalvelut on usein luotu myös toimimaan useilla eri käyttöjärjestelmillä, kuten Windows, Ios tai Android. (Microsoftin Azure www-sivut 2017.)

Pilvipalveluiden suuren kysynnän vuoksi ICT-palveluyritykset pystyvät koko ajan kehittämään uusia kustannustehokkaita palvelumalleja ja tuotteita asiakkaidensa käyttöön. Tämä on tarkoittanut myös sitä, että kyseisten palveluyritysten on täytynyt muuttua laite- ja ohjelmistomyyjistä asiantuntijakumppaneiksi, jotka tarjoavat myymiensä palveluiden lisäksi niiden hallintaan ja käyttöönottoon liittyvää osaamista asiakkailleen. (Nuventurin www-sivut 2017.)

Tietoturvaan on luotu usein valmiita työkaluja, joten niitä käyttöönottamalla asiakas pääsee helpommalla kuin monissa on-premise -ratkaisuissa, joissa yritykset itse omistavat ja ylläpitävät fyysisiä palvelimiaan. Hyvät ohjelmointirajapinnat taas auttavat automatisoinnissa ja käskyttämisessä esimerkiksi skriptien avulla. (Anttila & Roine 2015, 30-31.)

3.5 Riskit ja huolenaiheet

Usein asiakkailla liittyy pilvipalveluihin myös erilaisia huolenaiheita. Palveluntarjoajat antavat tietoa palveluidensa teknisestä toteutuksesta varsin rajallisesti ja heidän omiin tiloihinsa ei juurikaan pääse tutustumaan. Asiakkaalla täytyy siis olla luottamusta palveluntarjoajan ratkaisuihin. Alan toimijat vastaavat kysymyksiin esimerkiksi erinäisten laatusertifikaattien avulla, joilla pyritään vakuuttamaan luottamusta asiakkailleen. (Salo 2012, 36-37.)

Asiakkaalla voi olla esim. dataan liittyviä huolia, kuten tietojen yksityisyys, saavutettavuus ja pysyvyys sekä muut tietosuojaan liittyvät asiat. Tietojen tulee olla suojassa ulkopuolisilta niin, että vain asiakas itse pääsee niitä käsittelemään. Lainsäädäntökin voi vaikuttaa esimerkiksi siihen, missä maassa palveluntarjoajan fyysiset konesalit sijaitsevat ja millä tavalla tieto on sinne tallennettu. Myös sopimusteknisiin asioihin liittyy huolia. Erityisesti yrityksien, mutta myös yksittäisten käyttäjien, olisi syytä lukea palveluiden käyttäjäehtoja ennen, kuin ottavat pilvipalveluratkaisuja käyttöönsä. Mitä kriittisempää toiminta on, sitä tarkemmin ehdoista tulisi olla tietoinen. Esimerkiksi pilvitallennuspalvelun käyttäminen ei tarkoita samaa kuin tiedostojen varmuuskopiointi. Pilvipalveluista löytyy usein erillinen pilvivarmuuskopiointi. Varsinkaan ilmaisissa palveluissa palveluntarjoajan vastuut eivät ole niin suuret kuin maksullisissa. Tietosuojalain tiukentamisesta johtuen asiakkaan kannattaa myös selvittää missä tiedot maantieteellisesti säilytetään, jotta niitä ei vastoin tietosuojapykäliä esimerkiksi siirretä EU-alueen ulkopuolelle. (Salo 2012, 36-45; Nuventurin www-sivut 2017.)

Myös suorituskykyyn liittyy riskejä. Palvelun täytyy olla luotettava ja suorituskyvyn tasaista. Palvelun yhteyksien katkeaminen tai muu tekninen häiriötoiminta voivat aiheuttaa asiakkaille päänvaivaa. Vikatilanteissa palveluntarjoajille onkin tärkeää tiedottaa asiakkaitaan ja saada viat korjattua mahdollisimman nopeasti. (Salo 2012, 36-37.)

Verkkoyhteydet ylipäätään ovat ratkaisevassa asemassa pilvipalveluissa. Mitä kauempana data fyysisesti sijaitsee, sen alttiimpaa se on yhteyksien mukana tuomille ongelmille. Saavutettavuuden kannalta on myös usein ongelmallista, kuinka palvelu pystyy toimintaympäristöön tulevista muutoksista huolimatta tarjoamaan tasaista palvelua. Mikään pilvipalvelu ei ole täysin varma, kuten ei myöskään yrityksen omaan konesaliin tehty järjestelmä. Esimerkiksi Microsoft lupaa maksullisille Office 365 -palveluille 99,9 prosenttisen käytettävyysajan (uptime). (Salo 2012, 40; Microsoftin Office Products www-sivut 2017a.)

4 TIETOTURVA

Yleinen määritelmä tietoturvalle on tiedon eheyden, luottamuksellisuuden ja käytettävyyden turvaaminen. Tietoturvaa toteutetaan yrityksissä teknisten ja hallinnollisten toimien kautta. Usein tietosuoja ja tietoturva sekoitetaan keskenään. Tietosuojalla tarkoitetaan yksityisyyden ja ihmisten tiedollisen itsemääräämisen suojaamista, kun taas tietoturva tarjoaa ratkaisuja ja toimintamalleja tietosuojan ylläpitämiseen. Jo lainsäädäntö määrittelee pitkälti tietosuojaa koskevia asioita ja tietoturvan avulla tätä tietoa pyritään pitämään suojassa. (Laaksonen, Nevasalo & Tomula 2006, 17.)

Tekniikan kehittyessä koko ajan myös lainsäädäntöön on jouduttu tekemään muutoksia liittyen tietosuojaan. EU:n tietosuoja-asetus GDPR (General Data Protection Regulation) luotiin vuonna 2016 ja sen säädökset tulevat voimaan vuoden 2018 toukokuusta alkaen. Myös tämä on saanut pilvipalveluiden tarjoajat muuttamaan palveluitaan.

Esimerkiksi Microsoft on ottanut tuotteidensa tietoturvassa huomioon uuden tietosuoja-asetuksen tuomat muutokset. Käyttäjien on päästävä käsiksi henkilökohtaiseen dataansa tarvittaessa muuttaakseen tai poistaakseen tietoa. Yritysten täytyy suojata käyttäjien henkilökohtaista tietoa koskevat asiat oikeaoppisesti ja ilmoittaa asiakkailleen ja työntekijöilleen, että mitä tietoa heistä kerätään. GDPR sisältää useita sivuja muitakin säädöksiä, jotka yritysten tulee ottaa huomioon tietojärjestelmissään. (Microsoftin www-sivut 2017a.)

Microsoftin maksullisiin Office 365 -palveluihin on määritelty jo lähtökohtaisesti tietoturvaa lisääviä asioita. Ainoastaan valtuutetut työntekijät pääsevät heidän palvelinkeskuksiin ja tiedot on turvattu monella eri tasolla fyysisesti esimerkiksi kuluvalvonnan, liiketunnistimien, videokameravalvonnan ja hälytyslaitteiston avulla. Palvelun käyttäjien tietoja ei käytetä mainostarkoituksiin, eikä louhintaan, ainoastaan palvelun toimittamiseen. Myöskään asiakkaiden sähköpostilaatikkoja ei tarkkailla. (Microsoftin Office Products www-sivut 2017b.)

Tietoturva lähtee jo laitteistosta ja laiteohjelmistosta. Microsoft määrittelee verkkosivuillaan Windows 10 -käyttöjärjestelmää koskevat tietoturvastandardit, jotka on määritelty sekä rauta- että laiteohjelmistopuolelle. Suorittimeksi Microsoft suosittelee Intelin tai AMD:n seitsemännen sukupolven tai sitä uudempia, 64-bittisiä ratkaisuja tukevia suorittimia. Muistin määräksi suositellaan vähintään kahdeksaa gigatavua. Järjestelmän laiteohjelmiston tulisi käyttää esimerkiksi Unified Extension Firmware Interface (UEFI) versiota 2.4 tai uudempaa ja UEFI-luokkaa 2 tai 3. UEFI määrittelee rajapintamallin päätelaitteen käyttöjärjestelmän ja laiteohjelmiston välille. (Microsoftin Docs www-sivut 2017a; UEFI:n www-sivut 2017.)

5 TYÖN TEKNINEN TOTEUTUS

5.1 Microsoft Office 365

Omafirma Oy:n vaatimuksia varten valittiin käytettäväksi Microsoftin Office 365 -ratkaisu. Microsoftin tuotteet ovat useille pk-yrityksille tuttuja jo on-premise -ratkaisuina, joten ne ovat helposti lähestyttäviä ja yritysten työntekijöillä on usein kokemusta niiden käytöstä jo etukäteen. Työ aloitettiin ottamalla käyttöön kokeilujakso Office 365 Business Premium -paketista, joka löytyy Microsoftin verkkosivuilta. Kyseinen paketti valittiin, koska se sisältää laajan valikoiman eri palveluita. Osaa Microsoftin tuotteista pystyy kokeilemaan rajoitetun ajan ja myöhemmin niiden käyttöä voi jatkaa ostamalla ne käyttöönsä.

Office 365 on palvelupaketteihin pohjautuva ratkaisu, joka sisältävää mm. Office-sovellukset ja muita internetin avulla käytettäviä pilvipalveluita. Office 365 -ratkaisuja on mahdollista saada sekä yritys- että kotikäyttöön. Opinnäytetyössä käytetty Office Business Premium -paketti sisältää kyseiset päätelaitteisiin asennettavat sovellukset: Outlook, Word, Excel, Powerpoint, OneNote ja Access, sekä seuraavat palvelut: Exchange, OneDrive, SharePoint, Skype for Business, Microsoft Teams ja Yammer. Microsoftin tarjoamien palveluiden ja pakettien sisältö ja hinnat muuttuvat aika tiheään tahtiin, joten sen kummemmin tässä opinnäytetyössä ei oteta kantaa siihen, minkä paketin yrityksen kannattaa ottaa käyttöönsä. Yrityksen koko ja eri sovellusten tarve

vaihtelee usein. Business Premium -paketti valittiin tähän opinnäytetyöhön, koska se on laajuudeltaan kattavin pk-yrityksille tarkoitetuista paketeista.

5.2 Hinnoittelu

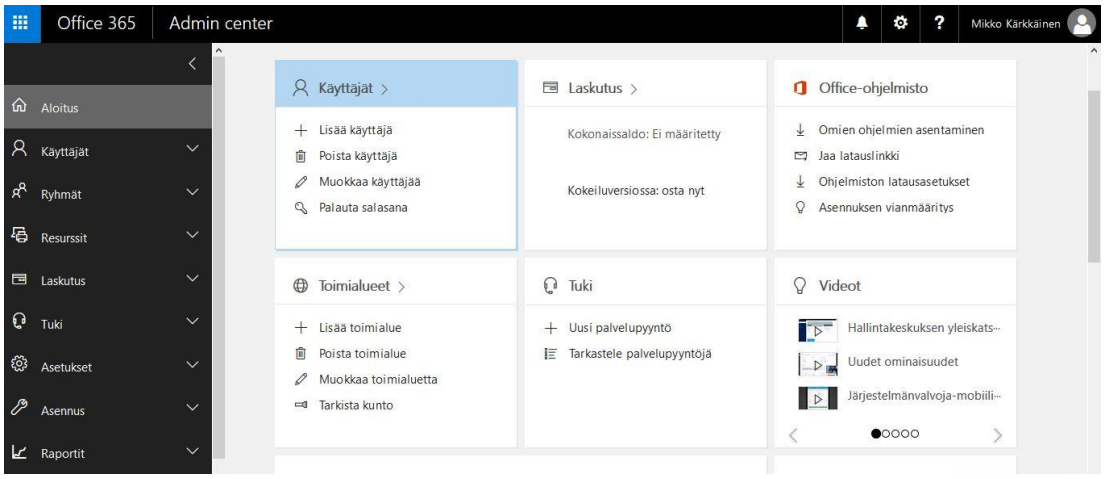
Hinnoittelu on määritelty käyttäjäkohtaiseksi. Jokaista palvelua tai palvelupakettia käyttävää henkilöä kohden tulee tietyn suuruinen kuukausi- tai vuosimaksu. Palveluista on saatavana useita erilaisia ratkaisuja ja yritys voikin katsoa itselleen sopivat paketit. Hinnoittelu määräytyy aina sen mukaan, mitä palveluita mikäkin paketti sisältää. Microsoftin myymien pakettien sisällöt vaihtuvat aika nopeaan tahtiin ja uusia palveluita tulee saataville koko ajan lisään.

5.3 Palvelun käyttöönotto

5.3.1 Rekisteröinti ja toimialueeseen liittäminen

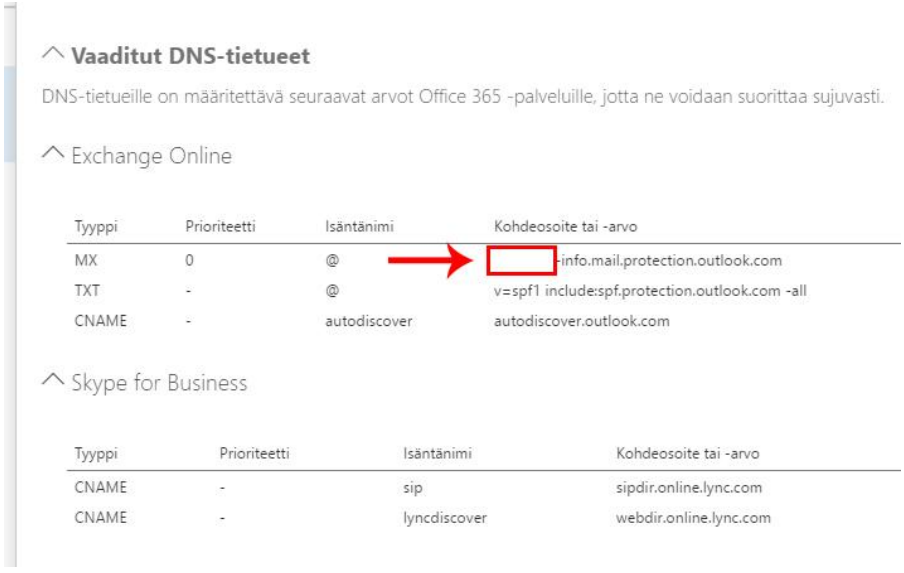
Kun tuote Office 365 Business Premium on valittu Microsoftin sivuilta, voidaan siirtyä rekisteröimään tuotetta. Tuotteen rekisteröivä henkilö asetetaan automaattisesti myös palvelun järjestelmänvalvojaksi, joka pystyy hallinnoimaan käyttäjiä, lisenssejä ja tilejä. Kyseinen järjestelmänvalvoja voi myöhemmin antaa myös muille käyttäjille järjestelmänvalvojan oikeuksia. Tässä opinnäytetyössä rekisteröin tuotteen itselleni ja Omafirma Oy:n tuotetta käyttäväksi yritykseksi. Käyttäjätunnus luotiin sähköpostiosoitteella: *mikko.karkkainen@omafirmaoy.onmicrosoft.com*, joka samalla toimii järjestelmänvalvojan kirjautumistunnuksena. Kirjautuminen hallintaportaaliin ja muihin palveluihin tapahtuu osoitteessa: *https://login.microsoftonline.com/*.

Kun valittu paketti on otettu käyttöön ja tuote rekisteröity tunnuksille, palvelu ilmoittaa kestoksi n. 30 – 60 minuuttia, että palvelu on täysin käyttökunnossa. Valitaan aloitussivulta **Hallinta** -painike, joka vie Officen Admin centerin aloitussivulle eli hallintaportaaliin, jonka alkunäkymä on esitetty kuvassa 1.



Kuva 1. Office 365 Admin Center

Alkuun on syytä lisätä palvelu omaan toimialueeseen, mikäli sellainen yritykseltä löytyy. Lisääminen tapahtuu vasemman navigointi-palkin kohdasta **Asennus > Toimialueet**. Valitaan **lisää toimialue** ja lisätään oma toimialue. DNS (Domain Name System) -tietueet voidaan määrittää automaattisesti tai tarvittaessa manuaalisesti, kun käytetään omia DNS-asetuksia. DNS eli nimipalvelujärjestelmä muuntaa verkkotunnukset IP-osoitteiksi. DNS-tietueita asetettaessa on syytä ottaa huomioon MX-tietue, johon lisätään oman toimialueen etuliite, kuten kuvassa 2 on esillä. (Microsoftin Office Support www-sivut 2017.)

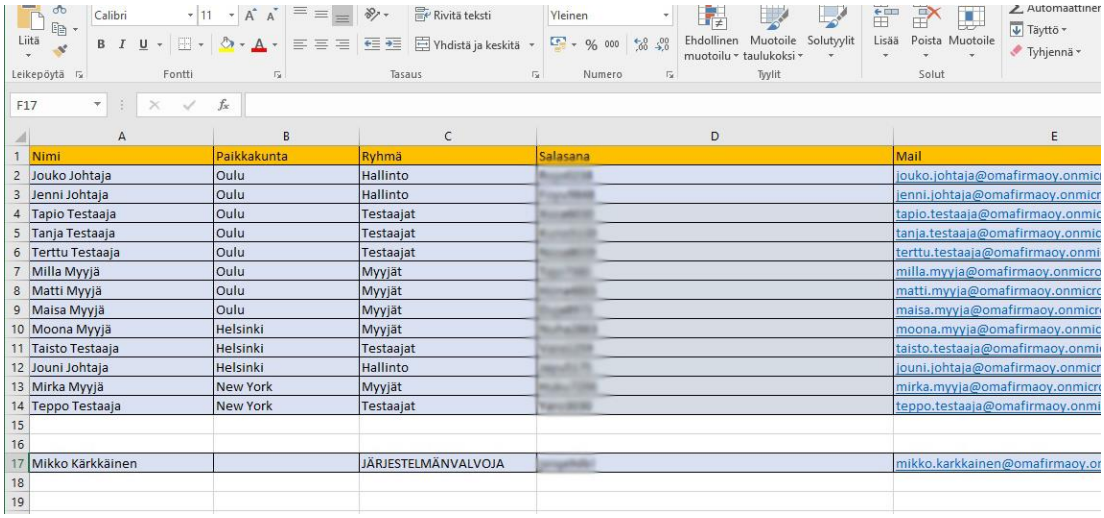


Kuva 2. MX-tietue

Opinnäytetyössä käytettiin Microsoftin automaattisesti luomaa ”omafirmaoy.onmicrosoft.com” -toimialuetta, joten MX-tietuetta ei tarvinnut muuttaa, vaan asetukset olivat automaattisesti oikein. MX-tietueet ohjaavat sähköpostiliikennettä haluttuihin palveluihin, joihin sähköpostin verkkotunnus on liitetty. Jos haluttaisiin käyttää yrityksen omaa toimialuetta, niin Office 365 -palvelu neuvoo, mitä käyttäjän tulee tehdä, jotta toimialue saataisiin käyttöön. Hallintaportaalista valitaan **Toimialueet > Lisää toimialue**. Kirjoitetaan oman toimialueen nimi ja siirrytään kohtaan **Tarkista toimialue**. Täältä löytyvät ohjeet tietueen lisäämiseen toimialueen tarkistamisessa. Kopioidaan MS = msXXXXXXXX arvo ja seurataan ohjeita. Luodaan TXT tai MX-tietue DNS-isännöintipalvelussa ohjeiden mukaan ja lopuksi vahvistetaan toimialue Office 365:ssa.

5.3.2 Käyttäjät ja ryhmät

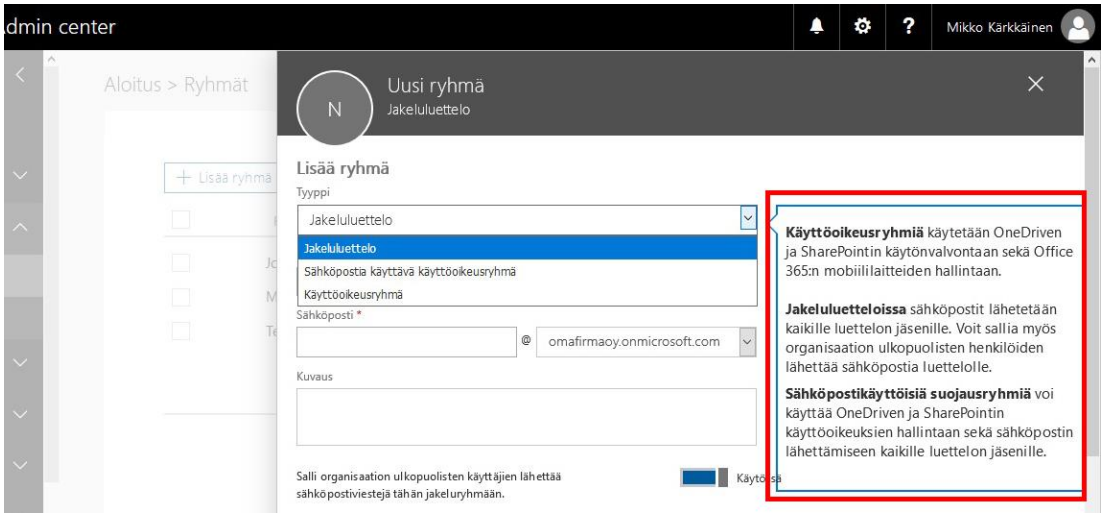
Seuraavaksi lisättiin Omafirma Oy:n työntekijät palveluun kohdasta **Käyttäjät** > **Aktiiviset käyttäjät** > **Lisää käyttäjä**. Lisätyt käyttäjät siirtyvät Azuren aktiivihakemistoon (Azure Active Directory), joka hallitsee muun muassa käyttäjien tunnistusta, kirjautumista ja rekisteröityjä laitteita. Käyttäjän nimen lisäksi myös muut yhteystiedot kannattaa lisätä, jotta ne ovat muille työtekijöille helposti löydettävissä. Puhelinnumeron lisääminen auttaa myöhemmin myös monimenetelmäisen todentamisen käyttöönotossa. Salasanan voi luoda itse, tai antaa palvelun luoda salasana, jonka käyttäjä voi muuttaa ensimmäisellä sisäänkirjautumiskerrallaan. Jos antaa palvelun luoda salasanan, niin se kannattaa ottaa talteen viimeisessä vaiheessa. Salasanan voi myöhemmin halutessaan palauttaa alkuperäiseksi järjestelmänvalvojan roolissa. Kenelle tahansa käyttäjälle voi myös samasta valikosta antaa rooleja, kuten esimerkiksi järjestelmänvalvojan rooli. Järjestelmänvalvojan rooleja on eritasoisia riippuen siitä, miten niitä yrityksessä halutaan myöntää. Opinnäytetyössä yleisenä järjestelmänvalvojana oli ainoastaan alkuperäinen käyttäjä *mikko.karkkainen@omafirmaoy.onmicrosoft.com*. Kuvassa 3 on esitetty Omafirma Oy:n työntekijät, jotka lisättiin palveluun. Excel-taulukko on hyvä apukeino, kun käyttäjiä lisätään palveluun.



	A	B	C	D	E
1	Nimi	Paikkakunta	Ryhmä	Salasana	Mail
2	Jouko Johtaja	Oulu	Hallinto		jouko.johtaja@omafirmaoy.onmic
3	Jenni Johtaja	Oulu	Hallinto		jenni.johtaja@omafirmaoy.onmicr
4	Tapio Testaaja	Oulu	Testaajat		tapio.testaaja@omafirmaoy.onmic
5	Tanja Testaaja	Oulu	Testaajat		tanja.testaaja@omafirmaoy.onmic
6	Terttu Testaaja	Oulu	Testaajat		terttu.testaaja@omafirmaoy.onmi
7	Milla Myyjä	Oulu	Myyjät		milla.myyja@omafirmaoy.onmicro
8	Matti Myyjä	Oulu	Myyjät		matti.myyja@omafirmaoy.onmicro
9	Maisa Myyjä	Oulu	Myyjät		maisa.myyja@omafirmaoy.onmicr
10	Moona Myyjä	Helsinki	Myyjät		moona.myyja@omafirmaoy.onmic
11	Taisto Testaaja	Helsinki	Testaajat		taisto.testaaja@omafirmaoy.onmi
12	Jouni Johtaja	Helsinki	Hallinto		jouni.johtaja@omafirmaoy.onmicr
13	Mirka Myyjä	New York	Myyjät		mirka.myyja@omafirmaoy.onmicr
14	Teppo Testaaja	New York	Testaajat		teppo.testaaja@omafirmaoy.onmi
15					
16					
17	Mikko Kärkkäinen		JÄRJESTELMÄNVALVOJA		mikko.karkkainen@omafirmaoy.or
18					
19					

Kuva 3. Excel-taulukko käyttäjistä

Kun käyttäjät on lisätty, voidaan luoda ryhmiä, joihin käyttäjät lisätään. Ryhmät luodaan vasemman sivun valikosta valitsemalla **Ryhmät** ja avautuvalta sivulta **Lisää ryhmä**. Ryhmiä voivat olla esimerkiksi myyjät, testaajat, johtajat jne. Ryhmille voidaan myöhemmin määritellä erilaisia käyttäjäoikeuksia ja yksi henkilö voi olla useammankin ryhmän jäsen. Ryhmiä voi olla kolmea eri tyyppiä, jotka on esitetty kuvassa 4.



Kuva 4. Ryhmien tyypit

Tässä työssä luotiin kolme sähköpostia käyttävää käyttöoikeusryhmää: Johtajat, Myynti ja Testaajat. Kyseinen ryhmätyyppi valittiin, jotta pystyttiin valvomaan ja hallitsemaan kyseisten ryhmien jäsenten käyttämiä mobiililaitteita. Ryhmien luomisessa

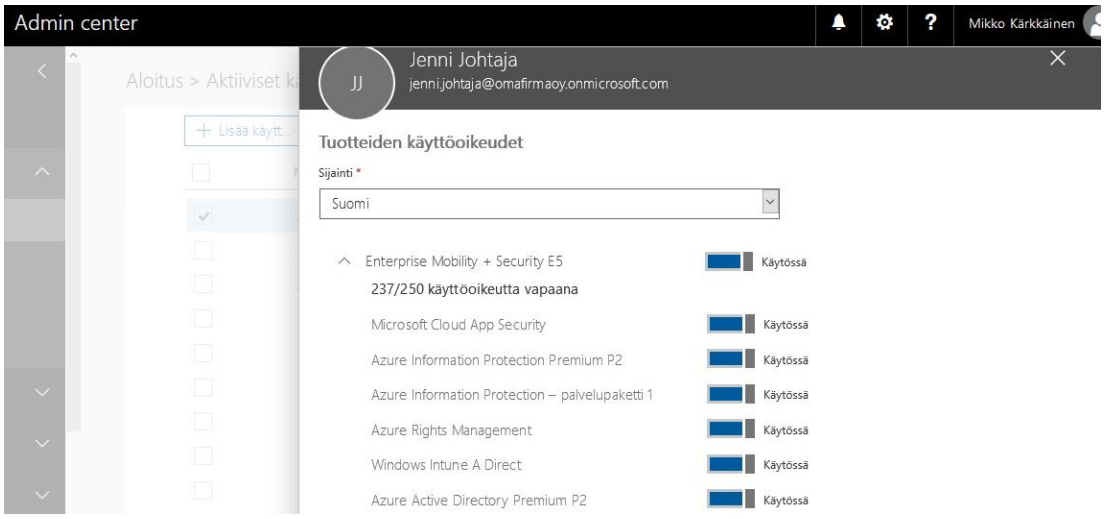
kestää aina muutamia minuutteja ennen kuin ne tulevat näkyviin, koska ryhmät linkittyvät Azure AD:n kautta moniin eri sovelluksiin.

Valitsemalla tietty käyttäjä voidaan muuttaa esimerkiksi käyttäjän kirjautumistilaa estämällä kirjautuminen. Tämä on kätevää, jos vaikka käyttäjän laite tai tunnukset sattuvat joutumaan vääriin käsiin. Käyttäjäkohtaisesta valikosta voidaan milloin tahansa määritellä myös mm. sähköpostiin ja Onedriveen liittyviä asetuksia sekä käyttäjän rooleja ja ryhmien jäsenyyksiä. Käyttäjille on syytä määrittää ainakin pääasiallinen maantieteellinen sijainti, missä työntekijä työskentelee. Tämä vaikuttaa tiettyjen tietoturvaominaisuuksien käyttöön myöhemmässä vaiheessa.

Samalla kun käyttäjät lisätään hallintaportaalin kautta, niin ne myös automaattisesti liittyvät Azure Active Directoryn (Azure AD) käyttäjiksi. Azure AD:n tarjoamat hakemisto- ja tunnistautumispalvelut helpottavat mm. monimenetelmäisen todentamisen ja kertakirjautumisen (single sign-on) mahdollisuuksia. Myös tietoturvaan ja kirjautumisiin liittyviä raportteja on helpompi seurata pilvipalveluna tarjottavan aktiivihakemiston kautta. (Anttila & Roine 2015, 38.)

5.3.3 Palveluiden lisääminen

Seuraavaksi valittiin yritykselle halutut palvelut valikosta: **Laskutus** > **Osta palveluita**. Täältä otettiin käyttöön kokeilujaksot palveluista: Office 365 Business Premium ja Enterprise Mobility + Security E5 Trial. Tietoturvaominaisuuksia lisäävään Enterprise Mobility + Security -pakettiin palataan myöhemmin työn aikana. Ostetut palvelut lisätään käyttäjille kohdassa: **Laskutus** > **Tilaukset**. Valitaan ostettu palvelu ja valitaan **Määritä käyttäjille**, jonka jälkeen valitaan halutut käyttäjät ja lisätään heille tuotteiden käyttöoikeudet. Käyttäjille voidaan helposti antaa eri tuotteiden käyttöoikeuksia ja myöskin tarvittaessa poistaa niitä käytöstä. Kuva 5 havainnollistaa lisenssien hallintaa.



Kuva 5. Lisenssien käyttöoikeudet

Järjestelmänvalvojalle ei ole pakko antaa käyttöoikeuksia sovelluksiin tai palveluihin, jos hän ei niitä käytä, kuten tässä opinnäytetyössä tehtiin. Järjestelmänvalvojana tässä työssä oli Nuventur Oy:n työntekijä ja Omafirma Oy kuvitteellisesti osti palvelun Nuventurilta. Nuventur Oy siis hallinnoi palveluita, joita Omafirma Oy käyttää. Kun käyttäjille on annettu oikeus sovelluksiin ja palveluihin, niin ne ovat valmiita käytettäviksi. Useat sovellukset ja palvelut kuitenkin vaativat järjestelmänvalvojalta konfigurointia, jotta ne olisivat tietoturvallisia ja muutenkin käyttäjäystävällisempiä.

5.4 Tietoturvaominaisuudet

5.4.1 Enterprise Mobility +Security

Enterprice Mobility +Security (EMS) on Microsoftin käyttäjäpohjaista lisäsuojausta tarjoava paketti, joka laajimmillaan sisältää Intunen, Azure AD Premiumin ja Azure Information Protectionin, Advanced Threat Analyticsin ja Cloud App Securityn. Tässä opinnäytetyössä käsiteltiin tarkemmin lähinnä Intunen ominaisuuksia, mutta muistakin EMS:n sisältämistä palveluista voi saada lisää tietoturvaa yrityksen toimintaan. (Microsoftin www-sivut 2017b.)

Azure Information Protection auttaa yrityksiä luokittelemaan ja suojaamaan dokumentteja ja sähköposteja joko järjestelmänvalvojan määrittelemillä ehdoilla tai manuaalisesti käyttäjien toimesta. Tiedostoja voidaan suojata riippumatta siitä, mihin ne on

tallennettu tai kenen kanssa niiden käyttöä on jaettu. Tiedostoihin voidaan myöntää lukuoikeuksia, mutta esimerkiksi tiedostojen muokkaaminen tai tulostaminen voidaan estää. (Microsoftin Docs www-sivut 2017b.)

Advanced Threat Analytics (ATA) on on-premise -pohjainen alusta, joka auttaa seuraamaan tietoturvaan liittyviä uhkia yrityksen verkossa. ATA ilmoittaa poikkeamista ja ehdottaa tarvittavia toimia niiden ehkäisemiseksi. ATA analysoi tiedon kulkua ja oppii normaalin ja epänormaalin toiminnan tunnistamiseen. (Microsoftin Docs www-sivut 2017c.)

Cloud App Security auttaa löytämään ja selvittämään pilvipohjaisina käytettyjen sovellusten riskejä. Sovelluksien toimintaa voidaan hallita ja rajoittaa tiettyjen ehtojen mukaisesti. Näitä ehtoja voidaan määritellä esimerkiksi käyttäjän, laitteen tai sijainnin mukaan. Cloud App Securityn käytöstä on selitetty tarkemmin myöhemmin opinnäytetyössä. (Microsoftin Docs www-sivut 2017d.)

Opinnäytetyötä varten otettiin käyttöön EMS E5 Trial, jonka sai koekäyttöön n. neljän kuukauden ajaksi. Paketista on olemassa myös E3-versio, josta on karsittu tiettyjä ominaisuuksia. Jokaiselle käyttäjälle asetettiin kaikki E5-paketin palvelut käyttöön.

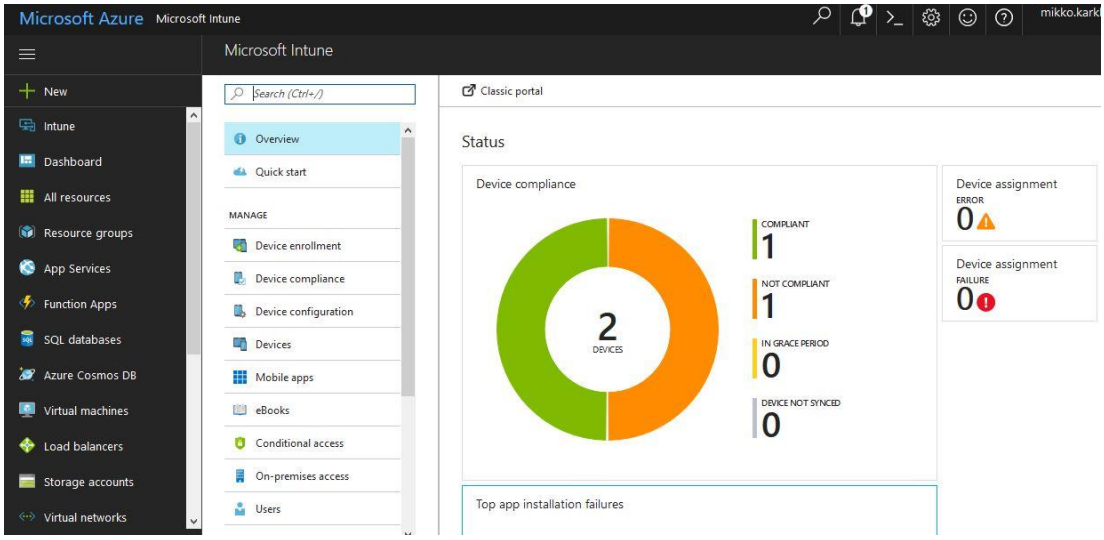
5.4.2 Intunen hallinta

Intunen avulla saadaan lisää tietoturvaa yrityksen toimiin päätelaitehallinnan avulla. Intune sisältää useita määritettäviä toimintoja ja antaa monia erilaisia ominaisuuksia yrityksen käyttöön. Se antaa esimerkiksi mahdollisuuden laitteiden kirjaamiseen (enroll) yrityksen järjestelmään sekä kirjattujen laitteiden hallintaan. Käyttäjien laitteisiin sisäänkirjautumisia pystytään myös tarkastelemaan ja rajoittamaan Intunen avulla. (Microsoftin Docs www-sivut 2017e.)

Intune sisältää MDM:n (Mobile Device Management), joka mahdollistaa laitehallinnan. On-premise -ympäristön Configuration Manager toimii MDM:n rinnalla tarvittaessa Hybrid MDM -muodossa. Pelkästään Microsoftin MDM:n dokumentaatio on yli 3000 sivua pitkä, joten asetuksia löytyy todella paljon. Configuration Managerin

Group Policy:t on pyritty korvaamaan MDM:n tarjoamilla mahdollisuuksilla, mutta molemmista löytyy ominaisuuksia mitä toisesta ei löydy. Normaalin pk-yrityksen pilviympäristön luomisessa läheskään kaikkia asetuksia ei tarvitse säätää erikseen, vaan asetukset voidaan tehdä tapauskohtaisesti yrityksen tarpeita vastaaviksi. (Microsoftin Docs www-sivut 2017e.)

Järjestelmänvalvoja pääsee Intunen hallintavalikkoon valitsemalla hallintaportaalin vasemmasta alareunasta **Hallintakeskukset** > **Intune**. Hallinta tapahtuu englanninkielisen Azure-portaalin ympäristössä. Kuvassa 6 on esitetty Intunen hallintavalikon päänäkymä.

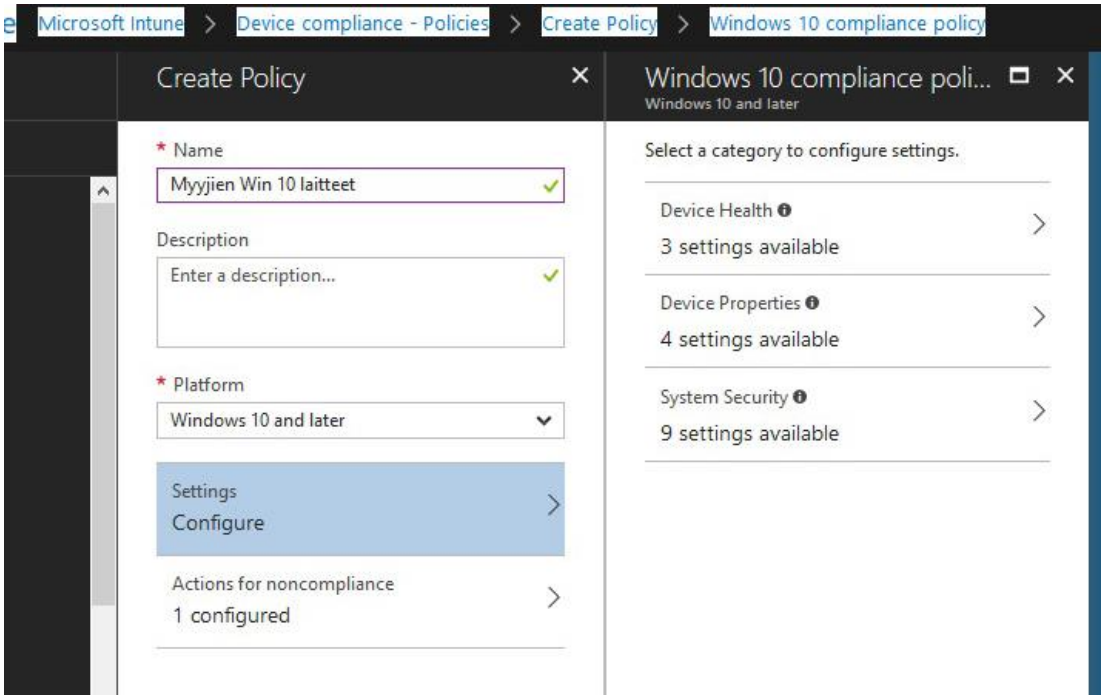


Kuva 6. Intunen hallintavalikko

5.4.3 Laitteiden hallinta

Käyttäjien työpaikan ja henkilökohtaisetkin päätelaitteet voidaan kirjata (enroll) yrityksen portaaliin sekä Azure AD:n että Intunen alaisuuteen. Laitteiden käyttöjärjestelmistä tuetaan ainakin iOS, macOS, Windows 8.1 (ja uudemmat) sekä Android. Suurta osaa Intunen ominaisuuksista voidaan hallita hallintakeskuksen kautta, mutta joissain tapauksissa on ainakin toistaiseksi käytettävä Intunen omaa, vanhaa portaalia: *https://admin.manage.microsoft.com*. Microsoft on hiljalleen siirtänyt ominaisuuksia vanhasta hallintaportaalista uuteen Azure-portaaliin, jotta kaikkia sovelluksia hallittaisiin tulevaisuudessa sitä kautta. (Microsoftin Docs www-sivut 2017e.)

Aluksi asetetaan käytännöt (policy), jonka mukaan käyttäjät tai järjestelmänvalvoja voivat laitteita kirjata. Esimerkkinä käytetään Moona Myyjää, joka käyttää omaa konettaan työn tekemiseen. Myös yritys voisi kirjata yritykselle kuuluvat koneet, mutta esimerkissä käytettiin BYOD-periaatteen mukaista toimintaa. Käytäntöjen määrittely aloitetaan menemällä Azuren Intune portaaliin ja valitaan **Device compliance** > **Policies** > **Create policy**. Valitaan haluttu alusta (platform) ja muut laitteeseen liittyvät tiedot kuten Kuvassa 7.



Kuva 7. Käytännöt laitteiden kirjaamiseen

Tässä tapauksessa laitettiin Windows 10 mobiililaitteiden kirjaaminen sallituksi Myynti -ryhmälle valitsemalla luotu käytäntö ja sen jälkeen **Assignments** > **Include** > **Select groups to include** > **Myynti**. Käytäntöjä pystyy ainoastaan lisäämään ryhmille, ei suoraan yksittäisille käyttäjille. Seuraavaksi käyttäjä kirjautuu omaan Windows 10 -käyttöjärjestelmän sisältävään tietokoneeseen Omafirma Oy:n hänelle luoduilla tunnuksilla. Käyttäjän tulee olla laitteen paikallinen admin eli järjestelmänvalvoja. Heti kirjauduttuaan koneelleen firmansa tunnuksilla Intune ottaa automaattisesti käyttöön Windows Hello -palvelun, joka vaatii mobiililaitteeseen tai tietokoneeseen monimenetelmäisen kirjautumisen, kun yrityksen tunnuksilla kirjaudutaan koneeseen. Tämä tarkoittaa joko sormenjälkitunnistusta tai puhelimeen tekstiviestillä tai soitolla saatavaa kertakäyttöistä koodia. Kun koodi on kertaalleen asetettu, käyttäjä

voi asettaa pin-koodin myöhempää käyttöä varten. Windows Hellon voi halutessaan ottaa pois käytöstä jo aikaisemmin yritykselle kirjatuista koneista, kirjautumalla järjestyksenvalvojana osoitteeseen: https://admin.manage.microsoft.com. Käytetyn selaimen tulee olla riittävän uusi versio jostain tunnetuimmista selaimista. Valitaan **Järjestelmänvalvoja** > **Mobiililaitteiden hallinta** > **Windows** > **Windows Hello yrityksille** > valitaan **Poista Windows Hello yrityksille käytöstä**.

Kun käyttäjä on kirjautunut tietokoneeseen, voidaan kone kirjata yritykselle. Yritys pystyy seuraamaan tiettyjä asioita, kun se on kirjattu. Kuvassa 8 näkyy mitä tietoja yritys näkee ja mitä se ei näe.

What IT cannot see	What IT can see
Calling and web browsing history	Model
Location	Serial number
Personal email	Operating system version
Text messages	App names
Contacts	Owner
Passwords to your personal accounts	Device name
Calendar events	Manufacturer (for devices not made by Apple)
Pictures, including what's in the photos app or camera roll	Phone number (for work devices, the whole number. For personal devices, just the last four digits.)

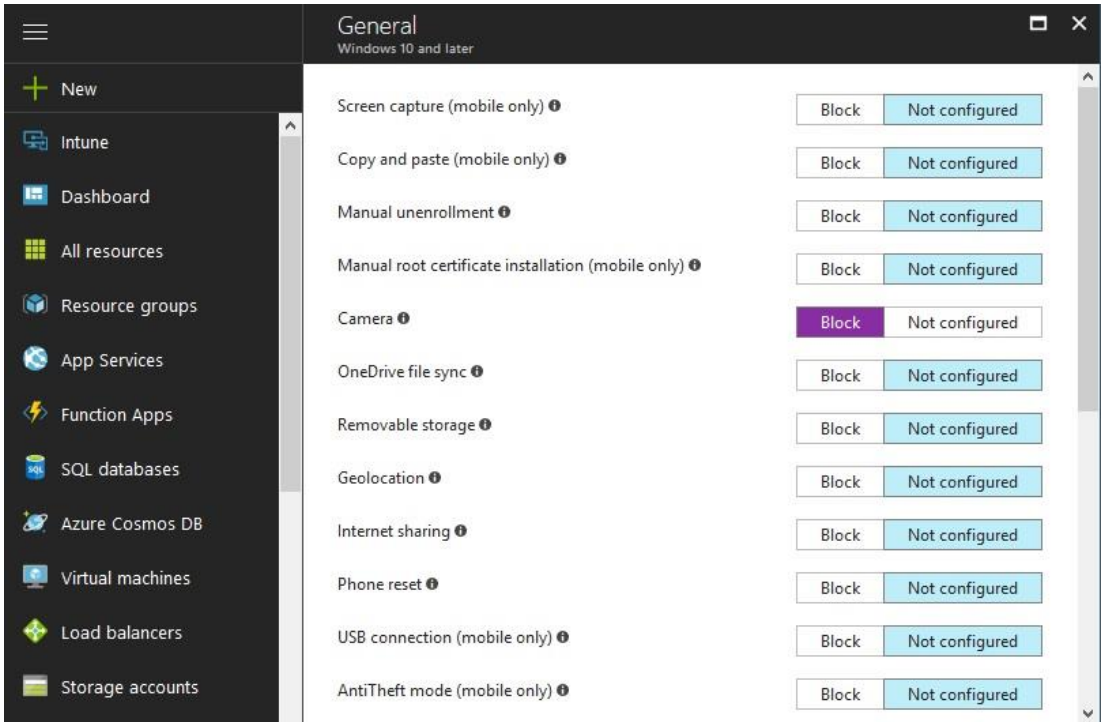
Kuva 8. Yritykselle välittyvät asiat kirjatusta laitteesta

Windows-laitteilla käyttäjä asentaa Microsoft Store -kaupasta löytyvän Yritysportaalin (Intune Company Portal). Kun ohjelma on asennettu, se avataan ja käyttäjä kirjautuu tunnuksillaan siihen. Ohjelma auttaa portaittain käyttäjän kirjaamaan koneensa yrityksen järjestelmään.

Kirjaus voidaan säätää myös automaattiseksi, jos kone kirjataan yrityksen Azure AD:hen. Azuren hallintaportaalista valitaan: **Azure Active Directory** > **Mobility (MDM and MAM)** > **Microsoft Intune** > **MDM user scope ALL**.

Jos yritys ei salli käyttäjille omien koneidensa käyttämistä työntekoon, se voi kirjata työpaikan koneet itse ja asettaa niihin haluttuja rajoitteita. Käyttäjien tietotekniset taidot on hyvä ottaa huomioon, kun päätetään, millainen kanta työntekijöiden omien koneiden käyttöön työtehtävissä otetaan. Ohjeistus laitteiden kirjaamiseen on myös syytä olla kunnossa.

Yritys voi vaikuttaa yrityksille kirjattujen laitteiden asetuksiin. Intunen avulla laitteista voidaan tehdä tietoturvallisempia. Käyttäjille on hyvä ilmoittaa laitteiden kirjaamisen aiheuttamista rajoitteista ja asetuksista erityisesti silloin, kun kyseessä on käyttäjän oma laite, johon asetukset vaikuttavat. Intunen hallintaportaalista valitaan: **Device configuration > Profiles > Create profile**. Ensin nimetään profiili ja valitaan haluttu alusta, esimerkiksi **Windows 10 and later** sekä profiilin tyyppi, esimerkiksi: **Device restrictions**. Tämän jälkeen päästään estämään tiettyjen sovelluksien käyttäminen, pakottamaan salasanan vaihtaminen tai vaikkapa poistamaan laitteen kamera käytöstä, kuten kuvassa 9 on tehty.



Kuva 9. Device restrictions – Block Camera

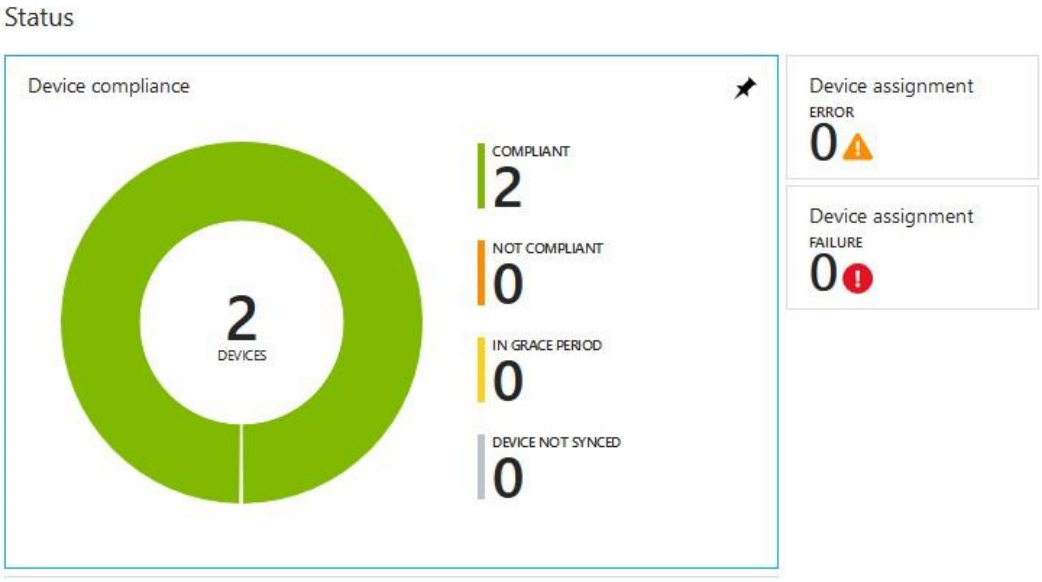
Profiilityypistä voidaan valita esimerkiksi **Endpoint protection**, josta päästään säätämään Windows Defenderin palomuuriasetuksia tai salaamaan kiintolevyn tietoja BitLockerin avulla. BitLockerin salakirjoituksella (encrypt) voidaan lisätä turvaa, jos

laite katoaa tai se varastetaan. Ulkopuolinen käyttäjä ei pääse käsiksi kiintolevyn dataan ilman BitLockeriin määritettyjä tunnuksia, jotka avaavat salauksen.

Myös VPN (Virtual Private Network) eli virtuaalinen erillisverkko voidaan muodostaa yritysten verkkojen ja koneiden välille valitsemalla profiilityypistä **VPN** ja asettamalla yrityksen käytössä olevan VPN-verkon tiedot kenttiin. VPN salaa verkkoyhteyden ja lisää internetin käyttäjän yksityisyyttä urkinnalta. VPN-yhteydet voidaan määritellä kaikille Intunen tukemille alustoille.

Kun halutut asetukset on säädetty, painetaan **OK**. Tämän jälkeen kohdistetaan profiili halutuille ryhmille: **Assignments > Select groups to include >** valitaan ryhmät **> OK > Save**. Asetukset tulevat käyttöön, kun profiilin piiriin kuuluvan ryhmän käyttäjä kirjautuu laitteelleen.

Onnistuneesti kirjatut laitteet näkyvät Intunen Device compliance -valikossa, kuten kuvassa 10. Opinnäytetyötä tehdessä kirjattiin kaksi Windows 10 Pro -mobiililaitetta yrityksen järjestelmään.



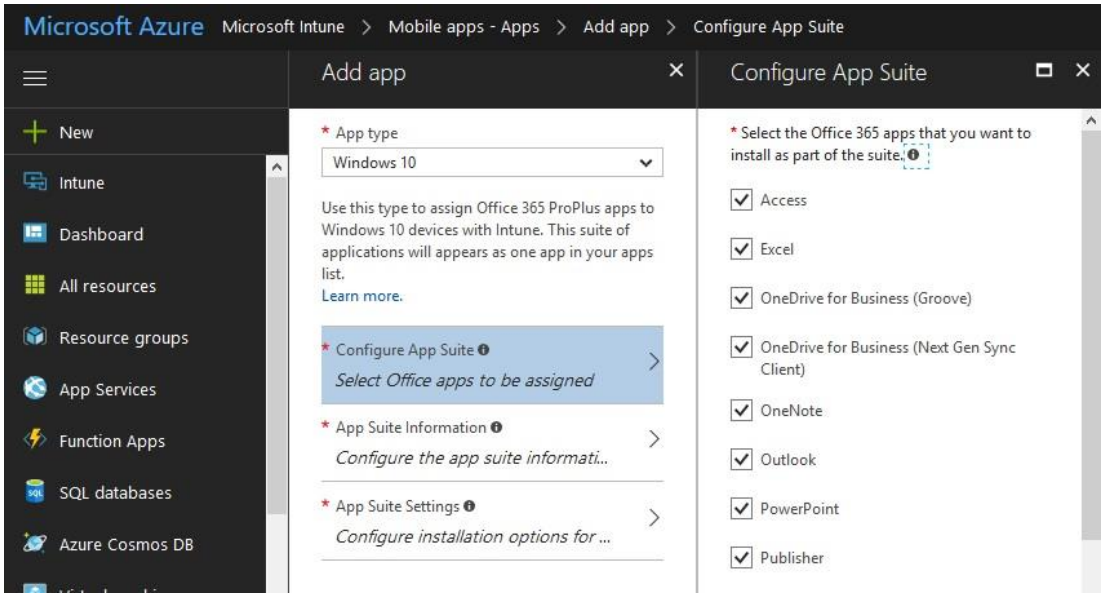
Kuva 10. Device compliance

COMPLIANT tarkoittaa, että laite noudattaa järjestelmänvalvojan siihen kohdistamia käytäntöjä (policy). NOT COMPLIANT tarkoittaa, että laite ei noudata yhtä tai use-

ampaa siihen kohdistetuista käytännöistä tai, että käyttäjä ei ole hyväksynyt järjestelmänvalvojan koneeseen kohdistettuja käytäntöjä. IN GRACE PERIOD tarkoittaa, että laitteeseen on kohdistettu käytäntöjä, mutta käyttäjä ei vielä ole ottanut niitä käyttöönsä, mutta ne oletettavasti otetaan käyttöön. DEVICE NOT SYNCED tarkoittaa, että laite ei ole kyennyt ilmoittamaan käytäntöjen noudattamisesta, koska laitetta ei ole yhdistetty verkkoon tai se on muusta syystä ollut kykenemätön kommunikoimaan Azure AD:n tai Intunen kanssa. Mikäli laitteiden kirjaamisessa on ristiriitoja määritettyjen käytäntöjen tai ongelmia verkkoon yhdistymisessä, niin ne ilmenevät listalla FAILURE tai ERROR -kohdissa.

5.4.4 Sovellusten jakaminen

Intunen avulla voidaan jakaa sovelluksia yritykselle kirjattuihin laitteisiin. Sovellusten jakaminen tapahtuu Intunen valikosta: **Mobile apps > Apps > Add**. Valitaan haluttu alusta ja määritellään jaettavat sovellukset, kuten kuvassa 11.



Kuva 11. Sovellusten jakaminen

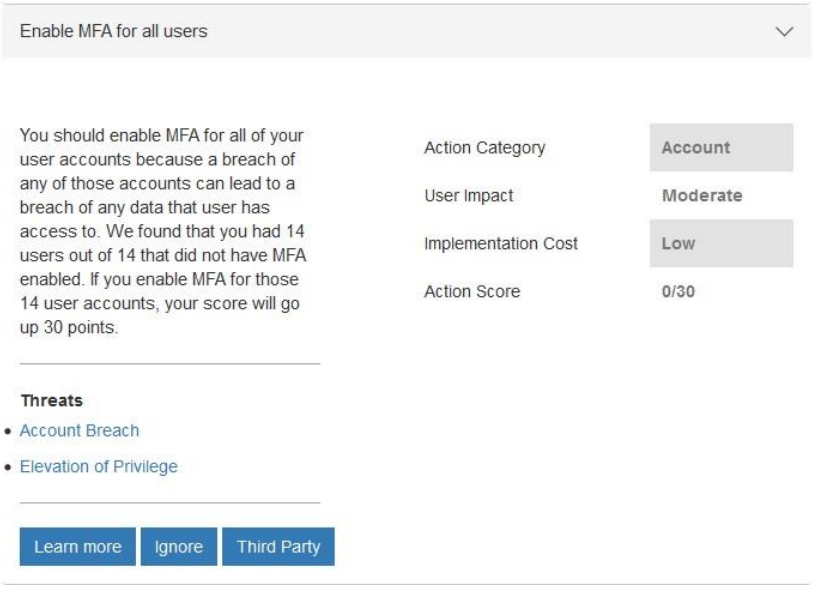
Valikosta voidaan valita Office 365 -pakettiin kuuluvia sovelluksia, joihin käyttäjille on määritelty käyttöoikeudet. Yrityksen käyttämiä muita sovelluksia voidaan jakaa, kun sovellustyypiksi valitaan **Line-of-business app**. Jaettavan tiedoston tulee olla muotoa msi, ipa, apk, xap, appx tai appxbundle. Exe-tiedostojen jakaminen ei tois-

taiseksi onnistunut uuden portaalin kautta, mutta vanhemmalla Intunen classic -portaalilla tämäkin onnistuu. Järjestelmänvalvoja kirjautuu osoitteeseen: *https://manage.microsoft.com/*, valitaan **Sovellukset > Lisää sovellus**. Tämän jälkeen ladataan koneelle ohjelmistojulkaisija -sovellus ja määritellään jaettava sovellus ohjeiden avulla. Kun sovellus on määritelty ja ladattu, se voidaan jakaa Intunen Yritysportaalin avulla. Myös **Web app** -tyyppisiä sovelluksia voidaan jakaa valitsemalla sovellustyypiksi **Web app** ja määrittelemällä www-sivu, josta sovellusta ylläpidetään.

Sovellukset voidaan asettaa joko pakollisiksi (Required) tai vapaaehtoisesti asennettaviksi (Available) valitsemalla **Mobile Apps > Apps >** valitaan haluttu sovellus, joka on jo määritelty **> Assignments > Type**. Samasta valikosta voidaan määrittää myös sovellus poistettavaksi (Unsinstall).

5.4.5 Office 365 Secure score

Secure score analysoi Office 365:ta käyttävän yrityksen tietoturvaan liittyvien asetusten perusteella ja antaa sen mukaan pisteytyksen tietoturvasta. Pistemäärä on 0 – 452, mutta opinnäytetyötä varten käytetyissä palveluissa maksimi oli 364. Secure score löytyy Admin centeristä: **Hallintakeskukset > Security & Compliance > Siirry Secure Scoreen**. Tietoturvaominaisuuksia onkin hyvä lähteä tarkastelemaan Secure Scoren kautta. Secure score -sivun alaosassa on määritelty eri ominaisuudet ja niiden käyttöönoton lisäämät pisteet. Kuvassa 12 on käytetty esimerkkinä monimenetelmäisen todentamisen (Multi-Factor Authentication, MFA) käyttöönoton antama maksimi pistemäärä ja vaikutus käyttäjiin.



Kuva 12. Monimenetelmäinen todentaminen

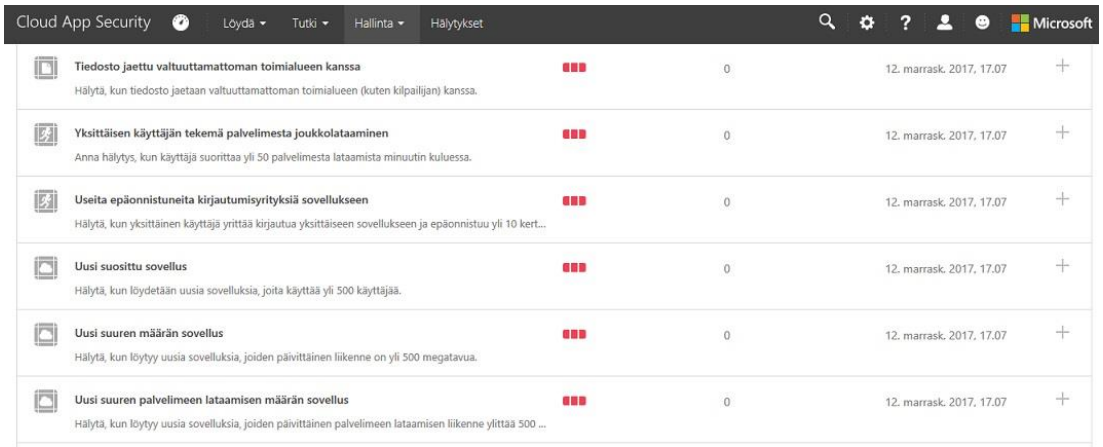
Monimenetelmäinen todentaminen voidaan ottaa käyttäjäkohtaisesti käyttöön myös valitsemalla **Käyttäjät** > **Aktiiviset käyttäjät** > **Lisää** > **Määritä Azuren monimenetelmäinen todentaminen**. Monimenetelmäinen todentaminen lisää tietoturvaa, jos käyttäjätunnukset ja salasana päätyisivät vääriin käsiin. Esimerkiksi käyttäjälle asetuksista määriteltyyn puhelinnumeroon lähetettävä koodi tekstiviestillä tai soitolla voivat toimia monimenetelmäisen todentamisen toisena vaiheena. Ainakin admin-tunnuksia käyttävillä käyttäjillä olisi syytä olla monimenetelmäinen todennus käytössä, koska heidän tunnuksiensa joutuminen vääriin käsiin voisi aiheuttaa paljon ongelmia yritykselle.

Secure score arvioi myös tietoturvaominaisuuksien vaikutusta käyttäjiin. Jotkin ominaisuudet eivät juurikaan näy käyttäjille, mutta käyttäjäkokemuksesta voi saada myös monimutkaisen lisäämällä lukuisia tietoturvaominaisuuksia. Onkin syytä kartoittaa mistä ominaisuuksista yritys hyötyy. Kun tietty ominaisuus halutaan ottaa käyttöön, valitaan kyseinen ominaisuus ja painetaan **Learn more > Apply, Review** tai **Launch now**. Sivusto ohjaa oikeaan paikkaan asetusten käyttöönottoon. Kannattaa huomioida, että Secure score ei päivitä pistemäärää reaaliajassa, vaan päivittämiseen voi kulua 24 – 48 tuntia. Koska erilaisia tietoturvaa lisääviä ominaisuuksia ja asetuksia on yli viisikymmentä, niitä kaikkia ei tässä opinnäytetyössä käydä läpi.

Secure scoren kautta voidaan tarkastella esimerkiksi maantieteelliseen ja aikaan pohjautuvaa kirjautumisen valvontaa: **Review signs-ins from multiple geographies report weekly**. Mikäli havaitaan, että käyttäjä on kirjautunut eri valtioissa, joissa hänen ei ole oletettu olevan, tai hänen matka-aikansa ei ole ollut realistinen, voidaan hänen tunnuksensa sulkea. Myös muiden käyttäjiin liittyvien toimien säännöllinen tarkastelu lisää Secure scoren pistemäärää. Tietoturvan lisäämiseksi voidaan myös laittaa käyttäjien tilit lukkiutumaan, mikäli niitä ei ole käytetty 30 päivän aikana. Järjestelmänvalvoja voi myöhemmin tarvittaessa aukaista tilit uudestaan käyttöön.

5.4.6 Cloud App Security

Cloud App Securityn avulla voidaan luoda erilaisiin tietoturvariskityyppeihin liittyviä toiminta- tai tiedostokäytäntöjä SaaS-ympäristössä. Palvelulla voidaan esimerkiksi tarkkailla tietyn käyttäjän, useasta lyhyen ajan sisällä tapahtuneesta epäonnistuneesta kirjautumisesta johtuvia tapahtumia. Käyttäjän epäilyttävistä toimista voidaan halutessa saada hälytyksiä järjestelmänvalvojan sähköpostiin tai puhelimeen, pyytää käyttäjä kirjautumaan uudestaan tai ottaa käyttäjän tunnukset automaattisesti pois käytöstä, mikäli asetuksista määritelty tilanne toteutuu. Cloud App Securityn asetuksia voidaan määritellä Admin centeristä valitsemalla: **Hallintakeskukset > Cloud App Security > Luo käytäntöjä**. Seuraavaksi valitaan halutut käytännöt ja halutessa muutetaan oletusmäärityksiä ja valitaan: **Luo**. Valmiita käytäntömalleja löytyy noin kolmekymmentä, joista on esitetty esimerkkejä kuvassa 13.



Kuva 13. Cloud App Security - käytännöt

6 JOHTOPÄÄTÖKSET

Käyttäjänhallinta on mahdollista tehdä entistä helpommaksi Office 365 -pilvipalveluiden avulla. Suurimpana ongelmana havaitsin ominaisuuksien käyttämisen yhdessä vanhojen Azure-portaalien ja uudemman Admin-portaalin kanssa. Kaikkia ominaisuuksia ei vielä ollut saatavilla uudesta portaalista ja tämä vaikeutti hallintaa. Palvelut ja ominaisuudet myös päivittyvät ja vaihtuvat tiheään tahtiin, joten ajan tasalla olevien ohjeistusten kanssa on oltava tarkkana. Osa uusista toiminnoista oli vielä demo-asteella, kun niitä hiljalleen on lisätty palveluun.

Pilvipalvelut ovat lisänneet yritysten työntekijöiden mahdollisuuksia toimia etänä, poissa omilta työpisteiltään. Myös pilvipalveluiden käyttöönotto on tehty kohtuullisen helpoksi verrattuna perinteisiin on-premise -ratkaisuihin. Palvelut uusiutuvat nopeaa tahtia ja ne pyrkivät vastaamaan asiakkaiden kysyntään. Erityisesti uusille yrityksille tai vanhoja laitteita uusiville yrityksille pilvipohjaiset ratkaisut ovat käteviä, johtuen käyttöönoton nopeudesta ja helposti ulkoistettavan ylläpidon kannalta. Myös kustannuksissa voi säästää, kun yrityksien ei tarvitse sijoittaa rahaa rautaan ja palvelimien viemään tilaan. Niille pk-yrityksille, joilla jo on toimivat ja kohtuullisen uudet on-premise -ratkaisut ei pilvipalveluista välttämättä ole niin paljon hyötyä.

Intune tarjoaa pilvipohjaisena palveluna paljon mobiililaitteiden hallintaan keskittyviä ratkaisuja, joilla pystytään korvaamaan aikaisemmin Group Policy -objekteina tehtyjä ratkaisuja. Kaikkia täysin samoja asetuksia Intunen MDM:llä ei ole vielä ainakaan toistaiseksi pystynyt kuitenkaan tekemään, mutta joitain täysin uusiakin ominaisuuksia on sen myötä tullut saataville. Uusien käyttäjien lisääminen ja vanhojen poistaminen palvelusta on nopeaa ja helppoa. Myös laitteiden hallintaan on olemassa laajat työkalut yritysten tarpeisiin. Enterprice Mobility +Security on hyvä paketointi Microsoftin tuotteista, mikäli yrityksen tietoturvaa halutaan lisätä, jotta kaikkia palveluita ei tarvitse ostaa erikseen.

Tietoturvaan on selkeästi panostettu Microsoftin tuotteissa ja sen ympärille onkin luotu paljon ominaisuuksia. GDPR on pakottanut palveluntarjoajat ottamaan tietosuo-

jalain vaatimat asiat huomioon. Tietoturvan tasoa pystyy Office 365 -palvelussa säätämään hyvin sen mukaan, kuinka tärkeänä asiakas sen kokee. Luottamus palveluiden joustavaan toimintaan ja korkeaan tietoturvaan on tärkeää asiakkaille. Korkeasta tietoturvasta voikin olla yritykselle myös kilpailuetua, kun asiakkaat valitsevat palveluntarjoajiaan. Lopuksi voidaankin todeta, että Office 365 onkin monipuolinen ja toimiva pilvipohjainen ratkaisu pienten ja keskisuurten yritysten käyttäjänhallintaan sekä tietoturvaan tällä hetkellä ja tulevaisuudessa varmasti entistä enemmän, kunhan yhä useammat yritykset siirtyvät käyttämään pilvipohjaisia ratkaisuja.

LÄHTEET

Anttila, J. & Roine, J. 2015. SharePoint & Office 365: Hyvät, Pahat ja Rumat. Helsinki: SharePoint HPR.

Heino, P. 2010. Pilvipalvelut. Helsinki: Talentum Media Oy.

Laaksonen, M., Nevasalo, T. & Tomula, K. 2006. Yrityksen tietoturvakäsikirja – Ohjeistus, toteutus ja lainsäädäntö. Helsinki: Edita Publishing Oy.

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Jyväskylä: Docendo Oy.

Microsoftin www-sivut. 2017a. Viitattu 4.10.2017.
https://www.microsoft.com/en-us/TrustCenter/Privacy/gdpr/default.aspx

Microsoftin www-sivut. 2017b. Viitattu 12.10.2017.
https://www.microsoft.com/fi-fi/cloud-platform/enterprise-mobility-security-pricing

Microsoftin Azure www-sivut. 2017. Viitattu 24.10.2017.
https://azure.microsoft.com/en-gb/

Microsoftin Docs www-sivut. 2017a. Viitattu 18.10.2017.
https://docs.microsoft.com/en-us/windows-hardware/design/device-experiences/oem-highly-secure

Microsoftin Docs www-sivut. 2017b. Viitattu 18.10.2017.
https://docs.microsoft.com/en-us/information-protection/understand-explore/what-is-information-protection

Microsoftin Docs www-sivut. 2017c. Viitattu 18.10.2017.
https://docs.microsoft.com/en-us/advanced-threat-analytics/what-is-ata

Microsoftin Docs www-sivut. 2017d. Viitattu 16.11.2017.
https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

Microsoftin Docs www-sivut. 2017e. Viitattu 16.11.2017.
https://docs.microsoft.com/en-us/intune/introduction-intune

Microsoftin Office Products www-sivut. 2017a. Viitattu 3.12.2017.
https://products.office.com/en-us/business/office-365-for-business-support-options

Microsoftin Office Products www-sivut. 2017b. Viitattu 3.12.2017.
https://products.office.com/en-us/business/office-365-trust-center-top-10-trust-tenets-cloud-security-and-privacy

Microsoftin Office Support www-sivut. 2017. Viitattu 30.11.2017.
https://support.office.com/en-us/article/Gather-the-information-you-need-to-create-Office-365-DNS-records-77f90d4a-dc7f-4f09-8972-c1b03ea85a67

Nuventurin www-sivut. 2017. Viitattu 3.12.2017. https://www.nuventur.fi/

Salo, I. 2012. Hyötyä pilvipalveluista. Jyväskylä: Docendo.

UEFI:n www-sivut. 2017. Viitattu 3.12.2017. http://www.uefi.org