TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Anna Budris
185600IAAB

MOBIILSETE SEADMETE HALDAMINE VÄIKEETTEVÕTTE NÄITEL

Bakalaureusetöö

Juhendaja: Edmund Laugasson
MSc

Tallinn 2021

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Oma uurimuses kasutatud teiste autorite töödele, olulistele seisukohtadele, kirjandusallikatele ja mujalt pärit andmetele olen lisanud allikaviite.

Autor: Anna Budris

17.05.2021

Annotatsioon

Käesoleva bakalaureusetöö eesmärk on luua ja testida lahendus, mis tagab mobiilsete seadmetele (näiteks telefonid, sülearvutid, tahvelarvutid) kontrollitud ligipääsu pilveteenustele.

Lõputöö käigus loodud probleemi lahendus tagab ettevõtte võimalust hallata ja kontrollida kasutajate mobiilseid seadmeid, mida kasutatakse kaugtööks.

Väljatöötatud lahenduse käigus seadistatakse *Microsoft Intune* teenused *MS Endpoint Manager* keskkonnas ja konfigureeritakse seda. Koostatakse reeglistikud ja registreeritakse mobiilsed seadmed. Viiakse läbi haldamistestimised.

Lõputöö tulemuseks on võimalus hallata kasutajate mobiilseid seadmeid, kontrollida neid ja pakkuda turvalist ligipääsu ettevõtte pilveteenustele. Vajadusel saab ettevõtte kaugseadmetest tööandmed ära kustutada.

Lõputöö on kirjutatud eesti keeles keeles ning sisaldab teksti 33 leheküljel, 10 peatükki, 9 joonist, 1 tabeli.

Abstract

Mobile Device Management on the example of a Small Business

The aim of this bachelor's thesis is to create and test a solution that provides controlled access to cloud services for mobile devices (eg phones, laptops, tablets).

The solution to the problem created during the dissertation provides the company with the ability to manage and control users' mobile devices used for remote work.

During the developed solution, Microsoft Intune services are configured in the MS Endpoint Manager environment. Rules are drawn up and mobile devices are registered. Management testing is being performed.

The result of the dissertation is the possibility to manage users' mobile devices, control them and provide secure access to the company's cloud services. Work data can be deleted from the company's remote devices on demand.

The thesis is in Estonian language and contains 33 pages of text, 10 chapters, 9 figures, 1 table.

Lühendite ja mõistete sõnastik

AAD Connect	Azure Active Directory Connect
AD	Active Directory
BYOD	Bring Your Own Device
CISA	Cybersecurity and Infrastructure Security Agency
CMG	Cloud Management Gateway
MAM	Mobile Application Management
MDM	Mobile Device Management
MEM	Microsoft Endpoint Manager
MFA	Multifactor Authentication
MS	Microsoft
*NIX	UNIXi-laadsed operatsioonisüsteemid
OOBE	Out-of-box experience
VOSK	Võta Oma Seade Kaasa
WAN	Wide Area Network
WSUS	Windows Server Update Services

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Bakalaureusetöö eesmärk on luua ja testida lahendus , mis tagab mobiilsete seadmetele kontrollitud ligipääsu pilveteenustele. Metoodika järgi valitakse efektiivne lahendus, mille testimine toimub virtuaalkeskkonnas. Seejärel tehakse süntees, kokkuvõtte tulemustest ja analüüsitakse neid.

Probleemiks, mida autor lahendab, on ebapiisav kontroll ettevõtte mobiilsete seadmete üle, mis võib põhjustada ettevõtte andmekadu. Samuti puudub kontrollitud ligipääs ettevõte pilveteenustele.

Lõputöös käsitlev teema on aktuaalne antud ettevõttes, mis kasutab Microsofti pilveteenuseid. Probleemi ettevõttes ei ole eelnevalt proovitud lahendada, lõputöös käsitletud metoodikat ei ole varem ettevõttes proovitud rakendada. Kuigi töös kirjeldatud probleemi lahendus on läbi viidud konkreetse ettevõtte näitel, võib probleemi lahendust rakendada ka teistes ettevõttetes, kus kasutatakse Microsofti pilveteenuseid.

Lõputöö koosneb kaheksast peatükist. Esimeses peatükis kirjeldatakse ettevõtte hetkeolukord ja olemasolevad probleemilahendused. Teises peatükis kirjeldatakse probleem ja sellega kaasnevad olukorrad. Kolmandas peatükis kirjeldatatake ettevõte poolt määratud lähtetingimused ja piirangud, mis antud probleemi lahendamisse ei kuulu. Neljandas peatükis kirjeldatakse lõputöö eesmärgi. Viiendas peatükis kirjeldatakse metoodika, mis sisaldab endas ülevaade metoodikast, tööriistadest ning tarkvara võrdlev analüüs vastu ettevõtte nõuetele. Kuues peatükk on tulemused, kus kirjeldatakse vajaliku tarkvara seadistamist ja testitakse probleemi lahendust. Seitsmes peatükk on tulemuste analüüs, kus antakse hinnang lahendusele ja tehakse järeldused. Kaheksandas peatükis autor kirjeldab võimalikud tuleviku arendused ettevõttes.

2 Hetkeolukord

Ettevõttes on Microsoft põhjal taristu. Ettevõtte kasutab oma igapäevases tegevuses Microsoft 365 pilveteenused, mis on Microsoft Configuration Manager keskhalduses, millega on võimalik kontrollida ja hallata ettevõtte kontoris olevaid arvuteid.
Erakorralise seisukorra tõttu tekkis enamikul ettevõtte töötajatest vajadus töötada kodus ja kuna ettevõte polnud selleks eriti valmis, ei olnud kesksed seadistus tööriistad selliseks olukorraks ette valmistatud. Ei olnud võimalik teada saada, kuidas töötajad kasutavad tööandmeid, milline on autentimise meetod. Samuti juhul, kui isiklik seade kaotakse, ei ole võimalik kaitsta ettevõtte andmed, mis asuvad seal. Kuna turvalisus on kaugtöös võtmekontseptsioon, pidid lõputöö autor ja ettevõtte IT-meeskond leidma lahendused kaugel asuvate seadmete kontrolli ja turvalisuse puudumise probleemile. Kaugtöö võimalus püsib ka pärast pandeemiat. Lõputöö autor ja ettevõtte IT-meeskond soovivad tagada, et nende väljatöötatud ja juurutatud lahendus kestab kaua ning on jätkuvalt võimalikult turvaline. Probleemi lahendamiseks otsustati võtta kasutusele uued lahendused, mis on seotud Microsoft platvormiga.

Kuidas lahendati antud probleem ettevõttes varem? Arvutite haldus on olemas, ettevõttesiseselt on arvutid hallatud *Microsoft Endpoint Configuration* Manager abil, mis haldab mingil määral mobiilseid arvuteid läbi *Cloud Management Gateway*. *Cloud management gateway* (CMG) pakub lihtsat viisi Configuration Manageri klientide haldamiseks Interneti kaudu. CMG juurutatakse pilveteenusena Microsoft Azure'is. Seejärel saab ilma täiendava kohapealse taristuta hallata kliente, kes liiguvad Internetis või asuvad kogu WANi harukontorites. Samuti ei pea ettevõtte pakkuma juurdepääsu oma asutusesisesele taristule. [14] CMG kaudu saavad sülearvutid ka uuendused kätte, mida nad peavad paigaldama.
Ettevõttes varem ei ole kunagi mobiiltelefone hallatud. Kõige tähtsam kontrolli osa on see, et ettevõttel oleks võimalus kaitsta andmeid, mis asuvad mobiiltelefonidel, mis kasutatakse kaugtööks. Kõige raskem on hallata töötajate isiklikud mobiilseadmed, mis võivad olla kaugtöös kasutuses ja endas hoida ettevõtte konfidentsiaalsed andmed.

Ettevõttel puudub garantii, et töötajad kasutavad oma mobiilseadmeid ohutult ja säilitavad ettevõtte andmeid turvaliselt. Töötajad võivad olla hooletusest hoolimata, eeskirja teadmata või seda mugavuse huvides tahtlikult rikkuda ega teadvustada kaasnevaid riske. See kehtib eriti mobiiltelefonide kohta, kus isikliku kasutamise ja ärikasutuse vahelised piirid ei pruugi olla selged või neid lihtsalt ignoreeritakse. Kasutajate käitumise tõttu tekkivate haavatavuste näited hõlmavad turvarakenduste, näiteks viirusetõrjetarkvara või tulemüüride, keelamist, nakatunud rakenduste allalaadimist Internetist, eeskirja rikkumisega kiirsuhtlustarkvara või -failide kasutamist, tundliku teabe paigutamist eemaldavatesse salvestus seadmetesse ja tundliku teabe postitamist e-kirjadesse saadetakse volitamata saajatele. [13]

Kaugtöö jaoks kasutatakse ainult sülearvutid. Arvutid antakse välja ettevõtte poolt kindlate konfiguratsioonidega. Osaline kontroll on olemas, näiteks võimalus hallata autentimismeetodit, paigaldada operatsioonisüsteemi ja oluliste programmide värskendusi, samuti kontrollida viirusetõrje ja tulemüüri olemasolu. Kuid see ei olnud piisav ettevõtte kaugtöö jaoks.

Probleeme, mis oleksid seotud andmete lekkimisega või mobiilsete seadmete väärkasutamisega, täna ettevõttes ei ole tuvastatud, kuid võimaliku riski vältimiseks on ettevõte IT-meeskond otsustanud võtta kasutusele vastav probleemilahendus, et kaitsta ettevõtte andmeid tulevikus.

Siiski maailmapraktikast on teada, et on olemas näited andmete lekkimisest ja seadmete väärkasutamisest. Näiteks kaotatud ja varastatud telefonid/mobiilseadmed on tõsine probleem. 2010. aasta juunis teatas CIO.com, et viimase poole aasta jooksul oli New Yorgi taksodesse jäetud 31 544 nutitelefoni [1]. 2005. aastal küsitles Pointsec ja litsentsitud taksojuhtide ühendus taksojuhte Londonis ja teistes linnades. Londoni taksojuhid teatasid, et kuue kuu jooksul jäid nende kabiinidesse üle 60 000 mobiiltelefoni, 5500 pihuarvutit ja 4500 sülearvutit. [13] Kui seade on kaotatud, siis ettevõtte andmed on lekkinud ja tekib riskiolukord. Sellisel juhul peab olema võimalus hallata seadmeid ja kustutada ettevõtte andmeid enne, kui neid saab kätte võõras isik.

3 Probleemi kirjeldus

Praegu on ettevõttes sisemine kontorisüsteem seadistatud Microsofti pilveteenustele, mis muudab konfiguratsioonide ja sätete haldamise kiireks ja mugavaks. Võimalus kontoriarvuteid täielikult kohandada ja tarkvara paigaldamist automatiseerida võimaldab ettevõttel oma andmeid kontrollida ja turvaliselt hallata.

Kaugtöö osas on siiski teatud puudusi. Kaugtöö tähendab töötaja võimet töötada väljaspool kontorit. Kasutatav mobiilseade võib olla kas ettevõtte poolt pakutav või inimese isiklik seade. Mobiilseadmed on sellised seadmed nagu tahvelarvutid, telefonid ja sülearvutid.

Probleem seisneb selles, et ettevõtel puudub võimalus piisavalt kontrollida ettevõtte väliseid seadmeid, mida kasutatakse töötamiseks väljaspool kontorit. Eriti puudutab see kasutajate isiklikke seadmeid, milles hoitakse töökontosid ja andmeid. Probleem puudutab kõiki töötajaid ettevõttes, kuna igal töötajal peab olema võimalus töötada kodust kaugtööna.

Kontrolli all mõeldakse võimalust hallata seadmeid (mis asuvad ettevõtte võrgust väljaspool) ning nendes olevaid andmeid. Haldamiseks nimetatakse võimalust konfigureerida seadmes olevaid sätteid, programmid, seadistada vajalikud nõuded ning kontrollida kasutajate ligipääsu ettevõtte andmetele. Samuti võimalust kustutada kasutajat ja temaga seotud seadet süsteemist, mis omakorda kustutab seadmes olevaid tööandmeid.

Samas tekib küsimus, millised probleemid võivad kaasneda, kui ettevõte ei saa kaugseadmete tööd ja andmekasutust jälgida?

Kui ettevõttel puudub võimalus kontrollida kaugseadmete tööd, siis võib see põhjustada ettevõttele andmekadu. Tulemusena võib lekkida ettevõtte konfidentsiaalset siseinfot, mis ei ole mõeldud kolmandatele isikutele. Ettevõtte andmeteks loetakse tööks kasutatavat e-posti (*MS Exchange*), faile (*MS OneDrive* ja *MS Sharepoint*) ja samuti privaatset suhtlemist (*MS Teams*). See on informatsioon, mis on mõeldud ainult ettevõtte töötajatele.

Neid andmed kasutatakse töö raames. Nõuetekohase kontrollita ei saa ettevõte olla kindel, et operatiivandmed on kaugseadmetesse õigesti salvestatud.

Näitena võib tuua erinevaid olukordi, mis võivad ettevõtte andmetele ohtu kujutada:

1. Olukord, kus inimene ajas isikliku kasutaja segi töökeskkonna kasutajaga ja esitas tööalase teabe töövälisest keskkonnast. On võimatu kontrollida ega garanteerida, et inimene kasutab tarkvara ainult tööotstarbel, et tema töökeskkond on eraldatud isiklikust keskkonnast. Selles olukorras satuvad andmed ebaturvalisse keskkonda, kus ettevõte ei saa teada nende edasist kasutamist.
2. Olukord, kus inimene kaotab oma mobiilse seadme või see varastatakse. Sellisel juhul pole ettevõttel võimalust seadmest tööandmeid tagasi saada või kustutada ning seeläbi on võimatu tagada mobiilseadmetes asuvate andmete turvalisust.
3. Olukord, kus töötajat koondatakse. Sellisel juhul saab tööandmete kustutamist tagada ainult füüsilise ligipääsuga seadmele ehk töötaja ja seadme tulekuga kontorisse. Juhul, kui inimene ise kustutab tööga seotud andmed, rakendused vmt, ei saa ettevõte tagada nende täielikku kustutamist seadmes, kuna puudub kontrolli mehhanism.
4. Olukord, kui mobiilsel seadmel olevad tööandmed ei ole piisavalt kaitstud. Mobiilsed seadmed peavad olema krüpteeritud ja nendel peavad olema sobivad autentimismeetodid ja mehhanismid. Näiteks parooli puudumisel on võõral isikul lihtsam seadmele ligi pääseda. Kui aga parool on olemas, siis peab see olema korrektne ja turvaline. Samuti ei saa ettevõtte olla kindel, et tööks kasutatav seade on krüpteeritud, mis samuti näitab seadme turvalisuse taset. Ettevõttel peab olema võimalus selliseid konfiguratsioone seadmel hallata ja kontrollida.

Praktilises osas töötatakse välja lahendused nende elu olukordade näidete lahendamiseks.

4 Eesmärk

Peamised uurimisküsimused, millele autor töö käigus vastata soovib, on järgmised:

1. Milline programm sobib kõige paremini ja vastab ettevõtte nõuetele tõstatatud probleemi lahendamiseks ?
2. Kuidas valitud programm aitab paremini kontrollida ja hallata mobiilseid seadmeid, mis kasutatakse ettevõtte kaugtööks?

Eesmärk on luua ja testida lahendus, mis tagab mobiilsete seadmetele kontrollitud ligipääsu pilveteenustele. Selleks, et eesmärki saavutada, töötas autor välja metoodika, mille järgi tegeletakse probleemi lahendamisega.

Eesmärk saavutatakse, kui antud küsimustele on vastatud ning ettevõtte probleem on lahendatud. See tähendab, et ettevõte on testkeskkonnas kasutusele võtnud valitud programmi ja teinud vajalikud seadistused mobiilsetele seadmetele. Samuti prooviti hallata seadmeid vastavalt ettevõtte nõuetele ning analüüsiti saavutatud tulemusi.

4.1 Mobiilsete seadmete turvalisus ja kontroll

Kennesawi osariigi ülikoolist Max Landmani sõnul on mobiilseadmete turvalisus sama oluline kui arvutite turvalisus. Tõhusad ettevõtte mobiilsete seadmete turvaprogrammid peavad arvestama kasutaja käitumist, seadmele ja võrgule juurdepääsu, side- ja andmesalvestust. Mobiilsed seadmed, nende kasutamise olemuse tõttu, hõlmavad kasutajate nõrku turvameetmeid. Krüptimist, tulemüüre, viirusetõrjetarkvara, digitaalseid sertifikaate ja kaugpuhastamise võimaluse saab kasutada seadmetele ligipääsu ja neile salvestatud andmete kaitsmiseks. Paroolikaitse peab olema tugev ja kasutada tuleb kaheastmelist isikutuvastust. [13]

Ettevõtte võime jälgida mobiilsete seadmete andmeid ja neid kontrollida on ettevõtte üldise turvalisuse seisukohalt väga tähtis. Näiteks nutitelefonide platvormidel on erinevad turvaomadused. Võimaluse korral peaks organisatsioon jälgima seadmete valikut ja pidama valiku kriitiliseks elemendiks nende turva võimalusi. Seadmete

kaughaldussüsteeme saab kasutada ka tulemüüri konfiguratsioonide värskendamiseks, võrgus olevaid telefone ähvardavate pahavara uute versioonide tuvastamiseks, pahavara telefoni sisenemise vältimiseks ja konfidentsiaalsete andmete lekkimise vältimiseks. Mobiilsete seadmete kaughaldus, eriti koos tulemüüri ja kontekstiteadliku juurdepääsu kontrolliga, võib pakkuda nutitelefonidele tõhusat turvalisust. [13]

4.2 BYOD strateegia

BYOD (ehk Bring Your Own Device) strateegia eesti keeles nimetatakse VOSK, mis tähendab "võta oma seade kaasa" [12]. BYOD on osa sellest, mida sageli nimetatakse IT kliendikeskseks, kus töötajad integreeruvad üha enam oma mobiilseadmetega ja eeldavad, et saavad neid kasutada ettevõtte võrkudega ühenduse loomiseks. Kuna töötajad kasutavad nüüd tõenäoliselt oma arvuteid ja mobiilseadmeid tööga seotud ülesannete täitmiseks - olenemata sellest, kas tööandja seda toetab või mitte -, muutub BYOD'i eeskiri, mille eesmärk on kontrollida selliste seadmete kasutamist, BYOD'i riskide maandamise seisukohalt üha olulisemaks.[15]

BYOD-lahenduse juurutamise käigus kerkib seadme kasutaja andmete privaatsuse ja turvalisuse küsimus. Kas on võimalik eristada isiklikku elu ja töökeskkonda BYOD'iga või mitte? Kui ei, siis kuidas inimene nõustub, et ettevõte näeb tema isiklikke asju. Sellised küsimused peaks ettevõte eelnevalt läbi mõtlema ja lahendama, et tulevikus probleeme ei tekiks.

Selge ja hästi kirjutatud BYOD-eeskiri võib olla esimene samm BYOD'i keskkondades turvalisuse ja privaatsuse kontrolli säilitamise suunas. BYOD'i kasutajad peaksid organisatsiooni teaberessurssidele juurde pääsemisel järgima mõningaid üldisi juhiseid.[27]

Kõik asjad, mis saavad mõjutada välja töötatud BYOD teenuse, võivad endast kujutada riskid. Selleks, et neid vältida, koostatakse töölepingule lisa, kus oleks kirjas BYOD eeskiri ja käitumisjuhend töötajatele. Töötajat teavitatakse andmekaitse meetoditest, kes ja kuidas saavad kasutada isiklikku mobiilseadet ning pääseda juurde töökeskkonnale.

Turvalisus ja privaatsus on pidev protsess, mis nõuab tähelepanu, administreerimist, ülevaatamist ja paindlikkust. BYOD'i turvalisuse ja konfidentsiaalsuse tagamiseks peab iga organisatsioon oma kohustusi õigeaegselt mõistma ja neid täitma [27].

5 Tingimused

Tarkvara ja teenused, mis valitakse antud lõputöö teema probleemi lahendamiseks peavad vastama ettevõtte seatud tingimustele ja nõuetele.

5.1 Tingimuste loetelu

Lõputöös püstitatud probleemi lahendamiseks oli vaja luua mitmeid tingimusi, millele lõputöö lahendus peab vastama. Lõputöö autor otsustas teha intervjuu IT-juhiga ja selgelt määratleda nõuete ja tingimuste loetelu. Vestluse tulemusel töötati välja järgmised tingimused, mis endast kujutavad võimalust hallata mobiilseid seadmeid, mille all mõeldakse järgmist:

- peab olema võimalik eemalt kustutada tundlikud ettevõtte andmed;
- võimalus kontrollida andmete turvalisust seadmel, kus neid hoitakse;
- seade peab vastama määratud nõuetele (peab olema krüpteeritud, vastavad uuendused ja autentimismeetodid);
- seadme keskne haldamine, vastavalt ettevõtte nõuetele: reeglistik, vastavus, juurutamine;
    - parool: pikkus, keerukus,
    - programmide paigaldamine, seadistamine, eemaldamine.
- haldustarkvara mitmeastmeline isikutuvastus (*MFA multifactor authentication*) ;
- erinevate operatsioonisüsteemide tugi: Android, Windows;
- võimalus töötajatel kasutada oma isiklikke seadmeid (privaatsuse tagamine).

5.2 Käesoleva töö piirangud

1. Antud töös räägitakse probleemi lahendusest, mida testitakse Windows ja Android operatsioonisüsteemidega mobiilsetel seadmetel. Linux / iOS / *NIX / Windows phone – need mobiilsed seadmed jäävad antud töö skoobist väljaspool. Kuid need seadmed lisatakse siiski tulevikuplaanidesse ning viiakse läbi uued testid ja kontrollid.

2. Töö probleem ja lahendus on seotud ainult ettevõtte pilveteenustega ehk IT taristuga, mis ei asu ettevõtte kontoris, vaid teenusepakkuja turvalises andmekeskuses. Antud ettevõtte puhul tegu on Microsoft pilveteenustega.

3. Praktiline osa ehk testimine toimub ainult kaugtööks mõeldud mobiilsete seadmetega. See tähendab, et kontoris olevad seadmed ja arvutid ei ole osa töö skoobist.

4. Mobiilsete seadmete kasutajateks on ainult ettevõtte töötajad ehk inimesed, kellel on olemas kasutaja ning ligipääs ettevõtte pilveteenustele. Samuti antud lahendus puudutab ka uusi töötajaid, kellele alles luuakse kasutajaid.

Antud lahendus ei puuduta ajutisi töötajaid, kellel puudub kasutaja või ettevõtte väliseid külalisi. Sellised inimesed ei ole vastavas sihtrühmas. Kuid nendele turvalise ja kontrollitud ligipääsu loomine võib olla tulevikuplaanide osas.

6 Metoodika

Lõputöö metoodika sisaldab endas intervjuud, teoreetilist ja praktilist osa.

Viiakse läbi intervjuu IT osakonna juhiga, kus seatakse ettevõtte poolt nõuded võimalikeks tarkvara lahendusteks. Saadakse ülevaade ettevõtte hetkeolukorrast ning probleemidest, mida soovitakse lahendada. Samuti pannakse paika ka lähtetingimused ja piirangud (lõputöö peatükis 5 neid kirjeldatakse).

Teoreetilises osas tehakse erinevate tarkvarade võrdlev analüüs, kõrvutades seda ettevõtte nõuetega. Autor analüüsis tarkvarade võrdluseks teaduslikke ja tehnilisi allikaid. Võrdluse tulemused analüüsitakse ning valitakse üks lahendustest. Samuti kirjeldatakse, kuidas valitud lahendust sobib ettevõtte probleemi lahendamiseks.

Praktilises osas seadistatakse valitud tarkvara. Toimub testimine, mille käigus proovitakse läbi erinevad mobiilsete seadmete haldamise võimalused. Mobiilseteks seadmeteks ettevõttes on sülearvutid Windows 10 operatsioonisüsteemiga ja mobiiltelefonid Android 10 operatsioonisüsteemiga.

6.1 Tööriistade ülevaade

Antud peatükis annab autor ülevaate otsitavatest tööriistadest ja võrdleb neid omavahel. Tulemuseks valitakse tarkvara, mis kasutatakse probleemi lahendamiseks.

6.1.1 Tööriistade võrdlus

"*Microsoft Azure: Planning, Deploying, and Managing Your Data Center in the Cloud*" raamatu andmete põhjal peetakse Microsoft Intune (mis on üheks Microsofti Endpoint Manageri osaks) tööriista ettevõtte probleemi lahendamiseks parimaks vahendiks [1], kuid lõputöö autor võttis teadmiseks ka muud tööriistad, mis sobivad selles lõputöös tõstatatud probleemi lahendamiseks.

Objektiivse otsuse langetamiseks otsustas töö autor võrrelda sarnaseid programme vastavalt ettevõtte seatud nõuetega. Alternatiivsed programmid valiti *AlternativeTo* ja *SourceForge* veebilehekülgedelt [4][5]. Programmid valiti tingimusel, et need saaksid olla lahenduseks selle lõputöös tõstatatud probleemi lahendamiseks. Võrdlemine toimub vastavalt ettevõtte seatud nõuetele ja lähtetingimustele.

Võrdluses kasutatakse järgmisi töövahendeid:

- Jamf Pro
- WSUS
- Miradore MDM
- Microsoft Intune

1. Jamf ja Intune: võrdlus

Jamf Pro on ettevõtte mobiilsuse haldamise tööriist, mis annab IT-spetsialistidele ja kasutajatele, keda nad toetavad, laiendatud kasutusvõimalused, ehk Apple'i seadmete lõpp-punkti haldamise funktsiooni. Jamf Pro on saadaval pilves või kohapeal. Jamf Cloud on pilvemajutuse lisandmoodul, mis pakub teie serveri üle paindlikkust ja kontrolli. [2] Antud programm on uudne ning on olemas erinevad versioonid vastavalt vajadustele (näiteks Jamf Pro, Jamf Now, Jamf School jne).

Võrreldes Intune'iga, toetab Jamf ainult MacOs platvormi. Asjaolu, et programm ei toeta Windowsi ja Androidi operatsioonisüsteemi, ei sobi ka ettevõtte esitatud tingimustega. Vaatamata sellele, et programmidel on pakkumiseks erinevad platvormid (kuigi Intune võimaldab ettevõttel juhtida ka MacOs seadmeid), on neil üks eesmärk - mobiilsete seadmete haldamine, kontroll ja kasutajate jaoks kasutamiseks mugav keskkond.

2020. aastal integreeriti Intune ja Jamf. Kui organisatsioon kasutab Jamf Pro programmi MacOS-seadmete haldamiseks, saab ta kasutada ka Microsofti Intune vastavuse eeskirju (koos *Azure Active Directory* (*Azure AD*) tingimusjuurdepääsuga), et veenduda, et organisatsiooni seadmed vastavad ettevõtte nõuetele, enne, kui lasta need ressurssidele juurde. [3] Kokkuvõtteks võib öelda, et Jamf eraldi programmina ei sobi selle probleemi lahendamiseks, kuid seda saab kasutada koos Intune'iga.

2. WSUS ja Intune: võrdlus

"WSUS-i võrguühenduseta värskendus" on tasuta tööriist, mis võimaldab turvaliselt, kiiresti ja internetiühenduseta värskendada kõiki arvuteid, milles töötab Microsoft Windows.[6] WSUS-i võrguühenduseta värskendus tööriistal on võimalus värskendus failid USB-mälupulgale kopeerida. Samuti võib luua ISO-pilte. [7] WSUS on ettevõttesisene lahendus, mida kasutatakse just ettevõtte siseses taristus.

Windows Intune töötab pilves ning ei vaja kohapealset taristu. Värskendused tarnitakse otse teie hallatavatesse arvutitesse, millel on internetiühendus. Ettevõtte probleemi lahenduseks peab valitud programm haldama mobiilseid seadmeid, mis kasutatakse kaugtöös. Intune võimaldab sujuvalt teha kaughaldust, see tähendab vaadata kõigi hallatavate arvutite plaastri olekut ja vastavust, olenemata sellest, kas need asuvad ettevõtte võrgus või väljaspool seda. WSUS seda teha ei võimalda. [8]

3. Miradore MDM ja Intune: võrdlus

Miradore Online on pilvepõhine mobiilseadmete haldamise lahendus, mis võimaldab kasutajatel kõiki mobiilseadmeid võimalikult täielikult turvata. Kuigi see on oma hinna poolest kindlasti populaarne, võib selle funktsionaalsus olla kallimate võimalustega võrreldes piiratum.[9] Miradore aitab tagada seadme ja andmete turvalisuse ning andmete vastavuse kogu organisatsioonis. Saate krüptida kõik konfidentsiaalsed andmed, eraldada äri- ja isiklikuks kasutamiseks, jõustada turvalised pääsukoodid ja ekraanilukud ning takistada soovimatute rakenduste kasutamist. [10]

Miradore on Intune'le üsna hea alternatiiv ja omab palju sarnaseid funktsioone. Kui aga arvestada, et ettevõtte taristu on Microsoft keskkond ning igapäevatöös kasutatakse Office 365 teenused, võib teha järeldust, et Intune sobib siiski probleemi lahendamiseks paremini. Intune on välja töötanud Microsoft ise, mis tähendab, et selle juurutamine ja kohandamine on ettevõttele odavam ja mugavam. Intune on paremini integreeritud Office 365 teenustega [11].

Lõplikud võrdlustulemused on toodud eraldi tabelis, kus (tabeli number 1). Number üks näitab funktsioonide olemasolu programmides, number null nende puudumist.

Tabel 1. Erinevate tarkvarade võrdlus

	Microsoft Intune	Jamf Pro	Miradore MDM	WSUS
OS tugi: Android, MS Windows	1	0	1	1
Pilveteenused	1	1	1	0
Uuenduste paigaldamine	1	1	1	1
Seadme keskne haldamine	1	1	1	0
Ühelduvus Azure Active Directory ja Office365 teenustega	1	0	0.5 *	0
Windowsi poolt pakutav tarkvara	1	0	0	1
Tulemus	**6**	**3**	**4.5**	**3**

* - ühelduvus ainult Azure'ga, tasulise versiooni puhul

6.2 Microsoft Intune'i kasutamine probleemi lahendamiseks

Microsoft Intune on loodud selleks, et aidata seadmeid kaitsta ja hallata, võimaldades samal ajal kasutajatel ettevõtte e-postile, andmetele ja rakendustele kaugjuurdepääsu. Kuna see on pilvepõhine, saab seadmeid hallata mis tahes toetatud veebibrauserist. Need tehnoloogiad võimaldavad ettevõtte andmeid kõrgemal tasemel kontrollida ja aitavad vältida tundlike andmete juhuslikku lekkimist. [1]

Kuna ettevõtte kasutab oma igapäevatöös Office 365 teenuseid, on tähtis, et Intune võimaldaks ka Office 365 ja muude rakenduste täpset juhtimist, võimaldades IT-administraatoritel piirata juurdepääsu meilidele või OneDrive'i äri dokumentidele, kui kasutaja logib sisse registreerimata seadmest. Samuti muudab Intune reeglite seadmise ja määratlemise lihtsaks ühe administraatori portaali kaudu, mis võimaldab reeglite konfigureerimist ja seadmete haldamist. Microsoft Intune pakub igakuist tellimisteenust (MS Intune on osa ettevõtte mobiilsuse ja turvalisuse paketist, mis on mõeldud ettevõtetele turbekaitseks). [29]

7 Tulemused

Tulemuseks on võimalus hallata kasutajate isiklikke mobiilseid seadmeid, võimalus pakkuda turvalist ligipääsu ettevõtte andmetele, mis annab võimaluse vabalt kasutada neid igal pool ja vajadusel efektiivselt kasutajad ja andmed ära kustutada seadmetest. Kontrolli tulemuseks on see, et seadmed vastavad ettevõttes kehtestatud turvaeeskirjale andes turvalise ligipääsu ettevõtte andmetele, mis annab töötajale rohkem võimalusi neid kasutada ja ettevõttele võimaluse andmeid kaitsta.

Probleemi lahenduseks valiti Microsoft Intune programm (valiku tegemine 6 peatükis). Praktilises osas toimub selle paigaldamine ja konfigureerimine. Registreeritake kasutajate mobiilsed seadmed ning tehakse haldamise testimist.

7.1 Ettevalmistused

Testimiskeskkonna loomiseks on vajalikud järgmised ettevalmistused:

1. Virtuaalse taristu loomine. Windows serveri seadistamine. Powershell skripti läbi mõtlemine ja kirjutamine. Powershell skripti eesmärk oli luua sada erinevat kasutajat testimiseks ning gruppide loomiseks.

2. Autor tegi Windows serveril AD (Active Directory) erinevad grupid. Need on vajalikud erinevate konfiguratsioonide suunamiseks ja õiguste jagamiseks. Sinna lisatakse kasutajaid. AD gruppides on mugavam lisada ja kustutada liikmeid ning määrata neile õigused.

3. Microsoft administraatori õigustega konto loomine. Administraatori õigustega on võimalik edukalt kasutada Microsoft Endpoint Manageri teenused ning viia läbi testimised probleemi lahendamiseks. Microsoft Endpoint Manageri osaks on Microsoft Intune, mida antud töös kasutatakse.

4. AAD ühendus (*AAD Connect ehk Azure Active Directory Connect*) on vahend kataloogiandmete edastamiseks ettevõttesisese ja pilve vahel [16]. See tähendab,

et AD kasutajad ja grupid sünkroniseeritakse Azure Active Directory'sse. Kasutajad saavad kasutada ühte identiteeti, et pääseda juurde kohapealsetele rakendustele ja pilveteenustele. Samuti sünkroniseerimine on vajalik, et määrata kasutajatele Office365 litsentsid, mis on vajalikud selleks, et oleks võimalus hallata ja konfigureerida kasutajad, kasutades Microsoft programmid. Kui kasutajakonto lisatakse AD gruppi või grupist eemaldatakse, määratakse grupitellimuste litsentsid automaatselt või tühistatakse kasutajakontolt.

5. Hankida sobivad mobiilsed seadmed. Testimiseks kasutati Lenovo firma tahvelarvuti Android operatsioonisüsteemiga ja Dell firma sülearvuti Windows 10 operatsioonisüsteemiga.

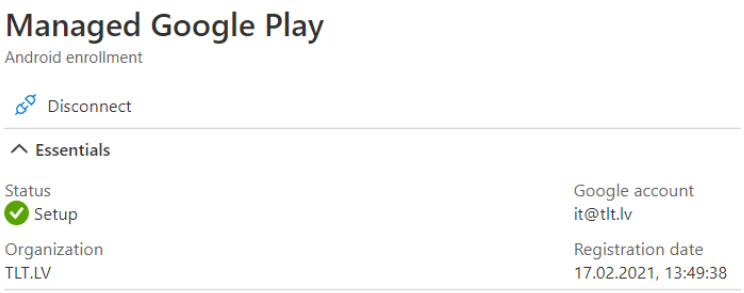
7.2 Microsoft Intune'i kasutusele võtmine

Microsofti otsepunktihalduri halduskeskusest (*Microsoft Endpoint Manager admin center* ehk *MEM admin center*) saab leida Microsofti Intune'i teenuse ja muud seadmehaldusega seotud seaded. Microsoft Intune, mis on osa Microsofti lõpp-punkti haldurist (*MEM*), pakub organisatsioonile pilvtaristu, pilvepõhise mobiilseadme haldust (*MDM*), pilvepõhise mobiilirakenduse haldust (*MAM*) ja pilvepõhist arvutihaldust. Intune aitab tagada, ettevõtte seadmed, rakendused ja andmed vastavad ettevõtte turvanõuetele. Samuti on õigus määrata, milliseid nõudeid tuleb kontrollida ning mis juhtub, kui neid nõudeid ei täideta. Intune'i abil tagatakse, et tööjõu korporatiivsed ressursid (andmed, seadmed ja rakendused) on õigesti konfigureeritud, neile on juurdepääs ja neid värskendatakse, mis vastavad ettevõtte vastavuseeskirjatele ning lähtetingimustele. [18][19] Intune'is seadmete haldamiseks tuleb seadmed kõigepealt registreerida Intune'i teenuses. Intune'i haldamiseks saab registreerida nii isiklikult kui ka ettevõtte omandis olevaid seadmeid. [20]

7.3 Android mobiilse seadme registreerimine

Intune muudab Androidi Enterprise halduse seadistamise ja kasutamise lihtsamaks. Järgmiste Androidi seadmete registreerumistüüpide toetamiseks peab alguses Intune kliendikonto ühendama hallatud *Google Play* kontoga (joonis 1). Pärast Google Playga ühenduse loomist lisab Intune administraatori konsoolile levinumat Androidiga seotud

rakendust nagu näiteks *Microsoft Intune*, *Microsoft Authenticator, Intune Company Portal, Managed Home Screen.* [21]



joonis 1. Google Playga ühenduse loomine

Enne mobiilse seadme registreerimist tuleb määrata vajalikud Android reeglistikud, milleks on **konfiguratsiooniprofiilid** (*Configuration profiles*) ja **vastavuseeskiri** (*Compliance policies*). Konfiguratsiooniprofiil ja vastavuseeskiri määravad õigused, piirangud ja nõuded kasutajate registreeritud mobiilsetele seadmetele. Need kaks komponenti on haldamise oluliseks osaks. Määratud reeglistikud olenevad mobiilse seadme registrtreerimise meetodi valikust ja ettevõtte tingimustest. Mobiilsetele seadmetele määratakse antud reeglistikud ja alles siis toimub registreerimine.

Microsoft Intune'i administraatorina saab Android mobiilseid seadmeid registreerida järgmistel viisidel: [17]

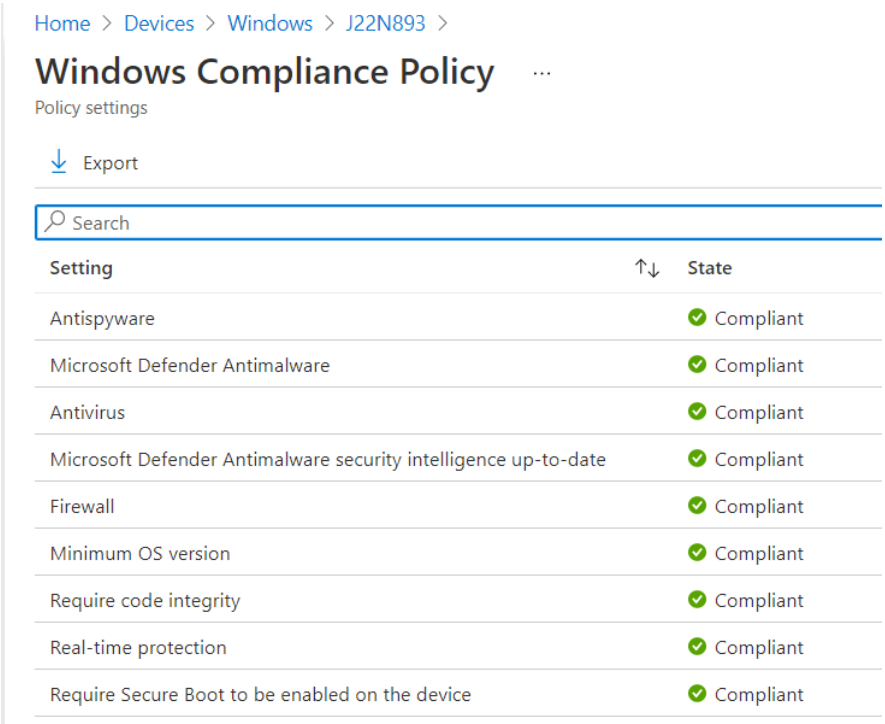
- **Android Enterprise isiklikult omandis ja tööprofiil. *Personally-owned with a work profile. (BYOD).*** Isiklikele seadmetele on antud juurdepääs ettevõtte andmetele. Administraatorid saavad hallata töökontosid, rakendusi ja andmeid. Seadmes olevaid isikuandmeid hoitakse tööandmetest eraldi ja administraatorid ei kontrolli isiklikke seadmeid ega andmeid.
- **Android Enterprise pühendatud. *Dedicated*.** Teisisõnu ettevõttele kuuluvad kioski seadmed. Ettevõtte omanduses olevatele ühekordseks kasutamiseks mõeldud seadmetele, näiteks digitaalsetele siltidele, piletite printimiseks või varude haldamiseks. Administraatorid blokeerivad seadme kasutamise piiratud hulga rakenduste ja veebilinkide jaoks. Samuti ei lase see kasutajatel seadmesse muid rakendusi lisada ega muid toiminguid teha.
- **Android Enterprise täielikult hallatud. *Full managed*.** Ettevõtte omanduses olevate ühekasutajate seadmete jaoks, mida kasutatakse ainult tööks, mitte isiklikuks kasutamiseks. Administraatorid saavad hallata kogu seadet ja jõustada

eeskirjade juhtelemendid, mis pole isikliku / ettevõtte omandis olevate tööprofiilide jaoks saadaval.

Antud lõputöö praktilises osas testis autor Android isiklikult omandis seadme ja Android täielikult hallatud seadme registreerimist ja haldamist.

7.4 Windows mobiilse seadme registreerimine ja haldamine

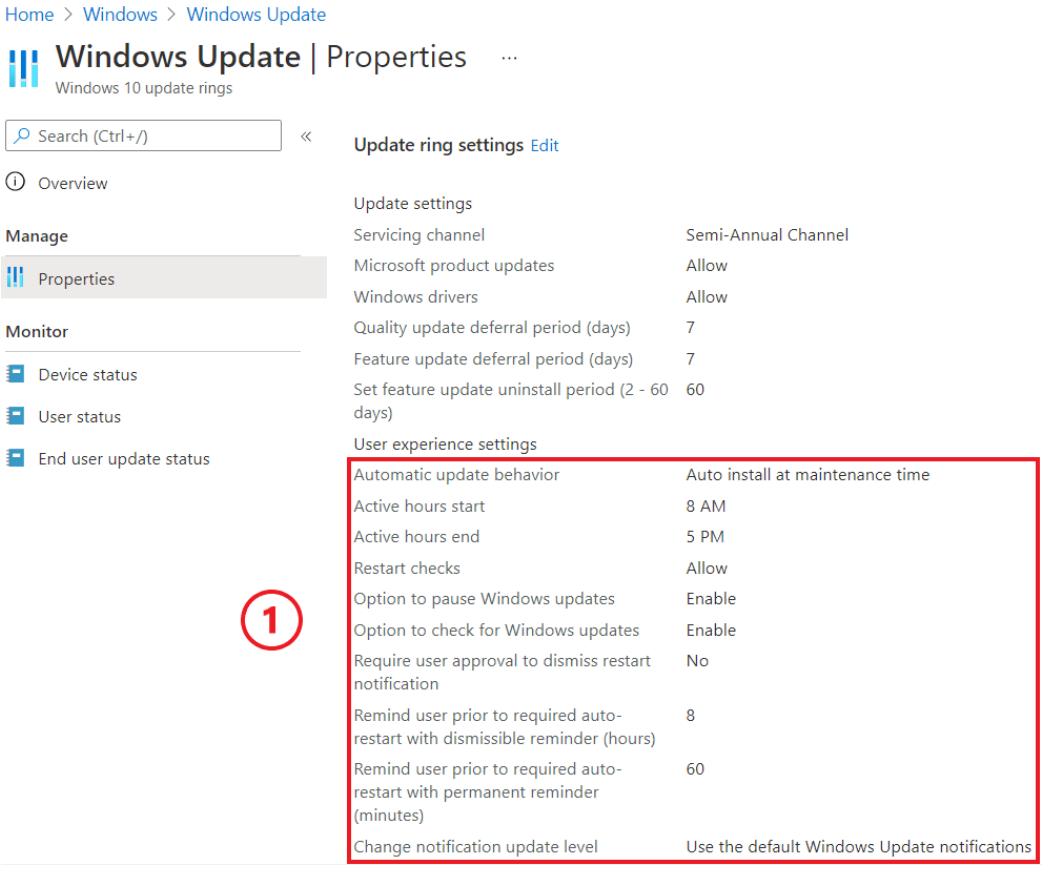
Eelduseks peavad olema ettevõttel *Azure Active Directory Premiumi* ja *Microsofti Intune* tellimused olemas. Samuti Mobiilse seadme kasutajal peab olema määratud kehtiv Intune'i litsents. [31] Täpselt nagu Androidi puhul, peab enne Windowsi seadmete registreerimist looma vajalikud reeglistikud ehk **konfiguratsiooniprofiilid** (*Configuration profiles*) ja **vastavuseeskiri** (*Compliance policies*). Vastavuseeskirjas määratakse arvuti turvataseme, näiteks Firewall, Antispyware kasutamise nõudmine (joonis 2). '*J22N893*' on Windows sülearvuti nimi. Oleku (*State*) veerus näidatakse, kas registreeritud seade vastab eeskirja komponentidele või mitte (joonis 2). Konfiguratsiooniprofiilis saab autor näiteks kasutajad vaikimisi sisse logida OneDrive sünkroniseerimise rakendusse, kasutase nende Windows mandaadi.



joonis 2. Windows Compliance Policy määramine

Windowsi seadmete haldamise võimalusteks on uuenduste laadimine arvutitele. MS Intune'i saab kasutada Windows 10 tarkvaravärskenduste paigaldamiseks haldamiseks, kasutades *Windows Update for Business* teenusest. Windows Update'i ärirakendus (*Windows Update for Business*) lihtsustab värskenduste haldamise kogemust. Süsteemiadministraator ei pea seadme rühmade jaoks üksikuid värskendusi kinnitama ja saab ettevõtte keskkonnas riske hallata, konfigureerides värskenduste levitamise strateegia. Intune võimaldab seadistada värskendus seadeid või neid edasi lükata. Samuti saab takistada seadmetel uute Windowsi versioonide funktsioonide paigaldamist, kui on vajadus. Intune pakub värskenduste haldamiseks *Windows 10 update ring* ja *Windows 10 feature updates* reeglistikud. [34]

Lõputöö autor konfigureeris *Windows 10 update ring* reeglistiku, kus määras vajalikud seadistused (joonis 3). Näiteks nendes konfiguratsioonides määratakse ajavahemik, mille jooksul saab värskendusi installida. Ajavahemik ei puuduta tööaega, värskendused ei tohiks kasutajaid töö ajal häirida. Samuti autor seadistab uuenduste teavitamise funktsiooni, mis ilmub kasutajale 60 minutit enne värskendust (joonis 3, number 1).



joonis 3. Uuenduste paigaldamise konfiguratsioonid Windows seadmele

Autor registreeris Windows seadme lubades Windows automaatse registreerimise (*Windows 10 automatic enrollment)*. Automaatne registreerimine võimaldab kasutajatel registreerida oma Windows 10 seadmed Intune'is. Registreerimiseks lisavad kasutajad oma töökonto oma isiklikele seadmetele või ühendavad ettevõtte omandis olevad seadmed Azure Active Directoryga. Taustal seade registreeritakse ja ühendatakse Azure Active Directory'ga. Pärast registreerimist hallatakse seadet Intune abil. [31]

Selleks, et Windowsi seadme registreerimine õnnestuks, pidi autor ennem tegema järgmised seadistused: [30] [31]

- Nii *Microsoft Intune'i* kui ka Microsofti Intune'i registreerimise (*Microsoft Intune Enrollment*) on näha *Azure AD* jaotises *Mobility (MDM ja MAM)*. Kui mõlemad on olemas, peab veenduma, et on seadistatud Microsoft Intune'i automaatse registreerimise sätted.

- Automaatne registreerimine (*Automatic enrollment*) on lubatud kõigile kasutajatele, kes registreerivad seadmed rakenduses Intune. *MDM user scope* peab olema määratud kui *Some* (Mõned) , et teatava gruppi kasutajad, kellel on vaja, saaksid seadme Intune'i registreerida. *MAM user scope* peab olema määratud kui *None* (Mitte keegi). Vastasel juhul on see säte *MDM scope* suhtes ülimuslik ja põhjustab probleeme.

Antud lõputöö praktilises osas testis autor Windows seade registreerimist, kasutades ***Azure Active Directory (Azure AD) Join*** registreerimise meetodi. *Azure AD Join* ühendab seadme Azure Active Directoryga ja võimaldab kasutajatel Windowsi sisse logida oma Azure AD-i mandaatidega. Kui automaatne registreerimine on lubatud, registreeritakse seade automaatselt Intune'i. Automaatse registreerimise eelis on kasutaja jaoks üheastmeline protsess. Vastasel juhul peavad nad registreeruma eraldi ainult MDM-i kaudu ja sisestama uuesti oma volitused. [32]

Kasutajad registreeruvad sel viisil kas Windowsi algse OOBE (*Out-of-box experience)* ajal või menüüst *Settings* (Seaded). Kui kasutaja on ühendanud töö omandis olev Windows seade organisatsiooni võrguga, toimuvad järgmised toimingud: [33]

- Windows registreerib kasutaja seadme organisatsiooni võrku, võimaldades töötaja isikliku konto abil töökeskkonnale juurde pääseda. Pärast seadme

registreerimist ühendab Windows seejärel seadme võrguga, et kasutaja saaks ressurssidele sisselogimiseks ja juurdepääsuks kasutada oma organisatsiooni kasutajanime ja parooli.

- Ettevõtte valikute põhjal võidakse paluda kasutajal seadistada kaheastmeline isikutuvastamise kinnitamist.

- Ettevõtte valikute põhjal registreeritakse kasutaja seade automaatselt mobiilseadmete halduse, näiteks Microsoft Intune'i.

- Organisatsiooni kontole, automaatse sisselogimise kaudu, juhitakse kasutaja läbi sisselogimise protsessi.

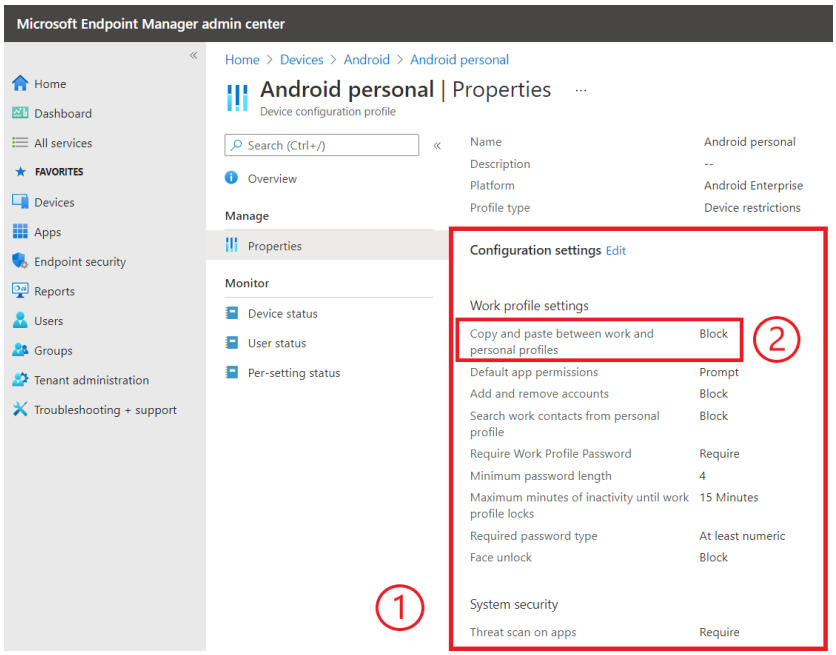
Lõputöö autor registreeris seade OOBE viisi järgi. Seade on Intune'is märgitud ettevõtte omandis olevaks seadmeks. Nüüd ettevõttel on võimalus paigaldada seadmele vajalikud rakendused, seadistada turvameetmed ning hallata seadmes olevaid tööandmeid. Kasutaja saab kasutada seade kaugtöö jaoks. Selleks, et rakendused paigaldada kasutades MS Intune'i, on vaja arvutis laadida Intune'i ettevõte portaal *(Company portal)*. Pärast seda toimub rakenduste automaatne paigaldus.

7.5 Haldamise meetodid eluliste olukordade lahendamiseks

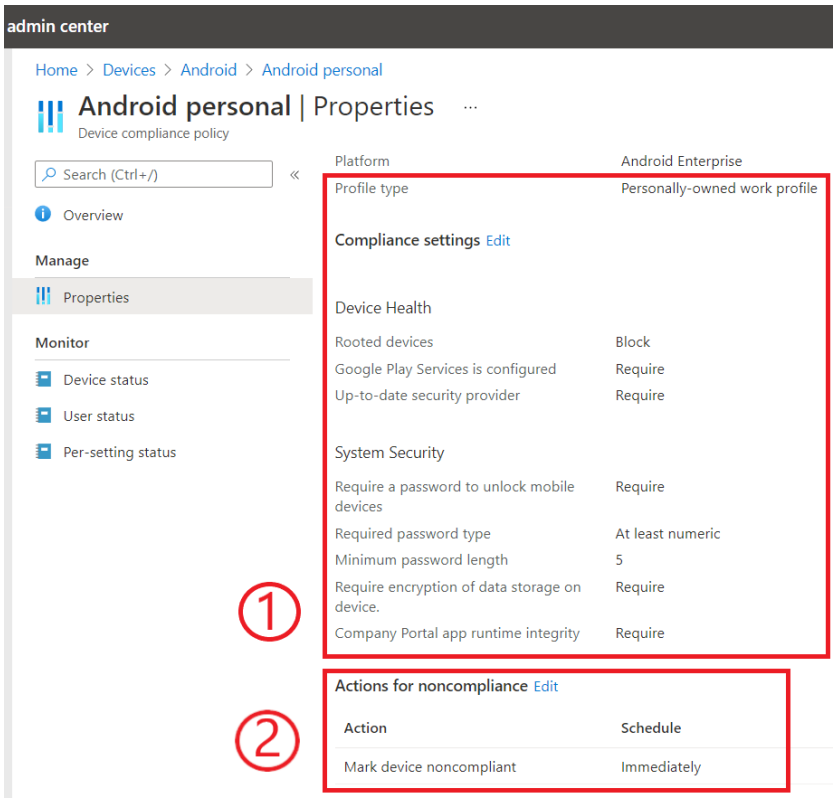
Eelnevalt esitas autor 4 erinevat olukorda, mis võivad tekkida ja kujutada ohtu ettevõtte andmetele (lõputöö peatükis 3). Selles osas näidatakse MS Intune'i abil nende probleemide lahendusi.

7.5.1 Kasutaja isiklikud andmed ja firma andmed

Probleem tekib siis, kui inimene kasutab tööks oma isikliku mobiilse seade (BYOD seade). Tavalises olukorras on võimatu kontrollida ja garanteerida, et seadme kasutaja töökeskkond on eraldatud isiklikust keskkonnast. MS Intune võimaldab lahendada BYOD seadme probleemi järgmiselt. Mobiilne seade registreeritakse kui **isiklik omand**. Selleks määratakse vastavad konfiguratsiooniprofiil (*Configuration profile*) (joonis 4, number 1) ja vastavuseeskiri (*Compliance policies*) (joonis 5, number 1). Üheks tähtsaks määramiseks on luba kopeerida andmeid tööprofiilist isikliku kasutaja profiili, mida blokeeritakse, et kaitsta ettevõtte andmeid (joonis 4, number 2). Samuti kui seade ei vasta ettevõtte määratud nõuetele, siis sellest antakse kohe teada (joonis 5, number 2).

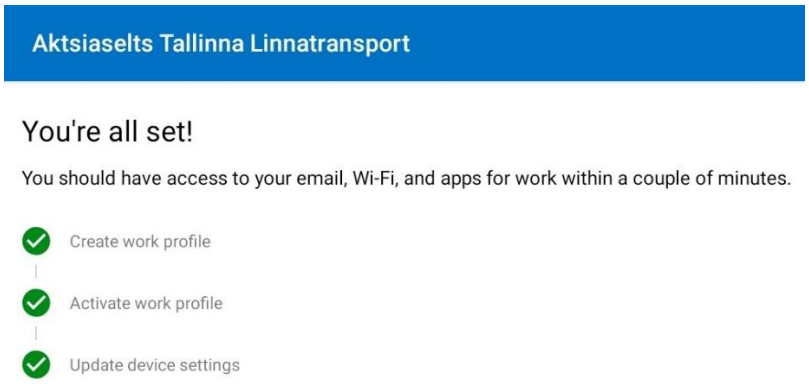


joonis 4.Configuration profile isiklikus omandis oleva seadmele määramine

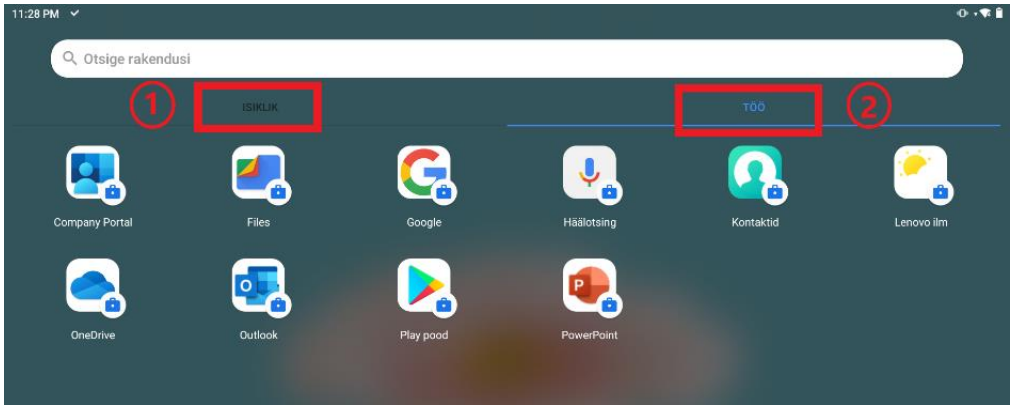


joonis 5.Compliance policies isiklikus omandis oleva seadmele määramine

Kui konfiguratsiooniprofiil ja vastavuseeskiri on määratud, seadistatakse tööprofiil mobiilsele seadmele. Tööprofiili seadistamiseks on vaja paigaldada Intune'i ettevõte portaal (*Intune Company Portal)* rakendust. Kui see on tehtud, siis kasutaja peab sisenema oma tööandja kasutaja kontoga ja läbima vajalikud seadistamise etapid.



joonis 6. Seadistamine on valmis



joonis 7. Tööprofiil on eraldatud

Pärast seadistuse läbimist näeb kasutaja järgmist akent (joonis 6), kus on näha, et kasutaja on edukalt loonud oma tööprofiili. Tööprofiil kujutab endast paigaldatud töö jaoks rakendused, mis tähistatakse töö märgiga (*work badge*) (joonis 7, number 2). Seadmel on nüüd eraldatud isiklikud rakendused töörakendustest (see kehtib ka samasuguste rakenduste puhul) (joonis 7, number 1). Selline lahendus tagab kasutaja privaatsuse ja garanteerib, et ettevõtel ei ole ligipääsu isiklikele andmetele ning ka vastupidi.

7.5.2 Mobiilse seadme kaotamine, varastamine

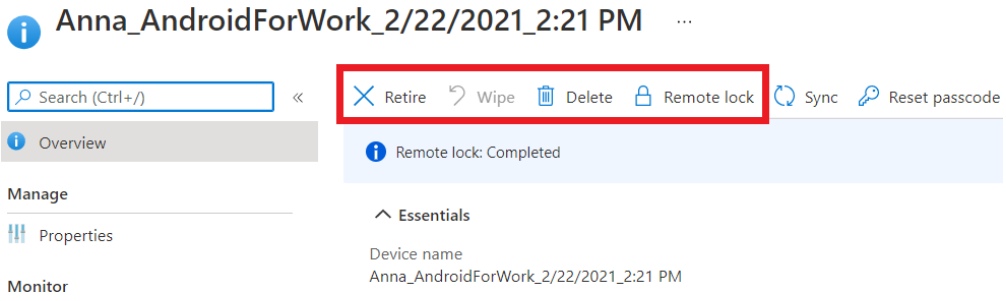
On võimatu ette näha olukorda, kus töötaja kaotab mobiilse seadme. Veelgi hullem on see, kui see varastatakse. Need on riskiolukorrad, mida peavad arvesse võtma nii ettevõtte IT-osakond kui ka seadme kasutaja. Mõlemas olukorras on ettevõtte andmed ohustatud ja keegi võõras saab neid pahatahtlikult kasutada. Juhul, kui selline olukord peaks juhtuma, MS Intune võimaldab lahendada seda järgmiselt.

Funktsioonide *Wipe* (kustutada) või *Retire* (toimingut lõpetada) abil on võimalik Intune'ist eemaldada seadmed, mida enam pole vaja, mis on ära kaotatud või varastatud. Toiming ***Wipe*** taastab seadme tehaseseaded. Kasutaja andmed salvestatakse, kui märkida

märkeruudu „Salvesta registreerimise olek ja kasutajakonto”. Vastasel juhul kustutatakse seadmest kõik andmed, rakendused ja seaded. Toiming ***Retire*** eemaldab Intune'i abil määratud hallatud rakenduse andmed, seaded ja e-posti profiilid. Seade eemaldatakse Intune'i haldusest. *Retire* jätab kasutaja isikuandmed seadmesse. [22]

1. Kui mobiilne seade on registreeritud kui **isiklikult omandis** olev seade tööprofiiliga, siis lahenduseks oleks *Retire* funktsiooni kasutamine. *Wipe* funktsioon isiklikult omandis olevatel seadmetel ei ole võimalik kasutada, see on tehtud kasutaja isiklike andmete kaitsmiseks.

2. Kui mobiilne seade on registreeritud kui **pühendunud või täielikult hallatud** seade, siis lahenduseks oleks *Wipe* funktsiooni kasutamine. Sellisel juhul võib valida, kas salvestada kasutajakonto või siis kustutada kõik andmed täielikult. *Retire* funktsioon täielikult hallatud seadmete puhul puudub.



joonis 8. Seadmest andmete eemaldamise võimalused

Ekraanipildil on näiteks toodud isiklikult omandis seadme funktsioonid (joonis 8). Samad funktsioonid on olemas kõikidel seadmete erinevatel registreerimise võimalustel. On olemas ka funktsioon ***Delete***. Kui administraator kasutab *Retire*, kuvatakse seade endiselt konsoolis, kuni käsk on edukalt täidetud. *Delete* väljastab ka käsu *Retire*, kuid erinevus on see, et *Delete* eemaldab seadme kohe Intune’st. [22] Funktsioon ***Remote block*** annab võimaluse blokeerida seadme iga hetk, kui on vaja. Pärast blokeerimist kasutaja peab sisestama parooli, et uuesti seadmesse siseneda. Täielikult hallatud seadmete puhul on olemas funktsioon ***Restart***, mis võimaldab seade taaskäivitada vajaduse korral.

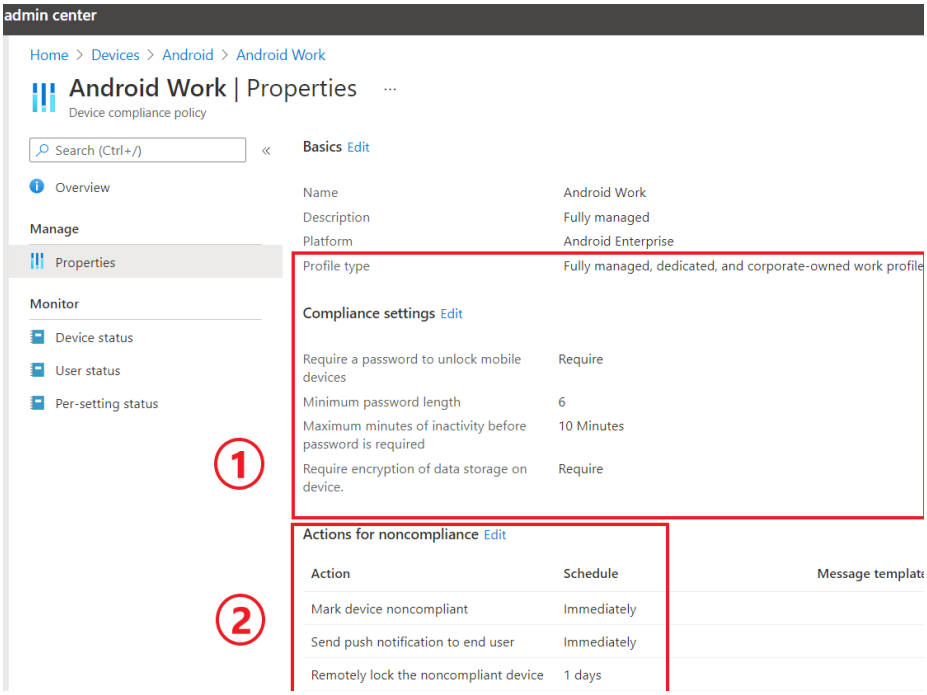
7.5.3 Töötajate lahkumine, koondamine

Kui töötajad lahkuvad töökohast, siis on vaja tagada, et tööandmed korrektselt eemaldatakse kasutajate mobiilsetest seadmetest. Lahenduseks oleks samuti kasutada kas *Wipe* või *Retire* funktsiooni, nagu 7.4.2 alapeatükkis kirjeldatud olukorras. Töötajate

lahkumine/koondamine ja seadme kaotamine/varastamine omavad üht funktsionaalsust – seadme blokeerimine ja andmete kustutamine on lahenduseks mõlema olukorra puhul.

7.5.4 Mobiilsel seadmel tööalaste andmete piisav kaitse

Seade ise peab olema krüpteeritud ja sellel peavad olema korrektsed paroolid. Paroolide olemasolu, pikkust ja turvalisust seadmesse sisselogimiseks määratakse ettevõtte nõuete järgi **vastavuseeskirjas** (joonis 5, number 1)(joonis 9, number 1). Antud funktsioonid ja konfiguratsioonid on saadaval nii isiklikult omandis olevatele seadmetele (joonis 5), kui ka täielikult hallatud seadmetele (joonis 9). Kui seade ei vasta ettevõtte määratud reeglistikule (näiteks kui puudub parool, krüpteerimine), siis seade märgitakse kui nõuetele mittevastav. (joonis 5, number 2). On võimalk seade blokeerida kas kohe, või mõni aeg hiljem (joonis 9, number 2). Selle aja jooksul peab kasutaja oma seade ettevõtte nõuetega vastavusse viima.



joonis 9. Compliance policy täielikult hallatud seadmele

8 Tulemuste analüüs

Lõputöö tulemusena paigaldati ettevõttesse MEM-i Intune teenused. Intune-teenused võimaldasid süsteemiadministraatoril hallata kasutajate igapäevatöös kasutatavaid mobiilseadmeid.

Esiteks võimaldab Intune'i kasutamine säästa nii kasutajate kui ka ettevõtte aega ja ressursse. Näiteks seadmesse täiendavate rakenduste või värskenduste paigaldamiseks ei pea kasutaja raiskama aega kontorisse tulles ja seadme süsteemiadministraatorile üle andes. Nüüd toimub juhtimine eemalt, seadmele tuleb teade ja hoiatus ning kasutaja peab lihtsalt protsessi jälgima. Üle interneti toimub paigaldamine kiiremini, mis on palju efektiivsem meetod.

Kui internetiühendust ei ole, siis ei ole ka võimalust rakendusi kasutada, kuna kõik ettevõtte teenused ja andmed asuvad pilves. See ei tähenda, et kasutaja peab alati olema internetiga ühenduses. Tööpäeva lõpuks, kui tööprofiil ei ole kasutusel, võib kasutaja vabalt teha oma seadmel vajalikud seadistused, näiteks interneti ühenduse katkestamine. Jah, sellel juhul ettevõtte ei saa andmetele reaalajas ligi, kuid mitte ainult ettevõtte, vaid ka seadme kasutaja. Ettevõtte andmeid seadmes endas hoidmine ei ole lubatud ettevõtte nõudmiste järgi. Juhul, kui seadmele on vaja uuendused paigaldada või rakendused lisada, tehakse konfiguratsioonid valmis ja saadakse seadmele käsu. Käsk ise hakkab toimima pärast interneti ühenduse loomist. Kasutajale tuleb teade sellest, millised muudatused tehakse. Töö ajal interneti ühendus peab olema kättesaadav.

Kõik registreeritud mobiilsed seadmed on MS Intune'i abil MEM'is nähtavad ja nüüd saab ka jälgida nende olekut. Näiteks värskendused ja vastavus seatud ettevõtte reeglitele. See tagab just ettevõtte nõutava kaitse ja kontrolli taseme, mis lähtetingimustes määratakse. Kui seadmel pole nõutavaid konfiguratsioone, saab ettevõte sellest kohe teada ning nõuab kasutajal sünkroniseerida oma seade määratud konfiguratsioonidega või teha vastavad muudatused/uuendused.

Samuti seadistatakse ettevõtte nõuete järgi seadmele paroolide olemasolu, nende pikkust ja keerukust. Selline funktsioon aitab tagada seadme turvalisust. Kui ettevõtte nõuab töötajaid kasutada paroole seadmetel, aga kontrollimise võimalus ettevõtel puudub, siis võib juhtuda, et kellegi parool ei ole näiteks piisavalt tugev. Need on riskid, mis võivad põhjustada andmete lekkimist. MS Intune'i abil on mobiilsete seadmete turvatase kõrgem.

Tööprofiiliga isikliku seadme lahendus võimaldab kasutajatel kasutada oma seadet tööotstarbel, minimeerides ettevõtte andmete kaotamise riski. Kasutajal võib tekkida küsimus, kuivõrd on võimalik ettevõttel isiklikule seadmele ligi pääseda, kas on olemas võimalus ekraanipildi kasutada ja sealt hallata seaded ning kas kasutaja privaatsus on ohustatud. Kuid tegelikkuses kasutajad ei pea muretsema privaatsuse rikkumise pärast, kuna ettevõttel on juurdepääs ainult ettevõtte andmetele, mis asuvad tööprofiili keskkonnas ning muud võimalused kontakteeruda isiklike andmetega ei ole. Samuti ei ole ettevõttel kaugseadmetel ekraanipildi võtmise võimalust (seda on võimalik teha ainult kontori siseste arvutitega, mis on ettevõtte omandis). Tööprofiili lahendus aitab kasutajatel seadet tõhusalt kasutada ja ettevõtte ei rikku kasutajate isiklikke piire. Ettevõte poolt on võimalus kontrollida, kuidas konfidentsiaalsed andmed seadmes kasutatakse ja kas vastavad nõuded on täidetud.

Kui mobiilne seade kaob või seda varastatakse, on Intune teenuste oluliseks osaks võimalus kustutada kasutaja, ettevõtte andmeid, tööprofiil või taastada tehaseseaded. Sellised meetodid tõstavad andmete turvalisust kasutajate mobiilsetel seadmetel. See on ettevõtte jaoks oluline juhtimis- ja kontrolli võimalus, sest iga ettevõte soovib, et andmed oleksid kaitstud ega satuks pahatahtlikele isikutele ja kolmandate isikute kätte. Kuid mis saab, kui seade ei ole võrgus? Kas sellisel juhul, kui ettevõtte ei ole jõudnud töökeskkonna eemaldada seadmest, on võimalik andmeid kätte saada?

Näiteks on võimalik seadmele ligi pääseda kasutades *Android Debug Bridge* (ADB). ADB on mitmekülgne käsurea tööriist, mis võimaldab seadmega suhelda. Adb-käsk hõlbustab mitmesuguseid seadme toiminguid, näiteks rakenduste paigaldamist ja silumist, ning failide kättesaamine. ADB ühendus saab teha kasutades Wifi või USB kaabliga. Kuid see ei ole nii lihtne, selleks on vaja eelnevalt lubada seadmel vajaliku funktsiooni ühenduse loomiseks (lubada *USB debugging* seadme süsteemi seadetes). [28] Kuigi andmed asuvad pilves, siiski võib olla tehtud rünnak, kus andmeid proovitakse

varastada. Aga kui internetiühendust ei ole, siis ei ole ka võimalust rakendusi kasutada ning andmeid kätte saada. Lisaks iga seade, mis kasutatakse töö jaoks, peab olema krüpteeritud ja sellised funktsioonid nagu *USB debugging* ei tohi olla lubatud isiklikul seadmel.

Töötajate lahkumisel/koondamisel ettevõttest tekib olukord, kus ettevõtte andmed ja kasutajakonto peavad olema isiklikust seadmest ära eemaldatud. Näiteks kui töötaja ise kustutab vajalikud andmed oma seadmest, siis ettevõtte ei saa kontrollida, kas kõik vajalikud andmed olid tõepoolest kustutatud. See on probleemiks, sest kasutaja võib unustada mingid andmed ehk eemaldamine toimub ebakorrektselt. Seega võimalus ettevõttel hallata ja kontrollida andmeid seadmetel on väga oluline osa, mida pakub just MS Intune. Ettevõtte omandis oleva mobiilsete seadmetega on olukord parem, kuna kui töötaja lahkub, tagastatakse ka vastav seade tagasi.

Windowsi seadme registreerimine võimaldas ettevõttel kasutada arvuteid kaugtöös ja ka neid hallata. Nüüd kasutavad kasutajad tööks juba konfigureeritud kontoga arvuteid, millel on kõik töö jaoks olulised rakendused. Nagu varem selgitatud, ei saa ettevõte andmeid hallata, kui kasutaja töötab oma isiklikust seadmest, ilma et sellel oleks töökeskkond, ja see on andmete kadumise oht. Samuti peab ettevõte kasutuslepingus märkima, et kasutaja hoiab tööseadmes ainult tööandmeid, kuid mitte oma isikuandmeid. Windows seadmete kasutamine kaugtöös annab võimaluse ettevõttel vabalt hallata arvuteid, olla kindel nende töövõimekuses ning selles, et andmed on turvatud.

Intune'i abil süsteemiadministraator saab Windows seadmes kontrollida vajalikke värskendusi ja kohandada nende paigaldamist. Näiteks ajavahemiku, millal saab seadmele laadida uuendused. See annab võimaluse vältida olukordi, kus uuendused hakatakse paigaldama tööajal. Selline olukord võib häirida ja aeglustada kasutaja tööprotsessi. Samuti kasutaja võib venitada Windows uuenduste paigaldamisega ning lükata edasi, mis võib põhjustada riskiolukorrad. Kui operatsioonisüsteemi ei ole pikka aega uuendatud, võivad nii rakendused, kui ka arvuti protsessid töötada halvemini. On oluline, et süsteemiadministraator saaks hallata uuenduste paigaldamist ning anda hinnangud, millised värskendused on vajalikud ja millal neid peab laadima. See võimaldab anda arvutitele ühised seadistused, mis tähendab, et ei pea igale arvutile eraldi uuendusi konfigureerima. Aega hoitakse kokku, seadistamine muutus mugavamaks.

8.1 Lähtetingimuste analüüs

Ettevõtte poolt määratud lähtetingimused ja nõuded olid suuremas osas täidetud.Tähtsam ettevõtte eesmärk oli kontrolli taseme tõstmine ehk võimalus kontrollida ja hallata mobiilseid seadmeid ning nendes olevaid andmeid.

Lähtetingimused, mis olid Microsoft Intune poolt saavutatud:

- Võimalus kasutada töötajatel oma isiklikud seadmed kaugtöös. Isiklikul seadmel on seadistatud tööprofiil, mis asub eraldi kasutaja isiklike andmetest. See tagab töötajate privaatsust ning turvalisust, kuna ettevõte haldab ainult töökeskkonnas olevaid andmeid. Samuti saab ettevõtte anda ka ettevõtte poolt täielikult hallatud seade töötajatele.

- Reeglistik määrab ära seadmete krüptimist, parooli (selle keerukust ja pikkust), autentimismeetodid. Süsteemiadministraator määrab kasutaja ligipääsu andmetele ning nende jagamise võimalust.

- Vastavuseeskiri määrab seadmele nõuded ja konfiguratsioonid, millele see peab vastama. Kui seade ei vasta nõuetele, siis annab teade nii kasutajale, kui ka ettevõttele. Pärast seda vastavuseeskiri viib seade vastavusse ettevõtte poolt määratud reeglistikuga.

- MS Intune'is on võimalik registreeritud mobiilseid seadmeid hallata ja monitoorida nende olekut. See tähendab, et süsteemiadministraator saab uuedused paigaldada ja töörakendused seadistada/kustutada. Kui tekib andmekadu oht, saab ettevõtte eemaldada seadmest tööandmeid. Näiteks isiklikul seadmel tööprofiili kustutamine, ettevõtte seade puhul saab taastada seadme tehaseseaded.

- MS Intune'is on erinevate operatsioonisüsteemide tugi. Lõputöös töötati välja lahendus Android ja MS Windows jaoks.

Lähtetingimused, mis ei ole probleemi lahendamise käigus saavutatud:

- Haldustarkvara mitmeastmeline isikutuvastus (MFA multifactor authentication). Intune saab kasutada Azure Active Directory (AD) tingimusjuurdepääsu reegleid (Conditional Access policies), et nõuda seadme registreerimisel mitme teguri autentimist (MFA), mis aitab ettevõtte ressursse kaitsta. Kuid probleemi lahendamise käigus antud lähtetingimus ei mahtunud töö skoopi, kuna tingimusjuurdepääsu reeglistik nõudis mahukat seadistamist ja testimist. Kuigi tulevikus ettevõtte saab kasutada selle Intune'i poolt pakutavat teenust, ei ole praeguseks seda realiseeritud ning ligipääsu turvameetmeteks on seadmetel paroolide määramine.

8.2 Autori panus lõputöösse

Autori töös tõstatatud probleemi lahendamises oli intervjuu läbiviimine, vajaliku tarkvara juurutamine ja kasutusele võtmine. Intervjuu kaudu sai autor teada ettevõtte probleemidest, võimalikest soovitud lahendustest ja nõudmistest. Oli püstitatud eesmärk ja arutatud tööpiirangud. See andis hea ülevaade olukorrast ning autor sai teada ettevõtte vajadused.

Pärast intervjuu läbiviimist tegi autor erinevate tarkvarade analüüsi ja võrdlust ning valis MS Intune probleemi lahendamiseks. Võib tekkida küsimus, kas autor teeb mingit erilist seadistamist või ettevõttele võib piisada vaikimisi olemasolevate konfiguratsioonidest, mida pakub valitud tarkvara? Probleem seisneb selles, et tarkvara vaikimisi seadistamisega õiget konfigureerimist teha ei ole võimalik, kuna antud probleemi lahendamine vajab järgmisi tegevusi:

- Reeglistiku määramine vastavalt ettevõtte nõuetele, mis tähendab vastavuseeskiri ja konfiguratsiooniprofiili loomist. Vaikimisi oleva seadistamisega ei ole võimalik korrektse reeglistiku luua, kuna iga konfiguratsiooni etapp vajab täpsustamist süsteemiadministraatori poolt. Muul juhul vaikimisreeglistikust ei ole mingit kasu, näiteks ei ole määratud õiget parooliseadet (millist tüüpi parool, kui pikk), seadme krüpteerimise nõuded, vajalikud täpsustused (nt. andmete jagamise blokeerimist isiklikel seadmetel). Vaikimise reeglistik ei vasta ettevõtte nõuetele ja selleks, et need oleksid korrektselt määratud, on vaja lisada vajalikud seadistused ja muudatused, millega autor tegeles.

- Kui ei ole olemas vajalikud reeglistikud, siis ei saa korrektselt mobiilseid seadmeid registreerida. Süsteemiadministraator peab tegema vastavad seadistused ja määrama, milline registreerimise viis peab olema mobiilsel seadmel. Samuti, kui seade on registreeritud, on vaja kontrollida nõuetele vastamist ning vajadusel parandada tekkivaid vigu.

Vaike seadete kasutamisega ei saa konfigureerida kõiki vajalike nõudeid,mida ettevõtte vajab. Kuigi MS Intune teeb mugavaks kogu seadistamist sellega, et paljud sammud on automatiseeritud. Näiteks ei pea kasutaja rakendused käsitsi paigaldama, samuti seotakse reeglistikud automaatselt vajaliku mobiilse seadmega. MS Intune teeb tööd mugavamaks ja efektiivsemaks, hoides kokku aega nii süsteemiadministraatori, kui ka kasutaja vaates. Kuid ise tarkvara ei saa vaikimisi tagada vajaliku kontrolli ning turvalisuse taseme. Seega ainult vajaliku tarkvara paigaldamist ja vaikimise seadmete seadistamisest ei piisa, et lõputöö probleem oleks lahendatud. Samuti selleks, et korrektselt hallata mobiilseid seadmeid, on vaja pidevat kontrolli, monitooringut ja uuendamist süsteemiadministraatori poolt.

9 Tuleviku arendused

Lõputöö probleemi lahendamine oli testitud ainult mobiilsetel seadmetel, mis töötavad Windows ja Android operatsioonisüsteemidel. Tulevikuplaanides võiks olla IOS-i ja MacOS-i mobiilsete seadmete testimine MEM keskkonnas ja testida MS Intune teenustega haldamist, mis selles lõputöös ei olnud skoopi osaks. See oleks vajalik just selleks, et laiendada mobiilsete seadmete kasutamise võimalust ja kõikidel ettevõtte pilveteenuste kasutajatel oleks võimalus tegeleda kaugtööga turvaliselt.

Samuti võib proovida MS Intune'i teiste programmidega integreerimise võimalusi. Näiteks Jamf tarkvara, mis on Apple'i ökosüsteemi juhtimisstandard. Jamf edastab Maci seadmete halduse oleku ja tervise kohta teavet Microsofti Intune'i seadmete vastavuse mehhanismile, mis integreeritakse Azure AD tingimusjuurdepääsuga, et organisatsioonid saaksid juhtimata ja nõuetele mittevastavaid Mac-seadmeid tuvastada ning neid parandada. See oleks suurepärane lahendus, et registreerida tulevikus MacOS ja IOS seadmeid mugavamalt. [23]

Kui mobiilsete seadmete registreerimise süsteem on piisavalt aega töötanud ja kasutatud, võiks ettevõtte IT osakond planeerida ja viia läbi turvatestimised. Turvatestimine on protsess, mille käigus testitakse koolitatud turvaekspertide poolt turvanõrkuste osas tarkvara (näiteks eetilised häkkerid). Sellise testi eesmärk on tugevdada tarkvaras sisalduvaid turvaauke, et häkkerite kogukond neid ära kasutada ei saaks. [24] Näiteks rakendab Microsoft jätkuvalt tehisintellekti ja masinõpet turvaprobleemide lahendamiseks ning andis välja ka avatud lähtekoodiga küberrünnaku simulaatori. [26]

Pärast turvatestimist saab läbi viia analüüsi. Näiteks Aviary on uus juhtpaneel, mille on välja töötanud CISA, et visualiseerida ja analüüsida 2020. aasta detsembris välja antud Sparrow avastustööriista tulemusi. Sparrow aitab võrgukaitsjatel tuvastada võimalikke rikutud kontosid ja rakendusi Azure/Microsoft Office 365 keskkondades. Aviary - Splunkil põhinev armatuurlaud - muudab Sparrow väljundi analüüsimise lihtsaks. [25] See tööriist annab võimaluse analüüsida Microsoft 365 keskkonna ohutegevusi.

10 Kokkuvõte

Bakalaureusetöö autor lahendas ettevõtte probleemi. Ettevõttel puudus võimalus piisavalt kontrollida ettevõtte väliseid seadmeid, mida kasutatakse töötamiseks väljaspool kontorit. Eriti puudutas see kasutajate isiklikke seadmeid, milles hoitakse töökontosid ja andmeid. Põhieesmärgiks oli luua ja testida lahendus , mis tagab töötajatele mobiilsete seadmetele kontrollitud ligipääsu pilveteenustele.

Lõputöö eesmärgi saavutamiseks autor viis läbi intervjuu ettevõtte IT meeskonna juhiga, tõi välja lähtetingimused ning nõuded tarkvarale. Teoreetilises osas autor analüüsis teaduslikke ja tehnilisi allikaid, tegi erinevate programmide võrdlust, analüüsis tulemusi ja tulemuseks valis Microsoft Intune. Praktilises osas paigaldati MS Intune teenused, määrati reeglistikud, seadistati konfiguratsioonid ja registreeriti mobiilseid seadmeid. Kui seadmete registreerimine oli tehtud, autor viis läbi haldamistestimised, kus lahendati erinevad riskiolukorrad.

Autor esitas lõputöös järgmised uurimisküsimused, millele vastas töö kirjutamise käigus:

1. Milline programm sobib kõige paremini ja vastab ettevõtte nõuetele tõstatatud probleemi lahendamiseks ? Analüüsides erinevate tarkvarade võrdluse tulemusi, oli autor valinud Microsoft Intune programm. MS Intune on hea lahendus ettevõtte probleemile, mis võimaldab hallata seadmeid vastavalt ettevõtte nõuetele ning omab endas kõik vajalikud haldamise funktsioonid.
2. Kuidas valitud programm aitab paremini kontrollida ja hallata mobiilseid seadmeid, mis kasutatakse ettevõtte kaugtööks? Microsoft Intune programm pakub hulga erinevaid teenuseid ja konfiguratsiooni võimalusi, mida saab kasutada seadmete kontrollimiseks ja haldamiseks. Nendeks võimalusteks on näiteks reeglistike seadistamine ja määramine, mobiilsete seadmete erinevad registreerimise meetodid, seadmete oleku monitooring ning kontrollitakse nende vastavust ettevõtte nõuetele. Paroolide, krüpteerimise nõudmine ja määramine. Kõige tähtsam on võimalus hallata tööandmeid kaugseadmel, mis tähendab, et riskiolukorras saab ettevõtte andmeid seadmest kustutada, kasutades Intune'i kaughaldust. Selline funktsioon takistab ettevõtte andmete lekkimise.

Lõputöö tulemuseks on ettevõttel võimalus kontrollida ja hallata mobiilseid seadmeid ning nendes olevaid andmeid turvaliselt. Samuti tagada kasutajatele kontrollitud ligipääsu ettevõtte pilveteenustele. Töötajad saavad kaugtöös kasutada oma isiklikke seadmeid, kus paigaldatakse tööprofiil ning samal ajal ei pea muretsema privaatsuse pärast. Isiklikud ja töö andmed on eraldatud, ettevõtte saab hallata ainult töökeskkonda.

Ettevõttel on haldamise testide tulemused ja kõik vajalikud ressursid, et tulevikus rakendada ettevõttes lahendus. Kirjeldatakse ka tuleviku arendused, millega saab tegeleda pärast MS Intune'i juurutamist. Kokkuvõteks autori hinnangul on lõputöös püstitatud eesmärk saavutatud.

Kasutatud kirjandus

[1] J. S. A. P. M. M. D. G. Marshall Copeland, Microsoft Azure: Planning, Deploying, and Managing Your Data Center in the Cloud, Apress, Berkeley, CA, 2015.

[2] jamf, „Jamf-Cloud,“ 2021. [Võrgumaterjal]. Available: https://www.jamf.com/products/jamf-cloud/. [Kasutatud 22 04 2021].

[3] Microsoft, „Integrate Jamf Pro with Intune for compliance,“ 24 09 2020. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/mem/intune/protect/conditional-access-integrate-jamf. [Kasutatud 22 04 2021].

[4] M. O. Ola Johansson, „Microsoft Intune Alternatives,“ 2021. [Võrgumaterjal]. Available: https://alternativeto.net/software/microsoft-intune/. [Kasutatud 22 04 2021].

[5] S. Media, „Microsoft Intune Alternatives,“ 2021. [Võrgumaterjal]. Available: https://sourceforge.net/software/product/Microsoft-Intune/. [Kasutatud 22 04 2021].

[6] M. O. Ola Johansson, „WSUS Offline Update,“ 2021. [Võrgumaterjal]. Available: https://alternativeto.net/software/wsus-offline-update/about/. [Kasutatud 22 04 2021].

[7] V. Ashiedu, „How to Use WSUS Offline Update Tool to Patch Offline Computers,“ 30 01 2021. [Võrgumaterjal]. Available: https://www.itechguides.com/wsus-offline-update/. [Kasutatud 22 04 2021].

[8] rafadelucca, „INTUNE AND WSUS,“ 09 08 2015. [Võrgumaterjal]. Available: https://rafadelucca.wordpress.com/2015/08/09/intune-and-wsus/. [Kasutatud 22 04 2021].

[9] N. Stanfield, „How To Choose Your Mobile Device Management Solution,“ 07 02 2020. [Võrgumaterjal]. Available: https://www.stanfieldit.com/mobile-device-management/. [Kasutatud 22 04 2021].

[10] M. Ltd., „Miradore,“ 2021. [Võrgumaterjal]. Available: https://www.miradore.com/. [Kasutatud 22 04 2021].

[11] L. Vetik, „Valminud on VOSK lähenemist tutvustav käsiraamat haridusjuhtidele,“ 17 11 2015. [Võrgumaterjal]. Available: https://koolielu.ee/info/readnews/473138/valminud-on-vosk-lahenemist-tutvustav-kasiraamat-haridusjuhtidele. [Kasutatud 25 04 2021].

[12] S. Media, „Microsoft Intune vs. Miradore MDM Comparison Chart,“ 2021. [Võrgumaterjal]. Available: https://sourceforge.net/software/compare/Microsoft-Intune-vs-Miradore/. [Kasutatud 22 04 2021].

[13] MobilityDojo.net, „AAD Connect,“ 2020. [Võrgumaterjal]. Available: https://aadguide.azurewebsites.net/dirsync/aadconnect/. [Kasutatud 25 02 2021].

[14] T. Inc., „Bring Your Own Device (BYOD),“ 2021. [Võrgumaterjal]. Available: https://www.techopedia.com/definition/29070/bring-your-own-device-byod. [Kasutatud 17 03 2021].

[15] Microsoft, „Cloud management gateway overview,“ 28 09 2020. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/mem/configmgr/core/clients/manage/cmg/overview. [Kasutatud 03 05 2021].

[16] M. Landman, „Managing smart phone security risks,“ *InfoSecCD 2010,* 10 2010.

[17] Microsoft, „Quickstart: Try Microsoft Intune for free,“ 14 04 2021. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/mem/intune/fundamentals/free-trial-sign-up. [Kasutatud 13 03 2021].

[18] Microsoft, „Tutorial: Walkthrough Intune in Microsoft Endpoint Manager,“ 12 04 2021. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/mem/intune/fundamentals/tutorial-walkthrough-endpoint-manager. [Kasutatud 13 03 2021].

[19] Microsoft, „Enroll Android devices,“ 09 11 2020. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/mem/intune/enrollment/android-enroll . [Kasutatud 10 03 2021].

[20] C. a. I. S. A. (CISA), „Using Aviary to Analyze Post-Compromise Threat Activity in M365 Environments,“ 08 04 2021. [Võrgumaterjal]. Available: https://us-cert.cisa.gov/ncas/current-activity/2021/04/08/using-aviary-to-analyze-post-compromise-threat-activity. [Kasutatud 03 05 2021].

[21] M. Funk, „Web Application Penetration Testing Checklist,“ 18 03 2019. [Võrgumaterjal]. Available: https://cybersguards.com/web-application-penetration-testing-checklist-updated-2019/#What_is_Penetration_Testing_or_Pen_Testing. [Kasutatud 03 05 2021].

[22] Jamf, „Jamf to Provide an Integrated Enterprise Solution to Protect Corporate Data in Collaboration with Microsoft Enterprise Mobility + Security (EMS),“ 2021. [Võrgumaterjal]. Available: https://www.jamf.com/resources/press-releases/jamf-to-provide-an-integrated-solution-with-microsoft-ems/. [Kasutatud 03 05 2021].

[23] Microsoft, „Remove devices by using wipe, retire, or manually unenrolling the device,“ 11 01 2021. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/mem/intune/remote-actions/devices-wipe. [Kasutatud 27 03 2021].

[24] Microsoft, „Connect your Intune account to your Managed Google Play account,“ 13 05 2019. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/mem/intune/enrollment/connect-intune-android-enterprise. [Kasutatud 13 03 2021].

[25] Microsoft, „Intune enrollment methods for Windows devices,“ 14 04 2021. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods. [Kasutatud 13 03 2021].

[26] A. Studio, „Android Debug Bridge (adb),“ developers, 18 02 2021. [Võrgumaterjal]. Available: https://developer.android.com/studio/command-line/adb. [Kasutatud 14 05 2021].

[27] J. A. D. M. Abubakar Bello Garba, „BRING YOUR OWN DEVICE ORGANISATIONAL INFORMATION,“ *ARPN Journal of Engineering and Applied Sciences,* 03 02 2015.

[28] M. 3. D. R. Team, „Gamifying machine learning for stronger security and AI models,“ 08 04 2021. [Võrgumaterjal]. Available: https://www.microsoft.com/security/blog/2021/04/08/gamifying-machine-learning-for-stronger-security-and-ai-models/. [Kasutatud 03 05 2021].

[29] G. Utley, „The 7 Top Microsoft Intune Features,“ 05 07 2018. [Võrgumaterjal]. Available: https://thinkred.redriver.com/top-microsoft-intune-features. [Kasutatud 14 05 2021].

[30] Microsoft, „Troubleshoot Windows 10 group policy-based auto-enrollment in Intune,“ 03 08 2020. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/troubleshoot/mem/intune/troubleshoot-windows-auto-enrollment. [Kasutatud 14 05 2021].

[31] Microsoft, „Set up enrollment for Windows devices,“ 14 04 2021. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enroll#enable-windows-10-automatic-enrollment. [Kasutatud 14 05 2021].

[32] Microsoft, „Intune enrollment methods for Windows devices,“ 12 04 2021. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/mem/intune/enrollment/windows-enrollment-methods. [Kasutatud 14 05 2021].

[33] Microsoft, „Join your work device to your organization's network,“ 03 08 2018. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/azure/active-directory/user-help/user-help-join-device-on-network. [Kasutatud 14 05 2021].

[34] Microsoft, „Manage Windows 10 software updates in Intune,“ 09 04 2021. [Võrgumaterjal]. Available: https://docs.microsoft.com/en-us/mem/intune/protect/windows-update-for-business-configure. [Kasutatud 15 05 2021].

Lisa 1 – Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks[1]

Mina, Anna Budris

1. Annan Tallinna Tehnikaülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Mobiilsete seadmete haldamine väikeettevõtte näitel", mille juhendaja on Edmund Laugasson
   1.1. reprodutseerimiseks lõputöö säilitamise ja elektroonse avaldamise eesmärgil, sh Tallinna Tehnikaülikooli raamatukogu digikogusse lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   1.2. üldsusele kättesaadavaks tegemiseks Tallinna Tehnikaülikooli veebikeskkonna kaudu, sealhulgas Tallinna Tehnikaülikooli raamatukogu digikogu kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. Olen teadlik, et käesoleva lihtlitsentsi punktis 1 nimetatud õigused jäävad alles ka autorile.
3. Kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest ning muudest õigusaktidest tulenevaid õigusi.

17.05.2021

1 Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või enam isikut oma ühise loomingulise tegevusega ning lõputöö kaas- või ühisautor(id) ei ole andnud lõputööd kaitsvale üliõpilasele kindlaksmääratud tähtajaks nõusolekut lõputöö reprodutseerimiseks ja avalikustamiseks vastavalt lihtlitsentsi punktidele 1.1. ja 1.2, siis lihtlitsents nimetatud tähtaja jooksul ei kehti.