Tallinna Ülikool

Digitehnoloogiate Instituut

MOBIILSEADMETE HALDUSTARKVARA KASUTAMINE JA TURVALISUS EESTI AVALIKU SEKTORI ASUTUSE NÄITEL

Magistritöö

Autor: Kristo Kaasan

Juhendaja: PhD Andro Kull

Autor: ..... „ ... . 2016.a.

Juhendaja: ..... „ ... . 2016.a.

Instituudi juhataja: ..... „ ... . 2016.a.

Tallinn 2016

AUTORIDEKLARATSIOON

Deklareerin, et magistritöö on minu töö tulemus ja seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud.

....

(kuupäev) (autor)

LIHTLITSENTS LÕPUTÖÖ REPRODUTSEERIMISEKS JA LÕPUTÖÖ ÜLDSUSELE KÄTTESAADAVAKS TEGEMISEKS

Mina Kristo KAASAN (sünnikuupäev: 28.11.1981)

1. annan Tallinna Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose **"Mobiilseadmete haldustarkvara kasutamine ja turvalisus Eesti avaliku sektori asutuse näitel"** mille juhendaja on Andro Kull, säilitamiseks ja üldsusele kättesaadavaks tegemiseks Tallinna Ülikooli Akadeemilise Raamatukogu repositooriumis.

2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile.

3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tallinnas, 02.05.2016

SISUKORD

MÕISTED JA LÜHENDID

Mõiste / lühend	Tähendus	Selgitus
Blacklist	Must nimekiri	Vahend soovimatu andmeliikluse tõkestamiseks, eriti rämpsposti kõrvaldamiseks: a) mitmesuguste organisatsioonide saitidel peetav spämmivate aadresside loetelu (mida võidakse tahtlike valeteadetega ka kuritarvitada), must register. b) kasutaja loodav soovimatute saatjate aadresside loetelu meileri filtris. c) soovimatute IP-aadresside loetelu marsruuteris, sh ummistusründe tõrjeks (Veldre et al., 2016).
Bluetooth	Bluetooth	WiFi sagedusalal ja raadioside standardil IEEE 802.15.1 põhinev traadita võrgu protokoll; on mõeldud kasutamiseks lühikestel mõnemeetristel vahemaadel, kuid võimalik on signaali volitamata püük ka kaugemalt (Veldre, Hanson, Laur, Buldas, & Krasnosjolov, 2016)
BYOD	Bring Your Own Device	vt. VOSK
CERT	RIA infoturbeintsidentide käsitlemise osakond	CERT Eesti tuvastab, jälgib ja lahendab Eesti arvutivõrkudes toimuvaid turvaintsidente, teavitab ohtudest ning korraldab ennetustegevusi (Riigi Infosüsteemi Amet, n.d.-a).
Dekompileerima	Decompile	kompileeritud programmikoodist lähtekoodi tuletama (Veldre et al., 2016).
DMZ tsoon	Demilitarized zone	Usaldatavat võrku ebausaldatavast, eriti organisatsiooni sisemist võrku välisest võrgust "neutraalse tsoonina" eraldav füüsiline ja/või loogiline alamvõrk, milles asuvad proksid (serverite mõlemapoolse kättesaadavuse võimaldamiseks) ja tulemüürid (Veldre et al., 2016).
EMM	Enterprise Mobility Management	Ettevõtte mobiilsuse haldus - kooslus inimestest, protsessidest ja tehnoloogiast, mis keskendub mobiilsete seadmete haldusele, traadita võrkudele ja teistele mobiilsetele arvutusseadmetele ettevõtte protsesse silmas pidades (Lua, 2015).
GPS	Global Positioning System	Ülemaailmne positsioneerimissüsteem - satelliidipõhine navigatsioonisüsteem, mis aluseks on 24 USA kaitseministeeriumi satelliiti; algselt loodi sõjaliseks otstarbeks, (Veldre et al., 2016).

IKT	Info- ja kommunikatsioonitehnoloogia	Andmete töötlemise, salvestamise ja edastamise tehniliste vahendite, meetodite ning võtete koondnimetus (Wikipedia, n.d.)
ISACA	Information Systems Audit and Control Association	Infosüsteemide Auditeerimise ja Juhtimise Assotsiatsioon - peaaegu kõigi majandusharude infosüsteemide audiitoreid, siseaudiitoreid, konsultante, koolitajaid, infoturbe spetsialiste ühendav autoriteetne kutseühing (asutatud 1969), millel on osakonnad enam kui 180s riigis; on välja töötanud infosüsteemide auditeerimise standardid, suunised ja protseduurid, tavakoodeksite kogu COBIT ja rea muid metoodilisi materjale, annab välja ajakirja ISACA Journal; tõendab IT-spetsialistide kvalifikatsiooni sertifikaatidega CISA, CISM, CRISC, CGEIT ja sarja CSX kuuluvatega (Veldre et al., 2016).
ISKE	infosüsteemide kolmeastmeline etalonturbe süsteem	ISKE väljatöötamisel ja arendamisel on aluseks võetud Saksamaa BSI (saksa k. Bundesamt für Sicherheit in der Informationstechnik, inglise k. Federal Office for Information Security) avaldatav infoturbe standard – IT Baseline Protection Manual (saksa k. IT-Grundschutz) (Riigi Infosüsteemi Amet, n.d.-a).
Jõurünne	Brute-force attack	Parooli, krüptovõtme vms mõistatamine kõigi võimalike variantide läbiproovimise teel (Veldre et al., 2016).
Juurimine	Rooting	Ülemkasutaja õiguste volitamatu omandamine (Veldre et al., 2016).
Juurkratt	Rootkit	Juurkasutaja õigustega kahjurvara, mis käivitub süsteemi igal buutimisel enne operatsioonisüsteemi täielikku laadimist ja on seetõttu raskesti avastatav; sisaldab vahendeid enda failide, protsesside ja kontode varjamiseks, näiteks failihalduri töö muutmise teel; sihtkohad pesitsemiseks on enamasti BIOS, alglaadur, opsüsteemi tuum (Veldre et al., 2016).
Lahtimurdmine	Jailbreaking	Kasutusviisi kitsenduste kõrvaldamine, näiteks mobiiltelefoni kasutamiseks teise operaatoriga või kolmandatelt pärit rakenduste installeerimiseks) ; mobiil-seadmete kontekstis on see Apple'i termin, Androidi (jt) puhul on ta vaste juurevargus (Veldre et al., 2016).
MAM	Mobile Application Management	Mobiilsete rakenduste haldus - rakenduste tasemel mobiilse seadme haldus

MCM	Mobile Content Management	mobiilne sisuhaldus lahendus - võimaldab kasutajatel juurdepääsu asutuse informatsioonile läbi nende mobiilse seadme (Terrence et al., 2015).
MDM	Mobile Device Management	Mobiilseadmete haldus - lisaks korralduslikele arvestus- ja turvameetmetele hõlmab tehnilisi meetmeid tarkvara, andmete ja konfiguratsioonide kaugseadmiseks ja -seireks (Veldre et al., 2016).
Mees vahepeal rünne	Man-in-the-middle attack - Vahendusrünne	suhtluspoolte teabevahetust manipuleeriv rünne, eeskätt autentimisprotseduuri aktiivne pealtkuulamisrünne, mille puhul ründaja valikuliselt muudab edastatavaid andmeid ja teeskleb tundliku teabe saamiseks üht sidepartneritest; kui ründaja vahetab ühe poole avaliku võtme enda omaga, saab ta dekrüpteerida tollele saadetud krüptogrammi (Veldre et al., 2016).
NFC	Near-Field Communication	Lähiväljaside - kokkupuutuvate või lähestikku (vahemaa alla 10 cm) seadmete vaheline traadita standardside (ISO/IEC 18092) (Veldre et al., 2016).
NIST	National Institute of Standards and Technology	Riiklik Standardi- ja Tehnikainstituut - USA kaubandusministeeriumi allasutus, mille infotehnoloogialabor töötab välja testimismeetodeid, teeb tehnilisi analüüse, koostab riigiasutustele ja nendega suhtlevatele ettevõtetele kohustuslikke standardeid ning annab välja olulisi metoodilisi ja juhendmaterjale infoturbe alal, eeskätt eripublikatsioonide sarjas SP 800 (Veldre et al., 2016).
Nuhkvara	Spyware	liik kahjurvara; petteprogramm või selle moodul, mis arvuti omaniku või kasutaja teadmata kogub ja saadab kolmandale poolele tundlikke andmeid kasutaja kohta (näiteks paroole, krediitkaardinumbreid, teavet käitatavate programmide, külastatavate saitide, sisestatud andmete kohta) (Veldre et al., 2016).
Petterünne	Spoofing attack	ründeotstarbeline teeskluslik elementide asendamine visuaalselt sarnastega aadressides, nimedes, liidestes jm (Veldre et al., 2016).
PSPP	Vabavaraline statistiliste andmete analüüsimise tarkvara	PSPP on tasuta alternatiiv IBM tootele SPSS - Statistical Package for the Social Sciences
RIA	Riigi Infosüsteemi Amet	Koordineerib riigi infosüsteemi arendamist ja haldamist, et riik saaks rahvast teenindada parimal võimaikul moel (Riigi Infosüsteemi Amet, n.d.-a).

Sõnaraamatu rünne	Dictionary attack - sõnastikrünne	jõurünne, mis parooli mõistatamiseks proovib mingist suurest ammendavast loendist võetud sõnu või nende kombinatsioone; võib sisaldada ettearvutust (Veldre et al., 2016).
SQL-süst	SQL injection	tarkvara nõrkusi (eeskätt sisendandmete valideerimise puudulikkust) ärakasutav rünne andmebaasipõhisele rakendusele (millel enamasti on veebipõhine liides): ründaja annab sobivalt koostatud SQL-päringu kaudu lubamatuid käske andmebaasiserverile; 2013. a. oli sagedaim veebirünne (Veldre et al., 2016).
Ummistusrünne	DDOS - Denial-of-service attack	sihilik teenusetõkestuse tekitamine, näiteks süsteemi või võrguühenduse ülekoormamisega (Veldre et al., 2016).
VOSK	Võta Oma Seade Kaasa	Tule oma seadmega Poliitika, mis lubab töötajatel või õpilastel kasutada oma isiklikke sülearvuteid, tahvelarvuteid, nutitelefone jms nii kodus kui ka tööl ja koolis (Vallaste, n.d.)
Whitelist	Valge nimekiri	musta nimekirja vastand, ainult lubatavaid meilisaatjaid, ressursse, programme, väärtusi vms loetlev filtreerimisvahend, mis tõkestab muud (Veldre et al., 2016).
WIFI	Wireless Fidelity ('traadita loomutruudus')	IEEE 802.11 sarja standarditel põhinev traadita kohtvõrgu tehnoloogia (Veldre et al., 2016).

JOONISED, TABELID JA DIAGRAMMID

1. SISSEJUHATUS

Järgnevas peatükis kirjeldab autor magistritöö uurimisprobleemi, teema aktuaalsust ning eesmärki. Samuti annab autor ülevaate uurimistöös kasutatud metoodikast ja kirjeldab magistritöö struktuuri.

1.1 Magistritöö uurimisprobleem

Maailm on kiires arenemises, kuid tehnoloogia, mida inimene loob areneb veelgi kiiremini. Ericssoni hinnangu järgi on aastaks 2020 maailmas kasutusel 9,2 miljardit mobiilside kasutuslepingut, millest 6,1 miljardit moodustavad mobiiltelefonid ning 7,7 miljardit mobiilset andmesidelepingut (Ericsson, 2015) .

Tänapäeva ühiskonnas hakkavad ära kaduma ranged piirid eraelu ja töö vahel ning koos nende piiride kadumisega ka üha enam hakatakse kasutama tööandja poolt soetatud mobiilseid seadmeid eraelulistel ja isiklikke seadmeid töö eesmärkidel.

Mobiilsus, tahvelarvutite ning mobiiltelefonide kasutusele võtmine ning nendega meie traditsioonilise arvuti väljavahetamine toob uusi väljakutseid nii ettevõtetele kui kasutajatele endile. Mobiilseid seadmeid tuleb kaitsta veelgi enam kui seda on tänaseni tehtud näiteks sülearvutite või lauaarvutite puhul. Peamiselt hakkavad muret tundma asutuste IT ja infoturbejuhid, kes märkavad, et üha enam informatsiooni liigub inimestega kaasas ja majast välja koos mobiilsete seadmetega. Radikaalseks ja kiireks lahenduseks oleks taolise tegevuse jäik piiramine ning e-postile ja dokumentidele juurdepääsu kaotamine mobiilsest seadmest, mis tooks kaasa informatsiooni liikumise alternatiivkanalites nagu Google Gmail ja Google Drive. Teiseks lahenduseks on kasutusele võtta mobiilsete seadmete haldustarkvara (MDM – Mobile Device Management), millest on välja kasvanud tänaseks juba ettevõtte mobiilsuse haldus lahendus (EMM – Enterprise Mobility Management), et tagada mobiilsete seadmete kasutamise konfidentsiaalsus, käideldavus ning terviklikkus koos kasutusmugavusega.

1.2 Magistritöö teema aktuaalsus

Töötades IT osakonna peadirektorina, näen lähedalt ohtusid, mis kaasnevad igapäevaselt asutuses mobiilsete seadmete kasutamisega. Kindlasti pole kõik avaliku sektori asutused

sellised, kus kogu informatsiooni peab kaitsma riigisaladusele vastavalt, kuid tänapäeval on isegi asutusesiseseks kasutamiseks mõeldud informatsiooni sattumine valedesse kätesse risk, mida ükski asutus ei sooviks võtta. Tulenevalt sellest ja soovist rakendada ka praktikas EMM lahendus, hakkasin koostama antud tööd teemal "Mobiilseadmete haldustarkvara kasutamine ja turvalisus Eesti avaliku sektori asutuse näitel". Antud töö koostamise hetkel ei olnud uuritud võta oma seade kaasa (VOSK) rakendamisega kaasnevad riske Eesti avalikus sektoris ja samuti puudub ülevaade MDM või EMM rakendamisest Eesti avaliku sektori asutuste hulgas. Taoline ülevaade ja hetkeseisu kirjeldamine annab asutuste infoturbe poolele ja juhtkonnale ülevaate, et kas antud valdkond on kriitilise olulisusega, kui soovitakse tagada asutuse enda informatsiooni konfidentsiaalsus. Autor tutvus magistritöö ettevalmistamisel 2015 aastal kaitstud Martin Palmi magistritööga teemal "Infoturve VOSK põhimõtte rakendamisel AS Eesti Telekomi näitel", kus Palm keskendus just VOSK vaatevinklist ning erasektori huvidest lähtuvalt infoturbe tagamisele. Kuna teaduslikku materjali ei ole MDM ja EMM teemadel palju välja antud, siis Palmi töö andis nii olemasoleva kirjanduse kui VOSK olemuse kohta väga hea ülevaate.

1.3 Magistritöö eesmärk

Magistritöö eesmärk on kirjeldada Eesti avaliku sektori hetkeolukorda seoses mobiilsete seadmete kasutamisega ja esitada praktilised soovitused, et mobiilsete seadmete kasutamine oleks turvaline ja samas kasutajasõbralik. Töö sisaldab nii online küsitlust kui EMM lahenduse praktilist rakendamist avaliku sektori asutuse (ministeeriumi) näitel, et kirjeldada lahenduse juurutamiseks vajalikke soovitusi.

Tulenevalt tööle seatud eesmärgist on koostatud uurimisküsimused järgmised:

- mil määral on Eesti avalik sektor endale püstitatud probleemi tunnistanud ja kuidas suhtuvad probleemi ja võimalikesse lahendustesse nii kasutajad kui turvalisuse eest vastutajad?
- millised ja kas on välja töötatud parimad praktikad avaliku sektori üleselt?
- millised probleemid võivad tekkida seoses EMM rakendamisega?
- milline EMM lahendus oleks Eesti avaliku sektori asutusele sobivaim?

Antud uurimustöö oodatavaks tulemuseks on kinnitus selle kohta, et avaliku sektori mobiilsete seadmete kasutajad ei ole endale tõstatanud turvalisuse probleemi, mis on vastand infoturbe eest vastutavatele isikutele. Suuremas osas ministeeriumides ei ole rakendatud MDM või EMM lahendust ja puudub poliitika mobiilsete seadmete kasutamise ja turvanõuete kohta. Magistritöö tulemusena valmib ülevaade hetkel avalikus sektoris valitsevast olukorrast, mis annab aluse riigi andmete konfidentsiaalsuse eest vastutavatele üksustele edasiste sammude tegemiseks. Samuti pakub autor välja soovitusi ettevõtte mobiilsuse halduskeskkonna rajamiseks, mille abil on võimalik juurutada EMM lahendus ka teistes asutustes.

1.4 Magistritöös kasutatud metoodika

Antud uurimistöö keskendub ühe konkreetse tehnilise lahenduse uurimisele ja seda läbi praktilise EMM lahenduse juurutamise, kui online küsitluse sooritamise nii turvalisuse valdkonna eest vastutajate kui ka lõppkasutajate hulgas. Sellest tulenevalt on tegemist kvalitatiivse juhtumiuuringuga. Juhtumiuuring on sageli seletava, avastusliku või kirjeldava olemusega ning võimaldab uurida juhtumit tema enda loomulikus keskkonnas (Pervez & Kjell, 2004), ehk siis antud hetkel MDM või EMM kasutamist avaliku sektori asutuste seas. Juhtumiuuring on eelistatud lähenemisviis, kui uuritakse reaalse elu keskkonnas aset leidvat nähtust ja kui uuritavat nähtust on raske uurida väljaspool selle loomulikku keskkonda. (Pervez & Kjell, 2004). Töötades läbi erialase kirjanduse, mis puudutab antud töö valdkonda, sain ülevaate tänastest aktuaalsetest teemadest ja lahendustest seoses MDM lahendustega. See ülevaade andis võimaluse läbi viia online küsimustik, et võrrelda parimaid praktikaid hetkel Eesti avalikus sektoris rakendatuna ning paigaldada EMM lahendus ka praktikas.

Online küsitluse viis autor läbi veebikeskkonnas, kuna see tagab kõige kiirema tagasiside küsitlusele ja võimaldab hõlmata võimalikult laiaulatusliku ja eeskujulikku valimit. Valimisse kaasati nii MDM juurutamise eest vastutavad isikud kui ka tavakasutajad. Saadud kvantitatiivseid tulemusi analüüsis autor PSPP tarkvara abil ja sai püstitatud hüpoteesid kas tõestada või ümber lükata.

Küsimustiku (vt. Lisa 1) loomisel võttis autor aluseks magistritöös esitatud eesmärgi ja küsimustik saadeti laiali kõikidele ministeeriumi IT ja infoturbejuhtidele ning samuti kaasati nii Välisministeeriumi kui teiste asutuste töötajaid andmaks ülevaadet tavakasutaja

kogemustest. Küsitluses osalejatele anti võimalus jätta oma kontaktid, et hilisemalt saada tagasisidet magistritöö tulemusest. Teistel juhtudel said osalejad kinnituse, et nende isikut ei seostata vastustega, ega ei tooda neid eraldi magistritöös välja. Küsimustik koosnes kokku kahekümneüheksast küsimusest, millest osalejad pidid vastama vaid nendele, mis tulenesid nende eelmistest vastustest. Tavakasutajatele ja valdkonna eest vastutavatele isikutele kuvati küsimustikust erinevaid küsimusi, et saada vastavalt sihtgrupile vastav tagasiside.

1.5 Magistritöö struktuur

Magistritöö koosneb kuuest peamisest etapist, millele lisanduvad eraldiseisvalt lisad ning lühendite ning mõistete selgitused.

Esimeses osas annab autor ülevaate püstitatud probleemi olemusest ja oodatud tulemustest koos magistritöö uurimismetoodika kirjeldusega. Samuti kirjeldab autor ära töö eesmärgi ning põhjenduse töö teema valikuks. **Teises osas** annab autor ülevaate mobiilsete seadmete haldustarkvara (MDM) ja ettevõtte mobiilsuse halduslahenduse (EMM) olemusest ja vajalikkusest. **Järgnevalt** kirjeldab autor erinevaid MDM lahendusi ning esitab Forresteri poolt koostatud raporti tulemused pika nimekirja kohta ning hindab lühikest nimekirja Saaty analüütiliste hierarhiate meetodi abil. Antud analüüsi aluseks on lähtutud reaalsest funktsionaalsuse vajadusest ja autor kirjeldab lisaks EMM lahenduse praktilist paigaldamist avaliku sektori asutuse näitel. **Neljas etapp** annab ülevaate läbiviidud uuringust ja selle metoodikast, mille valimi moodustasid avaliku sektori asutuste IT ja infoturbejuhid ning tavakasutajad avaliku sektori asutustest. **Viiendas etapis** analüüsib autor küsitluse tulemusi ning esitab püstitatud hüpoteeside tulemused koos järeldustega. **Viimane peatükk** annab ülevaate magistritöö tulemustest, kus autor esitab ka soovitused EMM lahenduse juurutamiseks.

Eelnevas peatükis kirjeldas autor magistritöö uurimisprobleemi, teema aktuaalsust ning eesmärki. Samuti andis autor ülevaate uurimistöös kasutatud metoodikast ja kirjeldas magistritöö struktuuri.

2. ETTEVÕTTE MOBIILSUSE HALDUSE OLEMUS

Järgnevas peatükis kirjeldab autor akadeemilisele kirjandusele toetudes ettevõtte mobiilsuse halduse lahendust. Selleks esitab autor mobiilse seadme definitsiooni ja kasutuse ülevaate ning kirjeldab EMM lahendusse kuuluvaid komponente koos mobiilsete seadmete halduslahendusega. Samuti toob autor välja MDM lahenduse ohud ja esitab pidepunktid ettevõtte mobiilsuse strateegia loomiseks.

2.1 Mobiilse seadme defineerimine

Mobiilse seadme võimalused on pidevas muutumises, seega on keeruline defineerida mõistet mobiilne seade. Kuid kuna seadmete võimalused arenevad, muutuvad ka ohud ja turvalisuse sätted, seega on vajalik kirjeldada ära põhiomadused, mille moodustavad mobiilse seadme võimalused (Souppaya & Scarfone, 2013). NIST (National Institute of Standards and Technology, Riiklik Standardi- ja Tehnikainstituut) poolt koostatud analüüsis "Guidelines for Managing the Security of Mobile Devices in the Enterprise" (Souppaya & Scarfone, 2013) defineeritakse mobiilne seade antud tööle sobivalt, milleks on:

- kujult väikese vormiga
- vähemalt üks traadita võrguliides andmesideühenduse jaoks. See liides kasutab kas WIFI, mobiilset andmesidet, või teisi tehnoloogiaid, mis ühendavad mobiilse seadme võrgu infrastruktuuriga koos interneti ühendusega või ühendustega teistesse andmevõrkudesse
- sisse ehitatud ja mitte eemaldatav andmekandja koos operatsioonisüsteemiga, mis ei ole täisfunktsionaalsusega nagu laua- või sülearvuti operatsioonisüsteemid
- võimalik paigaldada täiendavaid rakendusi

Samuti võib, kuid ei ole kohustuslik omada järgmisi funktsionaalsusi:

- üks või rohkem personaalse traadita võrgu ühendust nagu bluetooth või NFC (lähiväljaside (Veldre et al., 2016))
- üks või rohkem traadita võrguliidest kõneside jaoks

- GPS (ülemaailmne positsioneerimissüsteem) , võimaldab kasutada asukohateenuseid
- üks või rohkem foto/video salvestus seadet
- mikrofon
- sisse ehitatud võimalus sünkroniseerida andmeid teiste asukohtadega (laua- või sülearvuti, ettevõtte serverid, teenusepakkuja serveritega vms.)

Cybernetica AS poolt hallatav AKIT ehk andmekaitse ja infoturbe leksikon defineerib mobiilset seadet kui arvuti- või sidetehniline salvestusvõimeline kande- või pihuseade (sülearvuti, tahvelarvuti, pihuarvuti, mobiiltelefon, digitaalkaamera, helisalvesti vms) ISACA: ekraaniga ning puutesisestuse ja/või väikeklahvidega pihuseade massiga alla kilogrammi (Veldre et al., 2016)

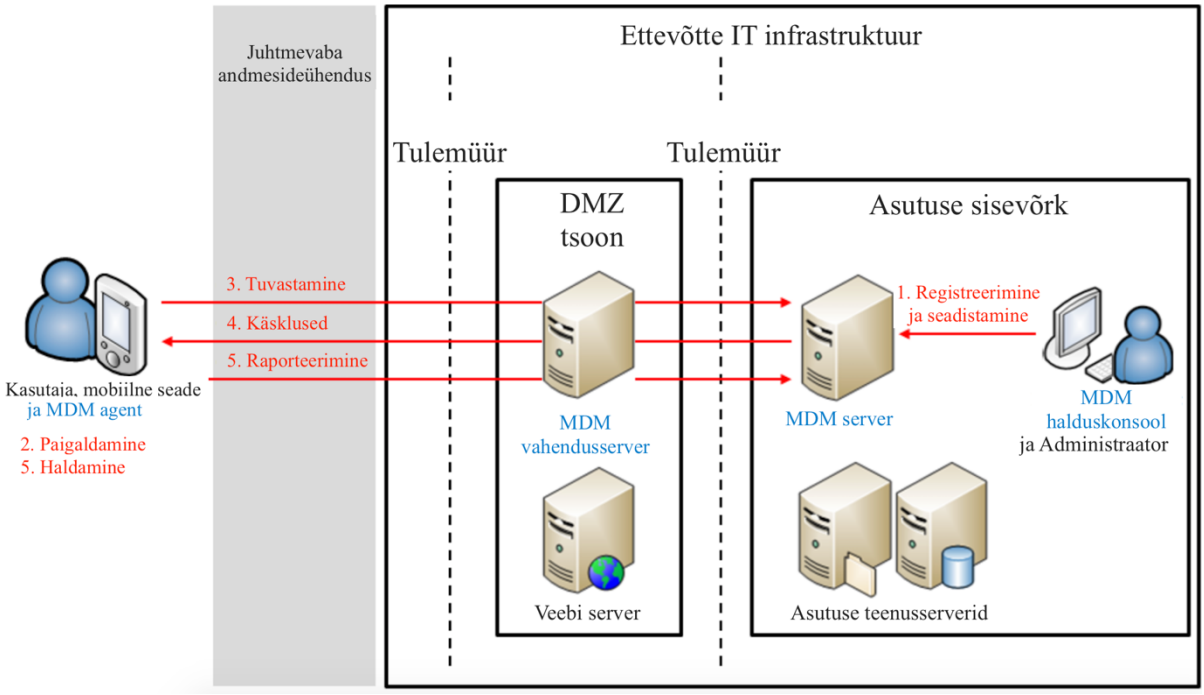
2.2 Mobiilsete seadmete kasutamine

Mobiilsete seadmete kasutamine kasvab väga kiires tempos. Mobiiltelefonide lepingute kasvu nähakse enam kui kahekordsena aastaks 2020 võrreldes tänasega. Selleks ajaks omab ligi 70% kogu maailma populatsioonist mobiiltelefoni. Samuti tasuks ära märkimist asjaolu, et internetti ühendatud seadmete arv kasvab samuti ning aastaks 2020 prognoositakse selleks koguseks 26 miljardit seadet (Ericsson, 2015).
ComScore poolt juunis 2014 läbi viidud uuringu tulemusel kasutas 57% üle kaheksateistkümne aastastest Ameerika kodanikest mobiiltelefoni igapäevaselt. Tahvelarvutite igapäevane kasutus jäi kahekümne kuue protsendi peale. Suure osa moodustas sotsiaalmeedia kasutus (34%) ning järgnes mängude mängimine (25%). Rakendustest esirinnas kõikidel platvormidel oli Facebook (ComScore, 2014).

2.3 Mobiilsete seadmete haldustarkvara

Mobiilsete seadmete haldamiseks on mitmeid erinevaid võimalusi. Vajadus seadmete kontrollimiseks ja asutuse infole juurdepääsu turvaliseks tekitamiseks, on saanud alguse VOSK (Võta Oma Seade Kaasa) ehk inglise keeles tuntud BYOD (Bring Your Own Device) laialdasest levikust. Martin Palm on oma 2015 aasta magistritöös pealkirjaga “Infoturve VOSK põhimõtte rakendamisel AS Eesti Telekomi näitel” esitanud hea teoreetilise aluse VOSK teema

mõistmiseks. Samuti andis Palm oma töös ülevaate VOSK nähtusest, võimalikest kasuteguritest, arhitektuurilistest ja tehnoloogilistest lahendustest, levinud ohtudest ning infoturbe tagamise meetmetest (Palm, 2015). Palmi töös on esitatud erinevad arhitektuurilised ja tehnoloogilised lahendused, mida VOSKi puhul organisatsioonides tüüpiliselt kasutatakse. Samuti tuuakse välja erinevate lahenduste plussid ja miinused. Üheks lahenduseks on MDM, mis on välja kujunenud traditsioonilisest laua- ja sülearvutite halduslahendustes vajadusega maandada mobiilsete seadmete laialdase kasutusega kaasnevaid riske. Tüüpiline MDM lahendus sisaldab serverrakendust, mille abil on võimalik saata sõnumeid ja käsklusi mobiilsele seadmele ja klientrakendust, mis on paigaldatud mobiilsele seadmele ja võtab käsklusi vastu. Kõik uuemad lahendused ei vaja enam klientrakendust, kuna viimane on mobiilse seadme operatsioonisüsteemi juba liidetud. Serverrakendust on võimalik paigaldada nii asutuse enda taristusse, kui ka on võimalik kasutada pilve-lahendusi (Braunstein, 2012). Tavapärane MDM tehniline lahendus asutuse enda infrastruktuuri paigaldatuna on järgnev.



joonis 1. MDM lahenduse loogiline skeem (Rhee, Jeon, & Won, 2012).

Joonisel 1 kirjeldatakse MDM lahendust, kui neljast peamisest komponendist koosnevat:

MDM agent – MDM agent kogub mobiilsete seadmete olekuinfot ja edastab selle MDM serverile. Samuti rakendab ta halduspoliitika, mis on MDM serveri poolt edastatud ja tagastab

MDM serverile informatsiooni halduspoliitika rakendamise kohta. MDM agent on paigaldatud mobiilsesse seadmesse rakenduse kujul.

MDM server – MDM server haldab registreeritud mobiilsete seadmete informatsiooni, kasutajaid ja jagab mobiilsetele seadmetele käsklusi ja rakendusi.

MDM halduskonsool – MDM halduskonsool on rakendus, mis võimaldab halduril ligipääsu MDM serverile ja hallata MDM süsteemi

MDM vahendusserver – MDM vahendusserver vahendab ning kontrollib informatsiooni voogu üksuste vahel mis ei saa turvalisuse tagamise või füüsilise asukoha pärast otse suhelda.

Suhtlus nende nelja komponendi vahel toimub järgmise viie sammuna:

Samm 1. Registreerimine/seadistamine – Mobiilse seadme ja kasutaja info registreeritakse MDM süsteemi ja igale hallatavale mobiilsele seadmele rakendatakse halduspoliitika.

Samm 2. Paigaldamine – MDM agent jagatakse ja paigaldatakse mobiilsetele seadmetele. MDM agenti on võimalik paigaldada nii seadme rakenduse poest, kui ka otse asutuse enda poolt.

Samm 3. Tuvastamine – Kui MDM agent käivitatakse peale paigaldamist, kindel mobiilse seadme informatsioon (IMEI, IP/MAC aadress, telefoni number, jmt.) edastatakse MDM serverile, et kontrollida, kas edastatud seadme info vastab süsteemis oleva registreeritud informatsiooniga.

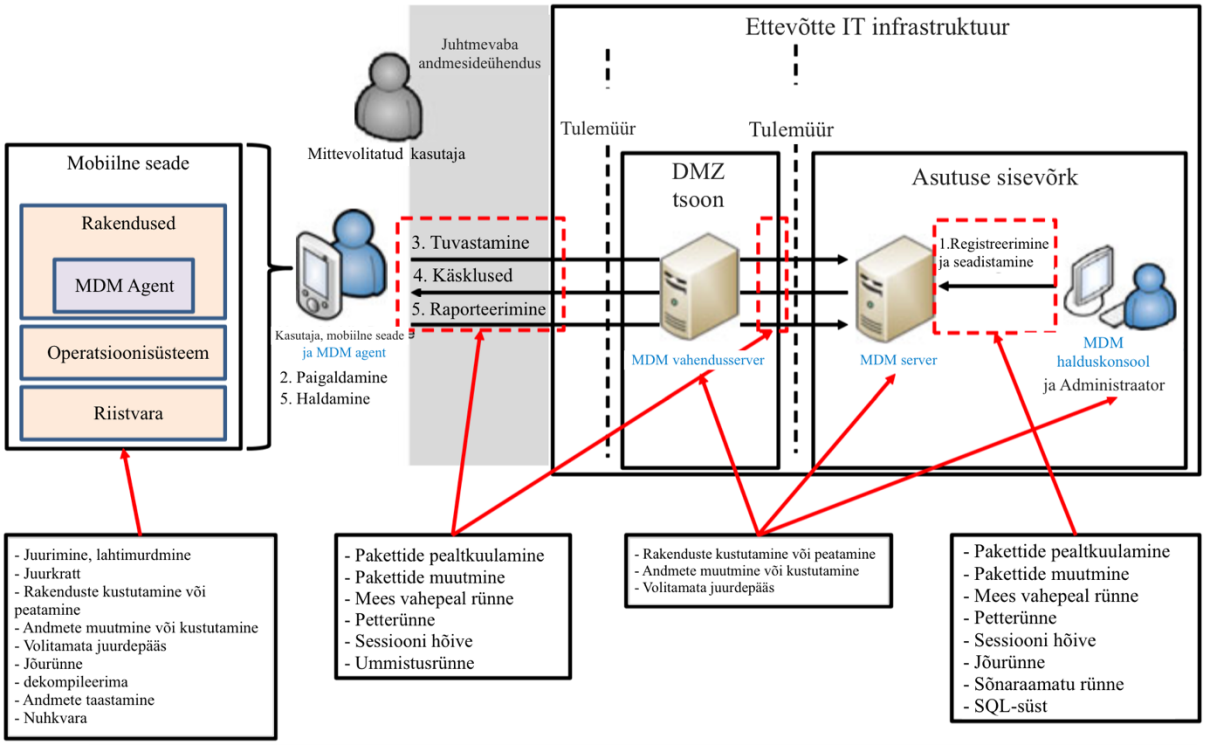
Samm 4. Käsklused – MDM server saadab igale mobiilsele seadme agendile mobiilse seadme halduspoliitika ja käsklusi tulenevalt mobiilse seadme või kasutaja olekuinfost nagu näiteks “remote wipe” ehk “kaugkustutus, mis on mobiilseadme turvafunktsioon: unustatud, kaotatud või varastatud seadmest andmete kustutamine vastava käsu saatmisega (Veldre et al., 2016).

Samm 5. Haldamine/raporteerimine – MDM agent haldab mobiilset seadet tulenevalt halduspoliitika või käskluste poolt edastatud informatsioonile ja edastab olekuinfot ja käskluste tagasisidet MDM serverile. (Rhee, Won, Jang, Chae, & Park, 2013)

MDM lahendus ei ole vajalik ainult VOSK võimaluse loomiseks vaid ka asutuste enda poolt antavate mobiilsete seadmete haldamiseks ja kontrollimiseks. Antud magistritöös ei keskendugi autor niivõrd VOSK nähtusele kui sellisele ja temast tingitud vajadusele rakendada MDM lahendus, vaid läheneb asutuse informatsiooni ja turvalisuse kaitse küsimustest lähtuvalt, jättes kõrvale mobiilsete seadmete omaniku küsimuse.

2.4 MDM ohud

Selleks, et suurendada mobiilsete seadmete turvalisust, võtavad ettevõtted kasutusele ja arendavad mobiilsete seadmete haldustarkvara lahendusi. Kui aga mobiilsete seadmete haldustarkvara on pahatahtlikult kasutatav, tekib juurdepääs nii mobiilsetele seadmete, kui ka informatsioonile, mida nad endas sisaldavad. Seetõttu on oluline teostada põhjalik ohtude hindamine ja arendada realistlik ja tähenduslik turvanõuete ja funktsionaalsuse loetelu (Rhee et al., 2013). Rhee Keunwoo, Jeon Woongryul ja Won Dongho on oma uurimistöös pealkirjaga "Security Requirements of a Mobile Device Management System" ehk Mobiilsete seadmete haldustarkvara turvanõuete loetelus analüüsinud hetkel kasutusel olevaid ohuhinnangute modelleerimise meetodeid ja pakkunud välja uue ohtude modelleerimise metoodika. Samuti esitlesid autorid kõiki võimalikke ohtusid seoses Mobiilsete seadmete haldustarkvaraga, analüüsides ja identifitseerides ohuallikaid, varasid ja kahjulikke tegevusi (Rhee et al., 2013). Lisaks asutuse informatsiooni lekkimise ohule, kaasnevad ka töötajale ohud privaatsuse rikkumise näol, kui neid ei osata õigesti maandada. Oluline on siinkohal silmas pidada, et mobiilse seadme kasutaja eraelulisele infole ei ole tööandjal õigus juurdepääsu omada ja seetõttu tuleb nii tehnoloogiliste meetmetega kui ka juhistega antud valdkond selgelt reguleerida.



Joonis 2. MDM süsteemi ohud (Rhee et al., 2013)

Joonis 2 kirjeldab kokkuvõtlikult, et millistele MDM süsteemi komponentidele millised ohud rakenduvad. Ohtude olemus on lahti kirjutatud tabelis 1. Ohuallikaid leiti olevat peamiselt kolm. Esimeseks halduskeskkonna administraator, kellel on juurdepääs kogu asutuse ressurssidele ja kelle konto hõivamisel on võimalik tekitada nii käideldavuse, konfidentsiaalsuse kui ka terviklikkuse kahju. Teise ohuallikana kirjeldasid autorid tavakasutajat, kellel on võimalus pahatahtlikult tekitada asutusele kahju. Kolmandaks ohuallikaks leiti olevat mittevolitatud kasutaja, kellel on olemas ressursid ja soov, et läbi MDM lahenduse asutuse informatsioonile juurdepääs tagada või tekitada läbi antud keskkonna muudmoodi kahju.

Tabel 1. MDM lahenduse ohtude nimekiri (Rhee et al., 2013).

Oht	Kirjeldus
Petterünne (admin kasutaja vastu)	Ohuallikas sooritab kahjuliku tegevuse edastatud või salvestatud andmetega, et omandada administraatori kasutajaõigused.
Petterünne (kasutaja/seadme vastu)	Ohuallikas sooritab kahjuliku tegevuse edastatud või salvestatud andmetega, et omandada seadme või kasutaja kasutajaõigused.
Lubamatu sisenemine	Ohuallikas sooritab kahjuliku tegevuse salvestatud andmetega, et juurde pääseda mobiilsele seadmele või MDM serverile administraatori või lubatud kasutaja õigustes.

Kasutajaõiguste muutmine	Ohuallikas sooritab kahjuliku tegevuse edastatud või salvestatud andmetega, et saada juurdepääs, mis ei ole ohuallikale määratud.
Möödaminek	Ohuallikas sooritab kahjuliku tegevuse lukustatud riistvara moodulile, et kasutada mobiilset seadet.
Ummistusrünne	Ohuallikas sooritab kahjuliku tegevuse edastatud või salvestatud andmetega, et kutsuda esile vigane toimimine.
Rikutud andmed	Ohuallikas sooritab kahjuliku tegevuse edastatud või salvestatud andmetega, et häirida uurimise läbi viimist.
MDM agendi töövõimetuks tegemine	Ohuallikas sooritab kahjuliku tegevuse MDM agendi vastu, et häirida tema tööd.
Rakenduse töövõimetuks tegemine	Ohuallikas sooritab kahjuliku tegevuse rakenduse nagu viirusetõrje või ärirakendus, et häirida nende toimimist.
Avalikustamine	Ohuallikas sooritab kahjuliku tegevuse konfidentsiaalse informatsiooni lekitamisega, milleks on administraatori kasutajatunnus või salasõna, enkrüpteeerimise/dekrüpteerimise võti, vms.
Ümberlükkamine	Ohuallikas sooritab kahjuliku tegevuse edastatud või salvestatud andmetega, et säilitada eelmised kasutaja õigused.
Moonutamine	Ohuallikas sooritab kahjuliku tegevuse rakenduse ja mobiilse seadme operatsioonisüsteemiga, et sooritada rünne.
Pahavara	Ohuallikas sooritab kahjuliku tegevuse mobiilse seadme operatsioonisüsteemiga, et paigaldada või käivitada pahavara.

Mobiilsete seadmete haldus on juba aastaid turul olnud, kuid kuna tehnoloogia areneb kiiresti, siis ei piisa tänapäeval infoturbe tagamiseks üksnes seadmete haldamisest vaid vajalik on kaitsta kogu asutuse infrastruktuuri ja keskkonda. Siinkohal tulebki kasutusele mõiste EMM (enterprise mobility management) ehk ettevõtte mobiilsuse haldus. EMM on kooslus inimestest, protsessidest ja tehnoloogiast, mis keskendub mobiilsete seadmete haldusele, traadita võrkudele ja teistele mobiilsetele arvutusseadmetele ettevõtte protsesse silmas pidades. (Lua, 2015)

2.5 EMM komponentide kirjeldus.

EMM sisaldab tavaliselt kõiki standardseid MDM võimalusi, kuid on kombineeritud lisa turvalisust ja võimalusi pakkuvate meetmetega, et moodustada veelgi terviklikum lahendus. See kõrgem turvalisuse kontroll ja kaitse annavad seadmete halduritele hallata nii seadmeid, sisu kui rakendusi, kuid samas hoides lahus ettevõtte ja personaalse info. See annab võimaluse

kasutada töötajatel nii isiklikke seadmeid töö juures, kui töö seadmeid isiklikuks otstarbeks ja kartmata sealjuures, et need kaks läheksid omavahel segi või et ettevõte saaks kontrolli isiklike andmete üle. Lisatud funktsionaalsus EMM lahenduse puhul sisaldab seadmete kasutuse monitooringut, seadme logisid ja ühilduvust asutuse infrastruktuuri lahendusega kuni võimalusena pakkuda kasutajatele asutuse enda rakendusi. (Lua, 2015)

Lisaks MDM funktsionaalsusele sisaldub EMM lahenduses veel mobiilsete rakenduste haldus (MAM - mobile application management). MAM rakendab haldus ja poliitika halduse funktsionaalsust eraldiseisvatele rakendustele, mida jagatakse asutuse rakenduste poe kaudu ja hallatakse lokaalselt mobiilses seadmes eneses läbi EMM haldusliidese. See funktsionaalsus on vajalik, kui seadme operatsioonisüsteem ei taga piisaval tasemel haldus ja turvameetmeid, või kui asutus ei soovi paigaldada seadmesse MDM agenti. MAM pakub samuti analüüsi võimalusi, et aidata lahenduse administraatoritel ja rakenduste omanikel saada ülevaadet rakenduste kasutamise kohta. MAM ja MDM funktsionaalsusi saab kasutada koos ja teineteist täiendavana. (Terrence et al., 2015)

Kolmandaks elemendiks EMM lahenduses on mobiilne identiteet, mis aitab tagada ainult volitatud seadmete ja kasutajate juurdepääsu asutuse rakendustele. Mobiilne identiteet võib endast kujutada ühte või rohkemat järgmistest tehnilistest lahendustest: Kasutaja ja seadme sertifikaadid, rakenduse koodi allkirjastamine, kastaja tuvastamine ja ainulogimisega pöördus, mis on pääsu reguleerimise funktsioon, mis võimaldab kasutajal pöörduda üheainsa logimisega paljude eri ressursside poole (Veldre et al., 2016). EMM vahendid hakkavad ühe enam kasutama kontekstilist informatsiooni (nagu asukoht ja aeg), et määrata juurdepääsuõiguseid (Terrence et al., 2015).

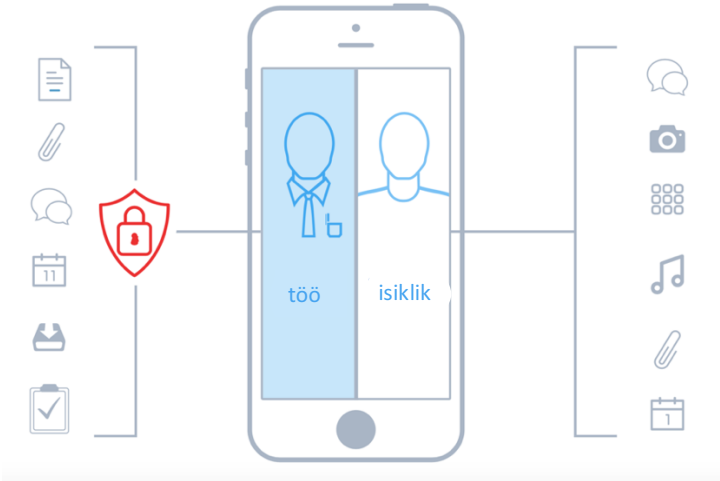
Viimase komponendi EMM lahenduses moodustab mobiilne sisuhaldus lahendus (MCM - Mobile content management). MCM võimaldab kasutajatel juurdepääsu asutuse informatsioonile läbi nende mobiilse seadme. MCM lahendusel on neli peamist funktsiooni:

- kliendipoolne rakendus, mis võimaldab kasutajal turvaliselt hoida informatsiooni oma mobiilses seadmas.. EMM saab rakendada poliitikaid kasutaja tuvastamise, dokumentide jagamise ja kopeerimise piirangute kohta. Andmed laekuvad erinevatest sisenditest, nagu e-post, asutuse failiserver või pilveteenustest.

- informatsioonile juurdepääs, mis tagab ühenduse asutuse infrastruktuuris oleva serveriga, kust on võimalik alla laadida sisu mobiilsesse seadmesse.
- informatsiooni levitamine, mis võimaldab mobiilsetesse seadmetesse andmeid keskselt ülesse laadida, asendada või kustutada.
- dokumentide tasemel õiguste kontroll, ei ole EMM lahendustes küll täisväärtuslik andmete kao vältimisele mõeldud lahendus, ega paku professionaalset informatsiooni õiguste haldust, kuid siiski on võimalik teatud piiranguid kataloogide ja faili tasandil määrata. (Terrence et al., 2015)

2.6 Ettevõtte mobiilsuse strateegia

Peamine väljakutse on koostada õige ettevõtte mobiilsuse strateegia, mis oleks seotud olemasolevate IKT ressurssidega ja töö üldise eesmärgiga. Strateegias peab olema kirjeldatud, et kui tihedalt ettevõtte äriprotsessid on seotud mobiilse IKT strateegiaga ja kuidas toetada mobiilseid töötajaid, kui nad kasutavad mobiilseid seadmeid oma töökohal. (Lua, 2015)



joonis 2. EMM lahendust illustreeriv joonis (Lua, 2015).

Ettevõtte mobiilsuse haldamise strateegia loomisel tuleks silmas pidada järgmist viite punkti:

- **töötajate peamine eesmärk on produktiivsus – mitte turvalisus**

  Töötajad kasutavad mistahes rakendusi, mis abistavad nendel saavutada endi eesmärke. Suutlikus on kõige olulisem, see aga tähendab, et turvalisus kannatab.

- **tarbija jaoks loodud rakendused on nagu sõel ettevõtte andmete kaitsel**

  Sa ei tea kunagi, kuhu tarbija rakendused salvestavad ettevõtte andmeid. Kasutada on vaja rakendust, mis on loodud ettevõtte jaoks.

- **mobiilsed töötajad ei kasuta kunagi sisse ehitatud rakendusi**

  Töötajad kasutavad seda, mis töötab paremini. Anna oma töötajatele tänapäevane ja kasutajasõbralik lahendus ning jälgi kuidas töö produktiivsus kasvab ja töötajate rahulolu suureneb.

- **töötajatel ja IT'l on omad selged mobiilsed vajadused**

  Töötajad vajavad nähtamatud jagamist – IT vajab turvalisust

  Töötajad vajavad mobiilseid töövoogusid – IT vajab lihtsaid lahendusi

  Parim lahendus töötab ja toimib mõlema osapoole jaoks

- **rakenduste musta nimekirja omamine ei ole jätkusuutlik**

  Rakendusi uuendatakse pidevalt ja hoida nimekirja võimalikest mitte lubatud rakendustest ei ole mõistlik ega võimalik.

Ettevõtte mobiilsuse haldus ei ole piiritletud üksnes arvutite, tahvelarvutite või mobiiltelefonidega. Targad seadmed, grupeerides neid nimetuse taha "Internet of Things" (IoT), ehk esemevõrk, mis on füüsiliste objektide (seadmete, toodete, taimede jms) ühese automaatse identifitseerimise ja nende virtuaalesituste võrgustuse kontseptsioon (Veldre et al., 2016), moodustavad lähitulevikus suure osa ettevõtte mobiilsuse haldamisest. Seadmed nagu Apple TV, printerid, nutikellad on ühed vähesed näited esemevõrgu seadmetest, mida on võimalik hallata juba täna EMM vahendite abil. (Terrence et al., 2015)

Eelnevas peatükis kirjeldas autor akadeemilisele kirjandusele toetudes ettevõtte mobiilsuse halduse lahendust. Selleks esitas autor mobiilse seadme definitsiooni ja kasutuse ülevaate ning kirjeldas EMM lahendusse kuuluvaid komponente koos mobiilsete seadmete halduslahendusega. Samuti tõi autor välja MDM lahenduse ohud ja esitas pidepunktid ettevõtte mobiilsuse strateegia loomiseks.

3. EMM LAHENDUSTE ÜLEVAADE

Järgnevas peatükis kirjeldab autor Forresteri raportile tuginedes populaarsemaid EMM lahendusi ning esitab Forresteri poolt koostatud hindamistabeli koos joonisega. Lisaks kirjeldab autor EMM lahenduse praktilist rakendamise protsessi avaliku sektori asutuse näitel ning teeb selle tulemusest kokkuvõtliku ülevaate.

Järgnevalt annab autor ülevate turul olemasolevatest EMM lahendustest ja esitab Forresteri raporti kokkuvõtte EMM funktsionaalsuste võrdlemisel. Forresteri raport koosneb kahekümne viiest erinevast hindamise kriteeriumist ja nende abil analüüsiti üheteistkümmet erineva toodet, kuhu hulka kuulusid: AirWatch by VMware, BlackBerry, Citrix, Good Technology, IBM, Landesk, Microsoft, MobileIron, SAP, Sophos, ja Soti (Kane, 2015).

Tooteid hinnati kolmes suuremas kategoorias:

Võimaluste ülevaade - Selles jaotuses hinnati, et kuidas EMM lahenduste võimalused aitavad kaasa ettevõtete mobiilsuse tagamisele koos erinevat tüüpi seadmete, rakenduste ja teenuste kasutamisega. Hinnati tootjaid nii väljatöötamise, toimivuse, arvutite halduse, operatsioonisüsteemide toe, võrgu turvalisuse, aruandluse, analüütika, rakenduste halduse, kulude halduse, rakenduste turvalisuse, konteinerlahenduste ja andmete halduse ning kasutajate juurdepääsukontrolli koos turvaliste rakenduste alusel

Strateegia – Et saada ülevaade ettevõtte sihist, hindas Forrester iga tootja strateegiat, tehnoloogilist visiooni, teekonna agressiivsust, partnerite ekosüsteemi, toetatavaid tooteid ja teenuseid, kasutajakogemust ning klientide kindlust tootja visiooni.

Esindatus turul – Hinnati turul esindatust klientide arvu, paigaldatud lahenduste, tulu ning globaalse haarde alusel.

Hindamine viidi läbi viie palli skaalal. Järgnev tabel sisaldab hinnatud toodete täpset versiooni ja tooteinfot:

Tabel 2. Forresteri poolt hinnatud EMM lahendused (Kane, 2015).

Tootja nimi	Toote nimi	Toote versioon
AirWatch by VMware	AirWatch Enterprise Mobility Management	8.1
BlackBerry	BES12	12.2
Citrix	XenMobile	10
Good Technology	Good Secure Mobility Solution	N/A
IBM	MobileFirst Protect	10.50, September 2015
Landesk	Landesk Mobility Manager	9.6
	Wavelink Avalanche	6.1
Microsoft	Enterprise Cloud Suite (sisaldab EMS and Office 365)	N/A
MobileIron	MobileIron	V8
SAP	Mobile Secure	3.2
	Mobile App Protection	3.3
	Mobile Documents	1.4
Sophos	Sophos Mobile Control (SMC)	5.1
	Sophos Cloud - Mobile	v.3
Soti	Soti MobiControl	12.3

Tootja valiku kriteeriumid

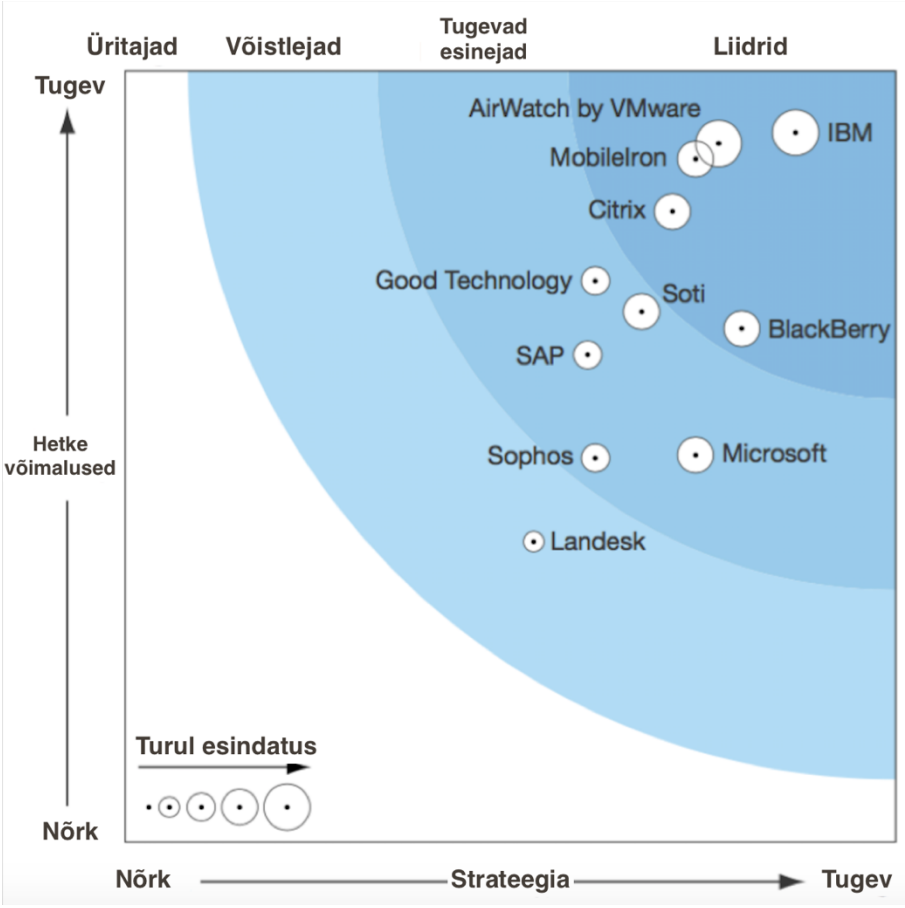
Komponendid, mis olid saadaval 2. septembri 2015 aasta seisuga. Funktsionaalsus, mis avaldati peale seda kuupäeva, ei olnud kaasatud hindamise protsessi, kuid võeti arvesse strateegilise visiooni hindamises. Enamus toodetest on peale hindamise kuupäeva välja lasknud uuendusi ja seega Forrester soovitab huvilistel küsida tootjatelt viimaste uuenduste sisu kohta.
Tõestus turul püsimajäämise kohta. Tootja peab tegema rohkem kui kümne miljoni USA dollari väärtuses käivet aastaselt mobiilsete seadmete halduslahendustega seotult ja peab omama üle 100 kliendi koos üle 3000 hallatava seadmega.
Mõttesamasus Forresteri klientide hulgas. Hinnati tootjaid, keda mainiti Forresteri päringutes, lühikestes nimekirjades, konsultatsiooni projektides ja näidislahendustes.

3.1 Forresteri EMM toodete hindamistabel

Tabel 3. Forresteri EMM toodete hindamistabel (Kane, 2015).

	Forresteri osakaalud	AirWatch by Vmware	BlackBerry	Citrix	Good Technology	IBM	Landesk	Microsoft	MobileIron	SAP	Sophos	Soti
HETKE FUNKTSIONAALSUS	50%	4.53	3.33	4.09	3.64	4.60	1.95	2.51	4.43	3.16	2.49	3.44
Paigaldus ja kasutusmugavus	7%	3.00	3.00	3.00	3.00	5.00	2.00	1.00	3.00	2.00	3.00	3.00
PC/Mac haldus	8%	5.00	1.00	3.00	1.00	5.00	5.00	3.00	5.00	3.00	0.00	5.00
Op. süsteemide tugi	7%	5.00	3.00	4.00	4.00	5.00	3.00	3.00	5.00	3.00	2.00	4.00
Mobiilsete seadmete haldus (MDM)	5%	5.00	3.00	5.00	3.00	5.00	3.00	3.00	5.00	3.00	3.00	3.00
Andmesidevõrgu turvalisus	7%	4.00	3.00	4.00	4.00	4.00	2.00	0.00	4.00	4.00	3.00	4.00
Raporteerimine ja analüüs	6%	5.00	4.00	5.00	5.00	5.00	2.00	2.00	5.00	1.00	2.00	5.00
Sidekulude haldus (TEM)	7%	3.00	5.00	3.00	5.00	5.00	0.00	0.00	5.00	1.00	1.00	1.00
Konteinerlahendus	6%	5.00	5.00	5.00	3.00	5.00	2.00	2.00	5.00	5.00	1.00	5.00
Rakenduste haldus	7%	5.00	4.00	4.00	5.00	4.00	3.00	4.00	5.00	3.00	3.00	3.00
Rakenduste turvalisus	6%	4.00	2.00	3.00	4.00	4.00	2.00	2.00	4.00	2.00	4.00	4.00
Ettevõtte poe laiendatavus	8%	5.00	3.00	4.00	2.00	4.00	1.00	4.00	4.00	4.00	3.00	2.00
Ettevõtet poe kasutuskogemus	6%	5.00	2.00	5.00	5.00	5.00	2.00	2.00	5.00	5.00	2.00	2.00
Andmete haldus ja turvalisus	6%	4.00	4.00	4.00	2.00	4.00	0.00	4.00	4.00	3.00	4.00	4.00
isiku ja juurdepääsukontroll	6%	5.00	3.00	5.00	4.00	4.00	1.00	2.00	5.00	3.00	4.00	4.00
Turvalised kontoritarkvara rakendused	8%	5.00	5.00	5.00	5.00	5.00	1.00	5.00	3.00	5.00	3.00	3.00
STRATEEGIA	50%	3.85	4.00	3.55	3.05	4.35	2.65	3.70	3.70	3.00	3.05	3.35
Tehnoloogiline visioon	20%	4.00	4.00	4.00	4.00	4.00	2.00	4.00	4.00	3.00	3.00	3.00
Tulevikuplaanide julgus	15%	4.00	5.00	5.00	4.00	5.00	5.00	5.00	4.00	4.00	3.00	3.00
Partnerite ekosüsteem	15%	3.00	4.00	3.00	3.00	3.00	1.00	4.00	5.00	2.00	3.00	3.00
Toetatud tooted ja teenused	15%	3.00	3.00	1.00	1.00	5.00	1.00	1.00	1.00	3.00	1.00	3.00
Kasutajakogemus	20%	4.00	4.00	4.00	3.00	5.00	3.00	4.00	4.00	3.00	4.00	4.00
Klientide kindlus visiooni	15%	5.00	4.00	4.00	3.00	4.00	4.00	4.00	4.00	3.00	4.00	4.00
TURU OSAKAAL	0%	4.25	4.00	3.75	2.75	4.25	1.50	3.50	3.25	2.75	2.50	3.25
Klientide arv	25%	5.00	3.00	4.00	4.00	5.00	3.00	4.00	4.00	3.00	3.00	5.00
Installatsioonide arv	25%	4.00	5.00	4.00	2.00	5.00	1.00	3.00	3.00	3.00	3.00	4.00
Käive	25%	3.00	3.00	3.00	3.00	3.00	1.00	3.00	3.00	2.00	1.00	1.00
Globaalne esindatus	25%	5.00	5.00	4.00	2.00	4.00	1.00	4.00	3.00	3.00	3.00	3.00

Asetades selle tabeli graafiku kujule tekib hea ülevaade hetkel turul valitsevast olukorrast. Autor on tutvunud ka Gartneri poolt loodud uuringuga (vt. joonis 3) ja saab kinnitada, et liidrite positsioonid on mõlemal juhul sarnaselt hinnatud. Taolised analüüsid ja hinnangud on hea alguspunkt asutusele oma toote ja lahenduse välja valimiseks.



Joonis 3. The Forrester Wave (Kane, 2015).

3.2 Forresteri EMM lahenduste raporti kokkuvõte

IBM, AirWatch by VMware, MobileIron, citrix, ja BlackBerry juhivad karja. Need tootjad esitlesid turgu vedavaid strateegiaid ja pakkusid nii mobiilide kui arvutite halduslahendusi, ohtude haldust kui ka töövoogude lihtsustamist. IBM'i terviklik haaratus koos tugeva partneri ja teenustena, katab enamuse klientide vajadustest. AirWatch'i meelekindlus, et lihtsustada mobiilsust klientide jaoks, loob neile võimaluse kasutada parimatid praktikaid ja arendada selge strateegia muutumiseks. MobileIron'i lihtne sidusus parimate lahendustega julgeoleku või analüütika valdkonnas tähendab klientidele, et nad ei pea tänastest partneritest või toodetest loobuma, et rakendada mobiilsete seadmete haldustarkvara. Citrixi keskendumine produktiivsusele ja kasutaja kogemusele tähendab tugevaid ärirakendusi ja äriprotsesside muutumisi. BlackBerry tugev võrgu ja andmete turvalisus koos hiljuti omandatud ettevõtte Good technology konteinerlahendusega uute seadmete ja rakenduste jaoks, suurendab veelgi juhtpositsiooni. (Kane, 2015)

Soti, Good Technology, Microsoft, SAP, ja Sophos pakuvad häid lahendusi. Igaüks antud nimekirjast võistleb ühe kindla lahendusega, mis katab teatud kliendi vajadused. Samas jääb kõigil puudu teatud võimalustest, mis võimaldaks neil turu liidriks pürgida. Soti ühilduvus oma riistvara ja turvatoodetega, muudab ta tugevaks lahenduseks android ja "sitkete" seadmete hulgas. Microsofti tugev identiteet, andmete turvalisus ja ühilduvus Microsofti seadmete haldusega, muudab ta tugevaks valikuks juba Microsofti lahendusi kasutava kliendi jaoks. SAPi rakendused, analüütika ja rakenduste arendus pakuvad tugevaid lahendusi neile, kes otsivad mobiilseid äriprotsesse. Sophose ühendatud ohtude haldus loob kliendile hea ülevaate ja halduse kõikide kasutatavate seadmete jaoks, mida tööks kasutatakse. (Kane, 2015)

Landesk langeb ringist välja ja jääb võistlejaks. Landeskil on tugev arvuti ja Maci haldusvõimekus, nagu ka "sitkete" ja "pool-sitkete" seadmete tugi. Ta on samuti teinud mitmeid soetusi seadmete haldusega, turvalisusega ja analüütikaga seoses ja loonud nendest ühise visiooni. Forrester ootab, et Landesk areneb läbi mitme valdkonna ja tulevikus nende positsioon tõuseb. (Kane, 2015)

3.3 EMM lahenduse praktiline rakendamine

Magistritöös esile toodud meetodite ja lahenduste testimiseks pidas autor vajalikuks läbi viia praktiline EMM keskkonna paigaldus. Praktiline lahenduse rakendamine annab võimaluse uurida nähtust tema loomulikus keskkonnas, mis toetab samuti magistritöös kasutatavat juhtumiuuringu metoodikat. Juhtumiuuring on eelistatud lähenemisviis, kui tuleb vastata kuidas- ja miks-küsimustele, kui uurija kontrollib sündmust vaid vähesel määral ja kui fookuses on reaalse elu kontekstis jooksev nähtus (Pervez & Kjell, 2004).

3.3.1 Ministeeriumi ja probleemi kirjeldus

Ministeeriumi näol on tegemist avaliku sektori asutusega, kelle missiooniks on Eesti julgeoleku ja heaolu kindlustamine ning huvide kaitsmine maailmas välispoliitika kavandamise ja teostamise ning välissuhete koordineerimise teel.

Ministeeriumi arengukava peamisteks eesmärkideks on:

- Julgeoleku kindlustatus ja jagamatus, rahvusvaheliste suhete stabiilsus ja ennustatavus;
- Eesti majanduse toimimise eelduste tagamine, liberaalsed majandussuhted ja majandusruum;
- Eesti isikute kaitse välismaal ja välissuhetes;
- Eesti mõjukus ja hea maine;
- Demokraatiat, inimõigusi, õigusriigi põhimõtteid, majandusvabadusi ja arengut edendav väärtuste ruum;

(Välisministeerium, 2014)

3.3.2 Probleemi kirjeldus

Ministeeriumis töötab üle 600 inimese, kellest pooled resideeruvad välisriikides ja enamustel on kasutusel üks kuni kaks mobiilset seadet (telefon või tahvelarvuti). Üha suureneva hulga informatsiooni viimine mobiilsetesse seadmetesse, on kasvatanud riski informatsiooni turvalisuse ja lekkimise osas. Täna on ministeeriumis kasutusel palju erinevaid mobiilsed platvorme, millede jaotuskava on järgmine:

- 60 % Android (HTC, Samsung, Sony, Google, Motorola);
- 30 % iOS (iPhone, iPad);
- 10 % Windows phone;

Tänases olukorras on ainukese haldusvahendina kasutusel Microsoft Exchange ActiveSync teenus, mille abil on võimalik registreerida telefone süsteemi külge, neid eemaldada ja taastada tehase sätteid.

Probleem seisneb selles, et lisaks ministeeriumi kirjavahetusele on telefon kasutusel ka era otstarbel ja nagu on selgunud viimasest nutiseadmete turvalisuse teadlikkuse uuringust, ei ole kasutajad alati just kõige hoolsamad. Suurimad riskigrupid on just Androidi kasutajad, kuna Google play poest on kõige kergem alla laadida pahavara sisaldavaid app'e. Windows'i ja Apple poodides on kontroll suurem, kuid ka sealt võib teadmatu kasutaja endale pahavara seadmesse laadida. (EMOR, 2014)

Antud probleemi lahendamine aitab kaasa ministeeriumi strateegias välja toodud eesmärkide saavutamisele, kuna turvalisem töökeskkond aitab kaasa kindlustada turvalisust ja hoida Eesti head mainet ja mõjukust.

3.3.3 Ministeeriumi erinõuded mobiilsete seadmete haldustarkvarale.

Selleks et vältida ministeeriumi informatsiooni lekkimist ja tagada seadmete turvalisus ja terviklik haldus, oleks vaja ministeeriumile võtta mobiilsete seadmete haldustarkvara, ehk MDM, mis peaks sisaldama järgmisi põhifunktsionaalsusi:

- Mobiilsete seadmete turvaline registreerimine;
- Rollide põhine õiguste jaotamine administratiivliideses;
- Seadmete kaughaldus sh. tehase sätete taastamine, turvakoodi muutmine, WIFI ja VPN seadete haldus, seadmete tehnilise info kuvamine;
- Kioski põhine seadmete kasutamise võimalus;
- Turvaline konteiner tüüpi e-posti klient koos mitme astmelise autentimisega;
- Musta nimekirja, valge nimekirja ja kohustusliku nimekirja tarkvara loetelu võimalus;
- Sharepoint keskkonnaga ühendamise tugi, failide kuvamise eesmärgil;
- VOSK tugi ja iseteenindusportaali olemasolu;

3.3.4 Ülevaade võimalikest lahendusvariantidest

Joonis 4. Gartneri "Magic Quadrant" ettevõtte mobiilsuse haldustarkvarade kohta

3.3.5 Lahendusvariantide pikk nimekiri

- AirWatch
- BlackBerry
- MobileIron
- Citrix
- Good Technology
- SAP
- IBM
- Sophos
- Tangoe
- MS Intune

3.3.6 Lahendusvariantide lühike nimekiri

Pikast nimekirjast kerkis esile kolm lahendust, mis vastavad ministeeriumi poolt esitatud erinõuetele ja mis on Gartneri uuringu kohaselt ka kasutajate seas populaarsed ning Eestis esindatud:

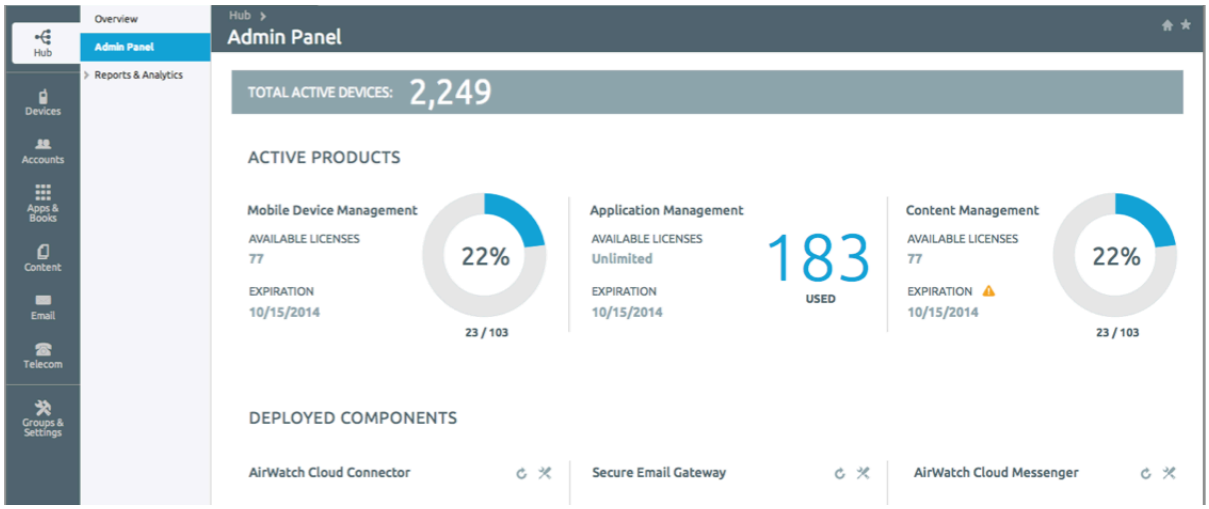
- VMware AirWatch
- Sophos MDM
- Microsoft Intune

VMware AirWatch

VMware omandas 2014 aastal veebruaris AirWatchi ja endiselt keskendutakse mobiilsete seadmete turvalisuse tagamisele, kuid üha enam pööratakse tähelepanu ka sülearvutitele ja lisaseadmetele. AirWatch lahendused on sobilikud nii väike- kui ka suurettevõtetele.

Airwatch MDM lahendus hõlmab mobiili rakendust, seadme, brauseri ja e-posti haldamist koos turvalise tööruumi juhtimise, mitme kasutaja juhtimise ja VOSK toetust. AirWatch lahendus tagab turvalisuse paljudele mobiilsetele operatsioonisüsteemidele, sh. Apple iOS, Android, BlackBerry, Windows Phone, Windows Mobile, Symbian, Apple TV, Mac OS X ja Windows 8 / RT / 32.

2013 aastal arendas AirWatch välja turvalise tööruumi. Tegemist on turvalise konteinerlahendusega, mis sisaldab erinevaid asutuse andmeid, nagu e-posti, dokumente, turvalist veebi sirvimist ja tagab asutuse andmete turvalisuse ja terviklikkuse ning eraldatuse eraandmetest. (Terrence et al., 2015)



Joonis 5. Airwatch halduskeskkond
(http://blogs.air-watch.com/2015/02/introducing-airwatch-8/)

Lahenduse tugevused:

AirWatch pakub laialdast tuge erinevatele mobiilsete seadmete platformidele, nagu näiteks iOS, Android, BlackBerry, Windows Mobile, Windows Phone, Symbian, Apple TV, Mac OS X ja Windows 8 / RT / 32.
Erinevaid kasutuselevõtu mudelid võimaldavad ministeeriumil valida kõige sobivam enda jaoks, nagu näiteks SaaS, valmis lahendus, või paigaldus enda serveritesse. Lisaks saab asutus valida kas liitumislepingule või püsilitsentsile põhineva maksustamise vahel.
AirWatch pakub turvalist sisu vaatamise ja koostöö tarkvara, mis ühildub MS Sharepoint tarkvara ja jagatud võrguketaste kasutamisega.
Saab kasutada turvalist veebi lehitsemise tarkvara, mis ühildub Apple iOS, Google Android and Windows Phone 8 seadmetega.

Lahenduse nõrkused:

Kuigi AirWatch on üks parema ja soodsama hinnastusega MDM lahendusi turul, võib AirWatch tunda survet veelgi hinna poliitika muutmise kohta, kuna hind MDM lahenduste hulgas on languse trendis.
AirWatch ei toeta S / MIME autentimise protokolli Google Android seadmetel. (Terrence et al., 2015)

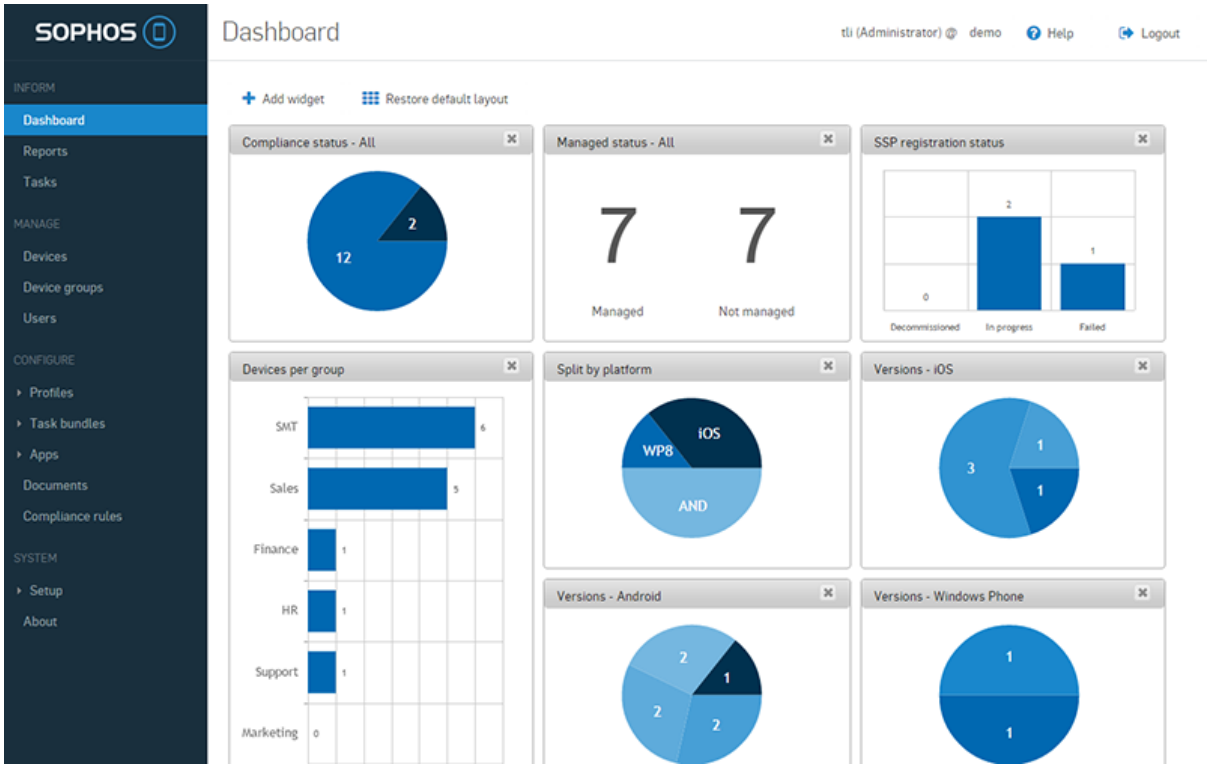
Sophos MDM

Sophos on eraettevõte, mille peakontorid asuvad Bostonis, USA's ja Oxfordis, Suurbritannias. Sophos pakub erinevaid andmekao vältimise lahendusi (DLP), viirusetõrje, UTM, krüpteerimise ja teisi turvalahendusi lauaarvutitele, serveritele ja mobiilseadmetele. Sophose rakendusi kasutavad erinevas suuruses ettevõtted. Eestis on esindajaks Datafox.

Sophos Mobile Control (SMC) on Sophose MDM lahendus, mis toetab Apple iOS, Google Android, Windows Phone 8, Windows Mobile ja BlackBerry seadmeid. Sophos SMC toetab seadmete krüpteerimist, parooli paigaldamist, seadmest andmete kustutamist (nii asutuse andmete kui kõikide andmete kustutamist). Sophose MDM lahendust saab kasutada nii pilvepõhise teenusena, kui ka ministeeriumi enda serverisse paigaldatuna.

Lahenduse tugevused:

Sophos pakub lihtsat litsentseerimise poliitikat: üks kasutaja / üks litsents. Seda tüüpi lahendusega saab asutus kontrollida lahenduse maksumust, sõltumata sellest, kui palju seadmeid töötaja kasutab. See võib tuua märkimisväärset kokkuhoidu ettevõttele, kelle töötajatel on palju erinevaid seadmeid käes.
Sophos pakub tugevat pahavara ja veebi kaitse funktsionaalsust. Vähesed teised MDM lahenduse pakkujad suudavad eemalt käivitada pahavara skaneerimist, blokeerida pahatahtlikke rakendusi ja skaneerida rakendusi nende paigaldamisel.
Sophos Mobile Encryption lahendus annab kasutajatele vahendi turvaliseks dokumentide lisamiseks, vaatamiseks ja redigeerimiseks pilve teenustes. Sophos Mobile Encryption toetab Dropbox, Microsoft OneDrive, Google Drive, Egnyte, Media Center ja WebDAV (nt OwnCloud, Windows Server) teenuseid. (Terrence et al., 2015)



Joonis 6. Sophos halduskonsool (https://partnerportal.sophos.com/en-us/microsite/products/mobile-control.aspx)

Lahenduse nõrkused:

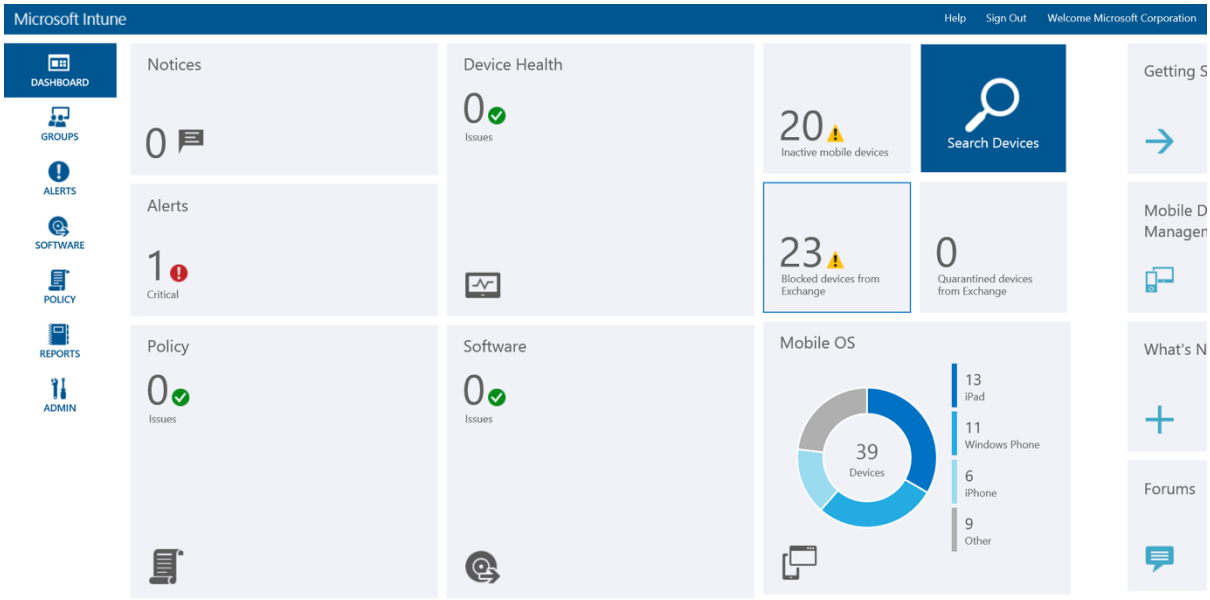
Sophos Mobile Encryption on saadaval ainult Apple iOS ja Google Android seadmetel.
Sophosel on piiratud rakenduste andmete kaitse, kuna ta ei toeta turvakonteinerit ja rakenduste "pakkimist"
Sophos ei toeta kõiki funktsioone Google Android seadmetel, nagu näiteks Motorola'l ja HTC'l. (Terrence et al., 2015)

Microsoft Intune

Windows Intune on Microsofti poolt loodud pilveteenus, mis jõudis tänavu suvel oma 3. versioonini. Windows Intune sihtgrupiks on keskmise suurusega ettevõtted ja tema eesmärk on aidata ettevõttel hallata ja turvata ettevõtte arvuteid. Alates 3. versioonist on võimalik lisada ka mobiilseid sidevahendeid, kuna toetatud on peale Windows süsteemi ka Android ja IOS

platvormid. Eestis on esindaja Microsoft Eesti, kuid kuna nemad ei tegele müügiga, siis pakuvad litsentse erinevad müüjad. Hinnad, on võetud Microsofi ametlikult leheküljelt.

Intune sisaldab iseteeninduspportaali nii pilves kui seadmes (Intune Company Portal).
Microsoft Intune on võimalik siduda kohaliku System Center Configuration Manageriga ja selliselt saab administraator hallata nutiseadmeid ja määrata neile poliitikaid tuttavast kasutajaliidesest. (Terrence et al., 2015)



Joonis 7. Microsoft Intune halduskonsool
(https://blogs.technet.microsoft.com/microsoftintune/2015/04/20/conditional-access-for-on-premises-exchange-using-microsoft-intune/)

Lahenduse tugevused:
Tsentraalne haldus kõikide Microsoft toodete jaoks ja hallatav läbi MS SCCM keskkonna.

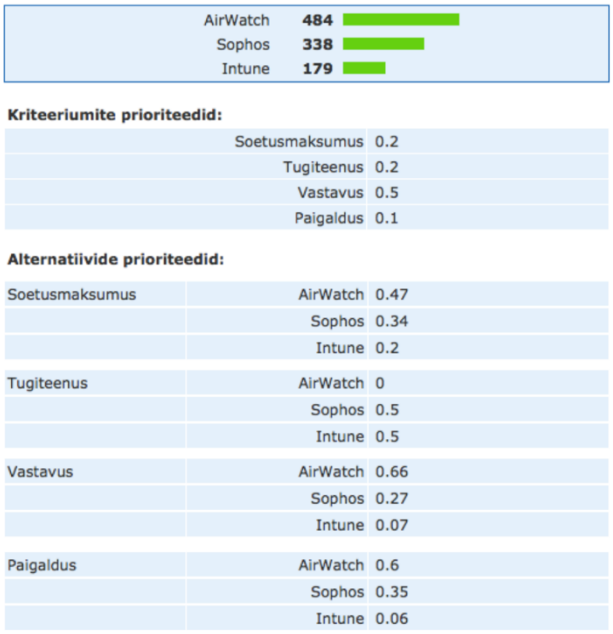
Lahenduse nõrkused:
Toetatud on ainult pilve põhine lahendus ja vajalik kogu AD info Azuri pilve kopeerimine. (Terrence et al., 2015) Autorile on teada, et Microsoft on tulnud turule ka asutuse enda infrastruktuuri paigaldatava lahendusega, kuid antud töö kirjutamise hetkel toetab sellina lahendus vaid Microsofti enda operatsioonisüsteemiga mobiilseid seadmeid.

3.3.7 Lahendusvariantide võrdlus

Lahenduste võrdlusel kasutas autor Thomas L. Saaty meetodit. Saaty meetod võimaldab keerukat otsustuse probleemi modelleerida hierarhilise struktuuri kaudu, mille moodustavad eesmärk, kriteeriumid, alamkriteeriumid, ja alternatiivid. Selle eelis seisneb võimaluses käsitleda nii kvalitatiivseid, kui ka kvantitatiivseid objekte; meetodi väljundiks on matemaatiliselt korrektne, kvantitatiivne hinnang analüüsitavatele alternatiividele. (Forman & Selly, 2003)

Saaty meetodi modelleerimiseks kasutas autor Netekspert poolt pakutavat veebi põhist tarkvara ChoicePlanner (Netekspert, 2016). Põhikriteeriumideks valis soetusmaksumuse 300 kasutaja seadme kohta, Tugiteenuse 3. aastase perioodi kohta, vastavuse ministeeriumi erinõudmistele ja paigalduse keerukuse. Selle tulemusena sai kõrgemad punktid AirWatch.

Tabel 4. Netekspert ChoicePlanner alternatiivide võrdlus.



Lisaks Saaty meetodile, hindasin ka praegust puhasväärtust, ehk NPV'd.

Tabel 5. NPV arvutus.

asutuse kapitali hind 11%

	AirWatch		Sophos		Intune	
	rahavoog	kum. Rahavoog	rahavoog	kum. Rahavoog	rahavoog	kum. Rahavoog
esialgne kulu	-21000	-21000	-29700	-29000	0	0
aasta 1	-5400	-26400	0	-29000	-16560	-16560
aasta 2	-5400	-31800	0	-29000	-16560	-33120
aasta 3	-5400	-37200	0	-29000	-16560	-49680
NPV	-€34 196,06		-€29 700,00		-€40 467,92	

Sellest arvutusest selgub, et kui ainult rahalist osakaalu arvestada, oleks soodsaim valik ministeeriumi jaoks Sophose takvara.

3.3.8 EMM lahenduse valiku kokkuvõte

Ministeeriumi erinõudeid ja eesmärke arvesse võttes ja nendest tingitud kriteeriumitest valikusse jäänud haldusvahenditest, oleks parimaks valikuks VMware AirWatch. Airwatch ei ole küll kõige soodsaim valik, kuid kui võtta arvesse pakutavat funktsionaalsust ja vastavust ministeeriumi poolt seatud eritingimustele, siis on AirWatch parim valik. Kui lähtuda Saaty meetodi hindamistabelist, siis ei jää Sophos palju maha. Sophose kasuks räägib soodsam hinnastus, kuid võimaluste piiratus võtab punkte maha.

Võttes arvesse nii Gartneri turuanalüüsi, kui tehtud võrdlused lühikese nimekirja toodete vahel, võeti vastu otsus, valida Mobiilsete seadmete haldustarkvaraks VMware AirWatch lahendus.

3.3.9 Juurutuse protsess

Peale otsuse tegemist ja kooskõlastamist ministeeriumi infoturbenõukogus, mis on ministeeriumi alaline nõuandva õiguse töörühm, mille ülesanne on nõustada infotehnoloogia ja diplomaatilise julgeoleku osakonda infoturbe ja IT-arendustega seotud tegevusstrateegiate väljatöötamisel, alustasime testkeskkonna loomiseks partneri otsinguid. Selgus, et Eestis on Airwatch toodete esindusõigus ja kompetents kahel ettevõttel. Küsides pakkumised mõlemalt ettevõttelt, valiti soodsaim pakkuja antud projekti juures tehniliseks partneriks. Seejärel

täpsustati ülesande skoop ja vastavalt tootja poolsetele juhenditele loodi keskkond. Antud lahendus täitis ära kõik ministeeriumi erinõuded ning võimaldas saada enim kasu EMM lahendusest, maandades ära riskid, mis ilma halduskeskkonda rakendamata esineksid.

3.3.10 Rakendusprojekti tulem

Selleks, et vältida töötajate poolset negatiivset vastukaja ja vähendada kasutajatoe koormust peale EMM lahenduse paigalduse otsuse välja kuulutamist, koostati korduma kippuvate küsimuste ja vastuste nimekiri:

- Millal rakendatakse AirWatch mobiilsetele seadmetele?
- Kuidas praktiliselt toimub?
- Millised mobiilsed seadmeid on lubatud kasutada? Kas neid saab valida?
- Kas isiklikku mobiiltelefoni on võimalik edasi kasutada?
- Milliseid rakendusi saab kasutada?
- Kas AirWatch rakendatakse ka kodusele seadmele nt arvuti?
- Kellel on õigus küsida mobiilset seadet?
- Mida on võimalik mobiilsest seadmest AirWatch rakendamisel näha/hallata?
- Kas isiklik E-post on asutuse poolt jälgitav?
- Kui mul on juba Google või Apple konto?
- Kes sanktsioneerib/menetleb/reguleerib?
- Kas mobiilset seadet jälgitakse?
- Kas mobiilse seadme haldustarkvara kasutuselevõtt on asutuse algatus või väljapoolt asutust tehtud soovitus?

Lisaks selgus projekti käigus, et tuleb piiritleda lahenduse juurutamisel mobiilsete seadmete ulatus ja riistvara mark. Kuigi Airwatch toode toetab kahtekümmet ühte erinevat Androidi operatsiooni süsteemiga mobiilset seadet ja lisaks veel Blackberry ja iOS seadet, on tugi erinevatele seadmetele ja operatsioonisüsteemi versioonidele erinev. Peale mobiilsete seadmete halduskeskkonna paigaldamist ja konfiguratsioonisätete uurimist selgus, et kõige paremini on funktsionaalsuse poolt toetatud Apple iOS ja Samsungi äriklassi seadmed, mis omavad sisse ehitatud riistvaralist Safe turvamoodulit. Toetatud seadmete haldamise võimalused on toodud lisas 2.

Eelnevas peatükis kirjeldas autor Forresteri raportile tuginedes populaarsemaid EMM lahendusi ning esitas Forresteri poolt koostatud hindamistabeli koos joonisega. Lisaks kirjeldas autor EMM lahenduse praktilist rakendamise protsessi avaliku sektori asutuse näitel ning tegi selle tulemusest kokkuvõtliku ülevaate.

4. UURING

Antud peatükis annab autor ülevaate Eesti avaliku sektori asutuste seas läbi viidud uuringust. Alustuseks kirjeldab autor avaliku sektori asutuste struktuuri, seejärel tutvustab metoodikat ning toob välja esinenud piiranguid.

4.1 Ülevaade avaliku sektori asutustest ja MDM rakendamisest

Ühe osa Eesti avaliku sektori asutustest moodustuvad Ministeeriumid ja nende allüksused. Eestis on 11 ministeeriumi koos üle 300 allasutusega (SA Eesti Koostöö Kogu, 2013). Suurim ministeerium inimeste arvult on Haridus- ja Teadusministeerium ja väikseim Välisministeerium. Ministeeriumite struktuur (vt. lisa 3) on üldjuhul sarnane. Eraldi IT üksused asutuse näol on loodud Rahandusministeeriumi, Justiitsiministeeriumi, Keskkonnaministeeriumi ja Siseministeeriumi haldusalade teenindamiseks. Teistel ministeeriumitel kuuluvad IT osakonnad ministeeriumi enda struktuuri.

Töö kirjutamise hetkel ei leidnud autor ühtegi eelnevat uuringut ega analüüsi, mis oleks läbi viidud Eestis avaliku sektori mobiilsete seadmete haldustarkvara kasutamise ja VOSK rakendamise kohta. Küll aga tutvus autor Martin Palmi 2015 aastal kaitstud magistritööga teemal "Infoturve VOSK põhimõtte rakendamisel AS Eesti Telekomi näitel", kus Palm keskendus just VOSK vaatevinklist ning erasektori huvidest lähtuvalt infoturbe tagamisele. Palm kirjeldas oma töös hästi lahti VOSK kui sellise nähtuse ja hindas riske Eesti Telekomi asutuse näitel.

Eestis koordineerib riigi infosüsteemi arendamist ja haldamist RIA (Riigi Infosüsteemi Amet), et riik saaks rahvast teenindada parimal võimalikul moel ('Riigi Infosüsteemi Amet', n.d.-b). Riigi infosüsteemi osa on kindlasti ka mobiilsed seadmed ja sellest tulenevalt on RIA kohustatud tagama reeglistiku, et oleks võimalik tagada mobiilsete seadmete turvalisus. RIA's on turvaintsidente ära hoidmiseks ja turvariskide vähendamiseks, seda eelkõige turvateadlikkuse tõstmise ja teavitamise abil moodustatud CERT (computer emergency response team, arvutiavariide tõrje rühm) (Veldre et al., 2016). Eesti riigi tasemel täidab CERT-i ülesandeid Riigi Infosüsteemi Ameti infoturbeintsidentide käsitlemise osakond

(Veldre et al., 2016). RIA küberturvalisuse teenistuse 2014 aasta kokkuvõte ei sisalda õnneks veel ühtegi intsidendi kirjeldust, mis oleks seotud mobiilsete seadmete väärkasutusega. Küll aga pöörati 2014 aasta aruandes tähelepanu libatugijaamade kasutamise ohule. RIA on lisaks koostanud näidis dokumendi mobiilsete seadmete turvapoliitika loomiseks. Kuna Eesti avalik sektor on üldjuhul ISKE infosüsteemide kolmeastmelise etalonturbe süsteemi rakendamise kohustlane, siis ka antud poliitika on koostatud ISKE moodulite kirjeldamise kaupa. ISKE moodul M 4.230 kirjeldab ära keskse haldustarkvara kasutamise ja teeb ettepaneku rohkem kui kümne seadme haldamiseks vastav lahendus kasutusele võtta (Riigi Infosüsteemi Amet, n.d.-a).

4.2 Metoodika

Uurimistöö keskendub ühe konkreetse tehnilise lahenduse uurimisele ja seda läbi praktilise EMM lahenduse juurutamise, kui online küsitluse sooritamise nii turvalisuse valdkonna eest vastutajate kui ka lõppkasutajate hulgas. Sellest tulenevalt on tegemist kvalitatiivse juhtumiuuringuga. Juhtumiuuring on sageli seletava, avastusliku või kirjeldava olemusega ning võimaldab uurida juhtumit tema enda loomulikus keskkonnas (Pervez & Kjell, 2004), ehk siis antud hetkel MDM või EMM kasutamist avaliku sektori asutuste seas. Juhtumiuuring on eelistatud lähenemisviis, kui uuritakse reaalse elu keskkonnas aset leidvat nähtust ja kui uuritavat nähtust on raske uurida väljaspool selle loomulikku keskkonda. (Pervez & Kjell, 2004). Töötades läbi erialase kirjanduse, mis puudutab antud töö valdkonda, sain ülevaate hetkel aktuaalsetest teemadest ja lahendustest seoses MDM lahendustega. See ülevaade andis võimaluse läbi viia online küsimustik, et võrrelda parimaid praktikaid hetkel Eesti avalikus sektoris rakendatuna ning rakendada EMM lahendus ka ühes avaliku sektori asutuses (ministeeriumis).

Online küsitluse viis autor läbi veebikeskkonnas Google Forms teenust kasutades, kuna see tagas kõige kiirema tagasiside küsitlusele ja võimaldab hõlmata võimalikult laiaulatusliku ja eeskujulikku valimit. Valimisse kaasati nii MDM juurutamise eest vastutavad isikud kui ka tavakasutajad. Saadud kvantitatiivseid tulemusi analüüsis autor PSPP tarkvara abil.

Küsimustiku loomisel võttis autor aluseks magistritöös esitatud eesmärgi ja küsimustik saadeti laiali kõikidele ministeeriumi IT ja infoturbejuhtidele ning samuti kaasati nii

Välisministeeriumi kui teiste asutuste töötajaid andmaks ülevaadet tavakasutaja kogemustest. Küsitluses osalejatele anti võimalus jätta oma kontaktid, et hilisemalt anda tagasiside töö magistritöö tulemusest. Teistel juhtudel said osalejad kinnituse, et nende isikuid ei seostata vastustega, ega ei tooda neid eraldi magistritöös välja. Küsimustik koosnes kokku kahekümneüheksast küsimusest, millest osalejad pidid vastama vaid nendele, mis tulenesid nende eelmistest vastustest. Tavakasutajatele ja valdkonna eest vastutavatele isikutele kuvati küsimustikust erinevaid küsimusi, et saada vastavalt sihtgrupile vastav tagasiside. Küsimustikule laekus kokku 161 vastust, millest 14 (8,7%) oli erinevate asutuste infoturbe või IT valdkonna eest vastutajate ja 147 (91,3%) tavakasutajate omad. Autor hindab saabunud vastuste arvu piisavaks, et kirjeldada ja hinnata hetkel avalikus sektoris valitsev olukord.

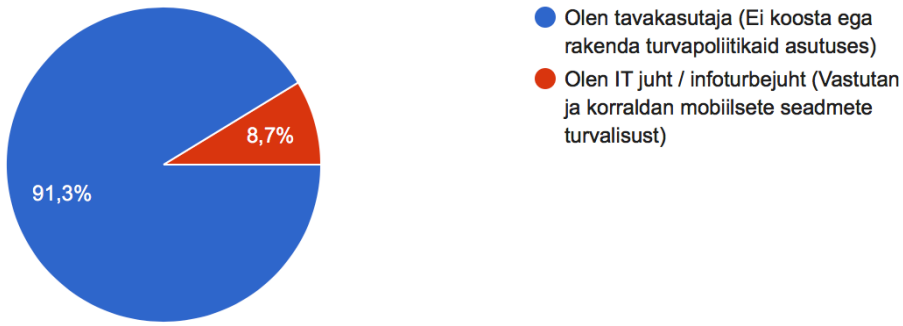


Diagramm 1. Küsitlusele vastanute ülevaade

4.3 Piirangud

Tulenevalt asjaolust, et paljude riigiasutuste IT süsteemide tehnilised lahendused ei ole avalik informatsioon, ei olnud võimalik nii mõnelgi asutusel küsimustikule vastata. Seda arvesse võttes ja lähenedes samuti informatsiooni kaitsvalt, ei ole autor välja toonud ühegi vastanud ministeeriumi ega asutuse nime.

Eelnevas peatükis andis autor ülevaate Eesti avaliku sektori asutuste seas läbi viidud uuringust. Alustuseks kirjeldas autor avaliku sektori asutuste struktuuri, seejärel tutvustas metoodikat ning esinenud piiranguid.

5. UURINGU TULEMUSTE ANALÜÜS

Käesolevas peatükis esitleb autor läbiviidud uuringu tulemusi ja analüüsib tulemusi tulenevalt püstitatud eesmärgist ja uurimisküsimustest lähtuvalt. Küsimustikule laekunud tulemuste analüüsimiseks ja töötlemiseks kasutab autor tarkvara PSPP. Kuna vabavaralisele tarkvarale PSPP ei ole sisse ehitatud graafikute funktsionaalsust, kasutab autor graafikute esitamiseks Google Forms poolt loodud diagramme.

Küsimus nr. 1

Küsimus "*Mis on Teie sugu?*" oli vajalik valimi kirjeldamise eesmärgil. Tulemustest selgus, et valimi moodustasid mehed (vastanutest 50,3%) ja naised (vastanutest 49,7%) peaaegu võrdselt. Kokku osales küsitluses 161 vastanut ja vastanuid kes oma soo avaldasid oli 159 (vt. diagramm nr.3).

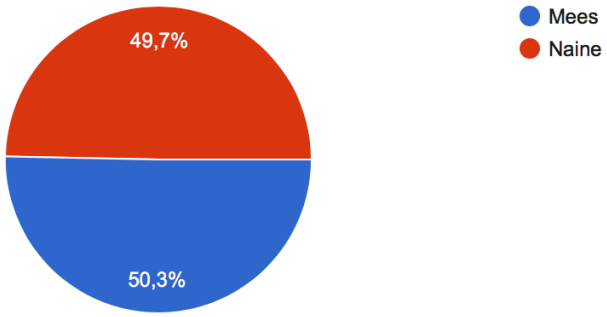


Diagramm 2. Meeste ja naiste osakaal küsitluses osalejate hulgas.

Küsimus nr. 2

Teine küsimus "*Mis on Teie vanus?*" kirjeldab samuti valimit. Selgub, et vastanud jagunevad pea võrdselt kahte suuremasse vanusegruppi. 33,1%, ehk 53 vastanut olid vanuses 41-50 eluaastat ja 38,1% ehk 61 vastanut olid vanuses 31-40 eluaastat. Kakskümmend kaheksa inimest, kes küsimustikule vastasid olid vanemad kui 51 eluaastat kellest seitse olid vanemad kui 61 eluaastat. Kaheksateist vastanut, ehk 11,3% vastanutest olid 21-30 aasta vanused. Alla 20 aasta vanuseid vastanuid ei olnud (vt. diagramm 4).

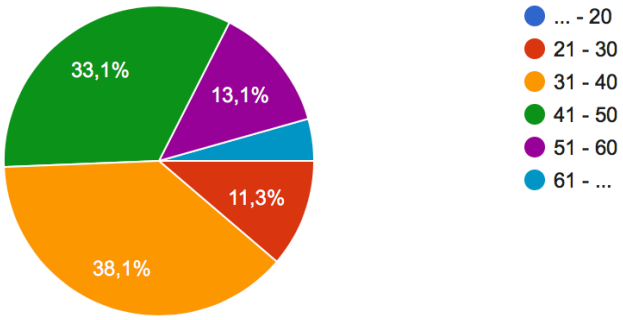


Diagramm 3. Küsitluses osalejate vanuseline jaotus.

Küsimus nr. 3

Kolmanda küsimusega "*Määratle enda roll*" sai autor ülevaate vastanute positsioonist. Autor koostas küsimustiku tavakasutajatele ja valdkonna eest vastutajatele eraldi suunatult ja seetõttu oli vajalik määratleda ka vastanute roll. Selgus, et vastanute hulka kuulus 14 isikut, kes olid kas IT või infoturbejuht, kes vastutavad või korraldavad mobiilsete seadmete turvalisust. 91,3% vastanutest, ehk 147 vastanut olid tavakasutaja rollis (vt. diagramm 5). Kuna neliteist valdkonna eest vastutajat esindasid kõik erinevaid asutusi, siis saab autor lugeda valimi esinduslikuks ja saadud järeldusi on võimalik üldistada ka laiemalt.

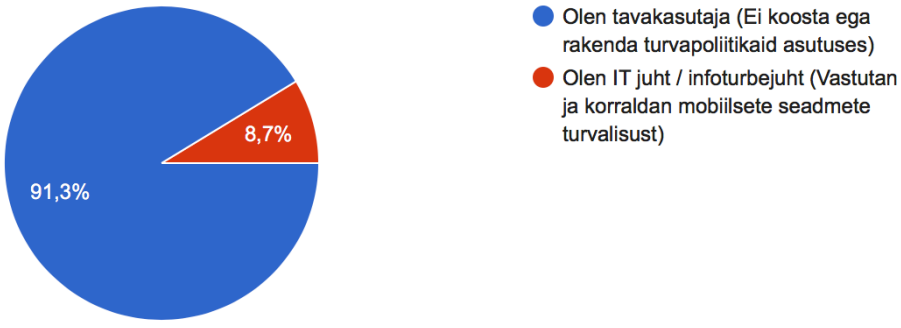


Diagramm 4. Küsitluses osalejate positsioon.

Küsimus nr. 4

Neljas küsimus "*Teie asutuse nimi?*" oli vabatahtlik ja oma asutuse nime avaldasid 94 vastanut mis teeb 58,4% kogu vastanute arvust. Autori jaoks näitab saadud tulemus, et valimisse õnnestus kaasata mitmeid erineva valdkonnaga tegelevaid asutusi. Asutuste suuruse ülevaate kirjeldab juba järgmine küsimus.

Küsimus nr. 5

Küsimus "*Kui palju on Teie asutuses töötajaid?*" kirjeldas ära valimis osalenud vastajate asutuste suurused. Tulemustest selgub, et valimisse kuulub erineva töötajate arvuga asutusi. Suurima osakaalu kuhu kuulub 62% vastanutest, ehk 98 vastajat, moodustab töötajate vahemik 501 – 1000. 32,9% ehk 52 vastanut kuuluvad alla 500 töötajaga asutusse. Kuus vastajat kuulusid üle 2001 töötajaga asutusse ja kaks asutusse, kus töötab 101 kuni 1500 töötajat (vt. diagramm 6).

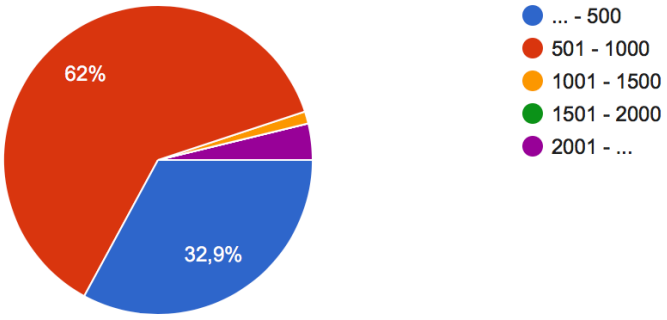


Diagramm 5. Küsitluses osalenud asutuste suurused.

Küsimus nr. 6

Kuuenda küsimusega "*Kas kasutate mobiiltelefoni?*" lootis autor leida vähemalt ühe vastaja, kes ei kasuta mobiiltelefoni, kuid see eesmärk jäi saavutamata. Kõik 161 küsitluses osalejat vastasid üksmeelselt, et kasutavad mobiiltelefoni (vt. diagramm 7).

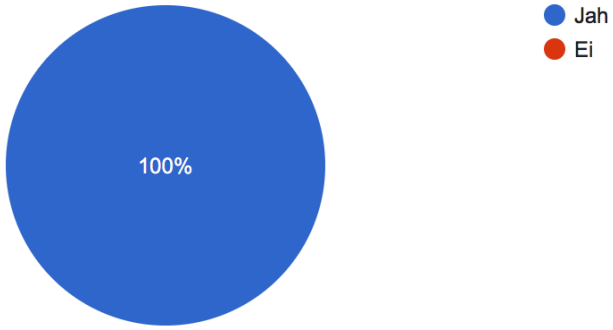


Diagramm 6. Mobiiltelefonide kasutuse ülevaade.

Küsimus nr. 7

Seitsmes küsimus "*Kas kasutate tahvelarvutit?*" andis natukene teistsuguse pildi aga tahvelarvutite kasutamise kohta. Selgus, et koguni 42,9% ehk 62 vastanut ei kasuta tahvelarvutit. Siinkohal eeldas autor, et tahvelarvutite kasutajate protsent tuleb kindlasti suurem kui 57,1% (vt. diagramm 8). Samas näitab tahvelarvutite kasutajate hulk seda, et kuigi mobiiltelefoni omavad ja kasutavad kõik vastanud, ei pea tahvelarvuti omamist kõik vajalikuks.

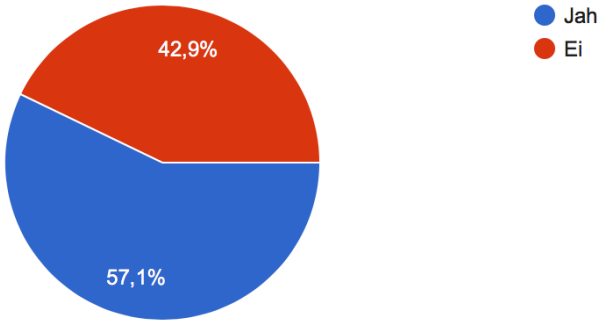


Diagramm 7. Tahvelarvutite kasutamise ülevaade.

Küsimus nr. 8

Kaheksas küsimus "*Mis operatsioonisüsteemiga telefoni kasutate?*" annab ülevaate küsimustikule vastanute kasutuses olevatest mobiiltelefoni operatsioonisüsteemidest. Selgub, et endiselt on android operatsioonisüsteemiga telefonid populaarseimad (50% ehk 71. Vastanut omab android operatsioonisüsteemiga telefoni), kuid Apple tooted ei jää enam kaugele maha,

sest vastanutest 45,1% ehk 64 vastanut kasutab iOS operatsioonisüsteemiga telefoni. Windows operatsioonisüsteemi kasutamine on oodatult tagasihoidlik. Vastanutest vaid 7% ehk 10 vastanut kasutab Windows operatsioonisüsteemi oma telefonil. Samuti leidus vastanute hulgas 4 vastanut, kes kasutavad muu operatsioonisüsteemiga telefoni (vt. diagramm 9). Antud tulemused on vajalikud, et hinnata ettevõtte mobiilsuse halduse poolt toetatavate seadmete tüüp ning annab võimaluse luua ettevõtte mobiilsusstrateegia vastavalt kasutuses olevatele seadmetele.

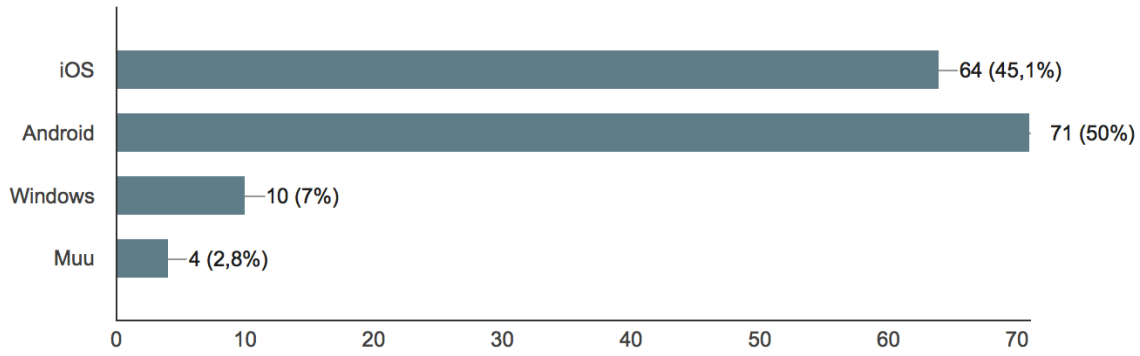


Diagramm 8. Mobiiltelefonide operatsioonisüsteemide jaotus.

Küsimus nr. 9

Üheksas küsimus "*Kas telefon on tööandja poolt antud?*" annab ülevaate küsimuses 8 kirjeldatud seadmete omaniku kohta. Selgub, et vastanutest 60,3%, ehk 88 vastanut, kasutab isiklikku telefoni ja vaid 39,7% ehk 58 vastajat on saanud telefoni tööandja poolt.

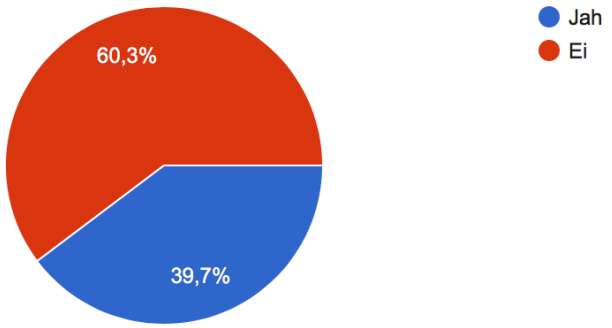


Diagramm 9. Ülevaade küsimusele, et kas mobiiltelefon on tööandja oma.

Küsimus nr. 10

Kümnes küsimus "*Mis operatsioonisüsteemiga tahvelarvutit kasutate?*" moodustab teistsuguse pingerea, võrreldes mobiiltelefonidega. Tahvelarvuti kasutajatest 62,4% ehk 51 vastanut kasutab tahvelarvutina Apple toodangut ja Android operatsioonisüsteem jääb 28 tahvelarvuti kasutajaga (33,7% tahvelarvuti kasutajatest) kaugele maha. Samuti on Windowsi operatsioonisüsteem 5 tahvelarvuti kasutajaga (6% vastanutest) ja muud operatsioonisüsteemid 2 tahvelarvuti kasutajaga (2,4% vastanutest) just mitte kõige levinumad operatsioonisüsteemid tahvelarvutite hulgas (vt. diagramm 10). Sellest võib järeldada, et kasutusmugavus ja lihtsus operatsioonisüsteemi puhul määrab palju ja mida rohkem kasutataks seadet muude funktsioonide täitmiseks kui helistamiseks, seda olulisem see on.

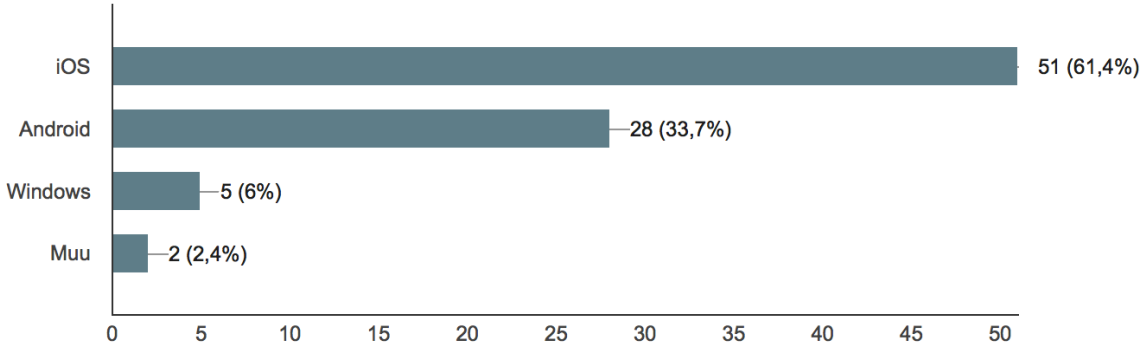


Diagramm 10. Tahvelarvutite operatsioonisüsteemide jaotus.

Küsimus nr. 11

Sarnaselt mobiiltelefonide kohta küsituga, küsis autor ka üheteistkümnendas küsimuses "*Kas tahvelarvuti on tööandja poolt antud?*" tahvelarvutite omaniku kohta. Selgus, et sarnaselt mobiiltelefonidele, on ka tahvelarvutid valdavalt isiklikud (tahvelarvutite kasutajatest 79,8%, ehk 67 kasutajat) ja vaid 20,2% ehk 17 tahvelarvuti kasutajat on saanud seadme tööandja käest (vt. diagramm 11). Siinkohal näeb autor ohtu, kuna tööandjatel puudub kontroll tahvelarvutis töödeldava informatsiooni üle ja kasutajad kasutavad tahvelarvuteid ka tööalaselt, siis võib asutuse infolekke risk olla suur.

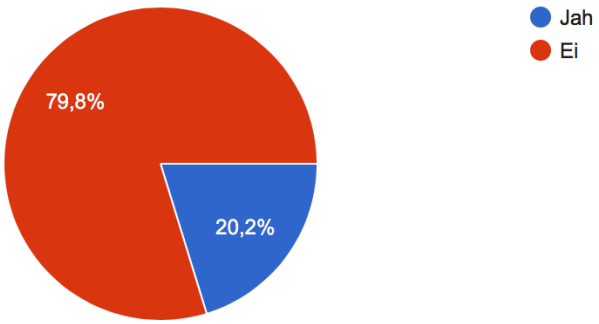


Diagramm 11. Vastus küsimusele, kas tahvelarvuti on tööandja oma.

Küsimus nr. 12

Kaheteistkümnes küsimus "*Kas jagate töötajatele asutuse mobiilse seadme?*" andis autorile ülevaate asutuste mobiilsete seadmete poliitika olemasolu kohta ja levinud praktika kohta seoses mobiilsete seadmete jaotamisega töötajatele. Küsimus oli suunatud IT ja infoturbejuhtidele ning vastustest selgus, et üheksal asutusel (64,3% vastanutest) ei ole selget poliitikat rakendatud ja seadmeid antakse lähtuvalt olukorrast. Kolm asutust (21,4% vastanutest) annab töötajale ise mobiilse seadme ja kaks asutust (14,3% vastanutest) ei jaga töötajatele mobiilseid seadmeid (vt. diagramm 12).

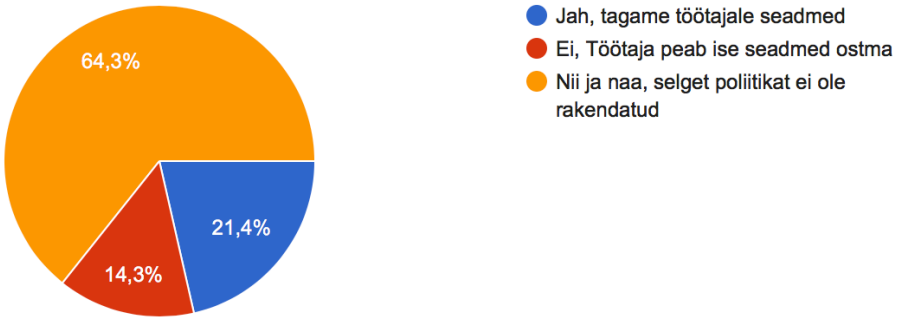


Diagramm 12. Ülevaade mobiilsete seadmete kasutusse andmisest.

Küsimus nr. 13

Küsimus kolmteist "*Kui oluline on teie jaoks mobiilsete seadmete turvalisus?*" on suunatud IT ja infoturbejuhtidele saamaks nende poolset hinnangut mobiilsete seadmete turvalisuse kohta. Üllatav oli autori jaoks tulemus IT ja infoturbejuhtide hinnangule mobiilsete seadmete turvalisuse olulisuse kohta. Autor palus hinnata Mobiilsete seadmete turvalisust seitsme palli skaalal, kus 1 oli vähe oluline ja 7 väga oluline. Selgus, et vaid 5 vastanut, ehk 35,7% IT ja infoturbejuhtidest pidas mobiilsete seadmete turvalisust väga oluliseks. Kolm vastanut (21,4%) hindas olulisust 6 palliga. Nelja ja viie palliga hindasid olulisust kaks vastanut (14,3%) ja nii kahe kui kolme palliga hindasid olulisust üks vastaja (7,1%) (vt. diagramm 12). Seitsme palli skaalal on IT ja infoturbejuhtide seas mobiilseadmete turvalisuse olulisuse keskväärtus 5,43 ja standardhälve 1,65 (vt. tabel nr.1).

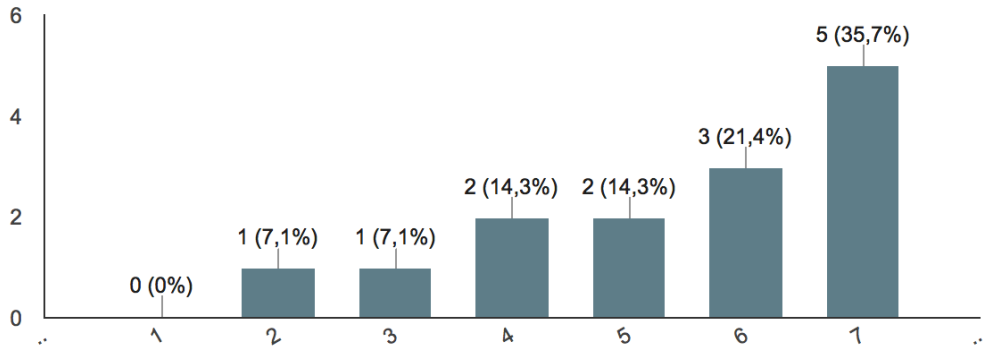


Diagramm 13. IT ja infoturbejuhtide hinnang mobiilsete seadmete turvalisusele.

Küsimus nr. 14

Küsimus neliteist "*Kui oluline on teie jaoks mobiilsete seadmete kasutusmugavus?*" oli sarnaselt küsimusele kolmteist suunatud IT ja infoturbejuhtidele, et saada nende hinnangut mobiilsete seadmete kasutusmugavusele. Selgus, et ootuspäraselt kõrgeks (keskväärtus 5,93, standardhälve 1,33) hinnati kasutusmugavust ja koguni 50% vastanutest ehk 7 IT ja infoturbejuhti hindas kasutusemugavust maksimaalse seitsme palliga. Kaks vastanud (14,3%) andis 6 palli, kolm vastanut (21,4%) andis 5 palli ja nii kolm kui neli palli andis üks vastanu, ehk 7,1% vastanutest (vt. diagramm 14). Tuleb välja, et IT ja infoturbejuhid hindavad mobiilsete seadmete kasutusmugavust (keskväärtus 5,93, standardhälve 1,33) kõrgemalt kui mobiilsete seadmete turvalisust (keskväärtus 5,43 ja standardhälve 1,65) (vt. joonis 1)

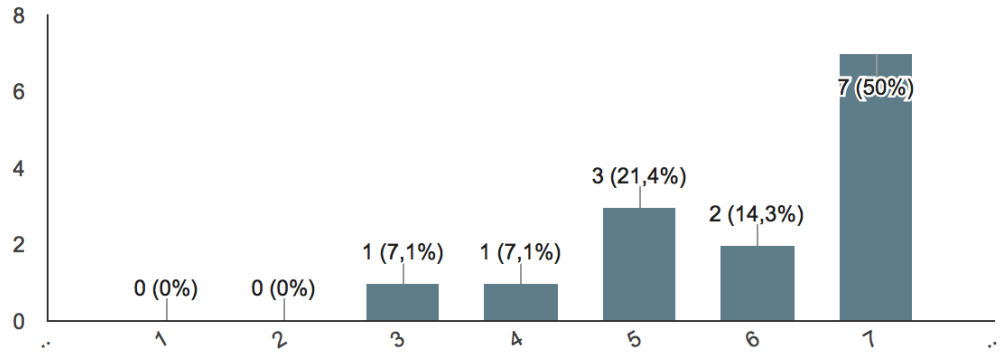


Diagramm 14. IT ja infoturbejuhtide hinnang mobiilsete seadmete kasutusmugavusele.

Küsimus nr. 15

Küsimus number viisteist "*Kas teie asutuses on loodud mobiilsete seadmete kasutamiseks poliitika?*" annab ülevaate asutustes kehtestatud mobiilsete seadmete kasutamise poliitika kohta. Selgub, et ligi pooltel (42,9% ehk kuus asutust) asutustel on välja töötatud ja rakendatud mobiilsete seadmete kasutamiseks poliitika. 28,6% ehk neli asutust on mobiilsete seadmete väljatöötamisega tegelemas ja neli (28,6% asutustest) asutust ei oma mobiilsete seadmete kasutamiseks poliitikat (vt. diagramm 15). Autor leidis, et poliitika olemasolu on tinginud ka küsimuses kaksteist selged piirid asutuste vahel kes annavad või ei anna mobiilseid seadmeid ja asutuste vahel, kellel ei ole selgelt antud tegevus piiritletud.

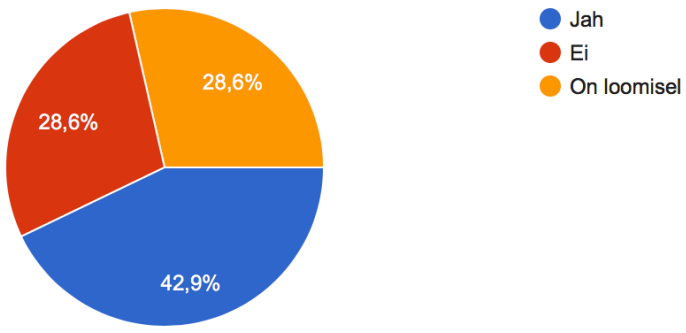


Diagramm 15. Mobiilsete seadmete kasutamiseks poliitika olemasolu asutustes.

Küsimus nr. 16

Küsimusega kuusteist "*Mis teenuseid lubate kasutada mobiilsetest seadmetest?*" soovis autor saada ülevaadet teenustest, mida asutused oma töötajatele pakuvad. 92,9% ehk 13 asutust lubavad kasutada oma töötajatel mobiilsest seadmest e-posti juurdepääsu võimalust. Asutuse siseveebile ja dokumendihaldusele lubab ligi kasutajaid viis (35,7% vastanud asutustest) asutust ja muudele infosüsteemidele lubab ligi kasutajaid kolm (21,4% vastanud asutustest) asutust (vt. diagramm 16). Selgub, et kõik küsitluses osalenud asutused peale ühe lubavad oma töötajate mobiilseid seadmeid ligi asutuse e-posti süsteemidele. Samas nagu selgus küsimusest viisteist, ei ole kõikides asutustes välja töötatud mobiilsete seadmete kasutamise poliitika ja nagu selgub järgmisest küsimusest, ei ole kõikides asutustes rakendatud ka mobiilsete seadmete haldustarkvara lahendus.

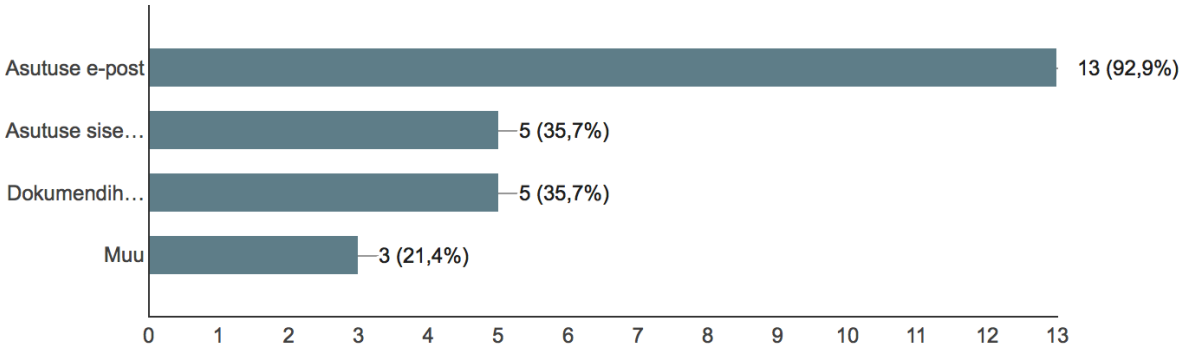


Diagramm 16. Mobiilsetes seadmetes lubatud teenused asutuste poolt.

Küsimus nr. 17

Küsimus number seitseteist "*Kas teie asutuses on kasutusel mobiilsete seadmete haldustarkvara lahendus?*" annab ülevaate vastanud asutustes kasutusele võetud või planeeritava mobiilsete seadmete haldustarkvara lahenduse kohta. Antud küsimusele järgneb täpsustav küsimus kasutusel või planeerimisel oleva tarkvara kohta. Selgub, et pooltel asutustel (50% vastanutest) ei planeeri ega oma mobiilsete seadmete haldustarkvara lahendust. Vaid kahel (14,3% vastanutest) asutusel on MDM lahendus kasutusel ja viis asutust (35,7% vastanutest) planeerivad nimetatud lahenduse kasutusele võtta (vt. diagramm 17).

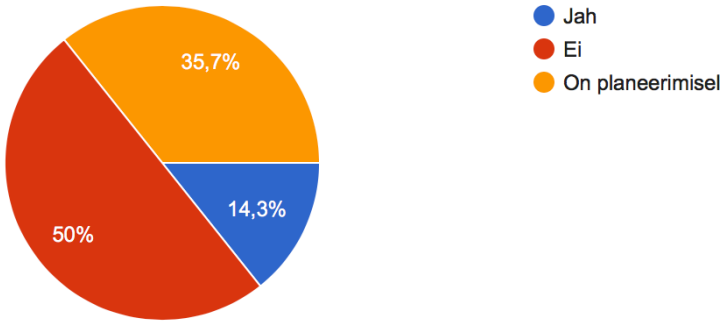


Diagramm 17. MDM lahenduste olemasolu asutustes.

Küsimus nr. 18

Küsimus number kaheksateist "*Millist MDM lahendust kasutate?*" oli suunatud neile, kes vastasid küsimuses seitseteist, et nad kasutavad või planeerivad kasutama hakata mobiilsete seadmete haldustarkvara lahendust. Vastustest selgus, et kõik kes planeerivad kasutama hakata MDM lahendust (5 asutust), kasutavad täna mobiilsetes seadmetes MS Exchange (ActiveSync) teenust (57,1% vastanutest) või muud (1 vastanud, ehk 14,3% vastanutest) lahendust e-postile juurdepääsu pakkumiseks. Asutused (2 asutust) kes on täna juba MDM lahenduse kasutusele võtnud, kasutavad Airwatch (1 asutus 14,3% asutustest) ja Sophos (1 asutus 14,3% vastanutest) MDM lahendust (vt. diagramm 18).

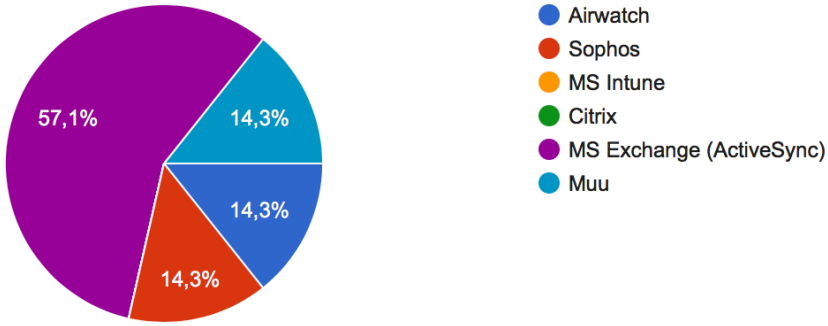


Diagramm 18. MDM tarkvara toodete kasutus asutustes.

Küsimus nr. 19

Küsimusest number üheksateist "*Kas kasutate pilveteenust või on-premise lahendust?*" selgus, et kõik kes kasutavad või plaanivad MDM lahendust kasutusele võtta, kasutavad On-premise, ehk kohalikus infrastruktuuris paiknevat lahendust (vt. diagramm 19).

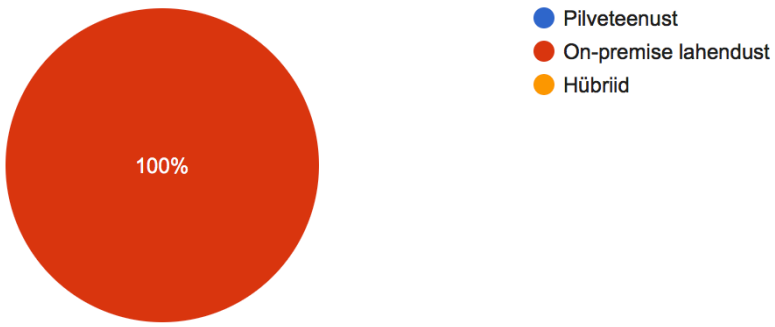


Diagramm 19. MDM pilveteeuste kasutamine asutustes.

Küsimus nr. 20

Küsimus number kakskümmend "*Märkige, et millised reeglid on MDM seadistuse juures olulised teie jaoks.*" oli viimane IT ja infoturbejuhtidele suunatud küsimus. Sellega soovis autor saada ülevaadet olulisematest MDM funktsioonidest. Selgus, et kõikidele vastanutele olid olulisemateks võimalusteks mobiilsete seadmete automaatne lukustus ja mobiilsete seadmete kaugtühjendus (7 asutust, ehk 100% vastanutest). Järgnesid 85,7% olulisusega mobiilsete seadmete klahviluku seadistamise, antiviiruse ja turvapoliitika vastavusreeglite loomise võimalused. Kolmandal positsioonil oli IT ja infoturbejuhtide arvates MDM poolt pakutav VPN tugi, mis võimaldaks mobiilsetel seadmetel ühenduda turvaliselt asutuse infosüsteemide külge. Järgnesid olulisuselt seadmete lokatsiooni tuvastamine ja tulemüüri olemasolu (olulisusega 57,1%), seadmete kasutusinfo saamine (olulisusega 42,9%). Ekraanipildi tegemise keelamine ning musta- ja valge nimekirja loomise võimalus rakenduste kohta olid vähem olulisemad funktsioonid (olulisus 28,6%) (vt. diagramm 20).

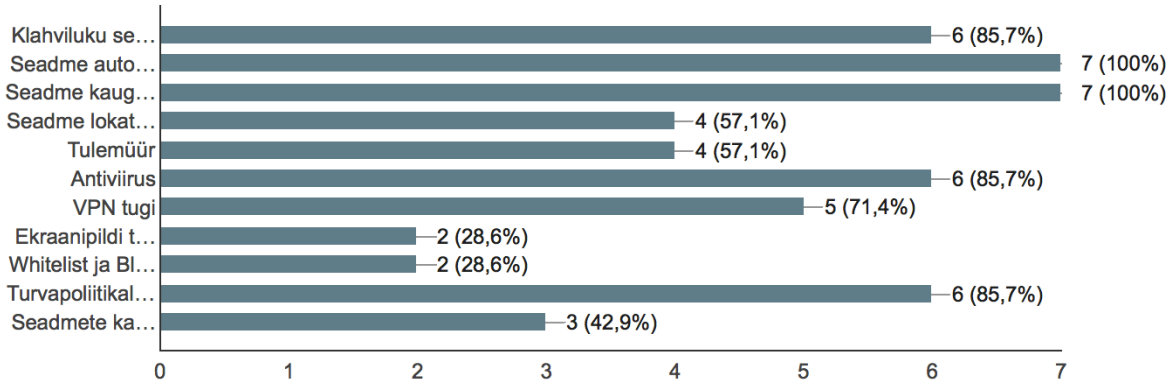


Diagramm 20. MDM funktsioonide olulisus IT ja infoturbejuhtide jaoks.

Küsimus nr. 21

Küsimus number kakskümmendüks "*Milliseid teenuseid oma mobiilsetest seadmetest kasutad?*" oli tavakasutajale suunatud, et saada ülevaade enim mobiilsetes seadmetes kasutatud rakendustest. Selgus, et mobiilset seadet kasutatakse enim (143 vastanut, ehk 97,3% vastanutest) interneti jaoks. 129 vastanut (87,8% vastanutest) kasutas mobiilset seadet pildistamiseks ning sellele järgnes kohe 124 vastanuga (84,4% vastanutest) isikliku e-posti kasutamine. Neljandal kohal pingereas on töö e-posti kasutamine, mida teeb 104 vastanut (70,7% vastanutest) ja üle poolte, ehk 86 vastanut (58,5% vastanutest) kasutab mobiilset seadet sotsiaalmeedia külastamiseks, milleks on näiteks Facebook. Vähem kasutatakse mobiilsetes seadmetes kontoritarkvara rakendusi (40 vastanut, ehk 27,2% vastanutest), Twitterit (28 vastanut, ehk 19% vastanutest) ja teisi rakendusi (24 vastanut, ehk 16,3% vastanutest) (vt. diagramm nr. 21).

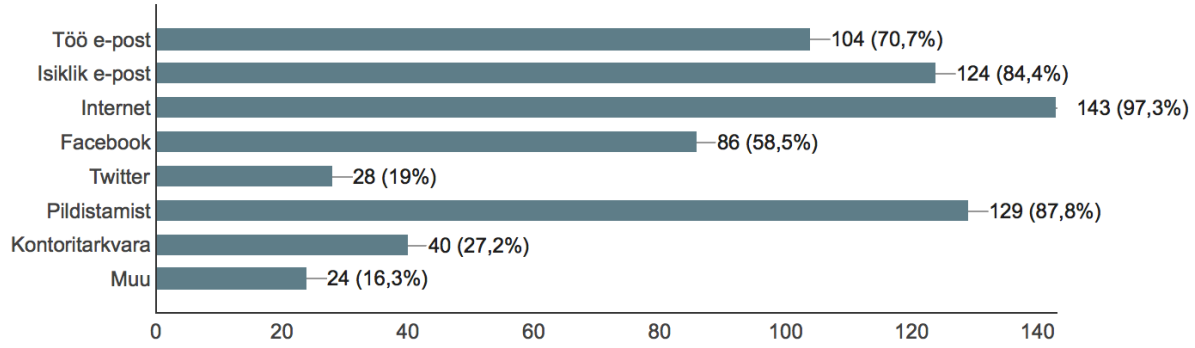


Diagramm 21. Mobiilsetes seadmetes kasutatavad teenused.

Küsimus nr. 22

Sarnaselt IT ja infoturbejuhtidele, küsis autor ka tavakasutajatelt küsimusega number kakskümmendkaks "*Kui oluline on teie jaoks mobiilsete seadmete turvalisus?*" arvamust mobiilsete seadmete turvalisuse olulisuse kohta. Vastanutest 63,3%, ehk 93 vastanud pidas tuvalisust väga oluliseks, hinnates seitsme palli skaalal seda seitsme palliga. Kuue palliga hindas turvalisuse olulisust 33 vastanut (22,4% vastanutest) ja 18 vastanut (22,4% vastanutest) hindas mobiilsete seadmete turvalisust viie palliga. Vaid 2% vastanutest, ehk 3 vastanut hindas turvalisuse olulisust 4 palliga, mis on siiski üle keskmise tulemus. Väiksemaid hinnanguid ei antud, mis teeb kõikide vastanute keskmiseks 6,47 palli. Siit tuleb ka autori üllatus püstitatud oodatud tulemuse kohta, mis tuleb ümber lükata, kuna selgub, et tavakasutajate hinnang ja suhtumine mobiilsete seadmete turvalisuse olulisusesse on kõrgem (keskväärtus 6,47 ja standardhälve 0,79) kui IT ja infoturbejuhtide oma (keskväärtus 5,43 ja standardhälve 1,65) (vt. diagramm nr. 22 ja tabel nr. 1).

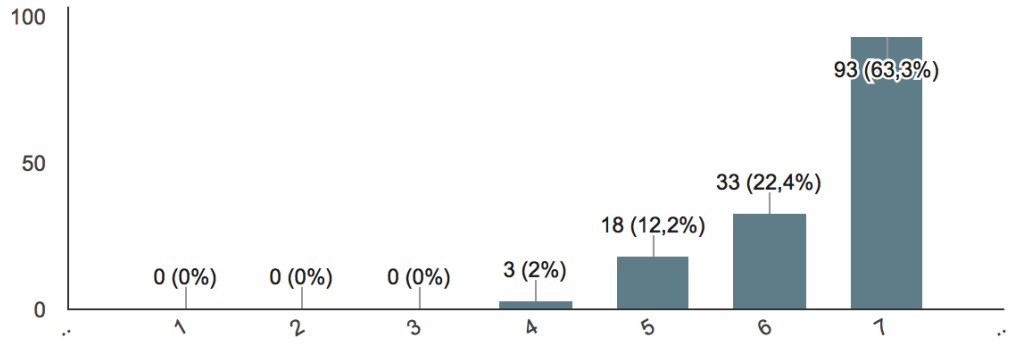


Diagramm 22. Tavakasutajate jaoks Mobiilsete seadmete turvalisuse olulisus.

Küsimus nr. 23

Küsimus kakskümmendkolm "*Kui oluline on teie jaoks mobiilsete seadmete kasutusmugavus?*" tavakasutajatele tõi oodatud tulemuse. Sarnaselt IT ja infoturbejuhtidele (keskväärtus 5,93, standardhälve 1,33) pidasid ka tavakasutajad mobiilsete seadmete kasutusmugavust (keskväärtus 6,62, standardhälve 0,75) kõrgemaks kui mobiilsete seadmete turvalisust (keskväärtus 6,47, standardhälve 0,79). Analüüsist selgub, et tavakasutajad on rohkem ühesuguse vaatega nii mugavuse kui turvalisuse olulisuse hindamisel. Keskväärtuse 6,47 maksimaalsest seitsmest pallist moodustasid 104 vastanut (70,7% vastanutest) maksimum

pallidega, 35 (23,8% vastanutest) vastajat kuue palliga, 6 (4,1% vastanutest) viie palliga ja madalaima neli palli andis vaid üks (0,7% vastanutest) vastanu (vt. diagramm nr. 22 ja tabel nr. 1).

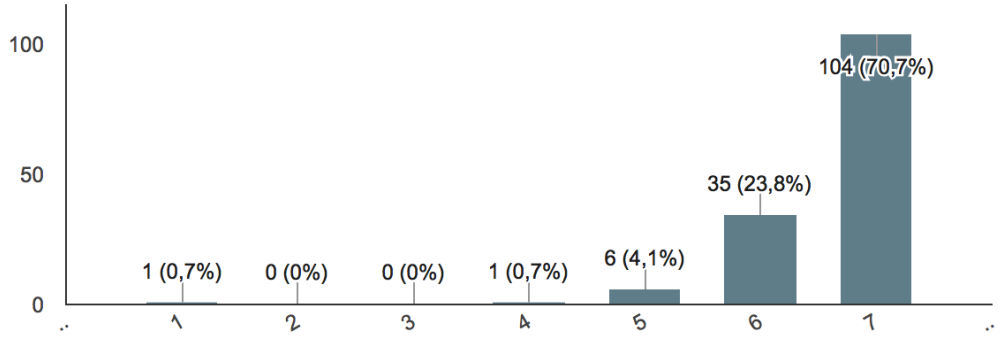


Diagramm 23. Tavakasutajate jaoks Mobiilsete seadmete kasutusmugavuse olulisus.

Tabel 6. Võrdlus IT ja infoturbejuhtide ning tavakasutajate suhtumisse mobiilsete seadmete turvalisusesse ja kasutusmugavusse.

Küsimus	Vastuseid	Keskmine	Standardhälve	Dispersioon	Ulatus	Miinimum	Maksimum
Kui oluline on juhile seadmete turvalisus	14	5.43	1.65	2.73	5.00	2.00	7.00
Kui oluline on juhile seadmete kasutusmugavus	14	5.93	1.33	1.76	4.00	3.00	7.00
Kui oluline on kasutajale seadmete turvalisus	147	6.47	.79	.62	3.00	4.00	7.00
Kui oluline on kasutajale seadmete kasutusmugavus	147	6.62	.75	.57	6.00	1.00	7.00

Küsimus nr. 24

Kahekümneneljas küsimus "*Kas teie seadmetel on seadistatud ekraanilukk?*" kinnitab tavakasutajate suhtumist turvalisuse olulisusesse. 147. vastanust koguni 141 (95,9% vastanutest) vastajat kinnitas, et nende mobiilsel seadmel on seadistatud ekraanilukk. Vaid kuus vastanut (4,1% vastanutest) ei olnud oma seadmel ekraanilukku aktiveerinud (vt. diagramm nr. 23). Kuna mobiilseid seadmeid kasutatakse üldjuhul erinevates asukohtades ja keskkondades ka väljaspool asutuse ruume, siis üheks suurimaks riskiks on mobiilsete seadmete kadumine ja vargus. Antud riskide maandamiseks saab kasutusele võtta mitmeid

meetmeid ja esimeseks selliseks ongi mobiilse seadme kasutaja tuvastamine läbi kasutaja ekraaniluku koodi sisestamise (Souppaya & Scarfone, 2013).

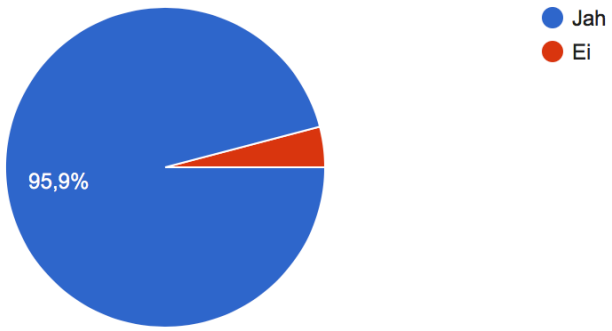


Diagramm 24. Ülevaade ekraaniluku rakendamisest.

Küsimus nr. 25

Küsimus kakskümmendviis "*Kas teie laps kasutab teie mobiilset seadet mängimiseks?*" andis veelkord kinnitust tavakasutajate poolsele kõrgele mobiilsete seadmete turvalisuse olulisuse hinnangule. Vastanutest vaid 12,9% (19 vastanut) annab oma mobiilse seadme lapsele kasutamiseks mängimise eesmärgil. 49,7% vastanutest (73 vastanut) kinnitas, et lapsed ei kasuta nende mobiilsed seadet ja 37,4% vastanutest (55. vastanul) ei olnud antud küsimusega üldse seost, sest nendel puudusid lapsed (vt. diagramm nr. 25).

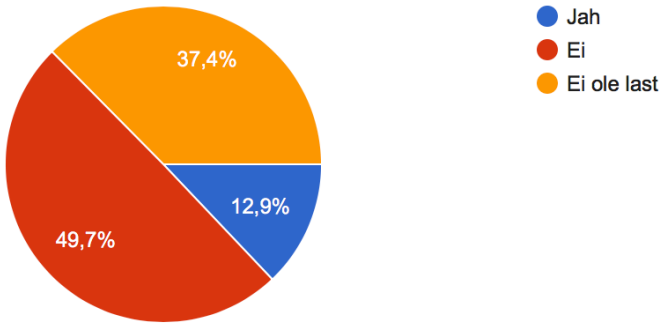


Diagramm 25. Ülevaade mobiilsete seadmete lastele kasutada andmisele.

Küsimus nr. 26

Küsimus number kakskümmendkuus "*Kas varundad oma mobiilseid seadmeid?*" andis ülevaate tavakasutajate suhtumisest nende mobiilsetes seadmetes oleva informatsiooni

terviklikkusesse. Selgus, et ligi pooled vastanud (48,3% ehk 71 vastanut) ei varunda oma mobiilset seadet. 27,9% (41 vastanut) vastanutest varundab mobiilseid seadmeid pilveteenustesse ja vaid 23,8% (35 vastajat) varundab oma mobiilset seadet arvutisse (vt. diagramm nr. 26). Antud tulemus peaks tegema murelikuks IT ja infoturbejuhte, sest andmete varundamine pilve teenustesse võiv küll tõsta käideldavust ja terviklikkust, kuid kindlasti vähendab andmete konfidentsiaalsuse tagamist. Nagu selgus ajakirjas "*Coputerweekly*" avaldatud Spiceworks uuringust, kardab 48% uuringus osalenud IT professionaalidest andmete kadu või konfidentsiaalsuse rikkumist, kui kasutatakse pilveteenuseid just andmete varundamiseks (Spiceworks, 2014).

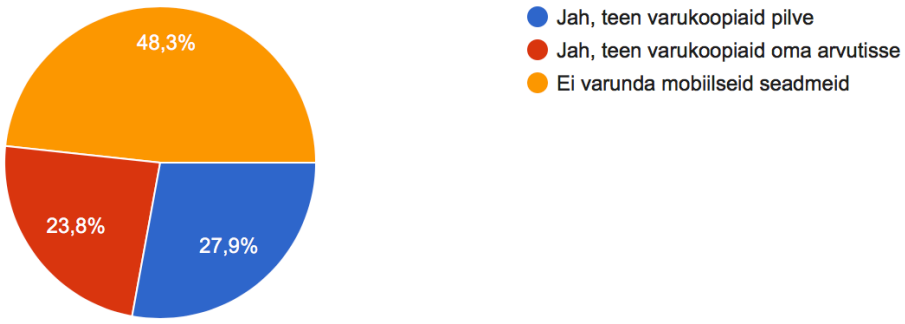


Diagramm 26. Ülevaade varukoopiate tegemisest

Küsimus nr. 27

Küsimusele kakskümmendseitse "*Kas teie mobiilne seade on tööandja kontrolli all?*" jagunesid vastused kolmeks peaaegu võrdseks osaks. Üks kolmandik (30,6%, ehk 45 vastanut) teadis, et nende mobiilne seade on tööandja kontrolli all. Teine kolmandik (32%, ehk 47 vastanut) olid veendumisel, et nende mobiilne seade ei ole tööandja kontrolli all ja viimane grupp (37,4% ehk 55 vastanut) ei olnud teadlik, et kas on nende mobiilne seade tööandja kontrolli all või mitte (vt. diagramm nr. 27). Antud suur protsent kõhklejaid viitab sellele, et kõikides asutustes ei ole välja töötatud või tutvustatud tavakasutajatele mobiilsete seadmete kasutamise poliitikat, kus vastavad tingimused oleks sätestatud. Timo Tarkmees on enda 2014 aasta magistritöö pealkirjaga "*Töökoht kui oht töötaja privaatsusele*" tulemusena öelnud, et: "*Seega võib väga selgelt väita, et töötajate privaatsus ning isikuandmete kaitse töösuhtes on hetkel sisuliselt täielikult kaitsmata ning olukorra parandamiseks tuleks esimesel võimalusel asjakohased meetmed kasutusele võtta. Alustada tuleb selgete regulatsioonide (seaduse)*

kehtestamisest, mis annaksid ühese selguse nii tööandjatele, kui ka töötajatele endile, et mis on tööandjale töötaja jälgimise juures lubatud ning mis mitte. " (Tarkmees, 2014)

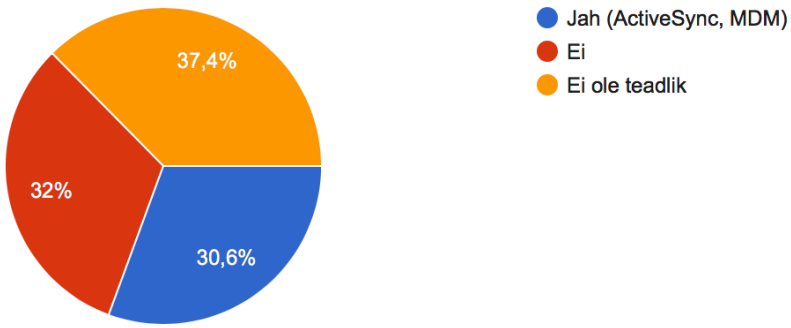


Diagramm 27. Tavakasutajate teadlikus mobiilse seadme tööandja poolse kontrolli kohta.

Küsimus nr. 28

Viimane küsimus number kakskümmendkaheksa "*Täitsin seda küsitlust ...* " andis autorile ülevaate hetke küsimustiku täitmiseks kasutatava seadme kohta, et näha mobiilsete seadmete kasutamise osakaalu antud küsimustiku täitmisel. Tulemustest selgus, et enamus (81.3% ehk 130 vastanut) vastasid küsimustikule kasutades lauaarvutit. 15% ehk 24 vastanut kasutas sülearvutit ja kõige vähem kasutati mobiilseid seadmeid (6 vastanut, ehk 3,7% vastanutest), mis jagunesid nelja kasutajaga (2,5% vastanutest) mobiiltelefonide ja kahe vastanuga (1,2% vastanutest) tahvelarvutite vahel (vt. diagramm nr. 28). Kõrge laua- ja sülearvutite osakaal viitab sellele, et küsimustikule vastati töö ajal ja enda töökohalt.

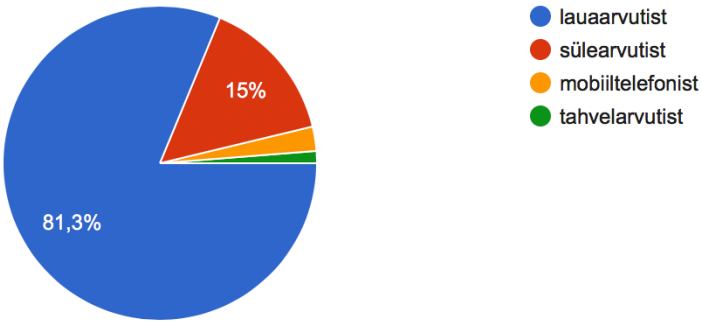


Diagramm 28. Ülevaade küsimustikule vastamiseks kasutatud seadmetest.

Möödunud peatükis esitles autor läbiviidud uuringu tulemusi ja analüüsis tulemusi tulenevalt püstitatud eesmärgist ja uurimisküsimustest lähtuvalt. Küsimustikule laekunud tulemuste analüüsimiseks ja töötlemiseks kasutas autor tarkvara PSPP. Kuna vabavaralisele tarkvarale PSPP ei ole sisse ehitatud graafikute funktsionaalsust, kasutas autor graafikute esitamiseks Google Forms poolt loodud diagramme.

6. MAGISTRITÖÖ JÄRELDUSED JA SOOVITUSED

Järgmises peatükis annab autor kirjeldava ülevaate uuringu tulemustest ja esitab soovitused EMM rakendamise ja mobiilsuse poliitika loomise kohta.

Eesti avalikus sektoris ei ole veel selgelt välja kujunenud ühtne mobiilsete seadmete kasutamise poliitika. Küll on mitu asutust juba võtnud kasutusele mobiilsete seadmete haldustarkvara lahendused, kuid autor leiab, et arvestades maailmas toimuvate muutuste kiirust, tuleks sellega aktiivsemalt ja kiiremini tegeleda. Ühe probleemina näeb autor korraldava ja kontrolliva asutuse, Riigi Infosüsteemi Ameti vähest mehitatus, et tulla toime antud valdkonnas toimuvate kiirete muutustega. Kahjuks ei õnnestunud autoril magistritöö esitamise ajaks saada RIA küberturvalisuse teenistuse käest tagasisidet kirjeldamaks riigi infoturbe eest vastutava asutuse poolset nägemust antud teemasse. Riigi Infosüsteemi Ametile esitatud küsimused on välja toodud lisa 1 lõpus.

Küsimustiku tagasiside põhjal tõdeb autor, et tavakasutajate teadlikkus mobiilsete seadmete turvalisuse kohta on kõrgel tasemel, kuid murelikuks teeb IT ja infoturbejuhtide hinnang mobiilsete seadmete turvalisuse olulisusele (vt. tabel nr. 6) . Kuigi küsitlusest selgub, et iOS operatsioonisüsteemiga telefonide osakaal (45,1%) ja tahvelarvutite osakaal (61,4%), on tavakasutajate hulgas suhteliselt kõrgel, mis autori hinnangul on rohkem turvalisust pakkuvad kui teise poole moodustavad android operatsioonisüsteemiga seadmed. Praktilise rakendamise käigus selgus, et Nii iOS kui ka Samsung Safe seadmed pakuvad enim hallatavuse võimalusi EMM lahenduste poolt, mis omakorda tagavad mobiilsete seadmete üldise turvalisuse.

Uuringust selgus, et avaliku sektori töötajad kasutavad peamiselt isiklikke mobiilseid seadmeid. Mobiiltelefonide puhul on osakaal küll väiksem *(vastanutest 60,3%, ehk 88 vastanut, kasutab isiklikku telefoni ja 39,7% ehk 58 vastajat on saanud telefoni tööandja poolt.)*, kui tahvelarvutite puhul *(isiklikud tahvelarvutid on 79,8% vastanutest, ehk 67 kasutajat ja vaid 20,2% ehk 17 tahvelarvuti kasutajat on saanud seadme tööandja käest (vt. diagramm 11))*, kuid siiski on üle pooltel töötjatel isiklikud seadmed. Tulenevalt isiklike seadmete kasutamisest, on ka mobiilsete seadmete riistvara ülevaade päris kirju. Mobiiltelefonide puhul on Android ja iOS seadmete kaalud peaaegu võrdsed, hõivates kumbki ligi poole kasutajate

arvust. Windows operatsioonisüsteemiga seadmed ja muud seadmed moodustavad vaid kümnendiku kogu seadmete arvust (vt. Diagramm 8). See on ka selge kinnitus väite kohta, et mobiilsete seadmete kasutusmugavus on toote valikul esmatähtis. Kasutusmugavus tahvelarvutite puhul ja sellest tehtud valik torkab küsitluse tulemustest eriti hästi silma. Suure ülekaaluga haaras esikoha Apple iPad, millele järgnes Android operatsioonisüsteemiga seadmete valik. Tahvelarvutite puhul moodustas Windows ja muude operatsioonisüsteemide hulk vaid 8,4% seadmete koguarvust (vt. Diagramm 10).

Autor leiab, et üha enam Eesti avaliku sektori asutusi hakkab endale tunnistama mobiilsete seadmete turvalisuse probleemi ja vajadust mobiilsete seadmete haldustarkvara järele. Kasutajate seisukohast tekib EMM lahendusega mitmeid õigustatud küsimusi, alates kasutaja isikuandmete kaitsest kuni kasutaja mobiilsete seadmete kasutusmugavuseni välja. Loodavad lahendused ei tohiks tuua kaasa teenuste kasutamisel ebamugavusi, kuna sellisel juhul pöörduvad kasutajad hoopis alternatiivsete ja käepärasemate lahenduste kasutamisele. Kuna hetkel ei ole autorile teada, et Eestis oleks välja töötatud parimad praktikad mobiilsete seadmete haldustarkvara juurutamise kohta, siis teeb autor siinkohal ettepaneku vastavad juhised RIA küberturvalisuse teenistusel luua. EMM lahenduse juurutamisega kaasnevad ka omad riskid, mida autor kirjeldas punktis 2.4. Võttes neid riske arvesse ja püüdes neid maandada on siiski võimalik pigem suurendada asutuse informatsiooni terviklikkuse, käideldavuse kui konfidentsiaalsuse tagamist. Uuringust selgus, et pooled vastanud asutused kasutavad või plaanivad kasutusele võtta EMM lahendust.

Samuti tuleks asutustel välja töötada ettevõtte mobiilsuse poliitika, kus oleks kajastatud ka nii kasutajate õigused kui kohustused. Selleks, et poliitikat hakata välja töötama, tuleks esitada endale mõned küsimused (Fiorenza, Tepe, Ribeira, & Vogel, 2012) :

- kes on seadme omanik?
- kes vastutab seadmele tekitatud kahju, kadumise või hoolduse eest?
- kuidas toimub seadmetele rakenduste paigaldamine?
- kes vastutab seadme tarkvara uuenduste eest?
- milliseid rakendusi võib seadmesse paigaldada ja kui on tegemist töötaja isikliku seadmega, siis millised õigused on tööandjal seadme üle?
- milliseid seadme funktsioone võib piirata?

- kas töötaja võib kasutada mobiilset seadet pildistamise ja videote tegemiseks?
- kuidas reegleid rakendada?
- Kuidas ettevõtte mobiilsuse poliitika läheb kokku teiste asutuses kehtestatud reeglistikuga?

Vastused osadele küsimustele tunduvad küll ilmselged, kuid nendele tuleks siiski poliitika loomise protsessis vastused fikseerida, et kogu protsess kulgeks plaanitult.

Näidisena poliitika loomise protsessiks võib kasutada järgnevat viite punkti (Fiorenza et al., 2012) :

- **kohtu kõikide osapooltega, et luua testgrupp, kes lahendust testima hakkaksid.**

  Vajalik on kaasata liikmeid nii juhtkonna tasandilt kui ka kõikidest sisupoolt esindavatest allüksustest, et saaks projekti tutvustada ja saaks vajaliku tagasiside juba esimeses faasis. See on vajalik, et asutusel tekiks ühtne arusaam ja visioon ettevõtte mobiilsuse poliitikast.

- **kohtu juristidega.**

  Kuna avaliku sektori asutuste hulgas on EMM lahendused veel suhteliselt uus nähtus, siis on vaja tutvustada juristidele antud lahendust, et arutada läbi võimalikud kaasnevad õiguslikud riskid.

- **koosta esialgne mustand ettevõtte mobiilsuse poliitika kohta.**

  Poliitika võiks sisaldada endas näiteks kirjeldust asutuse ressurssidele juurdepääsemise võimalustele, läbipaistvaid turvameetmeid, isikliku ja asutuse andmete lahususe printsiipe konteinerlahenduse näol, regulatsioone rakenduste kasutamise kohta, kirjeldust seadmete tugiteenuse kohta ja kirjeldust töö ning eraelu vahelise tasakaalu kohta. Samuti ei tohi ära unustada sisendit, mille andsid nii juristid kui teised seotud osapooled.

- **tutvusta mobiilsete seadmete halduslahendust töötajatele.**

  Iga uue tarkvara või rakenduse kasutajatele viimine on on seotud riskiga saada kriitilist tagasisidet. Koosta korralik teavituskava ja ole valmis vastama kõikidele tekkivatele küsimustele. Korduma kippuvate küsimuste olemasolu antud hetkel on ülimalt soovituslik.

- **hinda ja vaata üle saadud tulem ning paranda loodud poliitikat.**

  Kui mobiilsete seadmete haldustarkvara lahendus on juba kasutusele võetud, siis ära unusta perioodiliselt küsida tagasisidet nii kasutajatelt kui administraatoritelt lahenduse toimimise kohta. Saadud tagasiside koos püstitatud eesmärkidega on oluline, et parandada nii ettevõtte mobiilsuse poliitika, kui mobiilsete seadmete haldustarkvara toimivust.

(Fiorenza et al., 2012)

Riigi Infosüsteemi Ameti Kriitilise Informatsiooni Infrastruktuuri Kaitse osakond on tõdenud, et turvateadlikus nutitelefonide vallas ei ole väga kõrge ja seetõttu on loonud juhendi mobiilsete seadmete turvapoliitika loomiseks. Nimetatud juhendi eesmärk on anda põgus ülevaade nutitelefonide kasutamisega seotud ohtudest ja tutvustada nutitelefonide turvamiseks mõelduid meetmeid. Juhend põhineb ISKE's kirjeldatud turvameetmetel ja on abivahend kõikidele asutustele, kellel on kohustus ISKE-t rakendada. (Rattas, n.d.)

Eelnenud peatükis andis autor kirjeldava ülevaate uuringu tulemustest ja esitas soovitused EMM rakendamise ja mobiilsuse poliitika loomise kohta.

KOKKUVÕTE

Antud magistritöö eesmärk oli kirjeldada Eesti avaliku sektori hetkeolukorda seoses mobiilsete seadmete kasutamisega ja esitada praktilised soovitused, et mobiilsete seadmete kasutamine oleks turvaline ja samas kasutajasõbralik. Töö sisaldas nii online küsitlust kui EMM lahenduse praktilist rakendamist avaliku sektori asutuse (ministeeriumi) näitel, et kirjeldada lahenduse juurutamiseks vajalikud soovitused.

Esimeses osas andis autor ülevaate püstitatud probleemi olemusest ja oodatud tulemustest koos magistritöö uurimismetoodika kirjeldusega. Samuti kirjeldas autor ära töö eesmärgi ning põhjenduse töö teema valikuks. **Teises osas** andis autor ülevaate mobiilsete seadmete haldustarkvara ja ettevõtte mobiilsuse halduslahenduse olemusest ja vajalikkusest. **Järgnevalt** kirjeldas autor erinevaid mobiilsete seadmete haldustarkvara lahendusi ning esitas Forresteri poolt koostatut raporti tulemused pika nimekirja kohta ning hindas lühikest nimekirja Saaty analüütiliste hierarhiate meetodi abil. Antud analüüsi aluseks oli lähtutud reaalsest funktsionaalsuse vajadusest, millele tuginedes autor kirjeldas mobiilsete seadmete haldustarkvara lahenduse praktilist paigaldamist. **Neljas etapp** andis ülevaate läbi viidud uuringust ja selle metoodikast, mille valimi moodustasid neljateistkümne avaliku sektori asutuse IT ja infoturbejuhid ning tavakasutajad. **Viiendas etapis** analüüsis autor küsitluse tulemusi ning esitas püstitatud hüpoteeside tulemused koos järeldustega. **Viimane peatükk** andis ülevaate magistritöö tulemustest, kus autor esitas ka soovitused ettevõtte mobiilsuse halduse lahenduse juurutamiseks.

Tulenevalt tööle seatud eesmärgist olid koostatud uurimisküsimused järgmised:

- mil määral on Eesti avalik sektor endale püstitatud probleemi tunnistanud ja kuidas suhtuvad probleemi ja võimalikesse lahendustesse nii kasutajad kui turvalisuse eest vastutajad?
- millised ja kas on välja töötatud parimad praktikad avaliku sektori üleselt?
- millised probleemid võivad tekkida seoses EMM rakendamisega?
- milline EMM lahendus oleks Eesti avaliku sektori asutusele sobivaim?

Uurimistöö käigus leidis autor vastused kõikidele uurimisküsimustele. Selgus, et Eesti avalik sektor ei ole üheselt tunnistanud vajadust mobiilsete seadmete haldustarkvara järele ja ei ole üheselt aru saadud ohtudest, mis kaasnevad asutustele seoses mobiilsete seadmete laialdase ja kontrollimatu levikuga. Samuti selgus, et tavakasutajad muretsevad mobiilsete seadmete turvalisuse pärast rohkem, kui seda teevad asutuste IT ja infoturbejuhid. Seega peab autor ümber lükkama Magistritöö alguses püstitatud oodatava tulemuse , mis oli kinnitus selle kohta, et avaliku sektori mobiilsete seadmete kasutajad ei ole endale tõstatanud turvalisuse probleemi, mis on vastand infoturbe eest vastutavatele isikutele. Samuti sai autorile selgeks, et avaliku sektori asutuste üleselt ei ole Eestis täna välja töötatud parimaid praktikaid mobiilsete seadmete haldustarkvara juurutamiseks. Küll on Riigi Infosüsteemi Ameti Kriitilise Informatsiooni Infrastruktuuri Kaitse osakond loonud juhendi mobiilsete seadmete turvapoliitika loomiseks, mis põhineb ISKE meetmetel ja on mõeldud eelkõige abivahendiks ISKE-t rakendavate asutuste jaoks. Antud juhend on aga liiga üldine ja ei keskendu mobiilsete seadmete haldustarkvara lahendusele. Uuringust selgus, et küsitluses osalenud neljateistkümnest asutusest vaid seitsmel on kasutusel või planeerimisel mobiilsete seadmete haldamiseks lahenduse loomine. EMM lahenduse rakendamisega kaasnevad ka mitmed riskid ja probleemid. Uurimistööst selgus, et EMM lahenduse loomine moodustab asutuse informatsiooni konfidentsiaalsuse, terviklikkuse ja käideldavusele uued ja seni tundmatud riskid. Samas neid riske teadvustades ja õigesti maandades, on võimalik tagada piisav turvalisus asutuse informatsioonile. Kasutajate seisukohast toob lahenduse loomine kaasa mitmeid isikuandmete kaitsega seotud küsimusi. Siinkohal leidis autor, et on vajalik luua korrektne mobiilsete seadmete kasutamise poliitika, kus oleks ära kirjeldatud nii töötaja kui tööandja õigused ja kohustused. Sobivaim EMM tarkvara avaliku sektori asutuse jaoks peab katma ära nii asutuse poolse informatsiooni kaitse vajadused kui ka töötaja isiklikku informatsiooni privaatsuse. Kasutada tuleb konteinertüüpi tarkvaralisi lahendusi, mis hoiavad tööandja ja töötaja isikliku andmestiku lahus ja piiravad kontrollimatut ja pahatahtlikud andmete levikut mobiilsetest seadmetest. Kasutatavate mobiilsete seadmete tootja ja mark tuleb fikseerida projekti alguses, et välistada reeglite erandite tegemise vajadus tulenevalt seadmete iseärasustest.

Autor leiab, et magistritöö on täitnud püstitatud eesmärgi ja loob vajaliku ülevaate Eesti avaliku sektori hetkeolukorrast ja tegevustest, mida on tarvis rakendada, et mobiilsete seadmete kasutamine oleks turvaline ja samas kasutajasõbralik. Magistritöö annab lähtepinna riigi andmete konfidentsiaalsuse eest vastutavatele üksustele edasiste sammude tegemiseks.

RÉSUMÉ

Usage and Security of Mobile Device Management Software. The Case of an Estonian Public Sector Institution

Author: Kristo Kaasan

The world is changing rapidly, but the technology what man produces, develops even faster. In today's society the strict borders between personal and business life is vanishing and more personal devices are being used with work related tasks. Mobility and the use of tablets and mobile phones as replacements for personal computers and laptops, brings new challenges to employers and to employees themselves. The main persons who get concerned are CIO's and persons who are responsible for InfoSec, who will soon start noticing that more and more sensitive information are being carried along with employees' personal mobile devices. The radical steps would be to deny the possibilities to Access work relates information through mobile devices, but another solution is to implement Mobile Device Management system (MDM), what has become today Enterprise Mobility Management solution (EMM). With EMM solution we can assure, that with using mobile devices, the company's information confidentiality, integrity and accessibility.

The objective of this master's thesis is to give overview about the use of mobile device policy, most common mobile devices and the use cases regarding mobile devices. Also the author investigates, which solutions are being used to protect and to manage mobile devices and what are the threats what users and administrators see regarding the use of mobile devices.

Author has four research question in this master's thesis:

1. Has Estonian public sector organizations acknowledged itself the problems with using mobile devices and how do employees and the persons who are responsible about InfoSec concern to the outcome of possible solutions?
2. Are there best practices worked out across the public sector?
3. What could be possible problems when implementing Enterprise mobility management solution?

4. What kind of EMM solution would fit the best to the Estonian public sector organization?

Author split the master's thesis into two parts. First part introduced the theoretical background of MDM and EMM solutions which was complemented by practical EMM solution implementation at the example of Estonian Ministry of Foreign Affairs. Second part of master's thesis included the qualitative research carried out by the questionnaires within the heads of IT and information security departments within 14 different organizations and 161 employees.

The results of theoretical and research part showed, that all Estonian public sector organizations haven't acknowledged the need for EMM solutions and realised the threats what accompanied by the uncontrolled use of mobile devices. Research revealed that users are more concerned regarding the security issues of mobile devices as the persons who are in charge of IT or InfoSec. The lack of central authority who would introduce the policies for EMM solutions has its own consequences what are shown in the results of questionnaire also. Only seven organizations from fourteenth has introduced or are introducing the policy for use of mobile devices. Here the Estonian Information System Authority should take the leading role and introduce the threats and possible solution of using mobile devices within the public sector organizations. As the perspective of users, the EMM solutions bring several issues regarding the use of personal information. As organizations has the possibilities to locate your devices or remotely wipe them, there is need for strict policies where the rights and obligations are introduced for both, to user and to organization side. Author found out, that the right EMM solution should cover the protection of organization information and user personal information. The must is to use containerized solution to keep personal and business information separated and the type and manufacturer of mobile devices should be fixated to prevent changes in rules later as not all the devices share the same management possibilities.

The outcome of this master's thesis can be used for the next steps, to implement central regulations across public sector organizations to manage and handle information within mobile devices.

KASUTATUD KIRJANDUS

Braunstein, C. J. (2012). Mobile device management, 28–31.

ComScore. (2014). The U.S. Mobile App Report, 1–18.

EMOR. (2014). Nutiseadmete kasutajate turvateadlikkuse ja turvalise käitumise uuringuaruanne.

Ericsson. (2015). Ericsson Mobility Report.

Fiorenza, P., Tepe, L., Ribeira, J., & Vogel, V. (2012). Exploring Bring Your Own Device In The Public Sector.

Forman, E., & Selly, M. (2003). Decision by objectives. *Journal-Operational Research Society*, *54*, 1108. http://doi.org/10.1142/9789812810694

Kane, C. (2015). *The Forrester WaveTM: Enterprise Mobile Management, Q4 2015*.

Lua. (2015). *Enterprise Mobility Management 101*.

Netekspert. (2016). Saaty kalkulaator. Viimati külastatud 20 märts 2016 http://www.netekspert.com/calculators/saaty/setup_est.asp

Palm, M. (2015). Infoturve vosk põhimõtte rakendamisel as eesti telekomi näitel. *Magistritöö*.

Pervez, G., & Kjell, G. (2004). *Äriuuringute meetodid: praktilisi näpunäiteid*. Külim.

Rattas, R. (n.d.). Juhend mobiilsete seadmete turvapoliitika loomiseks Sissejuhatus, 1–7.

Rhee, K., Jeon, W., & Won, D. (2012). Security Requirements of a Mobile Device Management System. *International Journal of Security and Its Applications*, *6*(2).

Rhee, K., Won, D., Jang, S. W., Chae, S., & Park, S. (2013). Threat modeling of a mobile device management system for secure smart work. *Electronic Commerce Research*, *13*(3), 243–256. http://doi.org/10.1007/s10660-013-9121-4

Riigi Infosüsteemi Amet. (n.d.-a). ISKE juhendid ja materjalid. Külastatud 15 märts 2016, from https://www.ria.ee/ee/iske-dokumendid.html

Riigi Infosüsteemi Amet. (n.d.-b). Külastatud 4 Märts 2016, https://www.ria.ee/ee/index.html

SA Eesti Koostöö Kogu. (2013). Ülevaade riigiorganisatsioonist . Vahekokkuvõte, (4), 1–12.

Souppaya, M., & Scarfone, K. (2013). Guidelines for Managing the Security of Mobile Devices in the Enterprise. http://doi.org/10.6028/NIST.SP.800-124r1

Spiceworks. (2014). MAIN CONCERNS OF USING CLOUD BACKUP. *Computer Weekly*, *1/7*, p3–3. 1/4p.

Tarkmees, T. (2014). *Töökoht kui oht töötaja privaatsusele*.

Terrence, C., Smith, R., Silva, C., Taylor, B., Girard, J., & Basso, M. (2015). Magic Quadrant

for Enterprise Mobility Management Suites Market Definition / Description, (June), 1–12.

Välisministeerium. (2014). Arengukavad ja tegevuskavad. Külastatud 15 märts 2016, http://vm.ee/et/arengukavad-ja-tegevuskavad

Vallaste, H. (n.d.). vallaste.ee. Külastatud viimati 16 märts 2016, http://vallaste.ee/

Veldre, A., Hanson, V., Laur, M., Buldas, A., & Krasnosjolov, J. (2016). AKIT - Andmekaitse ja infoturbe seletussõnastik. Cybernetica AS. Külastatud 2 märt 2016, http://akit.cyber.ee

Wikipedia. (n.d.). et.wikipedia.org. Külastatud 16 märtd 2016, https://et.wikipedia.org

LISA 1. UURIMUSTÖÖ KÜSIMUSTIK

1. Mis on teie sugu?

    - Mees
    - Naine

2. Mis on teie vanus?

    - ... - 20
    - 21 - 30
    - 31 - 40
    - 41 - 50
    - 51 - 60
    - 61 - ...

3. Määratle enda roll

    - Olen tavakasutaja (Ei koosta ega rakenda turvapoliitikaid asutuses)
    - Olen IT juht / infoturbejuht (Vastutan ja korraldan mobiilsete seadmete turvalisust)

4. Teie asutuse nimi

    -

5. Kui palju on teie asutuses töötajaid

    - ... - 500
    - 501 - 1000
    - 1001 - 1500
    - 1501 - 2000
    - 2001 - ...

6. Kas kasutate mobiiltelefoni?

    - Jah
    - Ei

7. Kas kasutate tahvelarvutit?

    - Jah
    - Ei

8. Mis operatsioonisüsteemiga telefoni kasutate

    - iOS
    - Android
    - Windows
    - Muu...

9. Kas telefon on tööandja poolt antud?

    - Jah
    - Ei

10. Mis operatsioonisüsteemiga tahvelarvutit kasutate

    - iOS
    - Android
    - Windows
    - Muu...

11. Kas tahvelarvuti on tööandja poolt antud?

    - Jah
    - Ei

12. Kas jagate töötajatele asutuse mobiilse seadme?

- Jah, tagame töötajale seadmed
- Ei, Töötaja peab ise seadmed ostma
- Nii ja naa, selget poliitikat ei ole rakendatud

13. Kui oluline on teie jaoks mobiilsete seadmete turvalisus?

- Vähe oluline 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 Väga oluline

14. Kui oluline on teie jaoks mobiilsete seadmete kasutusmugavus?

- Vähe oluline 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 Väga oluline

15. Kas teie asutuses on loodud mobiilsete seadmete kasutamiseks poliitika?

- Jah
- Ei
- On loomisel

16. Mis teenuseid lubate kasutada mobiilsetest seadmetest?

- Asutuse e-post
- Asutuse siseveeb
- Dokumendihaldus
- Muu...

17. Kas teie asutuses on kasutusel mobiilsete seadmete haldustarkvara lahendus?

- Jah
- Ei
- On planeerimisel

18. Milliseid teenuseid oma mobiilsetest seadmetest kasutad?

- Töö e-post
- Isiklik e-post
- Internet
- Facebook
- Twitter
- Pildistamist
- Kontoritarkvara
- Muu...

19. Kui oluline on teie jaoks mobiilsete seadmete turvalisus?

- Vähe oluline 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 Väga oluline

20. Kui oluline on teie jaoks mobiilsete seadmete kasutusmugavus?

- Vähe oluline 1 ; 2 ; 3 ; 4 ; 5 ; 6 ; 7 Väga oluline

21. Kas teie seadmetel on seadistatud ekraanilukk?

- Jah
- Ei

22. Kas teie laps kasutab teie mobiilset seadet mängimiseks

- Jah
- Ei
- Ei ole last

23. Kas varundad oma mobiilseid seadmeid?

- Jah, teen varukoopiaid pilve
- Jah, teen varukoopiaid oma arvutisse
- Ei varunda mobiilseid seadmeid

24. Kas teie mobiilne seade on tööandja kontrolli all

- Jah (ActiveSync, MDM)
- Ei
- Ei ole teadlik

25. Millist MDM lahendust kasutate

- Airwatch
- Sophos
- MS Intune
- Citrix
- MS Exchange (ActiveSync)
- Muu...

26. Kas kasutate pilveteenust või on-premise lahendust?

- Pilveteenust
- On-premise lahendust
- Hübriid

27. Märkige, et millised reeglid on MDM seadistuse juures olulised teie jaoks.

- Klahviluku seadistamine
- Seadme automaatne lukustus
- Seadme kaugtühjendus
- Seadme lokatsiooni tuvastamine
- Tulemüür
- Antiviirus
- VPN tugi
- Ekraanipildi tegemise keelamine
- Whitelist ja Blacklist rakenduste nimekirjade olemasolu
- Turvapoliitikale vastavusreeglite loomine
- Seadmete kasutusinfo saamine

Lisaks antud küsimustikule saatis autor kommentaaride saamiseks järgmised küsimused Riigi infosüsteemi ameti küberturvalisuse teenistusele:

> 1. Kui suur oli mobiilsete seadmetega toimunud registreeritud turvaintsidentide arv aastatel 2014 ja 2015? (2014 aruandes on mainitud vaid libatugijaamade probleem ja 2015 aruannet veel ei ole väljastatud).
>
> 2. Kas RIA on teinud või planeerib teha mobiilsete seadmete turvalisust puudutavaid teavituskampaaniaid?
>
> 3. KIIK on loonud juhendi mobiilsete seadmete turvapoliitika loomiseks, mis on loodud ISKE's kirjeldatud moodulite alusel ja peaks olema rakendatud kõigil, kes on ISKE kohustlased. Minu 2016 aasta veebruaris tehtud küsitlus, näitas aga, et neljateistkümnest asutusest vaid kuuel oli kinnitatud mobiilsete seadmete kasutamise poliitika ja ülejäänutel kas oli loomisel või puudus üldse. Kas RIA'l on plaanis

uuendada antud soovitust ja kas võib leiduda võimalus, et muuta asutustele mobiilsete seadmete haldamine ja vastava poliitika loomine kohustuslikuks?

4. Kas RIA küberturvalisuse teenistus näeb ohtu mobiilsete seadmete kasutamises ilma täiendavate kontrollvahenditeta?

5. Kas mobiilsete seadmete turvalisus on üldse teema, millele tuleks ühtselt/keskselt tähelepanu pöörata?

LISA 2. AIRWATCH POOLT HALLATAVAD SEADMETE SÄTTED

Järgnevalt on esitatud Airwatch poolt toetatud iOS ja Android operatsioonisüsteemi hallatatavad funktsionaalsused, tuues välja ka toetatud operatsioonisüsteemi versiooni. Andmed pärinevad Airwatch administreerimise keskkonnast.

iOS seadmete funktsionaalsuse kirjeldus:

Device Functionality

Allow use of camera	
Allow video conferencing	
Allow screen capture	
Allow passcode modification	iOS 9 + Supervised
Allow Touch ID to unlock device	iOS 7
Allow Touch ID modification	iOS 8 + Supervised
Allow use of iMessage	iOS 6 + Supervised
Allow installing public apps	
Allow App Store icon on Home screen	iOS 9 + Supervised
Allow app removal	iOS 6 + Supervised
Allow in-app purchase	
Allow documents from managed sources in unmanaged destinations	iOS 7
Allow automatic app downloads	iOS 9 + Supervised
Allow changes to cellular data usage for apps	iOS 7 + Supervised
Allow documents from unmanaged sources in managed destinations	iOS 7
Force limited ad tracking	iOS 7
Allow Handoff	iOS 8
Allow automatic sync while roaming	
Allow voice dialing	
Allow internet results in Spotlight	iOS 8 + Supervised
Allow Siri	iOS 5
Allow Siri while device locked	iOS 5.1
Enable Siri Profanity Filter	iOS 6 + Supervised
Show user-generated content in Siri	iOS 7 + Supervised
Allow manual profile installation	iOS 6 + Supervised
Allow configuring Restrictions	iOS 8 + Supervised
Allow Erase All Contents and Settings	iOS 8 + Supervised
Allow device name modification	iOS 9 + Supervised
Allow wallpaper modification	iOS 9 + Supervised
Allow account modification	iOS 7 + Supervised
Require passcode on first AirPlay pairing	iOS 7.1
Allow Passbook notifications in Lock screen	iOS 6
Show Control Center in Lock screen	iOS 7
Show Notifications Center in Lock screen	iOS 7
Show Today view in Lock screen	iOS 7
Allow AirDrop	iOS 7 + Supervised
Enforce AirDrop as an unmanaged drop destination	iOS 9
Allow Apple Watch pairing	iOS 9 + Supervised
Enforce Wrist Detection on Apple Watch	iOS 8.3

Allow keyboard shortcuts	iOS 9 + Supervised
Allow predictive keyboard	iOS 8 + Supervised
Allow auto correction for keyboard	iOS 8 + Supervised
Allow spell check for keyboard	iOS 8 + Supervised
Allow definition lookup for keyboard	iOS 8 + Supervised

Applications

Allow use of YouTube	iOS 5 and below
Allow use of iTunes Music Store	
Allow use of iBookstore	iOS 6 + Supervised
Allow Game Center	iOS 6 + Supervised
Allow multiplayer gaming	
Allow adding Game Center friends	
Allow changes to Find My Friends	iOS 7 + Supervised
Allow use of Safari	
Allow News	iOS 9 + Supervised
Allow Radio Service	iOS 9 + Supervised
Allow Music Service	iOS 9 + Supervised
Allow Podcasts	iOS 8 + Supervised
Enable autofill	
Force fraud warning	
Enable JavaScript	
Block pop-ups	
Accept Cookies	
Show Apps	iOS 9 + Supervised
Hide Apps	iOS 9 + Supervised

iCloud

Allow backup	iOS 5
Allow document sync	iOS 5
Allow keychain sync	iOS 7
Allow managed apps to store data	iOS 8
Allow backing up Enterprise Books	iOS 8
Allow synchronizing Enterprise Books notes and highlights	iOS 8
Allow Photo Stream	iOS 5
Allow Shared Photo Stream	iOS 6
Allow iCloud photo library	iOS 9
Security and Privacy	
Allow user to trust unmanaged enterprise apps	iOS 9
Force iTunes Store password entry	iOS 5
Allow diagnostic data to be sent to Apple	iOS 5
Allow user to accept untrusted TLS certificates	iOS 5
Allow over the air PKI updates	iOS 7
Force encrypted backups	
Allow pairing with non-Configurator hosts	iOS 7 + Supervised
Media Content	
Ratings region	
Movies	
TV Shows	
Apps	
iBooks	iOS 6 + Supervised
Allow explicit music and podcasts	

Android seadmete funktsionaalsuse kirjeldus:

Restrictions

Device Functionality	
Allow Camera	Android 4.0+
Allow Microphone	Lenovo v1+
Allow Factory Reset	SAFE v2+
Allow Airplane	ModeLG v2.0+
Allow screen capture	SAFE v2+
Allow Mock Locations	SAFE v2+
Allow Clipboard	SAFE v2+
Allow USB Media Player	SAFE v2+
Allow NFC	SAFE v2+
Allow NFC State Change	SAFE v5+
Allow Home Key	SAFE v2+
Allow Email Account Addition	SAFE v4+
Allow Google Account Addition	SAFE v4+
Allow POP / IMAP Email	LG v1.0+
Allow Power Off	SAFE v3+
Allow Safe Mode	SAFE v4+
Allow Status Bar	SAFE v3+
Allow Notifications	SAFE v3+
Allow Wallpaper Change	SAFE v3+
Allow Audio Recording if Microphone is Allowed	SAFE v4+
Allow Video Recording if Camera is Allowed	SAFE v4+
Allow Ending Activity When Left Idle	SAFE v4+
Allow User to Set Background Process Limit	SAFE v4+
Allow Headphones	SAFE v5+
Allow All Location Services	Sony v5+
Allow Device Administrator Deactivation	Sony v6+

Sync And Storage

Allow USB	LG v1.0+
Allow USB Debugging	Lenovo v1+
Allow USB Mass Storage	Lenovo v1+
Allow Google Backup	SAFE v2+
Allow Google Accounts Auto Sync	SAFE v5+
Allow SD Card Access	Lenovo v1+
Allow OTA Upgrade	SAFE v3+
Allow SD Card Write	SAFE v3+
Allow USB Host Storage	SAFE v4+
Allow SD Card Move	SAFE v5+
Allow Local Desktop Sync	Sony v1+

Application

Allow Google Play	SAFE v2+
Allow YouTube	SAFE v2+
Allow Access To Device Settings	SAFE v2+

Allow Account Settings	Nook v1+
Allow Application Settings	Nook v1+
Allow Developer Options	Nook v1+
Allow Non-Market App Installation	Lenovo v1+
Allow Background Data	SAFE v2+
Allow Voice Dialer	SAFE v2+
Allow Google Crash Report	SAFE v3+
Allow Android Beam	SAFE v4+
Allow S Beam	SAFE v4+
Allow S Voice	SAFE v4+
Allow Amazon Mayday	Kindle v1+
Allow Copy & Paste Between Different Applications	SAFE v4+
Allow User To Stop System Signed Applications	SAFE v4+

Bluetooth

Allow Bluetooth	Lenovo v1+
Force Bluetooth On	Bluebird
Allow Outgoing Calls Via Bluetooth	SAFE v2+
Allow Bluetooth Discoverable Mode	SAFE v2+
Allow Bluetooth Limited Discoverable Mode	SAFE v2+
Allow Bluetooth Pairing	SAFE v2+
Allow Bluetooth Data Transfer	SAFE v2+
Allow Desktop Connectivity Via Bluetooth	SAFE v2+
Enable Bluetooth Device Restrictions	SAFE v3+
Enable Bluetooth Secure Mode	SAFE v4+

Network

Allow Wi-Fi	SAFE v2+
Force WiFi On	
Allow Cellular Data	SAFE v2+
Allow WiFi Profiles	SAFE v2+
Allow WiFi Changes	SAFE v2+
Allow Unsecure WiFi	SAFE v4+
Allow Auto Connection WiFi	SAFE v4+
Allow WiFi to Disconnect During Sleep	MX v1.3+
Allow Prompt for Credentials	SAFE v2+
Minimum WiFi Security Level	SAFE v2+
Allow Only Secure VPN Connections	SAFE v4+
Blocked WiFi Networks	SAFE v2+,LG v1.0+
Allow Sending SMS	LG v1.0+
Allow Native VPN	SAFE v2+
Allow WiFi Direct	SAFE v4+
Allow Infrared	Sony v4+

Roaming

Data Usage on Roaming	Lenovo v1+
Allow Automatic Sync on Roaming	SAFE v2+
Allow Push Messages on Roaming	SAFE v2+
Allow Roaming Voice Calls	SAFE v3+

Allow Auto Sync When Roaming Is Disabled	SAFE v4+

Tethering

Allow All Tethering	Lenovo v1+
Allow WiFi Tethering	Lenovo v1+
Allow Bluetooth Tethering	SAFE v2+
Allow USB Tethering	SAFE v2+

Browser

Allow Native Android Browser	SAFE v2+
Allow Pop-Ups	SAFE v2+
Allow Cookies	SAFE v2+
Enable Autofill For Android	SAFE v2+
Enable Java Script For Android	SAFE v2+
Force fraud warning	SAFE v2+

Location Services

Allow GPS Location Services	SAFE v2+
Allow Wireless Network Location Services	SAFE v2+
Allow Passive Location Services (Not Applicable for VzW SAFE Devices)	SAFE v2+

Phone And Data

Allow Non-Emergency Calls	SAFE v2+
Allow User to Set Mobile Data Limit	SAFE v4+
Allow SMS with storage	SAFE v4+
Allow MMS with storage	SAFE v4+
Allow WAP Push	SAFE v4+

Miscellaneous

Set Device Font	SAFE v4+
Set Device Font Size	SAFE v4+

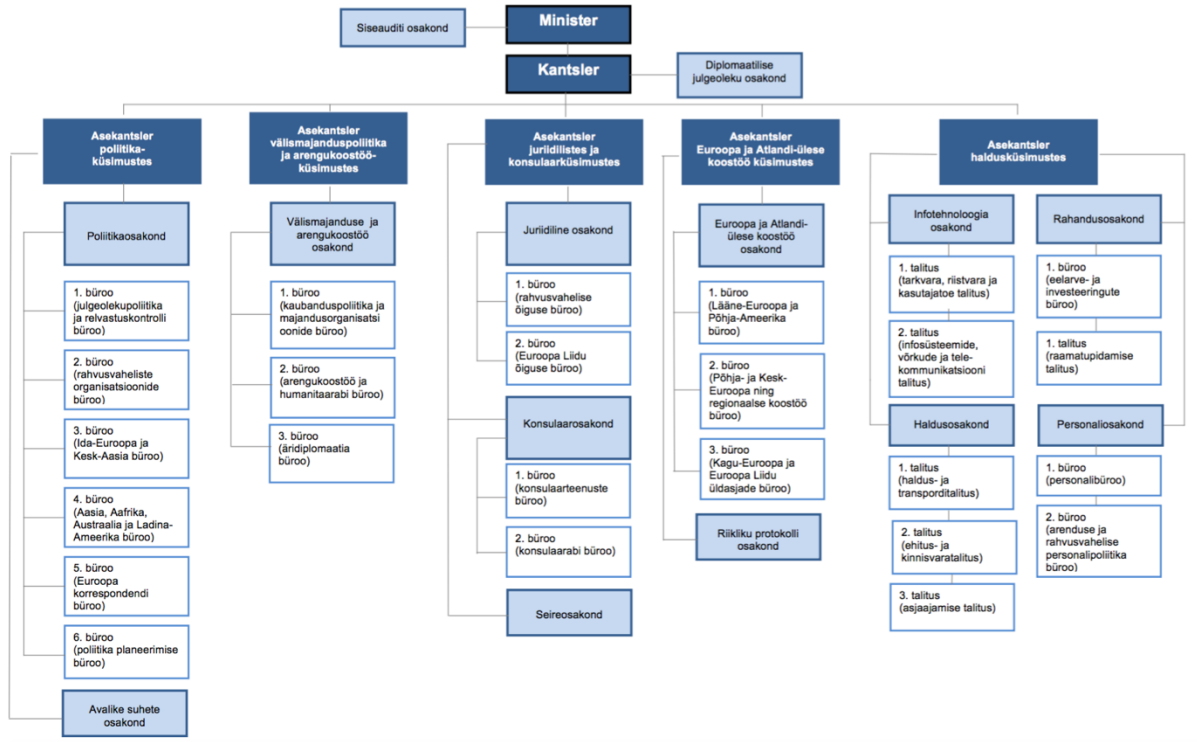
Hardware Restrictions

Allow System Bar	SAFE v3+
Allow Task Manager	SAFE v3+
Allow Menu Key	SAFE v3+
Allow Back Key	SAFE v3+
Allow Search Key	SAFE v3+
Allow Volume Key	SAFE v3+

Security

Allow Activation Lock	SAFE v5+
Force Fast Encryption	SAFE v5+
Allow Firmware Recovery	SAFE v5+
Allow Lock Screen Settings	SAFE v5+

LISA 3. MINISTEERIUMI STRUKTUURI NÄIDIS



Joonis 8. Ministeeriumi struktuur

(allikas: http://vm.ee/sites/default/files/content-editors/vm_struktuur.pdf)

Magistritöö elektrooniline versioon:

http://lingid.ee/YFjQS