TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Erki Toming 211246IDAR

Arvutivõrgu ülesehitus usuühendustele Karmeli koguduse näitel

Diplomitöö

Juhendaja: Siim Vene
MSc
Kaasjuhendaja: Mait Mutso
MS

Tallinn 2021

Autorideklaratsioon

Kinnitan, et olen koostanud antud lõputöö iseseisvalt ning seda ei ole kellegi teise poolt varem kaitsmisele esitatud. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on töös viidatud.

Autor: Erki Toming

[pp.kk.aaaa]

Annotatsioon

Lõputööst eesmärk on tõsta teadlikkust usuühenduse arvutivõrgu turvalisusest Rakvere Karmeli koguduse näitel. Töö sisaldab Arvutivõrgu uuringut hetkeseisust usuühendustes, Rakvere Karmeli koguduse arvutivõrgu ülesehitamist ja turvalisuse analüüsi.

Esimeses osas leiab uuringu, kus selgub hetkeolukord usuühenduste arvutivõrgust, ning uuringu tulemusest tulenevalt lühidalt soovitused arvutivõrgu turvalisuse tõstmiseks ilma kulutusi tegemata.

Teises osas leiab Rakvere Karmeli koguduse arvutivõrgu vajadused ning arvutivõrgu ülesehitust.

Kolmandas osas on keskendatud turvalisusele ning turvalisuse aluseks võtnud ISKE meetmed. Lõputöös leiab analüüsi Rakvere Karmeli koguduse arvutivõrgust ISKE meetmetega.

Töö tulemuseks on saadud Rakvere Karmeli koguduse uude kirikuhoonesse uus turvaline arvutivõrk, mida on võimalik väikeste kohendustega rakendata peaaegu kõigis usuühendustes.

Lõputöö on kirjutatud Eesti keeles ning sisaldab teksti 21 leheküljel, 8 peatükki, 4 joonist, 2 tabelit.

Abstract

Introduction of Computer network structure for religious associations on the example of Karmel church

The aim of this thesis is to find the best suitable and secure computer Network structure for religious associations, on the example of Karmel church, that can also be used for other religious associations. The other aim is to raise the awareness about secure network, amongst the religious associations.

In the first part of the paper, one can find a description of a religious association and an empirical research about the current situation of the network security amongst the religious associations. The research results will reflect the current situation of network security, the plans to renew it and also gives a small overview of the network security in general, amongst the religious associations in Estonia. There can also be find suggestions, that the associations can do today, in order to rise the security level, without making extra investments on it.

In the second part, there can be found the description of Rakvere Karmel church needs for the new church building computer network and the process to get the equipment needed. There can also be found the introduction of the software and devices analysis, that meets the needs of the church's needs and requirements.

In the third part can be found the Rakvere Karmel church computer Network description and security analysis, where it is being build up on the ISKE measures to get secure computer network system.

Rakvere Karmel church new building is currently already being partly used, that means that the computer network has also been taken to use successfully. Rakvere Karmel church computer network example can be easily used on others religious associations, with small adjustments, based on the needs of the association and to reach a secure computer network in the church, while doing so.

The thesis is in Estonian and contains 21 pages of text, 8 chapters, 4 figures, 2 tables.

Lühendite ja mõistete sõnastik

EEKBKL	Eesti Evangeeliumi Kristlaste ja Baptistide Koguduste liit
LAN	Kohtvõrk (*Local Area Network*)
ISKE	Infosüsteemide kolmeastmeline etalonturbe süsteem
IEEE 802.1x	Protokoll, mis rakendab võrguliikluseeskirju, mis põhinevad kasutaja identiteedil ja mandaatidel.
MAC-aadress	Meediumipöörduse juhtimise aadress (*Media Access Control address*) on füüsilise võrguliidese unikaalne identifitseerija
MAC-filter	Võimaldab MAC-aadressi põhiselt blokeerida ligipääsu
WiFi	Traadita kohtvõrk
Mbit/s	Andmeedastuskiiruseühik, Megabit sekundi kohta
Gbit/s	Andmeedastuskiiruseühik, Gigabit sekundi kohta. 1Gbit=1000Mbit
GHz	Andmeedastuskiirus, Gigaherts
VLAN	Virtuaalne kohtvõrk (*Virtual Local Area Network*)
VPN	Virtuaalne privaatvõrk (*Virtual Private Network*)
DNS	Internetiteenus, mis tõlgib domeeninimed IP-aadressiks (*Domain Name System*)
DHCP	Dünaamiline hostikonfiguratsiooni protokoll (*Dynamic Host Configuration Protocol*)
NAT	Võrguaadresside teisendus (*Network Address Translation*)
Web filter	Filtreerib veebi sisu ning reeglite põhjal takistab sisu edasi jõudmist
RADIUS	Teenus mille kaudu saab iga kasutaja enda kasutajanime ja parooliga sisse logida
POE	Elektrivoolu läbi internetikaabli. (*Power Over Ethernet*)

SNMP	Standard, millega kogutakse hallatavatest seadmetest andmeid ning nende andmete muutmist seadmete käitumise mõjustamiseks (*Simple Network Management Protocol*)
IEEE 802.11ac	Traadita võrgu standard, mis töötab sagedustel 5,15-5,825 GHz
DHCP snooping	Turvatehnoloogia arvutivõrgus, mis võimaldab kommutaatoris kontrollida DHCP-liiklust
ARP	Aadressiteisenduse protokoll on protokoll IP-aadressi vastendamiseks MAC-aadressiga (*Address Resolution Protocol*)
Loopback detection	Võimaldab leida võrguseadmetes ringlust
CAT6	Keerdpaarjuhtme (internetijuhtme) standart
IP-aadress	Internetiaadress, alaline või ajutine tunnusnumber, mille abil võrku ühendatud seadmed üksteist leiavad (*Internet Protocol address*)
Native VLAN	On VLAN, mis on ilma VLAN-märgiseta
RIA	Riigi infosüsteemide amet
E-ITS	Eesti infoturbestandart

Sisukord

Jooniste loetelu

Tabelite loetelu

1 Sissejuhatus

Võrgu turvalisus on väga oluline igale asutusele, kuid tihti ei ole usuühendused panustanud oma võrgule piisavalt vahendeid. Lõputöö eesmärk on leida säästliku, kuid turvalise lahenduse, mis oleks kohandatav usuühendustele, tehes seda Eesti Evangeeliumi Kristlaste ja Baptistide Koguduste Liidu Rakvere Karmeli koguduse näitel. Samuti on eesmärk tõsta IT-teadlikkust usuühendustes, et mida tähendab turvaline arvutivõrk ning mida iga kogudus saab teha, et tema arvutivõrk oleks turvaline.

Rakvere Karmeli kogudus on tegutsenud juba 126 aastat, teenides kogukonda enda ümber. Kogudus kuulub enam kui 85 kogudusest ja 6500 liikmega koosnevasse EEKBK liidu võrgustikku. Üks pealmisi prioriteete on läbi aastakümnete olnud ühistegevused laste ja noortega. [1] Kogudus sai püsiühenduse 2000. aastate algusaegadel ning sellest ajast on hakanud vajadused kasvama, näiteks sai alguse teenistuste salvestuse saatmine Kuressaare Pereraadiosse. Aastal 2010 alustati teenistuste videosalvestuste ning otseülekannetega Pildiraadio.com lehele. 2015. aastal sooviti pakkuda avaliku interneti kasutamist koguduse liikmetele. Aastal 2020 alustas Rakvere Karmeli kogudus endale uue ja modernse hoone ehitust, mida oleks võimalik kasutada ka erinevateks otstarveteks, nagu näiteks seimnarid, noorsootöö ja kontserdid. Koguduse sooviks oleks, et nende uues kirikuhooneks oleks turvaline arvutivõrk, mida saaks kasutada turvaliselt nii külaline kui ka koguduse tööline. Hoone soovitakse võtta osaliselt kasutusse 2021. aasta märtsis.

Lõputöö eesmärgiks on koostada turvaline ja säästlik arvutivõrk Rakvere Karmeli kogudusele, mida oleks võimalik võtta kasutusse teistel usuorganisatsioonidel väikese kohendamisega. Lõputöös hinnatakse usuühenduste arvutivõrgu hetkeseisu ja välja selgitada nende vajadusi. Lõputöö keskendub vabavaraliste tulemüüride analüüsile, kasutades soodsaid ja taaskasutatud seadmeid ning praktilise lahenduse väljatöötamisele.

Diplomitöö metoodikaks on valitud tegevusuuring. Töös võrreldakse ja analüüsitakse erinevaid seadmeid ja tarkvara ning seejärel paigaldatakse.

Töö koosneb kolmest osast. Esimeses osas on uuritud Eesti usuühenduste arvutivõrgu hetkeolukorda. Teises osas on esitatud Rakvere Karmeli koguduse vajadused ning vabavaralise tulemüüri analüüs ja seadmete hankimine. Kolmandas osa on Rakvere Karmeli koguduse arvutivõrgu ülesehitus ja turvalisus vastavalt ISKE meetmetele.

2 Usuühendused

Usulised ühendused on kirikud, kogudused, koguduste liidud ja kloostrid. Nende põhitegevus on oma usu tunnistamine ja välja elamine eeskätt jumalateenistuste, usuliste koosolekute ja talituste vormis, ning usutunnistusekohane või oikumeeniline moraali-, eetika-, haridus-, kultuuri-, diakoonia-, sotsiaalse rehabilitatsiooni alane või muu tegevus väljaspool kirikule või kogudusele iseloomulikke usuliste talituste ja teenistuste vorme. [2]

Eestis on registreeritud üle 600 usulise ühenduse, millest enamik kuulub kirikutesse või koguduste liitudesse. [3] 2013. aasta seigus on neist suurimad liidud on Eesti evangeelne luterlik kirik, kus on 166 kogudust ja 180 000 liiget , Moskva Patriarhaadi Eesti õigeusu kirik, kuhu kuulub 35 kogudust ja on liikmeid umbes 170 000. [4]

2.1 Usuühenduse arvutivõrgu erinevus teistest väikevõrkudest

Pandeemia on mõjutanud kõiki asutusi ja ettevõtteid, mille tagajärjel on hangituid uusi tehnilisi lahendusi ja on kasvanud arvutivõrgu tegevus. Nii on ka usuühendused kolinud enda teenistused ja muud sündmused interneti. Usuühendused erinevad suurestjaost oma tehniliste lahenduste kasutamisega, mida teistes väikevõrkudes ei kohta tihtipeale näiteks helitehnika lahendusi Waves või Dante, mis nõuavad katkematut võrgu ühendust. Samuti võib kirikutes olla üks päev kolm võrgu kasutajat, kuid teine päev teenistusel või konverentsil mitu sada võrgu kasutajat, seega peab võrk toimima ka suure hulga seadmetega, mida teistes väikevõrkudes ei kohta. Samuti kasutavad kirikud erinevaid usuühendustele mõeldud tarkvarasid näiteks ülekanne tegemiseks Dacast. Tihtipeale tehakse kirikutest mitmele platvormile korraga ülekandeid kirikus toimuvast. Tihti peale soovitakse ka külaliste arvutivõrku kontrollida rohkem, kui teist asutustes näiteks soovitakse blokeerida erootilist sisu. Usuühenduste arvutivõrku kasutatakse mitmekülgselt näiteks on kirikutes on pastoraat ja muusika produktsioon, seega on äärmiselt tähtis segmenteerida usuühenduste arvutivõrk.

2.2 Eesti Evangeeliumi Kristlaste ja Baptistide Koguduste Liidu Rakvere Karmeli Kogudus

Rakvere Karmeli kogudus on kristlik kogukond, kuhu kuulub üle 300 liikme ja kogudus ise kuulub Eesti Evangeeliumi Kristlaste ja Baptistide liitu, kus omakorda on 85 kogudust. [5] Karmeli koguduses käib iganädalaselt läbi üle kolmesaja inimese erinevas vanuses. Nende missiooniks on Jumala väes ja armastuses inimeste keskel neid teenides, et üksikisiku ja kogukonna parim potentsiaal realiseeruks ning kristlikel väärtustel rajanev terviklik heaolu kasvaks kogu ühiskonnas. [6]

Vana kirikuhoone, mis ehitati 1930ndatel, on jäänud liiga väikseks, seega otsustas kogudus ehitada uue hoone, mis vastaks tänapäevastele tingimustele. [7] Rakvere Karmeli koguduse motoks on „kogudus igaks päevaks“ [6], nii et kirikuhoonet ei kasutata ainult pühapäevasteks teenistusteks, vaid ka nädala sees toimuvad erinevad sündmused, näiteks Alfa, noorte õhtud ja koolitus „Kasvuhoone“. [8]

2.2.1 Rakvere Karmeli koguduse uus kirikuhoone

Uus hoone koosneb mitmest osast. Esimene majaosa on saali osa koos lava ja lavaaluse ruumide kompleksiga, mis mõeldud jumalateenistuste ning samuti erinevate kontserdite, teatrietenduste ja konverentside läbiviimiseks. Teiseks osaks on kogunemiseala, kohtumispaik, mille keskmeks on hubane kohvikuala koos selle ees asuva vestibüüli ja garderoobiga. Kolmas osa on Noorsookeskus, mille eriliseks aktsendiks peame täiemahulist katuseterrassi ning hoonetagust ”*greenroomi*” blokki suubuvat amfiteatrilaadset õueala osa arhitektuurset lahendust. Kogudusehoone juurde kuulub veel pastoraat ja külaliskorter. [9]

3 Empiiriline uuring

3.1 Uurimiseesmärk ja küsitluse läbiviimine

Lõputöö vajaduse püstitamise eesmärgil viidi läbi küsitlus usuühenduste arvutivõrgu hetkeolukorrast. Küsitluse jaoks kasutati Google Formsi ning seda jagati neljas erinevas liidus – nelipühi, baptisti, luteri ja metodisti. Kokku vastas küsitlusele 34 kirikut ja kõik vastanud pidasid vajalikuks, et usuühenduste arvutivõrk peab olema turvaline. Vastanute seas oli erisuuruses usuühendusi nii 50 liikmelisi, kui ka üle 350 liikme.

Küsimusele, et mis teeb arvutivõrgu turvaliseks, vastati tihti napisõnaliselt ja peamiseks vastuseks oli tulemüür või viirusetõrje. Vastanud koguduste vastustest võime järeldada, et kogudustel puudub enamasti suurema pildi nägemus ning teadmine turvalisest arvutivõrgust, sest ainult kaks vastanut oskas vastata täpselt võrkude eraldamisest. Üks vastanutest tõi välja, et kogudustel puudub teadmine turbepoolitika kohta ja vastavad inimesed, seega usuühenduste liit võiks võtta vastustuse turbepoliitika kohta ja anda sisendit. Samuti on ka lõputöö eesmärk tõsta usuühenduste teadlikkust turvalisest arvutivõrgust.

Küsitlusest selgus, et enamustel ei ole arvutivõrk segmenteeritud ja kasutavad teenusepakkuja ruuterit ainult seitsmel vastanul on teise tootja poolt toodetud tulemüür. Usuühenduste seast 26 vastanut arvas, et usuühenduste arvutivõrk võiks vastata ISKE meetmetele, kahjuks küsitluses selgus, et usuühenduste arvutivõrgud ei ole turvalised, ega ISKE meetmetega kooskõlas.

Täpsemalt küsitluse ja vastuste analüüsiga saab tutvuda Lisa 5.

3.2 Uuringu järeldus

Uuringus oli mitmeid puudulike ja ebakõlalisi vastuseid. Näiteks vastati, et külaliste võrk ei ole eraldatud ning järgneval vastusel oli, et võrgud on segmenteeritud, siis peaks külaliste võrk olema samuti eraldatud, kuid seda ei olnud.

Turvalise arvutivõrgu kohta oli ainult mõni tugev vastus. Samuti oli ka vastustes näha ebakõla, et ei teata, mis see turvaline arvutivõrk on. Üks vastanutest lisas, et kirikutel endal pole ressurssi ega teadmisi turbeplaanidest ning ootaks neid teadmisi liidult, kuhu kogudus kuulub. Konkreetne vastaja oli esimeste seas ja sellel ajal oli läinud küsitlus ainult Baptisti liitu, seega anti tagasisidet ka liidule. Sain teada, et liit oli aastaid tagasi üritanud ühtlast võrku kirikute vahel teha, aga see ei

sobinud kõigile ja projekt jäi kohe alguses seisma. Konkreetseid seadmeid ei saa anda ette, mida peab kasutama, vaid turbealaseid soovitusi, näiteks, kui raamatupidamistööd on koguduse arvutivõrgus, siis peab olema eraldatud külalistele eraldi arvutivõrk. Baptisti liit tunneb huvi valmis lõputööst ning soovib antud teemat käsitleda, et liitu kuuluvad kogudused saaksid teadlikumaks arvutivõrgu turvalisusest. Üks pealmistest eesmärkidest ongi tõsta usuühenduste teadlikkust ning näidata Karmeli koguduse näitel, et on võimalik ehitada säästlikult turvaline arvutivõrk.

Hea tulemusena on näha, et enamus tunnistab, et nende arvutivõrk vajaks uuendamist ning neil on plaanis teha uuendusi. Lõputöö on abiks arvutivõrkude uuendamisel ja seadistamisel. Küsitlusest tuli välja, et väga paljud kasutavad lihtsalt teenusepakkuja seadmeid, seega on vaja lihtsamaid soovitusi, mida saaks igaüks täna ära teha ilma, et peaksid tegema kulutusi.

3.3 Uuringust tulenevalt soovitused usuühendustele arvutivõrgu turvalisuse tõstmiseks

Koroonapandeemia on tõstnud usuühenduste arvutivõrgu vajadusi, sest kõik kirikud on kolinud oma teenistused ja kõik muud kohtumised internetti ning on kasvanud seadmete hulk arvutivõrgus. Lõputöö eesmärk pole ette anda seadmeid või tarkvarasid, mida peab võtma kasutusse, vaid tõsta teadlikust turvalisest arvutivõrgu ülesehitusest. Kuna koguduste suurused ja käideldavus on erinev, siis on võimatu öelda ka ühte seadet, mis oleks õige.

Järgnevalt võib leida mõned soovitused usuühendustele uute seadmete hankimisel.

- Kindlasti mõelda kasutaja mugavuse ja lihtsuse peale, sest kogudustes enamasti haldavad vabatahtlikud võrguseadmeid. Kasutaja mugavusest lähtudes on soovitatav osta ka sama tootja seadmed.
- Hallatavad seadmed, et oleks segmenteerida arvurtivõrku.
- 1 Gbps seadmed, sest hetkel koguduste tehnikavajadused arenevad ning ei ole mõistlik enam osta 100 Mbit/s seadmeid, mis võivad saada takistuseks. Tänapäeval nõuvad erinevad heli- ja videotehnikad 1Gbit/s võrku ning varjestatud võrgukaablit.
- Wifi seadmeid võiksid olla 5 GHz, et saavutada hea wifi kiirus ning väiksem tõenäosus, et naabri wifi seadme sagedus oleks sama.

- Wifi seadmetel võiks olla kas „instant mode“, ehk funktsioon kus üks tugijaam võtab kontrolleri rolli või tasuta tarkvaralise kontrolleri võimalus, et oleks võimalikult lihtne hallata erinevaid seadmeid. Kui rahaline võimekus olemas, võib ka tasuline ja füüsiline kontroller olla.

Usuühendusi on eri suuruses ja eri võimekuses, seega on eesmärk tuua esile sellised seadistusi, mida on võimalik ka kõige lihtsama teenusepakkuja poolt pakutaval ruuteril seadistada ning mis sobiks igale kirikule. Uuring tõi esile, et kirikutes toimub mitmekülgne elu ja kiriku arvutivõrku kasutatakse nii külaliste poolt, kui ka kiriku elamutes. Seega usuühenduste turvalise arvutivõrgu saavutamiseks peab olema arvutivõrk segmenteeritud ning piiratud ligipääsud külalistele. Samuti peaksid olema külaliste võrgul vähemalt kiiruse piirangud, et külalistel ei oleks võimalik takistada koguduse tööd. Segmenteeritud võrkude vahel peavad olema minimaalselt lubatud liiklused. Näiteks külaliste võrgust ilmselt ei pea saama sisevõrku printida, kuid kiriku elamust samas võib olla printimine lubatud, et usuühenduse juht ei peaks kodus olles võrke vahetama. Tulenvalt ISKE meetmest M 4.202 ei ole soovituslik kasutada segmenteerimisel vaikeseadistusena tulevat VLAN1. [10]

Tundlikumate võrkude puhul kasutada minimaalselt MAC-filtrit, et võõrad seadmed ei saaks ühendust võrguga, ilma et oleks seadme MAC-aadress lubatud. Turvalisem lahendus on kasutada portokolli IEEE 802.1x, kuid enamasti ei võimalda seda kasutada teenusepakkuja seadmed.

Seadmete haldamiseks peaks olemas eraldi segment, kuhu ühestki teisest võrgust ligi ei pääse. Samuti tulenvalt ISKE meetmest M 1.43 peaksid olema seadmed lukustatud ruumis või vähemalt lukustatud seadmekapis. [11] Kindlasti peaksid kõik võrguseadmed olema erineva parooliga ning erinevate sümbolitega, näiteks suure ja väikse tähe ja numbri kombinatsioon ning peab toimuma regulaarne muutmine, näiteks iga 90 päeva tagant tulenvalt ISKE meetmest M 2.11. [12]

Need on seadistused, mida iga usuühendus saab teha juba täna olenemata nende arvutivõrgu suurusest. Samuti ei nõua need seadistused rahalist investeeringut, vaid läbimõtlemist ja dokumenteerimist.

Suuremate arvutivõrkude puhul on soovitus jälgida Rakvere Karmeli koguduse näitel ehitatud arvutivõrku ning kohandada vastavalt enda koguduse vajadustele. Samuti käsitleda lõputöö Lisas 3 olevat ISKE tabelit enda arvutivõrgu turvalisuse tagamiseks.

4 Rakvere Karmeli koguduse arvutivõrgu ülesehitus

4.1 Rakvere Karmeli koguduse vajadused

Koguduse pealmine eesmärk on saada turvaline lahendus, mida oleks kerge hallata ja mis oleks töökindel. Samuti soovib koguduse juhtkond käia ajaga kaasas ja pakkuda tänapäevaseid lahendusi, mida oleks võimalik tulevikus kergelt uuendada. Uut hoonet ehitatakse annetustepõhiselt, seega on tähtis rahaline kokkuhoid, kuid mitte kaotada turvalisust ja käideldavust. Pakuti ka odavamaid uusi seadmeid pöörates tähelepanu kasutatud seadmete lühemale elueale. Pakutud lahendusega saab tutvuda punktis 4.5. Olles tutvunud pakkumistega on juhtkond otsustanud soetada kasutatud seadmed, tuues põhjenduseks uue ja kasutatud seadme hinnavahe. Samuti otsustati ka juurutada vabavaralist tarkvara oma arvutivõrgus.

Rakvere Karmeli koguduse uus kirikuhoone on multifunktsionaalne ning seda kasutatakse väga erinevate sündmuste ja tegevuste jaoks. Suures saalis on võimalik teha nii muusikalisi esinemisi kui ka konverentse koos tasemel tehnilise lahendusega. Kuna erinevatelt sündmustelt käib väga palju erinevaid inimesi ja seadmeid läbi, on oluline saavutada turvaline arvutivõrk, mis oleks segmenteeritud ning piiratud ligipääsudega.

Pandeemia piirangud on sulgenud koguduse ukse, mis on toonud kaasa uusi tehnilisi arenguid koguduse ellu ning nii teenistused kui ka teised sündmused on kolitud internetis leitavate platvormide peale, seega mängib koguduse elus aina enam rolli internet.

Karmeli kogudusel on tähtis, et nende ülekanded, helitehnika ning kõik muud teenused ja seadmed toimiksid võrgus laitmatult ja katkestuseta, seega on tähtis mõelda ette ja vähendada riske. Helitehnika juhtimiseks kasutatakse arvutivõrku, näiteks bändiliikmetel on võimalik enda kõrvamonitori seadistada telefonist ja heli paremaks muutmiseks kasutatakse lisamooduleid läbi arvutivõrgus oleva serveri. Samuti toimuvad ülekanded samal ajal ning ka külalistel on võimalik kasutada internetti. Nende eelpool nimetatud arvutivõrgus toimuvate tegevuste jaoks on tähtis katkematu ühendus. Katkematu ühenduse saavutamiseks on vaja võtta kasutusele tulemüüri klasterlahendus. Samamoodi tuleb vähendada riski ka kommutaatorite topoloogias ning ühendada kommutaatorid topelt ühendustega. Traadita kohtvõrgu pääsupunktid jagatakse kahe kommutaatori vahel ära, näiteks kui üks kommutaator peaks katki minema, siis jäävad saalis vähemalt pooled traadita pääsupunktid tööle.

Arvutivõrgu seadmed peavad võimaldama vähemalt 1 Gbit/s kiirust, mida nõuavad ka erinevad tehnilised seadmed koguduses.

Kuna seadmete hulk võib olla suur, siis peab tagama, et võrgu käideldavus ei kaoks ja kõik koguduse teenused, näiteks videoülekanne, toimiksid laitmatult, seega on oluline piirata üleslaadimiskiirust vähemalt külalistevõrgus. Samuti piiratakse ka allalaadimiskiirust ja ebasobivat sisu, näiteks torrenti kasutamist ja pornograafilist sisu.

Interneti käideldavuse tagamiseks on koguduse juhtkond mõelnud tulevikus ka lisada teise teenusepakkuja välisühendust. Seega peab tulemüür olema suuteline võtma vastu kaks välisühendust ning olema valmis suunama liiklust automaatselt ümber ühelt teisele või balansseerima ühendust.

Koguduse juhtkond peab väga tähtsaks turvalist arvutivõrku ning on tähtis, et seadmete haldamiseks oleks eraldatud eraldi segment arvutivõrgus ning piiratud ligipääs sellele segmendile. Samuti on oluline, et külalised ei pääseks teistesse koguduste võrkudesse ligi. Kuna heli- ja valgustehnika ei ole parooliga kaitstud, siis selletõttu on tehniline võrk tundlik ning peab tagama vähemalt MAC-aadressi piiranguga ligipääsu võrgule, et tehnikaoskamatu inimene ei saaks nõrkust ära kasutada. Oluline on sisevõrgu turvalisus, kuid samuti on väga oluline, et keegi ei saaks kasutada välisvõrgu ühendust kurjasti ära. Seega peab tulemüür tagama ka turvalise välisvõrgu ühenduse. Tähtis on ka seadmete turvalisus ning ostetavatel seadmetel peab olema kehtiv tootjapoolne tugi. Kuna kogudusel on serverid olemas, siis on otsustatud leida vabavaraline tulemüüri lahendus, mis oleks uuenduslik ja turvaline. Vabavaralise tulemüüri kasuks oli ka uuenduslikkuse ja võimekuse tagamine.

Koguduse suures saalis saab olema peaaegu 300 istekohta, seega wifi peab suures saalis vastu pidama vähemalt 400–600 seadet korraga. Seadmete arvus arvestasime, et tulevikus on plaanis saali kasutada ka konverentsideks, kuhu võidakse tulla sülearvutitega ja samaaegselt ühendada oma telefon, ehk 2 seadet inimese kohta. Samuti peab samal ajal tagama ka wifi käideldavuse teistes hoone osades ning traadita ühendus peab ka teiste tehniliste lahenduste jaoks toimima. Enne traadita kohtvõrgu kasutama hakkamist peab kasutaja olema teadlik koguduse arvutivõrgu kasutamisereeglitest ning piirangutest arvutivõrgus, seega on vajalik iseteenindusportaal, kus on võimalik anda nõusolek reeglitega tutvumisest.

Koguduse juhtkonnal on soov ligi pääseda välisvõrgust sisevõrku, et kasutada majasiseseid teenuseid, näiteks failiserveris olevatele failidele ligi pääseda. Seega peab selleks olema turvaline

ja lihtne VPN-lahendus. Turvalisuse tagamiseks peab VPN-lahendus olema krüpteeritud ja kaitstud vähemalt kasutajanime ja parooliga ning võimaluse korral ka pakkuma kahetasemelist autentimislahendust. Samuti peab turvalisuse huvides olema võimalik piirata VPN-võrgu kasutamist sisevõrgus olevate teenuste näol, näiteks läbi VPN-tunneli saab ainult ligi failiserveris olevatele failidele ning teisi teenuseid ei saa sisevõrgus kasutada.

Seadmete kasutamine ja haldamine peab olema kasutajasõbralik, et tulevikus IT-teadlik koguduseliige saaks võtta igapäevase haldamise enda peale. Seega peab saama seadistusi teha graafilisest kasutajaliidesest.

Kasutusse võetavad seadmed ja tarkvara peavad võimaldama varundust. Kuna kõik seadmed tulevad järelturult ning eeldatav eluiga on lühem, siis on oluline dokumenteerida ja varundada seadmete konfiguratsioon. Koguduse juhtkonnal on kohustus leida sobiv ja turvaline koht varunduseks ja dokumentatsiooni hoidmiseks, soovitatavalt väljaspool maja.

4.1.1 Täpsemad nõuded hankimiseks.

Järgnevalt on kaardistatud täpsemad nõuded tulemüüri tarkvara ja võrguseadmete hankimiseks.

4.1.1.1 Vabavaralise tulemüüri nõuded

- Pidevad turvauuendused
- Täiesti tasuta ja avatud lähtekoodiga
- Graafiline kasutajaliides, seejuures kasutajasõbralik
- Süsteem peab olema toimiv ja töötama hästi tavakasutaja jaoks
- Iseteenindus portaal
- Peab toetama dünaamilisi marsruutimisprotokolle, lisaks DNS-, DHCP-, NAT-teenuseid
- RADIUS-tugi
- VLAN-tugi
- VPN-võimalus
- Web Filter
- MAC-filter

4.1.1.2 Kommutaatorite nõuded

- Omama 1G porte vastavalt portide arvule

- Hallatav
- POE-tugi
- RADIUS
- Käsurea haldusliides üle IP-aadressi, graafiline kasutajaliides ja üle *serial*-liidese
- SNMP V3-tugi
- VLAN
- *Loopback detection*
- Kaitse DHCP/ARP rünnete ja IP võltsimise vastu (näiteks *DHCP snooping*, *ARP inspection*)
- Kommutaatoritega peavad olema kaasas osad seadmekappi paigaldamiseks
- Võimalik varundada ja taastada konfiguratsiooni

4.1.1.3 Traadita kohtvõrgu pääsupunkti nõuded

- IEEE 802.11ac
- POE
- Üks tugijaam peab võtma endale kontrolleri rolli (*instant mode*)
- 2,4 GHz ja 5 GHz
- 5 Ghz sagedust kasutades peab olema traadita andmeedastuskiirus vähemalt 600 Mbit/s
- Graafiline kasutajaliides
- Laekinnitus

5 Võimalike lahenduste analüüs ja seadmete hankimine

Järgnevalt on läbitöötatud usuühenduste küsitluse tulemused ja Rakvere Karmeli koguduse vajadused. Olen leidnud hetkel turul olevad sobilikud seadmed ja tarkvarad, mida põhjalikumalt hakata analüüsima, et teha lõplik valik.
Nii seadmete kui ka tarkvara seast valiti välja kolm hetkel enam levinumat, mis vastaks vajadustele, kasutajasõbralikkusele, turvalisusele, uuenduslikkusele ja oleks võimalikult madala kuluga.

5.1 Tulemüür

Selles osas valiti välja kolme parima täiesti tasuta vabavaralise tarkvara seast parima sobivuse usuühendustele. Valikut tehti kasutajate hulga ja hinnangute järgi. [13] [14] Samuti pidid kõik kolm vabavaralist tarkvara vastavama eelpool mainitud vajadustele.

5.1.1 pfSense

PfSense on FreeBSD põhjal loodud ning on litsentseeritud Apache License 2.0. PfSense on saadaval olnud alates 2006. aastast ning pika kogemusega. [15] Graafiline veebiliides on natuke aegunud ning menüü osa on keeruline. Kuid PfSense on olnud pikalt turul ning on saavutanud rohke kasutajate hulga. Kuna kasutajate hulk on suur, siis on võimalik leida väga palju juhendeid internetist. [16] Samuti on tarkvara hästi dokumenteeritud, mille leiab GitHub'ist. [17]

5.1.2 OPNSense

OPNSense hargnes PfSense'st ning on samuti HardenedBSD põhjal loodud tarkvara, mis ilmus esimest korda 2015. aastal ning on sellest ajast olnud üks kõige kiiremini arenevaid ruuteri ja tulemüüri süsteeme. HardenedBSD, mis on turvalisusele orienteeritud FreeBSD haru. OPNSense on toonud välja mõned põhjused hargnemisest: koodi kvaliteet, regulaarne uuenduslikkus, turvalisuseprobleemid, veebirakendusel on *root*-õigused. Kuna OPNSense on võtnud mitmeid komponente PfSense'st ning kirjutanud need natuke endale sobivaks, nagu näiteks logimine. [18] OPNSense kasutab Simplified BSD / FreeBSD litsentsi. [19]

5.1.3 IPFire

IPFire on avatud lähtekoodiga Linuxil põhinev ruuteri ja tulemüüri tarkvara. Alates 2. versioonist kirjutati IPFire ümber Linuxi-põhiseks ning tekkis võimalus paigaldada lisamooduleid. Kuna IPFire on Linuxi-põhine, saab kasutada ka Linuxile mõeldud tööriistu. Samuti vajab IPFire vähem serveri ressurssi kui teised eelpool nimetatud tarkvarad. [20] Nagu ka pfSense ja OPNSense, on ka IPFire täiesti tasuta kasutatav ning litsentseeritud GNU General Public litsentsiga. [21] Segmenteerimine on väga lihtne ja kasutajasõbralik, värvikoodide alusel ning ühest võrgust teise ei saa, kui pole loodud vastavat erandit tulemüüri reeglites.

5.2 Võrdlus tabeli kujul

Tabel 1. pfSense, OPNSense ja IPFire võrdlev analüüs nõude kaitsmiseks *[21] [22] [20] [15] [19]*

FUNKTSIOONID	**pfSense**	**OPNSense**	**IPFire**
operatsioonisüsteem	FreeBSD ja OpenSSL	HardenedBSD ja optional LibreSSL	Linuxil põhinev,
Hind	Tasuta (on võimalik osta tugiteenust)	Tasuta (on võimalik osta tugiteenust)	Tasuta
Litsents	AGPL 2.0	BSD klausel 2	GNU
Protsessorid	64bit	I386, x86-64	x86-64, i686, i586, ARM
Lisamoodulite võimalus	Jah	Jah	Jah
NAT	Jah	Jah	Jah
DHCP ja DNS	Jah	Jah	Jah
DMZ tsooni võimalus	Jah	Jah	Jah
Iseteenindusportaal	Jah	Jah	Jah
Web filter	Jah	Jah	Jah

FUNKTSIOONID	pfSense	OPNSense	IPFire
VPN	OpenVPN, IPsec, L2TP, IKEv2, Tinc, PPTP	WireGuard, OpenVPN, IPsec, L2TP, IKEv2, Tinc, PPTP	OpenVPN, IPsec, IKEv2
IPv4 ja IPv6	Jah	Jah	Jah
IDS	Jah	Jah	Jah
IPS	Jah (Snot ja Suricata moodulid)	Jah (Snot ja Suricata moodulid)	Jah (Suricata moodulid)
Multi-WAN	Jah	Jah	Ei
HA-Cluster	Jah	Jah	Ei
2FA	Osaliselt	Jah	Ei
Monitooring	Jah	Jah	Jah

5.2.1 Osutus valituks

PfSense ja OPNSense on oma loomuselt väga sarnased. OPNSense'i plussideks leian, et on modernsem ja kasutajasõbralik ning tuleb tihedamalt turvauuendusi, kui teistel välja toodud tarkvaradel. Samuti on plussiks, et OPNSense kasutab HardenedBSD-d. PfSense'il on küll suurem kasutajavõrgustik, kuid OPNSense'i kasutajate hulk kasvab jõudsalt ning on abivalmid erinevates foorumites. IPFire võimaldab kõiki vajalike seadistusi teha, et saavutada turvaline arvutivõrk. IPFire nõuab vähem serveri ressurssi kui pfSense ja OPNSense ning on ehitatud Linuxi baasil ja saab kasutada Linuxile mõeldud tööriistu. Samuti on IPFire'i puhul teistest lihtsam teha algseadistusi.

Kõik kolm lahendust toimivad hästi usuühenduste jaoks ja on võimalik saavutada turvaline arvutivõrk kõigi kolmega. Rakvere Karmeli kogudusele IPFire ei sobi, sest puudub võimalus korraga kahe teenusepakkuja internetti kasutada, selle funktsiooni soovib tulevikus koguduse juhtkond kasutusele võtta. Karmeli koguduse jaoks valiti välja OPNSense'i, sest see on moderne ja kasutajasõbralik, seda on võimalik hallata koguduse vabatahtlikel infotehnoloogia haridusega inimestel. Samuti on OPNSense'i kergem uuendada. Koguduse juhtkond leiab samuti, et OPNSense sobib neile hästi ja täidab tulemüürina kõik nende ootused ja vajadused.

5.3 Kommutaatorite hankimine

Eesmärk on leida samast seeriast vähemalt kolm kommutaatorit. Kõik kommutaatorid peavad vastama punktis 3.1.1.2 mainitud nõutele. Võrguruumi on vaja saada minimaalselt kaks kommutaatorit, portide koguarvuga 96 porti. Lisaks on vaja pastoraati üks 24-pordine kommutaator.

Kasutatud võrguseadmete pakkumisi võeti kolmest ettevõttest. Pakuti kahe erineva tootja seadmeid, HP ja Cisco. Kõik pakkumises olnud kommutaatorid vastasid eelmainitud nõuetele ja vajadustele ning olid sarnase konfiguratsiooniga seadmed. Võitjaks osutus parima hinnaga pakkumine, milles pakuti HP Procurve A5120 48G POE+ ja A5120 24G POE+ seadmeid. Kommutaatorite kogumaksumus oli 400 eurot.

5.4 Traadita kohtvõrgu pääsupunktide hankimine

Kasutatud traadita kohtvõrgu pääsupunktide pakkumisi võeti kolmest ettevõttest. Pakutavad seadmed pidid vastama punktis 3.1.1.3 esitatud nõudele. Pääsupunkte sooviti hankida 25 tükki. Kõik kolm ettevõtet pakkusid erineva tootja seadmeid, millest kõik vastasid nõutele ja vajadustele. Pakutud seadmed olid Ruckuse, Aruba ja Cisco tootjate omad.

Valituks osutus parima hinnaga pakkumine – Aruba IAP-205 seadmed. Pakkumises olid taastatud (*refurbished*) seadmed, mille maksumus oli kokku 2175 eurot.

5.5 Võrdluseks uute seadmetega lahendus

Kuigi Rakvere Karmeli kogudus otsustas valida kasutatud seadmed, pakuti siiski juhtkonnale ka uute seadmetega lahendust, mis oleks samuti turvaline ja kasutajasõbralik. Samuti toodi välja, et uute seadmete plussiks on palju pikem eluiga kui kasutatud seadmetel.

Uute seadmete lahendusena pakuti välja Ubiquiti lahenduse. Pakutud lahenduses oli Tulemüüriks Ubiquiti Unifi USG-PRO. Võrguruumi kaks US-48-500W ja pastoraati US-24-250W kommutaatorid. Traadita kohtvõrgu pääsupunktiks oli pakkumises AP-AC pro. Rakvere Karmeli kogudusele oleks uute seadmete kogumaksumus tulnud ligikaudu 7000 eurot, seega hind oleks olnud mitu korda kallim kui kasutatud seadmetel. Kui võtta pakutud lahendusest välja riistvaraline tulemüür ning selle asemel kasutada vabavaralist tulemüüri, siis oleks ikkagi hind mitu korda

kallim. Samuti ei oleks Rakvere Karmeli kogudus saanud olulist funktsionaalsust juurde uutest seadmetest, seega ei soovi koguduse juhtkond uusi seadmeid hankida.

6 Rakvere Karmeli koguduse arvutivõrgu ülesehitus

Rakvere Karmeli kogudus otsustas interneti teenusepakkujaks valida Telia Eesti AS, sest nende valguskaabel on kõige lähemal kirikuhoone krundile. Tulevikus on plaanis koguduse töö tagamiseks leida kõrvale ka teise teenusepakkuja lahendus, milleks võib olla ka läbi õhu leviv lahendus.

Kirikuhoones on kaks seadmekappi, kus ühest hargnevad ühendused keldrisse ja kirikuhoone esimesele korrusele ning teine seadmekapp on mõeldud pastoraadis olevate seadmete ühenduseks. Kõik kaablid kirikuhoones on CAT6. Enamik kaableid on varjestamata, kuid heli- ja videotehnika jaoks on veetud varjestatud kaablid, et tagada heli ja video kvaliteet.

Koguduse arvutivõrgu ülesehitusel on arvestatud ISKE L- ja M-taseme meetmeid.

Rakvere Karmeli koguduse arvutivõrgu ülesehitusest on võimalik leida võrgujoonis Lisas 2.

6.1.1 Tulemüür

Tulemüür on mõeldud arvutivõrgu reguleerimiseks ja turvakaalutustel piirama võrkudevahelist liiklust. Karmeli kogudusele valitutuks osutunud OPNSense'i tulemüüritarkvara, mis paikneb kahel serveril ning on omavahel klastris. Tulemüüri klaster tagab töökindluse arvutivõrgu töös ning võimaldab uuendada tarkvara ilma katkestuseta.

Kasutusel on kaks välist IP-aadressi, millest üks on külalistevõrgu oma ning teist välist IP-aadressi kasutatakse teiste sisevõrkude jaoks. Kaks erinevat välist IP-aadressi tagab, et pahatahtlikust külalise tegevusest või külalise teadmatusest ei satuks sisevõrgu väline IP-aadress musta nimekirja, mille tagajärjel võib koguduse töö olla häiritud.

Majas olev võrk on segmenteeritud: pastoraat, kontor, tehnika, külalised, seadmehaldus, serverid, valve ning kontori wifi ning tehnika wifi.

Pastoraadi segment on mõeldud kirikuhoones olevale elamule, mis on eraldatud kõigist muudest võrkudest, kuid on lubatud printimine kontorivõrku ning ligipääs failiserverile.

Kontorivõrk on mõeldud, kirikus töötavatele inimestele ning internetti vajavatele arvutitele, näiteks videoülekande arvuti.

Tehnika segmenti on lubatud ühendata heli- ja videotehnika juhtimiseks seadmeid, näiteks helipult või võimendi.

Külaliste võrku saavad kasutada kõik kirikut külastavad inimesed. Külaliste võrguga ühendamisel peab kasutaja nõustuma kasutusreeglitega portaalis ning seejärel on võimalik kasutada internetti, mis on kõigist teistest sisevõrkudest täiesti eraldatud. Samuti on külalistevõrgul kiiruspiirangud – allalaadimine 10 Mbit/s ja üleslaadimine 2 Mbit/s ning kasutame OPNSense'i Proxy web filteringi [23], et blokeerida ebasobivat veebisisu.

Võrguseadmete haldamiseks on eraldatud teistest võrkudest täielikult seadmehaldusvõrk, milles saab hallata näiteks traadita kohtvõrgu pääsupunkte või kommutaatoreid. Samuti on seadmehaldusvõrk eraldatud ka välisvõrgust.

Serverivõrk on mõeldud majas asuvatele serveritele, näiteks failiserver. Sellele võrgule on loodud kindlad ligipääsud kontorivõrgust, näiteks on võimalik pääseda ligi kontorivõrgust failiserveris olevatele failidele.

Valve segment on loodud videovalve jaoks, mis on piiratud ligipääsuga. Valvevõrgus puudub internetiühendus, kuid on võimalik jälgida kaameraid läbi kontorivõrgu vastavalt seadistatud tulemüüri reeglile.

Kontori ja tehnika wifi segment on loodud iseteeninduspportaali pärast, et igal kasutajal oleks enda kasutajanimi ja parool, millega ligi pääseda kontorivõrku. Kontori wifi segmendil on samad tulemüürireeglid, mis kontori segmendil. Samuti on tehnika wifi võrgul samad tulemüürireeglid nagu tehnika segmendil. Kontori LAN-võrgu ja kontori traadita võrgu segmendi vahel on lubatud omavaheline ühendus täielikult ning samuti tehnika LAN-võrgu ja tehnika traadita võrgu vahel. Kuna traadita ühenduse levikut ei saa kontrollida seina ja uksega, siis turvalisuse tagamiseks eraldatud traadita ühenduse segmendid aitavad ka tulevikus piirata ligipääse teenusepõhiselt võrgus, näiteks kui sisevõrgus on isikuandmed, siis saab piirata neile ligipääsu läbi traadita ühenduse.

Välisvõrgust on võimalik ligi pääseda kontovõrku VPN-tunneli abiga. VPN-lahenduse jaoks on paigaldatud WireGuard lisamoodul.

6.1.2 Kommutaatorid

Kommutaatorid on paigaldatud kahte kohta, võrguruumis olevasse kappi ja väiksemasse kappi pastoraadis. Võrguruumis olevate kommutaatorite kaablid hargnevad igale poole majas, välja

arvatud väiksema hoone teisele korrusele olevasse pastoraati. Pastoraadis on eraldi seadmekapp ja kaabeldus ning kommutaator ühendub otse tulemüüril oleva võrgukaardi külge.
Võrguruumis on kaks HP Procurve A5120 48G POE+ ja pastoraadis on HP Procurve A5120 24G POE+. HP seadmetel on eluaegne garantii, seega on seadmetel garantii hetkel olemas.
Võrguruumis olevad kommutaatorid on omavahel ühendatud topelt ühendustega ning kummassegi kommutaatorisse on ühendatud üks kahest tulemüürist, et tagada töökindlus. Vt Lisa 2. Topelt ühenduseks on töötamiseks seadistatud *loopback*, et ei tekiks võrgus ringlust, mis takistaks arvutivõrgu toimimist.
Kommutaatoreid on võimalik hallata konsooli kaabli kaudu või seadmehaldusvõrgus, sealjuures on kõik paroolid vahetatud ning asuvad krüpteeritud andmehoidlas. Kommutaatoritel on seadistatud vajalikud segmendid vastavalt pordis olevale seadmele ning ülejäänud pordid on suletud. Siinjuures pole kasutusel vaikimisi *native* VLAN-i. Seadistatud on turvameetmed vastavalt ISKE analüüsile peatükis 6, näiteks DHCP snooping ja ARP.

6.1.3 Traadita kohtvõrgu pääsupunktid

Traadita võrguühendusega on plaanis katta terve kirikuhoone. Kõik traadita kohtvõrgu pääsupunktid saavad POE toite kommutaatorist. Suures saalis, mis mahutab umbes 300 inimest, on planeeritud 400–600 seadmele traadita side. Ühe inimese kohta oleme arvestanud kaks seadet korraga – nutitelefon ning süle- või tahvelarvuti. Iga inimene, kes ühendab oma seadme traadita kohtuvõrgu pääsupunkti külge, võiks saavutada 10 Mbit/s. Eeldusel, et inimene ei kasuta kahte seadet korraga, oleme paigaldanud suure saali osasse viis traadita kohtvõrgu pääsupunkti, ehk 600 Mbit/s ühe pääsupunkti kohta. Rakvere Karmeli koguduse juhtkonna poolt valituks osutunud traadita kohtvõrgu pääsupunkti seadmed, Aruba 205 mudel, võimaldab 867 Mbit/s [24], seega on arvestatud varuga. Ülejäänud kirikuhoones ei ole tarvis nii suurte seadmete hulgaga arvestada, seega on jaotatud traadita side ühtlaselt, et majas ringi käies ei tekiks pikki katkestusi. Täpsema traadita kohtvõrgu pääsupunkti jagunemise leiab Lisast 3.
Lihtsamaks traadita kohtvõrgu haldamiseks on üks pääsupunkt võtnud kontrolleri rolli ning kõigile teistele pääsupunktidele jaganud enda seadistusi. Wifi võrke on neli – kontori, tehnika, külaliste ja pastoraadi. Kontori traadita võrk on iseteenindusportaal ning sinna pääseb ligi kasutajanime ja parooliga. Tehnika traadita võrk on mõeldud heli- ja videotehnika juhtimiseks tahvelarvutist.

Samuti on tehnika traadita võrgul iseteenindusportaal ning autentimine toimub kasutaja ja parooliga. Külaliste traadita võrgust pääseb ainult välisvõrku ning võrku pääsemiseks peab logima sisse parooliga ja nõustuma interneti kasutusreeglitega. Pastoraadis on traadita võrk, kuhu pääseb parooliga.

6.2 Rakvere Karmeli koguduse arvutivõrgu rakendamine teisele usuühendustele

Karmeli koguduse arvutivõrku on võimalik rakendata teistel usuühendustel väikese kohendamisega vastavalt nende vajadustele. Arvutivõrgu käideldavuse tagamiseks peaks jääma arvutivõrgu füüsiline lahendus samaks nagu on toodu välja lisa 2 joonisel Rakvere Karmeli koguduse arvutivõrgust, ehk topelt ühendused. Kuid teised usuühendused peaks muutma arvutivõrgu segmentide hulka vastavalt usuühenduse vajadusele, kuid siinjuures on soovituslik jälgida ISKE meetmeid. Traadita kohtvõrgu ühendusel tuleb arvestada usuühenduste suurust ja kasutajate hulka ja samuti seadistada sarnased kiiruspiirangud Karmeli kogudusega, siinkohal arvestada ka koguduse välisühenduse kiirust.

7 Turvalisus

Turvalisuse tagamiseks võeti aluseks ISKE meetmed. Ka usuühenduste arvutivõrgu küsitlusest selgus, et enamiku vastajate arvates võiks kirikute arvutivõrk olla kooskõlas ISKE meetmetega.

ISKE on infosüsteemide kolmeastmeline etalonturbe süsteem, mille väljatöötamiseks ja arendamiseks on võetud aluseks Saksamaa BSI (sks *Bundesamt für Sicherheit in der Informationstechnik*) avaldatud infoturbe standard. ISKE rakendamise eesmärk on tagada infosüsteemides töödeldavatele andmetele piisava tasemega turvalisus. Süsteem on küll loodud eelkõige riigiasutustele, kuid samahästi kasutatav ka erasektoris. [25]

ISKEs on kirjeldatud kolm turbe taset – madal (L), keskmine (M) ja kõrge (H). Andme turvaaste määrtakse teabe konfidentsiaalsuse, terviklikkuse, aegkriitilise teabe käideldavuse ja teabe hilinemise tagajärgede lubatavast kaalukusest lähtudes. [25]

Kuna Rakvere Karmeli kogudus ei kogu isikuandmeid ega salvesta konfidentsiaalset infot, siis sobib kõige madalam aste (L), kuid juhtkond otsustas kaasata ka keskmise (M) taseme meetmeid enda võrku, sest soovib ära hoida pikemaajalisist internetikatkestust oma arvutivõrgus.

Analüüsimiseks loodi ISKE tabel, kus on meetme nimetus ja kirjeldatud lühidalt Rakvere Karmeli koguduse arvutivõrgu hetkeolukorda ning kas meede on rakendatud või mitte. Täpsema ISKE analüüsi tabeli leiab Lisast 4.

RIA on välja töötamas ka uut infoturbestandardit E-ITS, mis vahetab 2024. aastal ISKE välja. [26] Rakvere Karmeli koguduse juhtkonnal on tulevikus soov kasutusele E-ITS ning plaanis läbi viia täpsem audit koos audiitoriga.

8 Kokkuvõte

Diplomitöö eesmärgiks on leida Rakvere Karmeli koguduse näitel usuühendustele sobiv turvaline lahendus, mis oleks lihtsasti kohandatav teistele usuühendustele. Samuti oli eesmärk tõsta usuühenduste teadlikkust turvalisest arvutivõrgust.

Töö esimeses osas on kirjeldatud, mis on usuühendus ning teostatud usuühenduste arvutivõrgu hetkeseisust empiiriline uuring. Uuringu tulemusel on võimalik välja selgitata arvutivõrgu hetkeseis, uuendamisplaanid ning saada aimu usuühenduste arvutivõrgu turvalisusest. Samuti leiab usuühendustele soovitusi, mida nad saavad täna kohe ära teha turvalisuse tõstmiseks ilma lisainvesteeringuta.

Teises osas on kirjeldatud Rakvere Karmeli koguduse uue kirikuhoone arvutivõrgu vajadusi ning uute seadmete hankimise protsessi. Samuti on tutvustatud tarkvara ja seadmete analüüsi, mis sobib koguduse vajadustele ja nõuetele.

Kolmandas osas leiab Rakvere Karmeli koguduse arvutivõrgu kirjelduse ning turvaanalüüsi, kus on võetud aluseks ISKE meetmed arvutivõrgu turvalisusest.

Rakvere Karmeli koguduse uus kirikuhoone on tänaseks osaliselt kasutusse võetud, seega on edukalt võetud kasutusse ka arvutivõrk. Olemasolevat Rakvere Karmeli koguduse arvutivõrgu ülesehituse näidet on edukalt võimalik võtta vajadusepõhiselt ja väikeste kohandustega kasutusele teistel usuühendustel ning luua kirikus turvaline arvutivõrk.

Kasutatud allikad

[1] „Karmeli info,“ [Võrgumaterjal]. Available: https://www.karmel.ee/info. [Kasutatud 28 04 2021].

[2] „Kirikute ja koguduste seadus §2.1, 3.1,“ [Võrgumaterjal]. Available: https://www.riigiteataja.ee/akt/121062014030. [Kasutatud 28 04 2021].

[3] „Usulised ühendused,“ [Võrgumaterjal]. Available: https://www.siseministeerium.ee/et/eesmark-tegevused/usulised-uhendused. [Kasutatud 28 04 2021].

[4] „Statistika kirikute liikmeskonnast,“ [Võrgumaterjal]. Available: https://www.siseministeerium.ee/sites/default/files/dokumendid/statistilisi_andmeid_liikmeskond_vaimulikke_kogudusi_01_01_2013.pdf. [Kasutatud 28 04 2021].

[5] „Baptisti liit,“ [Võrgumaterjal]. Available: https://kogudused.ee. [Kasutatud 28 04 2021].

[6] „Karmeli koguduse visioon,“ [Võrgumaterjal]. Available: https://www.karmel.ee/visioon. [Kasutatud 28 04 2021].

[7] „Karmelikoguduse ehitus,“ [Võrgumaterjal]. Available: https://karmelikogudus.wixsite.com/sihtasutus/eesmaerk. [Kasutatud 28 04 2021].

[8] „Rakvere Karmeli koguduse tegevused,“ [Võrgumaterjal]. Available: https://www.karmel.ee/tegevusvaldkonnad. [Kasutatud 28 04 2021].

[9] „Rakvere Karmeli koguduse uus kirikuhoone,“ [Võrgumaterjal]. Available: https://www.karmel.ee/uushoone. [Kasutatud 28 04 2021].

[10] „ISKE meede M 4.202,“ [Võrgumaterjal]. Available: https://iske.ria.ee/8_06/ISKE_kataloogid/7_Kataloog_M/M4/M_4.202. [Kasutatud 28 04 2021].

[11] „ISKE meede M 1.43,“ [Võrgumaterjal]. Available: https://iske.ria.ee/8_06/ISKE_kataloogid/7_Kataloog_M/M1/M_1.43. [Kasutatud 28 04 2021].

[12] „ISKE meede M 2.11,“ [Võrgumaterjal]. Available: https://iske.ria.ee/8_06/ISKE_kataloogid/7_Kataloog_M/M2/M_2.11. [Kasutatud 28 04 2021].

[13] „Parimad tasuta tulemüürid,“ [Võrgumaterjal]. Available: https://www.techradar.com/best/best-free-linux-firewalls. [Kasutatud 28 04 2021].

[14] „Parimad tasuta ruuter, tulemüüri tarkvarad 2019,“ [Võrgumaterjal]. Available: https://teklager.se/en/best-free-linux-router-firewall-software-2019/. [Kasutatud 28 04 2021].

[15] „pfSense wiki,“ [Võrgumaterjal]. Available: https://en.wikipedia.org/wiki/PfSense. [Kasutatud 21 04 2021].

[16] „pfSense Join The Discussion,“ [Võrgumaterjal]. Available: https://www.pfsense.org/get-involved/. [Kasutatud 28 04 2021].

[17] „pfSense tarkvara,“ [Võrgumaterjal]. Available: https://github.com/pfsense/pfsense. [Kasutatud 21 04 2021].

[18] „OPNSense ajalugu (About the Fork),“ [Võrgumaterjal]. Available: https://docs.opnsense.org/history/thefork.html. [Kasutatud 28 04 2021].

[19] „OPNSense wiki teadmik,“ [Võrgumaterjal]. Available: https://en.wikipedia.org/wiki/OPNsense . [Kasutatud 28 04 2021].

[20] „IPFire wikipedia,“ [Võrgumaterjal]. Available: https://en.wikipedia.org/wiki/IPFire. [Kasutatud 28 04 2021].

[21] „Comparison_of_firewalls,“ [Võrgumaterjal]. Available: https://en.wikipedia.org/wiki/Comparison_of_firewalls. [Kasutatud 28 04 2021].

[22] „Võrk kui tulemüür: Pfsensenss, Opnensensense ja IPfire võrdlemisel,“ [Võrgumaterjal]. Available: https://www.thomas-krenn.com/de/tkmag/wp-content/uploads/2017/04/20170503-webinar-les-network.pdf. [Kasutatud 28 04 2021].

[23] „OPNSense proxy web filter,“ [Võrgumaterjal]. Available: https://docs.opnsense.org/manual/how-tos/proxywebfilter.html. [Kasutatud 28 04 2021].

[24] „Aruba IAP-205 manuaal,“ [Võrgumaterjal]. Available: https://h20195.www2.hpe.com/v2/GetPDF.aspx/c05272665.pdf. [Kasutatud 28 04 2021].

[25] „Infosüsteemide turvameetmete süsteem ISKE,“ [Võrgumaterjal]. Available: https://iske.ria.ee/8_06. [Kasutatud 28 04 2021].

[26] „E-ITS vahetab ISKE välja,“ [Võrgumaterjal]. Available: https://www.ria.ee/et/riigi-infosusteem/infokiri/ris-infokiri-marts-2021.html#E-ITS. [Kasutatud 04 05 2021].

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

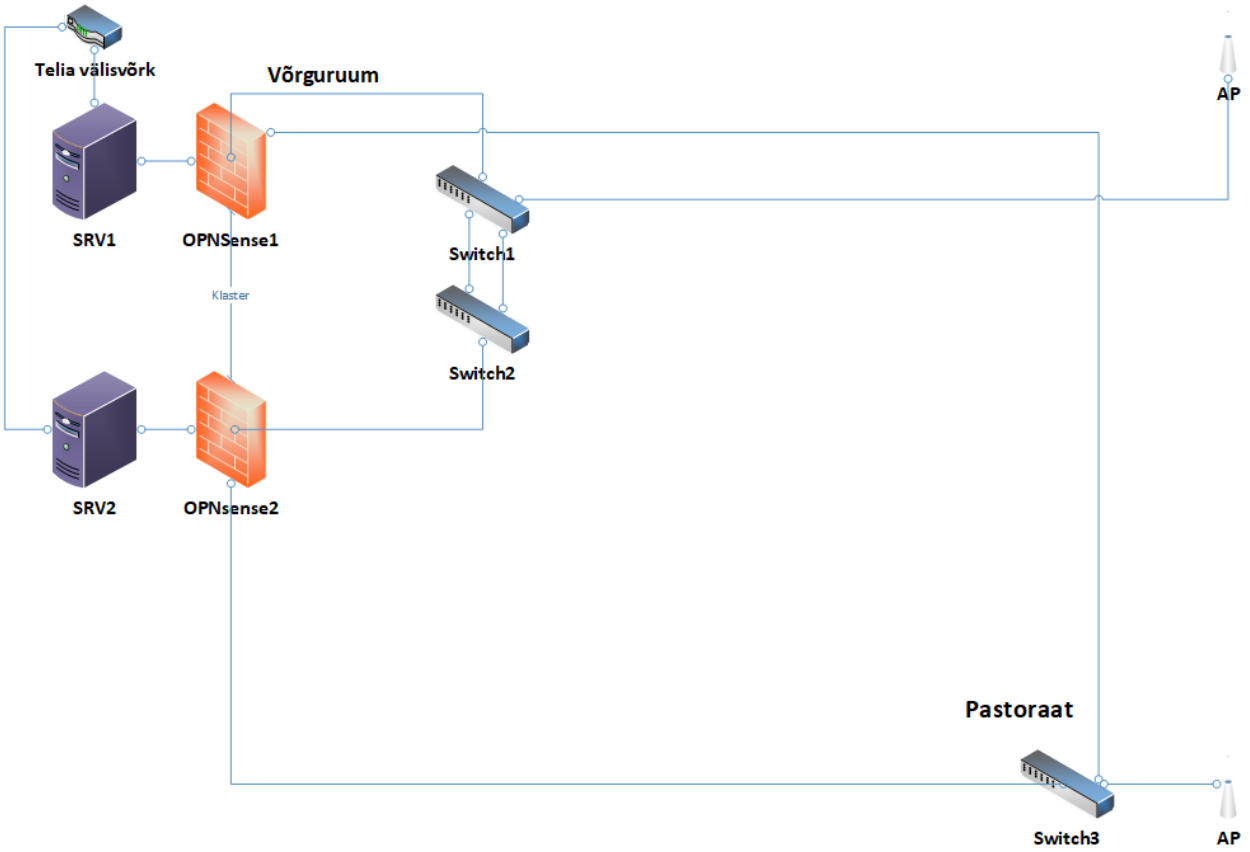
Mina, Erki Toming

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

[pp.kk.aaaa]

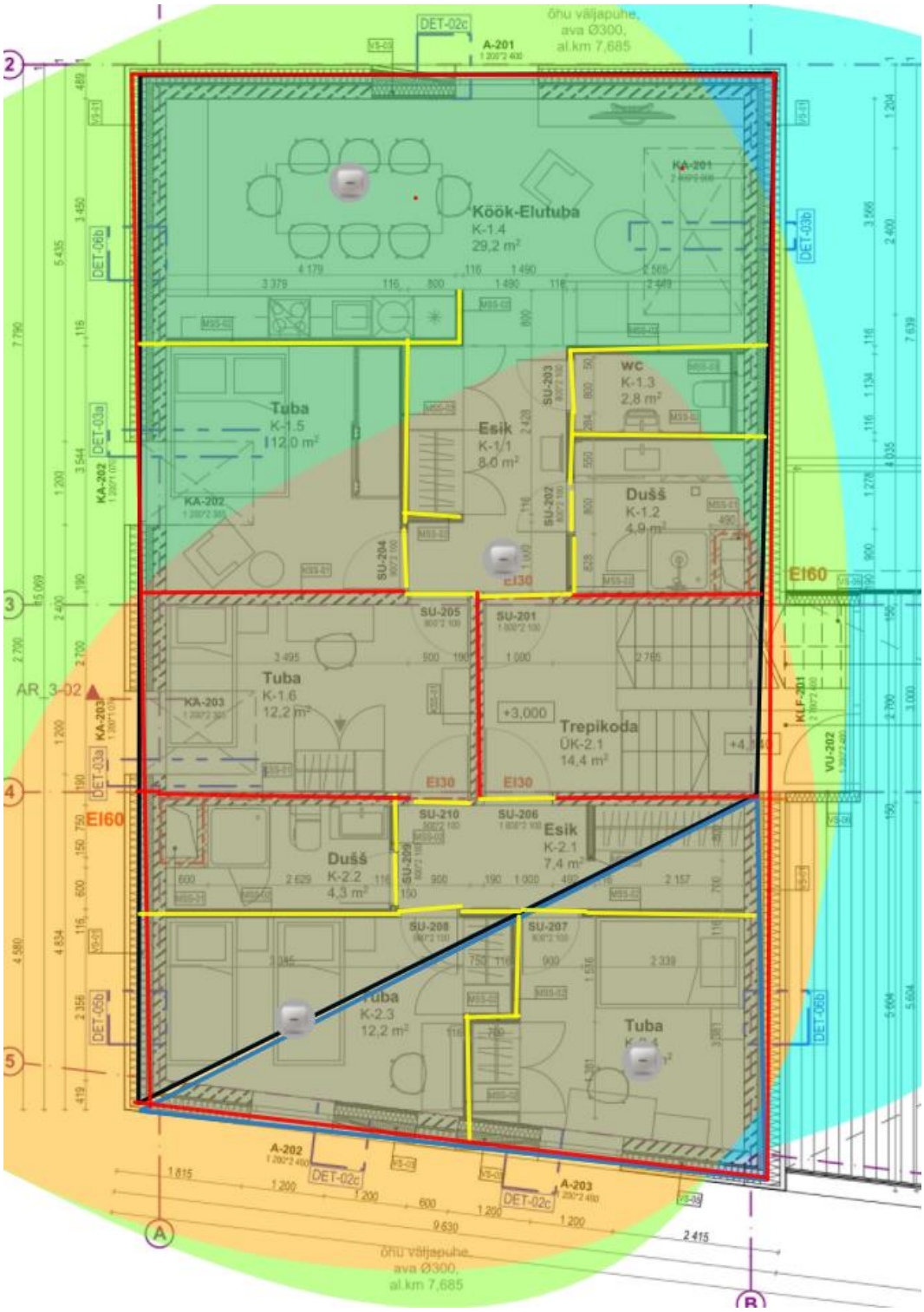
1 Lihtlitsents ei kehti juurdepääsupiirangu kehtivuse ajal vastavalt üliõpilase taotlusele lõputööle juurdepääsupiirangu kehtestamiseks, mis on allkirjastatud teaduskonna dekaani poolt, välja arvatud ülikooli õigus lõputööd reprodutseerida üksnes säilitamise eesmärgil. Kui lõputöö on loonud kaks või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

Lisa 2 - Rakvere Karmeli koguduse võrgujoonis

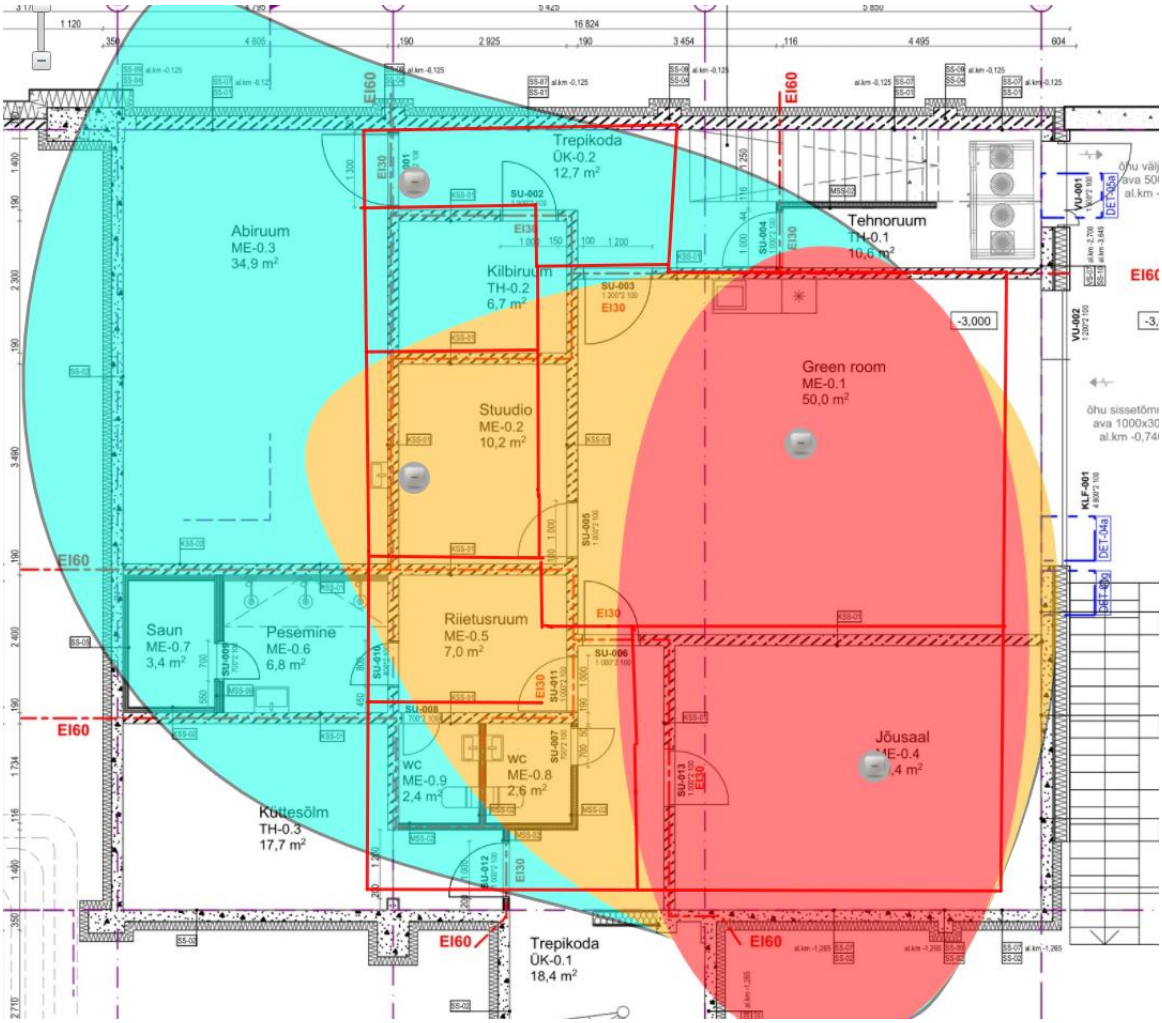


Joonis 1. Rakvere Karmeli koguduse võrgujoonis.

Lisa 3 - Traadita kohtvõrgu pääsupunkti jaotus kirikuhoones



Joonis 2. Traadita kohtvõrgu pääsupunktide jaotus pastoraadi osa.



Joonis 3. Traadita kohtvõrgu pääsupunktide jaotus keldris.

Joonis 4. Traadita kohtvõrgu pääsupunktide jaotus esimesel korrusel.

Lisa 4 - ISKE Analüüs tabeli kujul.

Tabel 2. ISKE meetmete analüüs *[25]*

0	**Meetme nr**	**Turbe-aste**	**Meetme nimetus**	**Olukorra kirjeldus**	**Meetme Staatus (rakendatud / osaliselt rakendatud / ei ole rakendatud / ei rakendata / ei saa rakendada)**
B 3.301 Turvalüüs (tulemüür)	M 2.70	L	Turvalüüsi (tulemüüri) kontseptsiooni väljatöötamine	Loodud on võrgu dokumentatsioon, kus on tulemüüride reeglistik välja toodud.	Rakendatud
B 3.301 Turvalüüs (tulemüür)	M 2.71	L	Turvalüüsi (tulemüüri) turvapoliitika	On välja töötatud teenused ja protokollid, mida läbi tulemüüri kasutatakse.	Rakendatud
B 3.301 Turvalüüs (tulemüür)	M 2.73	L	Sobiva turvalüüsi (tulemüüri) põhistruktuuri väljavalimine	On olemas tulemüür, kus kasutame paketifiltrit.	Rakendatud
B 3.301 Turvalüüs (tulemüür)	M 2.74	L	Sobiva paketifiltri valimine	Lubame võrkudevahelist liiklust minimaalselt ning on reeglid on dokumentatsioonis.	Rakendatud
B 3.301 Turvalüüs (tulemüür)	M 2.75	L	Sobiva rakenduslüüsi valimine	Kasutusel on ALG.	Rakendatud
B 3.301 Turvalüüs (tulemüür)	M 2.76	L	Sobivate filtreerimis-reeglite valimine ja kehtestamine	DMZ võrku pole hetkel vaja. Seest välja liiklust ei kontrollita. Segmentide vahel lubatud minimaalne liiklus. Vabatahtlikud koguduse liikmed administreerivad võrku ja reeglid on dokumenteeritud.	Osaliselt rakendatud
B 3.301 Turvalüüs (tulemüür)	M 2.77	L	Serverite integreerimine tulemüüri	Servereid kasutatakse ainult sisemisteks teenusteks. DMZ võrku pole vaja.	Ei rakendata
B 3.301 Turvalüüs (tulemüür)	M 2.78	L	Turvalüüsi (tulemüüri) turvaline kasutamine	Tulemüüril on kahetasemeline autentimine. Kontod on nimelised. HTTPS sertifikaat on ise	Osaliselt rakendatud

0	Meetme nr	Turbe-aste	Meetme nimetus	Olukorra kirjeldus	Meetme Staatus (rakendatud / osaliselt rakendatud / ei ole rakendatud / ei rakendata / ei saa rakendada)
				genereeritud. Turvauuendusi tehakse regulaarselt.	
B 3.301 Turvalüüs (tulemüür)	M 2.176z	L	Sobiva interneti-teenuse pakkuja valimine	Kasutusel on Telia ärikliendi internetilahendus.	Rakendatud
B 3.301 Turvalüüs (tulemüür)	M 2.299	L	Turvalüüsi (tulemüüri) turvapoliitika koostamine	Otseselt turvapoliitikad läbi töötatud ei ole, kuid osaline info on dokumentatsioonis kirjeldatud, näiteks kuidas toimib varundus.	Osaliselt rakendatud
B 3.301 Turvalüüs (tulemüür)	M 2.300	L	Turvalüüsi turvaline kõrvaldamine või selle komponentide asendamine	Uus võrk, siis pole veel midagi vaja olnud välja vahetada. Täpne seadmete hävitamine on juhtkonna otsustada.	Ei ole rakendatud
B 3.301 Turvalüüs (tulemüür)	M 2.301z	L	Turvalüüsi-teenuse väljast tellimine	Hetkel pole võrgutöödes kaughaldus lubatud ega teenust sisse ostetud.	Ei saa rakendata
B 3.301 Turvalüüs (tulemüür)	M 2.476	L	Interneti turvalise ühendamise kontseptsioon	Kontseptsioon on puudu. Hetkel on lubatud kõik liiklus seest välja.	Ei ole rakendatud
B 3.301 Turvalüüs (tulemüür)	M 3.43	L	Turvalüüsi administraatorite koolitus	Võrguseadmete administraatorid on väljaspool kirikut tööl ning on saanud vastava õppe tööga seoses.	Rakendatud
B 3.301 Turvalüüs (tulemüür)	M 4.47	L	Turvalüüsi operatsioonide logimine	Hetkel jäävad muudatuste logid ainult OPNsense'i serverisse. Analüüsitakse vajaduse põhiselt.	Ei ole rakendatud.
B 3.301 Turvalüüs (tulemüür)	M 4.100	L	Tulemüür ja aktiivsisu	Web filter turvaprofiili all blokeeritakse sisu külalistevõrgus. Sisevõrgus ei toimi blokeerimist.	Osaliselt rakendatud

0	Meetme nr	Turbe-aste	Meetme nimetus	Olukorra kirjeldus	Meetme Staatus (rakendatud / osaliselt rakendatud / ei ole rakendatud / ei rakendata / ei saa rakendada)
B 3.301 Turvalüüs (tulemüür)	M 4.222	L	Turvaprokside õige konfigureerimine	Külaliste võrgus on kasutusel web filtri kategooriad. FTP ja muude teenuste kasutamine on viidud miinimumi peale.	Osaliselt rakendatud
B 3.301 Turvalüüs (tulemüür)	M 4.227	L	Lokaalse NTP-serveri kasutamine aja sünkroni-seerimiseks	NTP teenus on installitud oma serverisse.	Rakendatud
B 3.301 Turvalüüs (tulemüür)	M 5.39	L	Protokollide ja teenuste ohutu kasutamine	Väljast sisse ei ole lubatud meetmes mainitud protokolle.	Rakendatud
B 3.301 Turvalüüs (tulemüür)	M 5.46	L	Autonoomsüstee-mide installeerimine interneti kasutamiseks	Pole täpset turvapoliitikat loodud, kuidas toimub seadmete haldus, kuid hetkel tehakse seda läbi serveri.	Osaliselt Rakendatud
B 3.301 Turvalüüs (tulemüür)	M 5.59	L	DNSi võltsimise tõrje	Tulemüüris on sisse lülitatud *IPS mode*.	Rakendatud
B 3.301 Turvalüüs (tulemüür)	M 5.70	L	Aadressi tõlkimine - Network Address Translation (NAT)	NAT-i kasutatakse sisevõrgu allikast internetiaadressi jaoks ja ka teises suunas: internetist päringud sisevõrgu serverini.	Rakendatud
B 3.301 Turvalüüs (tulemüür)	M 6.94	L	Turvalüüside hädaolukorraks valmisoleku plaan	Dokumentatsioonis on kirjeldatud varundamis-protsessi, kuid see ei sisalda taasteplaani.	Ei ole rakendatud
B 3.301 Turvalüüs (tulemüür)	M 2.302z	M	Turvalüüside kõrge käideldavuse tagamine	OPNsense on klastris.	Rakendatud
B 3.301 Turvalüüs (tulemüür)	M 4.224z	M	Virtuaalsete privaatvõrkude integreerimine turvalüüsidesse	Meede on soovituslik. VPN on dokumenteeritud ja logimine toimub kasutaja-põhiselt.	Rakendatud

0	Meetme nr	Turbe-aste	Meetme nimetus	Olukorra kirjeldus	Meetme Staatus (rakendatud / osaliselt rakendatud / ei ole rakendatud / ei rakendata / ei saa rakendada)
B 3.301 Turvalüüs (tulemüür)	M 5.71z	M	Sissetungi tuvastuse ja sellele reageerimise süsteemid	Tulemüüris on kasutusel IPS, web filter.	Osaliselt rakendatud
B 3.301 Turvalüüs (tulemüür)	M 5.115z	M	Veebiserveri integreerimine turvalüüsi koostisse	Ei ole väliseid veebiservereid.	Ei saa rakendata
B 3.301 Turvalüüs (tulemüür)	M 5.116z	M	Meiliserveri integreerimine turvalüüsi koostisse	Meili server asub teenusepakkuja juures	Ei saa rakendata
B 3.301 Turvalüüs (tulemüür)	M 5.117z	M	Andmebaasi-serveri integreerimine turvalüüsi koostisse	Ei ole väliseid servereid.	Ei saa rakendata
B 3.301 Turvalüüs (tulemüür)	M 5.119z	M	Veebi-, rakendus- ja andmebaasiserveritega veebirakenduse integreerimine turvalüüsi koostisesse	Ei ole väliseid teenuseid majutatud kirikuhoones.	Ei saa rakendata
B 3.301 Turvalüüs (tulemüür)	M 5.120	M	ICMP-protokolli käsitlus turvalüüsis	Väljast sisse pole lubatud. Segmendi piires on lubatud ICMP-protokoll.	Osaliselt rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 1.43	L	Võrgu aktiiv-komponentide turvaline paigutus	Seadmed asuvad lukustatud kapis. Paroolid on meetmele M 2.11 vastavad.	Rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 2.276z	M	Marsruuteri funktsionaalne kirjeldus	Soovituslik meede. Kirjeldav meede. Marsruutimine on tulemüüri funktsionaalsusena kasutuses ja müüri kaudu on teostatud ka VPN.	Rakendatud

0	Meetme nr	Turbe-aste	Meetme nimetus	Olukorra kirjeldus	Meetme Staatus (rakendatud / osaliselt rakendatud / ei ole rakendatud / ei rakendata / ei saa rakendada)
B 3.302 Marsruuterid ja kommutaatorid	M 2.277z	M	Kommutaatori funktsionaalne kirjeldus	Soovituslik meede. Kirjeldav meede. VLAN-id ja trunkimine on kasutuses.	Rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 2.278z	M	Marsruuterite ja kommutaatorite kasutamise tüüp-stsenaariumid	Soovituslik meede. Kirjeldav meede. Marsruutimine on tulemüüri funktsionaalsusena kasutuses ja müüri kaudu on teostatud ka VPN.	Rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 2.279	M	Marsruuterite ja kommutaatorite turvapoliitika koostamine	Turvapoliitika on kirjeldatud dokumentatsioonis.	Rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 2.280	M	Sobivate marsruuterite ja kommutaatorite ostmis- ja valimis-kriteeriumid	Seadmed ostetud vajaduse põhiselt.	Rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 2.281	M	Marsruuterite ja kommutaatorite süsteemi-konfiguratsiooni dokumen-teerimine	Konfiguratsiooni ei hallata tsentraalselt. Dokumentatsioonis on kirjeldatud konfiguratsioon ning tehakse konfiguratsioonist varundus.	Osaliselt rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 2.283	M	Marsruuterite ja kommutaatorite tarkvara hooldus	Administraatorid jälgivad meililisti kaudu uuenduste tootjapoolset infot ning seejärel uuendavad.	Rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 2.284	M	Marsruuterite ja kommutaatorite turvaline tööst kõrvaldamine	Hetkel pole vajadust seadmeid kõrvaldada. Koguduse juhtkond korraldab vanade seadmete kõrvaldamise.	Rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 3.38	M	Marsruuterite ja kommutaatorite koolitus adminis-traatoritele	Koguduse vabatahtlikud on oma ala spetsialistid ja saavad koolitusi töö kaudu.	Rakendatud

0	Meetme nr	Turbe-aste	Meetme nimetus	Olukorra kirjeldus	Meetme Staatus (rakendatud / osaliselt rakendatud / ei ole rakendatud / ei rakendata / ei saa rakendada)
B 3.302 Marsruuterid ja kommutaatorid	M 4.201	M	Marsruuterite ja kommutaatorite turvaline lokaalne alus-konfiguratsioon	Aluskonfiguratsioon kõikidele kommutaatoritele. Kõik seadmed varundatakse ja dokumenteeritakse.	Rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 4.202	M	Marsruuterite ja kommutaatorite turvaline võrgu-alus-konfiguratsioon	Eraldatud on seadmehaldusvõrk, kus saab võrguseadeid seadistada.	Osaliselt rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 4.205	M	Marsruuterite ja kommutaatorite töö logimine	Keskset logihaldust ei toimu.	Ei ole rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 4.206	M	Kommutaatori portide turvamine	Kasutuseta pordid on deaktiveeritud.	Rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 5.111	M	Marsruuterite pääsuloendite konfigureerimine	Kogudusel on hetkel kaks kindlat vabatahtlikust administraatorit. Kõik seadistused dokumenteeritakse. Seadistused ei tohi minna vastuollu ISKE meetmetega.	Rakendatud
B 3.302 Marsruuterid ja kommutaatorid	M 6.91	M	Marsruuterite ja kommutaatorite andmete varundus ja taaste	Kaetud teiste meetmetega. Vt M 6.52	
B 3.302 Marsruuterid ja kommutaatorid	M 6.92	M	Marsruuterite ja kommutaatorite hädaolukorraks valmisoleku plaan	Plaani ei ole tehtud. HP garantii toimub üldjuhul kiiresti.	Ei ole rakendatud
B 4.1 Heterogeensed võrgud	M 2.139	L	Olemasoleva võrgukeskkonna läbivaatus	On olemas võrgudiagrammid. Lisaks VLAN-ide ja subnettide tabelid.	Rakendatud
B 4.1 Heterogeensed võrgud	M 4.7	L	Algparoolide muutmine	Kõik paroolid on muudetud ja vastavad ISKE meetmele.	Rakendatud

0	Meetme nr	Turbe-aste	Meetme nimetus	Olukorra kirjeldus	Meetme Staatus (rakendatud / osaliselt rakendatud / ei ole rakendatud / ei rakendata / ei saa rakendada)
B 4.1 Heterogeensed võrgud	M 4.79	L	Kohapealse võrguhalduse turvalised pääsu-mehhanismid	Kõik paroolid on muudetud ja vastavad ISKE meetmele.	Rakendatud
B 4.1 Heterogeensed võrgud	M 4.83	L	Võrgu-komponentide riistvara ja tarkvara värskendamine ja täiendamine	Vabatahtlikud administraatorid jälgivad e-maili teavituse teel uuendusi ning vajadusel uuendavad.	Rakendatud
B 4.1 Heterogeensed võrgud	M 5.2	L	Võrgu sobiv topoloogia	Kommutaatorid on omavad liidestust L2 info vahetamiseks.	Rakendatud
B 4.1 Heterogeensed võrgud	M 5.13	L	Võrgu ühendus-aparatuuri õige kasutamine	Kirjeldav meede. kommutaatoreid ja ruutereid kasutatakse sihipäraselt.	Rakendatud
B 4.1 Heterogeensed võrgud	M 5.60	L	Sobiva magistraal-võrgutehnika valimine	Kirjeldav meede. Praegune kasutuses olev magistraalvõrgu tehnoloogia on täiesti piisav.	Rakendatud
B 4.1 Heterogeensed võrgud	M 5.62z	L	Sobiv loogiline segmenteerimine	On üksteisest eraldatud segmendid.	Rakendatud
B 4.1 Heterogeensed võrgud	M 2.140z	M	Võrgu hetkeolukorra analüüsimine	Soovituslik meede. Äsja püstitati uus lahendus ja käesolev audit aitab seda analüüsida ja nõrku kohti välja tuua.	Rakendatud
B 4.1 Heterogeensed võrgud	M 2.141	M	Võrgu-kontseptsiooni väljatöötamine	On olemas ajakohene võrgu dokumentatsioon.	Rakendatud
B 4.1 Heterogeensed võrgud	M 5.8	M	Võrgu regulaarne turvakontroll	Turvakontrolli tehakse vajaduse põhiselt. Ei toimu regulaarselt.	Ei ole rakendata
B 4.1 Heterogeensed võrgud	M 6.53z	M	Võrgu-komponentide liiasus	Komponendid omavad kahte eri liidest L2 info vahetamiseks.	Rakendatud

0	Meetme nr	Turbe-aste	Meetme nimetus	Olukorra kirjeldus	Meetme Staatus (rakendatud / osaliselt rakendatud / ei ole rakendatud / ei rakendata / ei saa rakendada)
B 4.1 Heterogeensed võrgud	M 6.54	M	Protseduurid võrgu tervikluse kao puhuks	Ei ole välja töötatud.	Ei ole rakendatud
B 4.1 Heterogeensed võrgud	M 6.75z	M	Varu-sidekanalid	Tulevikus on plaanis leida lahendus teise sidekanali jaoks.	Ei ole rakendatud
B 4.2 Võrgu- ja süsteemihaldus	M 2.146	L	Võrgu-haldussüsteemi turvaline kasutamine	Paroolid on loodud vastavalt ISKE meetmele. Välisvõrgust ei lubatud hallata võrke.	Rakendatud
B 4.2 Võrgu- ja süsteemihaldus	M 2.168	L	IT-süsteemi analüüs enne süsteemi-haldussüsteemi evitust	Enne lõputööd sai loodud ennetav analüüs.	Rakendatud
B 4.2 Võrgu- ja süsteemihaldus	M 4.91	L	Süsteemi-haldussüsteemi turvaline installeerimine	Installimisel on jälgitud ISKE meetmeid.	Rakendatud
B 4.2 Võrgu- ja süsteemihaldus	M 4.92	L	Süsteemi-haldussüsteemi turvalise töö tagamine	Võrguhalduse põhimõtted on kirjeldatud dokumentatsioonis.	Rakendatud
B 4.2 Võrgu- ja süsteemihaldus	M 6.52	L	Võrgu aktiiv-komponentide konfiguratsiooni-andmete regulaarne varundamine	Seadmete varundus toimub peale iga muutatust käsitsi.	Rakendatud
B 4.4 Virtuaalne privaatvõrk (VPN)	M 2.415	L	VPN-i vajaduste analüüs	VPN-i kasutamine on väljatöötatud ja dokumenteeritud.	Rakendatud
B 4.4 Virtuaalne privaatvõrk (VPN)	M 2.416	L	VPN-i kasutamise planeerimine	VPN-i ligipääsu on võimalik lubada kahel vabatahtlikul administraatoril ning dokumenteeritakse.	Rakendatud

0	Meetme nr	Turbe-aste	Meetme nimetus	Olukorra kirjeldus	Meetme Staatus (rakendatud / osaliselt rakendatud / ei ole rakendatud / ei rakendata / ei saa rakendada)
B 4.4 Virtuaalne privaatvõrk (VPN)	M 3.65w	L	Sissejuhatus VPN-i põhimõistetesse	Vabatahtlikud administraatorid on oma ala spetsialistid ja töötavad väljaspool kogudust samal erialal.	Rakendatud
B 4.4 Virtuaalne privaatvõrk (VPN)	M 4.320	L	VPN-i turvaline konfigureerimine	Kasutusel on WireGuard VPN-lahendus.	Rakendatud
B 4.4 Virtuaalne privaatvõrk (VPN)	M 4.322	L	Mittevajalike VPN-pääsude blokeerimine	Kontod on tulemüüris ja VPN-i vajaduse puudumisel blokeeritakse konto.	Rakendatud
B 4.4 Virtuaalne privaatvõrk (VPN)	M 5.122	L	Sülearvuti turvaline ühendamine kohtvõrguga	Split tunneling pole lubatud. VPN-i kasutajad peavad läbima ühendamiseks kahetasemelise autentimise.	Rakendatud
B 4.4 Virtuaalne privaatvõrk (VPN)	M 2.420	M	Trusted VPN-i teenusepakkuja valimine	Ei ole kasutusel	Ei saa rakendata
B 4.4 Virtuaalne privaatvõrk (VPN)	M 4.224z	M	Virtuaalsete privaatvõrkude integreerimine turvalüüsidesse	VPN-i jaoks on tulemüüri paigaldatud lisamoodul ning logisid näeb tulemüürist.	Rakendatud
B 4.4 Virtuaalne privaatvõrk (VPN)	M 5.77z	M	Alamvõrkude rajamine	Soovituslik meede. VPN-i kasutajad ei satu eraldi VLAN-i, vaid neile on määratud eraldi IP-vahemik. Logidest on näha autentimised ja võrgutoimingud (metadata tasemel).	Rakendatud
B 4.6 Traadita kohtvõrgud	M 1.63	L	Sobiv pääsupunktide paigutus	Kuna terve maja ei ole veel kasutusel, siis ei ole tehtud mõõdistust. Paigaldamisel kasutati vastavat tarkvara Aruba poolt	Osaliselt rakendatud

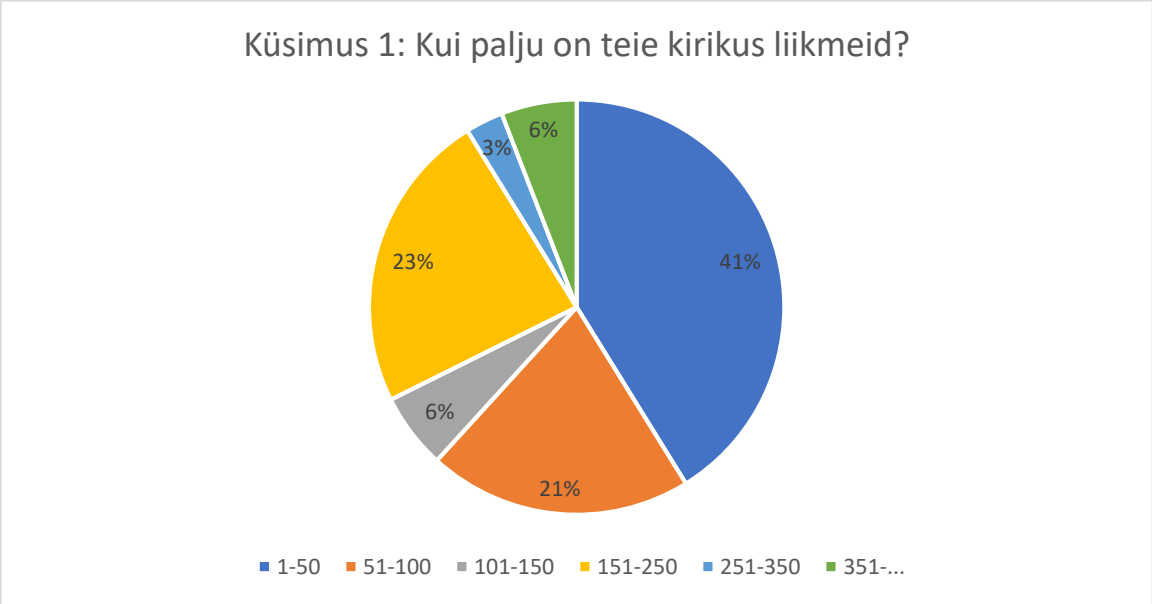
0	Meetme nr	Turbe-aste	Meetme nimetus	Olukorra kirjeldus	Meetme Staatus (rakendatud / osaliselt rakendatud / ei ole rakendatud / ei rakendata / ei saa rakendada)
B 4.6 Traadita kohtvõrgud	M 2.383	L	Sobiva traadita kohtvõrgu standardi valik	802.11a/n/ac, 802.11b/g/n on toetatud standardid. Sisevõrgus ja tehnika võrgus on kasutusel üksnes 5 GHz, külaliste võrgus on nii 2,4 GHz kui ka 5 GHz.	Rakendatud
B 4.6 Traadita kohtvõrgud	M 2.384	L	Sobiva traadita kohtvõrgu krüpteerimisviisi valik	Kontori ja tehnika traadita ühendusel on WPA2 parooli kaitse peal ning iseteenindusportaal, kus kasutaja ja paroolipõhine kaitse. Külaliste võrk on kaitstud WPA2.	Rakendatud
B 4.6 Traadita kohtvõrgud	M 2.385	L	Sobivate traadita kohtvõrgu komponentide valik	Arvestatud M-taseme ISKE meetmetega.	Rakendatud
B 4.6 Traadita kohtvõrgud	M 2.388	L	Asjakohane traadita kohtvõrgu võtmehaldus	Traadita side paroolivahetus pole veel välja töötatud.	Ei ole rakendatud
B 4.6 Traadita kohtvõrgud	M 3.59	L	Traadita kohtvõrgu turvalise kasutamise koolitus	Kasutajatele on plaanis teha juhend traadita side kasutamise osas.	Ei ole rakendatud
B 4.6 Traadita kohtvõrgud	M 4.296	L	Traadita kohtvõrgu sobiva haldussüsteemi kasutamine	Uus võrk on, seega ei ole logiandmeid veel analüüsitud. Pääsupunktid on dokumenteeritud	Osaliselt rakendatud
B 4.6 Traadita kohtvõrgud	M 4.298	L	Traadita kohtvõrgu komponentide regulaarne audit	Lahendus on uus, st eelmisi auditeid ei ole tehtud.	Rakendatud

0	Meetme nr	Turbe-aste	Meetme nimetus	Olukorra kirjeldus	Meetme Staatus (rakendatud / osaliselt rakendatud / ei ole rakendatud / ei rakendata / ei saa rakendada)
B 4.6 Traadita kohtvõrgud	M 5.139	L	Traadita kohtvõrgu turvaline ühendamine kohtvõrguga	WLAN ja LAN on eraldi segementeeritud.	Rakendatud
B 4.6 Traadita kohtvõrgud	M 5.140	L	Traadita kohtvõrgu jaotussüsteemi ehitus	AP-d on kaablitega (PoE). Segmenditud ja segmentide võrguskeemid või andmetabelid on olemas.	Rakendatud
B 4.6 Traadita kohtvõrgud	M 6.102	L	Käitumisreeglid traadita kohtvõrkude turvaintsidentide puhul	Intsidentide käsitlemise korda pole juurutatud.	Ei ole rakendatud
B 4.6 Traadita kohtvõrgud	M 2.386z	M	Traadita kohtvõrgu migratsiooni-etappide hoolikas planeerimine	Seadmete hankimisel sai tehtud analüüs asutuse vajadustest lähtuvalt.	Rakendatud
B 4.6 Traadita kohtvõrgud	M 2.387z	M	Kolmandate osapoolte kasutamine traadita kohtvõrgu paigaldamisel, konfigureerimisel ja nõustamisel	Ei kasutatud kolmandaid osapooli.	Ei ole rakendatud
B 4.6 Traadita kohtvõrgud	M 2.389z	M	Avalike pääsupunktide turvaline kasutus	Ei ole koolitusi.	Ei ole rakendatud

Lisa 5 – Usuühenduste küsitlus

Kui palju on teie kirikus liikmeid?

Küsimuse eesmärk on näha küsitluses erinevate koguduste suurusest tulenevalt teadmisi ja arvutivõrgu hetkeseisu. Samuti selgitada välja erinevate suuruses koguduste vajadusi. Vastanute seas oli nii väikeseid kui ka suuri kirikuid. Vastanud kirikute seas oli suur osakaal 1–50 liikmelistel kirikutel, kuid oli ka kaks üle 350 liikmega kogudust.

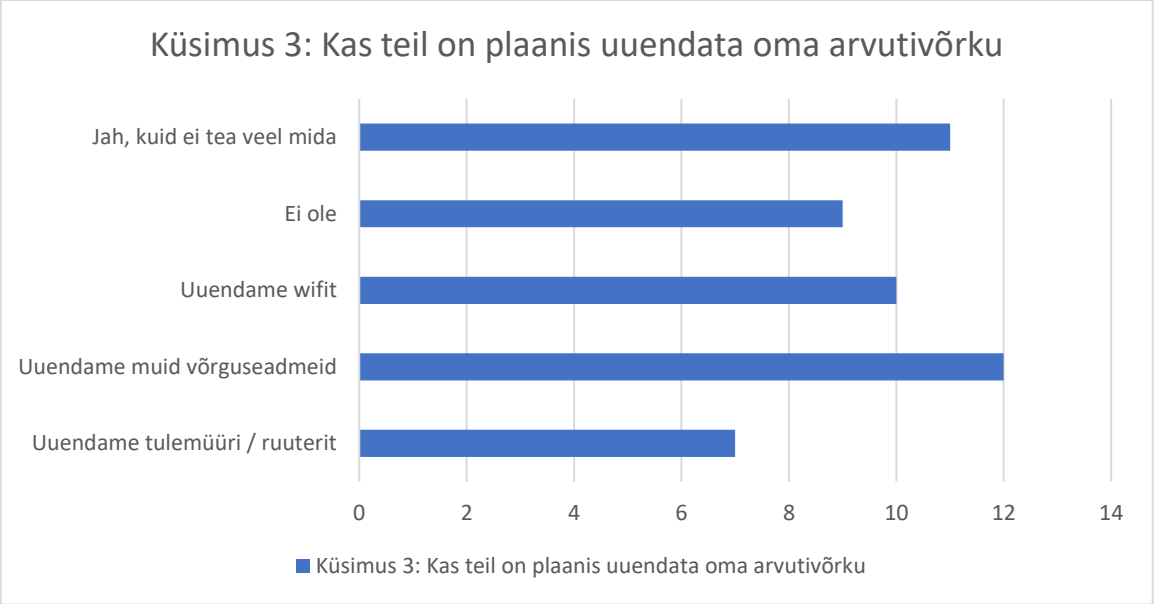


Kas teie arvutivõrk vajaks uuendamist?

Vastanute seast arvas 24 kogudust, et nende arvutivõrk vajaks uuendamist praegu. Eitavaid vastuseid oli 10 ja neist pooled olid kuni 50-liikmelised kogudused. Veel vastasid „ei“ üks 51–100, üks 100–150, kaks 151–250 ja üks üle 351-liikmeline kogudus.

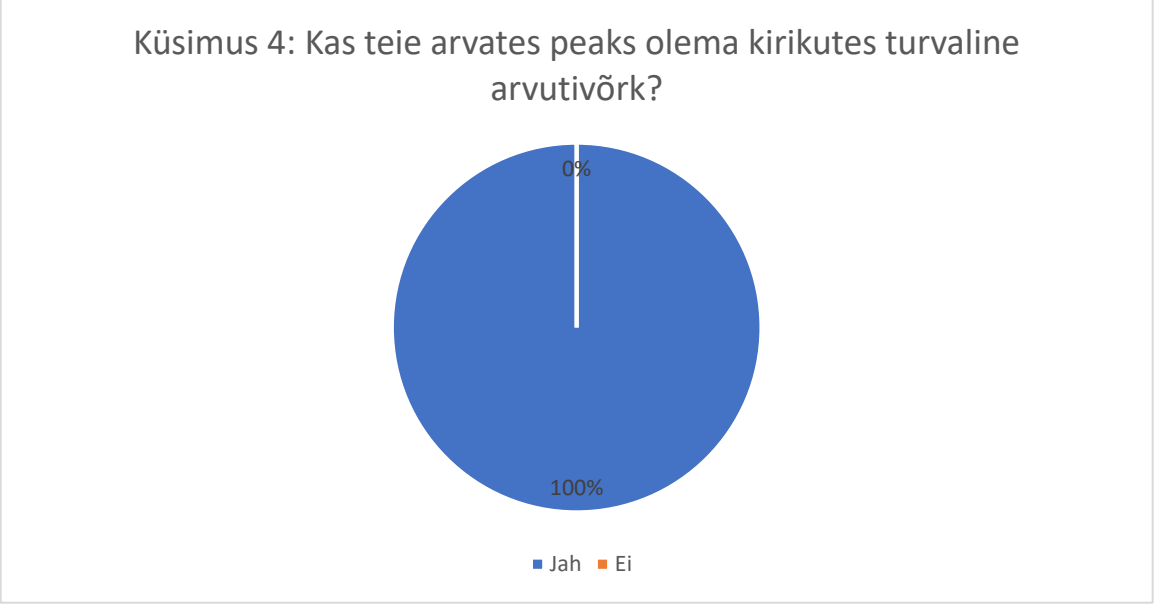
Kas teil on plaanis uuendada oma arvutivõrku?

24 kogudust vastasid, et neil on plaanis midagi võrgus uuendada, kuid leidus vastanute seas ebakõla eelmise küsimusega. Kolm kogudust, kes vastasid, et nende arvutivõrk ei vaja uuendust, on sellele küsimusele vastanud, et on plaanis teha mingi uuendus arvutivõrgus. Vastanute seast kolm kogudust, kes vastasid, et nende arvutivõrk vajaks uuendamist, ei plaani teha arvutivõrguga midagi. Vastanute seast 11 soovib uuendada enda arvutivõrku, kuid ei tea veel, mida. Lõputöö üheks eesmärgiks on, et ehitatud arvutivõrk Rakvere Karmeli kogudusele aitab jõuda selgusele, mida oleks vaja teha kogudustel, et nende võrk oleks turvaline.



Kas teie arvates peaks olema kirikutes turvaline arvutivõrk?

Hea tõdeda, et kõik 34 vastanut on ühel meelel, et ükskõik kui suur on nende kirik, siis arvutivõrk peab olema turvaline.



Mis teie arvates teeb arvutivõrgu turvaliseks?

Küsimuse eesmärk on selgitada välja vastanute teadmisi turvalisest arvutivõrgust. Vastused on pigem pinnapealsed ja napisõnalised. Mitmed vastasid, et tulemüür või viirusetõrje, ning samuti

on vastatud, et „pole kindel” või „ei tea”. Seega võib antud vastustest järeldada, et üksikutel vastanutel on teadmisi turvalisest arvutivõrgust, sest lihtsalt tulemüür ega viirusetõrje ei tee arvutivõrku turvaliseks, vaid administraatori poolt tehtud seadistused.

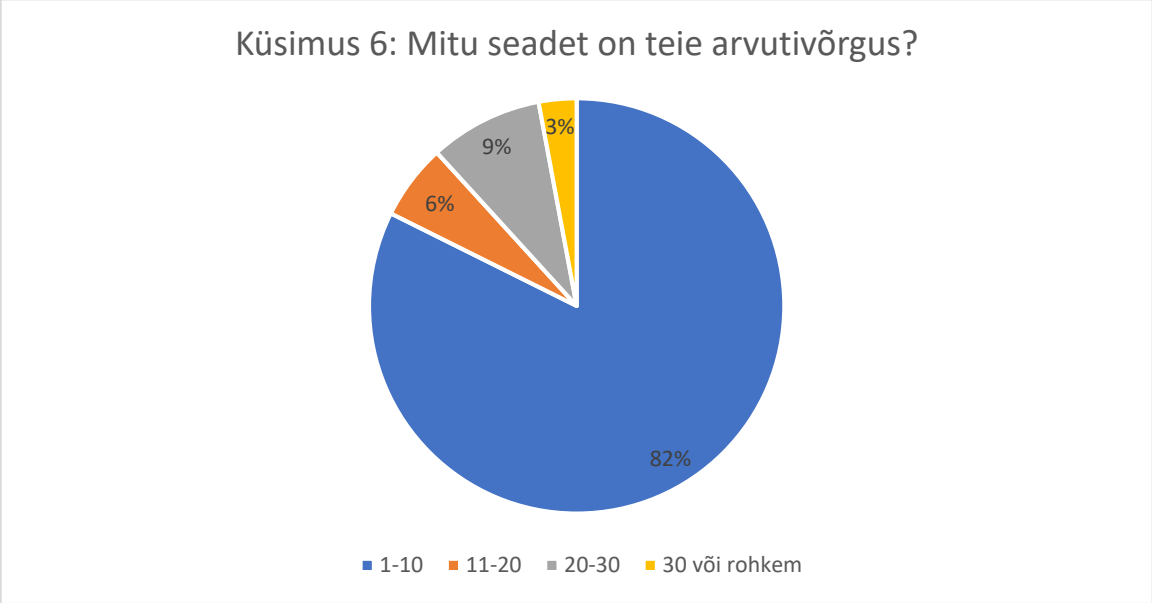
Küsimus 5: Mis teie arvates teeb arvutivõrgu turvaliseks?
Ei tea
Tulemüür, mitmeastmeline autentimine
See, kui võrku saavad kasutada vaid selleks loa saanud inimesed. Juhu- ja pahatahtlikud kasutajad ei saa võrku ligi
Viirusetõrje
Kaasaegne tehnika ja uusim tulemüür
Tulemüür, hästi konfitud võrguseadmed, võrgumonitooring, kasutuspoliitika ja -reeglid, võrguadministrator regulaarne töö
Ei ole kindel, aga arvan, et õige tulemüür ja ka kaasaegne viirusetõrje
Usaldusväärsete proffide nõustamine
Piiratud ligipääs võrguressursidele (paroolid, erinevad ligipääsu lahendused). Eraldatud võrguruumid sisevõrgule, külalistele, tehnikale jne kasutades VLAN-e
Kvaliteetne riistvara (ruuter tulemüüriga), regulaarne uuendamine – ennekõike *firmware*
Tulemüür ja pidevalt uuendatud viirusetõrjed
Süsteemne haldamine, hooldus
Tulemüür, paroolid
Igaüks ei pääse ligi ja viirusetõrje on tasemel
Professionaalsed inimesed
Tulemüür, viirusetõrje
Kaitsesüsteemid
Pakun, et viiruskaitse
Hea majutuse pakkuja ning internetiteenuse pakkuja
Kui ma suudan mingilgi määral kontrollida või näha, kes seda arvutivõrku kasutavad. Ei soovi, et kogudusevälised inimesed arvutivõrku kasutaks kogudusevälisteks tegemisteks (nt kui koguduse naabrid laevad filme või muid asju endale alla)

Kontrollitud haldus
Vastavad seadmed, õigeaegselt paigaldatud uuendused ja teadlikud kasutajad
Viirused ei pääse sisse
Paroolid, admete krüptimine ja turvalised võrgud
Kaasaegne tarkavara ja riistvara, korrektne arhitektuur, õige seadistus, monitooring, tarkvara ja riistvara *firmware*-värskendused
Viirusetõrje
Turvaline tulemüür
Kui andmed ei leki
Hea ühendus
Autentimine, võrkude lahusus, samuti võib lisada MAC-filtri ja wifi puhul vähendada leviala

Mitu seadet on teie arvutivõrgus?

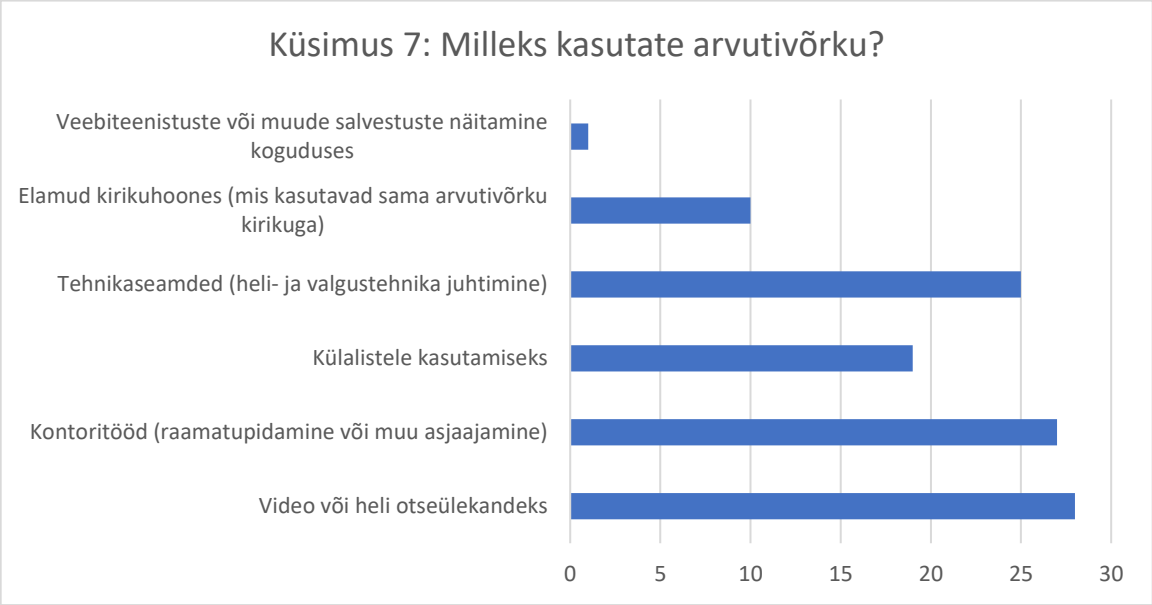
Antud vastuses võime järeldada, et usuühendustel on hetkel pigem vähe seadmeid, 28 vastanut vastas, et neil on 1–10 seadet. Küsimusest 9 näeme, et 23 kirikut kasutavad enda wifi leviala tekitamiseks teenusepakkuja seadet, seega saame järeldada, et neil pole muid võrguseadmeid, kui mõni arvuti.

Siinkohal peab arvestama, et küsitlus tehti enne, kui usuühendused said riigi käest toetust tehnika arendamiseks, seega võib seadmete arv olla juba tänaseks kasvanud.



Milleks kasutate arvutivõrku?

Selle küsimuse eesmärk on uurida, mis tegevusi tehakse kiriku arvutivõrgus ning sellest saab teha järelduse, kas arvutivõrku peaks segmenteerima. Vastanutest 28 usuühenduse liiget vastasid, et kasutavad internetti video- või heliülekannete jaoks. See number võib samuti olla juba kasvanud, sest valitsus on pannud uued piirangud peale kogudustele ning kõik kogudused arendavad enda süsteeme suuremaks, et pakkuda paremat ülekande kvaliteeti. Samuti tehakse igapäevaselt 27 kirikus kontoritöid.



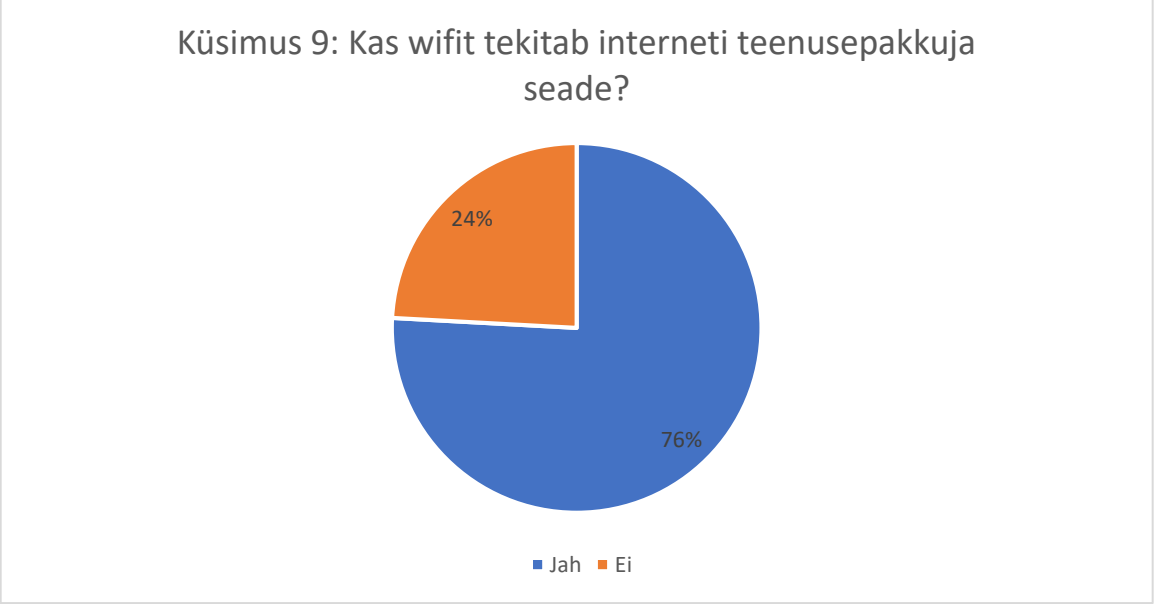
Kas teie kirikus on wifi?

Ainult 5 vastanutest ei olnud kirikuhoones wifit. Neist neli vastanut on väikese liikme arvuga usuühendused (1-50) ning üks vastanutest on 151-250 liikmeline.

Kas wifit tekitab interneti teenusepakkuja seade?

Siin küsimuses ei arvestatud kahte vastajat, sest vastasid 8 küsimuses, et neil ei ole wifit, seega nende teenusepakkuja seade ei tekitada wifit.

Enamus vastajatest tekitab wifit teenusepakkuja seade, seega võib järeldata, et enamustel ei ole suuri traadita võrke.



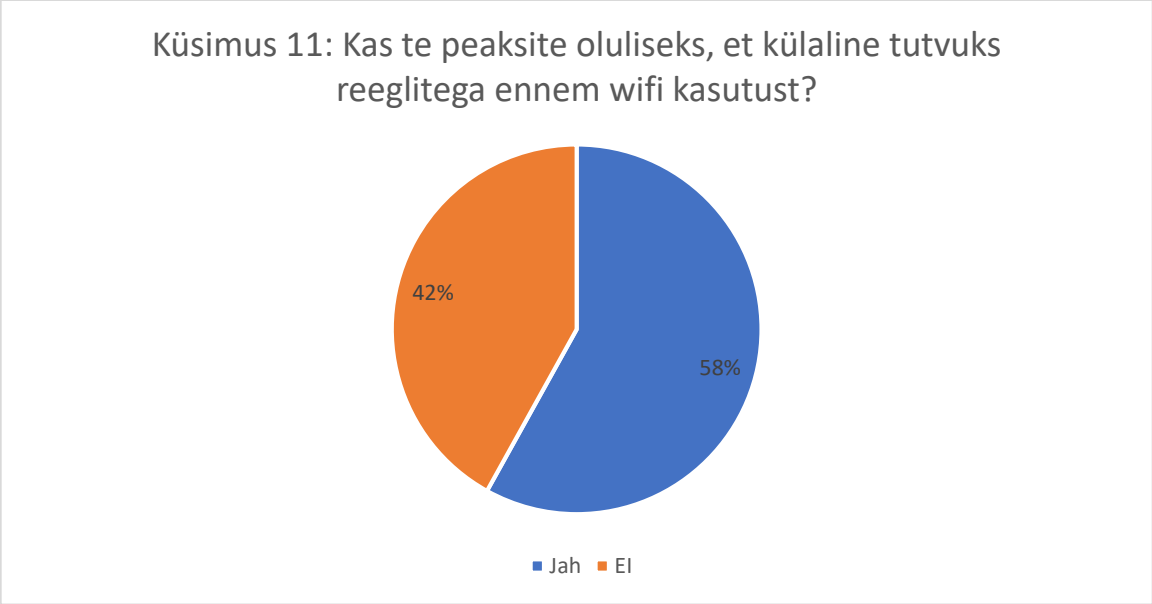
Kas külalistele on eraldatud eraldi wifi võrk?

Selles küsimuses ei arvestatud kahte vastajat, sest vastasid 8 küsimuses, et neil ei ole wifit, seega neil ei saa olla külaliste wifi eraldatud, kui neil polegi traadita võrku.

Vastanute seast üheksa kirikut kasutab arvutivõrku kontoritööks ja jagavad sama võrku külalistele või elamule kirikuhoones, kuid pole eraldatud kontorit ja külaliste võrku. Ja kõigil üheksal tekitab wifit teenusepakkuja seade. Neist üheksast kogudusest 5 on suuremad kui 100 liikmelised.

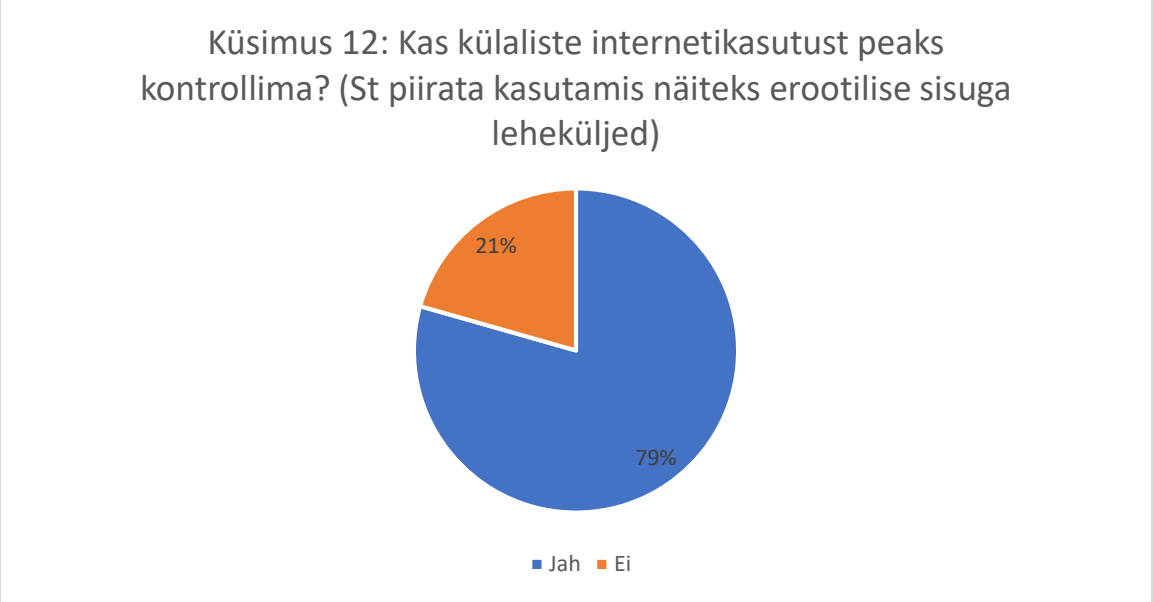
Kas te peaksite oluliseks, et külaline tutvuks reeglitega enne wifi kasutust?

Suurem osa kogudustest leiab, et kasutajad peaksid tutvuma koguduse wifi kasutamisreeglitega ning andma nõusoleku enne arvutivõrku lubamist. Seitse „Ei“ vastanutest olid alla 100-liikmelised kogudused. 14 „jah“ vastanutest on üle 100-liikmelised kogudused ning neli alla 100- liikmelised kogudused.



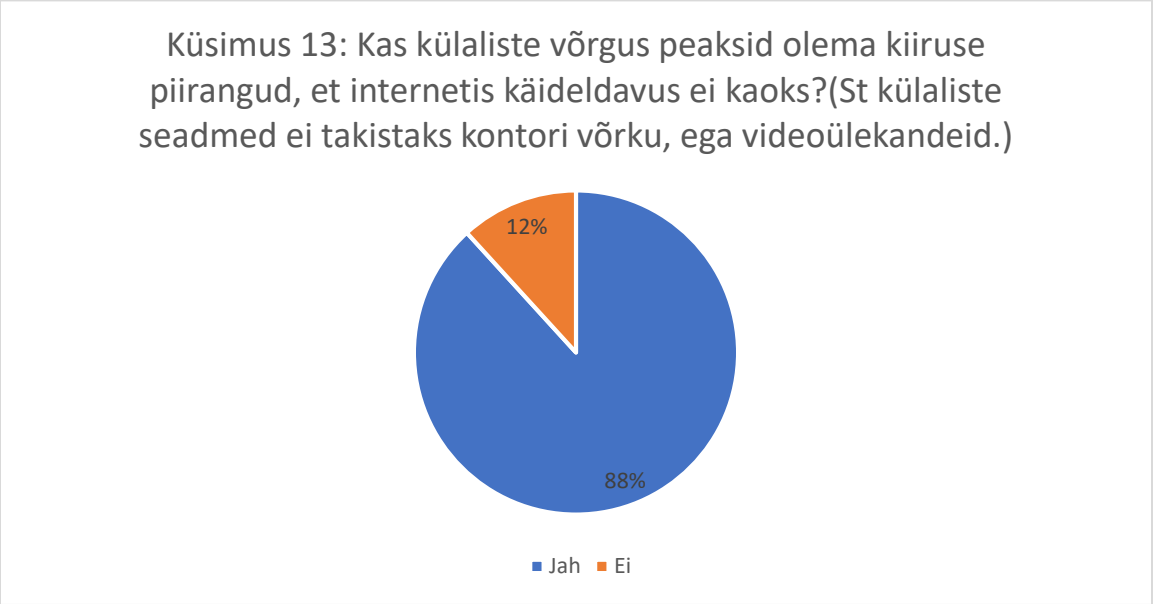
Kas külaliste internetikasutust peaks kontrollima?

„Ei“ vastanute seas oli nii väikseid kui ka suuremaid kogudusi, kuid ülekaalukalt ikkagi arvati, et peaks piirama külaliste võrgus olevat liiklust sisu poolest.



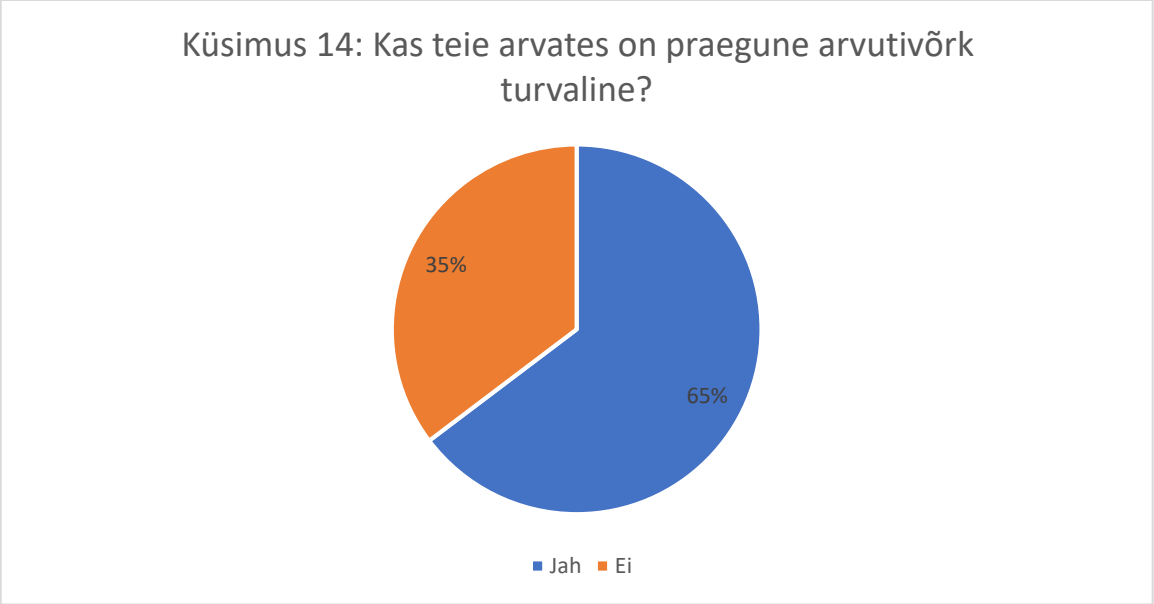
Kas külaliste võrgus peaksid olema kiiruse piirangud, et internetis käideldavus ei kaoks?

Peaaegu kõik vastanutest arvavad, et peaks piirama külalistevõrgu interneti kiirust. Neljast „ei“ vastanust kolm ei teinud vastamise hetkel otseülekandeid.



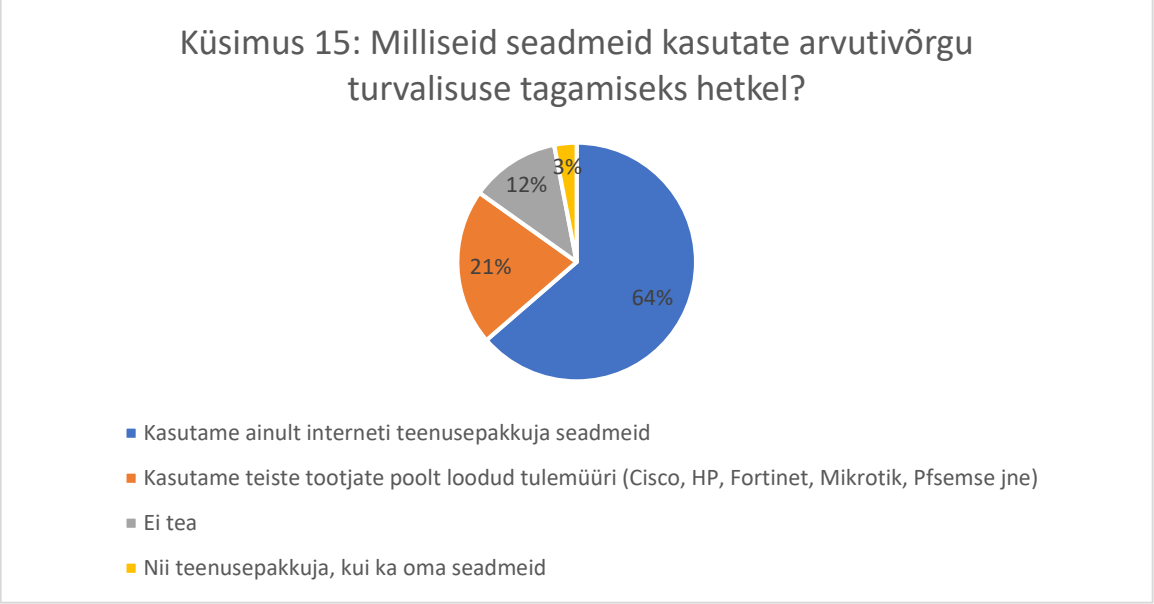
Kas teie arvates on praegune arvutivõrk turvaline?

Üle poole vastanutest arvas, et nende praegune arvutivõrk on turvaline, kuid nendest 13 kirikul pole eraldatud isegi külaliste võrku muust võrgust ning nende hulgast 12 kirikus tehakse kontoritööd. Külaliste võrku saab eraldada isegi teenusepakkuja seadmetest. Sellest vastusest saab teha järelduse, et isegi kõige lihtsam osa turvalisusest pole tagatud 13 kirikul, siis ei saa nende vastust lugeda õigeks.



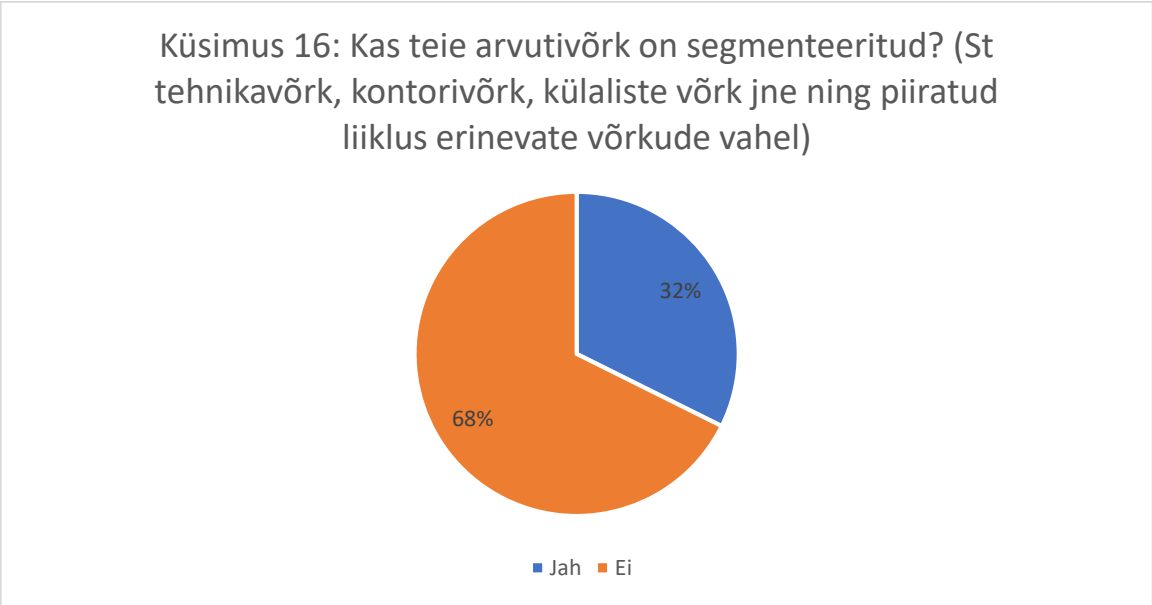
Milliseid seadmeid kasutate arvutivõrgu turvaliseks tagamiseks hetkel?

Vastanute seast 21 kirikut kasutab ainult teenusepakkuja seadmeid. Ainult 7 kirikul on eraldi tulemüür. Ning 4 vastanut ei tea üldse, mis seadmed neil on turvalisuse tagamiseks.



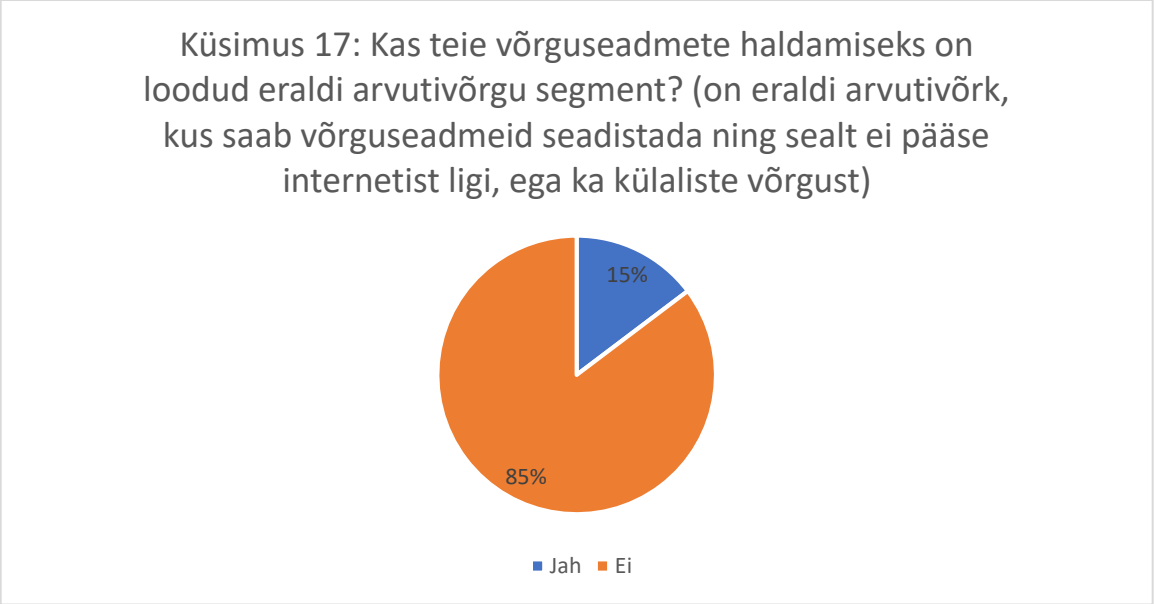
Kas teie arvutivõrk on segmenteeritud? (st tehnikavõrk, kontorivõrk, külaliste võrk jne ning piiratud liiklus erinevate võrkude vahel)

Üle poolte vastas, et arvutivõrk ei ole segmenteeritud, mille tagajärjel saab näiteks külaline ligi jagatud kaustadele või võtta helipuldi juhtimise üle. Üks „jah“ vastanu on vastanud 10. küsimusele, et nende külaliste wifi võrk ei ole eraldatud, seega võib eeldata, et pole ka teised võrgud segmenteeritud.



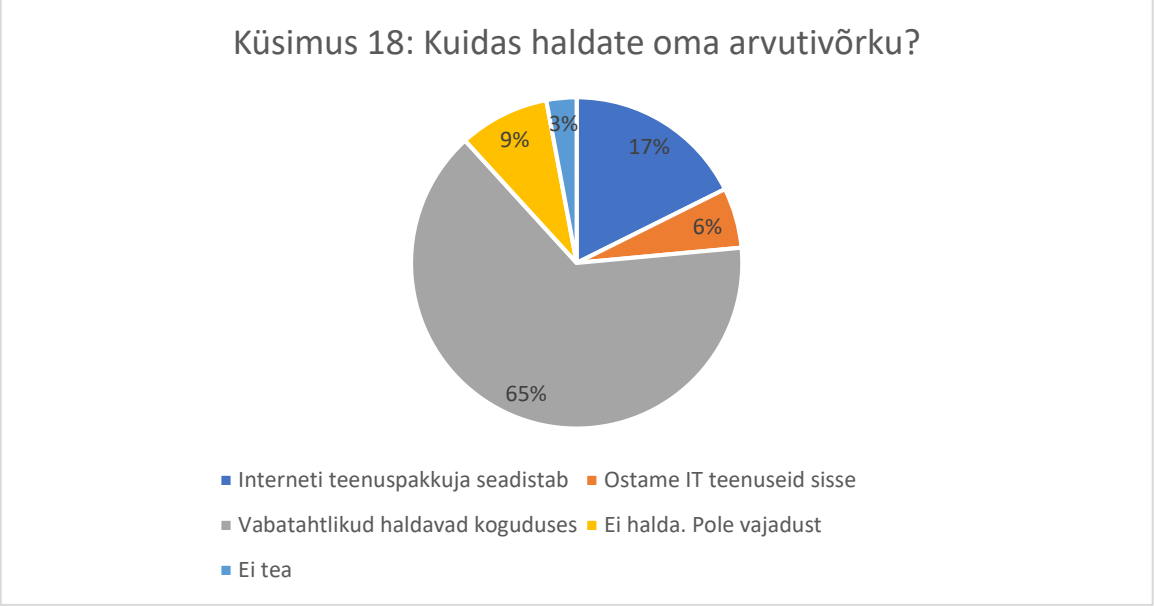
Kas teie võrguseadmete haldamiseks on loodud eraldi arvutivõrgu segment? (on eraldi arvutivõrk, kus saab võrguseadmeid seadistada ning sealt ei pääse internetist ligi, ega ka külaliste võrgust)

Vastanute seas „jah“ on vastanud ainult viis, et nende võrguseadmete haldamiseks on loodud eraldi segment. Kuid üks viiest vastas eelmisele küsimusele, et tema arvutivõrk ei ole segmenteeritud, samuti kasutab teenusepakkuja seadet. Seega võib teha järelduse, et ühel vastanul tegelikult ei ole loodud eraldi segmenti võrguseadmete haldamiseks.



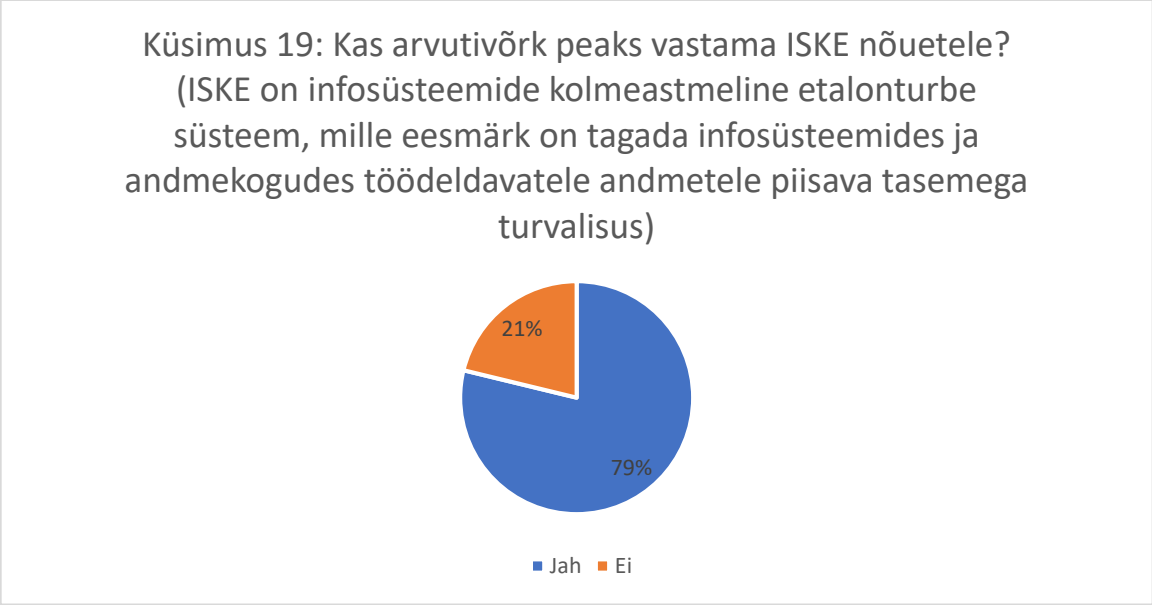
Kuidas haldate oma arvutivõrku?

Kolm vastanut ei näe vajadust võrku hallata. Ühel neist on väidetavalt teenusepakkujast erinev tulemüür. Kaks kogudust ostab võrguhaldusteenust sisse, kuid ühel neist pole eraldatud võrke, seega pole teenuse osutamisel tagatud elementaarne turvalisus. 12 vabatahtliku poolt hallatavat kiriku arvutivõrku pole segmenteeritud võrke.



Kas arvutivõrk peaks vastama ISKE nõuetele? (ISKE on infosüsteemide kolmeastmeline etalonturbe süsteem, mille eesmärk on tagada infosüsteemides ja andmekogudes töödeldavatele andmetele piisava tasemega turvalisus)

Enamus arvab, et usuühenduste arvutivõrgu turvalisuse loomiseks võiks võtta aluseks ISKE meetmed.



Küsimus 20: Kui soovite veel täpsustada oma arvutivõrku
Arvutivõrgu tänane nõrk koht on üks haldusisik. ISKE on kiriku arvutivõrgunõueteks päris suur tükk ja siinkohal olen ise lootnud, et koguduste liit aitaks juhtida koguduste arvutivõrkude turvalisust, mis puudutab just turbejuhte ja turbeplaanide tegemist. Tihti ei ole kogudustel selleks ressursse ja jõudu ja ka teadmisi.
Hetkel statsionaarne arvutivõrk puudub, aeg-ajalt kasutame LTE-ühendusega (USB-ühendusega läbi telefoni modemi) wifi ruuterit.
Vajame IT-oskustega inimesi.
Pole kompetentne detailides, kuna arvutivõrk jms kuulub kaastöölise ülesannete hulka. Tean teenusepakkujat, ja et meil on wifi ruuter, mille lülitame vajadusel sisse, ja parooli on seni jagatud ainult neile, kellel on seda sihtotstarbeliselt koguduse tööks vaja, sh koguduse külalistele kaasateenimiseks.

Kuna teenistused toimivad koolihoones, siis vastutab interneti eest ka kool. Kogudusel on lubatud kasutada kooli internetti (nii avalikku kui ka kinnist).
Wifi ruuter on lihtsalt kontoris. Töötab nagu kodune wifi. Midagi erilist juures pole. Tegelikult väga täpselt neid detaile ei tea selle kohta.
Hetkel 1 arvuti, mis on mõeldud laulusõnade kuvamiseks. Koguduse muid asju teeme kodus.