Tartu Rakenduslik Kolledž

IKT-osakond

ISO21

Martin Tambets

VÕRGUPROJEKT

Projekt

Juhendajad: Einar Mägi
Timo Puistaja
Liis Karilaid

Tartu 2022

SISUKORD

SISSEJUHATUS

Eesti Toode OÜ on ettevõte, kus töötab 150 töötajat ning on suurenemas, seoses kolimisega uutesse kontoritesse on vaja abi võrguprojekti loomisega. Ettevõte seadis projekti loojale põhilistemadest eesmärkidest koostada võrguplaan ning ehitada toimiv võrk. Projekti juures tuli kirjeldada erinevaid lahendusi alates kaabeldustöödest kuni seadmete valimise ja nende konfigureerimiseni välja.

1 PROJEKTI KIRJELDUS

Eesti Toode OÜ soov oli, et igas kontoris oleks samanimeline ja turvaline wifi võrk nii omadele töötajatele ning külalistele, viimane peab olema eraldatud ettevõte sisevõrgust turvalisuse huvides. Projektiga sooviti ka eelarvet ning riskianalüüsi. Lisaks sooviti, et loodaval süsteemil oleks monitooringulahendus koos teavitustega, avalikud serverid pidi olema eraldi võrkudes, et oleksid avalikult kätte saadavad ning töötajate jaoks vpn ühenduse võimekus.

2 VÕRGUSEADMED JA FÜÜSILINE KAABEL

2.1 Valitud seadmed

Ruuterite valikuks osutus Allied Telesis AR4050S ning AR2010V. Antud tootja seadmed vastasid ettevõtte poolt pandud kriteeriumitele, kuna ühes seadmes on võimekus toimida nii ruuteri kui tulemüürina, lisaks pakub tunneli ühenduse ja IPSec võimekust. Lisaks on võimalik antud seadmedes konfigureerida DHCP kui ka DMZ võrku.

Kommutaatoriteks sai valitud Allied Telesis AT-GS950 8-48 pordised 1U seadmed. Kuna erinevates harukontorites ei ole sama kogus lõppkasutajaid ning lõpp seadmeid siis on võimalik kasutada seadet millel on vastavalt vajadusele kas 8, 24 või 48 porti. Seadme valikul osutus määravaks energia kulu mida üks seade kasutab. Kuna kõik seadmed on ühe ja sama tootja omad, Allied Telesis, siis see lihtsustab seadmete konfigureerimist ning vähendab riske, et seadmed omavahelisel suhtlusel võib tekkida probleeme.

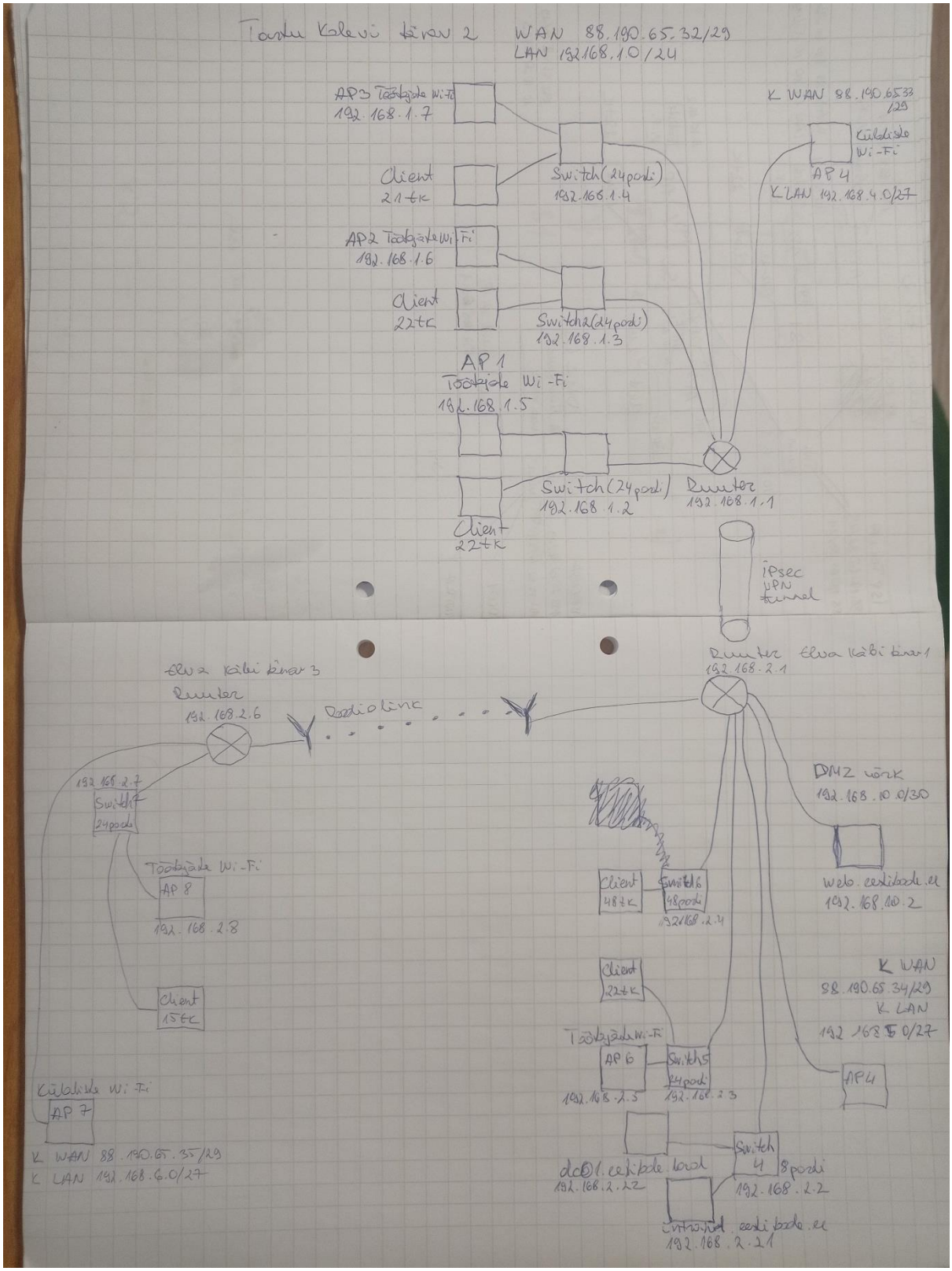
Pääsupunktide puhul valisin seadmed taaskord tootjalt Allied Telesis. Nende seade TQ5403. Seade on võimalik ühendada POE ühendusse ning seade on võimeline korraga jagama välja kahte 5GHz võrku. Mõeldes tulevikule siis on võimalik teha kaks erinevat töötajate võrku, näiteks üks võrk ettevõtte klient seadmetele ning teine töötajatele isiklikele seadmetele.

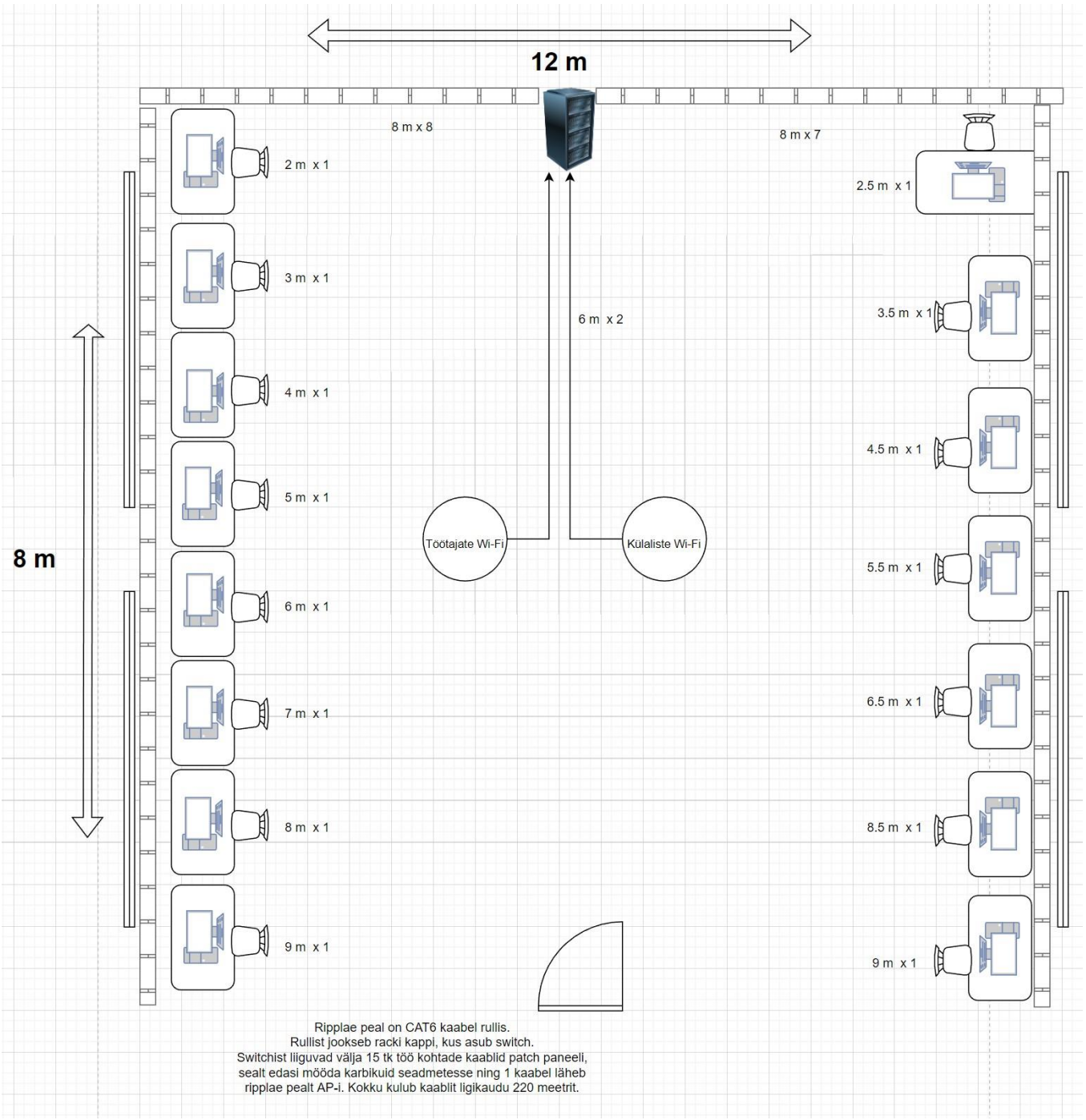
2.2 Hinnakalkulatsiooni tabel

Seadmed	Kogus	Hind	Hind kokku
AT-AR4050S-50 (ruuter)	2	915.52	1831.04
AT-AR4050S-50 racki kinnitus	2	167.99	335.98
AT-GS950/48-50 (switch)	1	815.89	815.89
AT-AR2010V-50 (ruuter)	1	416.4	416.4
AT-GS950/24-50 (switch)	5	499.41	2497.05
AT-GS950/8-50 (switch)	1	182.46	182.46
AT TQ5403 (access point)	8	700.97	5607.76
Paigaldus tarvikud			
Keerpaarkaabel Cat6, 305m, rull	1	67.99	67.99
Võrgukaabel Cat6 UTP 1.0m	15	1.3	19.5
Modularpesa RJ45 Cat6	34	2	68
Installatsioonirenn 2000 m x 60 mm x 40 mm	30	7.29	218.7
Kinnitusvahendid	1	20	20
		Kokku	12080.77
Paigaldustööd			
Käbi 3 tööruumi kaabeldus	17	20	340
Käbi 3 võrguseadmete paigaldus ja konfigureerimine	5	50	250
Käbi tn 1 võrguseadmete paigaldus ja konfigureerimine	8	50	400
Käbi tn 1 serverite paigaldus ja konfigureerimine	6	50	300
Kalevi tn 1 võrguseadmete paigaldus ja kongfigureerimine	9	50	450
		Kokku	1740
		Seadmed, paigaldus ja konfigureerimine kokku	13820.77

3 VÕRGU SEADISTAMINE, MONITOORING JA ANALÜÜS

3.1 Planeerimine





Ripplae peal on CAT6 kaabel rullis.
Rullist jookseb racki kappi, kus asub switch.
Switchist liiguvad välja 15 tk töö kohtade kaablid patch paneeli,
sealt edasi mööda karbikuid seadmetesse ning 1 kaabel läheb
ripplae pealt AP-i. Kokku kulub kaablit ligikaudu 220 meetrit.

3.2 Virtuaalne seadistamine

IP aadresside tabel

IP aadresside tabelid	
Võrk 192.168.1.0/24	
Võrguseadmed	192.168.1.1 - 192.168.1.20
Ruuter AT-AR4050S	192.168.1.1
Switchid 1-3	192.168.1.2 - 192.168.1.4
Wi-Fi AP-d 3 tk	192.168.1.5 - 192.168.1.7
DHCP Pool	192.168.1.21 - 192.168.1.90
VPN Pool	192.168.1.91 - 192.168.1.180
Töötajate Wi-Fi võrk	192.168.1.181 - 192.168.1.254
Võrk 192.168.2.0/23	
Võrguseadmed	192.168.2.1 - 192.168.2.20
Ruuter AT-AR4050S	192.168.2.1
Switchid 4-6	192.168.2.2 - 192.168.2.4
Wi-Fi AP	192.168.2.5
Ruuter AT-AR2010V	192.168.2.6
Switch 7	192.168.2.7
Wi-Fi AP	192.168.2.8
Serverid 192.168.2.21 - 192.168.2.30	
DC01	192.168.2.21
INTRANET	192.168.2.22
DHCP Pool	192.168.2.31 - 192.168.2.120
VPN Pool	192.168.2.121 - 192.168.2.210
Töötajate Wi-Fi võrk	192.168.3.1 - 192.168.3.254
Tagavara	192.168.2.210 - 192.168.2.254
DMZ Võrk 192.168.10.0/30	
Ruuter AT-AR4050S VLAN 10	192.168.10.1
Serverid	192.168.10.2-192.168.10.5
web.eestitoode.ee	192.168.10.2
Külaliste Wi-Fi Pool	
Wi-Fi Pool 1	192.168.4.1 - 192.168.4.254
Wi-Fi Pool 2	192.168.5.1 - 192.168.5.254
Wi-Fi Pool 3	192.168.6.1 - 192.168.6.254

Wan ühendused

WAN ühendust, ehk wide area network (laivõrk) avaliku ühendust kasutavad ruuterit selleks, et omavahel suhelda. Ruuteri saab mõtteliselt jagada pooleks. Kus üks pool suhtleb avaliku interneti ja teine pool sisevõrguga. Antud projekti puhul kasutusele võetav ruuter on võimeline korraga ühenduma kahte erineva avaliku interneti aadressi ning pakkudes seda teenust edasi sisevõrku.

LAN ühendused

LAN ühenduse, ehk local area network (sisevõrk) jaoks luuakse erinevad sisevõrgu aadressid, nendest 2 põhilisemat on Tartu Kalevi tänav 2 192.168.1.0 ning Elva Käbi tänav 1 192.168.2.0. Ruuterid antud võrkudes asuvad aadressidel 192.168.1.1 ning 192.169.2.1. Lisaks saab iga seade (kommutaator, server, pääsupunkt ja klient seade) endale oma IP aadressi.

IPsec VPN tunnel

Kahe suure harukontori, Tartu Kalevi tänav 2 ja Elva Käbi tänav 1 vahel on vaja luua selline ühendus mis oleks turvaline andmete edastamiseks avalikus interneti võrgus. Selleks võetakse kasutusele IPSec VPN (turvaline virtuaalne privaatvõrk) ühendus. Ühes ruuterist saadetakse välja krüpteeritud andmesidepaketid ning teises ruuteris võetakse need vastu ja dekrüpteeritakse. Selleks sai valitud ühe sama tootja identsed seadmed mis võimaldavad sellist ühenduse loomist.

Tulemüüri reeglid

Turvaliseks võrguühenduseks ning selleks, et seadmed saaks suhelda välisvõrguga on vaja seadistada ruuteris tulemüüri reeglid. Antud reeglid määravad ära tegevused kuidas tulemüüris peaks toimuma tegevus. IPSEC VPN tunneli jaoks on vaja lubada pordid 500 ja 4500. Intraweb jaoks on vaja lubada pordid 80 ning 443.

3.3 Monitooring

Kasutusele võetud Allied Telesis seadmed toetavad ettevõtte enda monitooringu süsteemi nimega Vista Manager EX. Antud programmis on võimalik jälgida ja monitoorida ettevõtte võrku. Muuta vajadusel seadistusi ning administraatorid saavad seadistada programmi saatma vajadusel teavitusi.

3.4 Riskianalüüs

3.4.1 Varad

	Varad	Kirjeldus
1	Ruuterid	Võrgu ülesehitamiseks ning haldamiseks
2	Kommutaatorid	Jagavad võrku klient seadmetele
3	Pääsupunktid	Laiendavad olemasolevat wifi võrku
4	Serverid	Hoiustavad andmeid, salvestuspinda, veebilehti
5	Klient seadmed	Lõppseadmed, kasutatakse ettevõtte töö ülesannete täitmiseks
6	Serveri kapp	Hoiustab erinevaid võrgu seadmeid

3.4.2 ohud

	Ohud	Ohud Ohu kirjeldus
1	Kurivara	Kurivaraga ligipääs süsteemi
2	DDoS	Ettevõtte serverile/veebilehe tehakse rünnak
3	Voolukatkestus	Käbi tänav 1 puudub elektriühendus
4	Ligipääsu süsteem	Kontorisse pääseb sisse isik, kes ei peaks seal olema

3.4.3 Haavatavused

	Haavatavus	Haavatus Haavatavuse kirjeldus
1	Uuendused	Seadmel ei toimu uuendamist, seade muutub haavataks rünnakutele
2	Töötaja	Arvuti juurest lahkumisel ei logita välja, igaüks pääseb seadmesse ligi
3	Seade	Seadistamisel jäetakse tehase seaded muutmata
4	Backup	Kui ei toimu backupi siis võivad osad ettevõtte andmed kaduma minna

3.4.4 Riskimaatriks

Riski maatriks					
		Uuendused	Töötaja	Seade	Backup
		H01	H02	H03	H04
Kurivara	O01	R0101	R0102	R0103	R0104
DDoS	O02	R0201	X	X	X
Voolukatkestus	O03	X	X	X	R0304
Ligipääsu süsteem	O04	X	R0402	R0403	R0404

3.4.5 Turvameetmed

Riski id	Riski tase	Riski vastus	Riski vastutuse omanik
R0101	KESKMINE	Seadmete uuendamine	Süsteemiadministraator
R0102	KÕRGE	Viia läbi töötajatele küberhügieeni koolitus	IT-juht
R0103	KESKMINE	Seadistamisel kasutada uusi kasutajaid ning paroole	Süsteemiadministraator
R0104	KESKMINE	Seadistada tulemüüri reeglid ning võimalusel mitu erinevat seadet kuhu toimub backup	Süsteemiadministraator
R0201	KÕRGE	Seadmete uuendamine	Süsteemiadministraator
R0304	MADAL	Kasutada UPSi	IT juht
R0402	KÕRGE	Logida välja arvutist	IT juht
R0403	KÕRGE	Uuendada sisselogimisandmeid	Süsteemiadministraator
R0404	KESKMINE	Kasutada biomeetrilisi sissepääsu süsteemi	Haldus juht

3.4.6 Riski lahti seletus

Risk id	Ohu id	id	riski nimetus	Tõenäosus	Mõju	riski tase	riski indikaator
R0101	O01	H01	Tulemüür ei tööta ja kurivaraga võimalik ligipääs süsteemi	1	9	keskmine	Seadme üle võetakse kontroll/paigaldatakse tagataustal töötav pahavara mis kogub andmeid
R0102	O01	H02	Arvuti juurest lahkumisel ei logita välja.	3	1	Kõrge	Kustutatud failid. Kõvakettad on krüpteeritud.
R0103	O01	H03	Seadistamisel ei muudeta tehaseseadeid sisselogimiseks	1	6	madal	Tehase seadede andmed on avalikult kätte saadavad internetis, tänu sellele teades mis seadme tegu on võimalik väga lihtsalt seadmesse sisse logida.
R0104	O01	H04	Kurivara võib backup välja lülitada	2	9	madal	Andmeid ei varundata ning selle tulemusena on väga tugevalt häiritud ettevõtte töö.
R0201	O02	H01	Uuendama seade ei ole võimeline vastu pidama DDoS rünnakule	1	5	madal	Seade/veebileht koormatakse nakatunud seadmete päringutega üle ning lakkab töötamast.
R0304	O03	H04	Serveriruumil kaob elektritoide.	1	9	Kõrge	Käbi tänav ja Käbi tänav 3 kontorites ei ole võimalik tööd teha ning ettevõtte veebileht ei tööta.
R0402	O04	H02	Ettevõtte väline isik saab kasutada seadet millest pole välja logitud	2	6	madal	Saadetakse seadme kasutaja nime alt viirusega emaile ning paigaldatakse pahavara.
R0403	O04	H03	Serveriruumi pääsedes on võimalik sisse logida erinevatesse võrguseadmetesse	1	9	kõrge	Seadme conf on muudetud ning seadmesse ei pääse enam kasutaja sisse.
R0404	O04	H04	Kurivara võib backup välja lülitada	4	3	kõrge	Andmeid ei varundata ning selle tulemusena on väga tugevalt häiritud ettevõtte töö.

4 Seire

Seireks kasutatakse Allied Telesis enda tarkvara Vista Manager EX. Selleks on vaja ühte virtuaalmasinat kuhu antud tarkvara paigaldatakse, peale mida tarkvara hakkab tuvastama võrku. Hilisemalt on võimalik tarkvara seadistada saatma automaat email teateid.

5 Kokkuvõte

Eesti Toode OÜ on 150 töötajaga ettevõte mis kasvades vajab suuremaid kontoripindu ning tulenevalt uutest kontoritest soovisid saada võrguprojekti nullist valmis lahendusena.

Ettevõte esitas omapoolsed soovid, millest mõned olid järgnevad:

- Igas kontoris peab olema samanimeline ja turvaline wifi nii töötajatele kui ka külalistele.
- Projekt on selgelt dokumenteeritud ja visualiseeritud.
- Projektiga esitlemisega kaasneb eelarve.
- Loodavale võrgule on tehtud riskianalüüs.
- Võrgu jaoks on lahendatud monitooringusüsteem koos erinevate teavitus võimalustega.
- Veebiserverid on avalikus võrgus kõigile kätte saadavad.
- Töötajatel on võimalik väljaspool kontorist turvaliselt töö keskkonda sisse logida.

Loodava projekti tarbeks tuli kõigepealt visualiseerida erinevate vahendite abil loodav võrk ning sealt edasi sai hakata planeerima võrgu ehitust. Lisaks tuli luua visuaalne kaabeldus plaan ühele kolmest kontoritest.
Alustati ip aadresside tabeli loomisest mille tulemusel tekkis arusaam võrgu suurusest ning milliseid seadmeid võib vaja minna ning mis koguses.
Seadmete valikul tehti otsus, et kõik seadmed tulevad ühe ja sama tootja poolt, mis lihtsustab võrgu ülesehitust ning seadmete omavahelist suhtlust ning vähendab tõrgete ning probleemide tekkimise võimalusi. Lisaks pakub otsus võimalust kasutada tootja poolset monitooringu lahendust mis omakorda vähendab veel riske ning tõstab võrgu töökindlust.
Seadmete valikule järgnes nende seadistamine ning erinevate tehniliste lahenduse loomine nende omavaheliseks ühendamiseks.
Kõige lõpus tuli teha tervele võrgule ning ettevõtte it infrastruktuurile riskianalüüs, kus käsitleti erinevaid probleeme ning olukordi mis võivad juhtuda ettevõtte igapäeva töös.

Projekti looja hindab ise projekti edukaks, kuna tegemist on esimest korda sellise loodava ülesandega ning andis väga hea ülevaate ja kogemuse. Lisaks andis sellise projekti loomine hea tagasiside ning ülevaate kuidas tulevikus samasugust ülesannet lahendades saaks teha erinevaid ülesandeid teisti.

6 Summary

Eesti Toode OÜ is a company with 150 employees that needs larger office spaces and as a result of the new offices, they wanted to get a network project as a ready-made solution from scratch.

The company presented its own requests, some of which were as follows:
- Every office must have the same name and secure wifi for both employees and guests.
- The project is clearly documented and visualized.
- A risk analysis has been performed on the network to be created.
- A monitoring system with various notification options has been solved for the network.
- Employees can securely log in to the work environment outside the office.

For the purpose of the project to be created, it was first necessary to visualize the network to be created with the help of various tools, and from there, it was possible to start planning the construction of the network. In addition, a visual cabling plan had to be created for one of the three offices.
Creation started with ip ip addresses table, which resulted in an understanding of the size of the network and which devices might be needed and in what quantity.
When choosing the devices, it was decided that all devices must come from the same manufacturer, which simplifies the network structure and the communication between the devices and reduces the chances of errors and problems. In addition, the decision offers the opportunity to use the manufacturer's monitoring solution, which in turn further reduces risks and increases network reliability.
The selection of devices was followed by their configuration and the creation of various technical solutions for connecting them together.
At the very end, a risk analysis had to be done for the entire network and the company's IT infrastructure, where various problems and situations that could happen in the company's daily work were displayed.

The creator of the project himself evaluates the project as a success, as it is the first time such a task has been created and it gave a very good overview, experience and feedback how tasks could be done differently in the future when solving the same kind tasks.