Raziskovalna naloga o lokalnem omrežju

Mentor: Boštjan Lubej, dipl. inž.

Šola: ŠCC, Srednja šola za kemijo, elektrotehniko in računalništvo

Avtorji: Luka Zabav, Nik Huzjak, Luka Posteržin

Datum: Februar, 2021

IZJAVA*

Mentor BOŠTJAN LUBEJ v skladu z 20. členom Pravilnika o organizaciji mladinske raziskovalne dejavnosti »Mladi za Celje« Mestne občine Celje, zagotavljam, da je v raziskovalni nalogi z naslovom Lokalno omrežje, katere avtorica je/so Luka Žabav, Nik Huzjak, Luka Posteršin

- besedilo v tiskani in elektronski obliki istovetno,
- pri raziskovanju uporabljeno gradivo navedeno v seznamu uporabljene literature,
- da je za objavo fotografij v nalogi pridobljeno avtorjevo dovoljenje in je hranjeno v šolskem arhivu,
- da sme Osrednja knjižnica Celje objaviti raziskovalno nalogo v polnem besedilu na knjižničnih portalih z navedbo, da je raziskovalna naloga nastala v okviru projekta Mladi za Celje,
- da je raziskovalno nalogo dovoljeno uporabiti za izobraževalne in raziskovalne namene s povzemanjem misli, idej, konceptov oziroma besedil iz naloge ob upoštevanju avtorstva in korektnem citiranju,
- da smo seznanjeni z razpisni pogoji projekta Mladi za Celje.

Celje, 12.4. 2022

ŠOLSKI CENTER CELJE SREDNJA ŠOLA ZA KEMIJO, ELEKTROTEHNIKO IN RAČUNALNIŠTVO 1 CELJE, Pot na Lavo 22

žig šole

Podpis mentorja

Podpis odgovorne osebe

*

POJASNILO

V skladu z 20. členom Pravilnika raziskovalne dejavnosti »Mladi za Celje« Mestne občine Celje je potrebno podpisano izjavo mentorja (-ice) in odgovorne osebe šole vključiti v izvod za knjižnico, dovoljenje za objavo avtorja (-ice) fotografskega gradiva, katerega ni avtor (-ica) raziskovalne naloge, pa hrani šola v svojem arhivu.

Kazalo

Vsebina

Kazalo slik

Kazalo grafov

Uvod

V tej raziskovalni nalogi, bomo raziskali ter predstavili probleme, ki jih lahko srečamo računalničarji pri vzpostavitvi lokalnega omrežja z javnim. Predstavili bomo katere naprave bomo uporabili, kako jih nastavimo ter morebitne pomanjkljivosti, ki bi jih še lahko izboljšali z kakšno drugo oz. boljšo napravo. Predstavili bomo izsledke naše ankete, kjer bomo ljudi povprašali kako se njim zdi takšno omrežje, ter le bi oni kaj dodali oziroma spremenili. Z grafičnim gradivom bomo prikazali kaj smo nastavili, da smo se povezali na javno omrežje, ter tudi kako smo zaščitili naše omrežje pred nepooblaščenim dostopom.

Opredelitev problema

V naši raziskovalni nalogi smo raziskali probleme pri varnosti v lokalnem omrežju in tudi probleme, ki jih lahko srečamo pri postavitvi takega omrežja. Pri izdelovanju takega omrežja in pravilno nastavljanje vseh naprav smo tudi sami še bolj neizkušeni, zato smo si kar veliko pomagali z internetom, da smo lahko lažje razumeli, kje lahko pride do problema in kako se mu izogniti oziroma ga rešiti.

V današnjem, zelo tehnološko razvitem svetu, je teh omrežji že zelo veliko in so izvedena na zelo veliko različnih načinov z opremo od različnih proizvajalcev. Mi smo se odločili za opremo, ki v Evropi še ni toliko razvita in poznana, a je uporabljena na drugih koncih sveta.

Metode raziskovanja

Za raziskovalno metodo smo uporabili metodo spletnega anektiranja, pri čemer je sodelovalo deset manjših podjetjih, dve večje, ter dvajset posameznikov, nekateri izmed teh so bili tudi zdravstveni domovi, ki že uporabljajo to opremo. Osredotočili smo se na ljudi oziroma podjetja, ki so že seznanjeni z tovrstnim omrežjem in napravam.

Hipoteze in cilji

Cilj raziskovalne naloge je bil kako učinkovito je naše omrežje, kako dobro je izvedeno, kako hitro lahko odpravimo napake.

Postavili smo si naslednje hipoteze:

1. Večina strank je zadovoljna z tem načinom omrežja
2. Napake hitro odpravimo
3. Po večini do napak ne pride

Lokalno omrežje

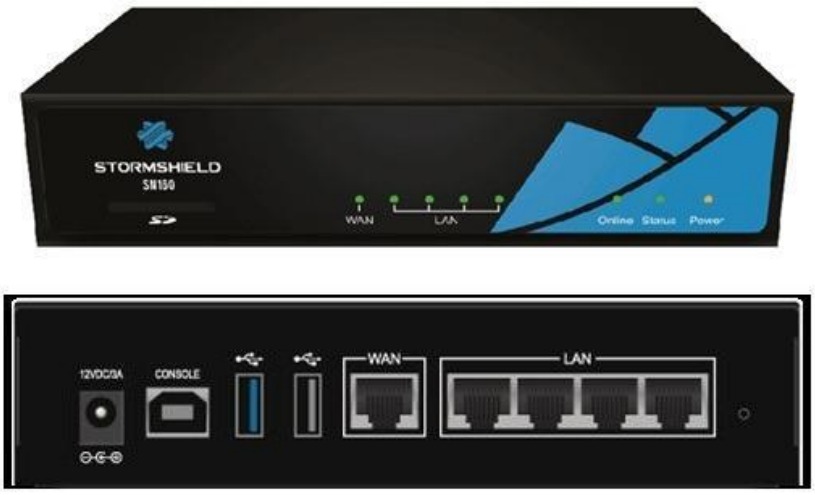
Da bi lahko razumeli kaj smo sploh naredili moramo poznati dva pojma – lokalno omrežje in javno omrežje. Lokalno omrežje je omrežje znotraj nekega podjetja ali omrežje ki ga imamo doma, ki se preko določene omrežne naprave poveže v javno omrežje, ki pa predstavlja vse uporabnike po svetu kot celoto, ki lahko komunicirajo drug z drugim.

Izbira opreme

Za opremo smo se odločili, ker jo že poznamo in nam je bila na voljo. Uporabili smo požarni zid podjetja Stormshield, ki je Evropsko priznano podjetje za izdelovanje požarnih zidov, stikalo Juniper, ki je eden vodilnih podjetij v IT okolju v Ameriki, ter Unifi dostopno točko, podjetja Ubiquti, ki je prav tako zelo poznana v Ameriki.

Požarni zid

V tej nalogi smo uporabili požarni zid Stormshield SN160, ki ima 5 fizičnih priklopov, eden za povezavo z javnim omrežjem, ter ostale 4 za povezavo z lokalnim omrežjem. Na požarnem zidu smo ustvarili 3 uporabnike, da ima vsak izmed nas dostop do požarnega zidu. Prav tako smo nastavili posebna vrata, na katerem se bo požarni zid odzval.



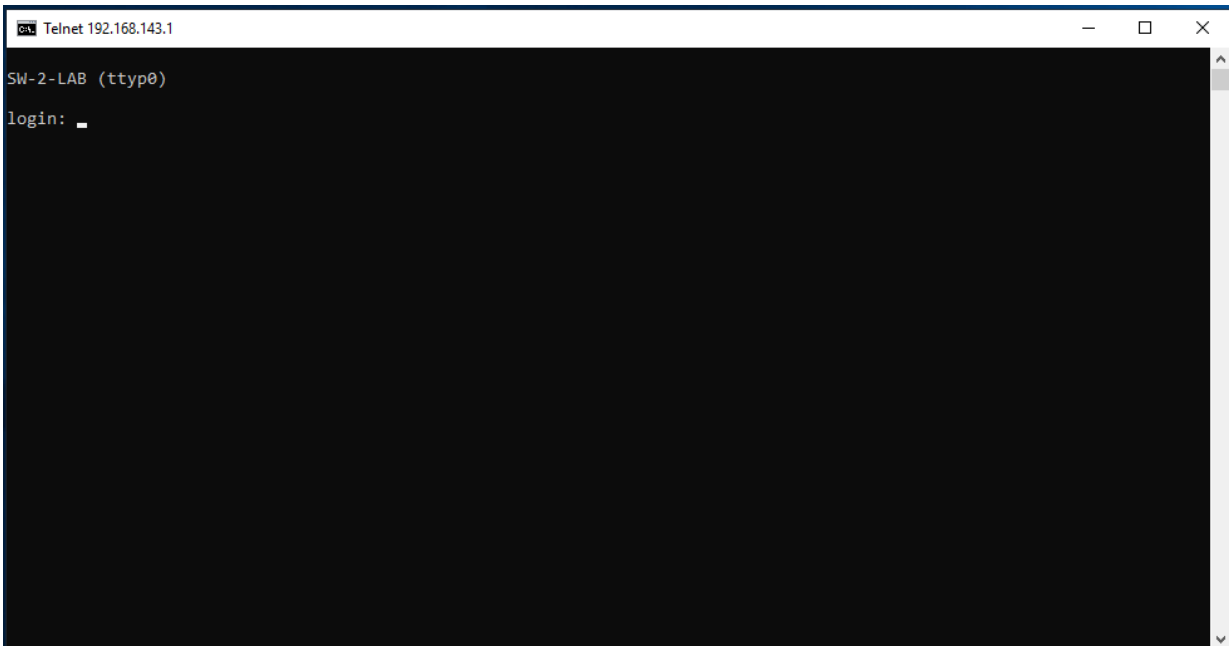
Slika 1 - Požarni zid

Slika 2 - Požarni zid prijavno okno

Stikalo

Pri tej nalogi smo uporabili stikalo Juniper EX2200 PoE (ang. Power over Ethernet). Tudi na njemu smo nastavili tri uporabnike, ter glavnemu uporabniku »root« nastavili geslo. Na njem smo definirali navidezna lokalna omrežja (VLAN), ter smo vsak priključek določili omrežju. Naredili smo 2 omrežja z ločenimi oznakami (TAG-i), ki pa delujeta kot ločena omrežja in prehod iz enega v drugega ni mogoč, ter smo tako poskrbeli za varnost službenega omrežja, z povezavo omrežja za goste. Stikalo ima 24 priključkov za RJ-45, ter 4 priključke za optično povezavo (single mode). Optične priključke bi lahko uporabili za povezavo dveh stikal med seboj.

Slika 3 - Slika Juniper stikala

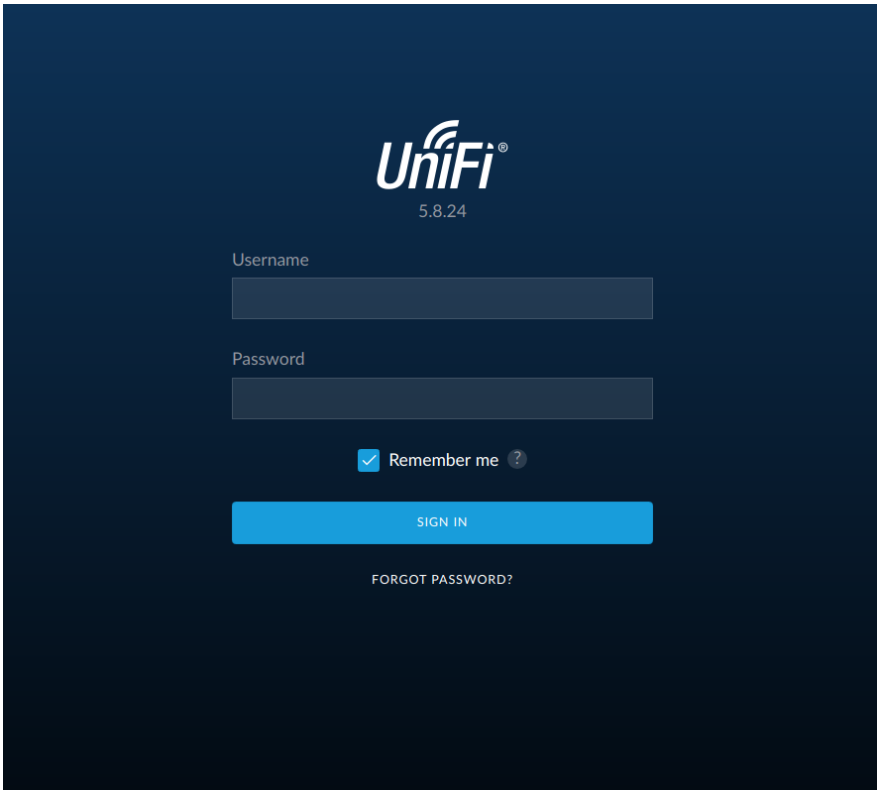


Slika 4 - Prijavno okno za stikalo

WiFi točka

Pri nalogi smo uporabili tudi WiFi točko Unifi Ap Ac Lr. Na stikalu smo določili en priklop, da ima dostop do obeh omrežji, ter na ta priklop povezali WiFi točko, na kateri smo potem naredili 2 brezžična omrežja, ter nastavili omrežje za goste, ter za nas (administratorje).

Slika 5 - Slika WiFi točke



Slika 6 - Prijavno okno na WiFi točki

Priprava in izdelava

Najprej smo se vsi pozanimali kako deluje vsaka naprava in kaj moramo na njej storiti, da bo vse delovalo kot smo si zamislili, ter potem začeli z izdelovanjem omrežja »na papir«. Narisali smo si skico ter zraven pripisali vse pomembne podatke za IP naslove, da se nam kasneje nebi kaj zamešalo, ter potem nadaljevali z poimenovanjem omrežji in njunimi oznakami. Ko smo imeli vse skicirano, smo morali to realizirati na napravah, ki smo jih med seboj povezali z UTP kabli. Vsako napravo smo skonfigurirali in postavili na mizo, da smo lahko preverili ustrezno delovanje vsake naprave posebej, ter odpravili napake, če je do njih prišlo.

Namen raziskovalne naloge

V tej raziskovalni nalogi bomo predstavili, kako se to omrežje postavi, kakšne so njegove pomanjkljivosti, ter predstavili bomo rezultate naše raziskave, ki smo jo naredili z pomočjo spletne ankete 1KA. Osredotočili se bomo na probleme pri povezovanju lokalnega omrežja z javnim in kako najbolje zavarovati naše omrežje. Primerjali ga bomo tudi z katerimi drugimi načini vzpostavitve omrežja ter predstavili naše ugotovitve. Našo anketo smo poslali tudi par omrežjih, da smo videli, kaj bi oni naredili drugače in če bi še kaj spremenili.

Nastavitve požarnega zidu

Pri požarnem zidu smo si pomagali z uradno dokumentacijo od samega podjetja, ter ker bi ta naj filtriral promet, kaj lahko spušča skozi in kaj ne, smo morali biti pri nastavljanju zelo pozorni in dosledni. Na začetku smo dovolili sprejemanje vseh paketkov, ki so tipa ICMP (za preverjanje, če je povezava do požarnega zidu delujoča), ter takoj za tem nastavili pravilo, da ves drug promet blokira. Po nastavitvi obeh omrežji na požarnem zidu, smo naredili pravilo, ki dovoli samo tema omrežjema dostop izven omrežja, in da se lahko samo na paketke poslane iz našega omrežja odgovarja. Ker ta požarni zid bere pravila od zgoraj navzdol, smo ti pravili postavili pred pravilo »blokiraj vse«. Pri nastavljanju varnostne politike smo odprli samo 3 vrata, ki so potrebna za povezavo v omrežje (http: 80; https: 443; DNS:53;). Po potrebi bi odprli še druga vrata.

Po nastavitvi varnostne politike, smo nastavili NAT(ang. Network Address Translation), ki v paketke namenjene v javno omrežje namesto lokalnega IP naslova vpiše javni naslov, ter pri odgovoru iz spletnih strani naredi obratno kot pa je naredil pri pošiljanju izven lokalnega omrežja. Ko smo to nastavili, smo zdefinirali priklop WAN(ang. Wide Area Network) da je to privzeti prihod in da naj na ta priklop pošlje vse paketke, ki so namenjeni javnemu omrežju.

Nastavitve stikala

Po nastavitvi 3 uporabnikov, smo ustvarili 2 različna lokalna omrežja (INT za zaposlene, in GST za goste v omrežju. Vsakemu smo določili svoj TAG(oznako paketkov, po kateri bo stikalo vedelo iz katerega omrežja je paketek prišel in kaj z njim narediti). Pri določitvi TAG-ov smo morali biti pazljivi, da smo dali različne oznake in da so smiselne (0 – neoznačen paketek, in ker je brez oznake ga bo naše stikalo zavrglo). Tako smo nastavili omrežju INT TAG 10, ter GST omrežju TAG 20. Ko smo imeli nastavljena omrežja, smo morali nastaviti še lokalne naslove omrežja in sicer INT 192.160.1.0/24 ter GST 192.168.2.0/24. Z tem smo dodelili IP naslove, ki pripadajo določenemu omrežju in bo z temi naslovi naše stikalo usmerjalo promet. Prav tako smo morali nastaviti IP naslov našemu stikalu, ki pa je po navadi takoj naslednji za privzetim naslovom prehoda. Naše stikalo je prav tako nosilec DHCP strežnika za dodeljevanje IP naslovov službenim uporabnikom. Ko smo nastavili DHCP strežnike ter oba omrežja smo definirali vsak priklop v katero omrežje spada in ali je Trunk ali Access. Trunk pomeni da je lahko član večjih omrežjih, Access pa da lahko pripada samo enemu in tako smo določili, da so vsi priklopi Access razen zadnjih dveh (22, 23), ki pa sta namenjena za povezavo požarnega zidu in WiFi točke, ter morata biti člana obeh omrežjih.

Nastavitve WiFi točke

Na WiFi točki smo prav tako morali nastaviti ti dve omrežji, ter nastaviti IP naslov točke, da smo se lahko na njo povezali preko grafičnega vmesnika. Ko smo ustvarili ti dve omrežji in smo jima prav tako določili iste TAG-e kot na stikalu in požarnem zidu smo morali nastaviti gesli za vsako brezžično omrežje posebej, ter ga povedati uslužbencem, da so se lahko nanj povezali.

Prednosti našega omrežja

Naše omrežje je zaradi specifičnosti primerno za manjša omrežja in zaradi lahke razširitve in povečave omrežja hitro razširljivo. Zaradi uporabljene opreme je naše omrežje tudi zelo hitro in je majhna verjetnost, da bi prišlo do tako imenovanega zabitja omrežja, in da bi naše omrežje počakalo in bi potrebovalo ponovni zagon vseh naprav. Z omogočenim oddaljenim dostopom lahko omogočimo našim strankam delo od doma. Prav tako lahko na napravah naredimo filtriranje MAC naslovov, in z tem še povečamo varnost našega omrežja. Z zunanjim dostopom smo si prav tako omogočili da se ne rabimo voziti od strank do strank, ampak lahko na daljavo rešimo morebitne težave. Izdelava našega omrežja je zelo preprosta in hitra. Če pride do izpada električnega omrežja, si naše naprave shranijo nastavitve in se ob ponovni vzpostavitvi električnega toka postavijo same in naše omrežje deluje naprej. Ker uporabljamo PoE tehnologijo, bi bila to velika prednost pri vzpostavitvi brezžične tehnologije, saj imamo točko, ki prav tako podpira tehnologijo PoE in bi se z tem izognili nepotrebnih kablov za napajanje takšnih naprav.

Slabosti našega omrežja

Ker smo izbrali malce dražje naprave, je takšno omrežje cenovno dražje kot pa nekatera. Ker smo se osredotočili na manjša oz. srednje velika omrežja, naše omrežje nebi bilo primerno za večja omrežja. Ker smo naredili 2 DHCP strežnika, lahko pride do zmešnjave, in lahko kakšna naprava dobi IP naslov od narobnega omrežja, kar pa se ne sme zgoditi. Pri komuniciranju z javnim omrežjem lahko pride do padca povezave zaradi katere izmed naše naprave in se potem tudi ta nebi odzvala na oddaljeno povezavo, ter bi se rabili voziti na firmo in ročno izklopiti napravo in jo potem nazaj vklopiti. Zaradi tehnologije PoE je večja verjetnost, da pride do pregrevanje stikala in bi ga zato morda rabili namestiti v posebno hlajeno sobo, ki bi hladila stikalo. Prav tako lahko pri takšnih tehnologijah večkrat pride do preskoka električnega toka in povzroči izklopitev PoE tehnologije, kar bi pomenilo da naše brezžično omrežje nebi več delovalo.

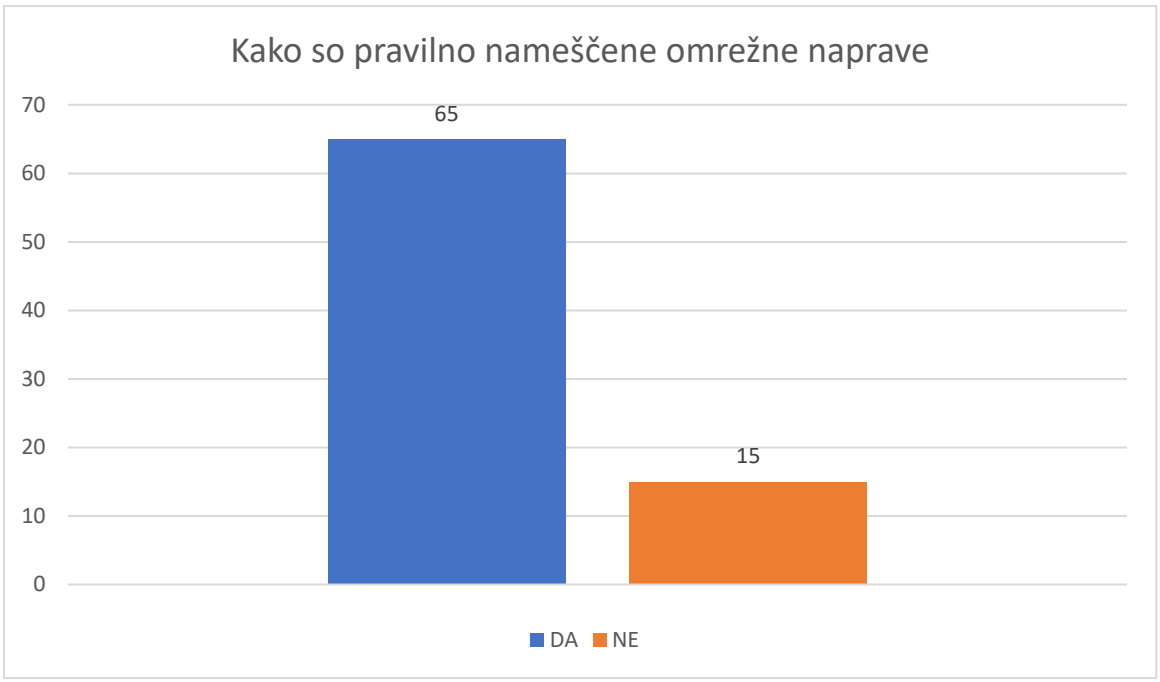
Opis rešitev za določen problem

Naše lokalno omrežje deluje na sistemu ki zagotavlja zelo dobro hitrost, ter tudi zelo dobro varnost vseh uporabnikov. Vse naše uporabnike bi lahko podučili o varnosti na spletu, ter z tem zagotovili še večjo varnost, prav tako bi jih lahko podučili, kako omrežje deluje in zaradi česa vsega lahko pride do izpada omrežja in kako se temu izogniti.

Analiza rezultatov

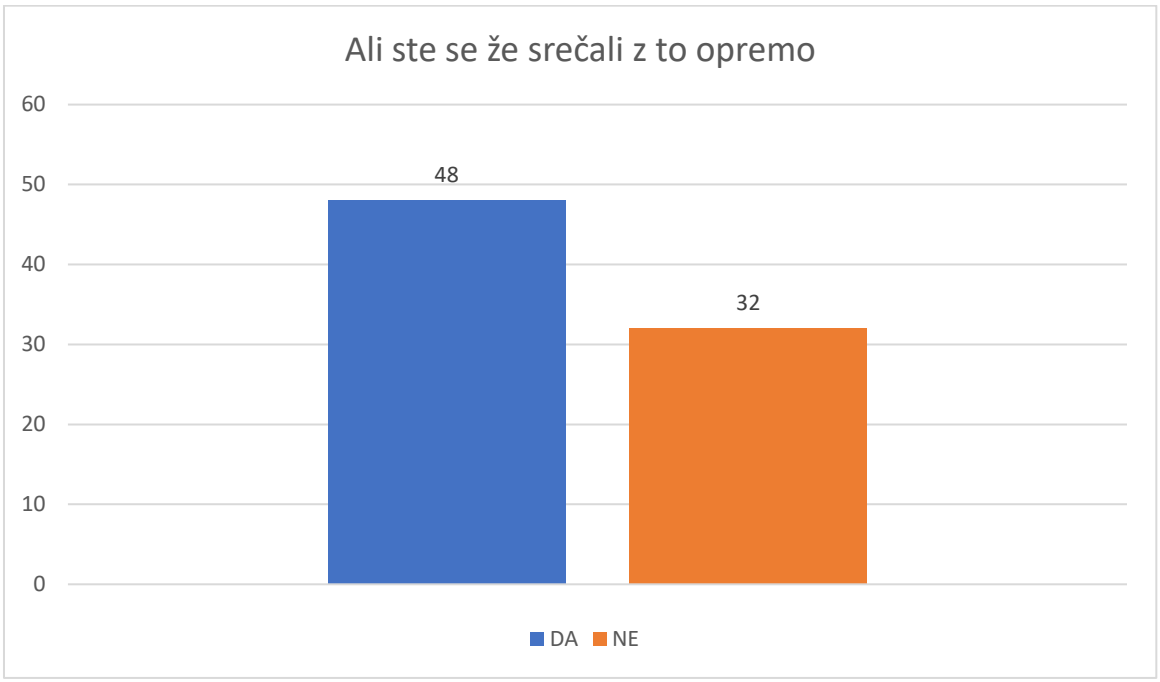
Za spletno anketo smo uporabili spletne ankete 1KA. Anketo je rešilo 80 anketirancev, večina od teh podjetij, ki so odgovarjali na vprašanja o varnosti na spletu in lokalnem omrežju, ter ali so zadovoljni z tako izvedbo omrežja.

Najprej smo anketirance vprašali, ali vedo kako so pravilno nameščene omrežne naprave, ter kje je to mesto. Večina anketiranih je odgovorila pravilno, da je to v skupni sobi oziroma prostoru, ki je namenjen za to, in je ustrezno zavarovan, da do njega ne more dostopati prav vsak.



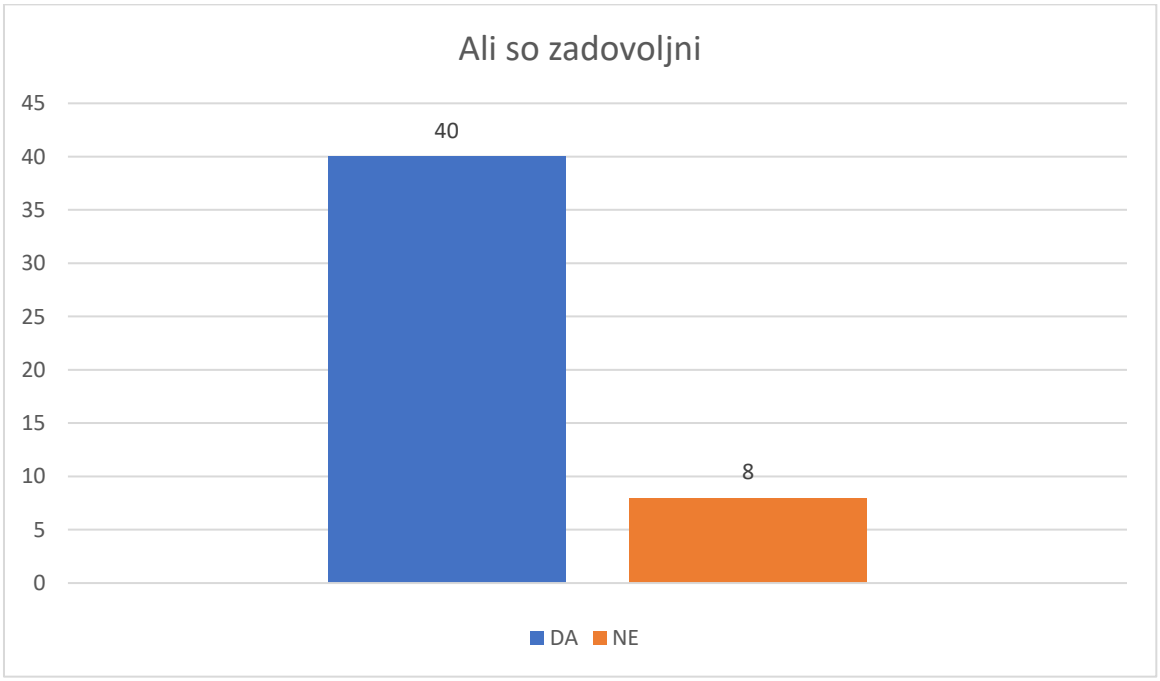
Graf 1 - Kako so pravilno nameščene omrežne naprave

Potem smo anketirance vprašali če so se že prej srečali z to opremo ali če so že zanj slišali in smo dobili zelo pozitiven rezultat, da je 48 vprašanih že poznalo to opremo oziroma že vsaj slišalo za njo.



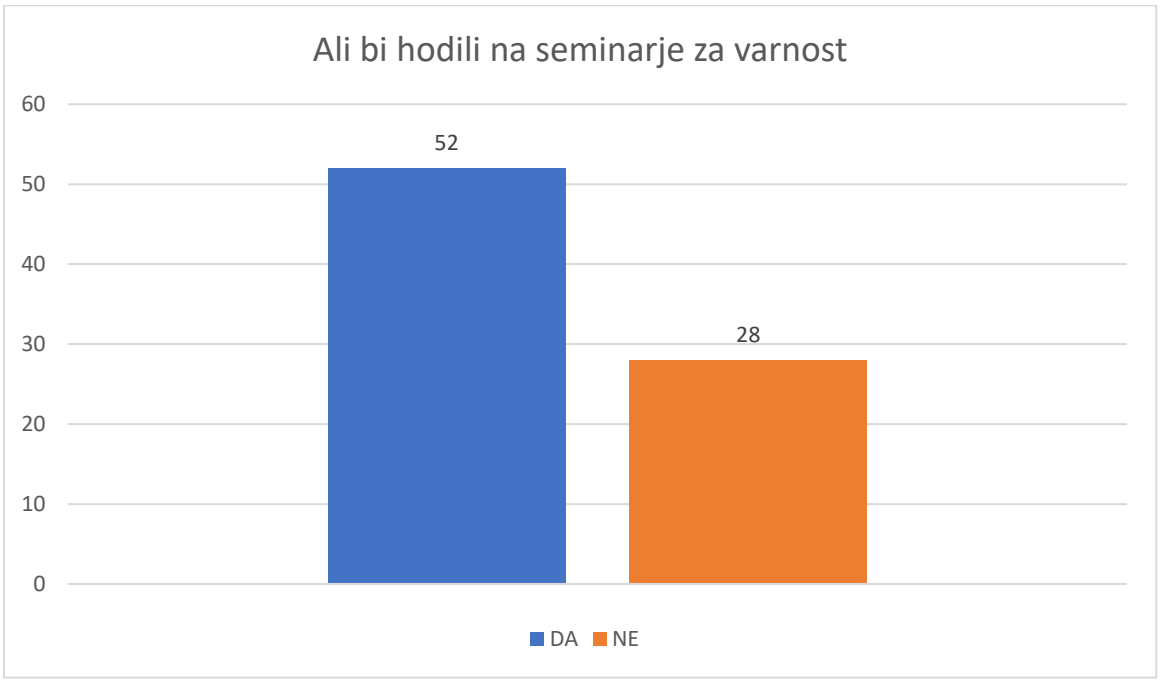
Graf 2 - Ali ste se že srečali z to opremo

Z naslednjim vprašanjem smo poizvedovali, ali so tisti, ki so že slišali za to opremo ali jo poznajo, ali so zadovoljni z njenim delovanjem in hitrostjo odpravitve težav, kjer pa so v 83% odgovorili da so zadovoljni z delovanjem takih omrežji.

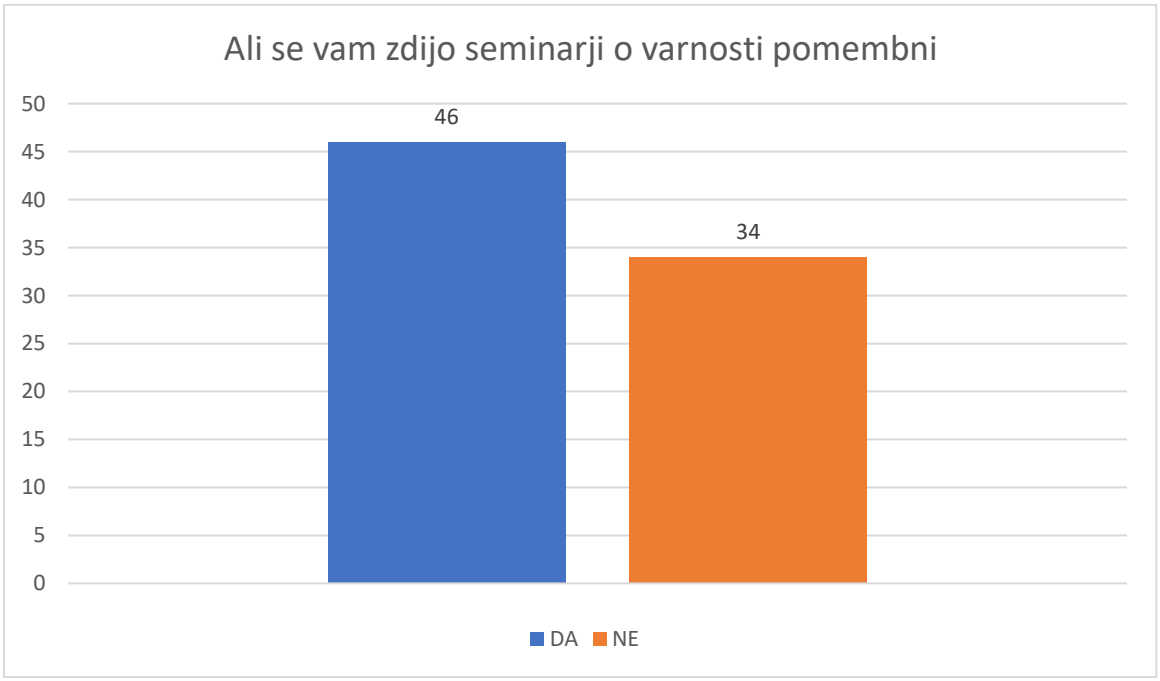


Graf 3 - Ali so zadovoljni z delovanjem

Naslednjima dvema vprašanjema je bilo namenjeno vsem podjetjem, ki imajo več zaposlenih in zelo veliko delujejo na spletu, če bi bili pripravljeni hoditi na seminarje, ter ali se jim zdi da so taki seminarji potrebni da ne pride do kakšnega nepooblaščenega dostopa.

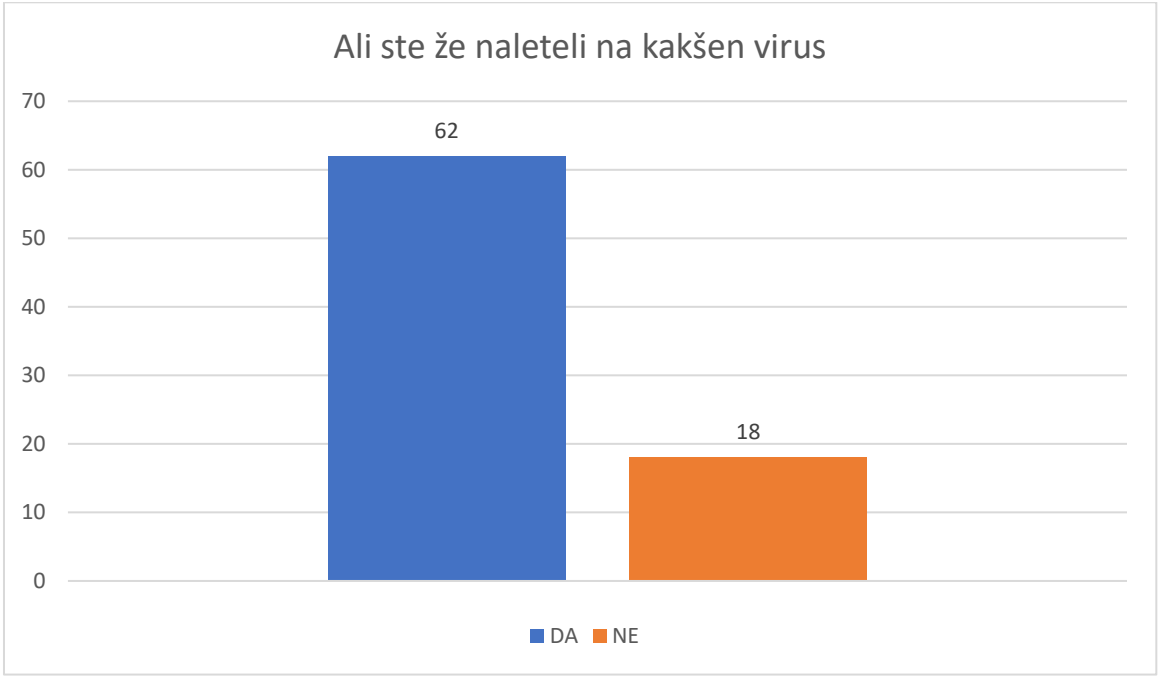


Graf 4 - Ali bi hodili na take seminarje



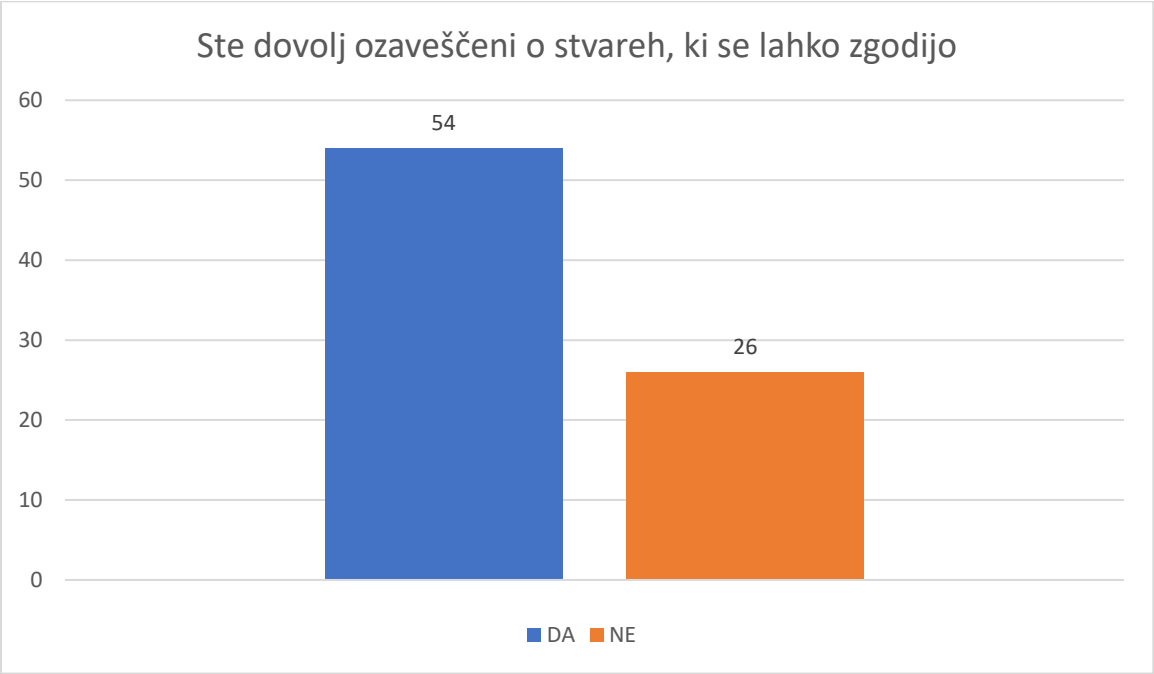
Graf 5 - Ali se vam zdijo seminarji o varnosti pomembni

Naslednje vprašanje je bilo glede njihove zgodovine, ali so že kdaj v preteklosti naleteli na kakšen računalniški virus ali če so že bili tarča kakšnih hekerjev, kjer pa je 62 ljudi že bilo v enem ali drugem primeru.



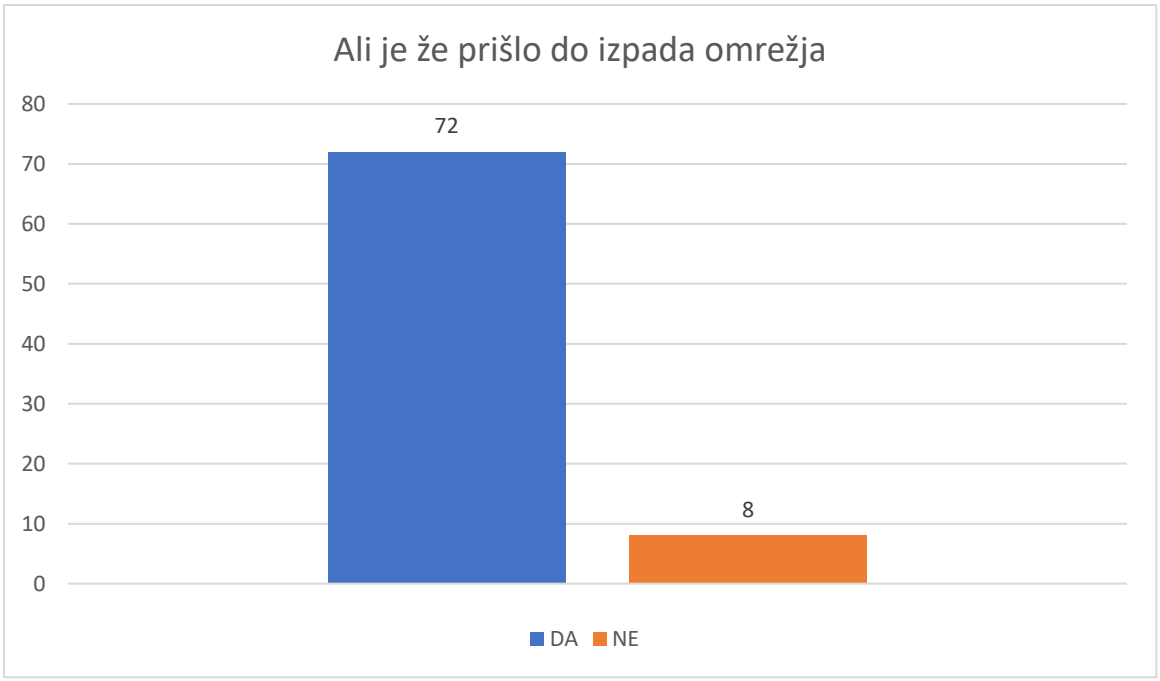
Graf 6 - Ali ste že naleteli na kakšen virus

Z naslednjim vprašanjem smo si odgovorili na vprašanje, ali se uporabnikom zdi, da so dovolj ozaveščeni o stvareh ki se nam lahko zgodijo, če nismo dovolj pazljivi, na kar pa je zelo velika večina prepričana da je in to kar v 68%.



Graf 7 - Ste ozaveščeni o stvareh, ki se lahko zgodijo

Za naslednjim vprašanjem smo anketirance vprašali ali se jim je že kdaj zgodilo, da je prišlo do izpada omrežja in če so odgovorili z da, nas je zanimalo kaj so takrat naredili, ter so vsi odgovorili, da so poklicali tehnično pomoč ter počakali da je tehnik spet vzpostavil povezavo.



Graf 8 - Ali je že prišlo do izpada omrežja

Analiza hipotez

Glede, na naše podatke, ki smo jih pridobili z raziskovalno nalogo, smo potrdili oziroma ovrgli naše hipoteze. Naše hipoteze smo vse potrdili.

Prvo hipotezo smo potrdili, saj je večina anketirancev odgovorila da je zadovoljna z takim načinom delovanja.

Drugo hipotezo smo potrdili, saj če pride do izpada omrežja imamo narejen oddaljen dostop, tako da lahko v zelo hitrem času odpravimo težavo.

Tretjo pa smo zaradi prilagoditve našega omrežja za manjša podjetja potrdili, saj nimajo toliko prometa in ne pride do napak v omrežjih.

Primeri napak v omrežju

Primer napake v našem omrežju bi lahko bil isti IP naslov na klientih, in ker ne moreta imeti dva klienta isti IP naslov sočasno je to potrebno odpraviti. V takšnem primeru bi lahko z našim oddaljenim dostopom resetirali ARP tabelo, ter počistili vse dodeljene IP naslove in tako ponovno zagnali protokol za dobivanje IP naslovov na vseh klientih. To bi lahko odpravili tudi tako, da ročno vnesemo ukaz za ponovno dobivanje IP naslova na računalniku ali pa izklopili prenosni medij in ga potem nazaj priključil v napravo.

Prav tako lahko imamo težavo z dvema DHCP strežnikoma, saj bi lahko eden izmed njiju zapolnil svojo ARP tabelo in po tem nebi več dodeljeval IP naslovov, ali pa bi enostavno prišlo do napake pri DHCP strežniku in prav tako nebi več deloval. V tem primeru bi potrebovali ponovni zagon naprave, na katerem bi prišlo do omenjena napake.

Prav tako lahko pride do izpada našega omrežja oz. ene od naših naprav. Če bi uporabniki izgubili povezavo do interneta bi lahko bila napaka v stikalu ali požarnem zidu, morda pa tudi pri našem ponudniku internetnih storitev. V takem primeru bi rabili ponoven zagon požarnega zidu oz. stikala ter če napak nebi bila odpravljena bi pomenilo, da je napaka v povezavi z našim internetnim ponudnikom.

Zaključek

V tej raziskovalni nalogi smo raziskali prednosti in slabosti našega omrežja, ter tudi povprašali ljudi o tem kakšno se jim zdi izvedba takšnega omrežja. Predstavili smo rezultate anketirancev, ter razložili in predstavili do kakšnih težav oz. napak bi lahko prišli v takšnem omrežju. Predstavili smo tudi slabosti in prednosti takšnega omrežja in povedali zakaj, se nam zdi, da je takšno omrežje primerno za manjše oziroma srednje veliko podjetje. Z enostavnim razširitvenimi možnostmi bi lahko v primeru da zmanjka priključkov na stikalu , enostavno dodali še eno stikalo, ki bi delovalo enako kot prvo in z tem povečali število priklopov. Z dobrim varnostnimi nastavitvami smo zaprli dostope do »čudnih« strani, ki bi lahko bile kakšne zlonamerne. Z lahkim administrativnim dostopom lahko enostavno popravljamo in urejamo naše varnostne police na požarnem zidu in tako da odpiramo potrebna vrata preko katerih lahko uporabniki dostopajo do raznih storitev (spletno bančništvo, FURS, …), do katerih nebi mogli če jim teh vrat nebi odprli.

Z majhnostjo in specifično našega omrežja smo dosegli zelo veliko hitrost in pretočnost omrežja, ter tako si lahko naše stranke kar se da hitro delijo podatke, datoteke ali pa brskali po internetu. Z možnostjo zaklepanje na ;AC naslove lahko zagotovimo, da se lahko na naše brezžično omrežje povežejo samo tisti, katerih MAC naslov smo mi ročno vpisali ter ga poznamo in z tem zaklenili dostop nepooblaščenim osebam v naše omrežje. Z uporabljenimi napravami bi stranke lahko dosegle največjo učinkovitost pri našem omrežju.

Zahvala

Zahvale gredo gospodu Boštjanu Lubeju, ker nas je skozi celotno delo raziskovalne naloge budno spremljal, nam pomagal, ter nas usmerjal v pravo smer. Zahvale gredo prav tako podjetju EGT d. o. o., Ulica Savinjske čete 7, 3310 Žalec, za izposojo opreme za predstavitev naloge, ter prav tako tudi Dejanu Grahku, za pomoč pri izdelavi omrežja in pri razlagi delovanja omrežnih naprav.

Viri in literatura

- https://ui.com/wi-fi (22.03.2022)
- https://www.juniper.net/us/en.html (22.03.2022)
- https://www.stormshield.com/ (22.03.2022)