Primjena tehnologija kratkog dometa kao metode socijalnog inženjeringa

Perlić, Mihovil

Sveučilište u Zagrebu

Fakultet prometnih znanosti

Mihovil Perlić

Primjena tehnologije kratkog dometa kao metode socijalnog inženjeringa

DIPLOMSKI RAD

Zagreb, rujan 2023.

Sveučilište u Zagrebu

Fakultet prometnih znanosti

DIPLOMSKI RAD

Primjena tehnologije kratkog dometa kao metode socijalnog inženjeringa

Application of short-range technology as a method of social engineering

Mentor: doc. dr. sc. Ivan Cvitić

Student: Mihovil Perlić

JMBAG: 0135245844

Zagreb, rujan 2023.

Zadatak

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI
POVJERENSTVO ZA DIPLOMSKI ISPIT

Zagreb, 23. svibnja 2023.

Zavod: **Zavod za informacijsko komunikacijski promet**
Predmet: **Sigurnost i zaštita informacijsko komunikacijskog sustava**

DIPLOMSKI ZADATAK br. 7320

Pristupnik: **Mihovil Perlić (0135245844)**
Studij: Promet
Smjer: Informacijsko-komunikacijski promet

Zadatak: **Primjena tehnologije kratkog dometa kao metode socijalnog inženjeringa**

Opis zadatka:

U okviru diplomskog rada potrebno je istražiti i pružiti pregled područja kibersigurnosti i politika u EU. Potrebno je analizirati karakteristike komunikacijskih tehnolgoija kratkog dometa, QR kod i NFS i provesti istraživanje utjecaja takvih tehnologija kao sredstvo provedbe kibernetičkih prijetnji. Na temelju razultata istraživanja potrebno je predložiti unaprijeđenja sigurnosti kod korištenje tehnologija kratkog dometa.

Mentor:

dr. sc. Ivan Cvitić

Predsjednik povjerenstva za diplomski ispit:

Sažetak

Sve većim napretkom digitalne komunikacijske tehnologije generira se i sve više digitalnih podataka koji mogu sadržavati osobne i osjetljive informacije korisnika koji koriste društvene mreže, internet usluge i različite tehnologije koje omogućavaju prijenos podataka. Sve te podatke napadač može iskoristiti u kreiranju socijal inženjering napada. Ovi napadi imaju za cilj navesti korisnike da izvrše radnje koje idu u korist napadačima ili da im svjesno ili nesvjesno pruže osjetljive podatke. Socijalni inženjering jedan je od specifičnih kibernetičkih napada jer iskorištava prirodnu ljudsku sklonost povjerenja i naivnosti.

Istraživanjem provedenim u okviru ovog diplomskog rada dan je pregled vrsta i načina provedbe kibernetičkih napada kao i mehanizama i metoda zaštite te su analizirane politike Europske unije nadležne za reguliranje i suzbijanje kibernetičkih napada. Nadalje, u radu su sa različitih aspekata opisane tehnologije kratkog dometa. Također, u sklopu rada provedeno je istraživanje utjecaja QR kod i NFC tehnologija kao kibersigurnosne prijetnje korisnika te su dani prijedlozi za unaprjeđenje sigurnosti u korištenju tehnologija kratkog dometa.

KLJUČNE RIJEČI: NFC, oznaka, QR, kod, kibersigurnost, tehnologija, socijal injženjering.

Summary

With the increasing progress of digital communication technology, more and more digital data is generated, which can contain personal and sensitive information of users who use social networks, Internet services and various technologies that enable data transmission. All this information can be used by the attacker to create a social engineering attack. These attacks aim to trick users into taking actions that benefit the attackers, or knowingly or unknowingly provide them with sensitive data. Social engineering is one of the specific cyber attacks because it exploits the natural human tendency to trust and naivety.

The research carried out as part of this diploma thesis provided an overview of the types and methods of implementing cyberattacks, as well as the mechanisms and methods of protection, and the policies of the European Union responsible for regulating and suppressing cyberattacks were analyzed. Furthermore, short-range technologies are described from

various aspects in the paper. Also, as part of the work, research was conducted on the impact of QR code and NFC technologies as a cyber security threat to users, and suggestions were made for improving security in the use of short-range technologies.

KEY WORDS: NFC, tag, QR, code, cyber security, technology, social engineering.

Sadržaj

1.Uvod

Sve većim razvojem i korištenjem tehnologija kratkog dometa, dolazi i do povećanja količina podataka koje ti uređaji prenose. Podaci koji se prenose često mogu sadržavati ključne informacije koje mogu biti od koristi napadačima da penetriraju korisnikove uređaje te da dođu u kontakt sa osjetljivim informacijama, preuzmu nadzor nad uređajem ili steknu financijsku dobit. U današnjem svijetu postoje raznolike vrste kibernetičkih napada ali i obrana od istih. Također, unutar Europske unije (EU) osnovane su razne organizacije kojima je cilj povećavanja kibersigurnosti državama članica Europske unije.

Naslov diplomskog rada jest: Primjena tehnologije kratkog dometa kao metode socijalnog inženjeringa. Rad je podijeljen u šest cjelina:

1. Uvod

2. Pregled područja kibersigurnost i kibersigurnosnih politika u EU

3. Analiza karakteristika NFC i QR kod tehnologije

4. Istraživanje utjecaja QR kod i NFC tehnologija kao kibersigurnosnih prijetnji

5. Prijedlozi za unaprjeđenje sigurnosti u korištenju tehnologija kratkog dometa

6. Zaključak.

U drugom poglavlju opisane su vrste kibernetičkih napada, načini obrane, kibersigurnost unutar Europske unije i pregled složenog okružja kibersigurnosne politike EU-a. Također, navedeni su te objašnjeni glavni akteri u EU-u nadležni za kibersigurnost, te su navedene uredbe i akti Europske unije sa gledišta kibersigurnosti.

U trećem poglavlju opisane su QR kod i NFC tehnologija sa gledišta njihovih karakteristika i načina primjene tehnologija od strane korisnika. Također, navedene su prednosti i nedostatci pojedine tehnologije te su analizirani sigurnosni rizici prilikom njihovog korištenja.

U četvrtom poglavlju analiziran je utjecaj tehnologija kratkog dometa na sigurnost korisnika. Svrha ovoga poglavlja jest utvrditi razinu sigurnosti i zaštite osobnih podataka te identifikacija sigurnosnih trendova i rizika u području tehnologija kratkog dometa.

U petom poglavlju navedeni su te istodobno i objašnjeni prijedlozi za unaprjeđenje sigurnosti u korištenju tehnologija kratkog dometa.

2. Pregled područja kibersigurnost i kibersigurnosnih politika u EU

U današnjem tehnološki brzo rastućem svijetu terminalni uređaji korisnicima uveliko pomažu i olakšavaju svakodnevne poslove, ali koliko god se čovjek pouzda na sigurnost informacija spremljenih na svom uređaju uvijek postoji mogućnost da napadač penetrira uređaj te da dođe u kontakt sa osjetljivim informacijama ili preuzme nadzor nad uređajem. Kako bi napadač ugrozio žrtvin uređaj koristi se raznim alatima i tehnikama.

U ovome poglavlju rada opisani su kibernetički napadi i načini obrane, kibersigurnost unutar Europske unije te pregled složenog okružja kibersigurnosne politike EU-a. Također, navedeni su i objašnjeni glavni akteri u EU-u nadležni za kibersigurnost, te su navedene uredbe i akti Europske unije sa gledišta kibersigurnosti.

2.1 Vrste i načini kibernetičkih napada

Postoje mnogi motivi za provedbu kibernetičkih napada, neki od njih su kriminalne radnje u cilju stjecanja financijske dobiti krađom novca ili podataka. Također, postoje osobno motivirani napadači kao što su nezadovoljni sadašnji ili bivši zaposlenici, koji će uzeti novac ili podatke kako bi ugrozili sustav tvrtke. Društveno-politički motivirani napadači koji tim putem promoviraju svoju ideologiju, također poznati kao haktivisti. Ostale motivacije za kibernetičke napade uključuju špijunažu kako bi se stekla nepravedna prednost nad konkurentima, te intelektualni izazov, [1].

Kibernetičke prijetnje mogu biti unutarnje i vanjske. Vanjske kibernetičke prijetnje uključuju pojedine kriminalce ili organizirane kriminalne skupine, profesionalne hakere te hakere amatere. Unutarnje prijetnje su korisnici koji imaju ovlašten i legitiman pristup imovini tvrtke i zlorabe ih namjerno ili slučajno. Pod unutarnje prijetnje spadaju, zaposlenici nemarni prema sigurnosnim politikama i procedurama, nezadovoljni sadašnji ili bivši zaposlenici, poslovni partneri, klijenti, izvođači ili dobavljači s pristupom sustavu, [1].

Nadalje, hakeri se također mogu podijeliti u tri skupine: crne, bijele i sive hakere. Crni hakeri su zlonamjerni hakeri čiji su glavni cilj kriminalne radnje. Bijeli hakeri spadaju pod skupinu dobronamjernih hakera čiji je glavni cilj penetriranje sustava kako bi otkrili slabosti

unutar sustava te na temelju toga dali svoje prijedloge za unapređenje sigurnosti sustava. Negdje između crnih i bijelih hakera nalaze se sivi hakeri oni rade slično kao i crni hakeri ali bez zlih namjera. Također su slični bijelim hakerima ali ujedno i različiti jer vrše penetriranje sustava bez znanja tvrtke te ne predlažu načine poboljšanja sigurnosti sustava nego samo penetriraju iz vlastite znatiželje, [2].

U današnjem digitalnom svijetu, kibernetički kriminalci koriste sofisticirane alate za pokretanje kibernetičkih napada na poduzeća. Njihove mete napada uključuju osobna računala, računalne mreže, informacijsko tehnološku (IT) infrastrukturu te IT sustave.

Tablica 1. Najčešće vrste kibernetičkih napada i njihovi opisi.

Vrste napada	**Opis napada**
Stražnja vrata Trojanski konj (engl. *Backdoor Trojan*)	Stražnja vrata Trojanski konj stvara stražnja vrata ranjivost u sustavu žrtve, dopuštajući napadaču da dobije daljinsku i gotovo potpunu kontrolu. Često korišteni za povezivanje skupine računala žrtava u *botnet* ili *zombi* mrežu, [1].
Cross-site scripting **(XSS)**	XSS napadi ubacuju zlonamjerni kod u legitimnu web stranicu ili skriptu aplikacije kako bi dobili informacije o korisniku, često koristeći web resurse trećih strana. Napadači često koriste *JavaScript* za XSS napade, ali se također mogu koristiti *Microsoft VCScript*, *ActiveX* i *Adobe Flash*, [1].
Napad uskraćivanjem usluge (engl. *Denial-of-service*), (DoS)	DoS i distribuirani napadi uskraćivanja usluge (DDoS) preplavljuju resurse sustava, preplavljuju ih i sprječavaju odgovore na zahtjeve za uslugom, što smanjuje sposobnost sustava. Često je ovaj napad priprema za još jedan napad, [1].

DNS (*Domain Name System)* tuneliranje (engl*. DNS tunneling*)	U početku DNS tuneliranje se koristilo kako bi korisnici izbjegavali plaćanje internetskih usluga u ugostiteljskim objektima jer je djelovao kao virtualna privatna mreža kako ugostitelj ne bi bio u mogućnosti naplatiti svoje usluge. Za DNS tuneliranje koriste se napadi zapovijedanja i kontrole (C&C). U ovakvoj vrsti napada žrtvino računalo konstantno generira nove DNS upite jer se DNS odgovor koji sadrži naredbe ne može poslati klijentu bez odgovarajućeg zahtjeva. Pošto ovakav napad generira veću količinu napada čini ga vidljivim i ranjivim te je to jedan od glavnih nedostataka ovakvih napada, [3].
Malware	*Malware* je zlonamjerni softver koji zaražene sustave može učiniti neoperativnim. Većina varijanti *malware- a* uništava podatke brisanjem te briše datoteka koje su ključne za rad operativnog sustava, [1].
Prevare krađe identiteta (engl*. Phishing*)	Prevare krađe identiteta pokušavaju ukrasti korisničke vjerodajnice ili osjetljive podatke kao što su brojevi kreditnih kartica. U ovom slučaju, prevaranti šalju korisnicima e-poštu ili tekstualne poruke dizajnirane da izgledaju kao da dolaze iz legitimnog izvora, koristeći lažne hiperveze, [1].

Ransomware	*Ransomware* je sofisticirani zlonamjerni softver koji se temelji na *Malware* napadu te koristi iste metode kao što su tehnika izbjegavanja, raspodjele tereta i mehanizama infekcije. Bitnija razlika od *Malware* napada jest ta što se *Ransomware* napad ne pokušava sakrivat već suprotno želi se žrtvi pokazati da je napadač preuzeo kontrolu na sustavom često pokazujući poruku kojom se traži otkupnina u zamjenu za oslobađanje sustava. Također kako bi *Ramsomware* napad bio uspješan potreban mu je pristup žrtvinom serveru zapovijedanja i kontrole (C&C). Kada napadač stekne kontrolu nad žrtvinim sustavom koristi slabosti sustava te snažnu enkripciju kako bi podatke ili funkcionalnost sustava držao kao taoca, [4].
SQL injekcija (engl. *SQL injection*)	*Structured Query Language* (SQL) napadi ubrizgavanja ugrađuju zlonamjerni kod u ranjive web aplikacije, dajući rezultate upita u pozadini baze podataka i izvodeći naredbe ili slične radnje koje korisnik nije zatražio. Neki od najčešćih vrsta SQL injekcija napada su napadi slijepim upitom (engl. *Blind Query Attack), Piggy-Backed Query Attack*, *UNION Query Attack*, napadi logički neispravnog upita (engl. *Logically Incorrect Query Attack*) i mnogi drugi, [5].

Iskorištavanje nultog dana (engl. *Zero-day exploit*)	*Zero-day exploit* napadi iskorištavaju prednosti nepoznatih hardverskih i softverskih slabosti. Ove ranjivosti mogu postojati danima, mjesecima ili godinama prije nego što programeri saznaju za nedostatke, [1].

Tablica 1 prikazuje vrste najčešćih kibernetičkih napada te njihove opise.

2.2 Pregled metoda zaštite od kibernetičkih napada

Kako u svijetu postoji sve više kibernetičkih napada sukladno tome proizlaze i razni alati i procesi pomoću kojih se sprečavaju, detektiraju ili uklanjaju kibernetičke prijetnje. Svaki alat je prilagođen određenoj vrsti kibernetičkog napada. U nastavku su predstavljeni načini obrane za različite napade.

2.2.1 Obrane od kibernetičkog napada *Backdoor trojan*

Backdoor trojan ima različite načine obrane. Jedna od obrana je da korisnik zatvori mrežne priključke koji se ne koriste jer otvoreni priključak na mreži može primati promet sa udaljenih lokacija što rezultira slabom točkom sustava. Korištenjem jake lozinke te ne korištenje iste lozinke na raznim aplikacijama i portalima pomaže prilikom obrane jer u slučaju napada napadač će imati pristup samo jednom računu dok će za ostale će morati provaliti. Pri održavanjem softverom ažurnim smanjuju se sigurnosni propusti koji su uočeni od strane izdavača softvera. Također, pri obrani pomažu razni antivirusi i vatrozidi koji blokiraju *backdoor* viruse prije nego što dospiju na žrtvino računalo, [6].

2.2.2 Obrane od kibernetičkog napada *Cross-site scripting*

Cross-site scripting (XSS) - Da bi XSS napadi bili uspješni, napadač mora umetnuti i izvršiti zlonamjerni sadržaj na web stranici. Svaka varijabla u web aplikaciji mora biti zaštićena. Osiguravanje da sve varijable prolaze kroz provjeru valjanosti, a zatim se uklanjaju ili dezinficiraju. Svaka varijabla koja ne prolazi kroz ovaj proces je potencijalna slabost. Okviri olakšavaju osiguravanje da su varijable ispravno provjerene, izbjegnute ili sanirane. Međutim, okviri nisu savršeni i još uvijek postoje sigurnosni nedostaci u popularnim okvirima kao što su React i Angular. Kodiranje izlaza i čišćenje HTML-a (engl. *HyperText Markup Language*) pomažu riješiti te nedostatke, [7].

2.2.3 Obrane od kibernetičkog napada uskraćivanja usluge

Ključna stvar u ublažavanju DoS i DDoS napada jest razlikovanje zlonamjernog prometa od normalnog prometa. Što je napad složeniji, veća je vjerojatnost da će se zlonamjerni promet teško odvojiti od normalnog prometa. Cilj napadača je što više se uklopiti, te što više otežati njegovo otklanjanje. Pokušaji ublažavanja koji uključuju neselektivno smanjenje ili ograničavanje prometa može ugroziti i normalni promet, a ne samo zlonamjerni. Napad se također može modificirati i prilagoditi kako bi se zaobišle protumjere. Kako bi se prevladao složeni pokušaj napada, slojevito rješenje će dati najveću korist, [8].

Neke od najčešće korištenih protumjera su, [8]:

- Ruta crne rupe (engl. *Blackhole routing*) - Rješenje koje koriste mrežni administratori je stvaranje rute crne rupe i usmjeravanje prometa na tu rutu. U svom najjednostavnijem obliku, kada se filtriranje crnih rupa implementira bez posebnih kriterija ograničenja i legitimni i zlonamjerni mrežni promet usmjerava se na nultu rutu ili crnu rupu i ispušta se iz mreže. Ako internetsko vlasništvo doživi DDoS napad, davatelj internetskih usluga (engl. *Internet service provider*) (ISP) tog posjeda može poslati sav promet web-mjesta u crnu rupu kao obranu. Ovo nije idealno rješenje, jer učinkovito daje napadaču njihov željeni cilj, a to je činiti mrežu nedostupnom.

- Ograničavanje broja zahtjeva (engl. *Rate limiting*) - Ograničavanje broja zahtjeva koje će poslužitelj prihvatiti tijekom određenog vremenskog okvira također je način ublažavanja napada uskraćivanja usluge. Iako je ograničenje brzine korisno za usporavanje krađe sadržaja i za ublažavanje pokušaja prijave grubom silom, ono samo po sebi vjerojatno neće biti dovoljno za učinkovito rukovanje složenim DDoS napadom. Ipak, ograničavanje brzine je korisna komponenta u učinkovitoj strategiji ublažavanja DDoS-a.

- Vatrozid web aplikacije (engl. *Web application firewall*) - Vatrozid web aplikacije (WAF) jest alat koji može pomoći u ublažavanju DDoS napada aplikacijskog sloja. Postavljanjem WAF-a između interneta i izvornog poslužitelja, WAF može djelovati kao obrnuti *proxy*, štiteći ciljani poslužitelj od određenih vrsta zlonamjernog prometa. Filtriranjem zahtjeva na temelju niza pravila koja se koriste za identifikaciju DDoS alata, napadi aplikacijskog sloja mogu se spriječiti. Jedna ključna značajka učinkovitog WAF-a je sposobnost brze implementacije prilagođenih pravila kao odgovor na napad.

2.2.4 Obrane od kibernetičkog napada *DNS tunneling*

DNS tuneliranje oslanja se na DNS upite za stvaranje zlonamjerne povezanosti s računalom kibernetičkog kriminalca. Stoga, se aktivnim nadziranjem sustava može detektirati i blokirati zlonamjerne upite, što je vrlo učinkovito u sprječavanju ovakvih napada.

Učinkovit sustav DNS filtriranja uključuje, [9]:

- Otkrivanje algoritama za generiranje domene koje kibernetički kriminalci koriste za proizvodnju nasumičnih domena za napade.
- Identifikacija i obavještavanje o čudnim obrascima DNS prometa.
- Usporedba svakog DNS zahtjeva s crnom listom identificiranih zlonamjernih domena.

2.2.5 Obrane od kibernetičkog napada *malware*

Robusni antivirusni softverski paket glavna je komponenta tehnološke obrane koju bi trebao imati svaki računalni sustav. Dobro osmišljena antivirusna zaštita ima nekoliko karakteristika. Provjerava svaki novo preuzeti program kako bi se uvjerio da nema zlonamjernog softvera. Povremeno skenira računalo kako bi otkrio i uništio mogući zlonamjerni softver. Redovito se ažurira kako bi prepoznao najnovije prijetnje. Dobra antivirusna zaštita također može prepoznati i upozoriti na čak i ranije nepoznate prijetnje zlonamjernim softverom, na temelju tehničkih značajki koje su karakteristične za zlonamjerni softver, [10].

2.3 Socijalni inženjering napadi

Socijalni inženjering napadi sve su veća kibersigurnosna prijetnja. Ovakav tip kibernetičkih napada oslanja se na manipulaciju korisnika kako bi korisnici otkrili vrijedne i osjetljive podatke u interesu kibernetičkih kriminalaca. Podaci koje napadač prikupi prilikom napada mogu biti korišteni za određene kriminalne radnje ili prodani na crnom tržištu. Svaki socijal inženjering napad ne mora biti isti ali se u principu vodi putem četiri koraka. Prvi korak jest prikupljanje informacija o meti. Nakon prvog koraka dolazi drugi korak gdje napadač pokušava ostvariti komunikaciju sa korisnikom. U trećem koraku napadač pokušava iskoristiti dostupne informacije i izvršiti napad. Četvrti korak služi napadaču da izađe bez tragova i bilo kakve povezanosti sa njim samim, [11].

Postoji više različitih kategorija socijal inženjering napada ovisno o različitim perspektivama, tako da postoji kategorija koja se klasificira prema tome koji je identitet uključen u napada to jest sudjeluje softver ili čovjek. Nadalje, mogu se klasificirati u tri kategorije prema načinu na koji je napad izveden tako da imamo društvene, tehničke i fizičke napade. Također, napadi mogu biti izravni i neizravni. Prilikom izravnih napada napadač fizičkim kontaktom, kontaktom očima ili glasovnom interakcijom vrši napad. Za razliku od izravnih napada neizravni socijal inženjering napadi ne zahtijevaju prisutnost napadača za pokretanje napada, [11].

Postoje različiti načini socijal inženjering napada, a neki od najčešćih su, [11]:

- *Phishing* - *Phishing* napadi su jedan od poznatijih napada korištenih u socijal inženjeringu. Ovakav tip napada dovode žrtve u zabludu kako bi dobili osjetljive i povjerljive informacije te uključuje lažne web stranice, e-poštu, oglase, antivirusne programe, PayPal web stranice i razne lažne nagrade. *Phishing* napadi se nadalje mogu podijeliti u pet kategorija, a to su: *pear phishing*, *whaling phishing*, *vishing phishing*, interaktivni glasovni odgovor *phishing* i poslovni *email phishing*.
- *Pretexting* – Ovakav tip napada sastoje se od izmišljanja lažnih i uvjerljivih scenarija kako bi se ukrali osobni podaci žrtve. Glavni cilj ovakvih napada jest da žrtva stekne povjerenje napadača. Napadi se izvode putem telefonskih poziva, e-pošte ili fizičkih medija.
- Mamljenje (engl. *Baiting*) – Ovakvi napadi ujedno se nazivaju i cestovne jabuke, napadi se baziraju na krađi identiteta koji pozivaju korisnike da kliknu na poveznicu kako bi dobili besplatne stvari. Ovakvi napadi su slični napadu trojanskom konju gdje napadač iskorištava nezaštićene računalne resurse kako bi preuzeo nadzor nad žrtvinim računalom.
- *Tailgating* – Ovakvi napadi su znani još i pod nazivima *piggybacking* i fizički pristup napadi. Ovakvi napadi izvode se na način da napadači posuđuju žrtvine mobilne uređaje ili računala kako bi bili u mogućnosti instalirati zlonamjeran softver na žrtvin uređaj.

Uz gore navedene načine socijal inženjering napada postoje i brojni drugi kao što su: *ransomware*, lažni softver napadi, napadi obrnutim socijal inženjeringom, napadi robotskih poziva, napadi surfanja ramenom i mnogi drugi, [11].

2.4 Kibersigurnosna politika Europske unije

Cilj ovoga potpoglavlja je pružiti pregled složenog okružja kibersigurnosne politike Europske unije i utvrditi glavne izazove u pogledu njezine djelotvorne provedbe.

Vijeće Europe 2001. godine donijela je Konvenciju o kibernetičkom kriminalu. Potpisana je u Budimpešti, 23. 11. 2001. godine sa državama članicama Europske unije i

državama nečlanica Europske unije koje su sudjelovale u njihovom sastavljanju. Konvencija je stupila na snagu 1. srpnja 2004. godine kao prvi međunarodni ugovor o računalnim zločinima. Odredbe Konvencije odnose se na kršenje autorskih prava, računalne prevare, dječju pornografiju, kršenje sigurnosti mreže, nezakonitog pristupa, ometanju podataka, ometanju sustava, zlouporabi uređaja i brojne druge kibernetičke prijetnje, [12].

Glavni akteri u EU-u nadležni za kibersigurnost su, [13]:

- Europska komisija koja nastoji povećati kapacitete i suradnju u području kibersigurnosti, ojačati položaj EU-a kao aktera u području kibersigurnosti i uključiti kibersigurnost u druge politike EU-a.
- ENISA (engl. *The European Union Agency for Cybersecurity*) Agencija Europske unije za mrežnu i informacijsku sigurnost.
- BEREC (engl. *Body of European Regulators for Electronic Communications*) Tijelo Europskih regulatora za elektroničke komunikacije.
- EC3 (engl. *European Cybercrime Centre*) Europolov Europski centar za borbu protiv kiberkriminala osnovan je radi jačanja odgovora tijela za provedbu zakona na kiberkriminal.
- CERT-EU (engl. *Computer Emergency Response Team*) Tim za hitne računalne intervencije koji podupire sve institucije, tijela i agencije EU-a.

2.4.1 Agencija Europske unije za mrežnu i informacijsku sigurnost i tijelo Europskih regulatora za elektroničke komunikacije

Agencija Europske unije za mrežnu i informacijsku sigurnost i tijelo Europskih regulatora za elektroničke komunikacije dvije su organizacije Europske unije koje igraju važnu ulogu u kibernetičkoj sigurnosti. ENISA je neovisna agencija Europske unije koja promiče i olakšava poboljšanje sposobnosti kibernetičke sigurnosti unutar EU-a. BEREC jest skupina nacionalnih regulatornih tijela koji reguliraju i koordiniraju provedbu telekomunikacijskih zakona i politika Europske unije. Obje organizacije surađuju kako bi osigurale sigurnost digitalne infrastrukture unutar EU-a, [14], [15].

ENISA je osnovana 2004. godine s ciljem poboljšanja sposobnosti kibernetičke sigurnosti EU-a i pomoći državama članicama u rješavanju rastuće prijetnje kibernetičkih napada. Djeluje kao centar stručnosti, pružajući savjete, smjernice i podršku državama članicama EU-a, kao i institucijama i agencijama EU-a. ENISA blisko surađuje s ostalim agencijama EU-a kako bi promicala koordinirani i učinkovit pristup kibernetičkoj sigurnosti unutar EU, [14].

Jedna od ključnih odgovornosti ENISA-e jest provedba strategija i politika kibernetičke sigurnosti na razini cijele Europske unije. To uključuje suradnju sa državama članicama Europske unije na razvoju nacionalnih strategija kibernetičke sigurnosti, kao i suradnju s međunarodnim partnerima u unapređenju standarda kibernetičke sigurnosti. ENISA također provodi istraživačke i razvojne aktivnosti kako bi pomogla unapređivanju najnovijih dostignuća u kibernetičkoj sigurnosti te pruža obuku i aktivnosti podizanja svijesti kako bi pomogla pojedincima i organizacijama da poboljšaju svoje vještine i znanja o kibernetičkoj sigurnosti, [14].

BEREC je odgovoran za koordinaciju provedbe telekomunikacijskih zakona i politika unutar država članica Europske unije. To uključuje osiguravanje usklađenosti država članica s propisima Europske unije o elektroničkim komunikacijama, kao što su Opća uredba o zaštiti podataka (engl. *General Data Protection Regulation*) (GDPR) i Kodeks elektroničkih komunikacija (engl. *Electronic Communications Code*) (ECC). BEREC također radi na promicanju razvoja jedinstvenog tržišta elektroničkih komunikacija unutar EU-a te osigurava da potrošači i poduzeća imaju pristup visokokvalitetnim i pristupačnim telekomunikacijskim uslugama, [15].

2.4.2 Tim Europske unije za odgovor na računalne hitne slučajeve

Tim Europske unije za odgovor na računalne hitne slučajeve je organizacija za kibernetičku sigurnost koja ima ključnu ulogu u zaštiti digitalne infrastrukture Europske unije. CERT-EU odgovoran je za kibersigurnosne incidente koji utječu na države članice Europske unije i upravljanje njima te radi na promicanju razvoja sigurnog digitalnog okruženja unutar Europske unije, [16].

CERT-EU osnovan je 2004. godine kao zajednička inicijativa Europske unije i njezinih država članica, a djeluje pod ingerencijom Agencije Europske unije za mrežnu i informacijsku sigurnost. Sjedište CERT-EU je u Bruxellesu u Belgiji, [16].

Jedna od primarnih odgovornosti CERT-EU je da služi kao prva kontaktna točka za kibersigurnosne incidente koji utječu na države članice Europske unije. To uključuje odgovor na kibernetičke napade, izbijanje zlonamjernog softvera i druge vrste kibernetičkih prijetnji koje mogu utjecati na digitalnu infrastrukturu Europske unije. CERT-EU blisko surađuje s ostalim agencijama EU-a kako bi koordinirali odgovor na kibernetičke incidente i osigurali poduzimanje odgovarajućih mjera za ublažavanje utjecaja tih incidenata, [16].

Osim uloge odgovora na incidente, CERT-EU također igra važnu ulogu u promicanju najboljih praksi i standarda kibernetičke sigurnosti unutar EU-a. To uključuje pružanje smjernica i podrške državama članicama EU-a, kao i institucijama i agencijama EU-a, kako bi im se pomoglo da poboljšaju svoje sposobnosti kibernetičke sigurnosti. CERT-EU također radi na podizanju svijesti o pitanjima kibernetičke sigurnosti među građanima i poduzećima EU-a te pruža resurse za obuku i obrazovanje kako bi pojedincima i organizacijama pomogao da poboljšaju svoje znanje i vještine o kibernetičkoj sigurnosti, [16].

2.4.3 Europolov Europski centar za borbu protiv kiberkriminala

Europski centar za kibernetički kriminal osnovao je Europol kako bi ojačao odgovor tijela kao što su ENISA, BEREC, CERT-EU te ostalih za provođenje zakona na kibernetički kriminal u EU i tako pomogao u zaštiti europskih građana, poduzeća i vlada od internetskog kriminala. Osnovan je 2013. godine, EC3 je dao značajan doprinos u borbi protiv kibernetičkog kriminala i bio je uključen u mnoge operacije visokog profila i stotine implementacija operativne podrške, [17].

Na razini operacija, EC3 se fokusira na sljedeće vrste kibernetičkog kriminala, [17]:

- Kiber ovisan kriminal.
- Seksualno iskorištavanje djece.
- Prijevara plaćanja.

Pružena podrška također se proteže na borbu protiv kriminala na *Dark Webu* i alternativnim platformama.

Među glavni ciljevima EC3 su, [17]:

- Da služi kao središte kriminalističkih informacija i obavještajnih podataka.
- Podupire operacije i istrage država članica nudeći operativnu analizu, koordinaciju i stručnost.
- Pruža podršku strukturama EU-a za upravljanje kriznim situacijama, olakšava operativnu, tehničku i stratešku suradnju između agencija za provođenje zakona i drugih kibernetičkih zajednica i institucija, tijela i agencija EU-a (npr. ENISA, CERT-EU, Komisija, Vijeće i druge...)
- Podupire osposobljavanje i izgradnju kapaciteta, posebno za relevantna tijela u državama članicama.

2.4.4 Uredbe i akti Europske unije sa gledišta kibersigurnosti

Europska unija donijela je nekoliko akata i propisa koji se bave pitanjem kibernetičke sigurnosti. Cilj ovih mjera je zaštititi kritičnu infrastrukturu EU-a, kao i osobne podatke građana EU-a, od kibernetičkih prijetnji i napada.

Jedan od glavnih akata koji se odnose na kibernetičku sigurnost u EU je ((EU) No. 2016/1148) Direktiva o mrežnim i informacijskim sustavima (NIS Direktiva). Ova direktiva utvrđuje minimalne sigurnosne zahtjeve za operatere osnovnih usluga i pružatelje digitalnih usluga u EU-u. Također uspostavlja okvir za suradnju između država članica kako bi se poboljšala njihova otpornost na kibernetičke prijetnje i odgovorilo na incidente, [14].

Drugi važan akt u pristupu EU-a kibernetičkoj sigurnosti je ((EU) No. 2016/679) Opća uredba o zaštiti podataka. Ova uredba utvrđuje pravila za prikupljanje, korištenje i zaštitu osobnih podataka. Odnosi se na sve organizacije koje obrađuju osobne podatke građana EU-a, bez obzira obrađuju li se podaci unutar ili izvan EU-a, [18].

EU je također uspostavio ECSO (engl. *European Cyber Security Organisation*) Europsku organizaciju za kibernetičku sigurnost, koja je odgovorna za koordinaciju provedbe mjera kibernetičke sigurnosti diljem EU-a. ECSO radi s državama članicama, industrijom i

akademskom zajednicom na razvoju i promicanju najboljih praksi u kibernetičkoj sigurnosti, [19].

Uz te akte i organizacije, EU je također uspostavio niz inicijativa i programa za rješavanje pitanja kibernetičke sigurnosti. Na primjer, EU je pokrenuo ((EU) No. 2019/881) Zakon o kibernetičkoj sigurnosti, čiji je cilj ojačati sposobnost EU-a da odgovori na kibernetičke prijetnje i incidente. Također je uspostavio mrežu kompetencija za kibernetičku sigurnost koja okuplja stručnjake iz cijelog EU-a radi razmjene znanja i stručnosti o kibernetičkoj sigurnosti, [20].

Općenito, EU je zauzeo aktivan pristup rješavanju pitanja kibernetičke sigurnosti, uz niz mjera za zaštitu svoje kritične infrastrukture i osobnih podataka svojih građana. Ove mjere pokazuju predanost EU-a održavanju sigurnog i pouzdanog internetskog okruženja za sve svoje građane.

3. Analiza karakteristika NFC i QR kod tehnologije

QR kod i NFC su dvije popularne tehnologije koje se koriste u svakodnevnom životu za različite svrhe, uključujući plaćanje, identifikaciju, dijeljenje informacija i mnoge druge.

NFC se pojavio na tržištu 2002. godine te je relativno nova tehnologija bežičnog povezivanja kratkog dometa koja je proizašla iz kombinacije postojeće tehnologije beskontaktne identifikacije i konektora. Charles Walton dobio je prvi patent za radio frekvencijsku identifikaciju 1983. godine (US 4,384,244). Patent za koncept radio frekvencijskog (RF) upravljanog transpondera prijavljen je 1970. i izdan M. Cardullu i W. Parksu 1973. kao (US 3,713,148), [21].

Godine 1994. Toyotina podružnica stvorila je QR kodove za praćenje automobilskih dijelova. QR kodovi su odmah postali popularni u Japanu kao način pristupa informacijama putem mobilnih uređaja. Međunarodno su priznanje stekli 2006. godine, kada je japanska tvrtka Denso Wave javnosti učinila dostupnom punu specifikaciju QR koda. QR kodovi se od tada koriste iz raznih razloga, od marketinga i oglašavanja do praćenja kontakata i sustava plaćanja. QR kodovi su u današnjem svijetu sveprisutna tehnologija, [22].

3.1 Karakteristike NFC tehnologije

Induktivna sprega koristi se u komunikaciji bliskog polja. NFC funkcionira pomoću magnetske indukcije između dvije antene u bliskom polju jedne druge. NFC radi na frekvenciji od 13,56 MHz i ima brzinu prijenosa podataka od 106 kbit/s do 424 kbit/s na udaljenosti od oko 10 cm. NFC koristi inicijator i najmanje jedan ciljni uređaj, pri čemu inicijator aktivno proizvodi RF polje koje može napajati pasivnu metu to jest oznaku,[21].

NFC omogućuje povratnu kompatibilnost s infrastrukturom pametnih kartica temeljenu na standardu ISO/IEC 14443 za beskontaktne pametne kartice, kao i standardima Sony FeliCa kartica. Novi protokol za razmjenu informacija između dva NFC uređaja razvijen je i opisan u standardima ECMA-340 i ISO/IEC 18092, [21].

Uređaji mogu raditi u aktivnom ili pasivnom načinu rada. U aktivnom načinu rada oba uređaja s omogućenom NFC-om stvaraju elektromagnetsko polje i razmjenjuju podatke. U

pasivnom načinu rada postoji samo jedan aktivan uređaj, a oznaka razmjenjuje informacije pomoću tog polja, [21].

ISO/IEC 18092 definira tri načina rada unutar dva modaliteta komunikacije, [21]:

- Čitaj/Piši: U ovom načinu rada telefon s omogućenim NFC-om može čitati ili pisati podatke u standardnom NFC formatu podataka u bilo koju od podržanih vrsta oznaka.
- *Peer-to-Peer*: Podaci se mogu slati između dva uređaja s omogućenom NFC-om. Mogu, primjerice, dijeliti WiFi (engl. *Wireless Fidelity*) ili Bluetooth vezu. Alternativno, podaci se mogu razmjenjivati u obliku virtualnih posjetnica i slika.
- Emulacija kartice: Dok telefoni s omogućenom NFC tehnologijom mogu funkcionirati kao čitači kada su u kontaktu s oznakama, telefon također može funkcionirati kao oznaka (beskontaktna kartica) za druge čitače (POS terminale) u ovom načinu rada.

Telefoni s omogućenom NFC-om mogu ispuniti zahtjeve aplikacije za plaćanje EMV beskontaktnom karticom navedene u EMV CCPS v2.0 i predstavljene American Express ExpressPay 2.0, MasterCard PayPass 2.0 i Visa payWave 2.1.1 u načinu emulacije kartice. Kao rezultat toga, ako NFC uređaj radi u načinu rada emulacije kartice u skladu sa zahtjevima ISO/IEC 18092, trebao bi biti kompatibilan s čitačem/pisačem (POS terminal) koji slijedi specifikacije ISO/IEC 14443, [21].

3.1.1 Primjene NFC tehnologije

NFC je svestrana tehnologija i svoju ulogu je našla u raznim industrijama, uključujući maloprodaju, prijevoz, bankarstvo i mnogim drugima. U nastavku su opisane neke od najčešćih primjena NFC tehnologije.

U beskontaktnom plaćanju NFC tehnologija se koristi za olakšavanje komunikacije između kartice za beskontaktno plaćanje ili aplikacije za mobilno plaćanje na pametnom telefonu sa terminalom za plaćanje. Kupci mogu platiti korištenjem NFC tehnologije na dva načina. Prvi način je putem kartice sa značajkom plaćanjem na dodir gdje se za kupnju koristi kartica s NFC tehnologijom za prijenos podataka o plaćanju između kartice i terminalom za plaćanje. Drugi način je uz pomoć pametnog uređaja koji koristi NFC tehnologiju te aplikaciju koja sadržava informacije o plaćanju te se kao u prvom slučaju uređaj prisloni uređaju za

plaćanje. Pri prislanjanju kartice ili pametnog uređaja na terminal za plaćanje on šalje radio frekvencijski signal na karticu ili pametni telefon. Ovaj signal sadrži zahtjev za informacijama o plaćanju. Platna kartica ili pametni telefon tada odgovaraju slanjem poruke natrag terminalu koja sadrži potrebne podatke o plaćanju, poput broja kartice i datuma isteka. Terminal zatim obrađuje plaćanje slanjem podataka korisnikovoj banci ili procesoru plaćanja, koji odobrava ili odbija transakciju, [23].

Kod kontrole pristupa NFC tehnologija se koristi za skeniranje NFC oznake koja se koristi u sustavu kontroliranog pristupa, kao što su uredi, hotelske sobe ili teretane. NFC oznaka nosi informacije koje može pročitati NFC čitač koji je povezan s kontrolnim sustavom i koristi se za kontrolu pristupa objektu, [24].

NFC čipovi mogu se ugraditi u tijela ljudi ili životinja za pohranu informacija koje NFC čitač može čitati. Čip se može koristiti za otvaranje vrata ili plaćanje, ali također može bilježiti medicinske podatke poput alergija, lijekova te ostale ključne podatke koje mogu biti od koristi za zdravlje osobe koja nosi implantat, [24].

NFC može pomoći u optimizaciji zadataka ili logistike olakšavajući praćenje i upravljanje tako što korisnik uz pomoć NFC oznaka te informacijama koje te oznake sadrže može brzo i lako prepoznati što treba učinit i kada to treba učiniti, [24].

3.1.2 Prednosti i nedostatci NFC tehnologije

Jedna od primarnih prednosti NFC tehnologije je njezina praktičnost. Korisnicima omogućuje slanje podataka ili informacija između dva uređaja bez upotrebe žica ili pristupa internetu. Ovo je osobito korisno za brzo dijeljenje manjih bitova podataka, kao što su podaci za kontakt, podaci o plaćanju ili podaci o lokaciji. Nadalje, NFC tehnologija standardizirana je diljem svijeta i nudi širok raspon primjena. NFC tehnologija također je iznimno sigurna. Štiti podatke koji se prenose između uređaja putem enkripcije, što otežava neovlaštenim korisnicima presretanje ili krađu informacija kao što su brojevi kreditnih kartica i druge osjetljive financijske podatke. Kao rezultat toga, NFC je savršena tehnologija za korištenje u sustavima mobilnog plaćanja koji prenose osjetljive financijske podatke, [25].

Jedna od mana koje NFC tehnologija ima jest vrlo mali domet od samo nekoliko centimetara. To znači da uređaji moraju biti dosta blizu jedan drugome kako bi se mogao odvijati prijenos podataka. Ako uređaji nisu dovoljno blizu jedan drugome, mogu se dogoditi komplikacije prilikom prijenosa informacija. Također, mana NFC tehnologije je ta što je vrlo ograničena brzinom kojom se šalju podaci od samo 400 Kbit/s, sa takvom brzinom prijenosa podataka ima ograničene sposobnosti rada te nije pogodna za prijenos velikih datoteka kao što zahtjeva na primjer prijenos video sadržaja. Međutim, mogu povezivati korisnike s određenim web-mjestima i web-stranicama tako da je dijeljenje materijala i dalje moguće ali samo kada je primatelj spojen na internet. Nadalje, mana NFC tehnologije je sama cijena zato što korištenje i prilagodba NFC oznaka podrazumijeva nabavu oznaka, metalnih ili drvenih kartica i NFC čitača za programiranje naljepnica. Cijena može biti minimalna za pojedinačnog korisnika, ali dramatično raste za tvrtke koje kupuju velike količine. Također, budući da prosječni klijent vjerojatno neće imati novca za kupnju skupog pametnog telefona s NFC-om, trgovine ne mogu brzo implementirati NFC tehnologiju i zamijeniti postojeće metode plaćanja beskontaktnim, [26].

3.1.3 Sigurnost NFC tehnologije

Niti jedna tehnologija ne dolazi bez rizika od korištenja, pa tako i NFC tehnologija sadrži određene sigurnosne rizike. U narednom tekstu biti će navedeni i objašnjeni jedni od najčešćih sigurnosnih rizika NFC tehnologije.

Prisluškivanje je jedan od najčešćih sigurnosnih problema s NFC tehnologijom. Ako bi treća strana presrela podatkovnu komunikaciju između pametnog telefona i čitača kreditnih kartica, teoretski bi mogla doći do podataka o kreditnoj kartici te osobe. Također mogu presresti dodatne osobne podatke koji se prenose između dva mobilna telefona. Ali to je vrlo teško izvesti pošto uređaji moraju biti veoma blizu jednog drugoga kako bi se izvršilo prijenos podataka te bi uređaj koji prisluškuje trebao imati vrlo male dimenzije ili dobro zamaskiran. Nadalje, što čini prisluškivanje NFC tehnologije otežano jest da NFC tehnologija koja se koristi kod plaćanja upotrebljava sigurne šifrirane kanale koje samo ovlašteni uređaji mogu dekodirati i pristupiti dijeljenim podacima, [27].

Oštećenje podataka, manipulacija ili presretanje se događa kada treća strana presretne signal, modificira ga i pošalje na njegovu rutu. Informacije koje prima druga strana mogu biti oštećene ili izmijenjene. Napadač može, ali i ne mora željeti ukrasti podatke. U nekim okolnostima, napadač samo želi spriječiti prijenos točnih informacija. Do oštećenja podataka može doći ako neovlašteni uređaj za čitanje kartica na neki način petlja u razmjenu podataka, kao što je autoriziranje plaćanja za veći iznos od onog koji je prikazan na korisničkom zaslonu tijekom korištenja beskontaktne metode plaćanja, [27], [28]

Poradi povećanja broja korisnika koji koriste svoje pametne uređaja sa NFC tehnologijom za razna plaćanja, korisnici sadržavaju u svojim uređajima vrijedne informacije kao što su podaci o bankovnom računu i kreditne kartice. Stoga, napadači kreiraju raznolike viruse kako bi ekstrahirali te vrijedne informacije i stekli financijsku dobit, [27].

Ukoliko dođe do krađe kartice ili pametnog uređaja koji koriste NFC tehnologiju za plaćanje, kradljivac može kupovati sa ukradenom NFC tehnologijom ukoliko nije postavljena određena lozinka.

3.2 Karakteristike QR kod tehnologije

QR kod je vrsta barkoda koji kodira informacije kao niz piksela u mreži kvadratnog oblika i može se brzo očitati digitalnim uređajem. QR kodovi često se koriste u marketinškim i reklamnim aktivnostima za praćenje informacija o proizvodima u opskrbnom lancu. Međunarodna organizacija za standardizaciju (engl. *International Organization for Standardization*) (ISO) potvrdila ih je kao međunarodni standard 2000. godine, [29].

QR kodovi se sastoje od crnih kvadrata organiziranih u rešetku (matricu) na bijeloj pozadini prikazano na slici 1, a skenira ih specijalizirani softver koji može izvući podatke iz uzoraka u matrici. Ovi kodovi mogu sadržavati više informacija od standardnih barkodova i mogu primiti četiri vrste podataka: abecedne, numeričke, binarne i Kanji, [29].

Slika 1. Primjer standardnog QR koda

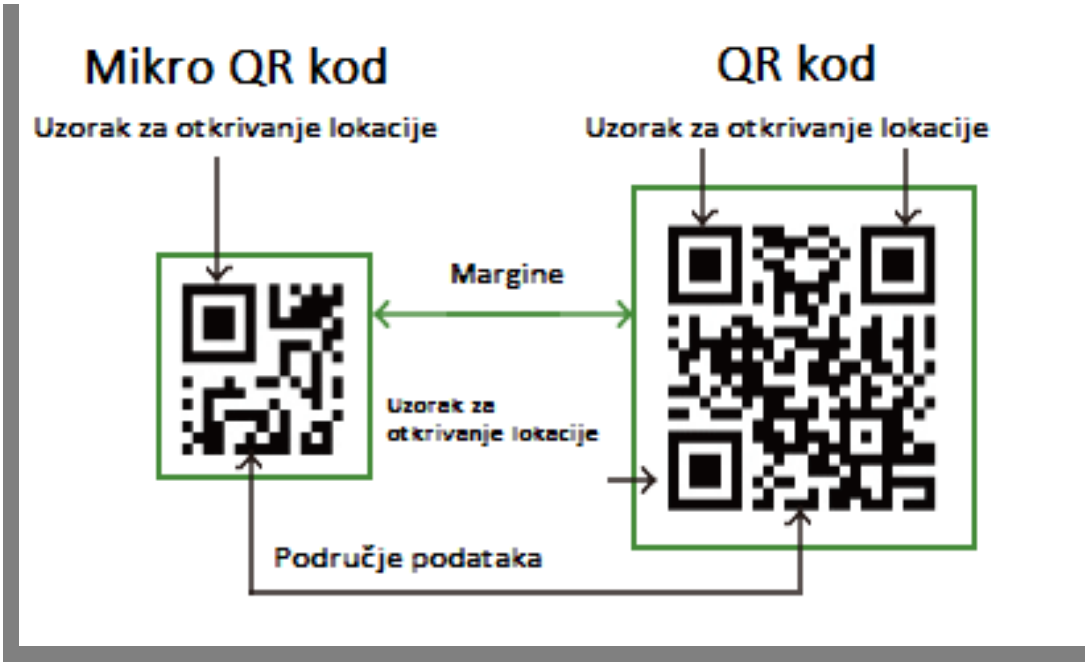
Izvor: [30].

Također, postoje raznolike verzije QR kodova koji se koriste ovisno o zahtjevima korisnika i situacijama u kojima će se koristiti. U narednom tekstu biti će opisane različite verzije QR kodova.

Model 1 i Model 2 QR kodovi su standardizirani kodovi. Model 1 je prethodnica modelu 2 te može pohraniti 1.167 brojeva. Model 2 jest model koji se najviše koristi u današnje doba, on je kreiran unaprjeđujući Model 1. Nadalje, Model 2 može teoretski pohraniti 7.089 brojeva. Model 2 se sastoji od triju različitih uzoraka koji služe za pozicioniranje, te sadrži četiri razine za ispravljanje greški, [31].

Mikro QR kod je umanjena verzija standardnog QR koda. Ovakav QR kod koristi se u situacijama kada je prostor iz nekoga razloga limitiran, kao što je slučaj kod označavanja nekih proizvoda malih fizičkih dimenzija, male tiskane pločice ili električne komponente i tako dalje. Poradi smanjenih dimenzija mikro QR kodovi nemaju mogućnost spremanja jednaku količinu podataka kao standardni QR kodovi te je limitiran na 35 brojeva to jest 128 bitova podataka. Nadalje, mikro QR kod sadrži samo po jedan uzorak za otkrivanje lokacije dok standardni QR kodovi se sastoje od triju različitih uzoraka pozicioniranja. Također, mikro QR kod ima do tri razine ispravljanja pogrešaka, dok konvencionalni QR kod ima do četiri razine. Konvencionalni QR kod zahtijeva široku granicu od četiri modula, dok mikro kod zahtijeva samo dva modula. Kao rezultat toga, postoji veća površina dostupna za kodiranje podataka u manje prostora, [32].

Slika 2 grafički prikazuje razliku između mikro te standardnog QR koda u vidu različitog broja uzoraka za otkrivanja lokacije, površine na kojoj se podaci mogu spremati te margina svakog od QR koda.



Slika 2. Razlika mikro I standardnog QR koda

Izvor: [33].

IQR kod podržava širok raspon veličina koda, od manjih od standardnog QR koda i mikro QR koda do većih koji mogu sadržavati više podataka. Ovaj se kod također može ispisati kao pravokutni kod, okrenuti kod, crno-bijeli inverzijski kod ili kod s točkastim uzorkom što omogućuje različite primjene u raznim poljima. Velika prednost iQR koda što može pohraniti više podataka od standardnog QR koda u ovisnosti o samoj fizičkoj veličini koda, [32]. Slika 3 prikazuje različite varijante iQR kodova.

Slika 3. iQR kodovi

Izvor: [34].

3.2.1 Primjene QR kod tehnologije

QR kodovi su revolucionarna tehnologija za pristupanju različitom spektru informacijama kao što su URL (engl. *Uniform Resource Locator*), tekstualni podaci, multimedijalni i tako dalje. Prvotno su bili dizajnirani za unaprjeđenje upravljanjem zalihama u automobilskoj industriji, ali kako je vrijeme odmicalo QR kodovi pronašli su svoju svrhu u različitim kutovima industrija te također kod privatnih osoba. U narednom tekstu objašnjene su različite upotrebe QR kodova te između ostalog i njihov utjecaj na današnju svakodnevnicu, [35].

QR kodovi su učinkoviti alati koji se koriste u svrhe marketinga i oglašavanja. QR kodovi mogu biti različitih veličina te različitih boja, oblika ili čak mogu sadržavati određene slike u sebi kako bi zaokupili pažnju ljudima. Mogu se implementirati na raznim mjestima te su iz toga razloga popularna opcija za oglašavanje. Također, istovremeno pruža tvrtkama analitiku u pogledu kao što je broj korisnika koji su skenirali određeni QR kod, poziciju na kojoj je skeniran te također ukazuje na vrijeme kada je skeniran, [35].

Svrha u koju se QR kodovi koriste proteže se čak do mobilnog plaćanja. Nakon što korisnik uz korištenje kamere svoga pametnog uređaja skenira kod, preusmjerava se na stranicu za plaćanje gdje će imati opciju unosa odabranih podataka o plaćanju ili korištenja posrednika za mobilno plaćanje, poput Apple-a ili Google Pay-a, za dovršetak transakcije, [35].

Za vrijeme dok je trajala Covid-19 pandemija QR kodovi su se koristili za pohranjivanje informacija o cijepljenosti građana. Građani bi dobili potvrdu da su cijepljeni ili preboljeli tu

bolest u pisanom obliku ali istovremeno i putem QR koda. Kada bi ovlaštene osobe skenirale QR kod mogle su uvidjeti podatke građana te utvrditi posjeduje li građanin potvrdu o preboljenu ili cijepljenju.

QR kodovi su pronašli svoju svrhu između ostalog i u području zabave te učenja. Muzeji i turističke atrakcije u svojoj blizini mogu sadržavati QR kodove koji mogu pružiti detaljne opise atrakcija ili umjetnina, audio vodiče ili interaktivna iskustva te tom prilikom povećati razumijevanje i angažman posjetitelja, [35].

Korištenje QR kodova kod sustava provjere autentičnosti. Korištenje QR kodova u ovome smislu radi na principu gdje korisnici mogu jednostavno generirati sliku QR-koda za autentifikaciju putem mobilne aplikacije na svojim pametnim uređajima. Sustav se uglavnom koristi u jeftinim sustavima provjere autentičnosti kao što je kontrola pristupa na vratima u zgradama i ostalim sustavima gdje je potrebna identifikacija korisnika, [36].

3.2.2 Prednosti i nedostatci QR kod tehnologije

Jedna od primarnih prednosti QR kod tehnologije jest ta što mogu pohraniti veliku količinu podataka u oblicima kao što su URL- ovi web stranica te stoga korisnici ne moraju vlastoručno upisivati URL tražene web stranice nego jednostavno skeniraju QR kod. Također, u QR kod se može pohraniti određene tekstualne ili multimedijalne sadržaje koje pružaju određene korisne informacije korisnicima koji ih skeniraj što pruža učinkovitost i praktičnost za korisnike koji ih koriste. Nadalje, jedna od prednosti koja se iskazuje kod QR kod tehnologije jest mogućnost analize u vidu aktivnosti kao što je broj korisnika koji su skenirali određeni QR kod, poziciju na kojoj je skeniran te također i vrijeme kada je skeniran. Gore navedene informacije mogu koristit raznim tvrtkama kako bi unaprijedili svoje poslovanje raznim pogledima. Između ostalog, skenirati QR kod mogu svi koji posjeduju pametni uređaj sa kamerom te to uveliko proširuje broj korisnika, a samim time nedvojbeno i nadmoć na tržištu u tom segmentu tržišta, [37].

Nedostatke koje sadrži QR tehnologija je ta da ukoliko je QR kod naljepnica fizički oštećena to jest ako ne izgleda vizualno kako bi trebala izgledati prilikom njezine proizvodnje doći će do pogreške prilikom skeniranja te se neće izvršiti aktivnost za koju je ta QR kod

naljepnica predviđena da uradi. Uzročno tome korisnik neće primiti potrebne informacije. Nadalje, ukoliko se na QR kod sprema URL od neke web stranice koja ima dugački URL može doći do komplikacija prilikom skeniranja koda. Također, sigurnost predstavlja nedostatak jer napadači mogu implementirati URL koji u sebi sadrži maliciozni sadržaj. Pored ostalog ne savjetuje se spremanje privatnih informacija na QR kod iz razloga što svatko tko je u prilici može ga skenirati te vidjeti te informacije koje bi mogle ugroziti intimu, [25].

3.2.3 Sigurnost QR kod tehnologije

QR kodovi postali su sve popularniji u raznim industrijama zbog svoje praktičnosti i jednostavnosti korištenja. Međutim, kao i svaka druga tehnologija, QR kodovi nisu imuni na sigurnosne prijetnje. U nastavku teksta biti će navedeni i objašnjeni jedni od najčešćih sigurnosnih rizika QR kod tehnologije.

U slučaju da se QR kodovi koriste u svrhu provjere autentičnosti donosi određene rizike. Ovakav slučaj korištenja QR kodova ranjivo je u pogledu lažiranja tuđeg identiteta kako bi se stekao pristup. QR kod jednostavno se može replicirati i duplicirati korištenjem pametnog uređaja i uz samo par radnji. Istodobno prijetnja u ovom slučaju korištenja može biti obrnuti inženjering koji koristi ranjive atribute korištene mobilne aplikacije. Također, obrnuti inženjering može se pojaviti na različitim komponentama za konfiguriranje sustava ali najviše tome riziku podliježe mobilna aplikacija, [36].

U novije tehnološki gledano doba gdje su QR kodovi sve prisutniji u ljudskim svakodnevnicama, a istodobno većina ljudi nije svjesna njihovih funkcionalnosti i mogućnosti koje pružaju te rizike koje njihovo korištenje može imati, stoga su tom prilikom itekako efektivni u napadima socijal inženjeringa. QR kodove prikaže kao legitimne i primamljive korisnicima kako bi ih skenirali. Napadi socijal inženjeringom jest da se štetne QR kodove prikaže kao legitimne i primamljive korisnicima kako bi ih skenirali. To se može učiniti na dva načina. Prvi način je gdje napadač zamijeni cijeli QR kod u potpunosti gdje je kreiran na takav način kako bi privukao što više žrtava. Drugi način je taj da postojeći legitiman QR kod izmjeni da ljudskom oku nije primjetno ali je dovoljno da promijeni strukturu QR koda i promijeni njegovu funkciju u svoju korist, [35].

Napadači mogu koristiti ovakav tip napada kako bi dobili pristup povjerljivim podacima neke organizacije ili privatne osobe. Kada žrtva skenira kod svojim pametnim telefonom ili drugim uređajima, preusmjerava je na zlonamjernu web stranicu ili datoteku. Ta stranica može tražiti žrtvu da upiše svoje povjerljive informacije kao što su razne lozinke, osobni identifikacijski broj, broj telefona te ostale osjetljive informacije bez da žrtva ikada shvati da je upisala svoje povjerljive informacije na stranicu napadaču umjesto na neku legitimnu i sigurnu stranicu. QR napadi društvenim inženjeringom je efektivan način napada, a razlog njihove efektivnosti je u tome što pametni uređaji kojima se skeniraju štetni QR kodovi često sadrže osjetljive i privatne podatke koje napadači mogu iskoristiti u svoju korist kako bi stekli kontrolu nad žrtvinim uređajem, organizacijom ili stekli financijsku dobit iznuđivanjem, [38].

4. Istraživanje utjecaja QR kod i NFC tehnologija kao kibersigurnosnih prijetnji

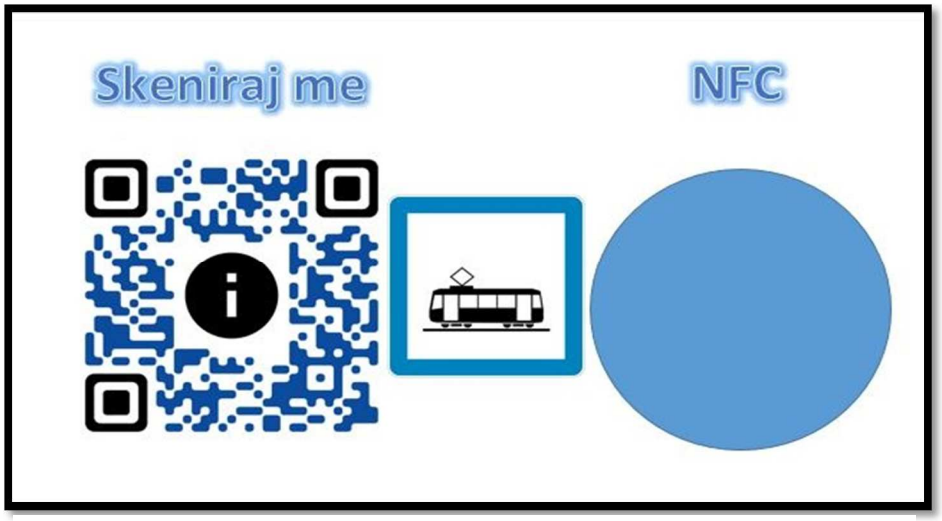
Cilj ovoga istraživanja je analizirati utjecaj tehnologija kratkog dometa na sigurnost korisnika. Svrha ovoga istraživanja jest utvrditi razinu sigurnosti i zaštite osobnih podataka te da se identificiraju sigurnosni trendovi i rizici u području tehnologija kratkog dometa. Ovakvo istraživanje može pomoći u razvoju politika i strategija za zaštitu korisnika od kibersigurnosnih prijetnji, kao i poboljšanju postojećih mjera. Sukladno tome, istraživanje može pomoći u osvještavanju korisnika o važnosti sigurnosti na internetu te kako se zaštititi od kibersigurnosnih prijetnji koje proizlaze od tehnologija kratkog dometa kao što su NFC i QR kod.

U ovom istraživanju dobiveni su kvantitativni rezultati u vidu broja korisnika koji su skenirali specifične QR kodove ili NFC oznake u svrhu pružanja uvida u učestalost kibernetičkih prijetnji povezanih s QR kodovima i NFC tehnologijom. Nadalje, u sklopu istraživanja provedeno je anketiranje korisnika putem web stranice gdje su dobiveni anketni rezultati koji će dati jasniji uvid u strukturu i karakteristike korisnika koji su podložni ovakvim vrstama kibernetičkih napada.

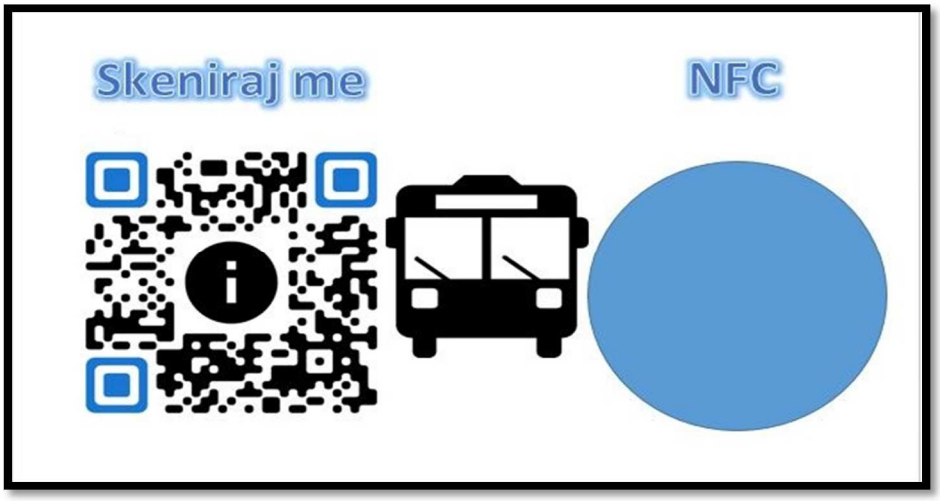
Vremenski period istraživanja u kojemu su se prikupljali podaci te provodila statistička analiza skeniranih QR kodova i NFC oznaka jest od 10. lipnja do 10. srpnja 2023 godine.

QR kodovi i NFC oznake smješteni su zajedno na pojedinoj naljepnici, razlog tome je sama jednostavnost pri implementiranju. Nadalje, naljepnice koje se koriste u ovome radu su samoljepljive papirnate naljepnice koje su naknadno plastificirane kako bi mogle odolijevati različitim vanjskim vremenski uvjetima. Različite dizajni naljepnica i QR kodova korišteni su kako bi bila privučena određena skupina korisnika kojima je namijenjena. Prilikom osmišljavanja dizajna naljepnica pazilo se da su unutar zakonskih regulativa te tako naljepnice nisu smjele predstavljati na nešto šta nisu te se nisu smjele implementirati ikone različitih postojećih tvrtki. U istraživanju su korišteni pet različitih dizajna naljepnica za pojedine slučajeve. Tako su osmišljene i dizajnirane naljepnice za parkirališne aparate prikazano na slici 4, tramvajske stanice (Slika 5), autobusne stanice (Slika 6), stanice za vlak i HŽ aparati za kupovinu karata (Slika 7) te punionice za električne automobile (Slika 8).

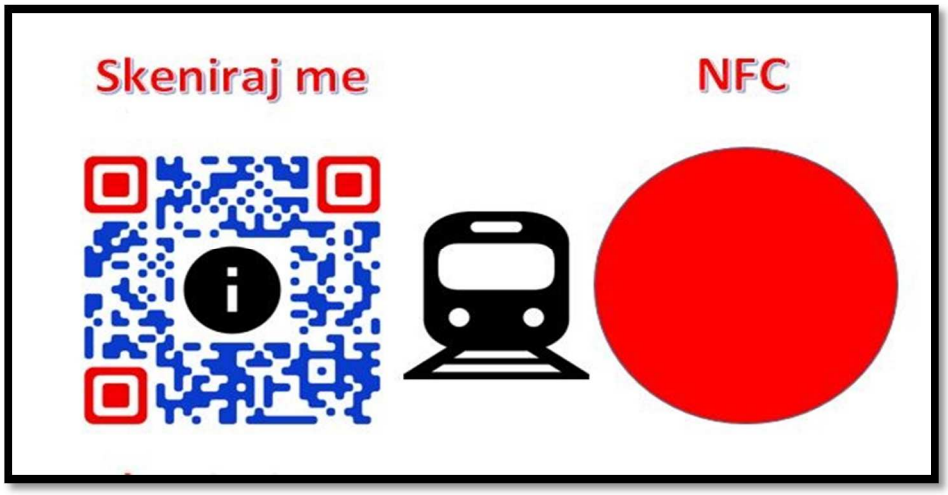
Slika 4. Naljepnica korištena za parkirališne aparate



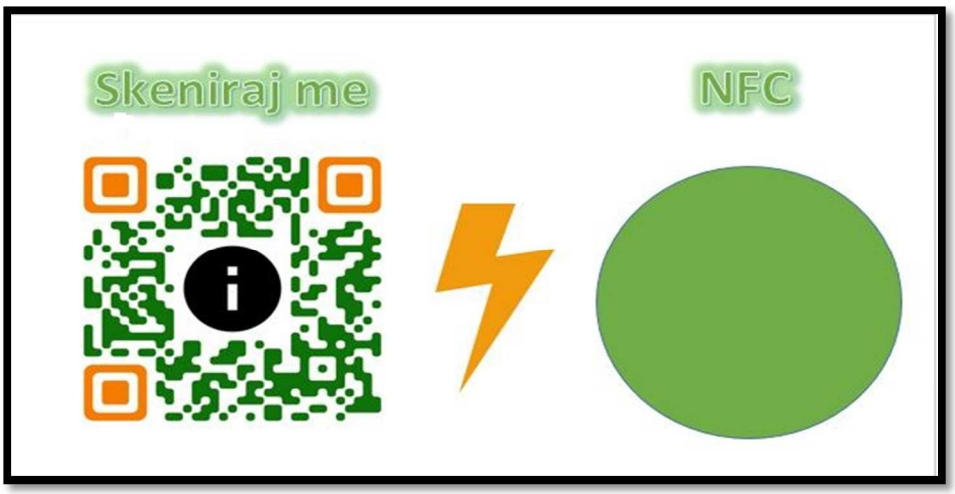
Slika 5. Naljepnica korištena za tramvajske stanice



Slika 6. Naljepnica korištena za autobusne stanice

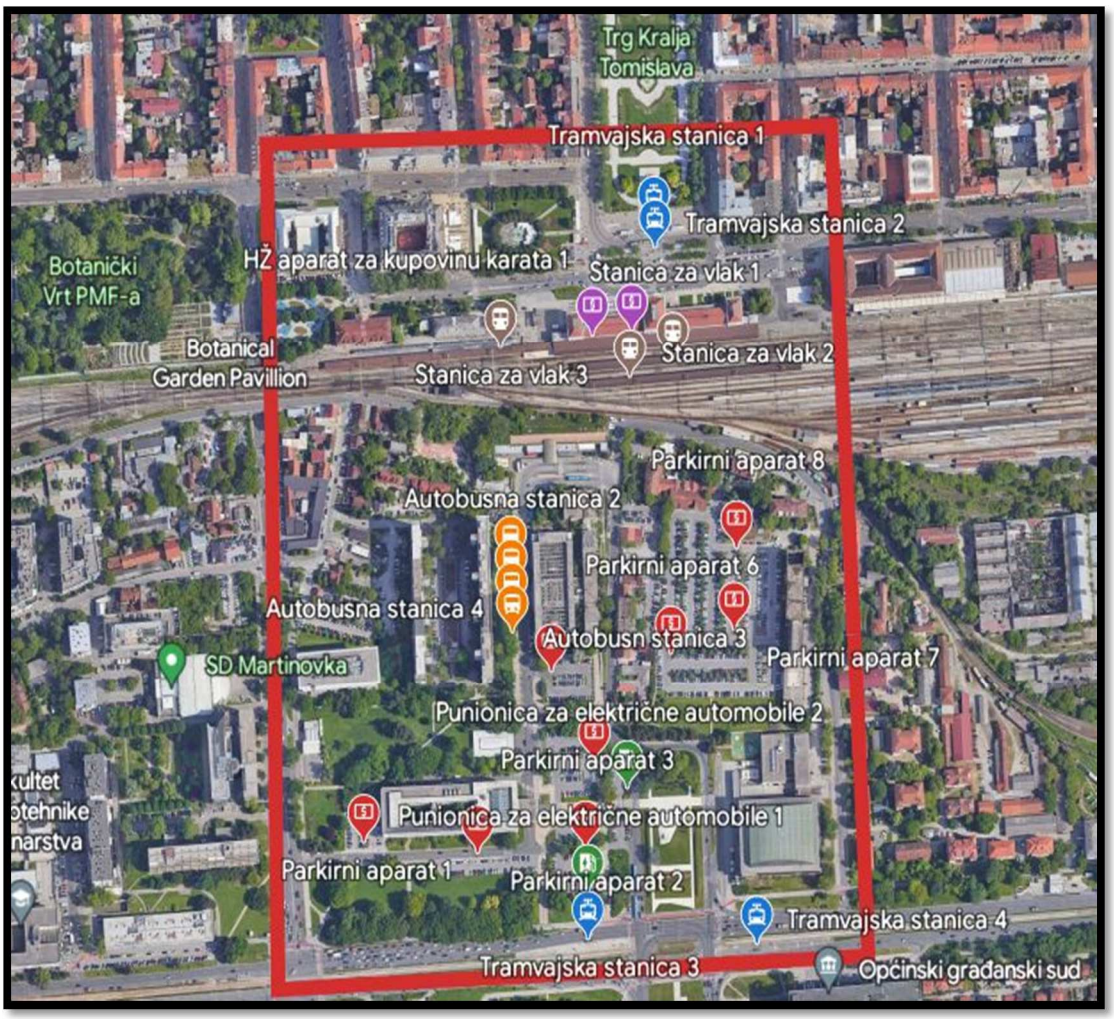


Slika 7. Naljepnica korištena za HŽ aparate i perone



Slika 8. Naljepnica korištena za punionice za električna vozila

Područje koje je odabrano za provedbu ovoga istraživanja sastoji se od Trga kralja Tomislava, Glavnog kolodvora, parkirališta Paromlin te ostalih koji su grafički prikazani na slici 9. Područje istraživanja koje je označeno crvenom bojom na slici 9 odabrano je iz razloga što u tom području prometuju različiti modaliteti prijevoza kao što su osobni automobili, javni gradski prijevoz koji se sastoji od autobusa, tramvaja, te također u tom području prometuje vlak. Promatrano područje uz prethodno navedeno sadrži i značajan broj parkirališnih mjesta što čini to područje idealno za provođenje istraživanja poradi velike koncentracije ljudi. Nadalje ovo područje sadrži i dvije punionice za električne automobile.



Slika 9. Područje istraživanja

Tramvajska stanica Glavni kolodvor nalazi se između Glavnog kolodvora i Trga kralja Tomislava. Prikazana je na slici 9 kao tramvajske stanice jedan i dva (tramvajska stanica 1 za jedan smjer, te tramvajska stanica 2 za drugi smjer). Kroz ovu postaju prolaze dnevne linije 2, 4, 6, 9 i 13, te noćne 31, 33, 34. Uz pomoć voznog reda tramvajskih linija izračunato je da kroz stanicu Glavni kolodvor kroz jedan radni dan prođe otprilike 1080 tramvaja. Na tramvajskoj stanici jedan implementirane su po dvije naljepnice, također po dvije naljepnice se nalaze na tramvajskoj stanici dva.

Tramvajska stanica KD Vatroslav Lisinski smještena je na Ulici grada Vukovara, na slici 9 prikazana je kao tramvajske stanice tri i četiri (tramvajska stanica 3 za jedan smjer, te tramvajska stanica 4 za drugi smjer). Kroz ovu stanicu prolaze dnevne linije 3 i 13 sa ukupnim

tramvajskim prometom od 318 kroz jedan radni dan. Isto kao kod tramvajske stanice jedan i dva na tramvajskim stanicama tri i četiri implementirane su po dvije naljepnice.

Peron 5 označen je na slici 9 kao autobusna stanica 1. Tim peronom prometuje linija 281, Glavni kolodvor - Novi Jelkovec. Ova linija kroz jedan radni dan ima 39 odlaska te isto toliko dolaska.

Peron 4 označen je na slici 9 kao autobusna stanica 2. Tim peronom prometuje linija 268, Zagreb (Glavni kolodvor) - Velika Gorica. Ova linija kroz jedan radni dan ima 96 odlaska te sukladno tome i isti broj odlaska.

Peron 3 označen je na slici 9 kao autobusna stanica 3. Tim peronom prometuje linija 330, Zagreb (Glavni kolodvor) - Velika Gorica (brza linija). Ova linija kroz jedan radni dan ima 28 odlaska te 25 odlaska.

Peron 2 označen je na slici 9 kao autobusna stanica 4. Tim peronom prometuju linije 218 (Glavni kolodvor - Savica – Borovje) te 241 (Glavni kolodvor - Veliko Polje). Ove dvije linije zajedno kroz jedan radni dan rade ukupni promet od 58 odlaska te isto toliko odlaska.

Što se tiče obujma prometa koji proizlazi od Glavnog kolodvora Zagreb u 2017. godini putem vlaka prevezeno je 2,465,296 putnika. Sukladno tome, dnevni promet vlakova u 2017. godini iznosio je 363 (dolazaka + odlazaka). Nadalje, u vremenskom razdoblju od 04:00 do 00:00 sata, u Glavni kolodvor prosječno pristiže 9 vlakova, a otpremi se također 9. Najveća količina prometa od 17 vlakova u dolasku na Glavnom kolodvoru je između 07:00 i 08:00 sati, [41].

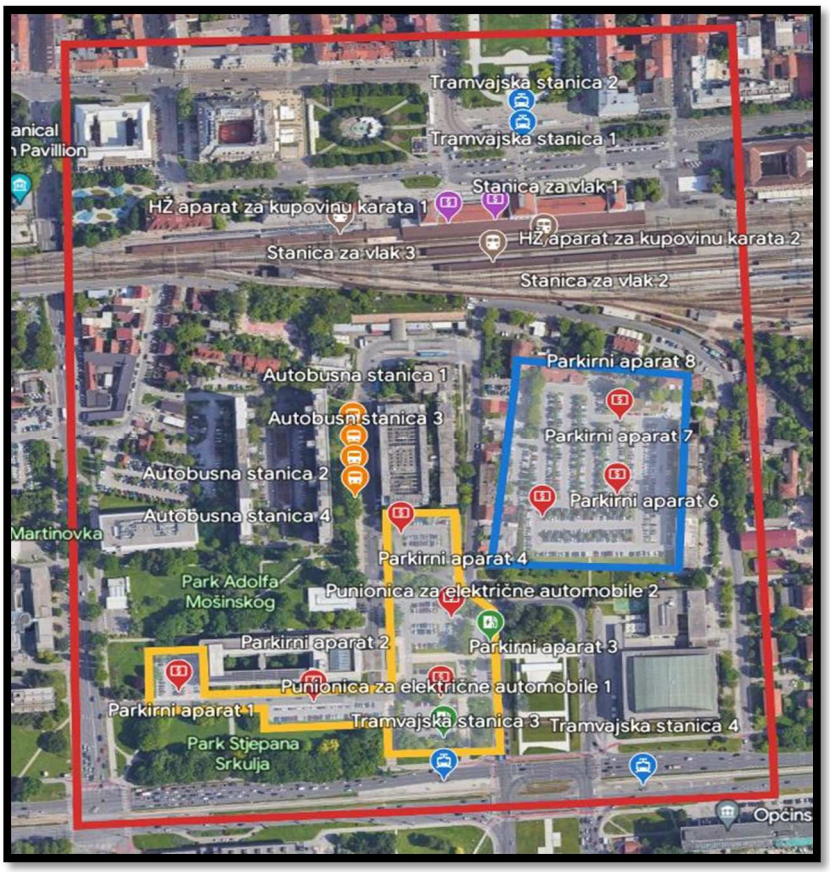
Glavni kolodvor posjeduje dva aparata za kupovinu prijevoznih karata Hrvatskih željeznica, na oba aparata implementirana je po jedna naljepnica na način da ne ograničava samu funkcionalnost aparata te na ikakav način ne otežava korisnicima njihovo korištenje. Nadalje, na peronima dva, tri, četiri, implementirane su iste naljepnica na svakom peronu po dvije.

Parkiralište Paromlin označen plavom bojom na slici 10 spada pod četvrtu zonu ZagrebParking zagrebačkog holdinga. Dnevna parkirališna karta iznosi 1.32 Eura, te maksimalno vrijeme parkiranja nije ograničeno kao što je slučaj za prve i druge parkirališne zone. SMS kod kako bi korisnici mogli kupiti kartu jest 700107. Broj parkirnih mjesta je

izračunat putem satelitske snimke *Google Earth-a* te iznosi okvirno 660 mjesta. Unutar parkirališta Paromlin nalaze se tri aparata za kupovinu parkirališnih karata. Na svaki od aparata implementirana je po jedna naljepnica na takav način sa kojim ne ugrožava funkcionalnosti aparata.

Slika 10. Parkiralište Paromlin

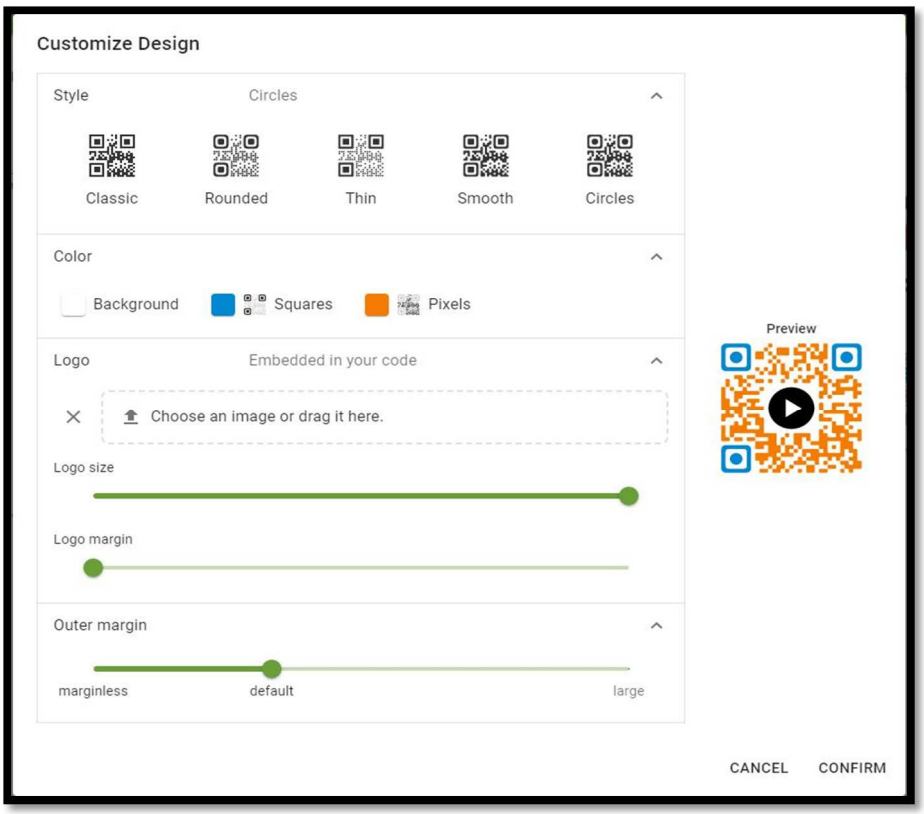
Parkiralište Paromliska cesta označeno na slici 11 žutom bojom spada pod drugu zonu ZagrebParking zagrebačkog holdinga. Parkirališna karta po jednome satu iznosi 0,70 Eur/h, te za razliku od Parkirališta Paromlin ima ograničeno maksimalno vrijeme parkiranja automobila u vremenu od 3 sata. Kao i u slučaju parkirališta Paromlin broj parkirnih mjesta je izračunat putem satelitske snimke *Google Earth-a* te iznosi okvirno 330 mjesta. Unutar područja parkirališta Paromlinska cesta nalazi se po pet aparata za kupovinu parkirališnih karata. Naljepnice su implementirane na isti način kao što je slučaj unutar parkirališta Paromlin. Također, unutar parkirališta Paromlinska cesta nalaze se dvije punionice za električna vozila. Te dvije punionice mogu istodobno puniti i do dva električna automobila. Na svaku punionicu je implementirana po jedna naljepnica isto kao i prethodne na način da ne ograničavaju njihove funkcije i korištenje.



Slika 11. Parkiralište Paromlinska cesta

4.1 Primjena QR kod tehnologije u svrhu istraživanja

Za kreiranje QR kodova korišten je besplatni alat dostupan na internetu pod nazivom QR Code Generator. Ovaj alat omogućuje kreiranje statičkih ali istovremeno i kreiranje dinamičkih QR kodova. Unutar QR koda moguće je isprogramirati jedan ili više URL-ova, tekst, telefonske brojeve, PDF (engl. *Portable Document Format*) datoteke, predložak elektroničke pošte te predložak SMS (engl. *Short Message Service).* Također, QR kodove unutar alata je moguće stilizirati po želji.



Slika 12. Sučelje QR Code Generator za uređivanje QR kodova

Slika 12 prikazuje sučelje alata QR Code Generator koji služi za uređivanje QR kodova. Putem sučelja moguće je odabrati stil sa kojim će biti QR kod generiran. Korisniku je dano na biranje pet različitih stilova klasično, zaobljeno, usko, glatko te kružno. Nadalje, korisnik unutar sučelja može mijenjati pozadinsku boju, boju kvadrata QR koda te također i boju piksela. Pri odabiru boja korisnik treba biti oprezan da boje imaju što veći kontrast međusobno kako bi senzor kamere uređaja što lakše moga skenirati QR kod. Također, unutar sučelja korisnik može umetnuti sliku po želji na svoj QR kod te odabrati količinu prostora koja će ta slika zauzimati na QR kodu. Za potrebe ovoga istraživanja kreirano je pet različitih QR kodova ovisno o mjestu gdje će biti implementirani i vrsti korisnika kojima ti QR kodovi trebaju privući pažnju da ih sa svojim uređajem skeniraju. Sukladno tome kreirani su QR kodovi za autobusne stanice, parking aparate, tramvajske stanice, punionice za električna vozila te HŽ aparati i peroni.

Slika 13. QR kod autobusna stanica

Slika 13 prikazuje dizajn QR koda dizajniranog za implementiranje na autobusne stanice sa ciljem da privuče što veći broj korisnika. Boje plava i crna su odabrane zato što čine dobar kontrast ali i ujedno plavu boju koristi javni gradski prijevoz (ZET) prema kojemu se ravnao iznad prikazan QR kod kako bi izgledao što legitimnije.

Uz samo kreiranje statičkih i dinamičkih QR kodova ovaj alata između ostalog ima i funkciju statistike napravljenih QR kodova. Neki od statističkih podataka koje je moguće pratiti jest ukupan broj skeniranog koda od kada je kreiran, ukupan dnevni broj svih skeniranih QR kodova, praćenje broja dnevnog skeniranja pojedinog QR koda te državu i grad u kojoj je QR kod skeniran ovisno o zadnjoj lokaciji pohranjenoj na uređaju korisnika.

Za potrebe istraživanja na QR kodove iskorištene za ovo istraživanje programiran je URL koji vodi korisnike do ankete napravljene uz pomoć alata Google Forms. Više o samoj anketi i alatu Google Forms objašnjeno je u potpoglavlju „4.3 Rezultati istraživanja“.

4.2 Primjena NFC tehnologije u svrhu istraživanja

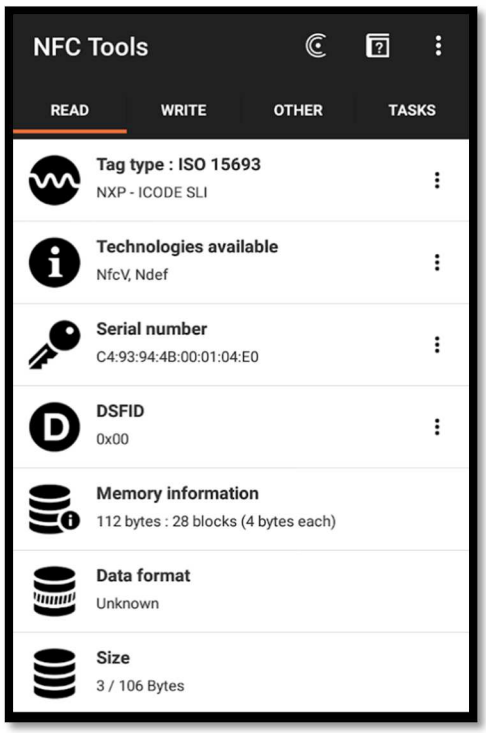
U svrhu istraživanja osim QR kod tehnologije korištena je i NFC tehnologija. NFC oznake koje su programirane u svrhu istraživanja kriju se ispod naljepnica korištenih u ovom istraživanju prikazanih na slikama (Slika 4), (Slika 5), (Slika 6), (Slika 7), (Slika 8), smještene su iza obojanog kruga te ispod riječi „NFC“. Razlog prekrivanja NFC oznaka ispod naljepnica jest smanjenje mogućnosti oštećivanja te otuđivanja samih oznaka. NFC oznaka korištena u svrhu ovoga istraživanja jest ISO 15693 NXP-ICODE SLI te je prikazana na slici 14.

Slika 14. NFC oznaka ISO 15693

Izvor: [42].

Razlog korištenja ovoga tipa NFC oznake jest poradi njezine tankoće, samoljepljivosti i tehničkih specifikacija koje su dostatne u svrhu ovoga istraživanja. Njezina tankoća je skoro pa neprimjetna kada je implementirana ispod naljepnica korištenih u ovome istraživanju.

Aplikacija NFC Tools i pametni uređaj Sony Xperia Z1 Compact korišteni su u svrhu programiranja NFC oznaka prethodno navedenog tipa. Aplikacija NFC Tools je besplatna aplikacija koja se može skinuti putem Trgovina Play na android uređajima. Slika 15 prikazuje sučelje NFC Tools aplikacije.



Slika 15. Sučelje NFC Tools aplikacije

Unutar aplikacije postoji opcija „*Read*“ prikazano na slici 15 koja omogućava čitanje tehničkih specifikacija skenirane NFC oznake kao što je vrsta oznake, tehnologije sadržane unutar oznake, serijski broj oznake, informacija o memoriji oznake, mogućnost interakcije sa oznakom te mnoge druge informacije od oznake. Nadalje, funkcija „*Write*“ unutar aplikacije omogućava programiranje oznake sa raznim opcijama. Neke od mogućnosti su dodavanje teksta na oznaku, URL- ova, datoteka, predložak elektroničke pošte i SMS-a, telefonskog broja, lokaciju. Također, moguće je programirati oznaku da komuniciraju sa komponentima na uređaju kao što je Buethooth, Wi-Fi, kamera, mikrofon, zaslon te ostale komponente uređaja koji skeniraju oznaku.

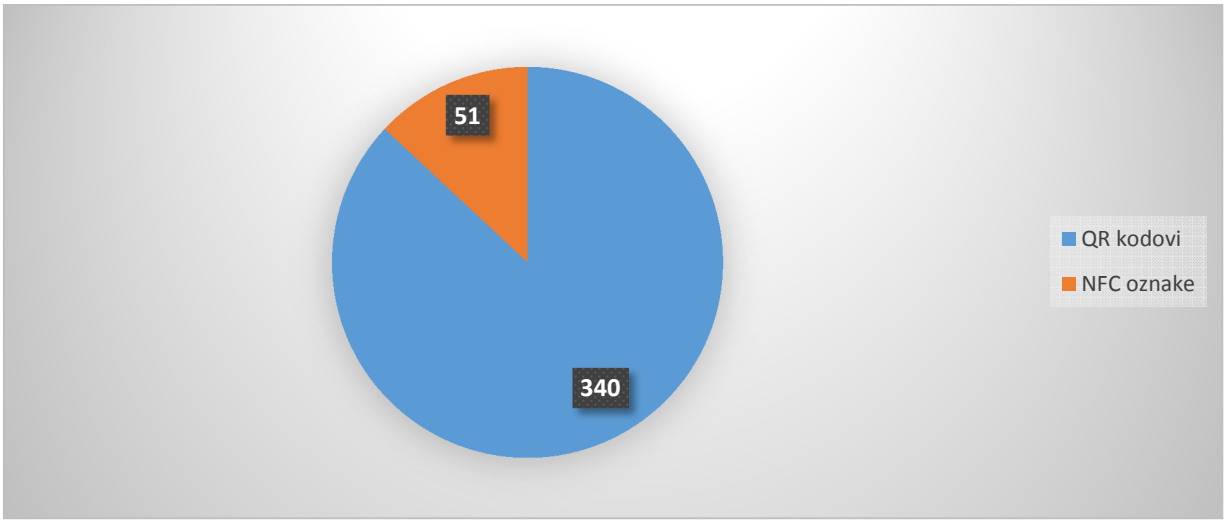
NFC oznake se sa NFC Tools aplikacijom programiraju tako što se unutar aplikacije odabere opcija „*Write*“ gdje je korisnik prethodno odabrao koje mogućnosti želi programirati na oznaku. Potom korisnik odabere funkciju „*Write*“ te približi oznaku prema stražnjoj strani uređaja. Nakon nekoliko trenutaka aplikacija prikazuje tekstualnu poruku gdje obavještava korisnika da je programiranje prošlo uspješno ili neuspješno ovisno o situaciji.

Za razliku od QR koda gdje je programiran URL od jedne ankete kreirane na Google Forms alatu kojim je vršeno anketiranje, za potrebe NFC anketiranja korišten je alat

LimeSurvey. Razlog zbog čega je korišten drugi alat za anketiranja jest uočen problem pri prikupljanja broja skeniranih NFC oznaka. Oznake korištene u ovome istraživanju nemaju mogućnost kao i QR kodovi za praćenje broja skeniranja. Bitna razlika između alata Google Forms i LimeSurvey jest ta da LimeSurvey ne zapisuje samo ispunjene ankete nego i ne ispunjene ankete to jest korisnik nije primoran ispuniti anketu kako bi se uočila aktivnost na anketi. Za potrebe ovoga istraživanja kreirano je pet anketa iste po sadržaju ali sa različitim pristupnim URL-om kako bi se mogla voditi statistika o broju skeniranih NFC oznaka za pojedine slučajeve. Više o sadržaju te statističkim podacima te ankete objašnjeno je u sljedećem potpoglavlju.

4.3 Rezultati istraživanja

Rezultati istraživanja praćeni su uz pomoć alata za kreiranje i analizu anketa Google Forms i LimeSurvey. Za vrijeme trajanja istraživanja od 10. lipnja do 10. srpnja 2023 godine jedanput je vršena provjera stanja naljepnica dana 21. lipnja 2023 godine. Prilikom provjere utvrđeno je da su većinom sve naljepnice u dobrom stanju i netaknute osim onih koje su bile implementirane na parkirališnim aparatima. Iz nekoga razloga naljepnice na svim parkirališnim aparatima bile su uklonjene te se to može primijetiti na grafu 4 gdje se vidi smanjenje broja skeniranih QR kodova parkirališnih aparata. Sukladno tome naljepnice su zamijenjene sa novima te se više nisu vršile provjere nad naljepnicama niti njihovo nadomještanje. Sveukupni broj skeniranih QR kodova i NFC oznaka jest 391, od čega je 340 skeniranih QR kodova, a 51 je ukupno skeniranih NFC oznaka.



Graf 1. Prikaz broja ukupno skeniranih QR kodova i NFC oznaka

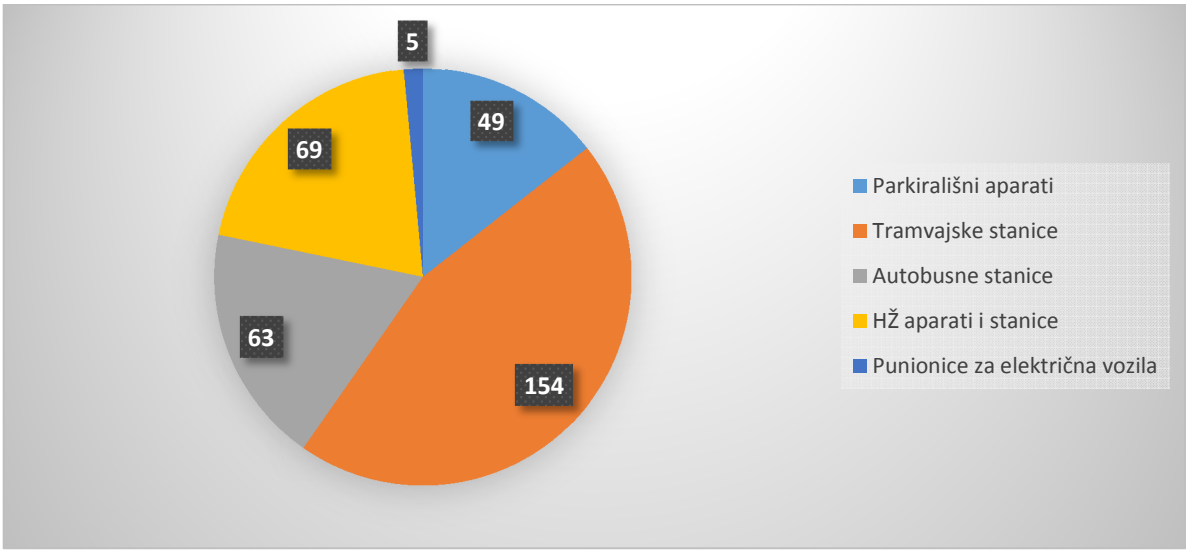
Graf 1 grafički prikazuje broj skeniranih QR kodova i NFC naljepnica gdje se može primijetiti kako dominiraju skenirani QR kodovi.

Za potrebe istraživanja sudionici su sudjelovali u lažnoj kibernetičkoj prijetnji tehnologija kratkog dometa koja je igrom slučaja itekako mogla biti prava prijetnja. Jedna od glavnih prijetnji kibernetičkih napada ovakvog tipa su socijal inženjering napadi koji su opisani u potpoglavlju 2.3 Socijalni inženjering napadi. Također, prijetnje kojima su sudionici mogli biti izloženi su sigurnosne prijetnje NFC tehnologije kao što su: prisluškivanje, oštećenje podataka, manipulacija ili presretanje koji su detaljnije opisani u pod potpoglavlju 3.1.3 Sigurnost NFC tehnologije. Nadalje, prilikom skeniranja QR kodova sudionici su mogli biti uključeni u kibernetičke napade QR kodova opisanim u pod potpoglavlju 3.2.3 Sigurnost QR kod tehnologije.

4.3.1 Rezultati skeniranih QR kodova i ankete Google Forms

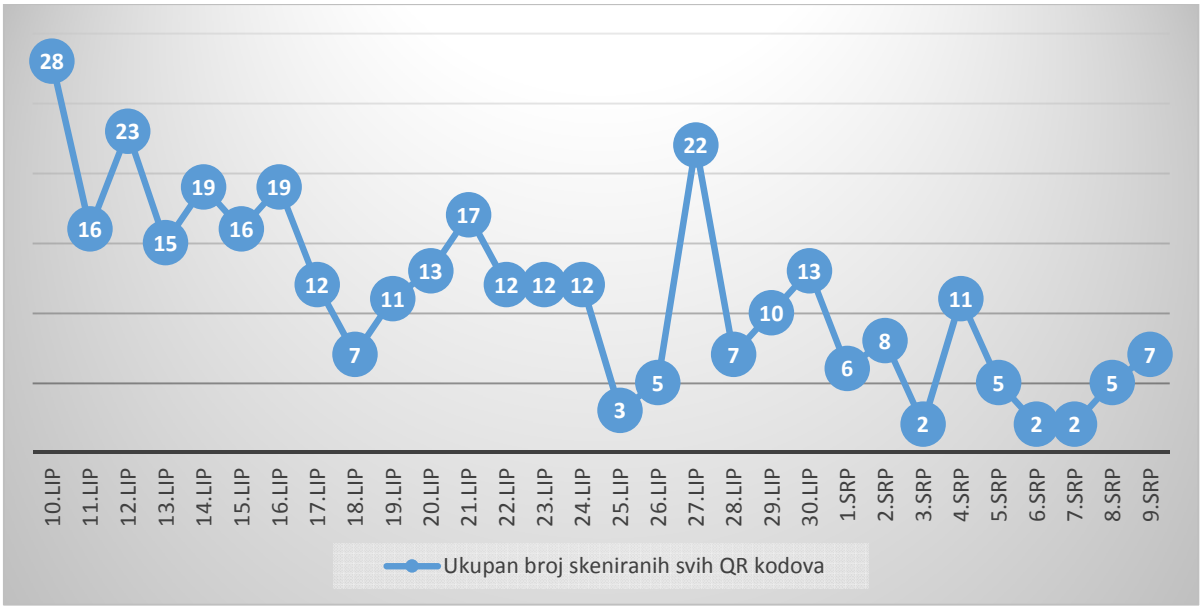
Ukupni broj skeniranih QR kodova iznosi 340, od čega 49 iznosi broj skeniranih naljepnica od parkirališnih aparata, 63 autobusnih stanica, 154 tramvajskih stanica, 69 HŽ peroni i aparati za kupovinu karata te 5 punionica za električne automobile. Graf 2 grafičkih prikazuje iznad navedene podatke te se može primijetiti kako najviše ima skeniranih QR kodova sa tramvajskih stanica dok QR kodovi koji se nalaze punionicama za električna vozilima

ima najmanji broj. Prilikom provedbe istraživanja bilo je očekivano manji broj skeniranja QR kodova punionica za električna vozila pošto se samo dvije nalaze na području istraživanja.



Graf 2. Broj skeniranih QR kodova

U nastavku poglavlja sadržani su grafovi koji ukazuju na broj skeniranih pojedinih QR kodova po danima.

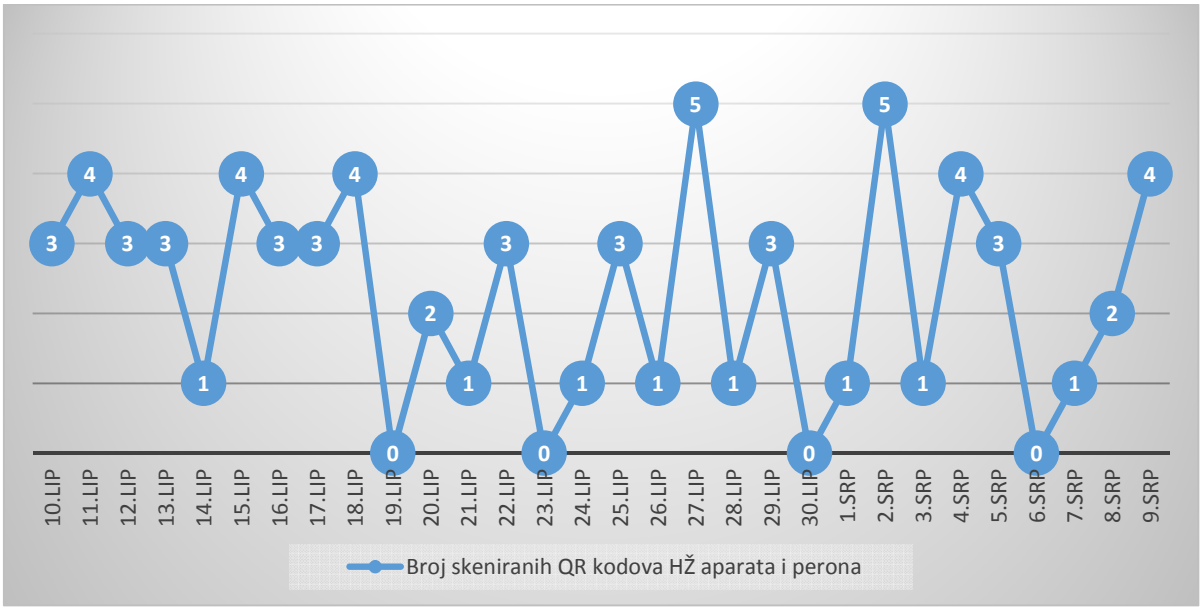


Graf 3. Ukupan broj skeniranih svih QR kodova po danima

Graf 3 prikazuje ukupan broj skeniranih svih QR kodova po danima. Na grafu se može uočiti kako 10. Lipnja bio najveći broj skeniranih QR kodova od 28 skeniranja, a 3, 6 i 7. Srpnja najmanji broj skeniranih QR kodova u iznosu od 2 skeniranja. Također, iz grafa se može uočiti kako nakon 21. Lipnja prosječni broj skeniranja QR kodova je manji. Mogući razlog tome je što je završila nastavna godina te sukladno tome došlo je do manjeg broja skeniranja QR kodova.

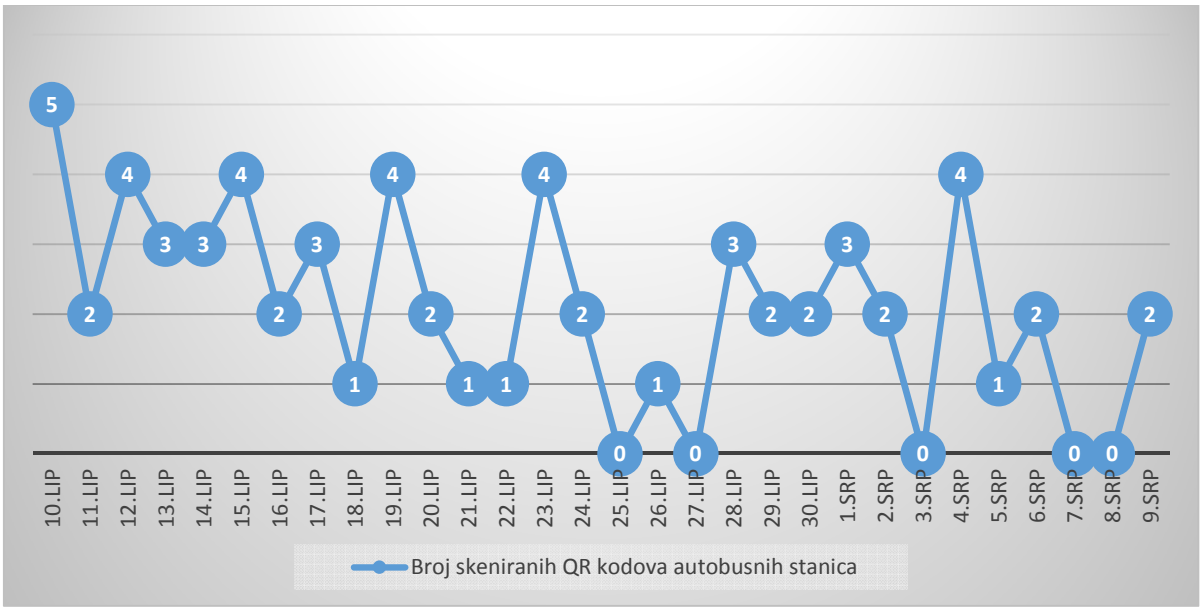
Graf 4. Broj skeniranih QR kodova parkirališnih aparata po danima

Prema podacima iz grafa 4 najveći broj skeniranih QR kodova parkirališnih aparata jest 10.Lipnja, dok dana 18,19,22,23,25,26,27,28,29,30. Lipnja te 1,2,3,4,5,6,7,8,9. Srpnja najmanji broj skeniranja. Razlog malom broju skeniranja jest uklanjanje naljepnica od strane treće osobe.



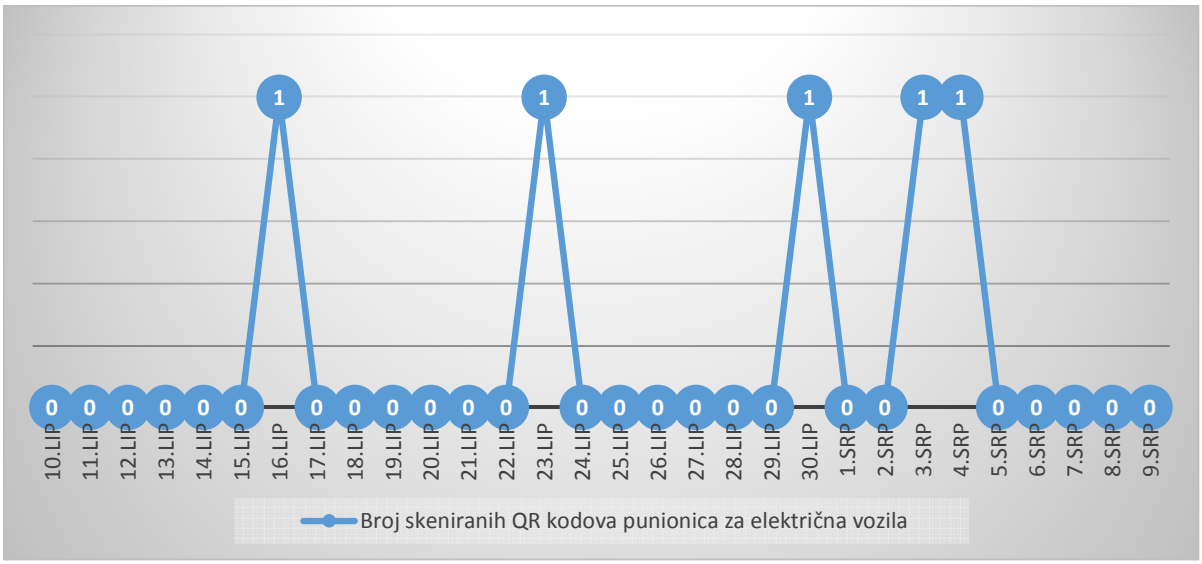
Graf 5. Broj skeniranih QR kodova HŽ aparata i perona po danima

Graf 5 prikazuje broj skeniranih QR kodova HŽ aparata i perona po danima te se može uočiti da krivulja nema neki obrazac ponašanja. Dana 19,23,30. Lipnja, te 6. Srpnja najmanji je broj skeniranih QR kodova, dok dana 27. Lipnja te 6. Srpnja najveći broj skeniranja.



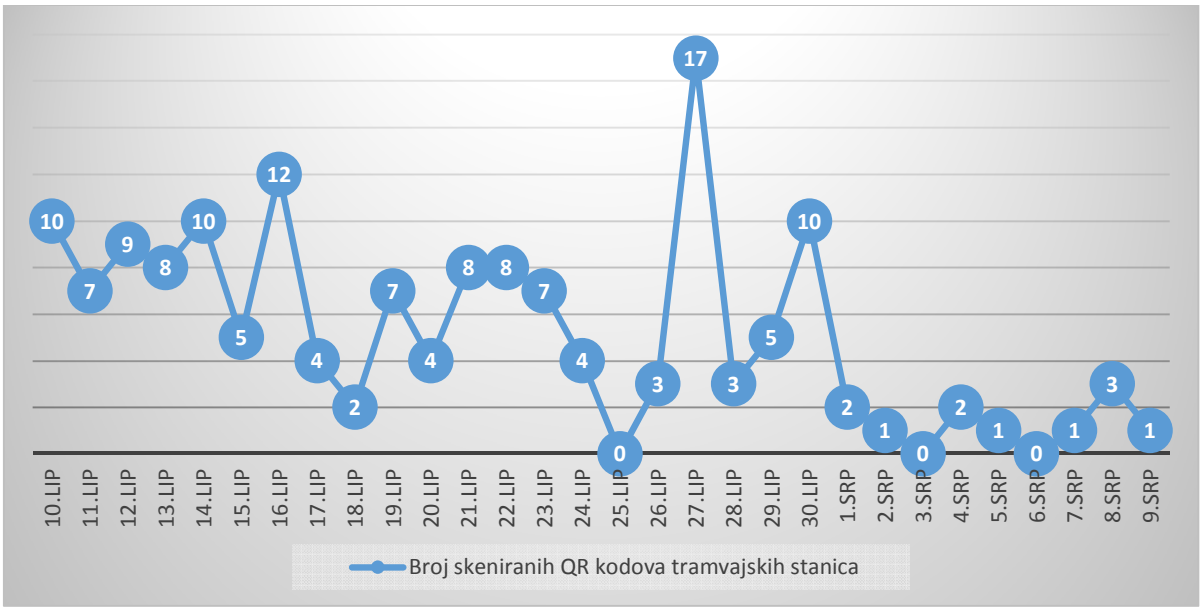
Graf 6. Broj skeniranih QR kodova autobusnih stanica po danima

Prema podacima iz grafa 6, može se uočiti kako 10. Lipnja je najveći broj skeniranih QR kodova, dok dana 25, 27. Lipnja, ta 3,7,8. Srpnja najmanji broj skeniranih QR kodova autobusnih stanica. Također, može se uočiti kako nakon 21. Lipnja smanjuje se dnevni broj skeniranja QR kodova.



Graf 7. Broj skeniranih QR kodova punionica za električna vozila po danima

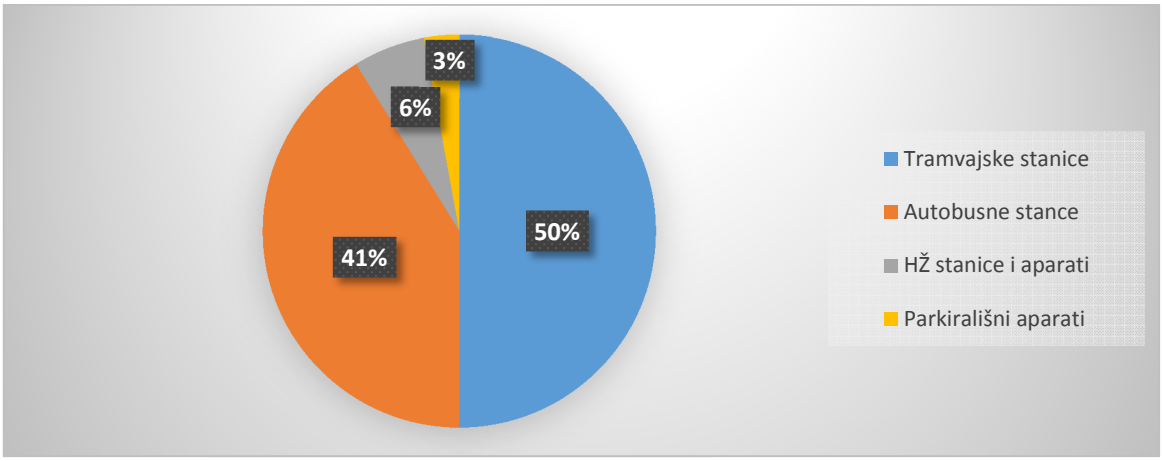
Graf 7 prikazuje broj skeniranih QR kodova punionica za električna vozila po danima. Na grafu se može uočiti kako su QR kodovi rijetko skenirani te da dnevni broj skeniranja QR kodova ne prelazi preko jedan.



Graf 8. Broj skeniranih QR kodova tramvajskih stanica po danima

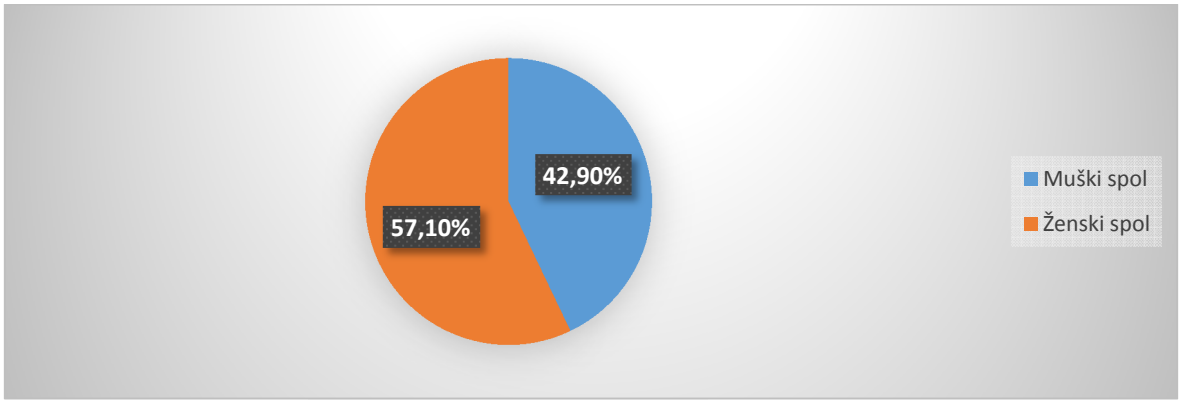
Graf 8 prikazuje broj skeniranih QR kodova tramvajskih stanica po danima te su ujedno ti QR kodovi najviše puta skenirani. Dana 27. Lipnja je najveći broj skeniranih QR kodova i iznosi 17 skeniranja, dok dana 25. Lipnja, ta 3,6 .Srpnja najmanji broj skeniranih kodova.

Za vršenje anketiranja korisnika koji su skenirali QR kod korištena je anketa Google Forms. Anketa se sastoji od 11 pitanja koja bi trebala stvoriti sliku o profilu korisnika. Anketu je ispunilo ukupno 35 korisnika što čini 10 % od ukupno skeniranih QR kodova. Nadalje većina korisnika koji su odgovorili na anketu skenirali su QR kod na tramvajskim stanicama i iznosi 50%. Poslije tramvajskih stanica slijede QR kodovi autobusnih stanica sa 41%, potom HŽ stanice i aparati za kupovinu karata sa 6% te parking aparati sa 3%. Te je sve grafički prikazano na grafu 9.



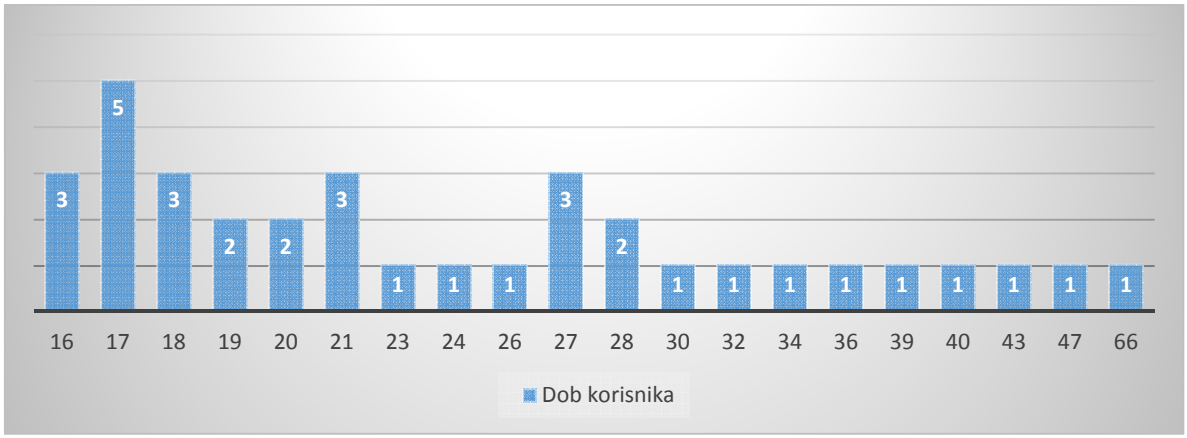
Graf 9. Grafički prikaz skeniranih QR kodova od strane korisnika koji su ispunili anketu

Nadalje, od 35 korisnika koji su odgovorili na anketu 57% je bilo ženskog spola dok je 43% bilo muškog spola. Te je grafički prikazano na grafu 10. Veći postotak odgovora ženskog spola ne mora značiti da ženski spol više podliježe socijal inženjering prevarama nego možda samo da su voljnije ispuniti anketu.



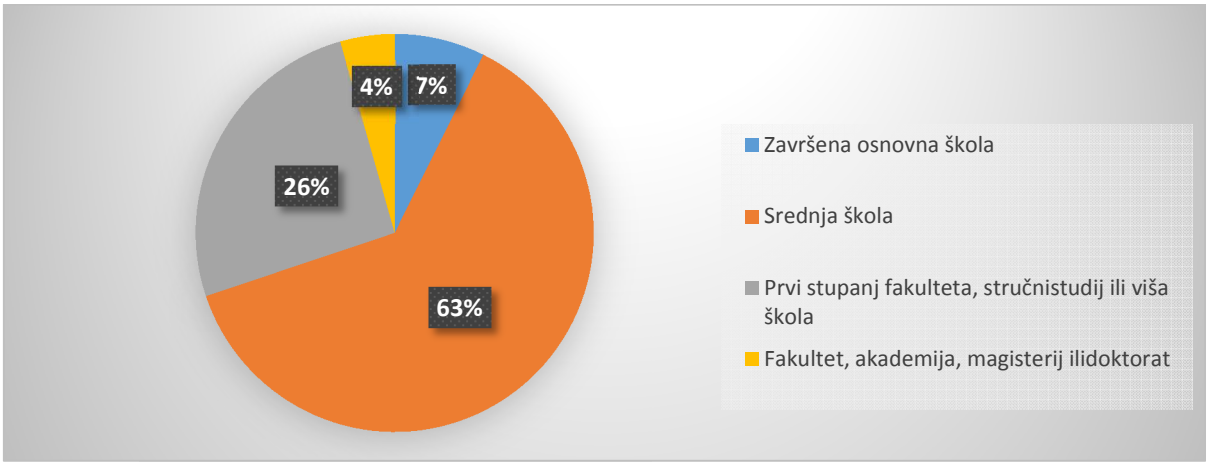
Graf 10. Spolovi korisnika koji su ispunili anketu za QR kodove

Također, unutar ankete pitalo se korisnika za njihovu dob. Graf 11 prikazuje dob korisnika koji su ispunili anketu. Na grafu se može primijetiti kako je široki raspon godina uključen od 16 do 66 godina. Nadalje, najveći broj korisnika koji su ispunili anketu imali su 17 godina.



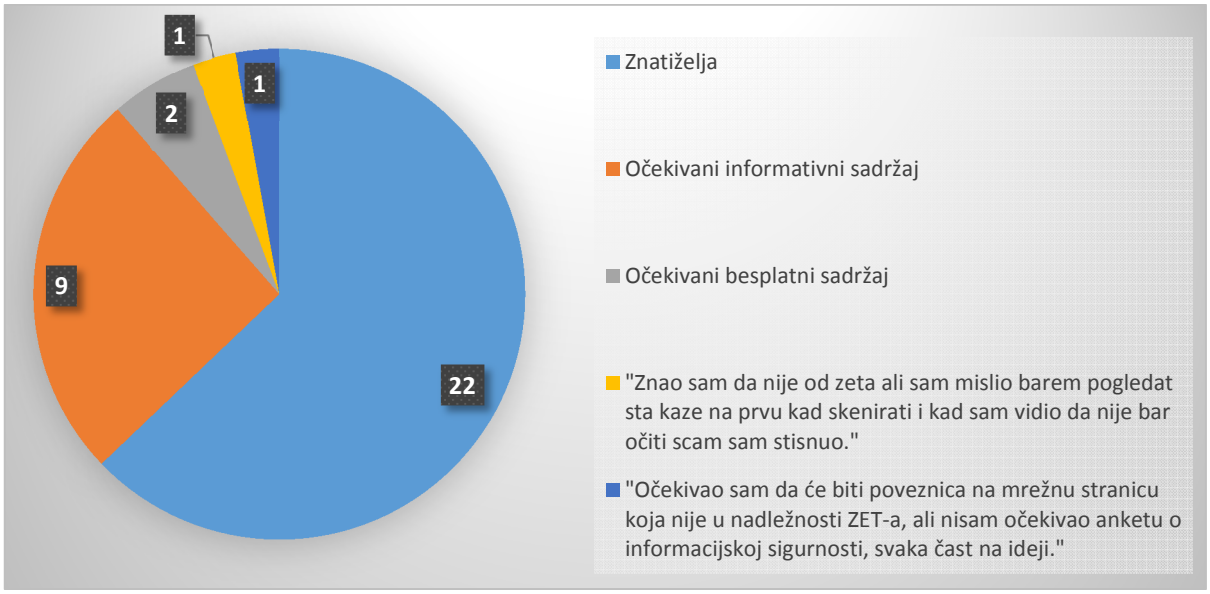
Graf 11. Dob korisnika koji su ispunili anketu za QR kodove

Također, jedno od pitanja unutar ankete jest da korisnici napišu svoj stupanj obrazovanja. Od 35 korisnika 2 ih je završilo osnovnu školu, 17 srednju školu, 7 prvi stupanj fakulteta, stručni studij ili viša škola te 9 ima završeno fakultet, akademiju, magisterij ili doktorat. Sve to grafički je prikazano na grafu 12.



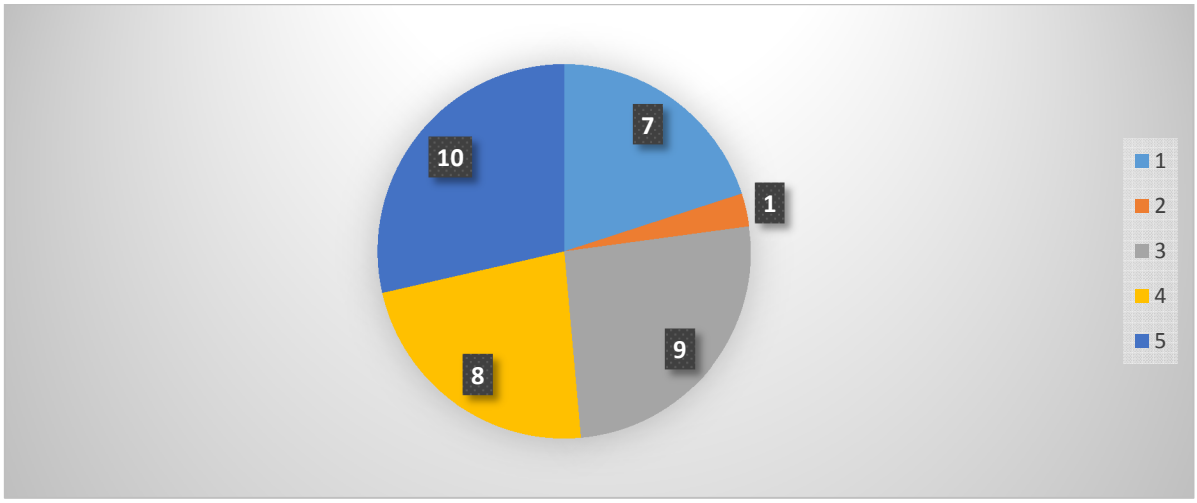
Graf 12. Stupanj obrazovanja korisnika koji su ispunili anketu za QR kodove

Unutar ankete korisnike se pitalo da odaberu ili napišu svojim riječima razlog skeniranja QR koda. Od ponuđenih odgovora imali su za odabrati: znatiželja, očekivao sam besplatni sadržaj, očekivao sam informativni sadržaj, očekivao sam neki vid nagrade te su korisnici imali opciju da sami upišu svoj razlog. Graf 13, grafički prikazuje odgovore na pitanje.



Graf 13. Razlog skeniranja QR kodova

Nadalje, korisnike je pitano da prema svojem mišljenju odgovore koliko su svjesni o negativnom utjecaju kibernetičkih prijetnji te su imali na izbor od 1 - Uopće nisam svjestan do 5 - Potpuno sam upoznat sa mogućim prijetnjama. Graf 14 grafički prikazuje rezultate pitanja te se može primijetiti kao je najviše odgovorilo kako su potpuno svjesni o mogućim kibernetičkim prijetnjama.



Graf 14. Osviještenost korisnika o kibernetičkim prijetnjama

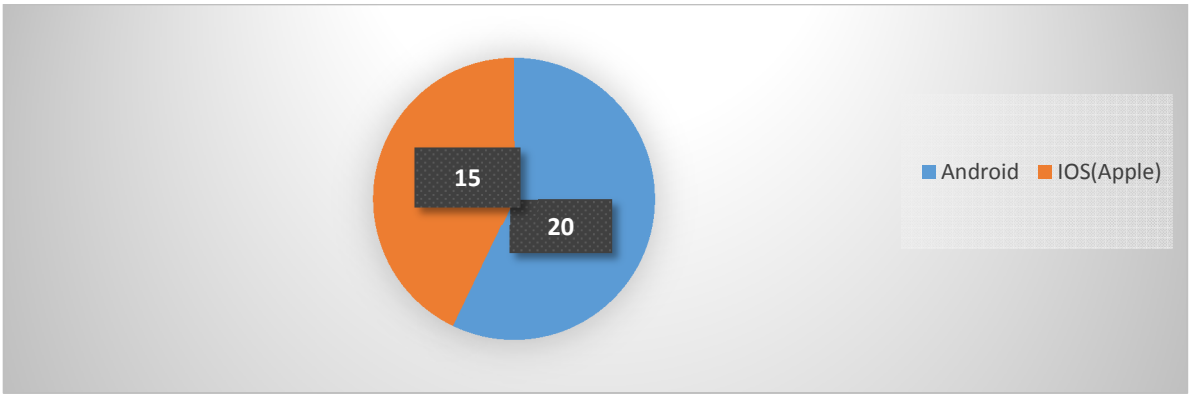
Također, unutar anketa postoje 4 kratka pitanja sa „DA“ i „NE“ odgovorima. Pitanja i njihovi rezultati nalaze se na tablici 2.

Tablica 2. Četiri pitanja QR kod ankete vrste odgovora: DA/NE

Pitanje	Odgovor DA	Odgovor NE
Smatrate li da znate prepoznati kibernetičke prijetnje?	19 ili 54.3%	16 ili 45,7%
Jeste li upoznati sa terminom "Socijalni inženjering"?	15 ili 42,9%	20 ili 57.1%
Jeste li upoznati sa terminom "*Phishing*"?	21 ili 60%	14 ili 40%
Smatrate li da znate kako prevenirati napade QR kod i NFC tehnologija?	11 ili 31.4%	24 ili 68.6%

Prema podacima iz tablice 2 može se zaključiti kako većina korisnika smatra da zna prepoznati kibernetičke prijetnje. Nadalje, kako je termin „Socijal inženjering“ manje poznatiji među korisnicima od termina „*Phishing*“. Također, većina korisnika smatra kako ne bi znali prevenirati napade QR kod i NFC tehnologija.

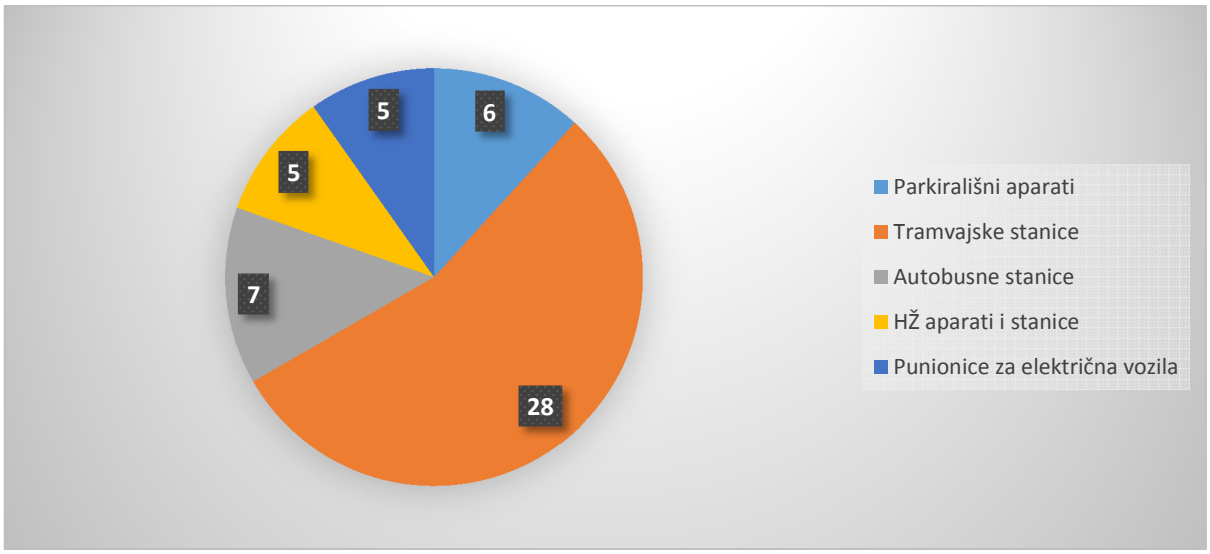
Također, jedno o pitanja koje se postavilo korisnicima bilo je da odaberu ili napišu koji operativni sustav koriste. Na izbor su imali za odabrati: Android, IOS (Apple), Linux ili su korisnici mogli sami upisati neki drugi operativni sustav. Rezultati pitanja prikazani su grafom 15.



Graf 15. Operativni sustav korisnika

4.3.2 Rezultati skeniranih NFC oznaka i ankete LimeSurvey

Ukupni broj skeniranih NFC oznaka iznosi 51, od čega 6 iznosi broj skeniranih naljepnica od parkirališnih aparata, 7 autobusne stanice, 28 tramvajske stanice, 5 HŽ peroni i aparati za kupovinu karata te 5 punionice za električne automobile. Graf 16 grafičkih prikazuje iznad navedene podatke.



Graf 16. Broj skeniranih NFC oznaka

Za potrebe QR kodova bila je dostatna samo jedna anketa, ali za potrebe praćenja NFC oznaka te kako bi se moglo razlikovati skenirani broj oznaka i anketiranja korisnika morale su se napraviti 5 anketa posebno za svaki slučaj i korišten je program za kreiranje anketa LimeSurvey. Razlog tome je što se broj skeniranih NFC oznaka nije moglo drugačije pratiti osim putem ankete. Sve ankete imaju ista pitanja kao i kod QR kodova.

Tablica 3 prikazuje listu pojedinih anketa kreiranih u programu LimeSurvey sa gledišta broja njihovog pristupanja te djelomičnog ili punog odgovaranja na njih. Ukoliko je djelomično odgovoreno znači da je korisnik skenirao NFC oznaku ali nije ispunio anketu.

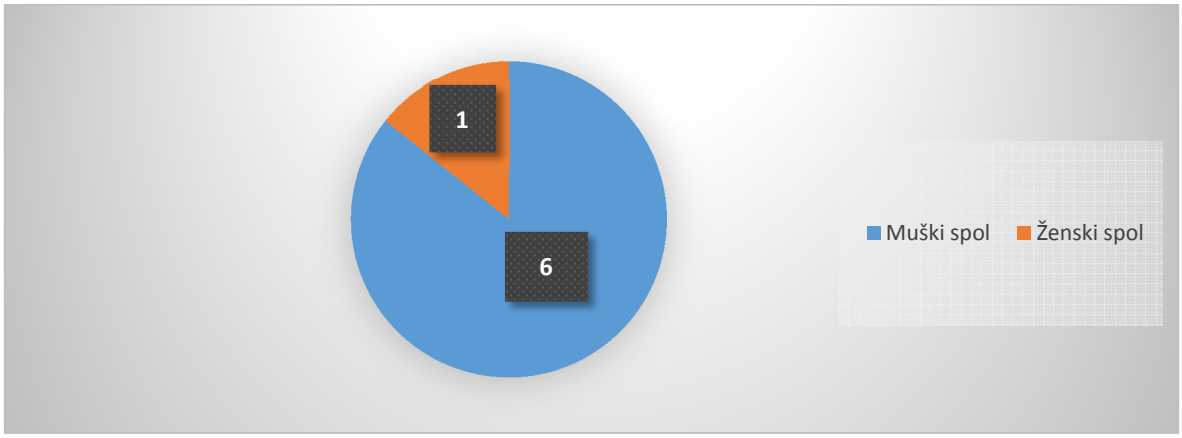
Tablica 3. Broj pristupa i ispunjenja različitih NFC anketi

Anketa	**Djelomično**	**Puno**	**Ukupno**
Parkirališni aparati	6	0	6
Tramvajske stanice	21	7	28

Autobusne stanice	7	0	7
HŽ aparati i stanice	5	0	5
Punionice električnih vozila	5	0	5

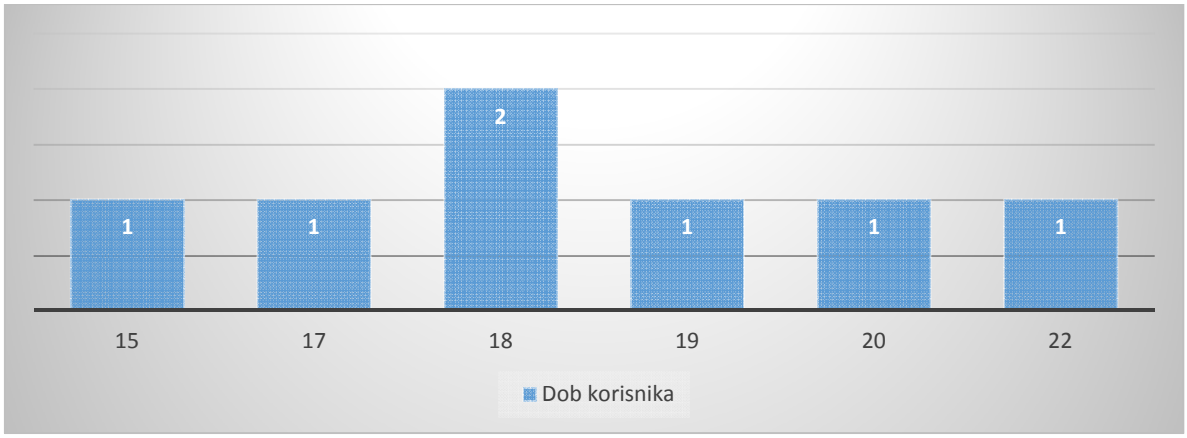
Na tablici 3 može se primijetiti da jedino anketa „Tramvajske stanice“ ima odgovorena pitanja te će sukladno tome jedino njezini odgovori biti analizirani.

Od 7 korisnika koji su odgovorili na anketu 6 je bilo muškog spola dok 1 ženskog spola. Te je grafički prikazano na grafu 17.



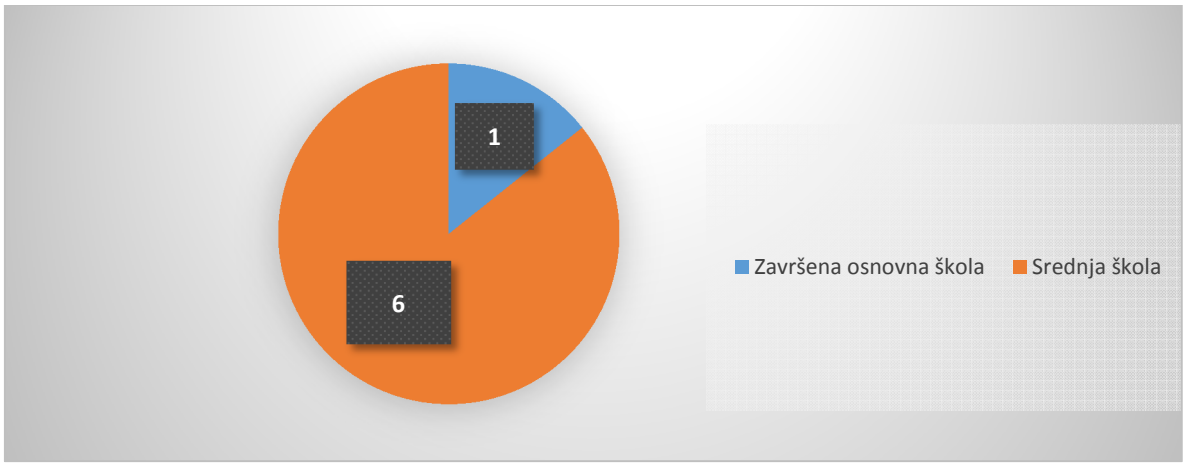
Graf 17. Spolovi korisnika koji su ispunili anketu za NFC

Nadalje, unutar ankete pitalo se za dob korisnika. Najviše skeniranih NFC oznaka jest od strane korisnika 18 godina starosti što se može vidjeti na grafu 18.



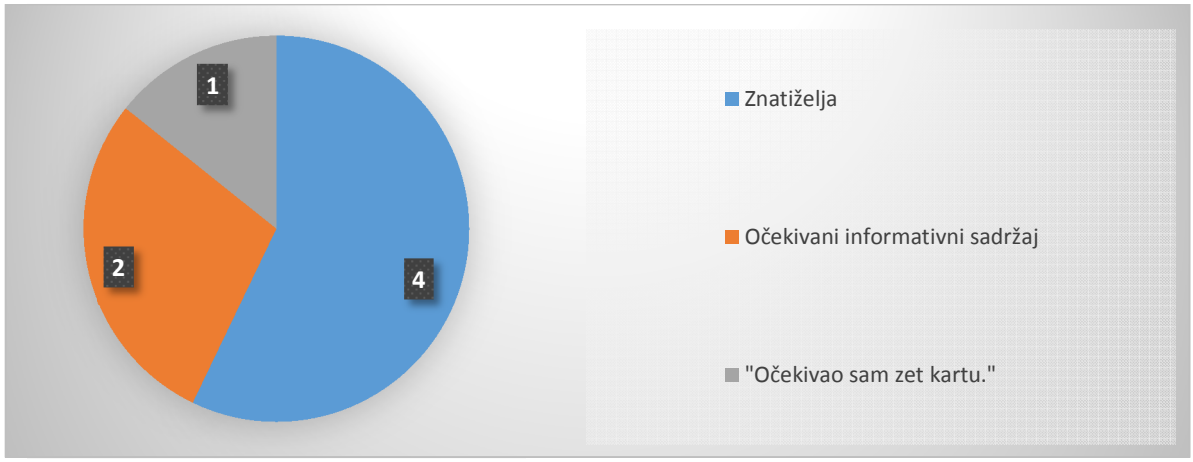
Graf 18. Dob korisnika NFC oznaka tramvajski stanica

Unutar ankete također se tražilo da korisnici napišu svoj stupanj obrazovanja. Od 7 korisnika 1 ih je završilo osnovnu školu, 6 srednju školu. Sve to grafički je prikazano na grafu 19.



Graf 19. Stupanj obrazovanja korisnika NFC ankete za tramvajske stanice

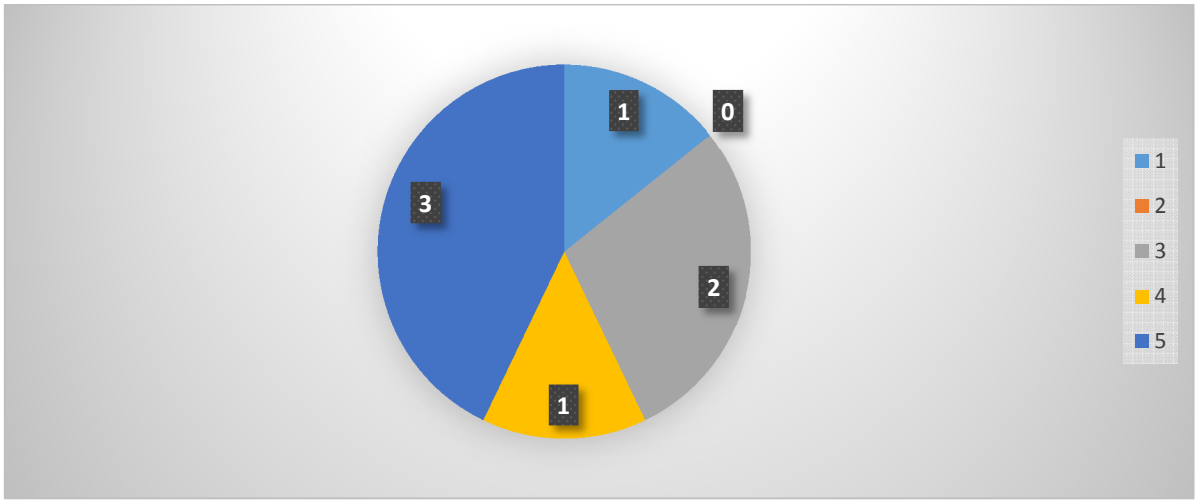
Također, unutar ankete pitalo se korisnike da odaberu ili napišu svojim riječima razlog skeniranja QR koda. Od ponuđenih odgovora imali su za odabrati: znatiželja, očekivao sam besplatni sadržaj, očekivao sam informativni sadržaj, očekivao sam neki vid nagrade te su korisnici imali opciju da sami upišu svoj razlog. Graf 20 grafički prikazuje odgovore na pitanje te se može primijetiti kako je znatiželja najveći razlog zašto su korisnici skenirali NFC oznake.



Graf 20. Razlozi skeniranja NFC oznaka za tramvajske stanice

Također, korisnike je pitano da prema svojem mišljenju odgovore koliko su svjesni o negativnom utjecaju kibernetičkih prijetnji te su imali na izbor od 1 - Uopće nisam svjestan do 5 - Potpuno sam upoznat sa mogućim prijetnjama. Graf 21 grafički prikazuje rezultate pitanja

te se može primijetiti kao je najviše odgovorilo kako su potpuno svjesni o mogućim kibernetičkim prijetnjama.



Graf 21. Svjesnost korisnika NFC ankete o utjecaju kibernetičkih prijetnji

Unutar ove ankete također postoje 4 kratka pitanja sa da i ne odgovorima. Pitanja i njihovi rezultati nalaze se na tablici 4.

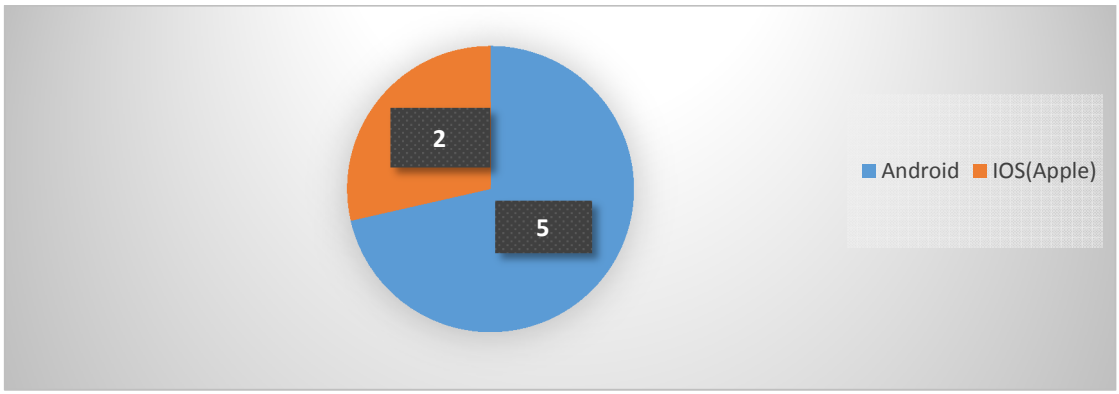
Tablica 4. Četiri pitanja NFC ankete vrste odgovora: DA/NE

Pitanje	Odgovor DA	Odgovor NE
Smatrate li da znate prepoznati kibernetičke prijetnje?	6 ili 85%	1 ili 15%
Jeste li upoznati sa terminom "Socijalni inženjering"?	3 ili 42%	4 ili 58%
Jeste li upoznati sa terminom "*Phishing*"?	6 ili 85%	1 ili 15%
Smatrate li da znate kako prevenirati napade QR kod i NFC tehnologija?	5 ili 71%	2 ili 29%

Podaci unutar tablice 4 ukazuju na to da većina korisnika misli da zna prepoznati kibernetičke prijetnje. Također, manji postotak njih je upoznat sa terminom „Socijal

inženjeringa“, za razliku od „*Phishing*“ koji većinu korisnika zna. Nadalje, većina korisnika misli kako znaju prevenirat napade QR kod i NFC tehnologija.

Također, anketa sadrži pitanje gdje se pitaju korisnici koji operativni sustav koriste. Petero njih odgovorilo je da koriste Android dok dvoje njih je odgovorilo IOS (Apple). Sve navedeno prikazano je na grafu 22.



Graf 22. Operativni sustav korisnika koji su ispunili NFC anketu

5. Prijedlozi za unaprjeđenje sigurnosti u korištenju tehnologija kratkog dometa

U današnjem sve više tehnološki razvijenom svijetu tehnologije kratkog dometa kao što su NFC, QR kodovi i njima srodne postaju neizostavni dio naše svakodnevnice. Istovremeno, s porastom korištenja ovih tehnologija dolaze i potencijalni sigurnosni izazovi. Kako bi tehnologije kratkog dometa bile što sigurnije za korištenje treba ih unaprjeđivati i educirati korisnike za njihovo korištenje. U ovome poglavlju navedeni su te istodobno i objašnjeni prijedlozi za unaprjeđenje sigurnosti u korištenju tehnologija kratkog dometa.

Edukacija korisnika jest jedan od ključnih aspekata za unaprjeđenje sigurnosti u korištenju tehnologija kratkog dometa koji se može primijeniti kod svih tehnologija kratkog dometa i općenito u svijetu kibersigurnosti. Edukacija korisnika vrlo je bitna iz razloga što korisnici često nisu svjesni potencijalnih prijetnji i sigurnosnih rizika koji mogu proizaći iz neispravnog korištenja tih tehnologija. A upravo krajnji korisnici su ti koji su često prva linija obrane od napada.

Postoje različiti načini i modeli po kojima se pružaju edukacije krajnjim korisnicima kao što su na primjer televizijske i radijske reklame, raznoliki letci, novine, oglasi, plakati i njima sličnim. Također, veliki dio edukacije se vrši putem interneta korištenjem različitih društvenih mreža kao što su facebook, instagram, youtube, forum i na još mnogim drugim društvenim mrežama.

5.1 Prijedlozi unaprjeđenja sigurnosti korištenja NFC tehnologije

Niti jedna tehnologija nije apsolutno sigurna za korištenje pa tako ni NFC tehnologija, ali se sa načinom korištenja tehnologije i određenim koracima predostrožnosti razina rizika itekako može smanjiti. U nastavku teksta objašnjeni su koraci koje bi korisnik trebao poduzeti prilikom korištenja NFC tehnologije te što napraviti ukoliko se skenira zlokobna NFC oznaka.

Prilikom korištenja NFC tehnologije korisnik se može zaštititi tako što redovno ažurira svoje pametne uređaje jer kako se problemi pojavljuju i otkrivaju, dobavljači razvijaju i izdaju

ažuriranje softvera za uređaje, te također ažuriraju softverske aplikacije koje krpaju javno objavljene sigurnosne rizike u određenim NFC implementacijama, aplikacijama i hardveru.

Nadalje, obavještavanje korisnika o potencijalnom kršenju privatnosti koje NFC oznaka može omogućiti još je jedan način za smanjenje rizika. Na primjer, korisnici koji koriste Apple uređaje te skeniraju AirTag dobivaju upozorenja kao dio novog ažuriranja softvera. Upozoravanje se svodi na upozoravajuću poruku da je u mnogim zemljama diljem svijeta kazneno djelo pratiti pojedince bez njihovog pristanka. Također, Apple uvodi dodatna ažuriranja za pomoć u prepoznavanju neželjenog praćenja sa značajkom preciznog pronalaženja. To se implementira u svrhu da se utvrdi prati li nepoznati i neželjeni AirTag korisnika. Nadalje, jedan od načina kako bi se smanjio sigurnosni rizik prilikom korištenja NFC tehnologije jest da korisnici ne skeniraju NFC oznaku ili POS terminal koji izgleda sumnjivo i ne legitimno, te koji se nalazi na sumnjivim mjestima. Između ostalog, korisnici na svome pametnom uređaju mogu ugasiti automatsko skeniranje NFC oznaka, te sukladno tome korisniku se nudi dijaloški okvir koji od korisnika traži da klikne gumb kako bi omogućio preuzimanje, [28].

U slučaju kada se NFC tehnologija koristi u svrhu novčanih transakcija osobito se treba obratiti pažnja na POS terminale, jer su vrlo ranjivi ako nisu adekvatno zaštićeni. Svi uređaji za plaćanje trebaju biti opremljeni autentifikacijom korisnika i kontrolom pristupa kako bi se osiguralo da osjetljive informacije ne padnu u pogrešne ruke. To uključuje fizičku sigurnost uređaja, osposobljavanje zaposlenika za održavanje sigurnosti mobilnih POS sustava i omogućavanje kontrole pristupa svim terminalima za plaćanje. Također, način na koji se povećava sigurnost korištenja NFC tehnologije tijekom akcije plaćanja jest taj da prijenos podataka o plaćanju tijekom NFC transakcije treba biti šifriran kako bi se ti podaci najsigurnije zaštitili. Istodobno, korisnike se savjetuje da koriste materijale koje blokiraju NFC povezivanje. Postoji nekoliko različitih materijala koji mogu blokirati NFC signale te novčanici sačinjeni od tih materijala koji su stanju blokirati NFC signale. Korištenje NFC blokatora u novčaniku ili torbici u blizini kartica ili uređaja za praćenje s omogućenim NFC-om može ublažiti potencijalne rizike od neželjenog praćenja ili prijevare. Jer napadači često iskorištavaju područja sa velikom koncentracijom ljudi kako bi svoj terminal koji je napravljen i programiran kako bi napravio novčanu transakciju na štetu korisnika bez korisnikovog znanja. To je moguće jer platne kartice novije generacije omogućavaju beskontaktno plaćanje do određenog iznosa

te stoga nije potrebno da korisnik pri određenom iznosu unese svoju lozinku kako bi se transakcija odvila, [39].

5.2 Prijedlozi unaprjeđenja sigurnosti korištenja QR kod tehnologije

Kako NFC tehnologija ima sigurnosne rizike prilikom korištenja tako i QR tehnologija nije iznimka te podliježe određenim rizicima prilikom uporabe od strane korisnika. U nastavku teksta objašnjeni su koraci koje bi korisnik trebao poduzeti prilikom skeniranja QR kodova te što napraviti ukoliko skenira zlokobni QR kod.

Jedan od načina kako korisnik može zaštiti svoje privatne informacije sa uređaja jest taj da prilikom skeniranja QR koda provjeri odredišnu stranicu na koju taj specifični QR kod navodi. To jest korisnik bi trebao provjeriti ima li pogrešno napisanih riječi unutar URL-a što daje određenu razinu sumnje na legitimnost stranice. Također, stranice koje su sigurne u većini slučajeva će koristiti HTTPS (engl. *Hyper Text Transfer Protocol Secure*) protokol umjesto HTTP (engl. *Hyper Text Transfer Protocol*) te će sadržavati ikonu lokota pored URL-a. Nadalje, korisnici bi trebali izbjegavati skeniranje QR kodova koji se nalaze na raznim mjestima i elektroničkoj pošti. Ukoliko korisnik nije siguran čemu taj QR kod služi to jest koja mu je svrha preporučeno mu je da ga ne skenira. Često zlonamjerni QR kodovi mogu izgledat primamljivo te nuditi razne nagrade i popuste mameći korisnike u svoju klopku. Isto tako korisnicima se preporučuje da izbjegavaju preuzimanje razni aplikacija za skeniranje QR kodova i koriste QR kod skener koji su dobili prethodno instaliranog unutar svoga pametnog uređaja, [40].

Ukoliko se korisnik nađe u situaciji u kojoj je skenirao zlonamjerni QR kod može poduzeti neke od sljedećih radnji, a to je da u početku koristiti autentifikaciju u dva faktora koja uveliko otežava napadaču jednostavan pristup privatnim i krucijalnim informacijama korisnika. Također, uz prethodno navedeno korisnik može promijeniti svoje lozinke različitih računa kako bi bio u mogućnosti na taj način zaštititi svoje račune te kako ne bi bio podvrgnut iznuđivanju novaca te ostalim radnjama napadača. Nadalje, savjetuje se korisniku da prekine vezu sa WiFi ili mobilnom mrežom, na taj način smanjuje je se rizik da će zlonamjerni softver poslati osjetljive informacije napadaču jer pametni uređaj nema pristup prema internetu. Između ostalog, korisniku se savjetuje da ima napravljenu sigurnosnu kopiju važnih podataka.

Sigurnosna kopija može uveliko pomoći u situaciji u kojoj nakon skeniranja zlonamjernog QR koda napadač šifrira korisnikov disk i iznuđuje novac. Ukoliko korisnik ima sigurnosnu kopiju može lako povratiti bitne informacije koje su mu zaključane. Također, ukoliko korisnik koristi svoj pametni uređaj za internet bankarstvo preporučuje se da se javi svojoj bankarskoj organizaciji koja će u tom slučaju zamrznuti korisnički račun kako se napadač ne bi mogao novčano okoristiti nad žrtvom, [40].

6. Zaključak

Kibernetičkih napada svakim danom je sve više i više te postaju domišljatiji i kompleksniji. Kako bi napadač bio u mogućnosti penetrirati sustav i napraviti ekstrakciju informacija mora biti korak ispred trenutnih obrambenih mehanizama kibernetičkih napada koji trenutno postoje.

Socijalni inženjering napadi sve su veća kibersigurnosna prijetnja. Oni se oslanjaju na naivnost i manipulaciju korisnika kako bi korisnici otkrili vrijedne privatne podatke u interesu kibernetičkih kriminalaca.

ENISA i BEREC dvije su važne europske organizacije koje rade na osiguravanju sigurnosti i otpornosti digitalne infrastrukture unutar EU-a. Europska unija donijela je nekoliko akata i propisa koji se bave pitanjem kibernetičke sigurnosti. Jedan od glavnih akata koji se odnose na kibernetičku sigurnost u EU je Direktiva o mrežnim i informacijskim sustavima. Drugi važan akt u pristupu EU-a kibernetičkoj sigurnosti je Opća uredba o zaštiti podataka. EU je također uspostavio Europsku organizaciju za kibernetičku sigurnost.

QR kod i NFC su dvije popularne tehnologije koje se koriste u svakodnevnom životu za različite svrhe uključujući plaćanje, identifikaciju, dijeljenje informacija i druge te su svakim danom sve više zastupljenije u cijelom svijetu. Njihovo korištenje donosi i određene rizike u pogledu kibersigurnosti gdje ih napadači koriste u raznim situacijama kako bi ugrozili žrtvu.

Istraživanje utjecaja QR kod i NFC tehnologija kao kibersigurnosnih prijetnji dalo je rezultate od 391 skeniranih QR kodova i 340 NFC oznaka. Utvrđeno je da su korisnici podložni na Socijal inženjering napade iako mnogi nisu htjeli priznat. Prilikom analize anketa većina korisnika je odgovorilo kako smatraju da znaju prepoznati kibernetičke prijetnje što je kontradiktorno pošto samim time što su skenirali QR kod ili NFC oznaku su sudjelovali u lažnoj kibernetičkoj prijetnji koja je mogla biti stvarna. Nadalje, utvrđeno je da su korisnicima poznatiji *Phishing* napadi od Socijal inženjering napada. Korisnici koji su ispunili anketu su u većini ženskog spola te različite dobi u rasponu od 15 do 66 godina. Najviše korišteni operativni sustav od strane korisnika jest Android. Razlozi skeniranja QR kodova su bili razni ali najistaknutiji jest znatiželja. Nadalje, većina korisnika koja je skenirala QR kodove posjeduje srednjoškolski stupanj obrazovanja.

Postoje mnogi načini kako bi se korisnici obranili od različitih napada tehnologija kratkih dometa ali jedna od ključnih obrana je edukacija korisnika. Sa kvalitetnom edukacijom korisnika može se znatno smanjiti broj napada tehnologija kratkog dometa ali i svih ostalih napada jer je korisnik u većini slučaja najslabija karika unutar lanca kibersigurnosti.

Popis literature

1. IBM Portal. Preuzeto sa: https://www.ibm.com/topics/cyber-attack - [Pristupljeno: Lipanj 2023.].
2. Vrančić, I. (2019) Hakeri i njihova etika. Diplomski rad. Zagreb: Sveučilište u Zagrebu, Filozofski fakultet.
3. Kristoffer Skow, T. (2016) Protection Against DNS Tunneling Abuses on Mobile Devices. Norwegian University of Science and Technology.
4. Kharraz, A. (2017) Techniques and Solutions for Addressing Ransomware Attacks. College of Computer and Information Science Northeastern University.
5. Ali Naqi Kazmi, M. (2019) SQL Injection Detection and Exploitation Framework for Penetration Testing. PhD Thesis. Intelligent systems Research Centre School of Computing and Digital Media London Metropolitan University England.
6. Gridinsoft Portal. Preuzeto sa: https://gridinsoft.com/backdoor - [Pristupljeno: Lipanj 2023.].
7. Owasp Portal. Preuzeto sa: https://cheatsheetseries.owasp.org/cheatsheets/Cross_Site_Scripting_Prevention_Cheat_Sheet.html - [Pristupljeno: Lipanj 2023.].
8. Cloudflare Portal. Preuzeto sa: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/ - [Pristupljeno: Lipanj 2023.].
9. Brightsec Portal. Preuzeto sa: https://brightsec.com/blog/dns-tunneling/ - [Pristupljeno: Lipanj 2023.].
10. Xu, Z. (2014). Analysis and Defense of Emerging Malware Attacks. (Doctoral dissertation). Texas A&M University.
11. Salahdine, Fatima, and Naima Kaabouch. 2019. "Social Engineering Attacks: A Survey" Future Internet 11, no. 4: 89.
12. Narodne novine Portal. Preuzeto sa: https://narodne-novine.nn.hr/clanci/medunarodni/2002_07_9_119.html - [Pristupljeno: Lipanj 2023.].
13. Europski revizorski sud Portal. Preuzteo sa: https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_HR.pdf - [Pristupljeno: Lipanj 2023.].
14. Enisa Portal. Pruzeto sa: https://www.enisa.europa.eu - [Pristupljeno: Lipanj 2023.].

15. Berec Portal. Preuzeto sa: https://www.berec.europa.eu/en/berec/tasks - [Pristupljeno: Lipanj 2023.].
16. Cert Portal. Preuzeto sa: https://cert.europa.eu/ - [Pristupljeno: Lipanj 2023.].
17. Europol Portal. Preuzeto sa: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3 - [Pristupljeno: Lipanj 2023.].
18. Gdpr Portal. Preuzeto sa: https://gdpr.eu/ - [Pristupljeno: Lipanj 2023.].
19. Esc Portal. Preuzeto sa: https://ecs-org.eu/ - [Pristupljeno: Lipanj 2023.].
20. Eur-lex.europa Portal. Preuzeto sa: https://eur-lex.europa.eu/eli/reg/2019/881/oj - [Pristupljeno: Lipanj 2023.].
21. Techpats Portal. Preuzeto sa: https://www.techpats.com/evolution-near-field-communication-nfc/ - [Pristupljeno: Lipanj 2023.].
22. Qrcode Portal. Preuzeto sa: https://www.qrcode.com/en/history/ - [Pristupljeno: Lipanj 2023.].
23. Kevin Portal. Preuzeto sa: https://www.kevin.eu/blog/nfc-payments/ - [Pristupljeno: Lipanj 2023.].
24. Pxl-vision Portal. Preuzeto sa: https://www.pxl-vision.com/en/blog/10-everyday-use-cases-of-nfc-near-field-communication - [Pristupljeno: Lipanj 2023.].
25. Smart-tec Portal. Preuzeto sa: https://www.smart-tec.com/en/auto-id-world/nfc-technology - [Pristupljeno: Lipanj 2023.].
26. Nfctagify Portal. Preuzeto sa: https://nfctagify.com/pros-and-cons-of-nfc-tags-infographic/ - [Pristupljeno: Lipanj 2023.].
27. Nearfieldcommunication Portal. Preuzeto sa: http://nearfieldcommunication.org/nfc-security-risks.html - [Pristupljeno: Lipanj 2023.].
28. Techtarget Portal. Preuzeto sa: https://www.techtarget.com/whatis/feature/6-potential-enterprise-security-risks-with-NFC-technology - [Pristupljeno: Lipanj 2023.].
29. Investopedia Portal. Preuzeto sa: https://www.investopedia.com/terms/q/quick-response-qr-code.asp - [Pristupljeno: Lipanj 2023.].
30. https://play-lh.googleusercontent.com/ufwUy4SGVTqCs8fcp6AjxfpaeObNImN1Rq2cXUjWI7jlmNMCsXgQE5C3yUEzBu5Gadkz - [Pristupljeno: Lipanj 2023.].
31. Qrcode Portal. Pruzeto sa: https://www.qrcode.com/en/codes/ - [Pristupljeno: Lipanj 2023.].

32. Dynamsoft Portal. Preuzeto sa: https://www.dynamsoft.com/barcode-reader/barcode-types/micro-qr-code/ - [Pristupljeno: Lipanj 2023.].
33. Qrcode Portal. Preuzeto sa: https://www.qrcode.com/en/codes/microqr.html - [Pristupljeno: Lipanj 2023.].
34. Qrcode Portal. Preuzeto sa: https://www.qrcode.com/en/codes/iqr.html - [Pristupljeno: Lipanj 2023.].
35. Krombholz, K., Frühwirt, P., Kieseberg, P., Kapsalis, I., Huber, M., & Weippl, E. (2015). QR Code Security: A Survey of Attacks and Challenges for Usable Security. In Proceedings of the 10th International Conference on Availability, Reliability and Security (ARES) (pp. 38-49). SBA Research, Vienna
36. Sung, Siwon & Lee, Joonghwan & Kim, Jinmok & Moon, Jongho & Won, Dongho. (2015). Security Analysis of Mobile Authentication Using QR-Codes. Computer Science & Information Technology
37. Scanova Portal. Preuzeto sa: https://scanova.io/blog/advantages-of-qr-code/ - [Pristupljeno: Lipanj 2023.].
38. Whitehatinstitute Portal. Preuzeto sa: https://whitehatinstitute.com/generate-a-qr-code-attack-vector/ - [Pristupljeno: Lipanj 2023.].
39. Staxpayments Portal. Preuzeto sa: https://staxpayments.com/blog/nfc-security/ - [Pristupljeno: Lipanj 2023.].
40. Heimdalsecurity Portal. https://heimdalsecurity.com/blog/quishing/ - [Pristupljeno: Lipanj 2023.].
41. Balaš, I. (2018) Analiza tehnologije rada Zagreb Glavnog kolodvora. Diplomski rad. Zagreb: Sveučilište u Zagrebu, Fakultet Prometnih znanosti.
42. https://hecere.en.made-in-china.com/product/pmQYqfrVoGkU/China-Paper-ISO15693-NXP-Icode-Slix-Slix2-Sli-S-RFID-Tag-NFC-Sticker-Printable-RFID-Labels.html- [Pristupljeno: Lipanj 2023.].

Popis kratica i akronima

QR (*Quick-response code*) Kod za brzi odgovor

NFC (*Qear-field communication*) Komunikacija u blizini polja

IT (*Infotech*) Informatička tehnologija

XSS (*Cross-site scripting*) Napad skriptiranja na više stranica

DoS (*Denial-of-service*) Napadi uskraćivanja usluge

DDoS (*Distributed Denial-of-Service*) Distribuirani napadi uskraćivanja usluge

DNS (*Domain Name System*) Sustav naziva domene

C&C (*Command & Conquer*) Server zapovijedanja i kontrole

SQL (*Structured Query Language*)

HTML (*HyperText Markup Language)*

ISP (*Internet service provider*) Davatelj internetskih usluga

WAF (*Web application firewall*) Vatrozid web aplikacije

EU (*European Union*) Europska unija

ENISA (*The European Union Agency for Cybersecurity*) Agencija Europske unije za mrežnu i informacijsku sigurnost

BEREC (*Body of European Regulators for Electronic Communications*) Tijelo europskih regulatora za elektroničke komunikacije

GDPR (*General Data Protection Regulation*) Opća uredba o zaštiti podataka

ECC (*Electronic Communications Code*) Kodeks elektroničkih komunikacija

EC3 (*European Cybercrime Centre*) Europolov Europski centar za borbu protiv kiberkriminala

ECSO (*European Cyber Security Organisation*) Europska organizacija za kibernetičku sigurnost

CERT-EU (*Computer Emergency Response Team*) Tim za hitne računalne intervencije

RF (*Radio frequency*) Radio frekvencija

URL (*Uniform Resource Locator*)

WiFi (*Wireless Fidelity*)

PDF (*Portable Document Format*) Prijenosni format dokumenta

SMS (*Short Message Service*) Usluga kratkih poruka

HTTPS (*Hyper Text Transfer Protocol Secure*)

HTTP (*Hyper Text Transfer Protocol*)

Popis ilustracija

Popis slika

Popis grafikona

Popis tablica

Sveučilište u Zagrebu
Fakultet prometnih znanosti
Vukelićeva 4, 10000 Zagreb

IZJAVA O AKADEMSKOJ ČESTITOSTI I SUGLASNOSTI

Izjavljujem i svojim potpisom potvrđujem da je diplomski rad
(vrsta rada)
isključivo rezultat mojega vlastitog rada koji se temelji na mojim istraživanjima i oslanja se na objavljenu literaturu, a što pokazuju upotrijebljene bilješke i bibliografija. Izjavljujem da nijedan dio rada nije napisan na nedopušten način, odnosno da je prepisan iz necitiranog rada te da nijedan dio rada ne krši bilo čija autorska prava. Izjavljujem, također, da nijedan dio rada nije iskorišten za bilo koji drugi rad u bilo kojoj drugoj visokoškolskoj, znanstvenoj ili obrazovnoj ustanovi.

Svojim potpisom potvrđujem i dajem suglasnost za javnu objavu završnog/diplomskog rada pod naslovom Primjena tehnologije kratkog dometa kao metode socijalnog inženjeringa , u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 1.9.2023.

(ime i prezime, *potpis*)