Razvijanje svijesti o kibernetičkoj sigurnosti među građanima Republike Hrvatske

Ladiš, Andrej

Master's thesis / Diplomski rad

2024

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Transport and Traffic Sciences / Sveučilište u Zagrebu, Fakultet prometnih znanosti**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:119:043148

SVEUČILIŠTE U ZAGREBU
FAKULTET PROMETNIH ZNANOSTI

Andrej Ladiš

RAZVIJANJE SVIJESTI O KIBERNETIČKOJ SIGURNOSTI MEĐU GRAĐANIMA REPUBLIKE HRVATSKE

DIPLOMSKI RAD

Zagreb, 2024.

Sveučilište u Zagrebu
Fakultet prometnih znanosti

DIPLOMSKI RAD

RAZVIJANJE SVIJESTI O KIBERNETIČKOJ SIGURNOSTI MEĐU GRAĐANIMA REPUBLIKE HRVATSKE

DEVELOPING CYBER SECURITY AWARENESS AMONG THE CITIZENS OF THE REPUBLIC OF CROATIA

Mentor: dr. sc. Melita Milenković, mag.iur.

Student: Andrej Ladiš, univ. bacc. ing. traff.

JMBAG: 0246070565

Zagreb, ožujak 2024.

ZAHVALA

Iskreno se zahvaljujem mentorici dr. sc. Meliti Milenković na ukazanom povjerenju, vodstvu i pomoći pri izradi diplomskog rada.

SADRŽAJ

RAZVIJANJE SVIJESTI O KIBERNETIČKOJ SIGURNOSTI MEĐU GRAĐANIMA REPUBLIKE HRVATSKE

SAŽETAK:

Diplomski rad kroz provedeni Anketni upitnik istražuje razinu svijesti o kibernetičkoj sigurnosti među građanima Republike Hrvatske. Cilj je bio analizirati percepciju korisnika o rizicima i sigurnosnim praksama u digitalnom okruženju. Anketni upitnik sadrži osnovne pojmove za razumijevanje kibernetičke sigurnosti, stoga su postavljena pitanja vezana za kibernetičke odnosno *cyber* prijetnje kao i kibernetičku sigurnost „Interneta stvari“ (engl. Internet of Things). Diplomski rad također obrađuje pitanja sigurnosti umjetne inteligencije te njihove prednosti i nedostatke u području kibenetičke sigurnosti. Također, diplomski rad navodi uredbe Europske Unije kojima se nastoji postići visoka zajednička razina kibernetičke sigurnosti.

KLJUČNE RIJEČI: Kibernetička sigurnost, *cyber* prijetnje, „Internet stvari“, Europska Unija.

DEVELOPING CYBER SECURITY AWARENESS AMONG THE CITIZENS OF THE REPUBLIC OF CROATIA

SUMMARY:

The master's thesis, conducted through a survey questionnaire, explores the level of awareness of cyber security among the citizens of the Republic of Croatia. The aim was to analyze users' perceptions of risks and security practices in the digital environment. The survey questionnaire contains basic concepts for understanding cyber security, thus posing questions related to cyber threats as well as the cyber security of the Internet of Things. The thesis also addresses issues of artificial intelligence security and their advantages and disadvantages in the field of cyber security. Additionally, the master's thesis cites European Union regulations aimed at achieving a high common level of cyber security.

KEY WORDS: cyber security, cyber threats, Internet of Things, European Union.

1. Uvod

U današnjem digitalnom dobu, kibernetička sigurnost postala je ključna i neizostavna komponenta globalne informacijske infrastrukture. Sveprisutna upotreba interneta, rastući broj povezanih uređaja i brza digitalna transformacija društva i gospodarstva otvorili su vrata novim mogućnostima i izazovima. Dok je digitalna tehnologija omogućila inovacije, efikasnost i globalnu povezanost, istovremeno je stvorila nove ranjivosti.

Kibernetički napadi, krađe podataka, hakiranja, odnosno neovlašteno korištenje tuđih računa, podataka i slični incidenti postali su sve češći, ozbiljniji i sofisticiraniji. Kao rezultat toga, kibernetička sigurnost postala je imperativ za organizacije i pojedince. S obzirom na sve veći broj kampanja razvijanja svijesti o kibernetičkoj sigurnosti u organizacijama, isto bi trebalo primjeniti za fizičke osobe (pojedince), odnosno građane. Neuspjeh u zaštiti digitalnih resursa i informacija može imati ozbiljne posljedice, uključujući financijske gubitke, gubitak povjerenja javnosti, kršenje privatnosti i čak ugrožavanje nacionalne sigurnosti. Uz pravilnu edukaciju i osviještenost, građani mogu biti zaštićeniji od kibernetičkih napada.

U radu je predstavljena Anketa o osviještenosti građana RH o kibernetičkoj sigurnosti kroz koju se lakše i efikasnije mogu identificirati prijetnje i napadi s kojima se fizičke osobe (pojedinici) susreću danas. Nadalje, Anketa pokazuje ulogu osvještavanja građana RH te je temeljem rezultata za svaku cjelinu u radu ponuđen adekvatan uzorak koji objašnjava razumijevanje fizičkih osoba (pojedinca), odnosno građana.

Ovaj diplomski rad podijeljen je u 7 cjelina:

1. Uvod
2. Rezultati provedene Ankete o osviještenosti građana RH u svezi kibernetičke sigurnosti
3. Kibernetička sigurnost
4. Kibernetička sigurnost Interneta stvari
5. Kibernetička sigurnost tehnologija umjetne inteligencije
6. Izvještaji razvijanja svijesti o kibernetičkoj sigurnosti kroz norme agencija EU
7. Zaključak

Druga cjelina sadrži pitanja i rezultate Ankete o osviještenosti građana RH. Usporedbom dobivenih rezultata Ankete na temelju 237 ispitanika i dosadašnjih izvješća Europske Unije, dobiven je stvaran prikaz trenutne osviještenosti građana Republike Hrvatske.

Trećom cjelinom objašnjen je pojam kibernetičke sigurnosti te su navedene vrste kibernetičkih napada. Kibernetički napadi uključeni u Anketi detaljno su objašnjeni. Sukladno raznim izvješćima, spomenuti su i potencijalni mogući kibernetički napadi, no primarni zadatak ovog diplomskog rada je pružiti trenutni uvid u razinu osviještenosti građana te je iz tog razloga usredotočenost na trenutnim prijetnjama.

Četvrta cjelina odnosi se na kibernetičku sigurnost Interneta stvari. U prvom poglavlju cjeline objašnjen je pojam Interneta stvari (engl. IoT- *Internet of Things*) u svrhu lakšeg razumijevanja mogućih prijetnji na takav sustav. Zatim su navedene prijetnje te stupnjevi zaštite koji pridonose zaštiti od istih. Osim same važnosti edukacije i osviještenosti korisnika, vrlo važan aspekt u zaštiti osobnih podataka predstavlja i enkripcija podataka. IoT uređaji često imaju ograničene resurse poput procesorske snage i memorije. Stoga, enkripcijski algoritmi trebaju biti optimizirani za rad na takvim uređajima kako bi se minimizirao utjecaj na performanse.

U petoj cjelini rada objašnjena je kibernetička sigurnost tehnologija umjetne inteligencije (engl. AI- *Artificial Intelligence*). AI je postao odličan alat u borbi protiv *cyber* prijetnji jer može pomoći u bržem otkrivanju, analizi i odgovoru na zlonamjerne napade. S druge strane, postoje određeni nedostaci i prijetnje omogućene korištenjem umjetne inteligencije. Dodatno, navedeno je nekoliko primjera kibernetičkih napada temeljenih na AI tehnologijama.

Šesta cjelina „Izvještaji razvijanja svijesti o kibernetičkoj sigurnosti kroz norme agencija EU“ detaljnije obrađuje već spomenuta izvješća Europske unije, temeljem izvješća objavljenih od strane agencije ENISA. U nastavku su navedene direktive Europske unije. Pravila EU-a o kibersigurnosti uvedena 2016. temeljen direktive NIS1 ažurirana su Direktivom NIS2 koja je stupila na snagu 2023. Zakon o kibernetičkoj sigurnosti, koji implementira odredbe Direktive NIS2, u Hrvatskoj je stupio na snagu 1. veljače 2024. godine.

Sedmo, ujedno i posljednje poglavlje je zaključno poglavlje u kojemu se nalazi kratki pregled rada te pregled dobivenih rezultata Ankete. Navedeni su i zaključci dobiveni provedbom analize dobivenih rezultata uspoređujući ih s dosadašnjim istraživanjima i izvješćima. Nakon zaključka u radu se nalazi popis literature te popis slika i grafikona korištenih pri izradi rada.

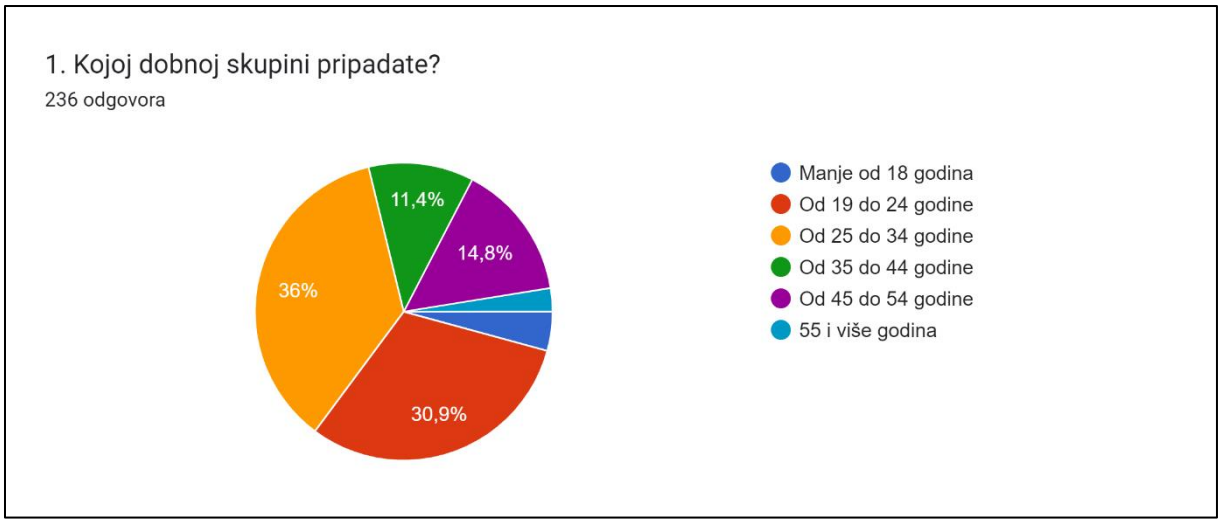
2. Rezultati provedene Ankete o osviještenosti građana RH u svezi kibernetičke sigurnosti

Anketa pod nazivom „Razvijanje svijesti o kibernetičkoj sigurnosti među građanima Republike Hrvatske“ objavljena je 5.8.2023. godine te je ista bila otvorena do 5.10.2023. Prikupljeno je 237 uzoraka, a kako bi anketa bila dostupna većem broju ispitanika, odnosno krajnjih korisnika korištene su različite društvene mreže. Time je dobiven reprezentativan uzorak ispitanika, dovoljan da bi se mogla prikazati upućenost stanovnika RH po pitanju poznavanja područja kibernetičke sigurnosti i zaštite osobnih podataka. Kao platforma za izradu iste je korišten i Google Forms. Prilikom proslijeđivanja Ankete korištene su primarno društvene mreže Instagram, LinkedIn, Facebook te je za proslijeđivanje kontaktima korištena mobilna aplikacija WhatsApp.

Nadalje, Anketa sadrži 10 pitanja koja imaju edukacijski pristup, s obzirom da su pojmovi koji služe kao odgovori detaljno objašnjeni, kako bi se na taj način doprinijelo razvijanju svijesti građana o kibernetičkoj sigurnosti.

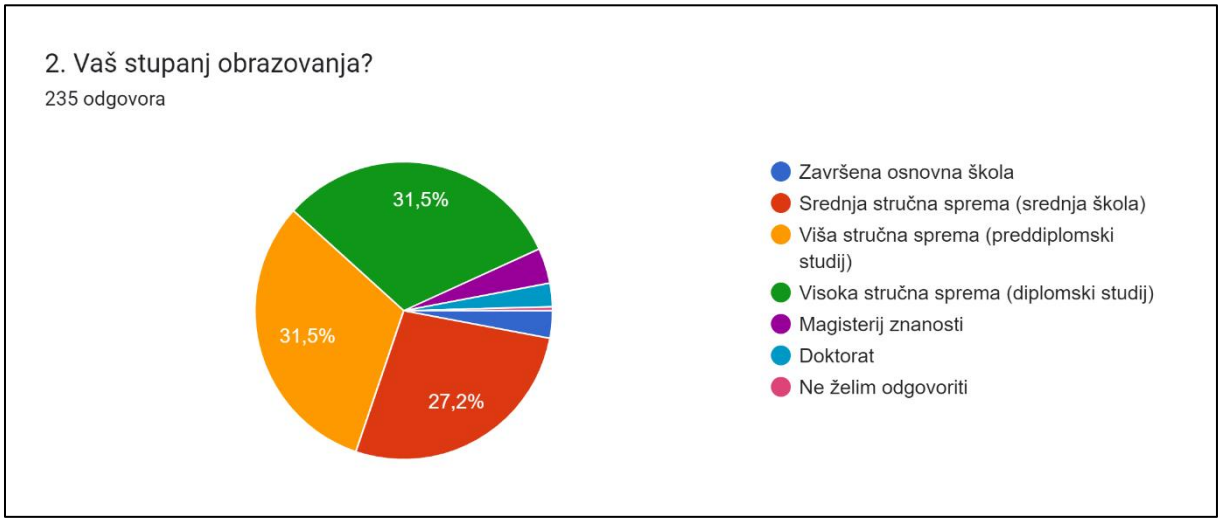
2.1. Prikaz Ankete

Poglavlje prikazuje grafikone za svako pitanje postavljeno u anketi. Tematika pojedinih pitanja dodatno je objašnjena kroz ostala poglavlja diplomskog rada. U prvom pitanju Ankete bilo je obrađeno pitanje u koju dobnu skupinu pripadaju ispitanici. Također, dobijeno je 236 odgovora, a prema kojima je vidljivo da je najveći broj ispitanika u dobi od 25 do 34 godine i to 36%. Slijedi grupacija ispitanika u dobi od 19 do 24 godine koja je zastupljena 30,9%. Ostale grupacije su zastupljene u manjem postotku. Navedeno može potvrditi da su ispitanici u dobi od 25 do 34 godine starosti najviše ispitana populacija u ovoj anketi, a obzirom da i sam autor pripada u dobnu skupinu navedene populacije.



Grafikon 1. Pitanje 1. Dobna skupina ispitanika

Grafikon 2. prikazuje pitanje pod brojem 2., a koje se odnosi na stupanj obrazovanja ispitanika. Na istom je moguće uočiti poprilično ravnopravan omjer ispitanika kada se radi od srednjoj, višoj i visokoj stručnoj spremi.

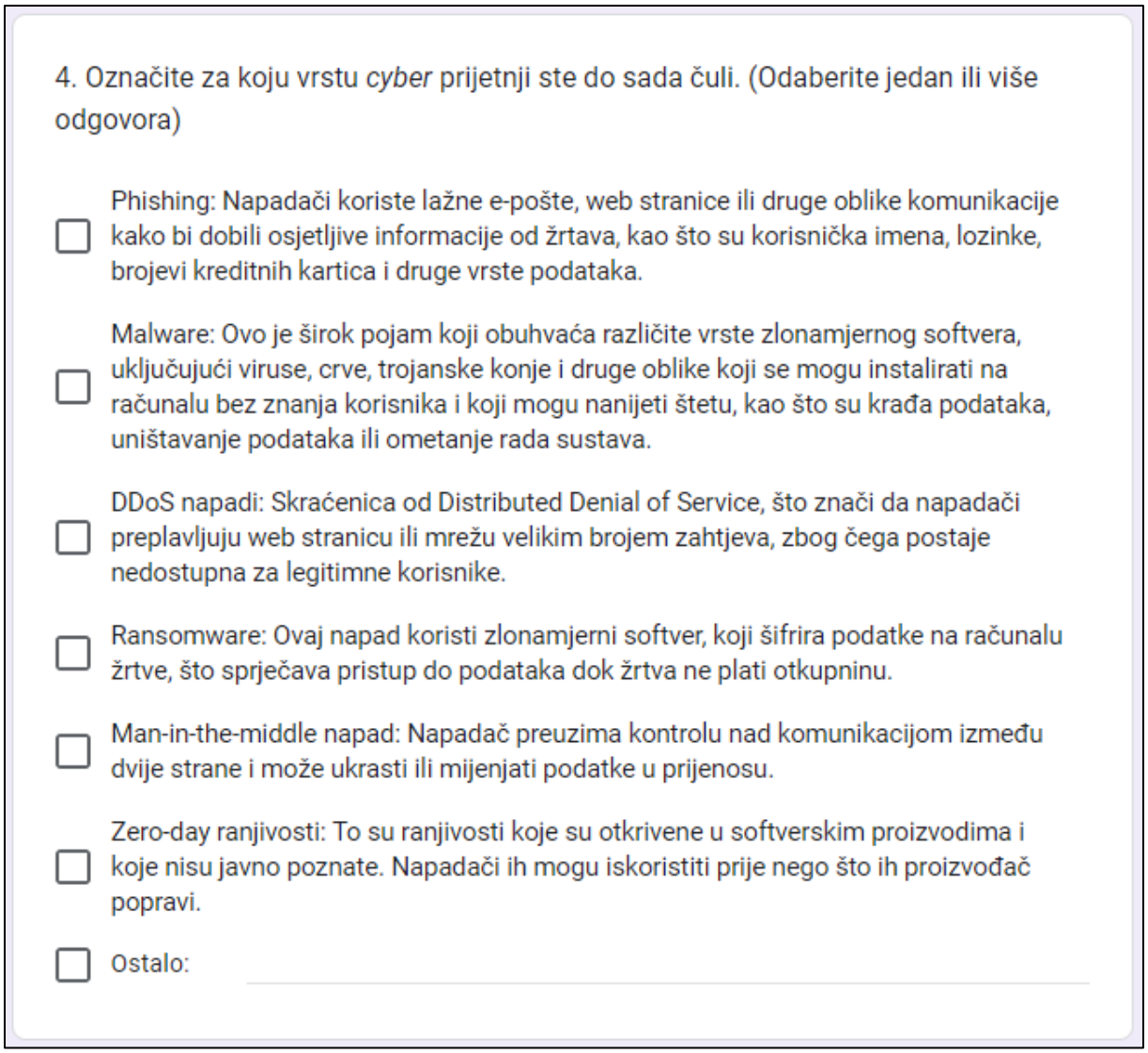


Grafikon 2. Pitanje 2. Stupanj obrazovanja ispitanika

Nastoji se za svaku od tehnologija koje su spomenute u diplomskom radu pružiti i konkretan uvid u mišljenje građana o tom predmetu. Stoga, važno je znati koliki je udio ispitanika uopće čuo za pojam kibernetičke sigurnosti. Isto je prikazano grafikonom 3., odnosno pitanjem broj 3. iz kojeg možemo iščitati kako čak 11,9% ispitanika nije čulo za pojam kibernetičke sigurnosti. To predstavlja potencijalni problem s obzirom da veći dio mlađe populacije nije upućen u poimanje pojma „kibernetička sigurnost" te navedena činjenica može ugroziti osobne podatke krajnjih korisnika u slučaju potencijalnog kibernetičkkog napada.

Grafikon 3. Pojam kibernetičke sigurnosti

Nastavno, ovdje je potrebno spomenuti da postoji više vrste kibernetičkih napada, a najzastupljeniji i samim time najpoznatiji su Phishing, Malware, DDoS napadi, Ransomware, Man-in-the middle napadi te Zero-day ranjivosti. Svaki od ovih napada biti će detaljno objašnjen u nastavku rada. Isti napadi bili su ponuđeni kao odgovori na 4. pitanje u anketi prikazano slikom 1. Dodatno, omogućena je opcija gdje su ispitanici mogli samostalno spomenuti cyber prijetnje za koje su čuli, a nisu ponuđene kao odgovori. Neki od odgovora su SQL injection, DNS *attack, Shoulder surfing*, što upućuje da su ispitanici u nekoj mjeri upućeni u različite vrte kibernetičkih napada.

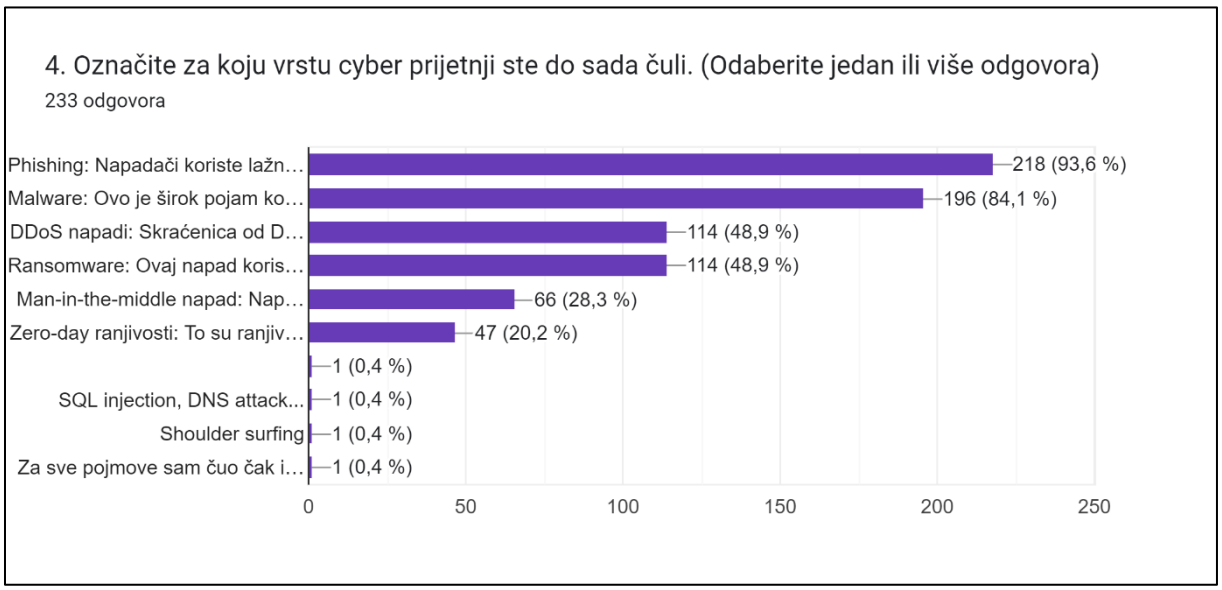


Slika 1. Ponuđeni odgovori za 4. pitanje

Uvidom u odgovore ispitanika prikazane grafikonom 4. vidljivo je kako značajan broj ispitanika zna za pojam Phishing, čak 93,6%, što nije nimalo iznenađujuće s obzirom na zastupljenost ove vrste napada. Također, velik broj današnjih kampanja ukazuje na opasnosti Phishinga s obzirom da se takva vrsta napada koristi u jednom od svaka tri napada, [1], što je dodatno razvilo svijest građana o opasnostima ovakve vrste kibernetičkog napada. Sve više kompanija nastoji kroz edukacije podići svijest o kibernetičkoj sigurnosti odnosno zaštiti povjerljivih podataka kompanije. Stoga, može se reći da je potrebno podići svijest izvan okvira radnog okruženja, odnosno i kod osoba koje nisu u radnom odnosu, djece, maloljetnika i starijih osoba nakon 65. godine života.

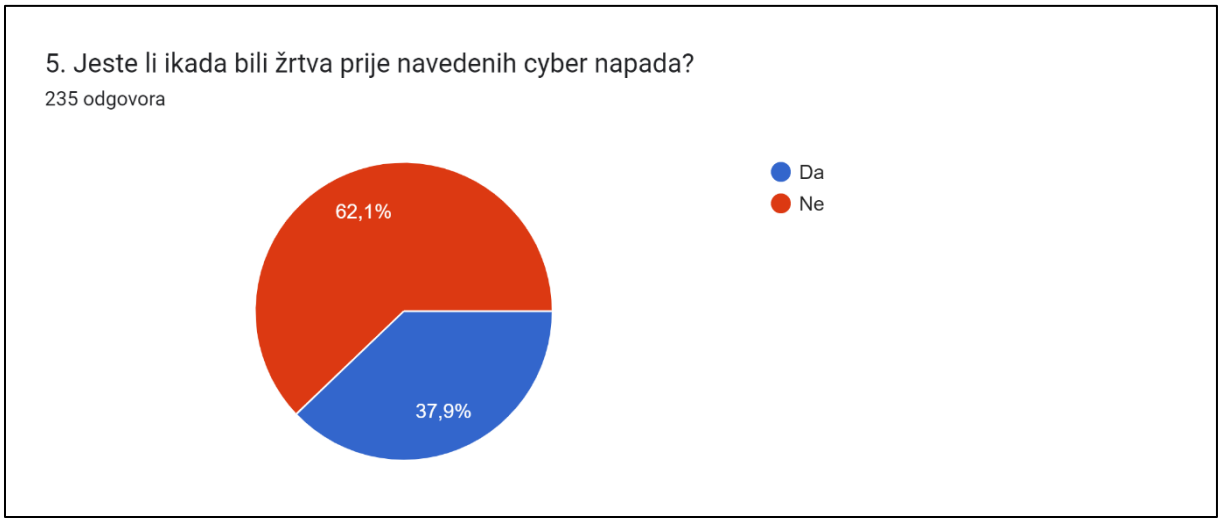
Najbolji primjer za to su banke. U današnje vrijeme, svatko ima otvoren bankovni račun kao osnovnu potrepštinu. Zastupljenost Internet bankarstva te interneta stvara prostor bankama za stvaranje sigurnog okruženja za podatke, kao i za razvijanje svijesti o mogućim prijetnjama

za podatke. Primjer je upozorenje Raiffeisen banke koja ukazuje na pojavu novih napada u kojima napadači traže povjerljive informacije putem SMS poruka, [2].



Grafikon 4. Pitanje 4. vrste *cyber* prijetnji

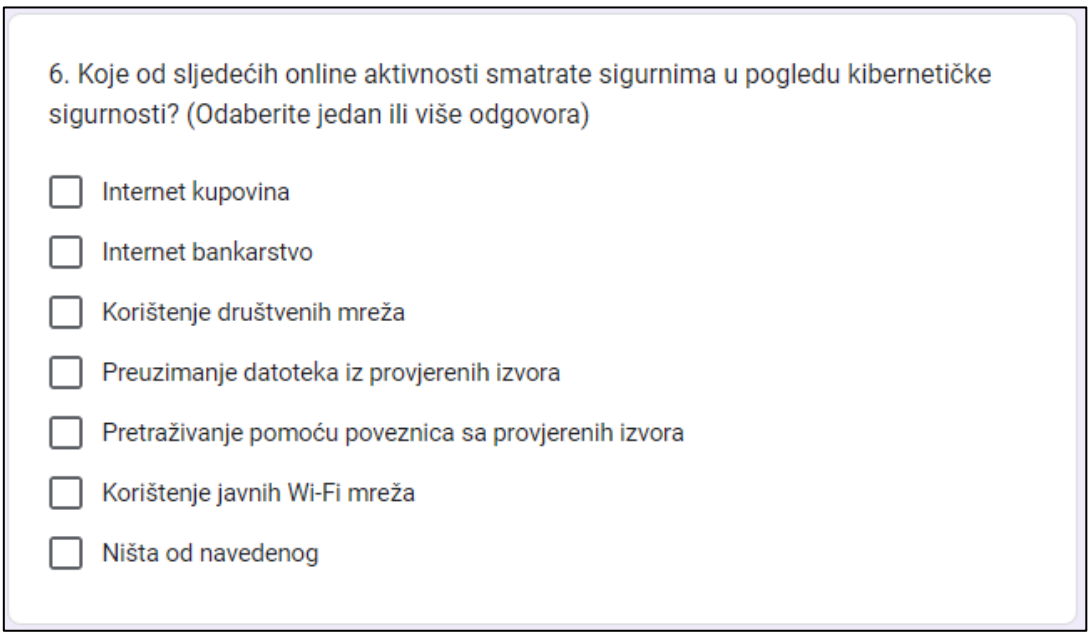
Nadalje, čak 62,1% ispitanika tvrdi kako su bili žrtvama *cyber* napada. Taj podatak prikazan je grafikonom 5. Upravo taj broj ispitanika koji su bili žrtve napada upućuje na nedovoljnu upoznatost građana s mogućnostima u cyber prostoru i potencijalnim opasnostima od ugroze njihovih podataka. Sigurnosno-obavještajna agencija, SOA upozorava na povećan broj kibernetičkih napada, [3].



Grafikon 5. Pitanje 5. udio ispitanika koji se susreo sa *cyber* napadima

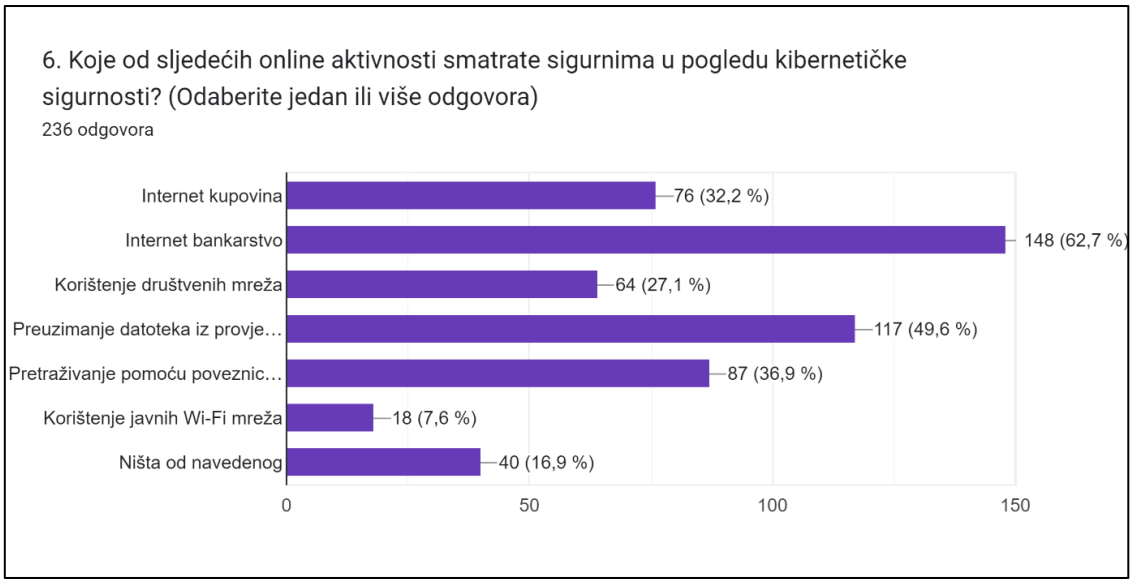
Slikom 2. prikazano je 6. pitanje u Anketi te su Grafikonom 6. prikazani odgovori na isto. Nadalje, odgovori na 6. pitanje daju najzorniji prikaz onoga što korisnici odnosno ispitanici smatraju „sigurnim“. Stoga je internet bankarstvo prema Anketi najsigurnija aktivnost. Čak

62,7% korisnika vjeruje da su njihovi podaci sigurni pri korištenju ovakvih usluga. Internet kupovina te korištenje društvenih mreža imaju sličan postotak sigurnosti među ispitanicima.

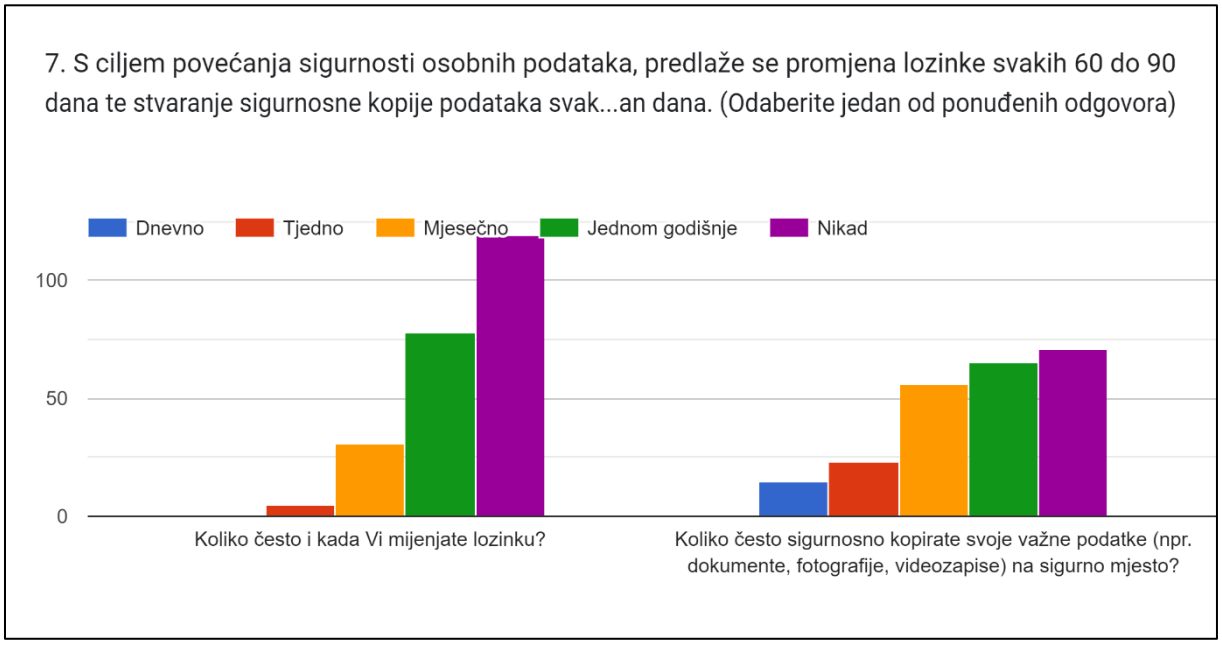


Slika 2. Ponuđeni odgovori za 6. pitanje

Vrlo je važno kako najmanji udio korisnika smatra korištenje javnih Wi-Fi mreža sigurnom aktivnošću, no ipak bi se trebalo težiti još manjem postotku s obzirom kako je korištenje istih vrlo nesigurno i otvara pristup privatnim podacima. U ovakvom okruženju, haker ima pristup svakoj informaciji koju korisnik pošalje korištenjem Interneta, važnim e-porukama, podacima o kreditnoj kartici i sl. [4] Također, 16,9% uopće ne osjeća sigurnost prilikom korištenja bilo koje od navedenih aktivnosti. Za taj dio ispitanika može se samo pretpostaviti da su dovoljno educirani da znaju kako je bilo koja radnja u cyberprostoru otencijalna opasnost za gubitak osobnih podataka. Preuzimanje datoteka iz provjerenih izvora se ispitanicima čini relativno sigurnim s obzirom da gotovo 50% vjeruje kako je to sigurna aktivnost.



Grafikon 6. Pitanje 6. Sigurnost *online* aktivnosti



Grafikon 7. Pitanje 7. Učestalost promjene lozinke i stvaranje sigurnosne kopije podataka

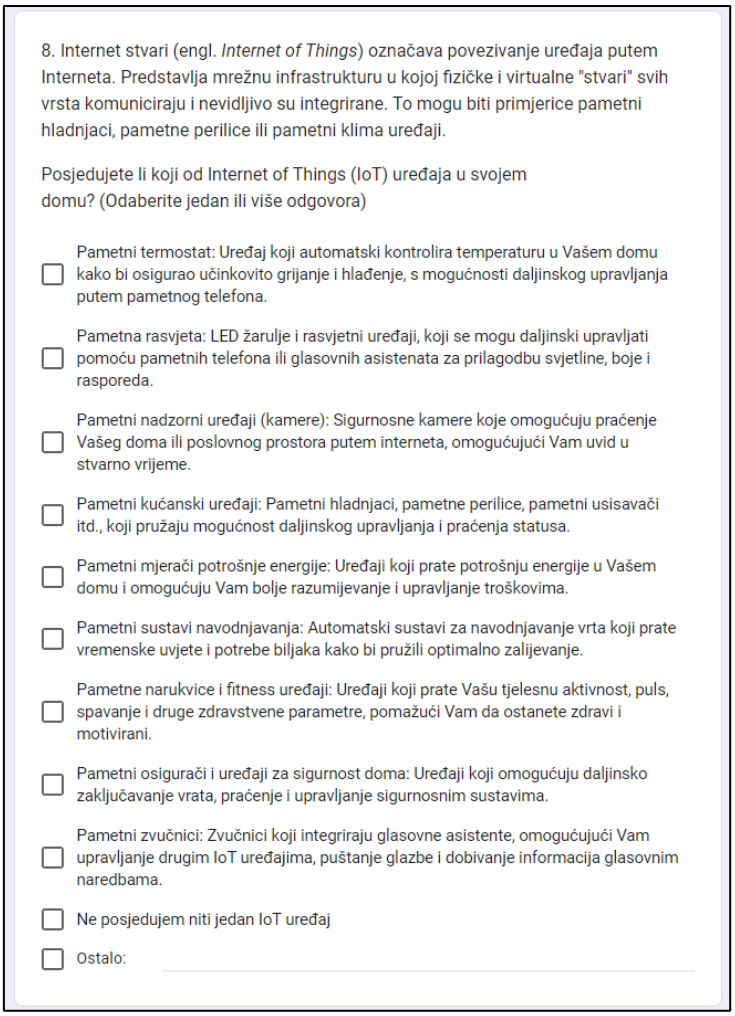
U većini slučajeva u informatičkom okruženju, autentifikacija predstavlja posljednju prepreku između korisnika i uređaja. Autentifikacija putem zaporke je široko rasprostranjena metoda. Postoje različiti oblici autentifikacije, no zbog svoje prihvaćenosti i jednostavnosti korištenja, zaporke su najkorišteniji oblik autentifikacije, [5]. Zaporka je definirana kao zaštićeni skup znakova koji se koristi kao autenfitikacija identiteta korisnika ili kao autorizacija pristupa resursu te bi, zbog tog razloga, ona trebala biti jedinstvena za svaki entitet. Prema

brojnim izvorima, između ostalog i prema agenciji ENISA[1] [6], predlaže se promjena zaporke svakih 90 dana. Na taj način se mogu spriječiti Man-in-the-middle napadi[2]. Kao što je prikazano Grafikonom 7. velik broj ispitanika uopće ne mijenja svoju zaporku kao što je predloženo, a neki korisnici gotovo nikada.

Nastavno, stvaranje sigurnosne kopije je vrlo važan aspekt sigurnosti organizacije kao i pojedinca. Svi pojedinci i organizacije riskiraju trajni gubitak važnih podataka ako ne naprave sigurnosnu kopiju svojih datoteka. Organizacije koje ne izrađuju sigurnosnu kopiju svojih datoteka, osobito svojih financijskih zapisa riskiraju oštećenje svog poslovanja, možda do te mjere da ih izgube. Mnoge se tvrtke oslanjaju na računala za vođenje cjelokupnog poslovanja: financije, ljudski resursi, obračun plaća, prodaja, marketing itd. U nekim slučajevima tvrtke koje ne mogu pristupiti svojim datotekama zbog slučajnih ili zlonamjernih razloga ne mogu nastaviti s radom, [7].

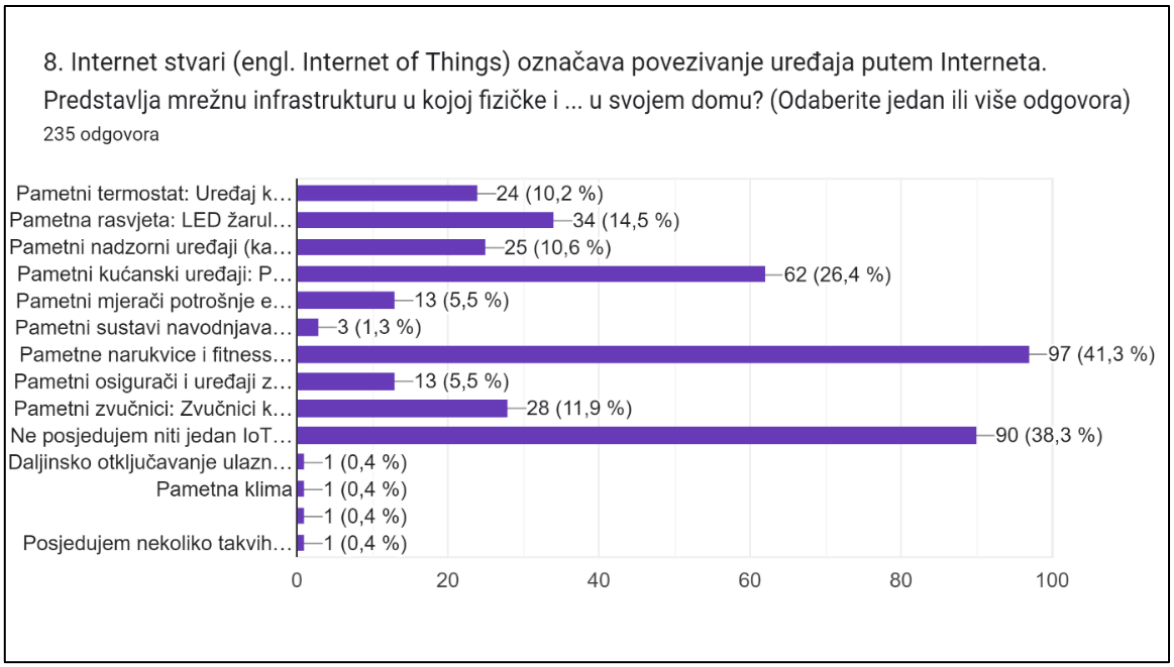
Naredna dva pitanja ankete odnose se na Internet of Things. IoT je detaljnije objašnjen u 4. poglavlju diplomskog rada. Slika 3. prikazuje pametne uređaje koji su bili ponuđeni kao odgovori na 8. pitanje Ankete. Dodatno, odgovori ispitanika prikazani su grafikonom 8. Svaki pametni uređaj kao i namjena su detaljno objašnjeni u svrhu lakšeg razumijevanja, s obzirom da je Anketa koncipirana laički kako bi i obični građanin naučio nešto korisno.

[1] ENISA- (engl. European Network and Information Security Agency) Agencija Europske unije za kibernetičku sigurnost, bavi pitanjima sigurnosti informacija i informacijskih mreža, definicija dostupna na str. 11.
[2] *Man-in-the-middle* napadi – napad gdje se neautorizirani entitet 'ubaci' između komunicirajućih korisnika te pokušava presreći razmjenu informacija, definicija dostupna na str. 26.



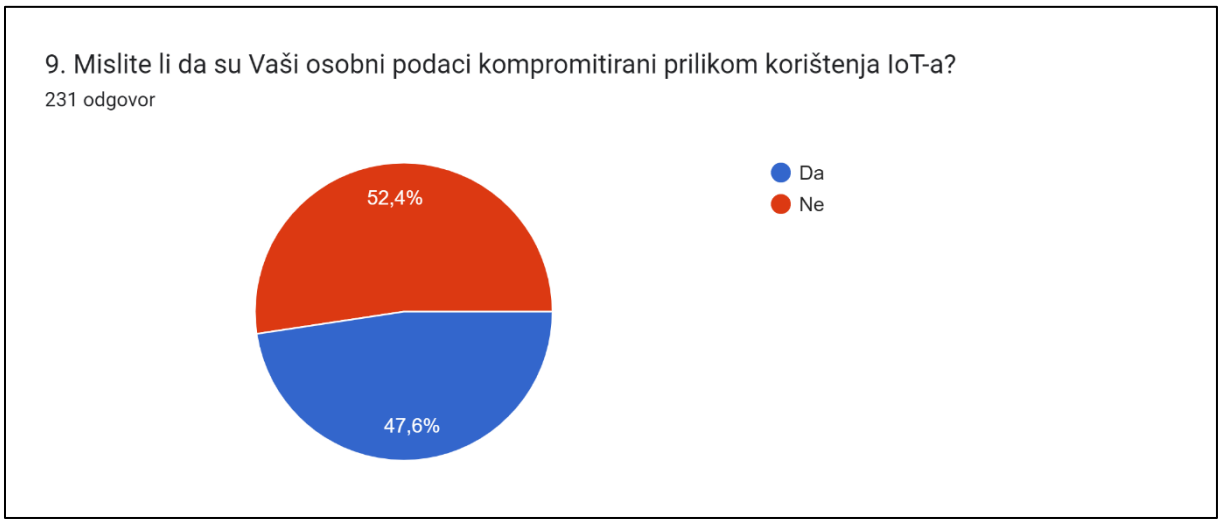
Slika 3. 8. pitanje u Anketi

Vidljivo je kako 38,3 % ispitanika uopće ne posjeduje niti jedan IoT uređaj, a ako posjeduje onda se radi o pametnim narukvicama i fitness uređajima. Također, 26,4 % korisnika posjeduje barem jedan pametni kućanski aparat kao što su hladnjaci, pametni usisavači, pametne perilice i sl. Dodatno, korisnici posjeduju uređaje kao što je pametna klima ili mehanizam za daljinsko otključavanje ulaznih vrata gdje se vrata otključavaju preko mobilnog uređaja.



Grafikon 8. Odgovori na Pitanje 8. najzastupljeniji IoT uređaji

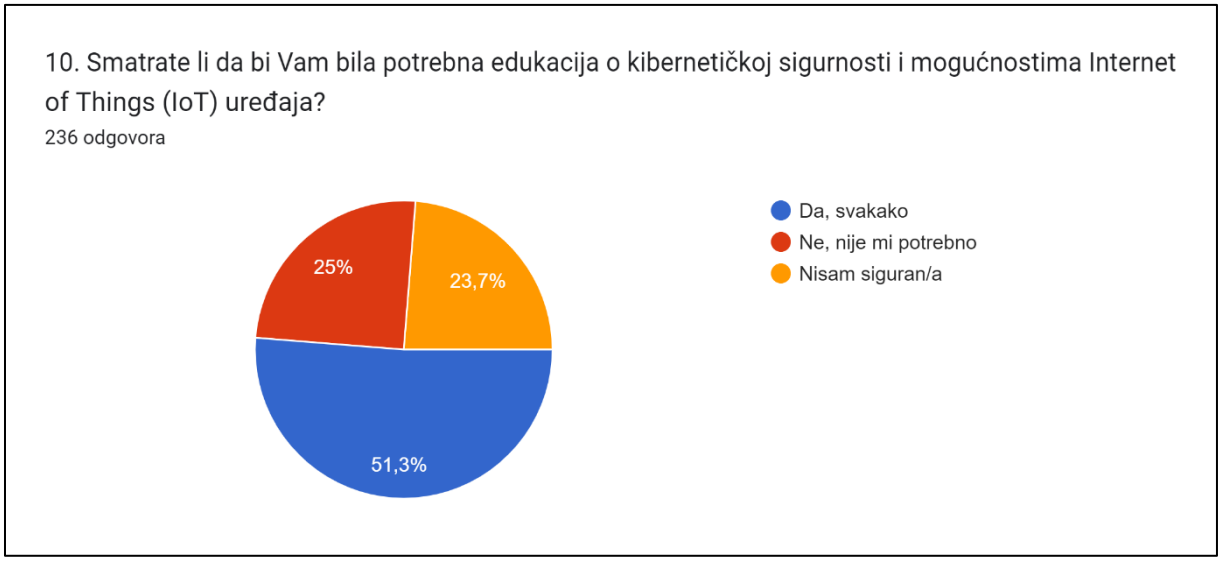
Nastavno na tematiku IoT-a, pitanje 9. ispituje što korisnici misle o sigurnosti IoT-a, odnosno jesu li njihovi podaci kompromitirani korištenjem IoT uređaja. Rezultat je poprilično izjednačen, no treba naglasiti da se više od polovice (52,4%) ispitanika osjeća sigurno pri korištenju IoT uređaja te ne smatraju kako bi njihovi podaci mogli biti kompromitirani.



Grafikon 9. Pitanje 9. kompromitiranost podataka

Prema Kaspersky, [8] pružatelju usluga kibernetičke sigurnosti i antivirusne zaštite, najveća zabrinutost izražena je oko sigurnosti kućnih nadzornih sustava, kamera povezanih s internetom te pametnih vrata i brava, pri čemu je otprilike trećina korisnika priznala da su vrlo zabrinuti za svoju sigurnost i zaštitu. Tako je 32 % korisnika nadzornih/sigurnosnih sustava priznalo da su

"jako zabrinuti" za sigurnost i zaštitu svojih uređaja. Dodatnih 53 posto bilo je ili "zabrinuto" ili "donekle zabrinuto". Iz prethodnog je moguće uočiti da se rezultat poklapa se rezultatom provedene Ankete. Također, Kaspersky navodi da se 56% korisnika osjeća odgovornim za kibernetičku sigurnost IoT uređaja.



Grafikon 10. Pitanje 10. edukacija o kibernetičkoj sigurnosti

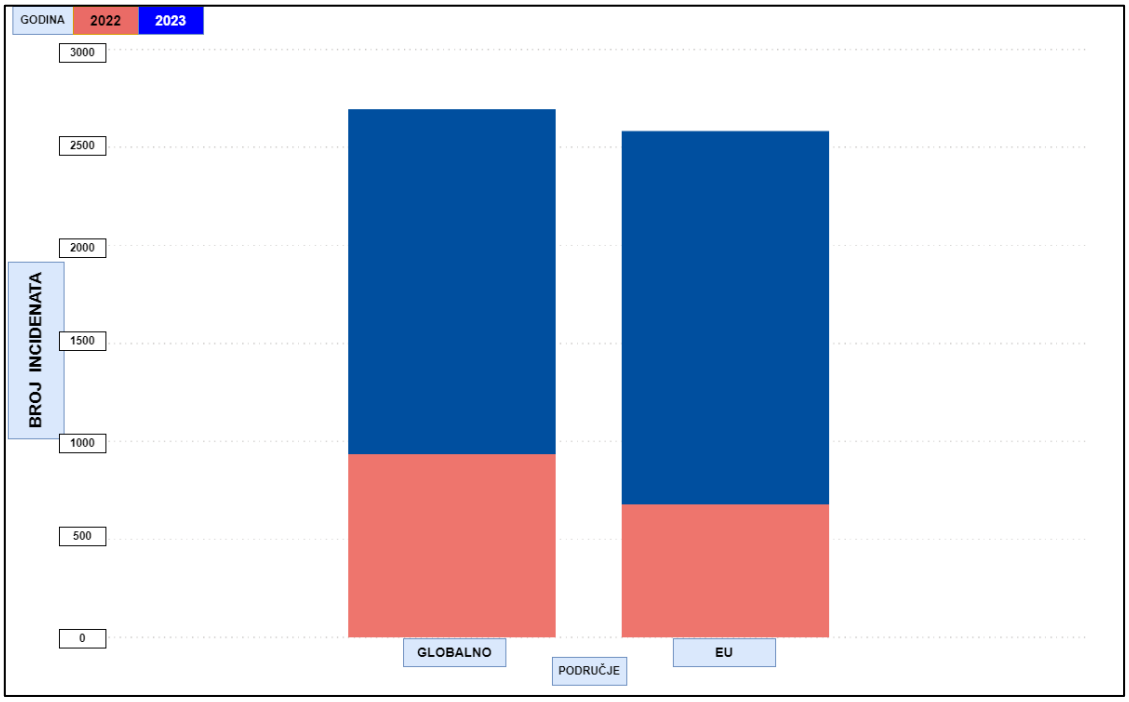
Posljednje pitanje u anketi daje odgovor na to jesu li korisnici zainteresirani za daljnju edukaciju, odnosno misle li da im je potrebna dodatna edukacija o kibernetičkoj sigurnosti. Rezultat je u najmanju ruku pozitivan, a obzirom da samo 25% ispitanika nije zainteresirano i misli kako im edukacija nije potrebna, a čak 51,3% bi rado pristupili edukaciji. Također, zanimljivo je kako u prethodnom 9. pitanju 52,4% ispitanika smatra da njihovi podaci nisu kompromitirani, no u 10. pitanju 51,3% smatra kako bi im bila potrebna dodatna edukacija o kibernetičkoj sigurnosti.

Iz navedenog se može zaključiti da korisnici, odnosno ispitanici nisu dovoljno upoznati s pojmom kibernetičke sigurnosti i kao takvi ostavljaju dojam djeluju nesigurnosti. S 10. pitanjem Ankete završava dio diplomskog rada koji se odnosi na odgovore iste te će u nastavku rada biti objašnjeni pojmovi sadržani u postavljenim pitanjima.

3. Kibernetička sigurnost

Kibernetička sigurnost obuhvaća skup procesa, mjera i standarda kojima se jamči određena razina pouzdanosti pri korištenju proizvoda i usluga u kibernetičkom prostoru, pri čemu sustavna zaštita računala i računalnih mreža, informatičke i informacijske infrastrukture, mobilnih uređaja i podataka od malicioznih napada tome značajno pridonosi, [9].

Kibernetičke prijetnje bilježe kontinuirani porast na globalnoj razini, što se može iščitati iz grafa predstavljenog u izvješću agencije ENISA iz 2023. godine, [10].



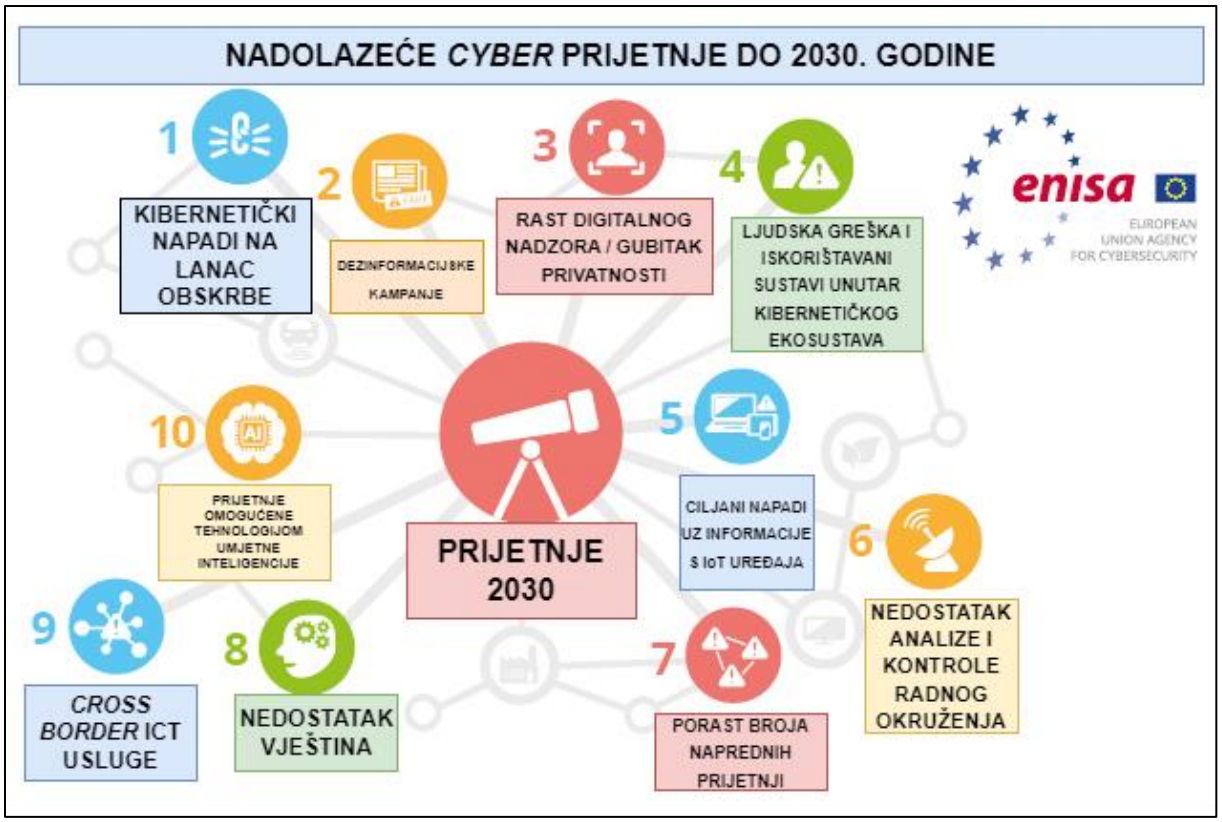
Slika 4. Porast broja kibernetičkih incidenata u 2023. godini
Preuzeo i modificirao autor od ENISA Threat Landscape [10]

Različite vrste napada u kibernetičkom prostoru postaju sve sofisticiranije i složenije i utječu na naš svakodnevni život i poslovanje. ENISA u obliku Threat Landscape-a ukazuje na najčešće korištene vrste napada [11] ali i člancima poput *Emerging Cyber-security Threats for 2030* nastoji predvidjeti nove vrste prijetnji te kako ih identificirati, [12]. Kao što je prikazano slikom 4. radi se o već poznatim prijetnjama kao što su prijetnje uzrokovane ljudskom pogreškom, nedostatkom kontrole kao i nedostatkom vještina. Također, navedene su prijetnje u području „Interneta Stvari[3]“ i Umjetne inteligencije.

[3] „Internet stvari“- (engl. Interner of Things) označava povezivanje uređaja putem interneta. Predstavlja mrežnu infrastrukturu u kojoj fizičke i virtualne "stvari" svih vrsta komuniciraju i nevidljivo su integrirane, str. 30.

Kako nalaže ENISA, prijetnje poput kibernetičkih napada na lanac opskrbe[4] te ICT[5] infrastruktura koja omogućuje *cross-border* [6] usluge mogle bi biti predmet napada. ICT Business navodi kako kibernetički napadi na lance opskrbe softverom nastavljaju rast. Ukupni trošak kibernetičkih napada u lancu opskrbe softvera premašit će 80,6 milijardi dolara na globalnoj razini do 2026., u odnosu na 45,8 milijardi dolara 2023., prema novoj studiji Juniper Researcha. Ovaj rast od 76 posto odražava sve veće rizike od nepostojanja sigurnosnih procesa u lancu nabave softvera i sveukupnu rastuću složenost lanaca nabave softvera. Nova studija naglašava potrebu za većim naglaskom na softverske elemente opskrbnog lanca kao kritičnu sigurnosnu ranjivost. Studija je analizirala kako su za rješavanje ovih rizika potrebni i pomaci u širim procesima kibernetičke sigurnosti i način razmišljanja oko upravljanja lancem nabave softvera. Studija također ispituje važnost lanaca nabave softvera u nekoliko vertikala, uključujući financijske usluge, vladu, automobilsku industriju i zdravstvo, čineći studiju ključnim štivom za ključne dionike u tim visokorizičnim industrijama, [13]. U izdanju iz 2022. godine Telecommunications Policy nastoji istaknuti potrebu za ograničenjem u razmjeni podataka, pogotovo na internacionalnoj razini. Trgovina digitalnom robom i uslugama bilježi sve veći rast posljednjih godina, popraćen odgovarajućim porastom protoka podataka preko nacionalnih granica. U isto vrijeme, vlade diljem svijeta donijele su podatkovne politike koje ograničavaju takve prekogranične protoke podataka u nastojanju da zatraže suverenitet nad podacima generiranim unutar svojih zemalja. [14]

[4] Lanac opskrbe- skup je aktivnosti, objekata i sredstava distribucije neophodnih za provođenje cjelokupnog procesa prodaje proizvoda.
[5] ICT- Informacijska i komunikacijska tehnologija, *IKT* je informacijsko-komunikacijska tehnologija.
[6] *Cross-border* usluge- prekogranične usluge.



Slika 5. Kibernetičke prijetnje u nastajanju 2030
Preuzeo i modificirao autor od ENISA [12]

Anketa „Razvijanje svijesti građana RH" u svrhu izrade diplomskog rada ne sadrži pitanja na temu nadolazećih napada, već je koncipirana kako bi mogla dati trenutni uvid u razumijevanje navedenih tema od strane ispitanika. Iz tog razloga su kao odgovor bili ponuđeni kibernetički napadi koji su navedeni u već spomenutom ENISA Landscape-u. Dodatno, svaki od tih napada biti će deteljnije pojašnjen dalje u tekstu.

Različiti maliciozni programi, računalne prijevare, zloporabe osobnih i financijskih podataka te zloporabe na društvenim mrežama samo su neki od njih. Upravo iz tog razloga vrlo je bitna svijest o mogućim kibernetičkim prijetnjama i kako se od njih zaštititi. Kao što je prikazano na grafikonu, 88% posto ispitanika Ankete se susrelo sa pojmom kibernetičke sigurnosti, što je ujedno loš rezultat jer pokazuje nedovoljnu educiranost ispitanika u teme ispitivane anketnim upitnikom.

3.1. Kibernetički napadi

Postoje različite vrste kibernetičkih odnosno *cyber* napada. Sljedeće su navedeni najčešći kibernetički napadi po uzoru za ENISA Threat Landscape, [10]:

1. Phishing: Napadači koriste lažne e-pošte, web stranice ili druge oblike komunikacije kako bi dobili osjetljive informacije od žrtava, kao što su korisnička imena, lozinke, brojevi kreditnih kartica i druge vrste podataka.

2. Malware: Ovo je širok pojam koji obuhvaća različite vrste zlonamjernog softvera, uključujući viruse, crve, trojanske konje i druge oblike koji se mogu instalirati na računalu bez znanja korisnika i koji mogu nanijeti štetu, kao što su krađa podataka, uništavanje podataka ili ometanje rada sustava.

3. DDoS napadi: Ovo je skraćenica od Distributed Denial of Service, što znači da napadači preplavljuju web stranicu ili mrežu velikim brojem zahtjeva, zbog čega postaje nedostupna za legitimne korisnike.

4. Ransomware: Ovaj napad koristi zlonamjerni softver koji šifrira podatke na računalu žrtve, što sprječava pristup do podataka dok žrtva ne plati otkupninu.

5. Man-in-the-middle napad: Ovo je napad u kojem napadač preuzima kontrolu nad komunikacijom između dvije strane i može ukrasti ili mijenjati podatke u prijenosu.

6. Zero-day ranjivosti: To su ranjivosti koje su otkrivene u softverskim proizvodima i koje nisu javno poznate. Napadači ih mogu iskoristiti prije nego što ih proizvođač popravi.

Ovih 6 primjera cyber napada, bili su ponuđeni kao mogući odgovori u Anketi „Razvijanje svijesti o kibernetičkoj sigurnosti među građanima Republike Hrvatske“ kroz pitanje prikazanom grafikonom.

3.1.1. Phishing napadi

Phishing napadi podrazumijevaju aktivnosti kojima neovlašteni korisnici korištenjem lažiranih poruka elektroničke pošte i lažiranih Web stranica financijskih organizacija pokušavaju korisnika navesti na otkrivanje povjerljivih osobnih podataka. Pritom se prvenstveno misli na podatke kao što brojevi kreditnih kartica, korisnička imena i zaporke, PIN kodovi i sl., iako postoje i druge alternative. Termin phishing dolazi od engleske riječi "*fishing*"

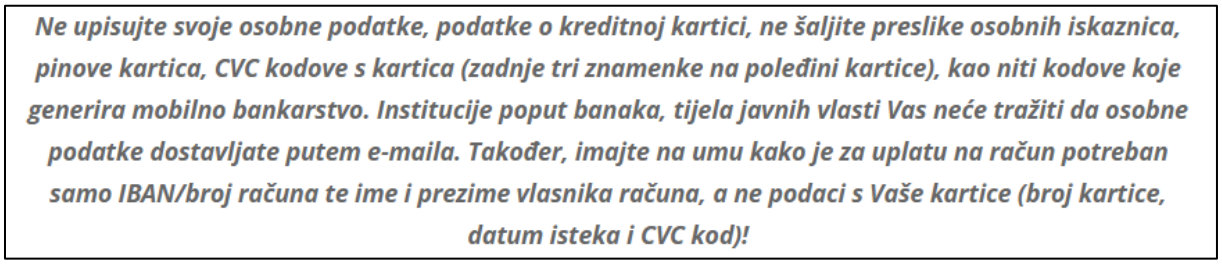
kojom se metaforički opisuje postupak kojim neovlašteni korisnici mame korisnike Interneta kako bi dobrovoljno otkrili svoje povjerljive podatke. Tijek provođenja phishing napada moguće je podijeliti u nekoliko faza, [16]:

1. osmišljavanje i pripremanje napada,
2. provođenje napada,
3. prikupljanje povjerljivih informacija i njihovo iskorištavanje.

Prvi korak osmišljavanja, odnosno pripreme napada podrazumijeva identifikaciju ciljne organizacije, detaljnu analizu sadržaja i uočavanje sigurnosnih propusta unutar Web stranica, identifikaciju ranjivosti na strani klijenta te druge slične postupke. Na temelju prikupljenih informacija napadač kreira lažiranu kopiju Web stranica ciljne organizacije te osmišljava sadržaj phishing poruka koje će prosljeđivati potencijalnim metama napada. Načini kreiranja lažiranih Web stranica ovise prvenstveno o iskustvu i vještini neovlaštenih korisnika, a slično vrijedi i za lažiranje poruka elektroničke pošte. U fazi provođenja napada, napadač šalje pripremljene poruke elektroničke pošte na adrese korisnika koji su odabrani kao potencijalne mete napada. Osim sustava elektroničke pošte, poruke je moguće distribuirati i putem *newsgrupa* i drugih sličnih *instant messaging* servisa, oglašavanjem putem *bannera* na Web stranicama i sl. U finalnoj fazi napada, napadač putem lažiranih Web stranica prikuplja povjerljive informacije od krajnjih korisnika i pohranjuje ih za kasnije korištenje. Prikupljeni podaci mogu se iskoristiti za izravno ostvarivanje financijske koristi ili ih je moguće dalje prodavati zainteresiranim osobama. Krajnji cilj ove faze je svakako financijska korist. Jedan od primjera Phishing napada, koji je nedavno bio poslan velikom broju korisnika je prikazan slikom 6. Otvaranjem poveznice prikazuje se brošura gdje se korisnika traži da upiše osobne podatke.

Slika 6. Primjer Phishing napada u RH
Izvor: Autor

AZOP, Agencija za zaštitu podataka [17] navodi kako se Phishing odnosi na internetske prijevare u vidu lažnih e-poruka koje izgledaju kao da su ih poslale legitimne organizacije (primjerice banka, tijelo javne vlasti ili internet stranica za kupovinu), a koje primatelja navode na dijeljenje osobnih, financijskih ili sigurnosnih podataka. Na ovaj način prevaranti dobivaju pristup korisničkim imenima, lozinkama ili podacima s kreditnih kartica. S obzirom na učestalost online prijevara, koje su često uspješne za napadača, AZOP kroz poruku prikazanu slikom 7. građane podsjeća na oprez prilikom slanja osobnih podataka putem e-poruka ili društvenih mreža.



Slika 7. Obavijest o zaštiti podataka upućena građanima, [17]

Također, Agencija za zaštitu podataka pruža jasne smjernice te primjere Phishing napada, kao i korake za zaštitu od istih.

3.1.2. Malware napadi

Prema Microsoft Security [18], pojam zlonamjerni softver (eng. Malware) odnosi se na zlonamjerne aplikacije ili kod koji oštećuje ili ometa normalno korištenje uređaja krajnjih točaka. Kada se uređaj zarazi zlonamjernim softverom, može doći do neovlaštenog pristupa, ugrožavanja podataka ili blokiranja pristupa uređaju ako ne bude plaćena otkupnina.

Osobe koje distribuiraju zlonamjerni softver, poznate kao računalni zločinci, motivirane su novcem i koristit će zaražene uređaje za pokretanje napada, primjerice za dobivanje bankovnih vjerodajnica, prikupljanje osobnih podataka koji se mogu prodavati, prodaju pristupa računalnim resursima ili iznuđivanje podataka za plaćanje od žrtava. Zlonamjerni softver može doći u mnogim obilcima, najčešći oblik je takozvani „Trojanski konj[7]“ koji sadrži viruse ili „crve[8]“. Trojanski se konji oslanjaju na to da će ih korisnici nesvjesno preuzeti jer djeluju kao bezopasne datoteke ili aplikacije.

[7] Trojanski konj- Trojanski konj ili kraće trojanac je zlonamjerni računalni program koji se lažno predstavlja kao neki drugi program s korisnim ili poželjnim funkcijama.
[8] Crv (engl. Worm) - Računalni su crvi programi koji sami sebe umnožavaju i šire se putem računalne mreže.

Kada se preuzmu, mogu:

- Preuzimati i instalirati dodatni zlonamjerni softver, kao što su virusi ili crvi.
- Koristiti zaraženi uređaj za prijevaru s klikovima.
- Bilježiti pritiske na tipke i posjećena web-mjesta.
- Slati podatke (npr. lozinke, podatke o prijavi i povijest pregledavanja) o zaraženom uređaju zlonamjernim hakerima.
- Računalnim zločincima dati kontrolu nad zaraženim uređajem.

Virusi su osmišljeni tako da ometaju normalno funkcioniranje uređaja zapisivanjem, oštećivanjem ili brisanjem podataka. Često se šire na druge uređaje na temelju prijevara zbog kojih korisnici otvaraju zlonamjerne datoteke. Crvi se najčešće nalaze u privicima e-pošte, SMS-ovima, programima za zajedničko korištenje datoteka, web-mjestima društvenih mreža, zajedničkom sadržaju na mreži i uklonjivim pogonima te se šire mrežom iskorištavanjem sigurnosnih slabih točaka i umnožavanjem samih sebe. Ovisno o vrsti crva, moguća je krađa povjerljivih podataka, promjena sigurnosnih postavki ili onemogućivanje pristupa datotekama, [18]. Zlonamjerni softver javlja se u mnogim oblicima. Prema, Microsoft-u, [18] to su:

- Krađa identiteta - Napad s ciljem krađe identiteta djeluje kao vjerodostojan izvor čija je namjena krađa povjerljivih podataka putem e-pošte, web-mjesta, SMS-a ili drugih oblika elektroničke komunikacije. Ti napadi stvaraju mehanizam isporuke zlonamjernog softvera. Napadima se najčešće kradu korisnička imena, lozinke, podaci o kreditnoj kartici i bankovni podaci. Te vrste napada zlonamjernim softverom mogu dovesti do krađe identiteta ili krađe novca izravno s osobnog bankovnog računa ili kreditne kartice. Na primjer, računalni zločinac može se predstaviti kao poznata banka i poslati poruku e-pošte s upozorenjem da je račun osobe blokiran zbog sumnjive aktivnosti, pozivajući ih da kliknu vezu u poruci e-pošte da bi riješili problem. Kada se veza klikne, instalira se zlonamjerni softver, [19].
- Špijunski softver - Špijunski softver funkcionira tako da se instalira na uređaj bez pristanka korisnika ili davanja odgovarajuće obavijesti. Kada se instalira, može nadzirati ponašanje na internetu, prikupljati povjerljive podatke, mijenjati postavke uređaja i smanjivati performanse uređaja.

- Trojanski konji - Trojanski se konji oslanjaju na to da će ih korisnici nesvjesno preuzeti jer djeluju kao bezopasne datoteke ili aplikacije. Kada se preuzmu, mogu:
  - ❖ Preuzimati i instalirati dodatni zlonamjerni softver, kao što su virusi ili crvi.
  - ❖ Koristiti zaraženi uređaj za prijevaru s klikovima.
  - ❖ Bilježiti pritiske na tipke i web-mjesta koja posjećujete.
  - ❖ Slati podatke (npr. lozinke, podatke o prijavi i povijest pregledavanja) o zaraženom uređaju zlonamjernim hakerima.
  - ❖ Računalnim zločincima dati kontrolu nad zaraženim uređajem.
- Napadi na opskrbni lanac - Ta vrsta zlonamjernog softvera cilja razvojne inženjere i davatelje usluga pristupanjem izvornim kodovima, procesima izgradnje ili mehanizmima ažuriranja u vjerodostojnim aplikacijama. Kada računalni zločinac pronađe neosigurani mrežni protokol, nezaštićenu poslužiteljsku infrastrukturu ili nesigurnu praksu kodiranja, provaljuje, mijenja izvorne kodove i skriva zlonamjerni softver u međuverziji i procesima ažuriranja.
- Crvi - Crvi se najčešće nalaze u privicima e-pošte, SMS-ovima, programima za zajedničko korištenje datoteka, web-mjestima društvenih mreža, zajedničkom sadržaju na mreži i uklonjivim pogonima te se šire mrežom iskorištavanjem sigurnosnih slabih točaka i umnožavanjem samih sebe. Ovisno o vrsti crva, moguća je krađa povjerljivih podataka, promjena sigurnosnih postavki ili onemogućivanje pristupa datotekama.
- Zlonamjerni softver bez datoteka - Ta vrsta računalnog napada u općenitom smislu opisuje zlonamjerni softver koji se za neovlašten pristup mreži ne oslanja na datoteke, primjerice zaraženi privitak e-pošte. Takvi se napadi primjerice mogu izvoditi putem zlonamjernih mrežnih paketa koji iskorištavaju ranjivost, a zatim instaliraju zlonamjerni softver koji se nalazi samo u memoriji jezgre. Prijetnje bez datoteka posebno je teško otkriti i ukloniti jer većina antivirusnih programa nije namijenjena skeniranju programske opreme.
- Ucjenjivački softver - Ucjenjivački softver vrsta je zlonamjernog softvera putem kojega se žrtvama prijeti uništavanjem bitnih podataka ili sustava odnosno blokiranjem pristupa njima sve dok se ne plati otkupnina. Napadi ucjenjivačkim softverom kojima upravljaju ljudi ciljaju tvrtku ili ustanovu kroz uobičajene pogreške u sustavu i sigurnosti te ulaze u tvrtku ili ustanovu, kreću se njezinom poslovnom mrežom i prilagođavaju okruženju i svim slabostima. Uobičajen način pristupanja mreži tvrtki ili ustanova radi isporuke ucjenjivačkog softvera krađa je vjerodajnica u sklopu koje računalni zločinac može ukrasti vjerodajnice stvarnog zaposlenika da bi se predstavljao

kao on i ostvario pristup računima tog zaposlenika. Napadači koji koriste ucjenjivački softver kojim upravljaju ljudi ciljaju na velike tvrtke ili ustanove jer mogu platiti višu otkupninu od prosječne osobe, a ta se otkupnina često mjeri u milijunima dolara. Budući da su kršenja sigurnosti te razine visokorizična, mnoge tvrtke ili ustanove odlučuju platiti otkupninu da im se ne bi dogodilo da povjerljivi podaci procure i jer ne žele riskirati daljnje napade računalnih zločinaca, iako plaćanje ne jamči da neće doći do takvog ishoda, [20].

3.1.3. Denial of Service napadi

DDoS[9] napad cilja web-mjesta i poslužitelje ometanjem mrežnih usluga u pokušaju iscrpljivanja resursa aplikacije. Napadači iza tih napada preplavljuju web-mjesto nasumičnim prometom, što rezultira lošom funkcionalnošću web-mjesta ili potpunim izbacivanjem s mreže, [21].

Tijekom DDoS napada niz *botova*[10] ili mreža *botova* preplavljuju web-mjesto ili servis HTTP zahtjevima i prometom. To u načelu znači da više računala napada jedno računalo, što izbacuje stvarne korisnike. Zbog toga pružanje usluge može kasniti ili na neki drugi način biti ometano tijekom određenog razdoblja. Hakeri tijekom napada mogu ući i u bazu podataka i pristupiti povjerljivim podacima. DDoS napadi mogu iskoristiti sigurnosne propuste i ciljati sve krajnje točke koje su javno dostupne putem interneta, [21].

Napadi s uskraćivanjem usluge mogu potrajati satima, pa čak i danima. Ti računalni napadi također mogu uzrokovati višestruke prekide tijekom jednog napada. Metom mogu postati i osobni i poslovni uređaji. Postoji nekoliko vrsta DDoS napada, [21]. Tri su primarne kategorije DDoS napada: volumetrijski napad, napad na protokol i napad na sloj resursa.

Volumetrijski napad preplavljuje mrežni sloj onime što se na početku čini vjerodostojnim prometom. Ta je vrsta napada najčešći oblik DDoS napada. Primjer volumetrijskog napada jest povećanje DNS-a (engl. *Domain Name Server*) u kojem se koriste otvoreni DNS[11] poslužitelji za preplavljivanje mete prometom odgovora na DNS.

[9] DDoS napad- (engl. Distributed Denial-of-service) - Napadi uskraćivanjem resursa pomoću posebno pripremljenih mrežnih paketa.
[10] Bot, botovi - skraćeni naziv za robota, u značenju računalnog programa koji se izvršava samostalno.
[11] DNS - Sustav domenskih imena ili DNS je hijerarhijski distribuirani sustav imenovanja za servise te računala i ostale uređaje spojene na Internet ili privatnu mrežu.

Napad na protokol uzrokuje prekid usluge iskorištavanjem slabosti u stogu protokola sloja 3 i sloja 4. Jedan od primjera je sinkronizirani ili SYN napad koji troši sve dostupne resurse poslužitelja. Napad na sloj resursa (ili aplikacijski sloj) cilja pakete web-aplikacija i ometa prijenos podataka između glavnih računala. Primjeri te vrste napada obuhvaćaju kršenja HTTP protokola[12], SQL injekciju[13], skriptiranje na više web-mjesta i druge napade na sloj.

Računalni napadači mogu koristiti jednu ili više vrsta napada na mrežu. Napad, primjerice, može početi kao jedna klasa napada, a zatim se pretvoriti u drugu ili se povezati s drugom prijetnjom da bi uzrokovao kaos u sustavu. Osim toga, svaka kategorija obuhvaća više različitih računalnih napada. Broj novih internetskih prijetnji sve je veći i očekuje se daljnji rast jer računalni zločinci postaju sofisticiraniji, [21].

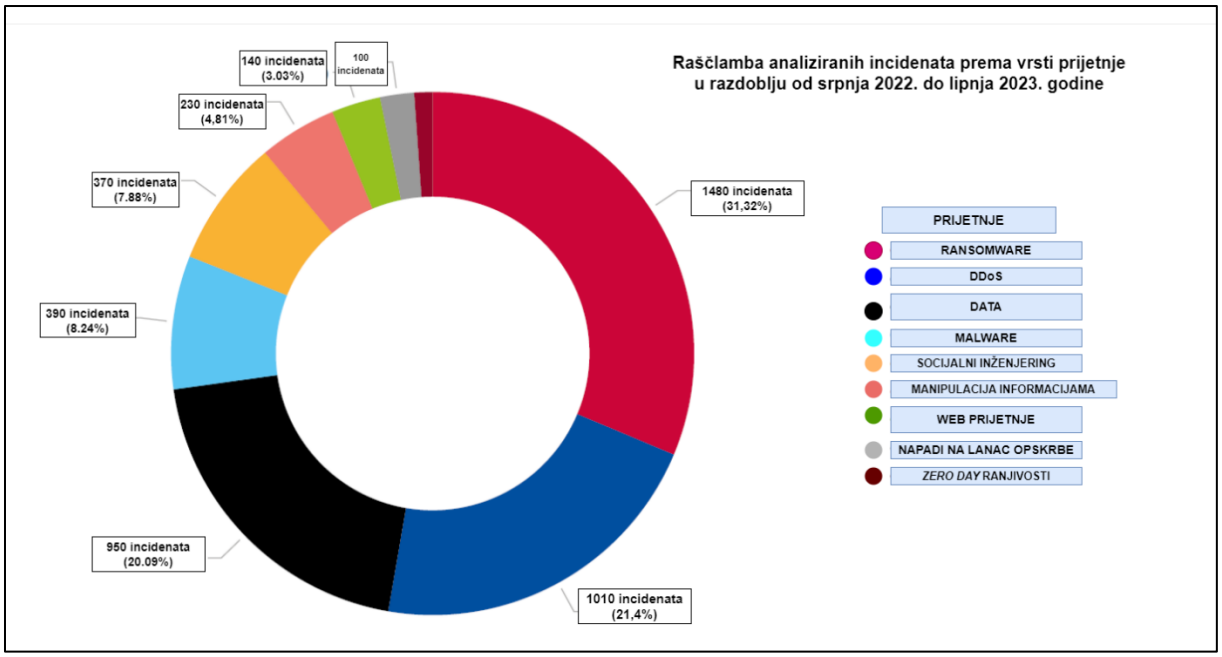
3.1.4. Ransomware napadi

Ransomware je naziv za skup zlonamjernih programa koji korisniku onemogućuju korištenje računala. Nakon zaraze ransomware može šifrirati datoteke ili onemogućiti korištenje tako da se pojavi početni ekran s određenom porukom koju nije moguće maknuti. Od korisnika čije je računalo zaraženo traži se otkupnina u zamjenu za daljnje normalno korištenje računala. U zadnje vrijeme sve je više slučajeva u kojem se pojavljuje prvi navedeni slučaj u kojem zlonamjerni softver šifrira korisničke podatke i u zamjenu za njihovo dešifriranje traži uplatu određenih novčanih sredstava, [22].

Razlikuju se dvije vrste Ransomware napada. Automatizirani napadi ransomwarea i napadi ransomwarea kojima upravljaju ljudi. Prije daljnje analize Ransomware napada, vrijedi napomenuti kako je prilikom analize incidenata provedenih od strane Agencije Europske unije za kibersigurnost, u razdoblju od srpnja 2022. do lipnja 2023. godine, čak 31,32% napada pripadalo Ransomware-u.

[12] HTTP – (engl. *Hypertext Transfer Protocol*) HTTP je glavna i najčešća metoda prijenosa informacija na Webu. Osnovna namjena ovog protokola je omogućavanje objavljivanja i prezentacije HTML dokumenata, tj. web stranica, definicija dostupna na str. 24.

[13] SQL Injection - U računalstvu, SQL injection je tehnika ubacivanja koda koja se koristi za napad na aplikacije vođene podacima, definicija dostupna na str. 28.



Slika 8. Raščlamba incidenata prema vrsti prijetnje
Preuzeo autor od ENISA Threat Landscape 2023 []

Napadi ransomwareom obično su automatizirani. Ti se kibernetički napadi mogu širiti poput virusa, zaraziti uređaje putem metoda kao što su krađa identiteta e-poštom i isporuka zlonamjernog softvera te zahtijevaju uklanjanje zlonamjernog softvera. To znači da je jedna od tehnika prevencije ransomwarea zaštita pošte moguća pomoću sustava poput Microsoft Defender za Office 365 ili Microsoft 365 Defender, kako bi se rano zlonamjerni softver i pokušaj krađe identiteta. Ransomware kojim upravljaju ljudi rezultat je aktivnog napada kibernetičkih kriminalaca koji se infiltriraju u lokalnu IT infrastrukturu organizacije ili IT infrastrukturu u oblaku, podižu njihove privilegije i postavljaju ransomware na kritične podatke.

Ovi napadi ciljaju na organizaciju, a ne na jedan uređaj. Ljudsko upravljanje znači da postoji ljudski napadač koji koristi svoje uvide u pogrešne konfiguracije uobičajenog sustava i sigurnosti kako bi se infiltrirao u organizaciju, kretao se mrežom i prilagođavao okruženju i njegovim slabostima u hodu. Obilježja ovih napada ransomwarea kojima upravljaju ljudi obično uključuju krađu te povećanje privilegija u ukradenim računima. Aktivnosti se mogu odvijati tijekom razdoblja održavanja. Cilj napadača je implementacija ransomwarea na sve resurse s velikim poslovnim utjecajem, [23].

Navedeno je nekoliko napada koje je objavio Microsoft Security Intelligence, [24]:

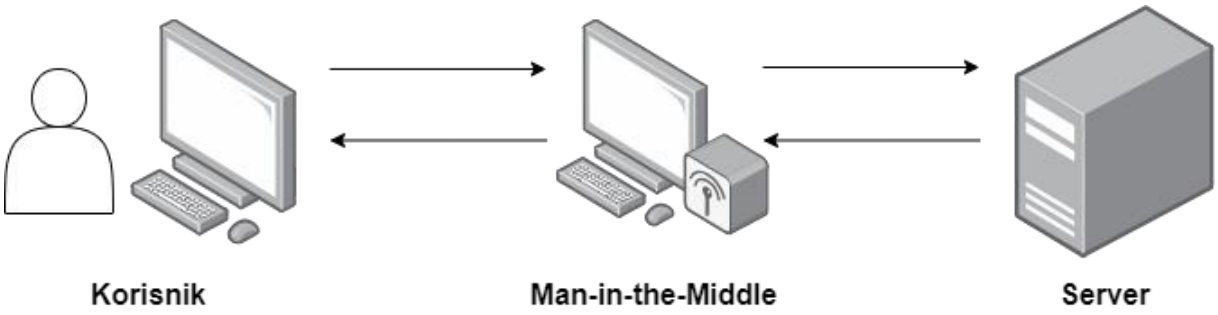
- U ožujku 2022. grčki je poštanski sustav postao žrtva ucjenjivačkog softvera. Napad je privremeno onemogućio dostavu pošte i obradu zahvaćenih financijskih transakcija.
- Jedna od najvećih indijskih zrakoplovnih tvrtki bila je meta napada ucjenjivačkim softverom u svibnju 2022. Posljedice tog Incidenta bila su kašnjenja i otkazivanja letova te stotine putnika koji su morali čekati.
- Velika tvrtka za ljudske potencijale bila je meta napada ucjenjivačkim softverom u prosincu 2021. i pritom je bio ugrožen sustav plaća i dopusta koji su upotrebljavali klijenti servisa u oblaku te tvrtke.
- U svibnju 2021. američki je sustav cjevovoda za gorivo prekinuo pružanje svojih usluga da bi spriječio daljnja kršenja sigurnosti nakon što su napadom pomoću ucjenjivačkog softvera ugroženi osobni podaci tisuća zaposlenika. Zbog toga su naglo porasle cijene goriva na cijeloj istočnoj obali.
- Njemačka tvrtka za distribuciju kemikalija bila je meta napada ucjenjivačkim softverom u travnju 2021. Ukradeni su podaci o više od 6000 osoba, i to datumi rođenja, brojevi socijalnog osiguranja i brojevi vozačkih dozvola, baš kao i neki medicinski podaci.
- Najveći dobavljač mesa na svijetu postao je meta napada ucjenjivačkim softverom u svibnju 2021. Nakon što je privremeno onemogućila pristup svom web-mjestu i zaustavila proizvodnju, tvrtka je platila 11 milijuna dolara u kriptovaluti Bitcoin.

Nastavno, Business Standard obavještava kako su hakeri sa sjedištem u Kini provalili u račune e-pošte europskih vlada, što je potvrđeno od strane Microsofta, [24]. Grupa je dobila pristup računima e-pošte koji su utjecali na oko 25 organizacija, uključujući vladine agencije i račune pojedinaca povezanih s tim organizacijama, a napad je bio neprimijećen oko mjesec dana dok se klijenti nisu žalili Microsoftu na visoke aktivnosti pošte.

3.1.5. Man-in-the middle napadi

Napad Man-in-the-Middle zahtijeva od napadača da se smjesti između dvije strane koje komuniciraju i da im šalje poruke, dok strane vjeruju da međusobno komuniciraju izravno i sigurno. Napadač tada može nadzirati i eventualno mijenjati sadržaj poruka. MitM koncept nije ograničen na računalnu sigurnost, slični napadi postojali su u fizičkom svijetu puno prije

računala. Izvođenje MitM napada na računalne mreže obično zahtijeva dva različita koraka: presretanje neobrađenih podataka i, ako postoji, zaobilaženje enkripcije i autentifikacije, [25]. MitM napadi postoje za mnoge komunikacijske protokole. Slikom 9. prikazana je ilustracija Man-in-the-Middle napada.



Slika 9. Ilustracija Man-in-the-Middle napada,
Izvor: Autor

Man-in-the-middle napadi tajno postavljaju dio softvera ili *rogue router* [14] između poslužitelja i korisnika za što ni administracija poslužitelja ni korisnik nisu svjesni. Man-in-the-Middle napada i presreće podatke te ih zatim šalje poslužitelju kao da odvija normalna komunikacija. Poslužitelj odgovara softveru, misleći da komunicira s legitimnim klijentom, [27].

3.1.6. Ostale vrste kibernetičkih napada

Važno je spomenuti i ostale vrste kibernetičkih napada. U sedmom izdanju CompTIA Security Study Guide-a spominju se napadi kao što su *Zero-day* ranjivosti i SQL Injection dok ENISA Threat Landscape navodi napad vezan uz manipulaciju informacijama.

Zero-day ranjivost je sigurnosni propust u računalnoj aplikaciji koji je otkriven i poznat je napadačima prije nego što za njega sazna proizvođač i javnost. Za takvu ranjivost proizvođač još nije objavio zakrpe koje uklanjaju problem. Izraz „zero day“ ili „nulti dan“ nastao je kao vremenska oznaka ranjivosti. Zero-day napad se obično javlja prije prvog ili nultog dana svjesnosti proizvođača o ranjivosti, što znači da proizvođač još nije imao priliku popraviti sigurnosni propust kojeg napadač koristi za pokretanje napada, [28]. Vrlo je teško odgovoriti na *zero-day exploit*. Ako napadači saznaju za slabost isti dan kad i programer, tada će imati mogućnost iskorištavanja sve dok se ne objavi *patch* odnosno „zakrpa“ za isti sustav, [27].

[14] *Rogue router* odnosno *Rogue Access Point* -Lažna pristupna točka je bežična pristupna točka koja je instalirana na sigurnu mrežu bez izričitog odobrenja administratora lokalne mreže, bilo da je dodao dobronamjerni zaposlenik ili zlonamjerni napadač, definicija dostupna na str. 27.

Nakon što prođe određeno vrijeme od objave zero-day ranjivosti tvrtka u čijem je programskom paketu otkrivena ranjivost može izdati zakrpe koje ju uklanjaju. Čak i u slučaju kada propust otkriju zlonamjerni korisnici, potrebno je neko vrijeme prije nego što ranjivost bude iskorištena za pokretanje napada jer oni obično prvo pokušaju prodati podatke o ranjivosti ili sami napisati zloćudni programski kod koji iskorištava ranjivost. Pisanje takvog programskog koda nije uvijek jednostavno. U tom vremenu tvrtka ima priliku ukloniti ranjivost prije nego ju netko zlouporabi. Međutim, iskustvo pokazuje da ranjivost najčešće otkriju zlonamjerni korisnici. U tom slučaju može se dogoditi da su i ranjivost i vektori napada objavljeni na isti dan, što znači da je programski paket u kojem je otkriven propust izuzetno podložan napadu protiv kojeg još uvijek ne postoji zaštita, [28].

SQL (engl. Structured Query Language) je strukturni upitni jezik, programski jezik visoke razine. Najpopularniji je računalni jezik za izradu, traženje, ažuriranje i brisanje podataka iz relacijskih baza podataka, [29].

Prilikom SQL Injection napada, napadač manipulira kodom baze podataka kako bi iskoristio slabost u njoj. Na primjer, ako sučelje očekuje od korisnika da unese vrijednost *string*, odnosno niz znakova, ali nije posebno kodirano na taj način, napadač bi mogao unijeti redak koda i taj bi se kôd zatim izvršio umjesto da bude prihvaćen kao vrijednost *string*, [27].

Skraćenica FIMI (engl. Foreign Information Manipulation and Interference) u posljednje je vrijeme naišla na veliki uspjeh te se stoga sve više koristi. Izraz je raširen u Europskoj uniji, unutar Europske službe za vanjsko djelovanje (EEAS[15] engl. European External Action Service) i diljem država članica, [30]. Opisuje uglavnom neilegalni obrazac ponašanja koji prijeti ili ima potencijal negativno utjecati na vrijednosti, postupke i političke procese. Takva aktivnost je manipulativnog karaktera, provodi se namjerno i koordinirano, [10].

[15] EEAS - European External Action Service, Europska služba za vanjsko djelovanje funkcionalno je autonomno tijelo Europske unije pod nadležnošću Visokog predstavnika Unije za vanjske poslove i sigurnosnu politiku.

4. Kibernetička sigurnost Interneta stvari

Razvojem IoT-a iz mreža ograničenog pristupa u distribuiranu javnu mrežu povećala se potreba za sigurnosnim alarmima za zaštitu međusobno povezanih IoT uređaja od upada kao što su modifikacije podataka, ubrizgavanje zlonamjernog koda, uskraćivanje usluge i mnogih drugih prijetnji. Povezivanje uređaja u Internet stvari, iako predstavlja učinkovitije i brže korištenje raznih sustava, zahtijeva i podatke (datume rođenja, adrese i druge podatke) bez kojih putem internetske veze ne bi bila moguća razmjena informacija s drugim uređajima ili nekom udaljenom bazom podataka. Zato je važna sigurnost sustava Interneta stvari, ali i osobnih podataka koji se razmjenjuju, [31].

Ne postoji jedinstvena definicija što je to Internet stvari i one se razlikuju ovisno o perspektivi iz koje se promatraju i širini pogleda na procese koji se događaju, ali većina se odnosi na spajanje uređaja koji se koristi svakodnevno na internetu u svrhu mjerenja, prikupljanja, pohrane i razmjene podataka s ostalim 'stvarima' i ljudima. Internet stvari daje mogućnost automatiziranja velike većine poslova i svakodnevnih aktivnosti, a "stvar" u Internetu stvari može biti doslovno svaki uređaj u stvarnom životu, od osobnog računala, pametnih telefona, automobila, strojeva, kućanskih aparata pa do vrata, prozora, namještaja i svega ostaloga što čovjek može zamisliti, [31].

Trenutno usvojeni sigurnosni protokol i kriptografske postavke zahtijevaju značajne resurse i IoT uređaje kao što su pametni telefoni, tableti, računala, usmjerivači, aktivni senzori ili pasivne RFID (engl. Radio Frequency Identification) oznake, a koji imaju vrlo ograničene resurse i mogućnosti za podršku implementaciji i prilagodbi tradicionalne sigurnosti protokolarnih rješenja. Stoga implementacija i prilagodba tradicionalnih sigurnosnih protokola i dalje ostaje izazov zbog čega je teško osigurati povjerljivost prijenosa podataka. Budući da se IoT uređaji ne nadziru jer rade na način samoodržavanja s ograničenim održavanjem (npr. nadzor), to dodatno dovodi do zabrinutosti u smislu integriteta podataka (povjerenja). Kao rezultat, podaci dobiveni s IoT uređaja vjerojatno će biti niske kvalitete ili oštećeni. Postoje različiti sigurnosni izazovi i ograničenja vezana uz IoT, a koja utječu na usvajanje velikih razmjera. IoT sigurnost jedan je od glavnih izazova kibernetičke sigurnosti današnjice. Postoji nekoliko izazova. IoT uređaji također mogu osigurati prostor za napadače koji žele provoditi distribuirane napade uskraćivanja usluge (DDoS), [32].

4.1. Prijetnje koje utječu na sigurnost IoT-a

Ovo poglavlje predstavlja niz prijetnji koje se smatraju najrelevantnijima u kontekstu „Interneta stvari“. Prema ENISA, *Guidelines for Securing the Internet of Things* postoji pet vrsta prijetnji, [33]:

1. Fizički napadi (Namjerni) – jedan od primjera su neispravni, odbačeni ili izgubljeni proizvodi mogu završiti na sivim tržištima koja postoje izvan odgovarajućih distribucijskih kanala. To može dovesti do nepredviđenih posljedica i dodati brojne poteškoće u provedbi strogih sigurnosnih standarda i standarda kvalitete ubacivanjem neprovjerenih i nepouzdanih proizvoda na tržište.
2. Gubitak intelektualnog vlasništva - Zlonamjerni akteri mogu biti u mogućnosti nezakonito steći, iskoristiti, pohraniti ili redistribuirati intelektualno vlasništvo i osjetljive dijelove informacija (npr. projektne dokumente, izvorni kod, vjerodajnice ili druge tajne). Oni pružaju uvid u ranjivosti određenih IoT proizvoda i mogu poslužiti kao vrijedna sredstva za napadače.
3. Podla aktivnost/zlonamjerni softver (engl. malware) - Napadačima se pruža mogućnost umetanja zlonamjernog softvera čiji je glavni cilj omogućiti nedopušteni pristup ili bilo koju drugu funkcionalnost koja je u suprotnosti s namjeravanom upotrebom sustava. Nesigurni mehanizmi ažuriranja i zatrovane usluge ažuriranja glavni su primjeri takvih prilika za ubacivanje zlonamjernog softvera. IoT pristupnici posebno su relevantni u ovom kontekstu; to su funkcionalni uređaji koji se obično nalaze u IoT arhitekturama, ali također mogu funkcionirati kao izvor prijetnji. IoT pristupnici obično imaju pomoćnu ulogu u opsegu sigurnosnih zahtjeva, oni su, međutim, put za kompromitiranje IoT uređaja za zlonamjernog aktera, pružajući pristup pouzdanim mrežama i metodu za prikupljanje podataka s podržanih ograničenih uređaja.
4. Legalne prijetnje - Posljedice zbog neusklađenosti sa standardima i propisima. Procesi projektiranja oko privatnosti/enkripcije izazov su na koji utječu postojeći zakoni i propisi o privatnosti te činjenica da neki akteri u ekosustavu opskrbnog lanca imaju različito razumijevanje sigurnosnih aspekata. SLA (engl. *Service Level Agreement*) se potpisuje između različitih sudionika u opskrbnom lancu kako bi se osigurao zajednički ugovorni pogled na sigurnosne aspekte. Svi uređaji trebaju biti u skladu sa sigurnosnim smjernicama koje zahtijevaju odgovarajuće industrije (npr. energetska, medicinska,

automobilska). Štoviše, GDPR i bilo koji drugi lokalni propisi trebaju se primijeniti kako bi se pokrili rizici povezani s nepridržavanjem standarda/propisa.

5. Nenamjerno oštećenje ili gubitak informacija - Ugrožavanje mrežnih sustava koji su neophodni za kontrolu procesa opskrbnog lanca i postoje u mreži moglo bi postati ugroženo bez odgovarajuće politike QoS-a ili vatrozida (engl. *Firewall*). Ova se imovina može koristiti kao oružje za orkestriranje, na primjer, napada uskraćivanja usluge (DoS) velikih razmjera ili za degradaciju rada opskrbnog lanca. Oni koji imaju pristup Internetu su najranjiviji, iako su izolirane interne mreže također u opasnosti od insajderskih napada.

OWASP projekt (eng. Open Web Application Security Project) koji je nastao kao rezultat rada sigurnosnih stručnjaka s ciljem otkrivanja postojećih ranjivosti i pružanja smjernica u osiguravanju web aplikacija započeo je 2014. godine s istraživanjem sigurnosti Interneta stvari. Rezultati istraživanja trebali bi utjecati na stvaratelje i korisnike Interneta stvari i potaknuti ih na donošenje boljih odluka pri razvijanju Interneta stvari, ali i pri njihovom korištenju. OWASP je 2018. godine izdao dokument „OWASP IoT Top 10“ u kojem navode deset stvari koje treba izbjegavati prilikom izgradnje, implementacije, korištenja i održavanja IoT sustava, [31]:

1. Slabe ili predefinirane lozinke - Korištenje slabih lozinki ili predefiniranih lozinki koje napadači mogu pronaći na internetskim stranicama samog proizvoda ili doći do njih nekom od hakerskih metoda kao što je *Bruteforce* metoda (pogađanje lozinki).
2. Nesigurne mrežne usluge - Veliku prijetnju predstavljaju nepotrebne ili nesigurne mrežne usluge koje se pokreću na samim uređajima, a napadači ih jednostavno mogu otkriti i iskoristiti za udaljeni pristup ili izvršavanje drugih zlonamjernih radnji. Posebno su ranjive one usluge direktno spojene na Internet koje ugrožavaju povjerljivost, integritet ili dostupnost informacija ili dopuštaju neovlašteno daljinsko upravljanje.
3. Nesigurno sučelje ekosustava - Nezaštićene web stranice, sučelja API-ja (eng. *Application Programming Interface* – aplikacijsko programsko sučelje), oblak ili mobilna sučelja u ekosustavu izvan uređaja koji dopuštaju kompromitiranje uređaja ili njegovih povezanih komponenti predstavljaju značajnu prijetnju. Uobičajeni problemi uključuju nedostatak autentifikacije / autorizacije, nedostatak ili slabe lozinke te nedostatak filtriranja ulaznih i izlaznih podataka.
4. Nedostatak mehanizma ažuriranja - Nedostatak mogućnosti sigurnog ažuriranja uređaja uključuje nedostatak provjere valjanosti firmware-a na uređaju, nedostatak

mehanizama za vraćanje u početni položaj i nedostatak obavijesti o sigurnosnim promjenama zbog ažuriranja.

5. Korištenje nesigurnih ili zastarjelih komponenti - Korištenje zastarjelih ili nesigurnih softverskih komponenti / biblioteka koje omogućuju kompromitiranje uređaja. To uključuje nesigurno konfiguriranje operacijskog sustava te korištenje softverskih ili hardverskih komponenti trećih strana iz nepouzdanih izvora.
6. Nedovoljna zaštita privatnosti - Osobni podaci korisnika pohranjeni na uređaju ili u ekosustavu koji se koriste nesigurno, nepropisno ili bez dopuštenja.
7. Nesiguran prijenos i pohrana podataka - Nedostatak enkripcije ili kontrole pristupa osjetljivim podacima bilo gdje unutar ekosustava, uključujući u mirovanju, u prijenosu ili tijekom obrade.
8. Nedostatak upravljanja uređajem - Nedostatak sigurnosne podrške na uređajima koji se koriste u IoT sustavima od proizvodnje do nadzora sustava.
9. Nesigurne zadane postavke - Uređaji ili sustavi isporučuju se s nesigurnim zadanim postavkama ili ne dopuštaju da korisnik sam postavlja sigurnosna ograničenja ili mijenja konfiguracijske postavke.
10. Nesigurnost fizičkog pristupa - Nedostatak kontrole fizičkog pristupa pojedinim dijelovima sustava omogućuju napadačima da dođu do osjetljivih podataka ili preuzmu kontrolu nad sustavom.

4.2. IoT Enkripcija

U kontekstu IoT-a, sigurnosni izazovi, uključujući privatnost, sigurnu pohranu, autorizaciju, komunikaciju, kontrolu pristupa i administraciju, temeljni su i složeni problemi. Budući da samo ovlašteni korisnik treba imati pristup podacima i često ih ažurirati za inteligentne aplikacije, IoT sigurnost treba poboljšati uz osiguranu povezanost. Najbolji algoritmi za IoT sigurnosne resurse su kriptografski algoritmi. U tom kontekstu, tradicionalni algoritmi šifriranja pružaju obradu podataka i sigurnost. Ovi algoritmi zahtijevaju velike matematičke operacije i trebaju veliku memoriju i snagu. Stoga nisu prikladni za enkripciju na IoT uređajima. Međutim, ti se uređaji trenutačno koriste u Internetu stvari, koji uravnotežuje performanse i sigurnost korištenjem lagane enkripcije, [34].

Enkripcija podataka osigurava da se transakcije ne mogu opozvati i omogućuje isporuku integriranih, tajnih poruka pravim krajnjim korisnicima ili sustavima. Ovdje provjera

autentičnosti pomaže objema stranama u komunikacijskom procesu u međusobnom utvrđivanju istinskog identiteta i identificiranju njihovih namjeravanih primatelja. Kada se poruka isporučuje povjerljivo, njen sadržaj ostaje privatan. Integracija osigurava da je sadržaj poruke sačuvan u obliku u kojem ga je izvorni korisnik poslao, [34].

Gadgeti povezani s IoT-om imaju lošu reputaciju zbog slabe sigurnosti, djelomično zato što su često napravljeni jeftino i na brzinu, a djelomično zato što im nedostaje računalna snaga. Konvencionalno govoreći, nije lako šifrirati sve te podatke s ograničenim resursima. Najveća sigurnosna prijetnja IoT sustava je da čak i korištenje uređaja za prikupljanje podataka iz stvarnog fizičkog svijeta može postati meta kibernetičkih napada, [35].

4.2.1 Vrste IoT enkripcije

Šifre koriste varijable poznate kao što su ključevi ili kriptografski ključevi za zaključavanje i otključavanje funkcija šifriranja ili dešifriranja. Korisnici stvaraju tajni sigurnosni kod poznat kao lozinka za generiranje ključeva. Oni rade na dvije vrste enkripcije, [35]:

- Simetrično šifriranje tajnim ključem - Kao što naziv definira, koristi isti jedan ključ za funkcioniranje enkripcije i dešifriranja. U ovom slučaju, nužno je da se pošiljatelj i primatelj dogovore oko zajedničkog tajnog ključa prije uspostavljanja zaštićene komunikacije. Ovisno o zahtjevu za razmjenom podataka, simetrična enkripcija radi na stream (1 bajt ili 1 bit) i blok šiframa (podaci fiksne veličine - obično 64 bita). Brži je, zahtijeva malu potrošnju energije i uključuje jednostavan, jasan proces od kraja do kraja.
- Asimetrična enkripcija s javnim ključem Za razliku od simetrične enkripcije, ona koristi par ključeva - javni ključ za šifriranje i privatni ključ za dešifriranje, koji su međusobno povezani matematički i logički. Svaki pošiljatelj može šifrirati podatke pomoću javnog ključa. Međutim, dešifriranje je moguće samo od strane namjeravanog primatelja korištenjem privatnog ključa. Stoga asimetrična enkripcija uključuje autentifikaciju s pojačanom sigurnošću. Budući da IoT arhitektura radi na heterogenom distribuiranom sustavu, koristi simetrični tip za enkripciju i asimetrični tip za dešifriranje kako bi se nosila sa sigurnosnim izazovima.

4.2.2. Prednosti i nedostaci IoT enkripcije

Poduzeća koja ulažu u tradicionalna rješenja za IT sigurnost žele kvalitetniju zaštitu podataka. Od vanjskih hakera do internog osoblja, zaštita podataka za različite formate i svrhe ogroman je zadatak. Enkripcija se brine za sljedeće zadatke, [35]:

1. Podržava postavljene propise i usklađenosti prema Standardu sigurnosti podataka industrije platnih kartica (PCI DSS- *Payment Card Industry Data Security Standard*) i drugim tržišnim naprednim standardima šifriranja. To ima za cilj zaštititi osjetljive podatke vlasnika kartice tijekom online transakcija.
2. Štiti povjerljivost, autentifikaciju, cjelovitost i privatnost podataka bez obzira na lokaciju (oblak (engl. *Cloud*)/lokalna pohrana). Pomaže u promicanju povjerenja i povećava sigurnost u svakom trenutku.
3. Neovisan je o platformi i štiti podatke u mirovanju, u upotrebi i u pokretu, na raznim IoT uređajima, naposljetku osiguravajući mrežnu komunikaciju.

Usred rastućih sigurnosnih ranjivosti podataka IoT-a, enkripcija je neophodna. Međutim, dolazi s nekoliko nedostataka, [35]:

1. Glavni problem je upravljanje ključem za šifriranje na razini poduzeća. Njegovo održavanje ogroman je zadatak, a ako se ne dešifrira odgovarajućim privatnim ključem, nikome ne daje pristup. Može ograničiti pristup čak i vlasnicima podataka. Dogovor implicira da će se svi pridruženi podaci izgubiti ako osobe izgube ključeve za šifriranje.
2. Uključuje znatno visoke troškove održavanja i nadogradnje sustava i rezervnih poslužitelja koji obavljaju zadatke sigurnosti podataka. Osim toga, operacija oporavka u katastrofi velikih razmjera oduzima puno vremena.
3. Proces šifriranja sigurnosne kopije i obnove složen je i ponekad se suočava s problemima kompatibilnosti tijekom integracije s IoT aplikacijama. To zauzvrat negativno utječe na svakodnevne rutinske operacije.

Stoga je za šifriranje podataka potrebna konkretna strategija za odvojeno sigurnosno kopiranje ključeva. Ključ mora biti siguran od *cyber* napadača i uljeza, ali lako dostupan vlasnicima podataka.

5. Kibernetička sigurnost tehnologija umjetne inteligencije

Artificial intelligence, (dalje: AI) umjetna inteligencija je napravila valove u gotovo svakoj industriji, a kibernetička sigurnost nije iznimka. Nekoliko tvrtki usvaja tehnologiju u različitim poslovnim funkcijama, kao što su logistika i IT, [36]. Kako AI brzo prodire u poslovno okruženje, također je bio predmet kritika. Nedavno su izvješća otkrila da 75% globalnih tvrtki razmatra ili je već provelo zabranu korištenja ChatGPT-a i drugih AI aplikacija na radnom mjestu, [36]. Ova odluka je posljedica prepoznatih rizika koje predstavljaju za kibernetičku sigurnost i privatnost podataka.

5.1. Prednosti umjetne inteligencije u području kibernetičke sigurnosti

AI je postao moćan alat u borbi protiv *cyber* prijetnji jer može pomoći u bržem otkrivanju, analizi i odgovoru na zlonamjerne napade. Postoji nekoliko prednosti, [36]:

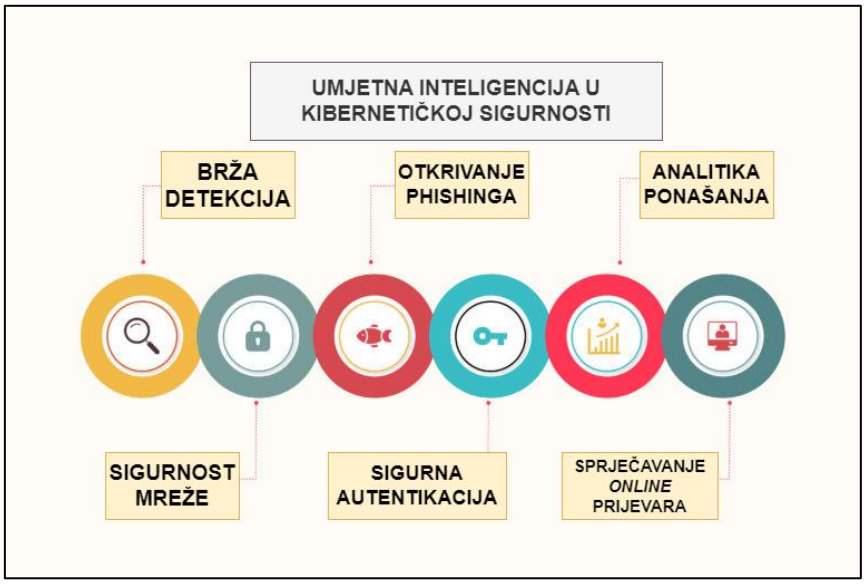
- Poboljšana točnost i učinkovitost - Sustavi kibernetičke sigurnosti temeljeni na umjetnoj inteligenciji pružaju poboljšanu točnost i učinkovitost u usporedbi s tradicionalnim sigurnosnim rješenjima. Na primjer, umjetna inteligencija može skenirati mnoštvo uređaja u potrazi za potencijalnim ranjivostima u djeliću vremena gdje bi ljudskim operaterima trebalo za isti zadatak veliki broj radnih sati rada. Nadalje, algoritmi umjetne inteligencije mogu prepoznati obrasce koje ljudsko oko može teško uočiti, što dovodi do točnijeg otkrivanja zlonamjernih aktivnosti.
- Veća skalabilnost i ušteda troškova - AI može automatizirati zamorne sigurnosne zadatke, oslobađajući vrijedne resurse za usredotočenje na druga poslovna područja. Također može brzo i precizno obraditi ogromne količine podataka kako bi identificirao prijetnje brže nego što bi to bilo koji čovjek mogao. To pomaže smanjiti vrijeme odgovora na sigurnosne incidente i pomaže u smanjenju troškova obrane od cyber prijetnji.

IBM je već implementirao takozvani IBM Security [37] koji pruža rješenja utemeljena na umjetnoj inteligenciji koja optimiziraju vrijeme analitičara ubrzavanjem otkrivanja prijetnji, ubrzavanjem odgovora i zaštitom korisničkog identiteta i skupova podataka a istovremeno drže

timove za kibernetičku sigurnost nadležnima. Takvi sustavi pružaju još nekoliko prednosti, [37]:

- Zaštita podataka u hibridnim okruženjima oblaka - AI rješenja mogu identificirati podatke u sjeni, nadzirati pristup podacima i upozoriti stručnjake za kibernetičku sigurnost o potencijalnim prijetnjama od bilo koga tko pristupa podacima ili osjetljivim informacijama. Također štedi dragocjeno vrijeme u otkrivanju i rješavanju problema u stvarnom vremenu.
- Usklađivanje potreba korisničkog pristupa i sigurnosti - AI modeli mogu pomoći u ravnoteži između sigurnosti i korisničkog iskustva analizom rizika svakog pokušaja prijave i provjerom korisnika putem podataka o ponašanju, pojednostavljujući pristup za provjerene korisnike i smanjujući troškove prijevare do 90%. Također, AI sustavi pomažu u sprječavanju krađe identiteta, zlonamjernog softvera i drugih zlonamjernih aktivnosti, osiguravajući visoko sigurnosno stanje.

Alati vođeni umjetnom inteligencijom također mogu pomoći u prepoznavanju zlonamjernih aktivnosti povezivanjem različitih podatkovnih točaka, omogućujući proaktivnu zaštitu sustava. Ova su rješenja lako skalabilna, što znači da mogu dobiti dodatnu zaštitu bez značajnih troškova hardvera ili osoblja, [36]. Slikom 10. prikazane su prednosti tehnologija umjetne inteligencije u kibernetičkoj sigurnosti.



Slika 10. Umjetna Inteligencija u kibernetičkoj sigurnosti, Preuzeo i modificirao Autor od Terranova Security, [36]

5.2. Nedostaci i prijetnje umjetne inteligencije u području kibernetičke sigurnosti

Sposobnost umjetne inteligencije da analizira velike skupove podataka velikom brzinom obećava neusporedivu zaštitu od *cyber* napada, a tvrtke širom svijeta ulažu velika sredstva u njegovu primjenu. Iako se sve više oslanja na umjetnu inteligenciju za jačanje sigurnosti, još uvijek postoje rizici u oslanjanju na ovu tehnologiju. Nedostaci su sljedeći, [36]:

- Pristranost i diskriminacija u donošenju odluka - Pristrano donošenje odluka u sustavima umjetne inteligencije može proizaći iz različitih izvora, uključujući skupove podataka koji sadrže pristrane informacije ili algoritme koji nemaju potrebnu objektivnost. Ako se ne upravlja ispravno, ove pristranosti mogu dovesti do diskriminirajućih odluka protiv određenih skupina ili pojedinaca i imati značajne posljedice za organizaciju. Na primjer, odluka koju je donio AI sustav na temelju pristranih inputa mogla bi dovesti do lažno pozitivnih rezultata i blokirati legitimne korisnike u pristupu sustavima tvrtke, što bi rezultiralo gubitkom produktivnosti ili kupaca.
- Nedostatak objašnjivosti i transparentnosti - Algoritmi koji se koriste za donošenje odluka o sigurnosnim prijetnjama nisu uvijek transparentni, ostavljajući korisnike ranjivima na mogućnost potencijalne pristranosti ili manipulaciju. AI može biti teško protumačiti pa je teško razumjeti zašto su donesene odluke ili kako i na koji način se mogu poboljšati. Ovaj nedostatak razumijevanja može dovesti do loših odluka, što može imati ozbiljne implikacije na sigurnost organizacije. Rješenja za kibernetičku sigurnost temeljena na umjetnoj inteligenciji možda neće uvijek točno identificirati svaku prijetnju ili potencijalno kršenje, što dovodi do toga da potencijalni rizici ostanu neprimijećeni i uzrokuju daljnju štetu.
- Mogućnost zlouporabe ili zlouporabe - Algoritmi umjetne inteligencije mogu se dizajnirati za brzo pretraživanje podataka i otkrivanje uzoraka, što ih čini metom za zlonamjerne aktere koji bi ih mogli upotrijebiti za pristup osjetljivim informacijama ili napad na infrastrukturu.

5.3. Primjeri kibernetičkih napada temeljenih na umjetnoj inteligenciji

Kao i svaka tehnologija, AI se može koristiti u dobre ili zlonamjerne svrhe. Akteri prijetnji mogu koristiti neke od istih alata umjetne inteligencije u svrhu organizacije kibernetičkog napada, [38]. Malwarebytes, anti-malware softver za Microsoft Windows, macOS, ChromeOS, Android i iOS navodi nekoliko primjera gdje AI može služiti kao alat pri organizaciji kibernetičkog napada, [38]:

1. Optimizacija cyber napada - Stručnjaci kažu da napadači mogu koristiti umjetnu inteligenciju i jezične modele za skaliranje napada na neviđenoj razini brzine i složenosti. Mogu koristiti generativnu umjetnu inteligenciju za pronalaženje novih načina za potkopavanje složenosti oblaka (engl. *Cloud*). Također mogu optimizirati svoje tehnike *ransomwarea* i *phishing* napada tako što će ih dotjerati generativnom umjetnom inteligencijom.
2. Automatizirani zlonamjerni softver – AI alat poput ChatGPT-a izvrstan je u preciznom izračunavanju brojeva. Prema profesoru Columbia Business School Odedu Netzeru, ChatGPT već može "prilično dobro pisati kod", [39]. Stručnjaci kažu da bi u bliskoj budućnosti mogao pomoći programerima softvera. Iako softver poput ChatGPT-a ima neke zaštite kako bi spriječio korisnike u stvaranju zlonamjernog koda, stručnjaci mogu koristiti pametne tehnike da ga zaobiđu i naprave zlonamjerni softver.
3. Fizička sigurnost - Kako sve više sustava kao što su autonomna vozila, proizvodna i građevinska oprema te medicinski sustavi koriste AI, rizici umjetne inteligencije za fizičku sigurnost mogu se povećati. Na primjer, istinski samovozeći automobil temeljen na umjetnoj inteligenciji koji pretrpi kršenje kibernetičke sigurnosti mogao bi dovesti do rizika za fizičku sigurnost svojih putnika. Slično tome, skup podataka za alate za održavanje na gradilištu napadač bi mogao manipulirati tako da stvori opasne uvjete.

6. Izvještaji razvijanja svijesti o kibernetičkoj sigurnosti kroz norme agencija Europske Unije

Prema izvještaju Agencije Europske unije za kibersigurnost (ENISA) objavljenog 2022. godine u mjesecu Studenom, [40] u 2020. i početkom 2021. uočen je globalni pad malware-a. Ovaj pad bio je povezan s COVID-19 pandemije i činjenice da su zaposlenici radili od kuće, čime se ograničava vidljivost infekcija zlonamjernim softverom jer se obično nalaze na korporativnim infrastrukturama. Do kraja 2021., kada se sve više ljudi počelo vraćati u urede zabilježen je veliki porast zlonamjernog softvera. Međutim, podaci pokazuju da povećanje nije linearno povezano s većim brojem ljudi u poslovnom okruženju, jednostavno zato što je bilo više zlonamjernog softvera.

6.1. NIS1

Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije [41] ili Direktiva o sigurnosti mreža i informacijskih sustava, europska je zakonodavna inicijativa usvojena kako bi se poboljšala sigurnost kritične infrastrukture i informacijskih sustava unutar Europske unije. NIS Direktiva, koja je stupila na snagu 2016. godine, ima za cilj osigurati visoku razinu sigurnosti mreža i informacijskih sustava u sektorima ključne važnosti, poput energetike, prometa, financija i zdravstva. Direktiva NIS 1 (Direktiva (EU) 2016/1148), akronim za sigurnost mrežnih i informacijskih sustava, usvojena je 2016. To je prva zakonodavna mjera na europskoj razini s ciljem poboljšanja suradnje između država članica i stvaranja prve razine harmonizacije u području kibernetičke sigurnosti, [42].

Glavni elementi NIS Direktive uključuju, [42]:

1. Zahtjeve za osiguravanje sigurnosti mreža i informacijskih sustava za operatore ključne važnosti i pružatelje digitalnih usluga.
2. Obvezu država članica da uspostave nacionalne strategije i sigurnosne agencije za praćenje i provedbu propisa.
3. Uspostavu sustava za izvješćivanje o ozbiljnim sigurnosnim incidentima i razmjenu informacija između država članica radi brze reakcije na cyber napade.
4. Promicanje suradnje između javnog i privatnog sektora radi poboljšanja sigurnosti mreža i informacijskih sustava.

NIS Direktiva predstavlja ključni korak prema jačanju cyber sigurnosti unutar EU-a i osiguravanju zaštite kritične infrastrukture od sve složenijih cyber prijetnji. Dostupna je na stranicama EUR-Lex[16]-a [41], internetskog portala za pravo Europske unije koji pruža službeni i potpun pristup njenim pravnim dokumentima. Dostupan je na sva 24 službena jezika EU-a i svakodnevno se ažurira. NIS Direktiva 1 identificira dvije kategorije subjekata na koje se odnose posebne odredbe, [42]:

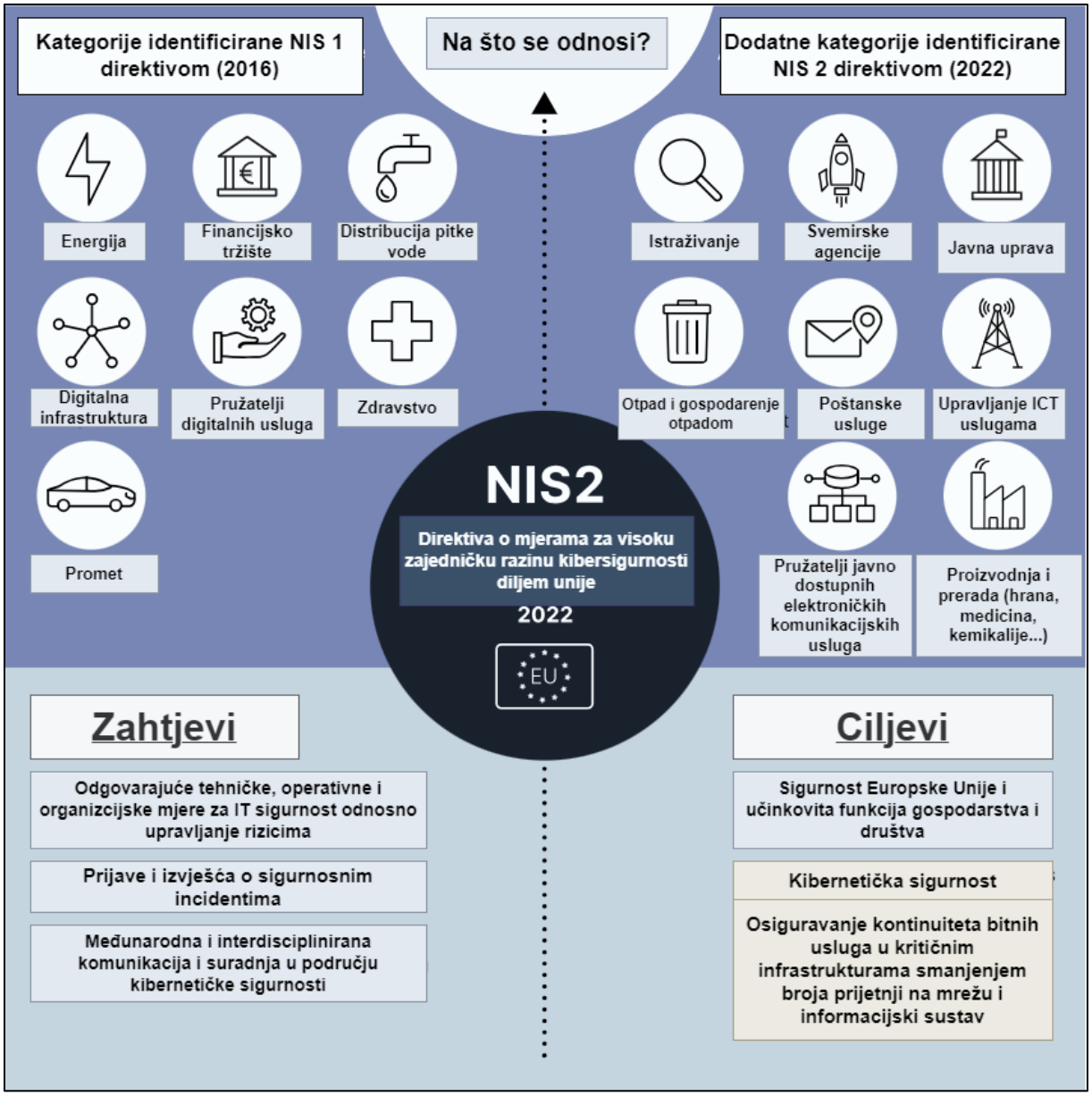
- Operatere osnovnih usluga odnosno OES (engl. *Operators of essential services*): javni ili privatni subjekti s važnom ulogom za društvo i gospodarstvo te koji pružaju osnovne usluge (obično se identificiraju kao kritična infrastruktura). Države članice izravno identificiraju OES-ove u kritičnim sektorima (energija, promet, bankarstvo, financijska tržišta, zdravstvo, opskrba i distribucija pitke vode te digitalna infrastruktura) na temelju toga koliko je usluga bitna te rizik povezan s incidentom koji utječe na uslugu.
- Pružatelji digitalnih usluga (DSP engl. Digital Service Providers): tvrtke koje pružaju usluge e-trgovine, računalstva u oblaku.

6.2. NIS 2

U siječnju 2023. godine stupila je na snagu Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibernetičke sigurnosti u Uniji, kojom se mijenjaju Uredba (EU) br. 910/2014 i Direktiva (EU) 2018/1972, i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2), [44]. Direktiva o mjerama za visoku zajedničku razinu kibernetičke sigurnosti diljem Europske unije, poznata kao Direktiva NIS2, važna je za organizacije diljem svijeta, ne samo unutar Europskog ekonomskog područja (EEA[17]). Direktiva NIS2 ima za cilj postizanje visoke zajedničke razine kibernetičke sigurnosti diljem Unije proširujući polje primjene u odnosu na prethodnu NIS direktivu. To znači da mnoga trgovačka društva i organizacije koje nisu bila obuhvaćena prijašnjim zakonom sada moraju ozbiljno razmišljati o unapređenju vlastite kibernetičke sigurnosti. Jedna od ključnih mjera kibernetičke sigurnosti, koju moraju implementirati svi subjekti pod Direktivom NIS2, je upravljanje rizicima. Upravljanje rizicima postaje od presudne važnosti, s obzirom na širok spektar prijetnji koje mogu utjecati na poslovanje, [45].

[16] EUR-Lex – pristup zakonodavstu Europske unije.
[17] EEA (engl. European Economic Area) – Europski gospodarski prostor.

U Hrvatskoj, Zakon o kibernetičkoj sigurnosti, koji implementira odredbe Direktive NIS2, stupio je na snagu 1. veljače 2024. godine, [46]. Nakon završetka procedure i objave u Narodnim novinama, zakon je stupio na snagu, pokrećući rok od godine dana za kategorizaciju subjekata. Direktiva NIS2, ključno zakonodavstvo o kibersigurnosti na razini Europske unije, predstavlja važan korak prema osiguranju pravnih mjera za povećanje opće razine kibersigurnosti u EU-u. Inicijalna pravila o kibersigurnosti EU-a, uspostavljena 2016., ažurirana su s ulaskom Direktive NIS2 na snagu 2023. godine, kako bi se prilagodila povećanoj digitalizaciji i dinamičnom okruženju prijetnji kibersigurnosti. Slika 9. prikazuje ažurirana pravila NIS2 u odnosu na prethodnu NIS1.



Slika 11. Usporedba NIS1 i NIS2 direktive
Preuzeo i modificirao autor od LANCOM systems [47]

Pravila EU-a o kibersigurnosti uvedena 2016. ažurirana su Direktivom NIS2 koja je stupila na snagu 2023. Modernizirala je postojeći pravni okvir kako bi se održao korak s povećanom digitalizacijom i promjenjivim okruženjem prijetnji kibersigurnosti. Proširenjem područja primjene pravila o kibersigurnosti na nove sektore i subjekte dodatno se poboljšava otpornost i kapaciteti za odgovor na incidente javnih i privatnih subjekata, nadležnih tijela i EU-a u cjelini.

Direktivom o mjerama za visoku zajedničku razinu kibersigurnosti diljem Unije (Direktiva NIS2) predviđene su pravne mjere za povećanje ukupne razine kibersigurnosti u EU-u osiguravanjem:

- Pripravnost država članica zahtijevajući od njih da budu odgovarajuće opremljene. Na primjer, s timom za odgovor na računalne sigurnosne incidente (CSIRT[18]) i nadležnim nacionalnim tijelom za mrežne i informacijske sustave (NIS),
- suradnja među svim državama članicama osnivanjem skupine za suradnju [19]radi potpore i olakšavanja strateške suradnje i razmjene informacija među državama članicama.
- kultura sigurnosti u svim sektorima koji su ključni za naše gospodarstvo i društvo i koji se u velikoj mjeri oslanjaju na informacijske i komunikacijske tehnologije, kao što su energetika, promet, voda, bankarstvo, infrastruktura financijskog tržišta, zdravstvena skrb i digitalna infrastruktura.

Poduzeća koja su države članice utvrdile kao operatore ključnih usluga u navedenim sektorima morat će poduzeti odgovarajuće sigurnosne mjere i obavijestiti relevantna nacionalna tijela o ozbiljnim incidentima. Pružatelji ključnih digitalnih usluga, kao što su tražilice, usluge računalstva u oblaku i internetska tržišta, morat će ispunjavati zahtjeve u pogledu sigurnosti i obavješćivanja iz Direktive, [48].

Direktiva stoga ima za cilj ojačati otpornost ovih kritičnih infrastruktura [20]u skladu s Europskim programom za zaštitu kritične infrastrukture (EPCIP[21] engl. European Programme

[18] CSIRT- je kratica za Computer Security Incident Response Team, odnosno nadležno tijelo za prevenciju i zaštitu od kibernetičkih incidenata, za koju se koristi i kratica CERT (Computer Emergency Response Team).
[19] Skupina za suradnju- engl. NIS Cooperation Group, skupina kojoj je cilj postići visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava u Europskoj uniji.
[20] Kritična infrastruktura- predstavlja infrastrukturu koja je vitalna za neku zemlju ili zajednicu i čije oštećenje ili gubitak vodi do gubitka isporuke neke usluge.
[21] EPCIP (engl. European Programme for Critical Infrastructure Protection) - Europski program za zaštitu kritične infrastrukture.

for Critical Infrastructure Protection) s različitim zahtjevima koji se odnose na stanje IT sigurnosti, obveze izvješćivanja, regulatorne revizije i još mnogo toga, [47].

7. Zaključak

Zaključno, rezultati provedene Ankete jasno ukazuju na potrebu za podizanjem razine svijesti o kibernetičkoj sigurnosti među ispitanicima. Analiza prikupljenih podataka otkriva da postoji značajan nedostatak informiranosti o osnovnim principima kibernetičke sigurnosti te svijesti o potencijalnim prijetnjama i ranjivostima. Poboljšanje svijesti o kibernetičkoj sigurnosti ne bi trebalo biti samo cilj organizacija, već pojedinaca te bi trebalo biti integralni dio društvenog i poslovnog djelovanja. Kroz suradnju između vlade, industrije, akademske zajednice i civilnog društva, mogu se razviti inicijative i politike koje promiču kulturu sigurnosti i potiču kontinuiranu edukaciju o kibernetičkoj sigurnosti. Provedena Anketa je primjer kako pristupiti razvijanju svijesti o kibernetičkoj sigurnosti izvan organizacija te se posvetiti pojedincu. Naravno, izvješća i istraživanja spomenuta u radu imaju itetako važan utisak u razvijanju svijesti. Izvješća Europske unije su recentna, a direktive Europske unije su temelj pravne regulative. Ostaje za zadatak na što jednostavniji način približiti i dati instrukcije građanima RH za sigurno korištenje digitalnih usluga.

Nadalje, treba težiti što većem poznavanju pojma kibernetičke sigurnosti. Kao što je već spomenuto, 11,9% ispitanika nije upoznato s istim. To može značiti da isti postotak već u početku neće prepoznati kibernetičku prijetnju te će daljnjim postupcima narušiti sigurnost svojih podataka. Što se tiče *online* aktivnosti, ispitanici Internet bankarstvo smatraju kao najsigurniji oblik i to 62,7% dok je Internet kupovina na 32,2%. Vrijedi naglasiti kako 16,9% ispitanika smatra kako nijedna *online* aktivnost nije u potpunosti sigurna. Iz navedenog je moguće zaključiti kako ostaje puno prostora za napredak te da bi postoci koji ukazuju na sigurnost korištenja usluga trebali biti puno veći.

U konačnici, podizanje razine svijesti o kibernetičkoj sigurnosti ključno je za stvaranje sigurnijeg i otpornijeg digitalnog okruženja, koje će omogućiti pojedincima i organizacijama da se uspješno nose s izazovima suvremenog digitalnog doba.

Literatura

[1] LinkedIn, The Importance of Cybersecurity Awareness for Businesses, https://www.linkedin.com/pulse/importance-cybersecurity-awareness-businesses-rainbowsecure/ [Pristupljeno: veljača 2024.]

[2] Raiffeisen Bank, Novi phishing napadi dolaze i u obliku SMS poruka, https://www.rba.hr/-/novi-phishing-napadi-dolaze-i-u-obliku-sms-poruka [Pristupljeno: veljača 2024.]

[3] ICT Business, SOA upozorava na povećan broj kibernetičkih napada, https://www.ictbusiness.info/vijesti/soa-upozorava-na-povecan-broj-kibernetickih-napada-i-to-poglavito-drzavno-sponzoriranih [Pristupljeno: veljača 2024.]

[4] kaspersky, How to Avoid Public WiFi Security Risks, https://www.kaspersky.com/resource-center/preemptive-safety/public-wifi-risks [Pristupljeno: veljača 2024.]

[5] LinkedIn, Password-Based Authentication vs. Passwordless Authentication: A Comprehensive Comparison, https://www.linkedin.com/pulse/password-based-authentication-vs-passwordless-comprehensive/ [Pristupljeno: veljača 2024.]

[6] ENISA, Tips for secure user authentication, https://www.enisa.europa.eu/news/enisa-news/tips-for-secure-user-authentication [Pristupljeno: veljača 2024.]

[7] kaspersky, Why You Need Backup Files, https://www.kaspersky.com/resource-center/preemptive-safety/backup-files [Pristupljeno: veljača 2024.]

[8] kaspersy, IoT users' cybersecurity outlook: every second user feels responsible for protecting their gadgets, with millennials caring most about security, https://www.kaspersky.com/about/press-releases/2023_iot-users-cybersecurity-outlook-every-second-user-feels-responsible-for-protecting-their-gadgets-with-millennials-caring-most-about-security [Pristupljeno: veljača 2024.]

[9] Središnji državni ured za razvoj digitalnog društva, Kibernetička sigurnost, https://rdd.gov.hr/kiberneticka-sigurnost-1436/1436 [Pristupljeno: veljača 2024.]

[10] ENISA, ENISA Threat Landscape 2023, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 [Pristupljeno: veljača 2024.]

[11] ENISA, Threats and Trends, https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends/?tab=details [Pristupljeno: veljača 2024.]

[12] ENISA, Cybersecurity Threats Fast-Forward 2030, https://www.enisa.europa.eu/news/cybersecurity-threats-fast-forward-2030 [Pristupljeno: veljača 2024.]

[13] ICT Business, Kibernetički napadi na lance opskrbe softverom nastavljaju rast, https://www.ictbusiness.info/poslovna-rjesenja/kiberneticki-napadi-na-lance-opskrbe-softverom-nastavljaju-rast [Pristupljeno: veljača 2024.]

[14] ScienceDirect, Impact of data trade restrictions on IT services export: A cross-country analysis, https://www.sciencedirect.com/science/article/abs/pii/S0308596122001057 [Pristupljeno: veljača 2024.]

[15] Narodne novine, Zakon o kibernetičkoj sigurnosti, https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html [Pristupljeno: veljača 2024.]

[16] CARNET – Hrvatska akademska i istraživačka mreža, Phishing napadi CCERT-PUBDOC

[17] Agencija za zaštitu osobnih podataka, Phishing napadi, https://azop.hr/phishing-napadi-kako-ih-prepoznati-i-zastititi-se/ [Pristupljeno: veljača 2024.]

[18] Microsoft Security, Definicija zlonamjernog softvera, https://www.microsoft.com/hr-hr/security/business/security-101/what-is-malware [Pristupljeno: veljača 2024.]

[19] Microsoft Security, Različite vrste napada krađe identiteta, https://www.microsoft.com/hr-hr/security/business/security-101/what-is-phishing [Pristupljeno: veljača 2024.]

[20] Microsoft Security, Definicija ucjenjivačkog softvera, https://www.microsoft.com/hr-hr/security/business/security-101/what-is-ransomware [Pristupljeno: veljača 2024.]

[21] Microsoft Security, Definicija DDoS napada, https://www.microsoft.com/hr-hr/security/business/security-101/what-is-a-ddos-attack [Pristupljeno: veljača 2024.]

[22] CERT.hr, Ransomware, https://www.cert.hr/19795-2/ransomware/] [Pristupljeno: veljača 2024.]

[23] Microsoft Security, Human Operated ransomware, https://learn.microsoft.com/en-us/security/ransomware/human-operated-ransomware [Pristupljeno: veljača 2024.]

[24] Business Standard, China-based hackers breached European govt email accounts: Microsoft, https://www.business-standard.com/world-news/china-based-hackers-breached-european-govt-email-accounts-microsoft-123071200539_1.html [Pristupljeno: veljača 2024.]

[25] ENISA, Man-in-the-Middle, https://www.enisa.europa.eu/topics/incident-response/glossary/man-in-the-middle [Pristupljeno: veljača 2024.]

[26] Khan Academy, Rogue access points, https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-

data-security/xcae6f4a7ff015e7d:cyber-attacks/a/rogue-access-points-mitm-attacks
[Pristupljeno: veljača 2024.]
[27] E. Dulaney and C. Easttom, CompTIA Security+ Study guide Seventh Edition, EXAM SY0-501
[28] CARNET- Hrvatska akademska i istraživačka mreža, Zero day ranjivosti - NCERT-PUBDOC-2010-01-289
[29] W3Schools, SQL Introduction, https://www.w3schools.com/sql/sql_intro.asp [Pristupljeno: veljača 2024.]
[30] EU Disinfo, FIMI: towards a European redefinition of foreign interference, https://www.disinfo.eu/publications/fimi-towards-a-european-redefinition-of-foreign-interference/ [Pristupljeno: veljača 2024.]
[31] CERT.hr, sigurnost „interneta stvari“ (IoT), https://www.cert.hr/sigurnost-interneta-stvari-iot/ [Pristupljeno: veljača 2024.]
[32] CompTIA, IoT Cybersecurity, https://www.comptia.org/content/articles/what-is-iot-cybersecurity [Pristupljeno: veljača 2024.]
[33] ENISA, Guidelines for Securing the Internet of Things, https://www.enisa.europa.eu/publications/guidelines-for-securing-the-internet-of-things [Pristupljeno: veljača 2024.]
[34] Science Direct, Cryptography Algorithms for Enhancing IoT Security, https://www.sciencedirect.com/science/article/abs/pii/S2542660523000823 [Pristupljeno: veljača 2024.]
[35] intuz, Securing The IoT Data Landscape: IoT Encryption Algorithms, https://www.intuz.com/blog/securing-the-iot-data-landscape-iot-encryption-algorithms [Pristupljeno: veljača 2024.]
[36] Terranova Security, AI in Cyber Security: Pros and Cons, https://terranovasecurity.com/blog/ai-in-cyber-security/ [Pristupljeno: veljača 2024.]
[37] IBM, Artificial intelligence (AI) cybersecurity, https://www.ibm.com/ai-cybersecurity [Pristupljeno: veljača 2024.]
[38] Malwarebytes, AI IN CYBER SECURITY, https://www.malwarebytes.com/cybersecurity/basics/risks-of-ai-in-cyber-security [Pristupljeno: veljača 2024.]
[39] CBS News, These jobs are most likely to be replaced by chatbots like ChatGPT, https://www.cbsnews.com/news/chatgpt-artificial-intelligence-chatbot-jobs-most-likely-to-be-replaced/ [Pristupljeno: veljača 2024.]

[40] ENISA, ENISA Threat Landscape 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022 [Pristupljeno: veljača 2024.]
[41] EUR-Lex, Direktiva (EU) 2016/1148 Europskog parlamenta i Vijeća od 6. srpnja 2016. o mjerama za visoku zajedničku razinu sigurnosti mrežnih i informacijskih sustava širom Unije, https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX%3A32016L1148 [Pristupljeno: veljača 2024.]
[42] DLA Piper, The NIS 1 Directive and the new NIS 2 Directive, https://www.dlapiper.com/en/insights/publications/law-in-tech/cyberitalia-the-nis-1-directive-and-the-new-nis-2-directive-in-a-nutshell [Pristupljeno: veljača 2024.]
[43] EUR-Lex, https://eur-lex.europa.eu/homepage.html?locale=hr, [Pristupljeno: veljača 2024.]
[44] EUR-Lex, Direktiva (EU) 2022/2555 Europskog parlamenta i Vijeća od 14. prosinca 2022. o mjerama za visoku zajedničku razinu kibersigurnosti širom Unije, izmjeni Uredbe (EU) br. 910/2014 i Direktive (EU) 2018/1972 i stavljanju izvan snage Direktive (EU) 2016/1148 (Direktiva NIS 2), https://eur-lex.europa.eu/eli/dir/2022/2555 [Pristupljeno: veljača 2024.]
[45] ICT Business, Potrebno je prilagoditi se NIS2, https://www.ictbusiness.info/poslovanje/potrebno-je-prilagoditi-se-nis2 [Pristupljeno: veljača 2024.]
[46] Narodne novine, Zakon o kibernetičkoj sigurnosti, https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html [Pristupljeno: veljača 2024.]
[47] LANCOM Systems, Network security according to NIS2, https://www.lancom-systems.com/solutions/network-security/network-security-according-to-nis2-directive
[Pristupljeno: veljača 2024.]
[48] Europska komisija, Direktiva o mjerama za visoku zajedničku razinu kibersigurnosti diljem Unije (Direktiva NIS2), https://digital-strategy.ec.europa.eu/hr/policies/nis2-directive
[Pristupljeno: veljača 2024.]
[49] Europska komisija, NIS Cooperation Group, https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group [Pristupljeno: veljača 2024.]
[50] Ministarstvo unutarnjih poslova – Ravnateljstvo civilne zaštite, Kritična infrastruktura, https://civilna-zastita.gov.hr/kriticna-infrastruktura/111 [Pristupljeno: veljača 2024.]

Popis slika

Popis grafikona

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 Razvijanje svijesti o kibernetičkoj sigurnosti među građanima RH, u Nacionalni repozitorij završnih i diplomskih radova ZIR.

Student/ica:

U Zagrebu, 12.03.2024.

Andrej Zadiš
(ime i prezime, *potpis*)