03

UPORABNA INFORMATIKA

2025 ‹ ŠTEVILKA 3 ‹ LETNIK XXXIII ‹ ISSN 1318-1882

U P O R A B N A
I N F O R M A T I K A
2025 ŠTEVILKA 3 JUL/AVG/SEP LETNIK XXXIII ISSN 1318-1882

Znanstveni prispevki

Kratki znanstveni prispevki

Informacije

2025 ŠTEVILKA 3 JUL/AVG/SEP LETNIK XXXIII ISSN 1318-1882

Ustanovitelj in izdajatelj
Slovensko društvo INFORMATIKA
Litostrojska cesta 54, 1000 Ljubljana

Predstavnik
Slavko Žitnik

Odgovorni urednik
Mirjana Kljajić Borštnar

Prelom in tisk
Boex DTP, d. o. o., Ljubljana

Naklada
110 izvodov

Naslov uredništva
Slovensko društvo INFORMATIKA
Uredništvo revije Uporabna informatika
Litostrojska cesta 54, 1000 Ljubljana
www.uporabna-informatika.si

Revija izhaja četrtletno. Cena posamezne številke je 20,00 EUR. Letna naročnina za podjetja 85,00 EUR, za vsak nadaljnji izvod 60,00 EUR, za posameznike 35,00 EUR, za študente in seniorje 15,00 EUR. V ceno je vključen DDV.

Revija Uporabna informatika je od številke 4/VII vključena v mednarodno bazo INSPEC.

Revija Uporabna informatika je pod zaporedno številko 666 vpisana v razvid medijev, ki ga vodi Ministrstvo za kulturo RS.

Revija Uporabna informatika je vključena v Digitalno knjižnico Slovenije (dLib.si).

Izid publikacije je finančno podprla Javna agencija za znanstvenoraziskovalno in inovacijsko dejavnost Republike Slovenije.

Vabilo avtorjem

V reviji Uporabna informatika objavljamo kakovostne izvirne prispevke domačih in tujih avtorjev z najširšega področja informatike, ki se nanašajo tako na poslovanje podjetij, javno upravo, družbo in posameznika. Prispevki so lahko znanstvene, strokovne ali informativne narave, še posebno spodbujamo objavo interdisciplinarnih prispevkov. Zato vabimo avtorje, da prispevke, ki ustrezajo omenjenim usmeritvam, pošljejo uredništvu revije po elektronski pošti na naslov ui@drustvo-informatika.si.

Avtorje prosimo, da pri pripravi prispevka upoštevajo navodila, ki so objavljena na naslovu http://www.uporabna-informatika.si.

Za kakovost prispevkov skrbi mednarodni uredniški odbor. Prispevki so anonimno recenzirani, o objavi pa na podlagi recenzij samostojno odloča uredniški odbor. Recenzenti lahko zahtevajo, da avtorji besedilo spremenijo v skladu s priporočili in da popravljeni prispevek ponovno prejmejo v pregled. Sprejeti prispevki so pred izidom revije objavljeni na spletni strani revije (predobjava), še prej pa končno verzijo prispevka avtorji dobijo v pregled in potrditev. Uredništvo lahko še pred recenzijo zavrne objavo prispevka, če njegova vsebina ne ustreza vsebinski usmeritvi revije ali če prispevek ne ustreza kriterijem za objavo v reviji.

Pred objavo prispevka mora avtor podpisati izjavo o avtorstvu, s katero potrjuje originalnost prispevka in dovoljuje prenos materialnih avtorskih pravic. Avtorji prejmejo enoletno naročnino na revijo Uporabna informatika, ki vključuje avtorski izvod revije in še nadaljnje tri zaporedne številke. S svojim prispevkom v reviji Uporabna informatika boste pomagali k širjenju znanja na področju informatike. Želimo si čim več prispevkov z raznoliko in zanimivo tematiko in se jih že vnaprej veselimo

Uredništvo revije

Navodila avtorjem člankov

Članke objavljamo praviloma v slovenščini, članke tujih avtorjev pa v angleščini. Besedilo naj bo jezikovno skrbno pripravljeno. Priporočamo zmernost pri uporabi tujk in, kjer je mogoče, njihovo zamenjavo s slovenskimi izrazi. V pomoč pri iskanju slovenskih ustreznic priporočamo uporabo spletnega terminološkega slovarja Slovenskega društva Informatika, Islovar (www.islovar.org).

Znanstveni prispevek naj obsega največ 40.000 znakov, kratki znanstveni prispevek do 10.000 znakov, strokovni članki do 30.000 znakov, obvestila in poročila pa do 8.000 znakov.

Prispevek naj bo predložen v urejevalniku besedil Word (*.doc ali *.docx) v enojnem razmaku, brez posebnih znakov ali poudarjenih črk. Za ločilom na koncu stavka napravite samo en presledek, pri odstavkih ne uporabljajte zamika.

Naslovu prispevka naj sledi polno ime vsakega avtorja, ustanova, v kateri je zaposlen, naslov in elektronski naslov. Sledi naj povzetek v slovenščini v obsegu 8 do 10 vrstic in seznam od 5 do 8 ključnih besed, ki najbolje opredeljujejo vsebinski okvir prispevka. Sledi naj prevod naslova povzetka in ključnih besed v angleškem jeziku. V primeru, da oddajate prispevek v angleškem jeziku, velja obratno. Razdelki naj bodo naslovljeni in oštevilčeni z arabskimi številkami.

Slike in tabele vključite v besedilo. Opremite jih z naslovom in oštevilčite z arabskimi številkami. Na vsako sliko in tabelo se morate v besedilu prispevka sklicevati in jo pojasniti. Če v prispevku uporabljate slike ali tabele drugih avtorjev, navedite vir pod sliko oz. tabelo. Revijo tiskamo v črno-beli tehniki, zato barvne slike ali fotografije kot original niso primerne. Slikam zaslonov se v prispevku izogibajte, razen če so nujno potrebne za razumevanje besedila. Slike, grafikoni, organizacijske sheme ipd. naj imajo belo podlago. Enačbe oštevilčite v oklepajih desno od enačbe.

V besedilu se sklicujte na navedeno literaturo skladno s pravili sistema IEEE navajanja bibliografskih referenc, v besedilu to pomeni zaporedna številka navajenega vira v oglatem oklepaju (npr. [1]). Na koncu prispevka navedite samo v prispevku uporabljeno literaturo in vire v enotnem seznamu, urejeno po zaporedni številki vira, prav tako v skladu s pravili IEEE. Več o sistemu IEEE, katerega uporabo omogoča tudi urejevalnik besedil Word 2007, najdete na strani https://owl.purdue.edu/owl/research_and_citation/ieee_style/ieee_general_format.html.

Prispevku dodajte kratek življenjepis vsakega avtorja v obsegu do 8 vrstic, v katerem poudarite predvsem strokovne dosežke.

Visoko-interaktivna Redis limanica z ELK analitiko

Marin Gazvoda de Reggi, Sara Mihalič, Samo Hribar, Ana Bračić, Matevž Pesek
Univerza v Ljubljani, Fakulteta za računalništvo in informatiko, Večna pot 113, 1000 Ljubljana
{mg4234, sm0770, sh8397, ab1165}@student.uni-lj.si, matevz.pesek@fri.uni-lj.si

Izvleček

Redis je zaradi svoje široke uporabe in pogosto nepravilne konfiguracije postal priljubljena tarča kibernetskih napadov, kar ustvarja potrebo po boljšem razumevanju in analizi varnostnih groženj. V tem delu predstavljamo implementacijo visoko-interaktivne Redis limanice (angl. honeypot), ki omogoča transparentno prestrezanje in beleženje vseh povezav ter ukazov na Redis strežnik. Sistem temelji na posredniškem strežniku v programskem jeziku Go, ki prestrežene povezave posreduje interni Redis instanci, pri tem pa vse interakcije v realnem času beleži in analizira preko integracije z naborom orodij ELK (Elasticsearch, Logstash, Kibana). Celotna rešitev je implementirana kot vsebniška aplikacija z uporabo tehnologije Docker. Eksperimentalna evalvacija je pokazala, da sistem učinkovito zaznava različne vrste napadov, od preprostih poskusov skeniranja do sofisticiranih večstopenjskih napadov. Razviti sistem predstavlja pomemben prispevek k boljšemu razumevanju varnostnih izzivov Redis strežnikov in demonstrira uporabnost limanic pri raziskovanju kibernetskih groženj.

Ključne besede: ELK analitika, kibernetska varnost, limanica, Redis, varnostne grožnje

High-interactive Redis honeypot with ELK analytics

Abstract

Redis has become a popular target for cyberattacks due to its widespread use and frequent misconfigurations, creating the need for better understanding and analysis of security threats. This work presents the implementation of a high-interactive Redis honeypot that enables the transparent interception and logging of all connections and commands to a Redis server. The system is based on a proxy server implemented in the Go programming language, which forwards intercepted connections to an internal Redis instance while logging and analysing all interactions in real-time through integration with the ELK stack (Elasticsearch, Logstash, Kibana). The entire solution is implemented as a containerized application using Docker technology. Experimental evaluation demonstrated that the system effectively detects various types of attacks, from simple scanning attempts to sophisticated multi-stage attacks. The developed system represents an important contribution to better understanding Redis server security challenges and demonstrates the utility of honeypots in cybersecurity threat research.

Keywords: Cybersecurity, ELK analytics, honeypot, Redis, security threats

1 UVOD

V sodobnem digitalnem okolju predstavljajo podatkovne baze eno ključnih komponent informacijske infrastrukture, saj podpirajo delovanje praktično vseh spletnih storitev, od družbenih omrežij do finančnih sistemov. Med njimi je pomnilniška podatkovna shramba Redis (Remote Dictionary Server), ki je postala ena najpogosteje uporabljenih rešitev za predpomnjenje in upravljanje s podatki v realnem času [1]. Redis je še posebej priljubljen v visoko-zmogljivih aplikacijah, pri katerih je ključen hiter dostop do podatkov, saj lahko izvede več kot 100.000 operacij na sekundo.

Žal njegova široka uporaba prinaša tudi večje varnostno tveganje. Wright [2] je v svoji raziskavi

odkril več kot 18.000 izpostavljenih Redis instanc na internetu, od katerih je bilo kar 72 % že tarča napada. Ta podatek jasno kaže na obseg problematike in potrebo po boljšem razumevanju varnostnih groženj. Kljub jasnim priporočilom razvijalcev, da Redis ni namenjen neposredni izpostavitvi na internet [3], se v praksi pogosto dogaja, da so instance nepravilno konfigurirane in nezaščitene. Posledice takšnih napak so lahko resne – od kraje podatkov do popolnega prevzema nadzora nad sistemom, kar lahko vodi v velike finančne izgube in okrnjen ugled podjetij.

Za učinkovito zaščito je zato ključno razumevanje načinov, kako napadalci odkrivajo in izkoriščajo ranljive Redis strežnike. Pri tem so limanice (angl. *honeypots*) oz. namensko vzpostavljeni navidezno ranljivi sistemi – postale ključno orodje v sodobni varnostni analitiki. Delujejo kot vabe, ki privabljajo napadalce in beležijo njihove aktivnosti ter tako nudijo vpogled v njihove tehnike, orodja in motivacije. Z natančnim spremljanjem in analizo teh interakcij lahko varnostni strokovnjaki identificirajo nove vrste napadov in razvijajo učinkovitejše obrambne mehanizme za zaščito kritične internetne infrastrukture.

Prav na opisanem principu delovanja limanic temelji naš pristop, s katerim smo se lotili proaktivnega odkrivanja in analize napadov na strežnike Redis. V ta namen smo razvili visoko-interaktivno limanico, integrirano z analitično platformo ELK (Elasticsearch, Logstash, Kibana). Implementirana rešitev omogoča natančno spremljanje poskusov vdorov, beleženje uporabljenih tehnik in analizo vzorcev napadov v realnem času. S tem prispevamo k boljšemu razumevanju varnostnih groženj in razvoju učinkovitejših zaščitnih mehanizmov za kritično internetno infrastrukturo.

2 TEORETIČNI KONCEPTI IN TEHNOLOGIJA

2.1 Redis podatkovna baza

Redis (Remote Dictionary Server) je odprtokodna, v pomnilniku delujoča podatkovna shramba, ki se uporablja kot podatkovna baza, predpomnilnik in posrednik sporočil [1]. Redisova ključna prednost je izjemna hitrost delovanja, saj podatke hrani v glavnem pomnilniku (RAM), kar omogoča zelo nizke latence pri dostopu do podatkov. Podpira različne podatkovne strukture, kot so nizi, seznami, množice, razpršene tabele in urejene množice, zaradi česar je primeren za širok nabor uporabniških scenarijev [4].

Redisova arhitektura temelji na modelu strežnik–odjemalec, kjer strežnik upravlja s podatkovnimi strukturami v pomnilniku, odjemalci pa komunicirajo s strežnikom preko preprostega tekstovnega protokola RESP (REdis Serialization Protocol) [5]. Taka zasnova, čeprav učinkovita z vidika hitrosti, predstavlja določena varnostna tveganja, še posebej v primeru nepravilne konfiguracije ali izpostavljenosti na javno omrežje.

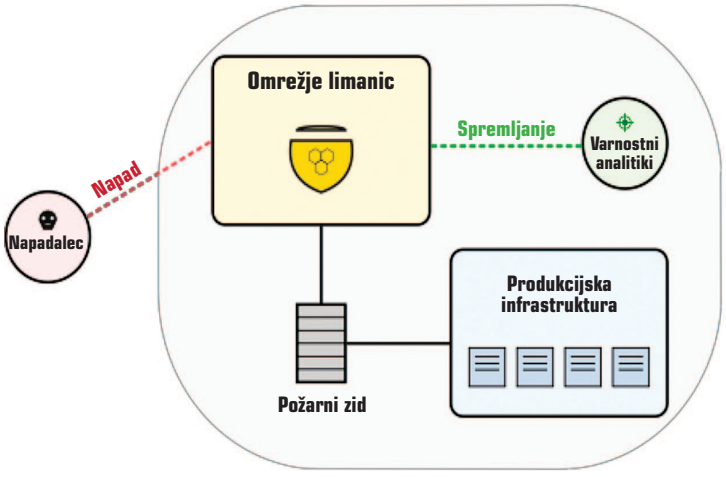
2.2 Limanice

Limanice (angl. *honeypots*) so varnostna orodja, zasnovana za simulacijo ranljivih sistemov z namenom privabljanja, odkrivanja in analize zlonamernih aktivnosti [6]. Po namenu uporabe jih delimo na raziskovalne in produkcijske limanice. Raziskovalne limanice so namenjene pridobivanju znanja o napadalčevih tehnikah, orodjih in motivacijah, medtem ko produkcijske limanice služijo zaščiti dejanske infrastrukture z odkrivanjem in upočasnitvijo napadov. Te delujejo kot vabe, ki preusmerijo napadalčevo pozornost s kritičnih sistemov na nadzorovan in izolirani sistem, kjer se njihova aktivnost beleži brez nevarnosti za ključno infrastrukturo.

Glede na stopnjo interakcije, ki jo dopuščajo napadalcem, jih delimo v tri kategorije:

- **Nizko-interaktivne limanice** simulirajo samo osnovne funkcionalnosti in so primerne predvsem za zbiranje statističnih podatkov o poskusih napadov.
- **Srednje-interaktivne limanice** ponujajo večji nabor funkcionalnosti in nudijo bolj poglobljeno analizo napadov, vendar še vedno v kontroliranem okolju.
- **Visoko-interaktivne limanice** predstavljajo popolnoma funkcionalne sisteme, ki zagotavljajo največjo stopnjo interakcije in s tem najnatančnejšo analizo napadalčevega vedenja [7].

Učinkovitost limanice je odvisna od njene prepričljivosti simulacije ciljnega sistema, pri čemer mora biti dovolj privlačna za napadalce, a hkrati varna za upravljanje in analizo [8]. Pri implementaciji je ključnega pomena ravnotežje med stopnjo realističnosti oz. pristnosti simulacije in varnostjo sistema.



Slika 1: **Napadalec skuša napasti produkcijsko aplikacijo, ki je zaščitena za požarnim zidom. Da preusmerimo napadalčevo pozornost in pridobimo informacije o napadalčevih tehnikah, namestimo limanico kot navidezno ranljivo tarčo. Limanica tako služi dvojnemu namenu: odvrne pozornost od kritične infrastrukture in hkrati omogoča varnostnim analitikom beleženje ter analizo napadalčevih aktivnosti za razvoj boljših obrambnih strategij.**

2.3 Nabor orodij ELK

ELK predstavlja nabor odprtokodnih orodij za zbiranje, procesiranje, shranjevanje in vizualizacijo podatkov [9]. Sestavljajo ga tri ključne komponente:

- **Elasticsearch:** porazdeljeno iskalno in analitično orodje, optimizirano za delo z velikimi količinami strukturiranih in nestrukturiranih podatkov.
- **Logstash:** orodje za procesiranje podatkovnih tokov, ki omogoča zbiranje podatkov iz različnih virov, njihovo transformacijo in posredovanje v Elasticsearch.
- **Kibana:** spletni vmesnik za vizualizacijo in analizo podatkov, shranjenih v Elasticsearch.

V kontekstu varnostne analitike je nabor orodij ELK uporaben za učinkovito zbiranje in analizo varnostnih dogodkov v realnem času. Zaradi njegove fleksibilnosti pri obdelavi različnih formatov podatkov in zmogljive možnosti vizualizacije je posebej primeren za analizo podatkov iz limanic [10].

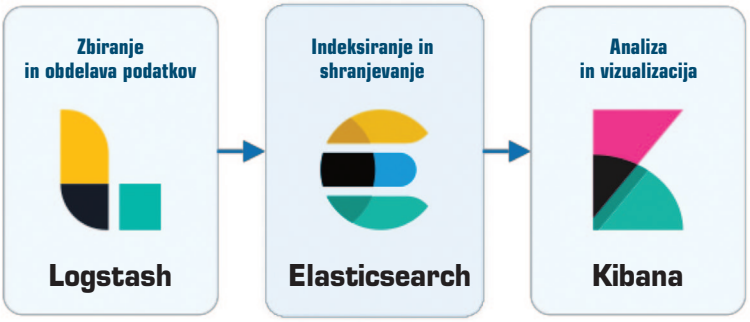
2.4 Integracija komponent

Redis limanica je v kombinaciji z naborom orodij ELK uporabna za celovito varnostno analizo, kjer limanica prestreza dostope do Redis strežnika, Logstash zbira in strukturira podatke o interakcijah, Elasticsearch jih shrani, Kibana pa ponuja njihovo vizualizacijo [11], [12].

3 PREGLED PODROČJA

Redis je zaradi svoje arhitekture, ki prednostno obravnava hitrost in enostavnost uporabe pred varnostjo, posebej ranljiv za različne vrste napadov. Carlson [1] v svojem delu izpostavlja, da ta zasnova dodatno povečuje tveganje za napade, še posebej v primerih nepravilne konfiguracije. Antirez [3] poudarja, da je Redis zasnovan za uporabo v zaupanja vrednih okoljih in ni namenjen neposredni izpostavitvi na internet.

Kljub temu pa raziskave kažejo, da so napačne konfiguracije in nena merna izpostavljenost Redis



Slika 2: **Nabor orodij ELK (Elasticsearch, Logstash, Kibana).**

strežnikov pogost pojav, kar odpira vrata različnim vrstam napadov [13].

Fan in sod. [14] v svojem preglednem delu identificirajo dva ključna elementa limanic – vabo (angl. *decoy*) in prestreznik (angl. *captor*), ki skupaj omogočata učinkovito simulacijo ranljivih sistemov in beleženje napadov. Holz in Raynal [7] opozarjata na izzive pri implementaciji prepričljivih limanic, saj napredni napadalci razvijajo tehnike odkrivanja in izogibanja le-tem.

Sodobni pristopi k analizi podatkov iz limanic se močno opirajo na napredna orodja za agregacijo in vizualizacijo podatkov. Yang in sod. [9] predstavljajo uporabo nabora orodij ELK za analizo kibernetskih napadov in učinkovito obdelavo velikih količin dnevniških zapisov v realnem času. V kontekstu oblačnih limanic so Izhikevich in sod. [10] identificirali ključni pomen geografske porazdelitve in selektivnosti napadalcev pri izbiri tarč.

Na področju Redis limanic obstaja več obstoječih implementacij. Onishi [15] je razvil osnovno Redis limanico, ki implementira najpogostejše Redis ukaze. Beelzebub [16] predstavlja naprednejši pristop z uporabo umetne inteligence za simulacijo vedenja sistemov. Oosterhof [17] je zasnoval Cowrie, srednje do visoko interaktivno SSH/Telnet limanico, ki omogoča tako emulacijo kot posredovanje povezav na dejanske sisteme. T-Pot [18] ponuja celovito platformo za postavitev različnih vrst limanic, vključno z vizualizacijskimi orodji. Anirudh in sod. [19] so pokazali, da so limanice posebej učinkovite pri zaznavanju in blaženju DoS napadov na IoT naprave, kar je relevantno tudi za Redis okolja. Vendar pa te implementacije bodisi ne ponujajo dovolj natančne simulacije Redis funkcionalnosti bodisi ne podpirajo učinkovitega prestrezanja in analize kompleksnejših napadov.

Raziskave kažejo, da so napadi na Redis strežnike pogosto avtomatizirani in sledijo predvidljivim vzorcem. Bythwood in sod. [20] v svoji analizi avtomatiziranih napadov ugotavljajo, da večina napadalcev cilja na znane ranljivosti in uporablja standardizirane pristope. To dejstvo dodatno poudarja potrebo po razvoju specializiranih limanic, ki lahko natančno simulirajo ranljive Redis instance in omogočajo podrobno analizo napadov.

Spitzner [6] izpostavlja pomembnost limanic pri odkrivanju notranjih groženj, medtem ko Wang in sod. [21] predstavljajo teoretični model za optimizacijo postavitve limanic z uporabo teorije iger. Učinkovitost limanic pri odkrivanju izsiljevalskih napadov je v svoji raziskavi predstavil Moore [22], Vishwakarma in Jain [23] pa predlagata uporabo strojnega učenja za izboljšanje zmogljivosti limanic pri odkrivanju botnet DDoS napadov.

Priya in Chakkaravarthy [11] sta raziskala uporabo vsebniških limanic v oblačnem okolju, ki zagotavlja boljšo skalabilnost in enostavnejše upravljanje. Rabzelj in sod. [24] so razvili fleksibilno in skalabilno HTTP platformo za limanice, ki lahko simulira različne spletne storitve. Izboljšan model limanice s poudarkom na večji interakciji z napadalci ob hkratnem ohranjanju integritete in privlačnosti sistema sta predstavila Abbas-Escribano in Debar [8], medtem ko so v preglednem članku o pomenu odprtokodnih limanic pri razvoju in raziskavah na področju kibernetske varnosti so svoje ugotovitve objavili Ilg in sod. [12].

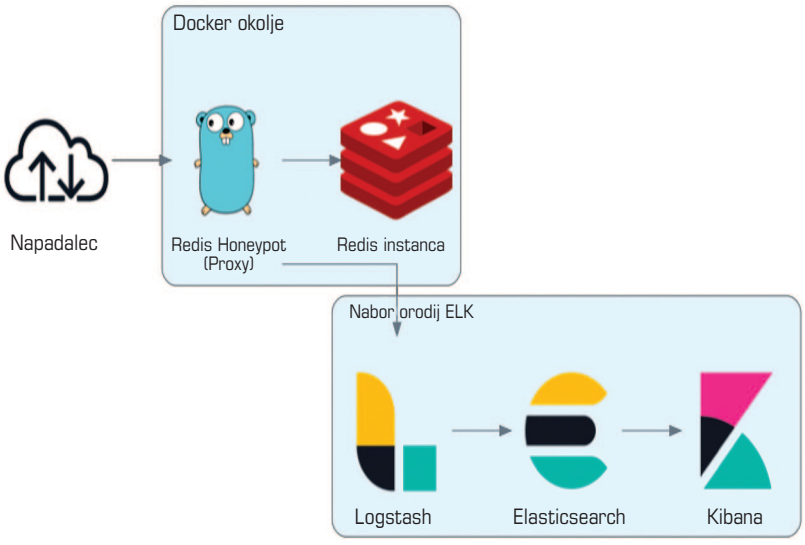
Sistematičen pregled obstoječih raziskav kaže, da trenutne implementacije Redis limanic in varnostne analitike ne zagotavljajo celovitega pristopa k spremljanju in analizi napadov. Večina obstoječih rešitev se osredotoča le na osnovno prestrezanje Redis ukazov ali splošno analitiko varnostnih dogodkov, pri čemer pogrešamo integracijo visoko-interaktivne Redis limanice z zmogljivostmi analize v realnem času.

4 METODOLOGIJA

V raziskavi smo uporabili kombinacijo eksperimentalnega in analitičnega pristopa, ki temelji na implementaciji visoko-interaktivne Redis limanice ter integraciji z naprednimi analitičnimi orodji. Naš metodološki okvir je zasnovan tako, da podpira celovito spremljanje in analizo poskusov vdorov v Redis strežnike, od začetnega odkrivanja do podrobne forenzične analize. Raziskava je potekala v treh ključnih fazah: razvoj limanice, implementacija analitike in validacija sistema.

V prvi fazi smo razvili posredniški strežnik v programskem jeziku Go, ki deluje kot transparentna limanica med napadalcem in interno Redis instanco. Ta komponenta je uporabna za natančno prestrezanje in beleženje vseh povezav ter ukazov, ne da bi napadalec zaznal prisotnost nadzornega sistema.

Druga faza je obsegala vzpostavitev analitične infrastrukture z uporabo sistema orodij ELK, kjer smo implementirali napredno procesiranje in vizualizacijo podatkov v realnem času. Celoten sistem smo implementirali kot vsebniško aplikacijo z uporabo tehnologije Docker, ki zagotavlja konsistentno



Slika 3: **Arhitektura sistema: Redis limanični posredniški (proxy) strežnika v Docker okolju prestreza napadalčeve povezave, nabor orodij ELK (Elasticsearch, Logstash, Kibana) pa beleži in analizira vse interakcije.**

delovanje v različnih okoljih in enostavno postavitev dodatnih instanc za potrebe skaliranja.

V zaključni fazi validacije smo sistem javno izpostavili na internetu ter spremljali in analizirali realne poskuse vdorov. Analiza zbranih podatkov nam je ponudila vpogled v njihove pristope, orodja in vzorce obnašanja.

4.1 Implementacija

Implementacija Redis limanice temelji na več ključnih komponentah, ki skupaj tvorijo celovito rešitev za prestrezanje in analizo Redis povezav. Arhitekturni diagram sistema je prikazan na Sliki 3.

4.1.1 Redis posredniški strežnik

Osrednji del sistema predstavlja posredniški strežnik, implementiran v programskem jeziku Go, ki nudi učinkovito upravljanje s sočasnimi povezavami in enostavno integracijo s protokolom RESP z uporabo knjižnice redcon. Strežnik deluje kot transparentni posrednik med odjemalcem in ciljnim Redis strežnikom. Posluša na standardnih Redis vratih (6379), kjer prestreza vse povezave in ukaze. Te zahteve nato posreduje na interno Redis instanco, ki teče na vratih 6380. Med delovanjem strežnik beleži vse interakcije med odjemalcem in ciljnim strežnikom.

Ključni del implementacije predstavlja struktura HoneypotServer, ki vzdržuje povezave s ciljnim Redis strežnikom, sistemom za beleženje in Logstash strežnikom:

- client – Redis odjemalec za komunikacijo z interno instanco
- logger – komponenta za lokalno beleženje dogodkov
- logstashConn – TCP povezava za pošiljanje strukturiranih zapisov

Naš pristop zagotavlja visoko stopnjo prepričljivosti za napadalce, kjer vaba temelji na avtentični Redis instanci namesto na simulaciji protokola. Tako zagotavljamo, da se sistem odziva z enako funkcionalnostjo, semantiko ukazov in lastnostmi kot produkcijski Redis strežniki. Posredniški strežnik deluje transparentno in ne spreminja Redis protokola RESP, zato napadalci ne zaznajo prisotnosti prestreznega sistema. To omogoča natančno analizo pristnih napadov brez tveganja za razkritje limanice.

4.1.2 Beleženje in analiza

Sistem implementira dvonivojsko beleženje dogodkov. Vsak dogodek se zabeleži lokalno v dnevniško datoteko in hkrati posreduje v Logstash za nadaljnjo analizo. Struktura zapisov je zasnovana tako, da podpira učinkovito analizo. Vsak zapis vsebuje časovni žig v ISO 8601 formatu ter IP naslov odjemalca, ki je vzpostavil povezavo. Poleg tega se beleži vrsta dogodka, ki je lahko vzpostavitev povezave, izvedba ukaza ali prekinitev povezave. Pri izvedbi ukazov se shranijo tako Redis ukaz kot njegovi argumenti. V primeru napak pri izvajanju se zabeležijo tudi podrobnosti o napaki.

Implementacija uporablja strukturo LogEntry za serializacijo podatkov v JSON format:

```
{
    "timestamp": "2024-12-24T15:04:05Z",
    "client_ip": "192.168.1.1",
    "command": "set",
    "arguments": ["key", "value"],
    "event_type": "command"
}
```

4.1.3 Vzpostavitev vsebniškega okolja

Sistem je zasnovan za izvajanje v vsebniških okoljih, kar zagotavlja enostavno vzpostavitev in skaliranje. Docker kompozicija vključuje štiri ključne storitve:

- redis-honeypot – glavni posredniški strežnik z interno Redis instanco
- elasticsearch – podatkovna baza za shranjevanje dogodkov
- logstash – procesiranje in razširjanje dnevniških zapisov
- kibana – vizualizacija in analiza podatkov

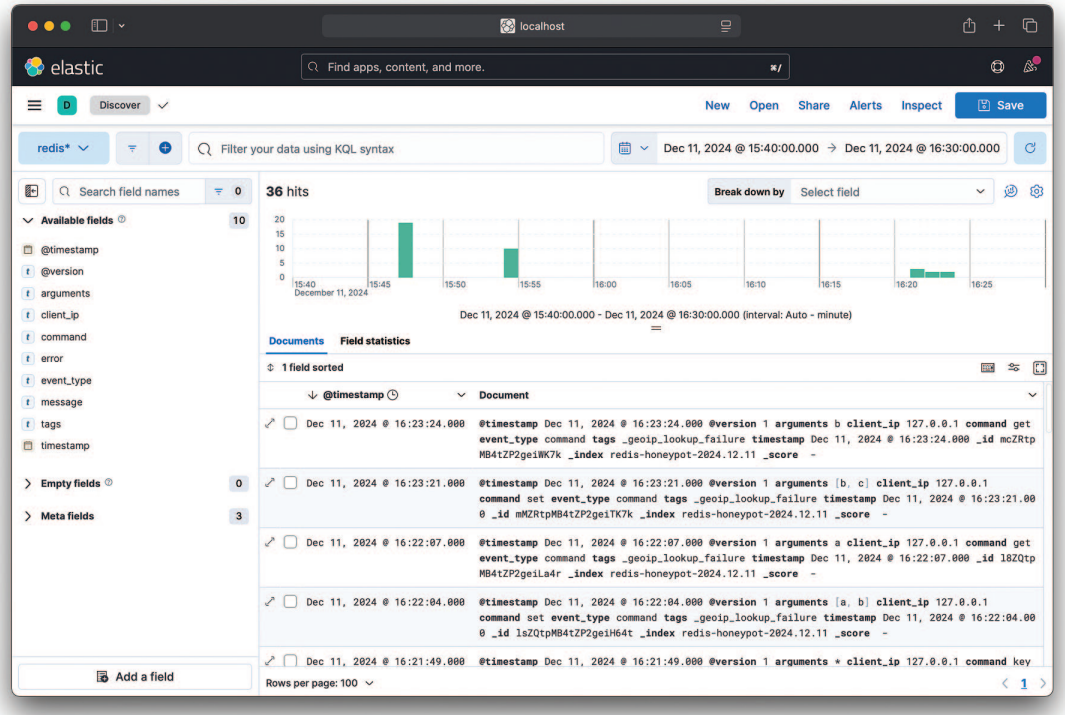
Postavitev sistema je avtomatizirana z uporabo Docker Compose, ki zagotavlja izolacijo posameznih komponent, trajnost podatkov med ponovnimi zagoni, omrežno povezljivost med vsemi storitvami ter centralizirano upravljanje z dnevniškimi zapisi. S tem pristopom je upravljanje celotnega sistema enostavno in zanesljivo.

4.1.4 Integracija z naborom orodij ELK

Logstash konfiguracija je optimizirana za obdelavo Redis dogodkov. Vključuje TCP vhod za sprejemanje JSON formatiranih zapisov ter časovno normalizacijo dogodkov. Sistem dodaja tudi geolokacijske podatke iz IP naslovov napadalcev. Vsi dogodki se indeksirajo v dnevno rotirajoče Elasticsearch indekse.

Elasticsearch shema je prilagojena učinkovitemu iskanju in združevanju podatkov o napadih. Kibana nudi vnaprej pripravljene nadzorne plošče za pregled geografske porazdelitve napadov in časovno analizo aktivnosti. Poleg tega so na voljo tudi statistični pregledi najpogostejših ukazov ter analiza poskusov izkoriščanja znanih ranljivosti v sistemu.

Za preverjanje delovanja smo sistem najprej testirali v nadzorovanem laboratorijskem okolju, kjer smo preizkusili različne scenarije Redis povezav in ukazov. Nadzorna plošča Kibane, prikazana na Sliki 4, nudi celovit pregled nad vsemi zabeleženimi dogodki v sistemu. Vizualizacija prikazuje časovno porazdelitev povezav oz. uporabljenih Redis ukazov. Sistem beleži in vizualizira vse ključne metrike: čas



Slika 4: **Pregled povezav in izvedenih ukazov na nadzorni plošči Kibane.**

povezave, izvorni IP naslov, uporabljene ukaze in njihove argumente ter morebitne napake pri izvajanju. Za hitro identifikacijo vzorcev v obnašanju odjemalcev je posebej uporabna možnost filtriranja in agregacije podatkov po različnih dimenzijah.

4.2 Eksperimentalna evalvacija

Za evalvacijo učinkovitosti implementirane Redis limanice smo sistem izpostavili na javno dostopnem strežniku. Instanca je bila dostopna 24 ur na privzetih vratih 6379 brez dodatnih varnostnih mehanizmov. Namen takšne konfiguracije je bil privabiti čim več potencialnih napadalcev in analizirati njihove tehnike izkoriščanja Redis strežnikov.

Opazovalno obdobje je bilo razmeroma kratko za poglobljeno znanstveno analizo, vendar smo z eksperimentom predvsem želeli preveriti, ali sistem v praksi deluje in tehnična implementacija izpolnjuje zastavljena pričakovanja. V tem okviru smo uspešno potrdili zanesljivo delovanje sistema ter demonstrirali, da limanica zazna tako osnovne kot tudi naprednejše napade na Redis strežnik.

Sistem smo namestili na virtualiziranem strežniku v podatkovnem centru. Za zagotavljanje konsistentnega delovanja smo uporabili Docker kompozicijo z vsemi potrebnimi komponentami (Redis, ELK stack) in poskrbeli za persistenco dnevniških zapisov. Vsi poskusi povezav in izvedenih ukazov so se v realnem času beležili lokalno in v Elasticsearch bazi.

5 REZULTATI IN ANALIZA

5.1 Enostavni napadi

Analiza dnevniških zapisov je razkrila povezave iz osmih različnih IP naslovov, pri čemer so se napadi razlikovali tako po kompleksnosti kot po namenu. Ti poskusi so bili večinoma kratkotrajni in so se zaključili po nekaj osnovnih ukazih, kar kaže na avtomatizirano odkrivanje potencialno ranljivih Redis strežnikov. To dodatno potrjujejo konstantni časovni intervali med ukazi, ki običajno trajajo med 100 in 200 ms. Pri večini poskusov je bilo opaziti tudi ponavljajoč vzorec prekinitev in ponovnih vzpostavitev povezave, kar je značilno za orodja, ki skenirajo velike bloke IP naslovov.

Podrobnejša analiza enostavnih napadov je razkrila več značilnih vzorcev. V prvi fazi so napadalci tipično uporabili ukaz INFO, s katerim so pridobili osnovne informacije o Redis strežniku, vključno z verzijo, operacijskim sistemom in konfiguracijo pomnilnika. Sledil je ukaz CONFIG GET *, s katerim so poskušali pridobiti podrobnosti o sistemski konfiguraciji. V več primerih so napadalci nato želeli spremeniti direktorij za shranjevanje podatkov z ukazom CONFIG SET dir, vendar brez nadaljnjih poskusov izkoriščanja.

Kljub svoji tehnični preprostosti ti osnovni napadi predstavljajo pomemben vpogled v začetne faze napadov na Redis strežnike in razkrivajo razširjeno uporabo avtomatiziranih orodij za iskanje ranljivih sistemov. Njihova pogostost in predvidljivi vzorci nakazujejo potrebo po razvoju naprednih varnostnih mehanizmov, ki bi omogočali zgodnje zaznavanje in blokiranje potencialnih vdorov.

5.2 Sofisticirani napadi

Posebej zanimiv je bil sofisticiran večfazni napad, ki je demonstriral napredne tehnike zlorabe Redis strežnikov. Napadalec je začel z osnovnim prepoznavanjem preko ukaza INFO SERVER, nato pa nadaljeval s poskusom namestitve zlonamerne kode preko SET ukaza z Base64 kodirano vsebino. Poskusil je tudi z izvajanjem Lua kode za vzpostavitev povratne povezave ter z namestitvijo SSH ključa za trajni dostop. Ko ti poskusi niso bili uspešni, je z ukazom SLAVEOF poskušal izkoristiti Redis replikacijski mehanizem ter naložiti zlonamerni modul.

Geografska analiza izvornih IP naslovov je pokazala globalno porazdelitev napadov in potrdila, da so Redis strežniki tarča avtomatiziranih napadov iz različnih delov sveta. Časovna porazdelitev napadov pa je pokazala enakomerno aktivnost s povečano intenziteto v večernih urah po UTC. Napadi so trajali tudi do 15 minut, z več premori med fazami.

Podrobneje si lahko pogledamo večfazni napad, ki je demonstriral tehnike zlorabe Redis strežnikov in je potekal v več jasno definiranih fazah:

1. **Pridobivanje informacij:** Napad se je začel z osnovnim prepoznavanjem preko ukaza INFO SERVER, s katerim so bile pridobljene informacije o različici in konfiguraciji Redis strežnika.
2. **Priprava okolja:** Sledil je ukaz FLUSHDB za čiščenje podatkovne baze, kar je tipična priprava za nadaljnje zlonamerne aktivnosti.
3. **Nameščanje zlonamerne kode:** Napadalec je poskusil namestiti zlonamerno kodo preko SET ukaza. Analiza Base64 kodirane vsebine je razkrila poskus vzpostavitve povratne povezave (reverse shell) na predefiniran IP naslov preko vrat 60148.

4. **Spreminjanje sistemske konfiguracije:** Nato je sledil poskus spreminjanja Redis konfiguracije za dostop do različnih sistemskih direktorijev. Tarče so bili /var/spool/cron/ za namestitev zlonamernih cronjob opravil, /root/.ssh/ za vstavljanje SSH ključev za trajni dostop in /tmp/ za pisanje v začasni direktorij.
5. **Izvajanje Lua kode:** Napadalec je nato poskusil z naprednejšo tehniko – izvedbo Lua skripte za povratno povezavo z ukazom eval.
6. **Zloraba replikacijskega mehanizma:** Po neuspehu je želel izkoristiti Redis replikacijski mehanizem z ukazom SLAVEOF <*IP*> 60148, kar bi omogočilo prenos zlonamernih podatkov preko Redis protokola.
7. **Nalaganje modulov:** Redis razširitveni sistem je bil tarča napada, ko je napadalec želel naložiti zlonamerni modul exp.so z uporabo ukaza MODULE LOAD.
8. **Čiščenje sledi:** Ob koncu napada je poskusil izbrisati sledi z ukazi system.exec za odstranitev datotek in MODULE UNLOAD za odstranitev modulov.

Dekodiranje sumljive Base64 vsebine je pokazalo poskus vzpostavitve povezave z oddaljenim strežnikom za potencialno vključitev v botnet. Napadalec je sistematično testiral različne tehnike vdora. SSH ključ, ki ga je poskušal namestiti, je bil generiran za uporabnika root@localhost.localdomain, kar razkriva uporabo standardnih napadalnih orodij.

Ta primer prikazuje sodobne napade na Redis strežnike, kjer napadalci spretno prilagajajo svoje pristope. Vse uporabljene tehnike izkoriščajo znane ranljivosti in pogoste napačne konfiguracije, kar kaže na nujnost temeljitega pregleda varnostnih nastavitev.

Rezultati potrjujejo uspešnost implementirane limanice pri beleženju napadov in identifikaciji različnih tehnik izkoriščanja, s čimer sistem služi kot učinkovito orodje za raziskovanje avtomatiziranih skeniranj Redis strežnikov.

6 DISKUSIJA

Predlagana rešitev v nasprotju z osnovnimi implementacijami, kot je Onishijeva limanica [15], ki simulira le izbrane Redis ukaze, uporablja dejansko Redis instanco. Ta pristop zagotavlja popolno podporo vsem funkcionalnostim in omogoča zaznavanje tudi sofisticiranih napadov, kot so Lua skripte, manipulacija datotečnih poti ali zloraba replikacijskih mehanizmov.

Ključna prednost sistema je integracija z naborom orodij ELK, ki v skladu z ugotovitvami Yanga in sod. [9] omogoča napredno analitiko in vizualizacijo podatkov v realnem času. Z uporabo vsebniške tehnologije Docker, podobno kot pri pristopu Priye in Chakkaravarthyja [11], zagotavljamo enostavno vzpostavitev in razširljivost sistema.

Kljub prednostim ima implementacija tudi določene omejitve. Izvajanje dejanske Redis instance zahteva več sistemskih virov v primerjavi z enostavnimi simulacijami, kar lahko pri velikem številu sočasnih povezav predstavlja performančno ozko grlo. Dodatno pomanjkljivost raziskave predstavlja relativno kratko obdobje opazovanja, saj bi daljša izpostavljenost omogočila bolj poglobljeno analizo različnih vzorcev napadov in časovnih trendov.

Opažanja iz naše študije se ujemajo z ugotovitvami raziskave Bythwooda in sod. [20], ki prav tako poroča o uporabi standardiziranih tehnik za izkoriščanje znanih ranljivosti. Tudi mi smo opazili, da so napadalci sledili predvidljivim vzorcem in uporabljali uveljavljene tehnike. Skladnost teh rezultatov kaže, da naša metodologija ustrezno odraža realne varnostne izzive v Redis okoljih.

7 ZAKLJUČEK

Predstavili smo implementacijo Redis limanice za učinkovito prestrezanje in analizo Redis povezav. Sistem temelji na transparentnem posredniškem strežniku, implementiranem v programskem jeziku Go, ki prestreže vse povezave na Redis vrata in jih posreduje interni Redis instanci. Ključni dosežek predstavlja uspešna integracija s sistemom ELK, ki omogoča celovito zbiranje, shranjevanje in vizualizacijo podatkov o povezavah in izvedenih ukazih.

Sistem je avtomatiziran z uporabo vsebniške tehnologije Docker, ki podpira enostavno vzpostavitev in upravljanje vseh komponent. Predstavlja celovito rešitev za spremljanje in analizo Redis povezav ter razumevanje varnostnih groženj.

Eksperimentalna postavitev je uspešno demonstrirala tehnično zmogljivost sistema pri zaznavanju in analizi različnih vrst napadov, od preprostih poskusov skeniranja do sofisticiranih večstopenjskih napadov z uporabo naprednih tehnik zlorabe Redis strežnikov. Ta validacija predstavlja temelj za prihodnje in obsežnejše raziskave.

Za nadaljnji razvoj sistema predlagamo več možnih izboljšav. Prva je implementacija samodejnega čiščenja oz. periodičnega resetiranja notranje Redis instance, s čimer bi preprečili prekomerno kopičenje podatkov in zagotovili tekoče delovanje sistema. Druga pomembna nadgradnja bi bila integracija strojnega učenja za analizo vzorcev napadov, ki bi prispevala k avtomatski identifikaciji in klasifikaciji zlonamernih aktivnosti.

Sistem bi lahko razširili v distribuirano arhitekturo z več instancami limanic in s tem omogočili zbiranje podatkov iz različnih geografskih lokacij in boljše razumevanje globalnih vzorcev napadov. Smiselna bi bila tudi implementacija avtomatiziranih odzivov na zaznane napade, kot so dinamično blokiranje IP naslovov ali prilagajanje simuliranega vedenja sistema. Dolgoročno bi lahko arhitekturo sistema razširili za podporo drugim protokolom in storitvam, kot so HTTP, SSH in Telnet, s čimer bi pridobili obsežnejši vpogled v različne vrste kibernetskih napadov.

Razviti sistem predstavlja pomemben korak k boljšemu razumevanju varnostnih izzivov Redis strežnikov in demonstrira uporabnost limanic pri raziskovanju kibernetskih groženj. Z implementacijo in eksperimentom smo dokazali, da je mogoče učinkovito združiti različne odprtokodne tehnologije v celovit sistem za varnostno analitiko, ki lahko pomembno prispeva k izboljšanju varnosti Redis postavitev v produkcijskih okoljih.

LITERATURA

[1] J. L. Carlson, Redis in action. USA: Manning Publications Co., 2013.

[2] J. Wright, “Over 18,000 Redis Instances Targeted by Fake Ransomware.” Accessed: Dec. 23, 2024. [Online]. Available: https://duo.com/decipher/over-18000-redis-instances-targeted-by-fake-ransomware

[3] antirez, “A few things about Redis security.” Accessed: Dec. 23, 2024. [Online]. Available: https://antirez.com/news/96

[4] Redis, “Redis Data Types.” Accessed: Dec. 24, 2024. [Online]. Available: https://redis.io/docs/data-types/

[5] Redis, “Redis Protocol specification.” Accessed: Dec. 24, 2024. [Online]. Available: https://redis.io/docs/reference/protocol-spec/

[6] L. Spitzner, “Honeypots: Catching the insider threat,” in 19th annual computer security applications conference, 2003. proceedings., Dec. 2003, pp. 170–179. doi: 10.1109/CSAC.2003.1254322.

[7] T. Holz and F. Raynal, “Detecting honeypots and other suspicious environments,” in Proceedings from the sixth annual IEEE SMC information assurance workshop, Jun. 2005, pp. 29–36. doi: 10.1109/IAW.2005.1495930.

[8] M. Abbas-Escribano and H. Debar, “An improved honeypot model for attack detection and analysis,” in Proceedings of the 18th international conference on availability, reliability and security, in ARES ’23. New York, NY, USA: Association for Computing Machinery, 2023. doi: 10.1145/3600160.3604993.

[9] C.-T. Yang, Y.-W. Chan, J.-C. Liu, E. Kristiani, and C.-H. Lai, “Cyberattacks detection and analysis in a network log system using XGBoost with ELK stack,” Soft Computing, vol. 26, no. 11, pp. 5143–5157, Jun. 2022, doi: 10.1007/s00500-022-06954-8.

[10] L. Izhikevich, M. Tran, M. Kallitsis, A. Fass, and Z. Durumeric, “Cloud watching: Understanding attacks against cloud-hosted services,” in Proceedings of the 2023 ACM on internet measurement conference, in IMC ’23. New York, NY, USA: Association for Computing Machinery, 2023, pp. 313–327. doi: 10.1145/3618257.3624818.

[11] V. S. D. Priya and S. S. Chakkaravarthy, “Containerized cloud-based honeypot deception for tracking attackers,” Scientific Reports, vol. 13, no. 1, p. 1437, Jan. 2023, doi: 10.1038/s41598-023-28613-0.

[12] N. Ilg, P. Duplys, D. Sisejkovic, and M. Menth, “A survey of contemporary open-source honeypots, frameworks, and tools,” Journal of Network and Computer Applications, vol. 220, p. 103737, 2023, doi: 10.1016/j.jnca.2023.103737.

[13] L. Labs, “Anatomy of a Redis Exploit.” Accessed: Dec. 23, 2024. [Online]. Available: https://www.lacework.com/blog/anatomy-of-a-redis-exploit

[14] W. Fan, Z. Du, D. Fernández, and V. A. Villagrá, “Enabling an anatomic view to investigate honeypot systems: A survey,” IEEE Systems Journal, vol. 12, no. 4, pp. 3906–3919, Dec. 2018, doi: 10.1109/JSYST.2017.2762161.

[15] K. Onishi, redis-honeypot. Accessed: Dec. 23, 2024. [Online]. Available: https://github.com/0n1shi/redis-honeypot

[16] M. Candela, beelzebub. Accessed: Dec. 23, 2024. [Online]. Available: https://github.com/mariocandela/beelzebub

[17] M. Oosterhof, cowrie. Accessed: Dec. 23, 2024. [Online]. Available: https://github.com/cowrie/cowrie

[18] D. T. S. GmbH, tpotce. Accessed: Dec. 23, 2024. [Online]. Available: https://github.com/telekom-security/tpotce

[19] M. Anirudh, S. A. Thileeban, and D. J. Nallathambi, “Use of honeypots for mitigating DoS attacks targeted on IoT networks,” in 2017 international conference on computer, communication and signal processing (ICCCSP), Jan. 2017, pp. 1–4. doi: 10.1109/ICCCSP.2017.7944057.

[20] W. Bythwood, J. Bentley, and I. Vakilinia, “Analyses of automated malicious internet traffic using open-source honeypots,” in SoutheastCon 2023, Apr. 2023, pp. 68–75. doi: 10.1109/SoutheastCon51012.2023.10115073.

[21] K. Wang, M. Du, S. Maharjan, and Y. Sun, “Strategic honeypot game model for distributed denial of service attacks in the smart grid,” IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2474–2482, Sep. 2017, doi: 10.1109/TSG.2017.2670144.

[22] C. Moore, “Detecting ransomware with honeypot techniques,” in 2016 cybersecurity and cyberforensics conference (CCC), Aug. 2016, pp. 77–81. doi: 10.1109/CCC.2016.14.

[23] R. Vishwakarma and A. K. Jain, “A honeypot with machine learning based detection framework for defending IoT based botnet DDoS attacks,” in 2019 3rd international conference on trends in electronics and informatics (ICOEI), Apr. 2019, pp. 1019–1024. doi: 10.1109/ICOEI.2019.8862720.

[24] M. Rabzelj, L. Š. Južnič, M. Volk, A. Kos, M. Kren, and U. Sedlar, “Designing and evaluating a flexible and scalable HTTP honeypot platform: Architecture, implementation, and applications,” Electronics, vol. 12, no. 16, 2023, doi: 10.3390/electronics12163480.

Marin Gazvoda de Reggi je študent na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Zanimajo ga področja razvoja programske opreme, kibernetske varnosti in umetne inteligence. Njegovi raziskovalni interesi zajemajo teorijo programskih jezikov in njihovo varnost.

▪

Sara Mihalič je študentka na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Navdušujejo jo področja povezana z digitalno forenziko, algoritmi in umetno inteligenco, najbolj pa jo zanima delo na interdisciplinarnih področjih, ki povezujejo tehnologijo z reševanjem konkretnih družbenih izzivov.

▪

Samo Hribar je študent na Fakulteti za računalništvo in informatiko Univerze v Ljubljano. Deluje na področju razvoja mobilnih aplikacij, zanima pa ga tudi hitro rastoče področje umetne inteligence. Na raziskovalnem področju ga zanima varnost aplikacij, od nizkonivojskih do spletnih.

▪

Ana Bračić je študentka na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Zanimajo jo področja kibernetske varnosti, kriptografije in umetne inteligence. Njeni raziskovalni interesi se osredotočajo na varnostne izzive v digitalnem okolju in uporabo naprednih tehnologij za zagotavljanje varnosti informacijskih sistemov.

▪

Matevž Pesek je izredni profesor in raziskovalec na Fakulteti za računalništvo in informatiko Univerze v Ljubljani, kjer je diplomiral (2012) in doktoriral (2018). Od leta 2009 je član Laboratorija za računalniško grafiko in multimedije. Od leta 2024 izvaja predmet Varnost programov.

Simulacija napada na komercialne sisteme IoT

Kristjan Bratašević, Matevž Pesek
Univerza v Ljubljani, Fakulteta za računalništvo in informatiko
kb90801@student.uni-lj.si, matevz.pesek@fri.uni-lj.si

Izvleček

Internet stvari ali IoT (Internet of Things) definira pametne naprave s senzorji in programsko opremo, ki se povezujejo z drugimi napravami in sistemi, za potrebe analize, nadzora ter avtomatizacije podatkov. Primeri takšnih naprav so pametne luči, pametni pralni, sušilni, pomivalni stroji, termostati, varnostne kamere za domove in druge, ki jih je večinoma mogoče enostavno upravljati tudi preko mobilnih aplikacij. Zaradi cenovne dostopnosti in naraščajoče razširjenosti teh naprav so vse pogostejše tudi težave, povezane s pomanjkljivimi podatkovnimi nabori in odsotnostjo avtomatiziranih posodobitev, kar predstavlja ključen varnostni in funkcionalni dejavnik zlasti pri napravah, ki so nenehno povezane z internetom. Napadalci lahko takšne varnostne pomanjkljivosti izkoristijo za nepooblaščeno zbiranje osebnih podatkov, onemogočanje delovanja naprav ali za zlorabo njihove računske moči naprave za vzpostavitev širših omrežij okuženih naprav (angl. botnet). Članek obravnava kritične probleme naprav skozi različne napade in njihov obseg ter strategije za obvladovanje ter preprečevanje napadov IoT. Dodatno analizira tudi večje pretekle napade, na primeru široko dostopnih naprav, kot so pametne žarnice in prezračevalni sistemi, pa prikaže enostavnost izvedbe napada. Prispevek kritično ovrednoti tudi trenutni trend nadomeščanja enostavnih naprav s "pametnimi" različicami, ki zaradi večje kompleksnosti in pomanjkljive varnostne zasnove postaja vse večji in težje obvladljiv varnostni izziv sodobnega digitalnega okolja.

Ključne besede: IoT, napadi DoS, napadi s ponavljanjem, napadi zaradi slabe avtentikacije, obramba pred napadi

Attack simulation on Commercial Iot systems

Abstract

Internet of Things (IoT) defines smart devices with sensors and software that connect to other devices and systems for data analysis, control, and automation purposes. Examples of such devices include smart lights, smart washers, dryers, dishwashers, thermostats, home security cameras, and other devices, most of which can be easily controlled via mobile applications. Due to the affordability and increasing prevalence of such devices, problems related to incomplete data sets and the absence of automated updates are also becoming more common, which is a key security and functional factor for devices that are constantly connected to the Internet. Attackers can exploit such security flaws to unlawfully collect personal data, disable devices, or misuse their computing power to build larger networks of infected devices (botnets). The article discusses critical device problems through various attacks and their scope, as well as strategies for managing and preventing IoT attacks. It also analyses major past attacks, and using widely available devices such as smart light bulbs and ventilation systems, it demonstrates the ease of attack implementation. The paper also critically evaluates the current trend of replacing simple devices with "smart" versions, which, due to increased complexity and inadequate security design, is becoming an increasingly challenging and difficult-to-manage security issue in the modern digital environment.

Keywords: Attack defence, DoS attacks, IoT, poor authentication attacks, reply attacks

1 UVOD

Internet stvari (IoT) je opredeljen kot omrežje, v katerem so fizični objekti, opremljeni s senzorji in aktuatorji, povezani prek brezžičnih in žičnih omrežij, kar omogoča nemoteno interakcijo in izmenjavo informacij med objekti v fizičnem in virtualnem svetu [1]. Pametne naprave v takšnem omrežju podpirajo analizo, obdelovanje in deljenje podatkov ter avtomatizacijo, s čimer spreminjajo funkcionalnost in uporabno vrednost vsakdanjih predmetov. Primer takšne integracije je sistem Flaura [2], ki preprost lonček za rastlino preoblikuje v avtomatizirano napravo IoT s funkcijo samodejnega zalivanja in oddaljenega obveščanja uporabnika o stopnji vlažnosti substrata na daljavo preko spleta.

Čeprav so mobilni telefoni, računalniki in druge splošno razširjene naprave, povezane na svetovni splet, redno deležne posodobitev operacijskih sistemov in aplikacij – te se pogosto izvajajo samodejno, v ozadju in brez posredovanja uporabnika –, pa naprave IoT, kot so pametne kamere, ključavnice, žarnice, gospodinjski aparati in termostati, takšnih avtomatskih nadgradenj večinoma ne prejemajo.

Medtem ko se uporabniki prvih že zavedajo, da posodobitve prispevajo k večji varnosti in prinašajo nove funkcionalnosti, ostaja pri napravah IoT to zavedanje nizko, čeprav so varnostna tveganja in ranljivosti primerljive ali celo večje [3]. Poleg tega naprave IoT delujejo v ozadju in redko opozarjajo na razpoložljive varnostne posodobitve ali odpravo kritičnih napak [4]. Proizvajalci takšnih naprav velikokrat ne ponujajo dolgoročne nadgradnje programske opreme, zato po odkritju varnostne pomanjkljivosti ostanejo trajno ranljive in pomenijo stalno grožnjo za uporabnike naprav [5].

Pametne naprave tako pogosto ostajajo neposodobljene bodisi zaradi pomanjkanja uporabnikove aktivne interakcije z napravo, bodisi zaradi razširjenega prepričanja – tako pri uporabnikih kot proizvajalcih –, da naprave IoT same po sebi ne predstavljajo resne nevarnosti ali bistvene grožnje. Prav ta zmotna predstava pa napadalcem ponuja signifikantno možnost za dostop in zlorabo naprav IoT [3]. Takšne naprave napadalci uporabljajo kot orodje za vohunjenje, zbiranje osebnih podatkov in vdor v človekovo zasebnost in dostojanstvo, pri čemer podatke izkoristijo sami ali pa jih prodajo naprej za nadaljnje zlorabe. Pridobljen dostop jim omogoča tudi zlorabo naprav za izvajanje napadov na druge storitve. Najbolj znan primer tovrstne zlorabe je DDoS (angl. Distributed Denial of Service) napad, pri katerem napadalci uporabijo računsko moč večjega števila, navadno nelegalno prisvojenih, pametnih naprav, da z množično obremenitvijo ciljnega sistema povzročijo njegovo nedelovanje. Takšni napadi se izvajajo z različnimi nameni: motenjem delovanja, izsiljevanjem (odkupnina), prikrivanjem drugih dejavnosti ali drugimi zlonamernimi cilji [6].

Namen in struktura članka sta pregleden prikaz trenutnega stanja naprav IoT, demonstracija napada na komercialne naprave IoT, ki so trenutno na voljo v Sloveniji, in ozaveščanje bralca o nevarnostih, povezanih s pomanjkanjem (samodejnih) posodobitev teh naprav. Prikazani napadi so kljub enostavni izvedbi precej resni, saj ne zahtevajo posebnih orodij in obširnega tehničnega znanja, ter izkoriščajo osnovne ranljivosti. Ravno ta enostavnost izvedb problematičnih napadov s proporcionalno malo zahtevanega truda in znanja, pa izpostavlja resnost in pogostost opisanih groženj v današnjem času.

2 PREGLED SORODNIH DEL

Razširjenost naprav IoT in hkrati pojav varnostno zaskrbljujočih napadov, povezanih z njimi, sta spodbudila podrobnejšo analizo in raziskovanje slednjih. Deogirikar in Vidhate sta tipe napadov razdelila na štiri kategorije: fizične, omrežne, programske in enkripcijske [7]. Predstavila sta, kako lahko napadalci škodijo napravam z različnimi pristopi – od fizičnih posegov, kot je neposredno vrivanje zlonamerne kode ali povzročanje fizične škode, do omrežnih napadov, kot je kopiranje RFID značk, in različnih aplikacijskih ter dekripcijskih napadov. Avtorja posebej izpostavljata nevarnost napadov z uporabo t. i. stranskih kanalov (angl. side-channel), ki ciljajo na pomanjkljivosti v implementaciji enkripcije. Pri takih napadih lahko napadalci pridobijo zaupne informacije na podlagi časovnih razlik v izvajanju kriptografskih operacij, ki so odvisne od pravilnosti ali nepravilnosti vnosa podatkov.

Butun idr. so možne napade na naprave IoT razdelili na 2 glavni kategoriji – pasivni in aktivni napadi – z dodatnimi podkategorijami [8]. Poudarili so, da je vsak napad, ki se ga ne da izslediti, kategoriziran kot pasivni napad. Ti napadi so usmerjeni predvsem v kršitev zaupnosti podatkov, npr. s prisluškova-

njem. Nasprotno pa aktivni napadi ne posegajo le v zaupnost, temveč tudi v izrabo celovitosti podatkov. Takšne napade je mogoče izslediti, vendar napadalci kljub temu pogosto skušajo ostati čim manj opazni in prikriti svojo dejavnost.

Da naprave IoT niso edini možni vektor napada preko programskih in strojnih ranljivosti, so predstavili Alrawi idr., ki so poudarili, da zasnova IoT ni omejena le na fizično napravo, temveč vključuje tudi vse spremljevalne komponente, ki omogočajo njeno delovanje [9]. Skoraj vsaka naprava IoT ima namreč pripadajočo mobilno aplikacijo, ki je pogosto lahko ranljiva že sama po sebi. Ker naprave te aplikacije prepoznajo kot zaupanja vredne, lahko napadalci izkoristijo ranljivosti aplikacij za pridobitev dostopa do naprav. Te aplikacije pogosto trpijo za pomanjkljivostmi, kot so dovoljenja s prevelikimi privilegiji, napake v programski kodi ter trdo kodirani (angl. hard-coded) občutljivi podatki. Dodatno varnostno tveganje predstavljajo tudi oblačne storitve tretjih oseb, ki so lahko napačno konfigurirane ali pa same uporabljajo ranljive storitve, kar povzroča nevarnosti pri prenosu podatkov. Veliko naprav namreč še vedno uporablja zastarele protokole, kot je UPnP, in redko kriptirajo informacije v lokalnem omrežju, kar jih dela dovzetne za napade s posrednikom (MITM).

Za zaščito naprav IoT sta Bhunia in Gurusamy predstavila novo ogrodje, imenovano SoftTings, ki temelji na zasnovi programsko določenih omrežij (SDN) in omogoča preprečevanje 98% vseh napadov na naprave IoT [10]. Avtorja sta prikazala, kako je mogoče stikala s podporo za tehnologijo SDN uporabiti za dinamično dodeljevanje in upravljanje pravil na omrežju. Na najnižji ravni omrežja se nahajajo same naprave, katerih promet usmerja stikalo SDN in ga posreduje nadrejenemu krmilniku. Krmilnik se v začetni fazi "nauči" običajnega obnašanja naprav – spremlja npr. število poslanih zahtevkov, neuspešnih prijav, porabo pasovne širine in podobno. Na podlagi vedenjskega vzorca nato sproti posodablja pravila, zaznava odstopanja in v primeru anomalij promet blokira, omeji ali preusmeri v karanteno. Poleg profiliranja običajnega vedenja naprav mora krmilnik za učinkovito delovanje imeti tudi dostop do znanih varnostnih informacij, kot so primeri že znanih napadov (npr. DDoS, poplavljanje TCP), naslovi prepovedanih IP številk na t. i. črni listi (angl. black list) in podobno.

3 ZGODOVINSKI PREGLEDI VEČJIH NAPADOV

3.1 Napadi na programsko opremo - mirai botnet

Mirai botnet je eden izmed najbolj prepoznavnih napadov na naprave IoT [4]. Leta 2016 se je pojavila prva različica Mirai botneta, kadar sta ponudnik strežnikov OVH, ter ponudnik internetnih storitev Dyn zaradi obsežnih napadov nenadno prenehala delovati. Izkazalo se je, da je OVH utrpel napad z obsegom 1.17TB prenosa podatkov na sekundo, medtem ko je izpad storitve Dyn povzročilo nedelovanje več spletišč, kot so Twitter, Netflix, Reddit in Github. Mirai je sestavljen iz 4 delov - robota (angl. bot) oz. zlonamerne kode, nadzornega strežnika (angl. command and control (C&C) server), nalagalnika (angl. loader), ki prevaja stojno kodo za različne arhitekture procesorjev, ter strežnika za poročila (angl. report server), ki shranjuje podatke o napadih. Mirai se širi z iskanjem naključnih IP-naslovov na vratih TCP od 23 do 2323. Na odkritih napravah s slabimi varnostnimi nastavitvami poskuša pridobiti dostop z uporabo slovarja gesel in v primeru uspešnega vdora pridobi dostop do ukazne lupine (angl. shell). Nadzornemu strežniku nato sporoči podatke o sami napravi, na napravo z orodjem wget pa prenese in zažene zlonamerno programsko kodo. Okužena naprava lahko nato prejema ukaze nadzornega strežnika in tako napade druge strežnike.

3.2 Napadi na strojno opremo - Stuxnet

Razvijalci naprav IoT ne razvijajo le programske kode, ki je lahko izpostavljena napadom, ampak tudi napravo, kot fizično entiteto. Relevantni so torej tudi napadi preko stranskih kanalov, kjer napadalci izkoriščajo ranljivosti izven programske opreme. Ti napadi lahko temeljijo na zaznavanju večjega magnetnega sevanja, porabe energije ali branju pomnilnika med delovanjem, kjer napadalci zajamejo pomnilnik ter z njega preberejo zaupne podatke. Poleg tega je lahko tudi ena izmed šibkih točk naprav nezaščiten dostop preko serijske povezave na matični plošči, preko katere lahko napadalci z napravo upravljajo. Prav tako je napade mogoče izvesti s spremembo zunanjega stanja, kot je npr. zunanja temperatura [11].

Znani napad na strojno opremo je bil Stuxnet leta 2010. Širil se je prek lokalnih omrežij in USB ključev ter povzročal fizično škodo na industrijskih sistemih. Njegova tarča so bile centrifuge iranske jedrske elektrarne, katerih hitrost vrtenja je povečal do te mere,

da je prišlo do njihovega fizičnega uničenja. Napad je bil zelo prikrit, saj iz sistemskega nadzora ni bilo mogoče zaznati nobenih posebnosti [12].

3.3 Napadi na tehnologije veriženja blokov - IOTA

Tehnologijo veriženja blokov (angl. blockchain tehcnology), prvotno razvito kot osnova za kriptovalute, so v preteklih letih začeli uporabljati tudi v različnih projektih IoT, kot sta DECENTER [13] ter BUILDCHAIN [14]. Njena uporaba omogoča številne prednosti, med katerimi izstopajo odprava enotnih točk odpovedi, izboljšana celovitost podatkov ter odpornost proti napadom DDoS [15], prinaša pa tudi določene izzive. Eden izmed njih je napad z 51-odstotnim nadzorom, pri katerem napadalci prevzamejo več kot polovico računske moči rudarjenja na verigi, kar jim ob uporabi tehnologije *proof-of-work* omogoča popoln nadzor nad verigo blokov. Poleg tega so za prenos podatkov uporabljene pametne pogodbe (angl. smart contracts), ki lahko vsebujejo varnostne ranljivosti v programski kodi. Te napake lahko privedejo do napačnega delovanja ali pa odprejo vrata zlonamernim napadom [16].

Zgovoren primer tovrstne ranljivosti se je zgodil leta 2020, ko je bila denarnica Trinity Wallet, ki jo je uporabljala platforma IOTA, tarča napada zaradi ranljivosti zunanje knjižnice, uporabljene v programski kodi pametne denarnice [17]. Napadalcem je uspelo pridobiti zasebne ključe uporabnikov in ukrasti kriptovaluto IOTA v vrednosti 2 milijonov ameriških dolarjev. Ta dogodek je tako pokazal, kako lahko že najmanjše varnostne pomanjkljivosti v podpornih komponentah resno ogrozijo celoten sistem.

4 EKSPERIMENTALNA IZVEDBA NAPADOV

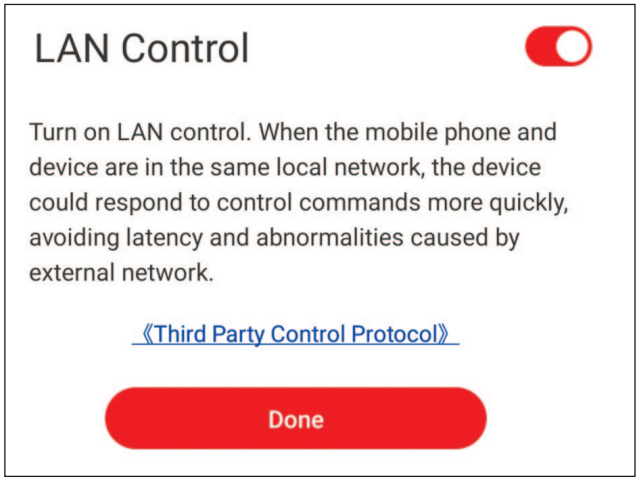
Za demonstracijske primere smo izbrali dve pametni napravi IoT - pametno žarnico tujega proizvajalca in pametni sistem za prezračevanje zraka. Napravi sta bili izbrani naključno, saj sta bili že na voljo, med analizo pa smo pri obeh zaznali različne možne oblike napadov. V okviru eksperimenta smo prikazali postopke napada z vidika napadalca. Predstavili smo obliko napada, katere pomanjkljivosti izkorišča, kakšen je njegov glavni namen in kako je videti iz omrežnega vidika. Nato smo opisali, kako napadalci zaznajo ranljivosti na ciljni napravi, katera orodja potrebujejo za izvedbo napada in kako poteka priprava na napad. Na koncu sledi še praktična predstavitev napada na izbrano napravo.

Napade smo izvedli v okolju, v katerem se pametni napravi najbolj uporabljata - to je navadno domače omrežje, v katerem se nahajajo vsakodnevne naprave uporabnikov s privzetimi varnostnimi nastavitvami usmerjevalnika, katere operaterji privzeto uporabnikom določijo. V to omrežje smo preko brezžične povezave povezali računalnik z operacijskim sistemom Linux, iz katerega smo nato naprej po omrežju prisluškovali, prestrezali in izvajali napade. Takšni napadi so bili ponovljeni večkrat, tudi tako, da smo naprave postavili na drugo omrežje, kjer smo simulacijo ponovno uspešno ponovili, tako da smo potrdili njihovo konsistentnost in prisotnost. Glavna omejitev eksperimentov je testiranje le dveh naprav IoT, katere so široko komercialno dostopne uporabnikom, vendar ne vključujejo širšega okolja drugih naprav IoT, predvsem naprav visoko zaupnih proizvajalcev.

4.1 Napad zaradi slabe avtentikacije

Napadi, ki izkoriščajo slabo avtentikacijo, so razmeroma enostavni za izvedbo. Zaradi odsotnosti avtentikacijskih mehanizmov ali slabe implementacije varnostnih praks lahko napadalci pridobijo neposreden dostop do naprave preko slabo zavarovanega vmesnika - bodisi z uporabo vmesnika API (Application Programming Interface), ki je namenjen pošiljanju strukturiranih, računalniško razumljivih ukazov (npr. v obliki JSON - JavaScript Object Notation) preko specifičnih vrat naprave, ali pa z uporabo spletnega vmesnika naprave. Ker vmesniki API pri takšnih napravah pogosto ne vključujejo mehanizmov za avtentikacijo, lahko napadalci napravi pošiljajo zahteve brez predhodne overitve. Prav tako pa so tudi nevarni spletni vmesniki naprav, saj velikokrat uporabljajo privzete oz. splošno znane prijavne podatke, kot so *admin, user, password, 123456* in podobne [18]. Zaradi teh šibkih nastavitev so naprave ranljive za napade s t. i. slovarji gesel (angl. password dictionaries), pri katerih napadalci s pomočjo računalnika ali druge naprave izvajajo avtomatizirano preverjanje velikega števila kombinacij uporabniških imen in gesel z namenom ugotavljanja uporabniških poverilnic.

Za ponazoritev tega varnostnega problema smo uporabili pametno žarnico. Ob prvemu povezovanju žarnice z lokalnim omrežjem aplikacija ponudi možnost vklopa t. i. lokalnega (LAN) nadzora, kot je prikazano na Sliki 1.

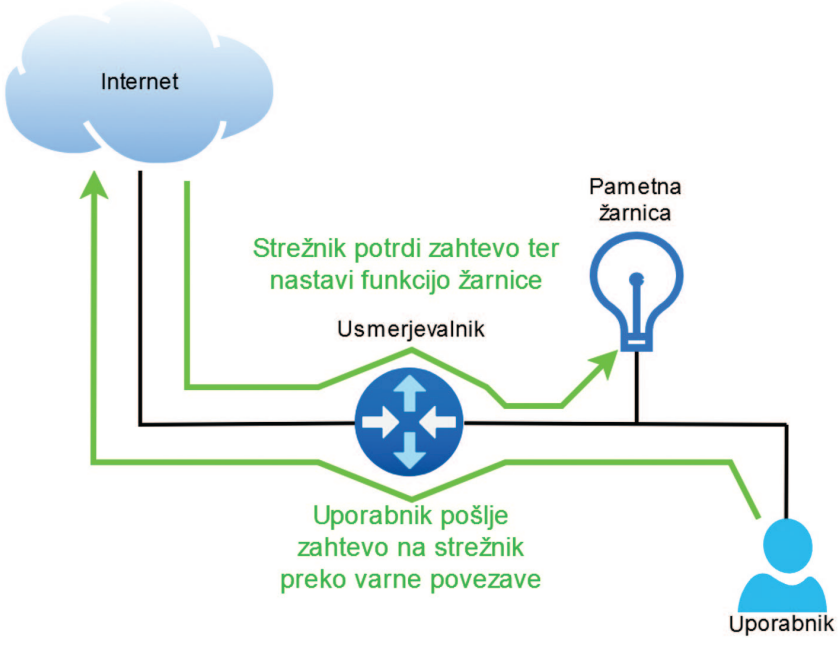


Slika 1: **Vklop možnosti LAN nadzora**

Brez uporabe te možnosti nadzor nad pametno žarnico lahko poteka le tako, da uporabniki z uporabo pametne naprave pošljejo zahtevo na oddaljen strežnik, le ta pa nazaj odgovori, ter ukaz pošlje na pametno žarnico. Celoten proces uporablja varovan protokol TLS, kjer je komunikaciji v celoti zavarovana pred napadalci proti napadom, kot sta ponavljanje ali prisluškovanje. Potek komunikacije je razviden na Sliki 2.

Ta možnost je zelo zavajajoča – uporabnikom namreč sporoča, da bo z vklopom te možnosti naprava hitreje odzivna na lokalnem omrežju. Poleg tega je ta možnost že privzeto vključena. Besede 'naprava', 'hitreje' in 'izogibanje zakasnitvam' uporabnike prepričajo, da gre za funkcijo, ki izboljša uporabniško izkušnjo, in jo zato pustijo vključeno. Opozorilo o potencialnih varnostnih tveganjih oziroma dejanski razlagi funkcionalnosti 'LAN nadzora' je na voljo šele s klikom na diskretno označeno modro besedilo 'Third Party Control Protocol' (nadzorni protokol tretje osebe). Glede na statistične podatke, da kar 91 % uporabnikov pogojev uporabe ne prebere [19], lahko sklepamo, da večina uporabnikov tudi tokrat ne bo prebrala teh informacij. Obenem smo z uporabo orodja Wireshark ugotovili, da pametna žarnica kljub vklopljeni možnosti LAN nadzora in povezavi mobilne naprave z istim omrežjem, ukaze še vedno pošilja na zunanji strežnik. V primeru izpada internetne povezave – ob sicer delujočem lokalnem omrežju – pametna žarnica ne deluje, kar pomeni, da je funkcionalnost 'LAN nadzora', ki je privzeto vklopljena in predstavlja veliko varnostno luknjo, zavajajoča in se je pri naši analizi izkazala za popolnoma lažno.

Ta funkcionalnost v resnici omogoča dostop do naprave preko lokalnega omrežja na vratih 55443. Pri analizi uporabe na teh vratih nismo zaznali nobenega omrežnega prometa, kar pojasnjuje, zakaj žarnica brez internetne povezave ne deluje. Napadalci lahko to privzeto nastavitev zlorabijo s pomočjo javno dostopne dokumentacije [20].



Slika 2: **Potek nadzora pametne žarnice**

{“id”:1,“method”:“set_power”,“params”:[“off”, “smooth”, 5]}

Slika 3: **Ukaz za izklop luči z uporabo nadzora LAN**

Z uporabo različnih orodij lahko napadalci identificirajo IP-naslov pametne žarnice, nato pa z uporabo programa, kot je *telnet*, pošiljajo ukaze neposredno napravi v strukturirani obliki, kot je navedena v proizvajalčevi dokumentaciji [20]. Za vzpostavitev povezave mora napadalec v ukazu telnet navesti IP-naslov naprave (v našem primeru 192.168.1.64) ter vrata (55443). Z zagonom ukaza telnet 192.168.1.64 55443 se vzpostavi povezava z napravo, napadalec pa lahko prične s pošiljanjem ukazov. Iz dokumentacije je razvidno, da je za izklop luči uporabljen ukaz, predstavljen na Sliki 3:

Ukaz vsebuje več polj, ki nadzirajo funkcionalnost pametne žarnice:

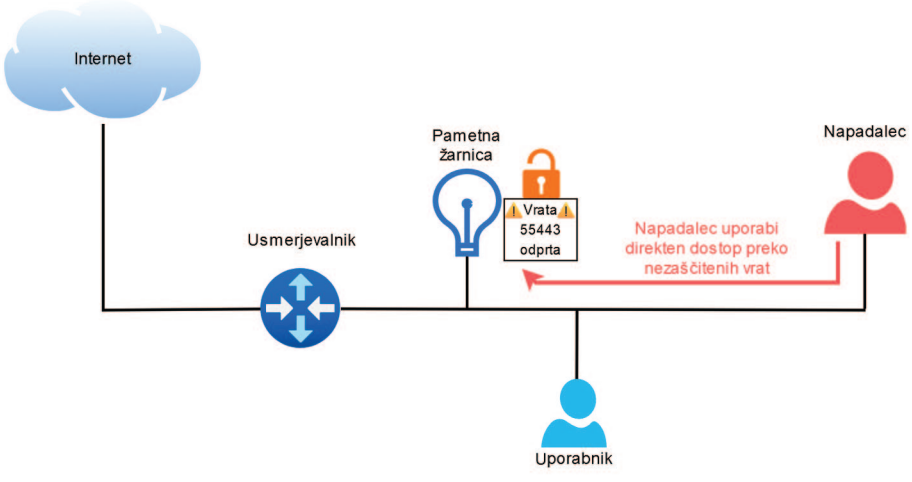
- Polje ‘id’ je identifikator, ki ga bi ga lahko uporabili za enolično identificiranje naprave, če bi razvijali aplikacijo za nadzor več luči. To nam omogoča enostavnejši nadzor nad več napravami, zato je v našem primeru vrednost tega polja lahko poljubna.
- Polje ‘method’ vsebuje ime metode, ki bo uporabljena. Ker želimo spremeniti stanje luči (vklop/izklop), bomo uporabili metodo ‘set_power’
- Polje ‘param’ sprejme število podatkov, odvisno od zahtevane metode. Ukaz ’set_power’ sprejme 3 parametre (opcijsko 4): Prvi parameter določa stanje luči. Za vklop je treba nastaviti vrednost ‘on’, za izklop pa ‘off’. Drugi parameter določa način spremembe stanja. Možnosti sta ‘sudden’, kjer se sprememba zgodi takoj, in ‘smooth’, kjer sprememba poteka postopoma v času, določenem v tretjem parametru. Tretji parameter določa čas v milisekundah, ki je potreben za enakomerno spreminjanje vrednosti, če je izbran način spremembe ‘smooth’. Čeprav je relevanten zgolj pri slednjem, mora biti čas definiran tudi v načinu ‘sudden’.

Za vklop luči moramo parameter ‘off’ zamenjati z ‘on’, če želimo spremeniti svetilnost luči na 50 %, pa uporabimo metodo ‘set_bright’ in namesto parametra ‘on’ oziroma ’off’ podamo numerično vrednost svetilnosti v odstotkih - v tem primeru 50.

Zaradi slabe informiranosti uporabnikov s strani proizvajalca lahko tako napadalci pridobijo popoln nadzor nad pametno žarnico in z njo upravljajo brez dovoljenja uporabnika, kot je prikazano na Sliki 4.

4.2 Napad DoS

S poplavljanjem naprave z zahtevki napadalci dosežejo, da naprava postane neodzivna ali nedosegljiva za običajne uporabnike. Temu pravimo napad DoS (Denial of Service). Tako kot je več pametnih naprav skupaj dovolj zmogljivih, da z napadom DDoS (distribuiran DoS, ki poteka iz več naprav) ohromijo druge naprave ali strežnike, pa so lahko tudi same žrtev enakega napada ali preprostejšega napada DoS, ki se izvaja iz ene same naprave. Ker imajo pametne naprave omejene računske zmogljivosti, jih je lažje ohromiti že z enostavnim napadom DoS, nasprotno pa je za



Slika 4: **Potek napada preko vrat 55443**

```
192.168.1.131   192.168.1.64    TCP     66 56379 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SA
192.168.1.64    192.168.1.131   TCP     60 80 → 56379 [SYN, ACK] Seq=0 Ack=1 Win=5744 Len=0 MSS=1436
192.168.1.131   192.168.1.64    TCP     54 56379 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
192.168.1.131   192.168.1.64    HTTP   425 GET / HTTP/1.1
192.168.1.64    192.168.1.131   TCP     60 80 → 56379 [ACK] Seq=1 Ack=372 Win=5373 Len=0
192.168.1.64    192.168.1.131   TCP    123 80 → 56379 [PSH, ACK] Seq=1 Ack=372 Win=5373 Len=69 [TCP
192.168.1.131   192.168.1.64    TCP     54 56379 → 80 [ACK] Seq=372 Ack=70 Win=64171 Len=0
192.168.1.64    192.168.1.131   HTTP    78 HTTP/1.1 404 Not Found  (text/html)
192.168.1.131   192.168.1.64    TCP     54 56379 → 80 [ACK] Seq=372 Ack=94 Win=64147 Len=0
192.168.1.131   192.168.1.64    TCP     55 [TCP Keep-Alive] 56379 → 80 [ACK] Seq=371 Ack=94 Win=6414
192.168.1.64    192.168.1.131   TCP     60 [TCP Keep-Alive ACK] 80 → 56379 [ACK] Seq=94 Ack=372 Win=
192.168.1.131   192.168.1.64    TCP     55 [TCP Keep-Alive] 56379 → 80 [ACK] Seq=371 Ack=94 Win=6414
192.168.1.64    192.168.1.131   TCP     60 [TCP Keep-Alive ACK] 80 → 56379 [ACK] Seq=94 Ack=372 Win=
192.168.1.131   192.168.1.64    TCP     55 [TCP Keep-Alive] 56379 → 80 [ACK] Seq=371 Ack=94 Win=6414
192.168.1.64    192.168.1.131   TCP     60 [TCP Keep-Alive ACK] 80 → 56379 [ACK] Seq=94 Ack=372 Win=
```

Slika 5: **Komunikacija pametne žarnice z orodjem Wireshark**

uspešen napad na zmogljivejše naprave in strežnike potreben večji sistem, ki ga zagotavlja DDoS.

V našem primeru smo analizirali pametno žarnico, ki je ranljiva za napad DoS, zaradi delujoče storitve **HTTP** na vratih **80**. Ko v spletni brskalnik vpišemo njen IP-naslov, naprava odgovori s sporočilom 'This URI does not exsist', z uporabo orodja Wireshark pa lahko preverimo komunikacijo med računalnikom, ki je poslal zahtevo, in pametno žarnico.

Z analizo prometa, prikazano na Sliki 5, smo potrdili, da naprava uporablja navaden protokol HTTP. Računalnik pošlje zahtevo tipa GET, pametna žarnica pa nanjo odgovori s prej omenjemin sporočilom. Odgovor je prikazan na Sliki 6.

Kljub temu da je odgovor velik le 22 bajtov, lahko za izvedbo napada DoS izkoristimo že samo delovanje protokola HTTP, saj temelji na protokolu TCP na transportni plasti. TCP ima sicer številne prednosti, kot so preprečevanje izgub, podvajanja, napačnega vrstnega reda in napak paketov, vendar ima tudi slabost, saj mora ob vsaki vzpostavitvi povezave opraviti t. i. trojno rokovanje. Na strani strežnika (v našem primeru pametne žarnice) to predstavlja nezanemarljivo obremenitev virov. Napadalci lahko to šibkost izkoristijo v napadu TCP SYN s poplavljanjem tako, da na žarnico pošljejo veliko TCP SYN (sinhroniziraj, angl. synhronize) zahtev. Zaradi množice teh zahtev je vsa računska moč žarnice porabljena za TCP ACK (potrdi, angl. acknowledge) odgovore, kot prikazuje Slika 7. Žarnica je s tem preobremenjena in zato ne bo uspela obdelati ukazov, ki jih bodo poslali legitimni uporabniki preko aplikacije.

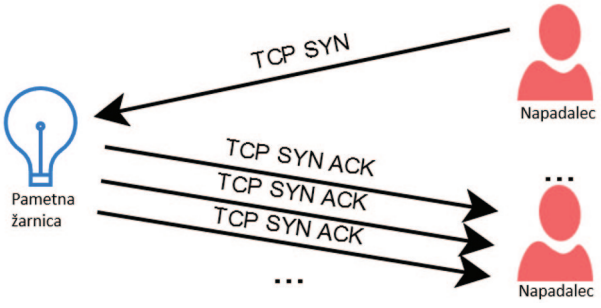
Za izvedbo napada DoS uporabimo orodje *hping3* za pošiljanje paketov na izbrani naslov in na ta način preobremenimo pametno žarnico do točke, ko postane neodzivna na uporabnikove zahteve.

Kot je razvidno s Slike 8, ukaz *hping3* vsebuje več dodatnih parametrov:

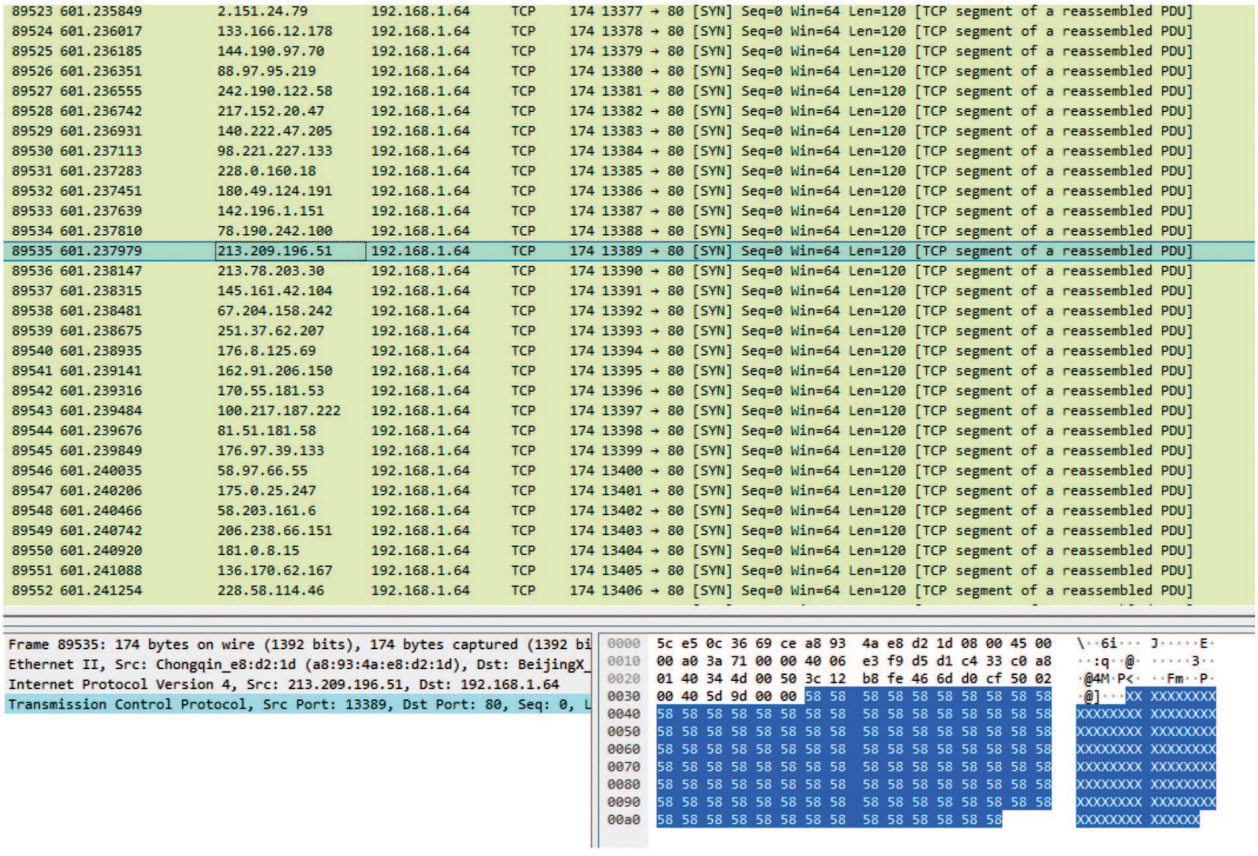
- Parameter **-c** (vrednost **10000**) določa število poslanih paketov pred zaustavitvijo programa.
- Parameter **-d** (vrednost **150**) določa velikost podatkovnega dela vsakega paketa v bajtih.
- Parameter **-S** je uporabljen za pošiljanje paketov **TCP SYN**.
- Parameter **-w** (vrednost **64**) določa velikost okna TCP, ki pove, koliko podatkov je lahko prenesenih, pred prejemom potrdila s strežnika (TCP ACK).
- Parameter **-p** (vrednost **80**) predstavlja vrata, na katerih teče strežnik. V našem primeru uporabimo 80, ki so privzeta za protokol HTTP.
- Parameter **–flood** omogoča način 'poplavljanja', kjer pošiljamo pakete čim hitreje, kar je ključnega pomena za napad DoS.

```
    [HTTP response 1/1]
    [Time since request: 0.113633000 seconds]
    [Request in frame: 252]
    [Request URI: http://192.168.1.64/]
    File Data: 22 bytes
Line-based text data: text/html (1 lines)
    This URI doesn't exist
```

Slika 6: **Odgovor pametne žarnice na HTTP zahtevo**



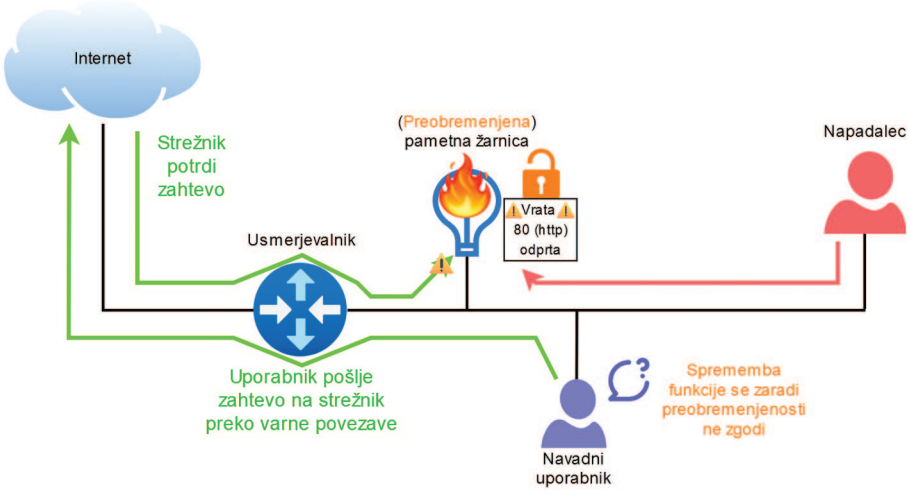
Slika 7: **Potek napada DoS**



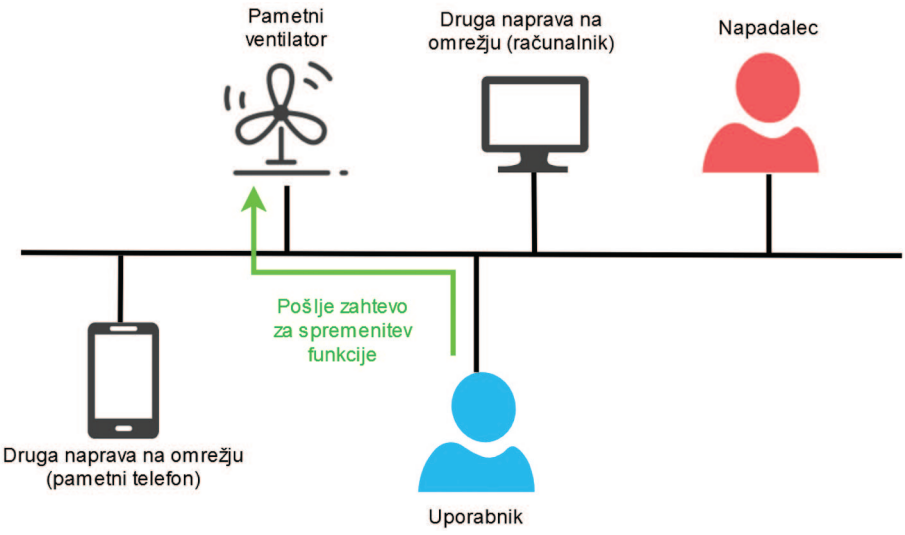
Slika 9: **Pregled prometa pri napadu DoS**

- Parameter **–rand-source** doda naključno generiranje izvornih IP-naslovov, ki lahko oteži zaznavanje napada in morebitno filtriranje s strani ciljne naprave.
- Na koncu je naveden še **IP-naslov** ciljne naprave (v tem primeru **192.168.1.64**).

Kot je razvidno iz izpisa orodja Wireshark (Slika 9), je zabeležen velik obseg prometa iz naključno generiranih IP-naslovov, ki je usmerjen proti pametni žarnici. Gre za izvedbo napada DoS. Zaradi velike količin zahtev je žarnica preobremenjena z obdelavo dohodnega prometa in se posledično ne odziva več na uporabnikove zahteve v aplikaciji (Slika 10).



Slika 10: **Vizualni prikaz omrežja pri napadu DoS**



Slika 11: **Pošiljanje ukaza pametni napravi**

Ko se izvajanje programa zaključi, se promet na omrežju zmanjša in posledično pametna žarnica po krajšem času ponovno postane odzivna na uporabnikove ukaze.

4.3 Napad s ponavljanjem

Napad s ponavljanjem je pri napravah IoT zelo pogost – kar 75 % naprav IoT je ranljivih na tovrstne napade [21]. Napadalec v takem primeru prestreže, zajame, ali kako drugače pridobi pakete, ki bi sicer potovali od uporabnikove naprave (npr. mobilni telefoni ali nadzorna plošča) do pametnih naprav IoT. Včasih so vmes tudi strežniki, vendar so takrat napadi težje izvedljivi, saj večina internetnega prometa – kar 97,6 % – poteka prek protokola SSL/TLS [22], ki onemogoča ponovno uporabo zajetih paketov.

Za tarčo v naši reprodukciji napada smo izbrali pametno napravo za prezračevanje zraka, ki ima lastno aplikacijo za pametne telefone. Za razliko od pametne žarnice ta naprava komunicira le v lokalnem omrežju in zahtev ne pošilja na strežnik. Zaradi tega je napad s ponavljanjem bistveno lažje izvedljiv, saj podatki ob prenosu zelo verjetno niso šifrirani. Slednje je potrdil tudi naš eksperiment.

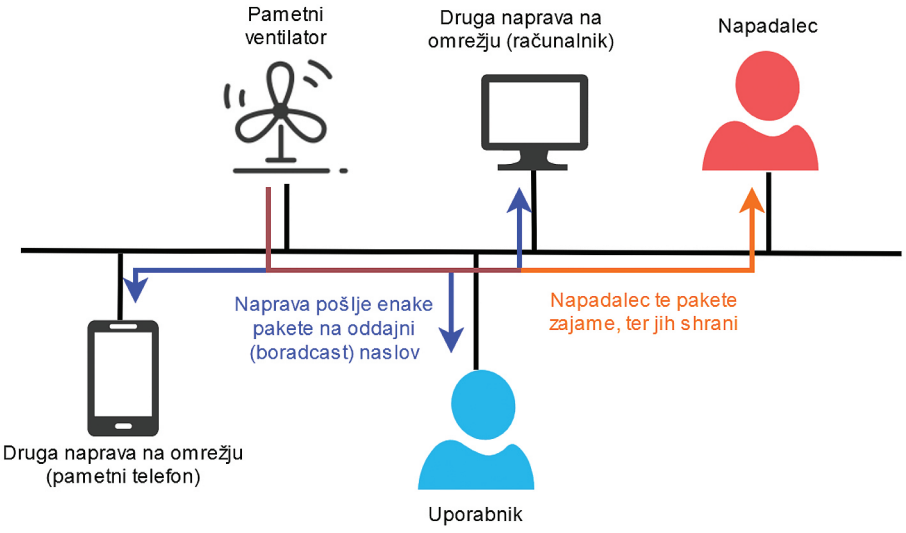
Ko smo iz mobilne naprave poslali ukaz (Slika 11), smo z orodjem Wireshark v omrežnem prometu opazili tri enake zaporedne pakete UDP, poslane z naslova pametne prezračevalne naprave na oddajni (angl. broadcast) naslov omrežja (Slika 12). Napravo je mogoče enostavno prepoznati že s prisluškovanjem, saj približno vsako sekundo pošlje enak paket UDP na oddajni naslov (Slika 13).

Iz vsebine paketov je bilo razvidno, da potujejo iz smeri pametne naprave na oddajni naslov omrežja. Poleg tega niso imeli nobenega mehanizma za prikrivanje, preverjanje integritete ali preverjanje enoličnosti.

Z uporabo orodja Wireshark smo pakete shranili in izvozili, s pomočjo orodja *tcpreplay* pa smo jih nato ponovno poslali po omrežju in tako uspešno izvedli napad s ponavljanjem.

```
2 1.025… 192.168.0.236  192.168.0.255  UDP   92 1028 → 1028 Len=50
3 1.029… 192.168.0.236  192.168.0.255  UDP   92 1028 → 1028 Len=50
4 1.034… 192.168.0.236  192.168.0.255  UDP   92 1028 → 1028 Len=50
```

Slika 12: **Trije zaporedni paketi UDP prezračevalne naprave**



Slika 13: **Prezračevalna naprava pošlje pakete na oddajni naslov**

```
tcpreplay --intf1=enp0s3 speed_fast.pcapn
```

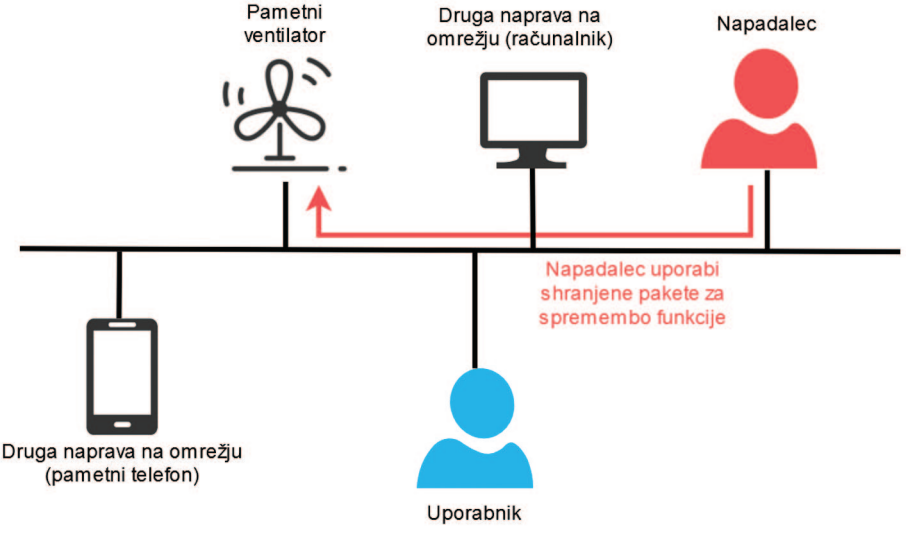
Slika 14: **Ponovno pošiljanje paketov s tcpreplay**

V ukazu na Sliki 14 smo parametru ---intf1 podali ime mrežnega vmesnika (enp0s3), s katerega smo želeli poslati pakete, ter ime datoteke (speed_fast.papn), ki smo jo izvozili z orodjem Wireshark. Komunikacija na nivoju omrežja je predstavljena na Sliki 15.

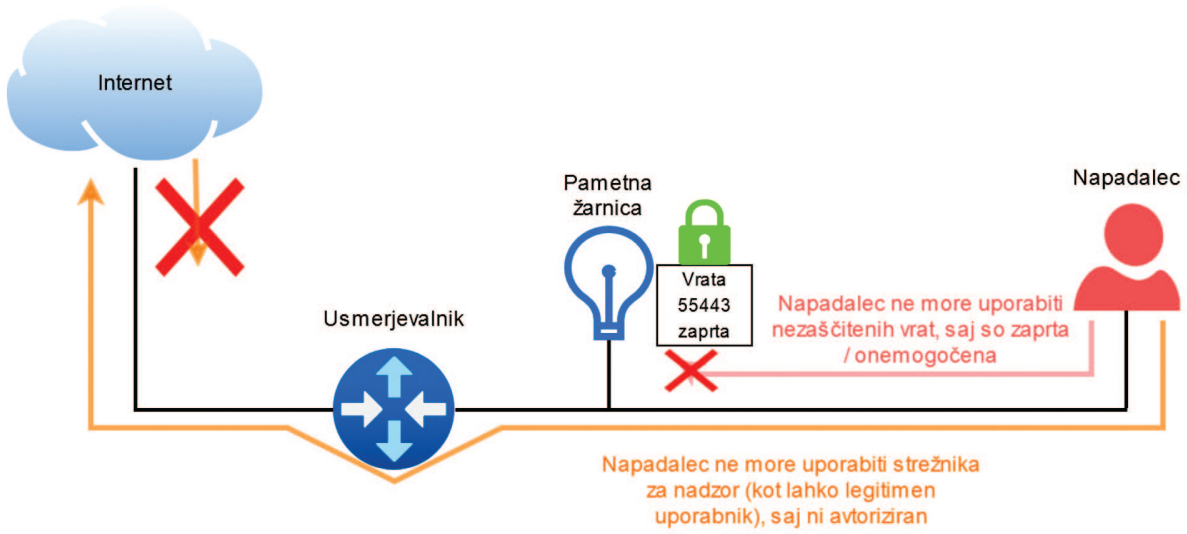
Po uspešni izvedbi ukaza nas program obvesti o poslanih paketih. Ker so bili ti paketi zajeti ob pošiljanju ukaza za hitrejše delovanje z mobilne naprave, se ob njihovi ponovni uporabi funkcija zopet aktivira.

5 OBRAMBA PRED NAPADI

Obrambo pred opisanimi napadi lahko deloma izvajajo uporabniki sami, v večini primerov pa gre za programske ranljivosti, ki jih morajo nasloviti proizvajalci. To odpira glavno vprašanje, ali je nujno, da je vsaka naprava pametna. Tudi če so uporabniki seznanjeni s tveganji, so zaradi napak ali malomarnosti proizvajalcev pogosto izpostavljeni ranljivostim, pred katerimi se ne morejo učinkovito zaščititi.



Slika 15: **Napadalec uporabi zajete pakete za spremembo funkcije**



Slika 16: **Napadalec nima več dostopa do upravljanja**

5.1 Preprečevanje napada zaradi slabe avtentikacije

V splošnem je preprečevanje takšnih napadov dokaj enostavno. Uporabniki morajo spremeniti privzeto geslo in upoštevati dobre prakse ustvarjanja močnih gesel.

Toda v obravnavanem primeru napad izhaja iz pomanjkanja implementacije osnovne avtentikacije iz strani proizvajalca nasploh. Takšne dobre prakse tako niso dovolj, če proizvajalec njihovo pomembnost zanemari. V tem primeru to predstavlja, da uporabniki pustijo omogočeno privzeto možnost lokalnega nadzora, kar odpre varnostno luknjo. Odgovornost proizvajalcev je, da uporabnike o nevarnosti ustrezno opozorijo.

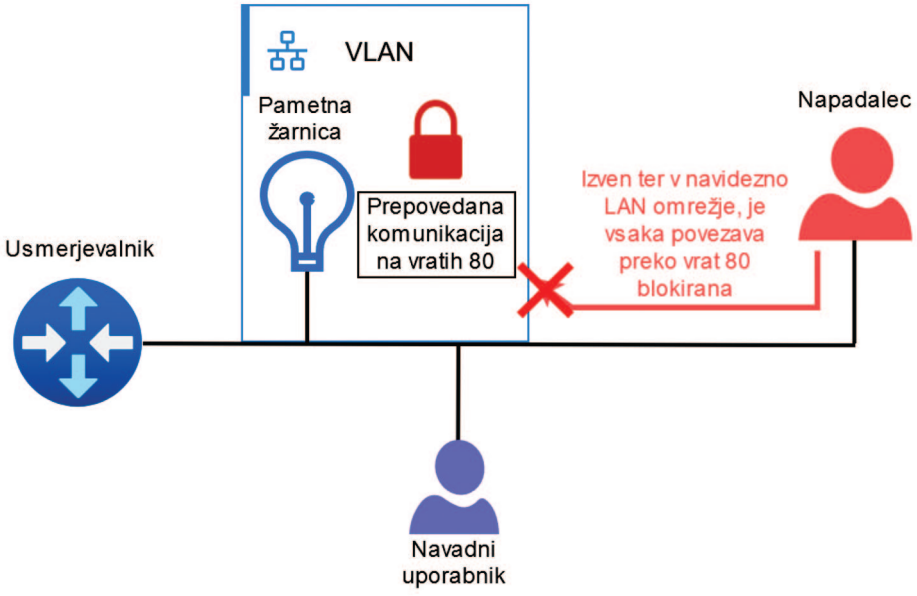
Z zaprtjem vrat 55433 napadalci izgubijo možnost nedovoljenega dostopa do upravljanja pametne žarnice, saj je po tem edini način spreminjanja nastavitev žarnice mogoč le preko uradnega strežnika. Ta povezava je povsem varna in zaščitena, za legitimno uporabo pa je potrebna ustrezna avtorizacija (Slika 16).

Kot proizvajalci naprav lahko takšne napade preprečimo z boljšim informiranjem uporabnikov o delovanju omenjene funkcije lokalnega nadzora. Še učinkovitejša rešitev je uvedba avtentikacije ob pošiljanju podatkov. Ker je ob prvi nastavitvi pametne žarnice v vsakem primeru potrebno ustvariti oz. se prijaviti v uporabniški račun, bi lahko ta proces, ki poteka preko strežnika z zaščitenim protokolom TLS 1.2, uporabili tudi za izmenjavo javnega in zasebnega ključa. Ta ključ bi se nato uporabljal za zaščito komunikacije znotraj lokalnega omrežja, s čimer bi bili podatki prikriti. Hkrati bi bila sama izmenjava ključev varno izvedena preko zaščitenega protokola.

5.2 Preprečitev napada DoS

Tudi pred napadi DoS se končni uporabniki težko zavarujejo, saj preprečevanje zahteva programsko implementacijo s strani proizvajalcev.

Uporabniki lahko napravo zgolj umestijo v ločen, zaščiten segment omrežja (VLAN), kjer je omejen dostop do vrat 80. Vhodni in izhodni paketi so tako nastavljeni na zavrnitev, kot je prikazano na Sliki 17. Analiza z orodjem Wireshark potrjuje, da se vrata 80 oziroma protokol HTTP sploh ne uporabljajo.



Slika 17: **Napadalec nima več dostopa do vrat 80**

Proizvajalci lahko težavo odpravijo tako, da vrata 80 oziroma spletno stran, ki ni uporabi, preprosto zaprejo. Če je uporaba teh še vedno potrebna, pa morajo vzpostaviti ustrezne mehanizme za preprečevanje DoS napadov. Ker večina povezav, razen lokalnega nadzora na vratih 55443 z uporabo ključev, poteka prek zunanjega strežnika, lahko proizvajalci uporabijo zaščito DDoS, kot je Cloudfare.

5.3 Preprečitev napada s ponavljanjem

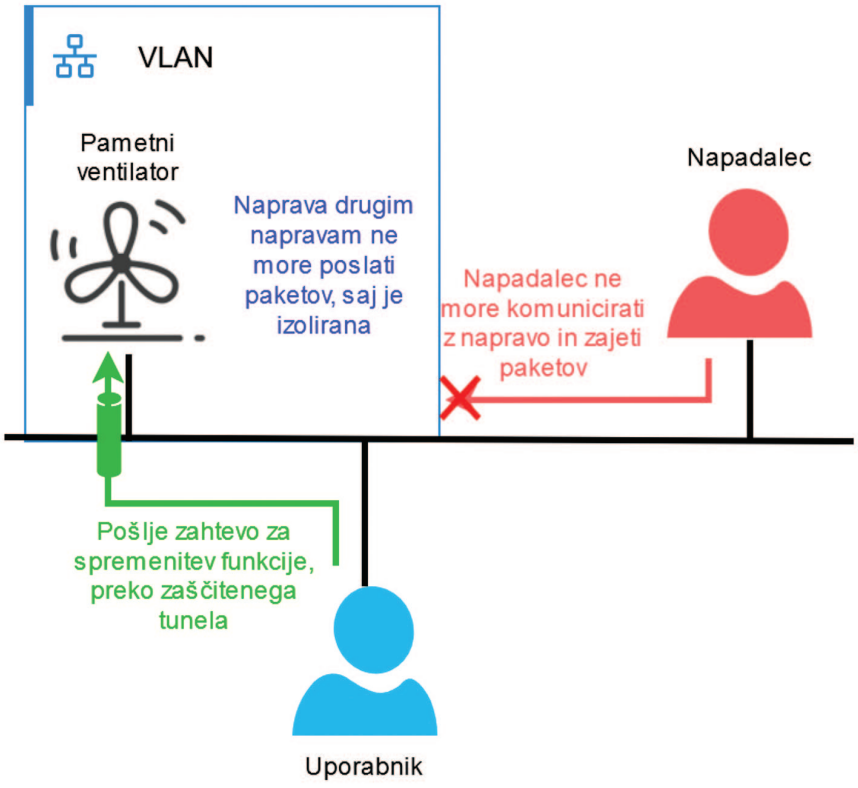
Napad je mogoče najenostavneje preprečiti z dobro programsko kodo, za kar so odgovorni proizvajalci. S strani uporabnikov je preprečevanje takšnih napadov bistveno težje, saj je izogibanje napadom skoraj nemogoče, če so napadalci že znotraj lokalnega omrežja in komunikacija poteka brez kakršnekoli zaščite.

Največ, kar lahko naredi uporabnik, je vzpostavitev ločenega zaščitenega omrežja VLAN, v katerega so povezane ranljive naprave. Za komunikacijo med mobilno napravo za nadzor funkcij in samo napravo IoT na omrežju VLAN moramo postaviti tudi zaščitni tunel, preko katerega se pošiljajo prekriti paketi, kar preprečuje prisluškovanje napadalcev, kot je prikazano na Sliki 18.

Pomembno je, da uporabimo najnovejše protokole za varovanje brezžičnega omrežja, kot sta WPA3 ali WPA2. V nasprotnem primeru je omrežje lahko popolnoma odprto in potencialnim napadalcem omogoča dostop do enostavno ponovljivih paketov, saj protokol UDP sam po sebi ne zagotavlja zaščite.

Implementacija ustrezne zaščite je torej nujna in mogoča predvsem na strani proizvajalcev že ob razvoju programske opreme. Eden od učinkovitih pristopov je uporaba enkratnih vrednosti (angl. nonce) za označevanje posameznih paketov. Ta preprečuje ponovno uporabo že poslanih paketov, saj bi bili neveljavni paketi zavrnjeni. Podobno pristop uporablja protokol TCP z zaščito proti ponavljanju.

Ker v našem primeru zaščita samih podatkov ni bistvena, šifriranje podatkov ni nujno, zato lahko še vedno uporabljamo protokol UDP. Na primer, dejstva, da smo spremenili moč naprave na najvišjo vrednost nam ni treba prikrivati, saj to sporočilo ne vsebuje zaupnih ali osebnih podatkov. V primerih, kjer pa bi bilo potrebno prikriti poslane podatke, bi pa bil potreben drugačen, varnostno okrepljen pristop.



Slika 18: **Napadalec ne more prisluškovati paketom**

6 DISKUSIJA

Naprave IoT izpostavljajo ključno vprašanje, kako zagotoviti varnost naprav, ki so vse bolj prisotne v vsakdanjem življenju, a zaradi neinformiranosti uporabnikov pogosto zapostavljene, kar nato privede do varnostnih incidentov. Čeprav je ozaveščenost uporabnikov ključnega pomena za varovanje lastnih naprav z zgoraj opisanimi metodami (uporaba močnih gesel, preverjanje stanja naprav, redne posodobitve), osrednja odgovornost za varnost še vedno leži na proizvajalcih pametnih naprav.

Dandanes lahko katerokoli podjetje, tudi nekvalificirano, začne proizvajati pametne naprave. To vodi v preplavljen trg, na katerem se pogosto znajdejo izdelki z varnostnimi pomanjkljivostmi in brez ustrezne regulacije. Medtem ko v Evropski uniji za naprave veljajo strogi varnostni standardi, so ti na nekaterih drugih trgih pogosto spregledani ali neobstoječi. Potrošniki, ki stremijo k znižanju stroškov, se zato pogosto odločajo za cenejše izdelke s tujih trgov, kar pa povečuje tveganje za uporabo nevarnih naprav.

Zaradi pomanjkanja nadzora proizvajalci pogosto tudi zanemarijo testiranje varnosti programske opreme naprav, posledice te odločitve pa nosijo končni uporabniki, ki morajo za varnost poskrbeti sami.

Optimalna rešitev za opisano težavo bi bila uvedba strožjih zakonodaj in regulacij, ki bi veljale tudi za uvoz naprav IoT s tujih trgov. Te bi morale določati minimalne varnostne zahteve za programsko kodo, kot je obvezna enkripcija podatkov med komunikacijo, ter jasno opredeljevati odgovornost proizvajalcev za posledice varnostnih pomanjkljivosti.

Zaradi obsežnosti globalnih trgov je uveljavitev takšnih ukrepov na globalni ravni izjemno zahtevna, zato za končne uporabnike še vedno predstavlja najboljšo prakso nakup naprav priznanih kvalificiranih proizvajalcev z dokazanimi varnostnimi standardi.

7 ZAKLJUČEK

Pomembnost rednega posodabljanja naprav in kakovostno zasnovane programske kode je pri napravah IoT, ki so povezane na splet, ključna. Že najmanjša napaka v kodi lahko privede do velikih varnostnih ranljivosti, ki omogočajo izvajanje napadov – od zbiranja podatkov do onemogočanja naprave ter zlorabe računske moči naprave.

V članku smo obravnavali tri ključne napade na programsko opremo.

Napadi zaradi slabe avtentikacije so pogosto posledica šibkih gesel ali celo popolne odsotnosti avtentikacije. Napadalcem omogočijo popoln dostop do naprave brez iskanja drugih ranljivosti in so enostavni za izvedbo. Za preprečevanje je nujno upoštevanje dobrih varnostnih praks ustvarjanja uporabniških računov.

Napadi DoS ohromijo delovanje pametnih sistemov. Preprečevanje tovrstnih napadov mora biti vključeno že v zasnovo programske opreme, saj lahko uporabniki sami zgolj izolirajo napravo v ločeno omrežje (VLAN). S tem tako preprečijo omrežno komunikacijo med takšno ranljivo napravo in ostalimi napravami v omrežju, ter preprečijo izvedbo napada DoS.

Napadi s ponavljanjem omogočajo ponovno uporabo poslanih podatkov, ki so bili zajeti med prenosom. Proizvajalci naprav jih lahko preprečijo z uporabo varnostnih mehanizmov, kot sta uporaba enkratnih vrednosti v paketu, in/ali šifriranje podatkov v paketu. Uporabniki se lahko zavarujejo zgolj z vzpostavitvijo izoliranega omrežja in uporabo t. i. tunelskega načina za prenos šifriranih podatkov.

Poleg omenjenih napadov obstajajo tudi drugi varnostni izzivi, ki so povezani z veliko rastjo popularnosti naprav IoT.

Uporaba umetne inteligence za varnost v napravah IoT

Z vse bolj razširjeno uporabo umetne inteligence v varnostnih sistemih nastajajo tudi nova orodja za zaznavanje in preprečevanje vdorov v pametne naprave. Napredni modeli so zmožni obdelati velike količine podatkov in z uporabo nevronskih mrež enostavneje prepoznajo vzorce, ki lahko opozorijo na oz. preprečijo napade [23].

Raziskava [24] predlaga nov sistem za zaznavanje vdorov (angl. Intrusion Detection System - IDS) v naprave IoT z uporabo integriranih konvolucijskih nevronskih mrež (CNN) in mrež z dolgotrajnim spominom (LSTM), ki z 99,52 % natančnostjo zaznajo zlonameren promet. Razvijajo se tudi prilagojene limanice (angl. honeypots), [25] ki z uporabo strojnega učenja omogočajo avtomatizirano interakcijo z napadalci. Ker je razvoj posebnih limanic za vsako napravo IoT neizvedljiv, uporabimo takšne metode, da nato napadalci porabijo več časa na prilagojenih limanicah, kot bi sicer na klasičnih. Hkrati pa je potrebno pomniti, da zaradi izjemne rasti uporabe naprav IoT in vedno večje integracije z našim vsakdanjim življenjem dosedanji protinapadi postajajo prešibki. Za učinkovito obrambo se bo tako potrebno tudi poslužiti naprednih pristopov, kot so strojno in globoko učenje[26].

Prihodnje raziskave se bi lahko osredotočale v smeri uporabe umetne inteligence in strojnega učenja v domačih okoljih za varovanje vsakodnevnih naprav IoT uporabnikov. Z razširitvijo domačega usmerjevalnika, kateremu bi bila dodana omenjena funkcionalnost, bi lahko izboljšali varnost celotnega obstoječega omrežja, saj se bi ta učila na podlagi delovanja omrežja, ter bi takoj ukrepala ob zaznavi nenormalnih anomalij.

Nevarnost predstavljajo tudi **napadi na osebne podatke**, saj naprave IoT zbirajo velike količine zaupnih osebnih podatkov. Ob pomanjkljivi zaščiti lahko to vodi do kršitev zasebnosti in zlorab, vključno s krajo ali preprodajo podatkov na črnem trgu [27].

LITERATURA

[1] G. Kipper, “Chapter 6 - visions of the future,” in Augmented reality, G. Kipper, Ed., Boston: Syngress, 2013, pp. 129–142. doi: 10.1016/B978-1-59-749733-6.00006-1.

[2] M. McMaker, “Smart, self-watering plant pot planter ‘flaura’.” https://www.thingiverse.com/thing:4921885, 2021.

[3] G. M. Køien, “Aspects of security update handling for IoT--devices,” Int. J. Adv. Security, vol. 10, no. 1, 2017.

[4] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, “DDoS in the IoT: Mirai and other botnets,” Computer, vol. 50, no. 7, pp. 80–84, 2017, doi: 10.1109/MC.2017.201.

[5] T. Bakhshi, B. Ghita, and I. Kuzminykh, “A review of IoT firmware vulnerabilities and auditing techniques,” Sensors, vol. 24, no. 2, 2024, doi: 10.3390/s24020708.

[6] S. T. Zargar, J. Joshi, and D. Tipper, “A survey of defense mechanisms against distributed denial of service (DDoS) flooding attacks,” IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp. 2046–2069, 2013, doi: 10.1109/SURV.2013.031413.00127.

[7] J. Deogirikar and A. Vidhate, “Security attacks in IoT: A survey,” in 2017 international conference on i-SMAC (IoT in social, mobile, analytics and cloud) (i-SMAC), 2017, pp. 32–37. doi: 10.1109/I-SMAC.2017.8058363.

[8] I. Butun, P. Österberg, and H. Song, “Security of the internet of things: Vulnerabilities, attacks, and countermeasures,” IEEE Communications Surveys & Tutorials, vol. 22, no. 1, pp. 616–644, Jan. 2020, doi: 10.1109/COMST.2019.2953364.

[9] O. Alrawi, C. Lever, M. Antonakakis, and F. Monrose, “SoK: Security evaluation of home-based IoT deployments,” in 2019 IEEE symposium on security and privacy (SP), IEEE, May 2019, pp. 1362–1380. doi: 10.1109/SP.2019.00013.

[10] S. S. Bhunia and M. Gurusamy, “Dynamic attack detection and mitigation in IoT using SDN,” in 2017 27th international telecommunication networks and applications conference (ITNAC), IEEE, Nov. 2017, pp. 1–6. doi: 10.1109/ATNAC.2017.8215418.

[11] I. Tudosa, F. Picariello, E. Balestrieri, L. De Vito, and F. Lamonaca, "Hardware security in IoT era: The role of measurements and instrumentation," in 2019 II workshop on metrology for industry 4.0 and IoT (MetroInd4.0&IoT), 2019, pp. 285–290. doi: 10.1109/METROI4.2019.8792895.

[12] M. Baezner and P. Robin, "Stuxnet," Center for Security Studies (CSS), ETH Zürich, 4, Oct. 2017. doi: 10.3929/ethz-b-000200661.

[13] P. Kochovski, R. Sakellariou, M. Bajec, P. Drobintsev, and V. Stankovski, "An architecture and stochastic method for database container placement in the edge-fog-cloud continuum," in Proceedings of the 33rd IEEE international parallel & distributed processing symposium (IPDPS 2019), IEEE, 2019, pp. 396–405. doi: 10.1109/IPDPS.2019.00050.

[14] P. Miri and V. Stankovski, "Blockchain-powered IoT for smarter infrastructure: Structural health monitoring use-case," in Proceedings of the 2024 IEEE international conference on computer communication and the internet (ICCCI), IEEE, 2024, pp. 145–149. doi: 10.1109/ICCCI62159.2024.10674173.

[15] Z. Shah, I. Ullah, H. Li, A. Levula, and K. Khurshid, "Blockchain based solutions to mitigate distributed denial of service (DDoS) attacks in the internet of things (IoT): A survey," Sensors, vol. 22, no. 3, p. 1094, 2022, doi: 10.3390/s22031094.

[16] S. Singh, A. S. M. S. Hosen, and B.-G. Yoon, "Blockchain security attacks, challenges, and solutions for the future distributed IoT network," IEEE Access, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.

[17] IOTA Foundation, "Trinity attack incident part 1: Summary and next steps." https://blog.iota.org/trinity-attack-incident-part-1-summary-and-next-steps-8c7ccc4d81e8/, 2020.

[18] S. Stahie, "Common credentials criminals use in IoT dictionary attacks revealed." https://www.bitdefender.com/en-au/blog/hotforsecurity/common-credentials-criminals-use-in-iot-dictionary-attacks-revealed, 2021.

[19] C. Cakebread, "You're not alone, no one reads terms of service agreements." https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11, 2017.

[20] L. Qingdao Yeelink Information Technology Co., "Yeelight WiFi light inter-operation specification." https://www.yeelight.com/download/Yeelight_Inter-Operation_Spec.pdf, 2015.

[21] S. Lazzaro, V. D. Angelis, A. M. Mandalari, and F. Buccafurri, "Is your kettle smarter than a hacker? A scalable tool for assessing replay attack vulnerabilities on consumer IoT devices," in Proceedings of the 2024 IEEE international conference on pervasive computing and communications (PerCom), IEEE, 2024, pp. 114–124. doi: 10.1109/PerCom59722.2024.10494466.

[22] W3Techs, "Usage statistics and market shares of SSL certificate authorities for websites." https://w3techs.com/technologies/overview/ssl_certificate, 2025.

[23] T. Mazhar et al., "Analysis of IoT security challenges and its solutions using artificial intelligence," Brain Sciences, vol. 13, no. 4, p. 683, 2023, doi: 10.3390/brainsci13040683.

[24] N. Ansar, M. S. Ansari, M. Sharique, A. Khatoon, M. A. Malik, and M. M. Siddiqui, "A cutting-edge deep learning method for enhancing IoT security," arXiv preprint arXiv:2406.12400, Jun. 2024, doi: 10.48550/arXiv.2406.12400.

[25] V. S. Mfogo, A. Zemkoho, L. Njilla, M. Nkenlifack, and C. Kamhoua, "AIIPot: Adaptive intelligent-interaction honeypot for IoT devices," arXiv preprint arXiv:2303.12367, Mar. 2023, doi: 10.48550/arXiv.2303.12367.

[26] F. Hussain, R. Hussain, S. A. Hassan, and E. Hossain, "Machine learning in IoT security: Current solutions and future challenges," arXiv preprint arXiv:1904.05735, Mar. 2019, doi: 10.48550/arXiv.1904.05735.

[27] H. Taherdoost, "Security and internet of things: Benefits, challenges, and future perspectives," Electronics, vol. 12, no. 8, p. 1901, 2023, doi: 10.3390/electronics12081901.

▪

Kristjan Brataševec je študent na Fakulteti za računalništvo in informatiko Univerze v Ljubljani. Zanima se za področje kibernetske varnosti in razvoja programske opreme, še posebej za vsakodnevno uporabo. Posveča se ustvarjanju varnih celovitih aplikacijskih sistemov, tako z vidika programske kode, kot s sistemskega in omrežnega vidika.

▪

Matevž Pesek je izredni profesor in raziskovalec na Fakulteti za računalništvo in informatiko Univerze v Ljubljani, kjer je diplomiral (2012) in doktoriral (2018). Od leta 2009 je član Laboratorija za računalniško grafiko in multimedije. Od leta 2024 izvaja predmeta Varnost programov in Varnost sistemov, kjer se raziskovalno ukvarja s poučevanjem konceptov in organizacijo dogodkov s področja računalniške varnosti.

Kompetenčne vrzeli in kadrovski izzivi na področju informacijske in kibernetske varnosti: analiza stanja v Sloveniji

Andreja Markun, Alenka Brezavšček
Fakulteta za organizacijske vede, Univerza v Mariboru, Kidričeva cesta 55a,4000 Kranj
andreja.markun@student.um.si, alenka.brezavscek@um.si

Izvleček

V času hitro rastoče digitalizacije postaja vprašanje kadrovskih kompetenc in zagotavljanja ustrezno usposobljenih in kompetentnih kadrov na področju informacijske in kibernetske varnosti vse bolj ključno za dolgoročno digitalno odpornost organizacij. V prispevku predstavljamo rezultate nedavne raziskave, ki je bila izvedena med slovenskimi organizacijami. Raziskava razkriva izrazite kompetenčne vrzeli na področju informacijske in kibernetske varnosti, pri čemer je bila kot glavna ovira za tako stanje izpostavljeno pomanjkanje usposobljenega kadra na trgu. Ugotovljeno je bilo, da organizacije, ki varnost vključujejo v strateške cilje, prej prepoznajo potrebe po kadrovskem razvoju, proaktivno načrtujejo izobraževanja ter bolj sistematično gradijo kompetenčne baze. Zaznani so bili tudi začetni učinki sprememb v zakonodajnih okvirih ZInfV-1 in NIS2, predvsem v obliki večjih vlaganj v usposabljanje in sodelovanje z zunanjimi izvajalci. Prispevek ponuja empirično podlago za oblikovanje sistemskih ukrepov in podpira strateško načrtovanje razvoja kadrov na področju informacijske in kibernetske varnosti za učinkovito obvladovanje digitalnih tveganj v slovenskem prostoru.

Ključne besede: kompetence, zagotavljanje kadrov, informacijska varnost, kibernetska varnost, digitalna odpornost, slovensko gospodarstvo

Skills gaps and workforce challenges in information and cyber security: Insights from Slovenia

Abstract

In the age of rapidly advancing digitalisation, the issue of workforce skills and the availability of appropriately trained and qualified information and cyber security professionals is becoming increasingly important for the long-term digital resilience of organisations. This paper presents the results of a recent study conducted among Slovenian organisations. The research reveals significant skill gaps in the area of information and cyber security, with the lack of qualified professionals in the labour market seen as the main obstacle. It was found that companies which integrate security into their strategic objectives recognise staff development needs earlier, plan training proactively, and build a skill base more systematically. Initial effects of the changes to the ZInfV-1 and NIS2 legal frameworks were also observed, particularly in the form of increased investment in training and collaboration with external providers. The paper provides an empirical basis for the development of systemic measures and supports strategic workforce planning for effective digital risk management in Slovenia.

Keywords: Competencies, workforce development, information security, cyber security, digital resilience, Slovenian economy

1 UVOD

Informacijska varnost (angl. information security) in kibernetska varnost (angl. cyber security) sta postali ključen dejavnik digitalne operativne odpornosti organizacij [1]. Čeprav se pojma v praksi pogosto (neupravičeno) uporabljata kot sinonima, med njima obstajajo pomembne razlike: informacijska varnost zajema zaščito vseh informacij, ne glede na obliko ali medij, kibernetska varnost pa kot njen ožji podsklop obsega predvsem varovanje digitalnih sistemov in omrežij ter s tem podatkov in informacij, ki se v njih obdelujejo. Hitro napredujoča digitalizacija poslovnih procesov, razpršena informacijsko-komunikacijska infrastruktura ter vse pogostejši napredni kibernetski napadi povečujejo tveganja in organizacije silijo v sistematičen pristop k varovanju informacijskih sredstev, kar obema področjema daje vse večjo težo. V ospredje zato stopa potreba po strokovnjakih, ki poleg tehničnih obvladujejo tudi organizacijske, pravne in komunikacijske vidike varnosti [2].

Na ravni Evropske unije sta kot odziv na zaznane primanjkljaje kompetenc na področju informacijske in kibernetske varnosti nastala dva ključna okvira: European e-Competence Framework (e-CF) in European Cybersecurity Skills Framework (ECSF). Prvi opredeljuje 41 IKT kompetenc, razporejenih v pet procesnih področij in pet stopenj zahtevnosti, drugi pa zajema 12 poklicnih profilov s področja kibernetske varnosti z natančno določenimi znanji, spretnostmi in odgovornostmi [3, 4]. Kljub temu se zdi, da številne organizacije nimajo pregleda nad ključnimi kompetencami, ki jih potrebujejo, niti ne izvajajo sistematičnih pristopov k njihovemu razvoju [5].

Podatki SI-CERT-a kažejo, da se v praksi kibernetske grožnje še vedno pogosto kažejo v obliki ciljnih napadov na uporabnike, pri čemer so napadi vse bolj izpopolnjeni, odzivni časi pa pogosto nezadostni [6]. V takšnem okolju postaja ključno, da organizacije krepijo svojo notranjo odpornost ne le z vlaganjem v tehnologijo, temveč tudi s kadrovskimi ukrepi [7].

Poleg tega v letošnjem letu sprejeti Zakon o informacijski varnosti (ZInfV-1) in evropska direktiva Network and information systems directive (NIS2) uvajata obveznosti za zavezance glede zagotavljanja ustreznih varnostnih ukrepov, postopkov obvladovanja tveganj in usposobljenosti osebja [8, 9]. Nova zakonodaja tako vpliva na organizacijsko strukturo, opredeljevanje vlog ter strateško umeščanje informacijske/kibernetske varnosti na strateško raven. Po drugi strani pa analize opozarjajo na praktične izzive, ki spremljajo implementacijo zakonodaje in zajemajo dejavnike od nejasnosti glede izvedbe in obsega zahtev, pri čemer se pomanjkanje usposobljenega kadra izpostavlja kot pomemben dejavnik [10, 11]. Ob tem se vse bolj poudarja tudi potreba po razvoju celostnih kompetenc na področju informacijske/kibernetske varnosti, ki poleg tehničnih znanj vključujejo tudi mehke veščine, razumevanje poslovnega konteksta, upravljanje tveganj in skladnost z zakonodajo [12, 13]. Raziskave kažejo tudi, da organizacije pogosto investirajo v tehnologijo, a zanemarjajo vlaganje v človeški kapital, ki je ključen za učinkovito delovanje varnostnih mehanizmov [14, 15].

Kljub številnim evropskim pobudam, kot so ECSF, e-CF in strategije ENISA, se zdi, da problematika zagotavljanja kompetentnih kadrov na področju informacijske/kibernetske varnosti ostaja pereč problem tako v Evropi kot širše. Najnovejša študija organizacije ISC2 opozarja, da v Evropi primanjkuje več kot 390.000 strokovnjakov s področja kibernetske varnosti, globalno pa več kot štiri milijone, pri čemer se vrzel ne zmanjšuje temveč celo povečuje [16]. Kot poročajo strokovni krogi, Slovenija pri tem ni nobena izjema [17, 18]. Avtorji opozarjajo na razmeroma nizko zanimanje mladih za poklicne poti v tej panogi in posledično na pomanjkanje ustrezno usposobljenih kadrov na trgu dela [19]. Kljub zaznanemu problemu pa na podlagi pregleda literature in dostopnih virov nismo zasledili nobene celovite raziskave, ki bi sistematično prikazala dejansko stanje na ravni slovenskih organizacij. S pričujočim prispevkom želimo to raziskovalno vrzel zapolniti.

V prispevku predstavljamo del rezultatov empirične raziskave, ki je bila izvedena sredi leta 2025 na vzorcu slovenskih organizacij [20]. Namen raziskave je bil prepoznati tista znanja in kompetence s področja informacijske in kibernetske varnosti, ki jih slovenske organizacije prepoznavajo kot ključne, oceniti njihovo aktualno pokritost in identificirati glavne ovire pri nadaljnjem razvoju kadrovskega potenciala na tem področju. Poleg tega smo želeli celovito analizirati povezavo med zaznanimi kompetenčnimi vrzelmi, organizacijskimi ukrepi in vplivom zakonodaje na kadrovske strategije. Rezultati in ugotovitve prispevajo k razumevanju stanja na ravni slovenskega gospodarstva in prikazujejo smernice za sistemska priporočila v smeri krepitve nacionalne kibernetske odpornosti.

2 METODOLOGIJA

2.1 Ozadje problema

Potreba po usposobljenem kadru na področju informacijske in kibernetske varnosti se v zadnjih letih uveljavlja kot ena ključnih razvojnih prioritet organizacij. Strateška umeščenost informacijske/kibernetske varnosti v poslovne cilje ni le odraz zrelosti organizacij, temveč vpliva tudi na oblikovanje kadrovskih politik, postopkov in struktur. Raziskave kažejo, da organizacije, ki informacijsko/kibernetsko varnost obravnavajo kot sestavni del strateškega upravljanja, bistveno pogosteje izvajajo načrtovan razvoj kompetenc in zagotavljajo notranje procese za krepitev varnostne kulture [21, 22]. Pri tem se kompetenčne vrzeli ne kažejo le v tehničnem znanju, temveč v širšem neskladju med potrebami delodajalcev, ponudbo izobraževalnega sistema in dejansko razpoložljivostjo kadra na trgu dela [23, 24].

V zadnjem desetletju so se oblikovali tudi teoretični modeli, ki sistematizirajo kibernetske kompetence in poklicne vloge. Med najpomembnejšimi sta ECSF, ki ga je razvila agencija ENISA, in ameriški National Initiative for Cybersecurity Education (NICE) Framework, ki je standardiziran pod okriljem NIST [25, 26]. Oba okvirja poudarjata potrebo po strukturiranem povezovanju delovnih mest, znanj in spretnosti, kar omogoča boljšo primerljivost, razvoj kadrov in načrtovanje izobraževanj. ECSF posebej izpostavlja pomen strokovne specializacije, obenem pa prepoznava tudi mehke in organizacijske kompetence, kar je pogosto zapostavljeno v tradicionalnih pristopih k izobraževanju [27].

Raziskave v zadnjih letih vse bolj opozarjajo na pomen človeškega dejavnika v informacijski/kibernetski varnosti. Nezadostno zavedanje zaposlenih, pomanjkanje vodstvene podpore in odsotnost celovite kompetenčne strategije pogosto vodijo do neučinkovitosti tudi pri sicer tehnično ustrezno vzpostavljenih varnostnih sistemih [28, 29]. S tem postaja razumevanje organizacijske kulture, notranje komunikacije in vloge vodstva neločljiv del učinkovitega obvladovanja tveganj.

Pomemben segment teoretičnega okvira predstavlja tudi vpliv zakonodaje na oblikovanje kadrovskih ukrepov. Direktiva NIS2 in nedavno sprejeti ZInfV-1 namreč zavezancem nalagata obveznost zagotavljanja ne le tehničnih temveč tudi kadrovskih in organizacijskih ukrepov. Odgovornost za izvajanje teh ukrepov je pogosto porazdeljena med več deležnikov znotraj organizacije, kar zahteva jasno opredeljene vloge in trajno izobraževanje zaposlenih [30, 11]. Vendar izkušnje iz prakse kažejo, da implementacija zakonodaje pogosto naleti na omejitve. Številne organizacije nimajo zadostnih resursov za izvajanje potrebnih usposabljanj, pogosto pa se soočajo tudi s pomanjkanjem usmeritev in nejasnostmi glede zahtev za implementacijo kakor tudi z visokimi stroški, ki jih implementacija prinese [30, 16].

V tem kontekstu je preučevanje kompetenčnih potreb, ovir in vpliva zakonodaje na kadrovske politike ključno za razumevanje, kako lahko organizacije dolgoročno krepijo svojo kibernetsko odpornost. Raziskava tako temelji na presečišču sodobnih kompetenčnih modelov, strateškega upravljanja varnosti in regulativnih zahtev, ob upoštevanju značilnosti slovenskega institucionalnega in tržnega okolja.

2.2 Načrt in izvedba raziskave

Osnovni namen raziskave je preučiti kompetenčne potrebe slovenskih organizacij na področju informacijske/kibernetske varnosti, zaznane ovire pri razvoju kadrovskih virov ter vpliv aktualne zakonodaje na izvajanje kadrovskih ukrepov. Za potrebe raziskave je bil razvit namenski vprašalnik, ki pokrival različne tematske sklope, povezane s strateškim pristopom k varnosti, oceno pomembnosti in pokritosti znanj in kompetenc, zaznanimi ovirami ter vplivom zakonodaje. Celoten vprašalnik je dostopen v [20]. Ciljna populacija so bile slovenske organizacije, ki se na kakršenkoli način srečujejo z informacijsko/kibernetsko varnostjo, pri čemer je bile k izpolnjevanju ankete povabljene predvsem osebe, odgovorne za informacijsko/kibernetsko varnost, kadrovski razvoj ali strateško upravljanje. Tak izbor je omogočil pridobivanje podatkov z visoko vsebinsko relevantnostjo in zajem različnih vidikov obravnavanega problema.

V sklopu raziskave smo želeli odgovoriti na več raziskovalnih vprašanj, pri čemer se v pričujočem članku osredotočamo na naslednja raziskovalna vprašanja:

RV1: Ali lahko trdimo, da je splošno stanje na področju zagotavljanja kompetentnega kadra za informacijsko/kibernetsko varnost v Sloveniji ocenjeno kot slabo?

RV2: Ali lahko trdimo, da se večina slovenskih organizacij sooča s pomanjkanjem ustrezno usposob-

ljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti?

RV3: Ali obstajajo statistično značilne razlike v zaznavanju pomanjkanja ustrezno usposobljenega in kompetentnega kadra glede na lastništvo organizacije (javno, zasebno, mešano)?

RV4: Ali organizacije, ki informacijsko/kibernetsko varnost obravnavajo kot strateško prioriteto, v večji meri zaznavajo pomanjkanje ustrezno usposobljenega in kompetentnega kadra na tem področju?

RV5: Katere ovire zaznavajo slovenske organizacije kot najbolj kritične pri razvoju kompetenc na področju informacijske/kibernetske varnosti?

RV6: Ali zavezanost organizacije zakonodajnem okviru ZInfV-1 in NIS2 vpliva na izvajanje dodatnih kadrovskih ukrepov na področju informacijske/kibernetske varnosti?

Raziskava je bila izvedena v maju in juniju 2025 preko orodja za spletno anketiranje 1KA (https://www.1ka.si/). Podatki so bili analizirani s programom IBM SPSS Statistics in Microsoft Excel.

3 REZULTATI

V nadaljevanju najprej predstavimo osnovne značilnosti vzorca sodelujočih organizacij, temu pa sledijo rezultati analize posameznih raziskovalnih vprašanj.

3.1 Predstavitev vzorca

Anketni vprašalnik je v celoti izpolnilo 235 organizacij iz različnih sektorjev slovenskega gospodarstva. Ključne lastnosti vzorca sodelujočih organizacij so strnjene v tabeli 1.

Razvidno je, da so v raziskavi sodelovale organizacije vseh velikostnih razredov, pri čemer prevladujejo velike, večinoma zasebne organizacije iz osrednjeslovenske regije. Dejavnost organizacij je raznolika. Največji delež predstavljajo organizacije iz sektorja informacijskih in komunikacijskih dejavnosti, sledijo jim organizacije iz finančnega sektorja, javne uprave, izobraževanja ter strokovnih in tehničnih storitev. Na 5-stopneski lestvici je bila ocenjena stopnja digitalizacije procesov v organizacijah večinoma srednja do visoka (M=3,4; SD=0,9), kar nakazuje na razmeroma visoko tehnološko zrelost sodelujočih organizacij. Glede statusa po zakonodaji ZInfV-1 in NIS2 se je približno polovica sodelujočih opredelila kot pomembni ali bistveni (skupaj 46 %) subjekt, medtem ko 27 % organizacij ni zavezancev. Prav tolikšen delež (27 %) pa se glede tega vprašanja ni znalo jasno opredeliti.

Tabela 1: **Struktura vzorca sodelujočih organizacij (n=235)**

Značilnost organizacije	Kategorija	Št. odgovorov (n)	Delež (%)
velikost	mikro (do 10 zaposlenih)	42	18
	mala (do 50 zaposlenih)	51	22
	srednja (do 250 zaposlenih)	55	23
	velika (nad 250 zaposlenih)	87	37
vrsta lastništva / financiranja	javno	73	31
	zasebno	125	53
	mešano	37	16
regija sedeža	Osrednjeslovenska	119	51
	Gorenjska	49	21
	ostale regije	67	28
glavna dejavnost po SKD	informacijske in komunikacijske dejavnosti	69	29
	finančne in zavarovalniške dejavnosti	18	8
	dejavnost javne uprave, obrambe, izobraževanja, zdravstva ipd.	59	25
	ostale dejavnosti	89	38
stopnja digitalizacije procesov	zelo nizka/nizka (1–2)	27	11
	srednja (3)	101	43
	visoka/zelo visoka (4–5)	107	46
status po ZInfV-1/NIS2	ni zavezanec	64	27
	pomembni subjekt	58	25
	bistveni subjekt	49	21
	ne vem	64	27

3.2 Ocena splošnega stanja na področju zagotavljanja kompetentnega kadra za informacijsko/kibernetsko varnost v Sloveniji

Organizacije, ki so v raziskavi sodelovale, so splošno stanje na področju zagotavljanja kompetentnega kadra za informacijsko/kibernetsko varnost v Sloveniji ocenjevale na lestvici od 1 do 5, pri čemer je 1 pomenilo »zelo slabo«, 5 pa »zelo dobro«. Povprečna ocena je bila 2,74 (*SD*=0,84), porazdelitev odgovorov pa je prikazana na sliki 1.

Da bi odgovorili na RV1, smo izvedli enostranski *t*-test, s katerim smo želeli preveriti, če je povprečna ocena splošnega stanja na področju zagotavljanja kompetentnega kadra za informacijsko/kibernetsko varnost v Sloveniji statistično značilno nižja od sredinske vrednosti 3 na ocenjevalni lestvici. Rezultati testa, predstavljeni v tabeli 2, so slednje potrdili ($t(234)=4{,}69$, $p<0{,}001$). Trditi torej smemo, da je povprečna ocena splošnega stanja na področju zagotavljanja kompetentnega kadra za informacijsko/kibernetsko varnost v Sloveniji statistično značilno nižja od sredinske vrednosti na ocenjevalni lestvici. Velikost učinka, izražena s Cohenovim *d* (–0,31), kaže na majhen do srednje majhen učinek, kar pomeni, da je razlika med ocenjenim stanjem in sredinsko vrednostjo sicer zanesljiva, a v praktičnem smislu zmerno izrazita. Na raziskovalno vprašanje RV1 tako lahko odgovorimo pritrdilno.

Tabela 2: **Rezultati t-testa za potrebe analize RV1**

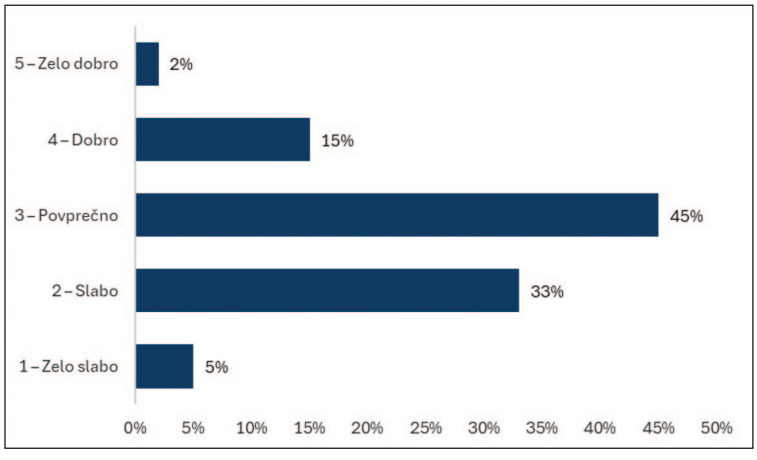
M	*SD*	*t*	*df*	*p*	Cohenov *d*
2,74	0,83	–4,694	234	<0,001	–0,306

Takšna ocena ni nepričakovana. Izkušnje iz prakse kažejo, da se organizacije že več let soočajo z izzivi pri zaposlovanju kadra, zlasti na področjih, ki zahtevajo specifična tehnična znanja, razumevanje regulatornega okvira (npr. ZInfV-1, NIS2) in sposobnost delovanja v visoko dinamičnem okolju. Razkorak med pričakovanji delodajalcev in dejansko razpoložljivostjo kadra se kaže ne le v številu razpoložljivih kandidatov temveč tudi v kakovosti njihovih znanj, kompetenc in izkušenj.

Zato nizka povprečna ocena ne odraža zgolj trenutnega stanja, temveč predstavlja jasno opozorilo o potrebi po dolgoročnem in usklajenem sistemskem ukrepanju. Ključno postaja vprašanje, ali trenutni izobraževalni sistem in obstoječe pobude za razvoj kadrov zmorejo ustrezno odgovoriti na identificirane potrebe. Rešitev ne tiči v kratkoročnih projektih ali posamičnih iniciativah, temveč v celoviti strategiji, ki vključuje:

- usklajevanje izobraževalnih programov s potrebami trga dela,
- stalno strokovno izpopolnjevanje na področju informacijske in kibernetske varnosti,
- razvoj nacionalnih standardov znanj in certifikacij,
- ter intenzivnejše povezovanje med gospodarstvom, državo in akademsko sfero.

V razmerah, kjer regulativni pritiski naraščajo, kibernetska odpornost pa postaja ključna za poslovno kontinuiteto, to vprašanje ni več zgolj razvojna prioriteta temveč osnovni pogoj za dolgoročno preživetje na trgu.



Slika 1: **Porazdelitev ocen o splošnem stanju zagotavljanja kadra za informacijsko/kibernetsko varnost v Sloveniji (n = 235).**

Ugotovitve o nizki zaznani razpoložljivosti strokovnjakov za kibernetsko varnost imajo neposredne implikacije za kadrovske in strateške politike slovenskih organizacij. Vodstva bi morale to zaznavo razumeti kot poziv k proaktivnemu upravljanju s talenti, intenzivnejšemu razvoju notranjih usposabljanj ter oblikovanju partnerstev z izobraževalnimi ustanovami. V pogojih omejene ponudbe se bodo konkurenčne prednosti gradile tudi na sposobnosti organizacij, da same razvijajo potrebne kompetence in ustvarjajo okolje, ki spodbuja zadrževanje ključnega kadra.

3.3 Soočanje s pomanjkanjem ustrezno usposobljenega in kompetentnega kadra v organizacijah

Za potrebe analize RV2 smo uporabili naslednje vprašanje iz anketnega vprašalnika: *»Ali v vaši organizaciji zaznavate pomanjkanje ustrezno usposobljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti?«*. Porazdelitev odgovorov ponazarja slika 2, iz katere je razvidno, da večina organizacij zaznava vsaj delno pomanjkanje kadra (ocena 2 ali 3).

Razvidno je, da je vzorčni delež organizacij, ki so na naše vprašanje odgovorili z oceno vsaj 2, kar 70,6 %. Da bi dobili celovit odgovor na RV2, smo izvedli binomski test deleža, kjer smo kot testno vrednost izbrali 0,5. Rezultati, podani v tabeli 3, nakazujejo, da je rezultat testa statistično značilen, saj je $p<0{,}001$. Na podlagi tega torej lahko trdimo, da večina slovenskih organizaciji (več kot 50 % le-teh) zaznava pomanjkanje ustrezno usposobljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti, kar pomeni, da na RV2 lahko odgovorimo pritrdilno.

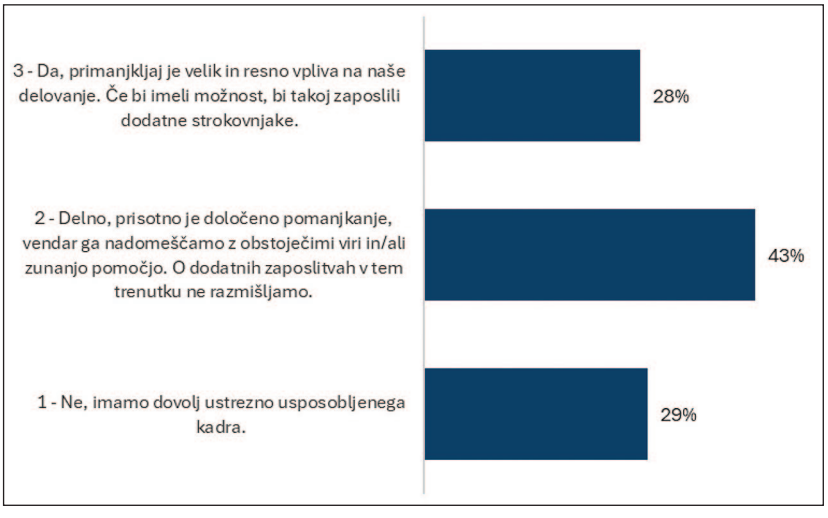
Tabela 3: **Rezultati binomskega testa za potrebe analize RV2**

Skupina	Št. odgovorov	Delež (%)	Testna vrednost	*p*
zaznavajo pomanjkanje (vsaj delno)	166	70,6	0,5	<0,001
ne zaznavajo pomanjkanja	69	29,4		

Ugotovitev, da je zaznavanje pomanjkanja splošna značilnost slovenskega organizacijskega prostora, je skladna z evropskimi analizami, kot je npr. ECSF [4], ki opozarjajo, da gre za strukturni in ne zgolj začasni primanjkljaj.

Z vidika kadrovske politike rezultati jasno nakazujejo, da posamezne organizacije same ne bodo mogle preseči vrzeli med potrebami in ponudbo. Potrebni so usklajeni sistemski ukrepi, ki vključujejo sodelovanje izobraževalnega sistema, državnih organov in gospodarstva. Dolgoročna kadrovska strategija mora obsegati usmerjeno krepitev strokovnih kompetenc, večjo prepoznavnost kibernetskih poklicev med mladimi ter prilagajanje izobraževalnih programov dejanskim potrebam trga.

Ker zaznano pomanjkanje presega posamezne sektorje in tipe organizacij, predstavlja le-to horizontalen problem slovenskega gospodarstva. To razu-



Slika 2: **Porazdelitev odgovorov na vprašanje »Ali v vaši organizaciji zaznavate pomanjkanje ustrezno usposobljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti?« (n = 235).**

mevanje mora postati izhodišče za oblikovanje ukrepov, ki bodo omogočili stabilno in dolgoročno vzdržno kompetenčno osnovo za kibernetsko varnost.

3.4 Razlike v zaznavanju pomanjkanja ustrezno usposobljenega in kompetentnega kadra glede na lastništvo organizacije

V sklopu RV3 smo nadalje želeli ugotoviti, ali se povprečna ocena zaznave pomanjkanja ustrezno usposobljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti razlikuje glede na tip lastništva organizacije (javno, zasebno, mešano). Za analizo smo uporabili isto vprašanje iz anketnega vprašalnika kot pri analizi RV2 v prejšnjem poglavju.

Opisne statistike (tabela 4) kažejo, da so javne organizacije v povprečju višje ocenile zaznano pomanjkanje kadra (M=2,45; SD=0,75) kot zasebne (M=1,79; SD=0,69) in mešane (M=1,73; SD=0,61) organizacije. Tudi 95 % intervali zaupanja nakazujejo, da so razlike med javnimi organizacijami in ostalimi tipi organizacij precej izrazite.

Tabela 4: **Opisne statistike za oceno zaznavanja pomanjkanja kadra glede na lastništvo organizacije (n = 235).**

Lastništvo organizacije	*n*	*M*	*SD*	95% interval zaupanja
javna	73	2,45	0,75	2,28 – 2,63
zasebna	125	1,79	0,69	1,67 – 1,91
mešana	37	1,73	0,61	1,53 – 1,93
skupaj	**235**	**1,99**	**0,76**	**1,89 – 2,08**

Da bi preverili, če so zaznane razlike med skupinami statistično značilne, smo uporabili enosmerno analizo variance (ANOVA). Pred izvedbo ANOVE smo preverili predpostavko homogenosti varianc s pomočjo Levenovega testa homogenosti varianc. Rezultati testa homogenosti varianc (F(2,232)=2,467, p=0,087>0,05) so pokazali, da ničelne domneve o enakosti varianc ne moremo zavrniti pri 5% tveganju, kar pomeni, da lahko nadaljujemo z interpretacijo tabele ANOVA (tabela 5).

Tabela 5: **Rezultati enosmerne analize variance ANOVA za potrebe analize RV3**

	Vsota kvadratov	*df*	Povprečni kvadrat	*F*	*p*	η^2
med skupinami	22,990	2	11,495	23,82	<0,001	0,17
znotraj skupin	111,971	232	0,483			
skupaj	**134,962**	**234**				

Rezulati analize ANOVA potrdjujo, da so razlike v povprečnih ocenah zaznavanja pomanjkanja kadra v proučevanih organizacijah statistično značilne, saj je p<0,001. Vrednost koeficienta η^2=0,17 kaže na srednje velik učinek, kar pomeni, da lastništvo organizacije razmeroma močno vpliva na zaznavanje kadrovskega pomanjkanja. Na podlagi teh rezultatov na RV3 lahko odgovorimo pritrdilno.

Rezultati torej dokazujejo, da je pomanjkanje usposobljenega kadra najbolj izrazito v javnem sektorju, kar lahko odraža omejitve v fleksibilnosti zaposlovanja, dolgotrajne postopke in manj konkurenčne plače v primerjavi z zasebnim sektorjem.

Ugotovitve tako odpirajo pomembna strateška vprašanja. Če lastniška struktura organizacije pomembno vpliva na zaznavanje razpoložljivosti kadrov, potem je treba pri oblikovanju ukrepov za reševanje kadrovske vrzeli upoštevati heterogenost organizacijskega okolja. Sistemski ukrepi naj bodo diferencirani glede na tip organizacije in naj vključujejo podporne mehanizme za tiste, ki imajo pri dostopu do kadrov večje omejitve. Le tako bo mogoče ustvariti pravične in učinkovite pogoje za dolgoročno kadrovsko vzdržnost slovenskega digitalnega prostora.

3.5 Povezanost strateškega pristopa k informacijski/kibernetski varnosti in zaznavanja pomanjkanja ustreznega kadra na tem področju

RV4 temelji na predpostavki, da organizacije, ki informacijsko/kibernetsko varnost razumejo kot strateško prioriteto, bolje razumejo potrebe po zagotavljanju kompetentnega kadra, so na tem področju bolj proaktivne in posledično v večji meri zaznavajo pomanjkanje ustreznega in kompetentnega kadra.

Da bi naše predvidevanja preverili, smo izvedli analizo, ki je temeljila na preseku dveh dimenzij: (1) oceni, v kolikšni meri vodstvo organizacije obravna-

va varnost kot strateško pomembno temo, ter (2) stopnji zaznanega pomanjkanja usposobljenega kadra s področja informacijske/kibernetske varnosti. Za preverjanje povezanosti med spremenljivkama smo uporabili hi-kvadrat (χ^2) test.

Kot je povedano že v poglavju 3.2, so anketirani na vprašanje, če v organizaciji zaznavajo pomanjkanje ustrezno usposobljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti, odgovarjali na 3 - stopenjski lestvici (1 – ne, 2 - delno, 3 - da). Na vprašanje, če vodstvo njihove organizacije obravnava informacijsko/kibernetsko varnost kot strateško pomembno področje, pa so anketiranci odgovarjali na 5 stopenjski lestvici:

1. Ne, informacijska/kibernetska varnost nista obravnavani kot strateška tema.
2. Deloma, o informacijski/kibernetski varnosti se pri nas občasno razpravlja, a področji nista vključeni v strateške dokumente.
3. Zmerno, informacijska/kibernetska varnost ima nekaj strateške teže, vendar (še) ni integrirana v širše poslovne cilje organizacije.
4. V veliki meri, vodstvo priznava pomen informacijske/kibernetske varnosti in ju vključuje v strateške razprave.
5. V celoti, informacijska/kibernetska varnost je jasno prepoznana kot strateška prioriteta in redno vključena v odločanje na najvišji ravni.

Kontingenčno tabelo kakor tudi rezultate χ^2 testa prikazuje tabela 6. Razvidno je, da organizacije, ki v celoti (kategorija 5) razumejo informacijsko/kibernetsko varnost kot strateško prioriteto, v polovici primerov (50,0 %) poročajo o vsaj delnem pomanjkanju kadra, medtem ko jih 50,0 % meni, da pomanjkanja ni. Pri organizacijah, ki varnost obravnavajo v veliki meri (kategorija 4), je delež organizacij z vsaj delnim pomanjkanjem nekoliko višji (52,0 %). Organizacije, ki varnost obravnavajo zmerno ali manj, pogosteje poročajo, da pomanjkanja ni ali da je le delno prisotno. Najmanj zaznanega pomanjkanja je pri organizacijah, ki varnosti ne obravnavajo strateško (kategorija 1). Rezultati χ^2 testa nadalje kažejo na statistično značilno povezanost med proučevanima veličinama ($\chi^2 = 59, 417$; $df = 8$; $p < 0{,}001$). Za oceno moči povezanosti smo izračunali še Cramérjev V, ki je enak 0,36. Ta vrednost kaže na zmerno močno povezavo med izbranima spremenljivkama.

Tabela 6: **Kontingenčna tabela in rezultati χ^2-testa za potrebe analize RV4**

		Zaznavanje pomanjkanja ustrezno usposobljenega in kompetentnega kadra s področja informacijske/kibernetske varnosti			
		1 – ne	2 – delno	3 – da	skupaj
Strateški pristop k informacijski/ kibernetski varnosti	1 – ne	7	10	1	18
	2 – deloma	4	8	14	26
	3 – zmerno	2	17	27	46
	4 – v veliki meri	21	36	18	75
	5 – v celoti	35	29	6	70
	skupaj	69	100	66	235

Rezultati χ^2-testa: $\chi^2 = 59{,}417$; $df = 8$; $p < 0{,}001$

Povzamemo torej lahko, da strateški pristop organizacij k informacijski/kibernetski varnosti vpliva na njihovo zaznavanje kadrovskih vrzeli. Bolj kot je varnost razumljena kot strateška prioriteta, večja je verjetnost, da organizacije zaznajo vsaj delno pomanjkanje ustrezno usposobljenega kadra. Ugotovitve torej kažejo, da je strateški odnos do informacijske/kibernetske varnosti več kot zgolj izraz zrelosti organizacijskega upravljanja, gre tudi za pomemben dejavnik pri oblikovanju in ohranjanju notranjih kadrovskih zmogljivosti. Organizacije, ki varnost integrirajo v strateške cilje, prej prepoznajo potrebe po kadrovskem razvoju, proaktivno načrtujejo izobraževanja ter bolj sistematično gradijo kompetenčne baze. Po drugi strani organizacije z manj razvitim strateškim pristopom tega pomanjkanja bodisi ne zaznavajo bodisi ga zaznavajo le delno, morda zaradi manjše osredotočenosti na kadrovske vidike varnosti. Tudi na RV4 torej lahko odgovorimo pritrdilno.

Naše ugotovitve imajo pomembne implikacije za slovenski kontekst, kjer večina organizacij deluje v okoljih z omejenimi viri in pomanjkanjem specializiranega kadra. Rezultati nakazujejo, da je eden izmed načinov za ublažitev kadrovske vrzeli ravno v tem, da se varnost ne obravnava zgolj kot tehnična naloga, temveč kot integralni del organizacijske strategije.

3.6 Ključne ovire pri razvoju kompetenc na področju informacijske in kibernetske varnosti

V sklopu analize RV5 smo želeli proučiti, katere zaviralne dejavnike organizacije zaznavajo kot najbolj problematične pri zagotavljanju, usposabljanju in ohranjanju kompetentnega kadra. Anketirancem smo ponudili 8 možnih odgovorov, pri čemer so anketiranci lahko izbrali največ 3 možnosti.

Rezultati deskriptivne analize odgovorov so prikazani v tabeli 7 in kažejo, da organizacije najpogosteje prepoznavajo naslednje tri ovire:

- pomanjkanje ustrezno usposobljenega kadra na trgu dela (64,4 % primerov),
- pomanjkanje sredstev za kadrovanje ali najem zunanjih strokovnjakov (50,6 %),
- velika fluktuacija in težave pri zadrževanju kadrov (47,8 %).

Manj pogosto so bile izpostavljene ovire, kot so nezadostna ponudba ali visoka cena izobraževanj ter nizka ozaveščenost vodstva.

Da bi bolje razumeli medsebojne povezave med ovirami, je bila izvedena faktorska analiza (metoda glavnih komponent z Varimax rotacijo), ki je potrdila prisotnost štirih latentnih dimenzij:

- **Faktor 1:** Organizacijska podpora in kultura, ki vključuje ovire, kot sta pomanjkanje načrtnega razvoja kompetenc znotraj organizacije in nizka ozaveščenost vodstva o pomenu kibernetske varnosti.
- **Faktor 2:** Zunanji viri in stroški, kamor sodijo visoki stroški ali nezadostna ponudba zunanjih izobraževanj.
- **Faktor 3:** Nestabilnost kadra, ki zajema pomanjkanje strokovnega kadra na trgu dela in visoko fluktuacijo zaposlenih.
- **Faktor 4:** Šibka notranja motivacija, ki odraža predvsem nizko motivacijo zaposlenih za pridobivanje dodatnih znanj.

Kaiser-Meyer-Olkinov indikator je bil 0,388, kar opozarja na šibkejšo povezljivost spremenljivk, vendar je Bartlettov test sferičnosti bil statistično značilen ($\chi^2 = 127{,}14$; $df=28$; $p<0{,}001$), kar upravičuje izvedbo faktorske analize. Identificirani faktorji pojasnjujejo 66,5 % skupne variance. Celotni rezultati faktorske analize so podani v magistrski nalogi [20].

Ugotovitve potrjujejo, da so ovire pri razvoju kompetenc na področju informacijske/kibernetske varnosti večdimenzionalne in pogosto medsebojno prepletene. To pomeni, da se organizacije ne soočajo zgolj z enim tipom izzivov temveč s kombinacijo ekonomskih, organizacijskih in kulturnih dejavnikov. Takšen vpogled ponuja uporabno osnovo za oblikovanje ukrepov na ravni organizacij, sektorjev in državnih politik.

Tabela 7: **Zaznane ovire pri razvoju kompetenc na področju informacijske in kibernetske varnosti**

Ovire pri razvoju kompetenc na področju informacijske in kibernetske varnosti	Št. odgovorov (n)	Delež glede na vse odgovore (%)	Delež anketirancev, ki so izbrali to možnost (%)
pomanjkanje ustrezno usposobljenega kadra na trgu dela	116	25,8	64,4
pomanjkanje sredstev za kadrovanje ali najem zunanjih strokovnjakov	91	20,3	50,6
velika fluktuacija strokovnjakov, težave pri zadrževanju kompetentnih kadrov (npr. majhno podjetje, neatraktivna regija ipd.)	86	19,2	47,8
pomanjkanje motivacije zaposlenih za pridobivanje dodatnih znanj	48	10,7	26,7
pomanjkanje načrtnega pristopa k lastnemu razvoju kompetenc znotraj organizacije	48	10,7	26,7
predraga ponudba zunanjih izobraževanj	26	5,8	14,4
nizka ozaveščenost vodstva o pomenu kibernetske varnosti	20	4,5	11,1
nezadostna ponudba zunanjih izobraževanj	14	3,1	7,8
skupaj	**449**	**100**	**249,4***

Opomba: Ker je bilo možnih več odgovorov, skupni % primerov presega 100 % Posamezni anketiranec je lahko označil več različnih ovir, zato je vključen v izračun odstotkov pri več postavkah.

3.7 Vpliv regulative na dodatne kadrovske ukrepe na področju informacijske in kibernetske varnosti

Uvedba nacionalnega ZInfV-1 in evropske Direktive NIS2 predstavlja pomemben institucionalni okvir za dvig ravni informacijske/kibernetske varnosti v slovenskih organizacijah [32]. Oba predpisa določata obveznosti za tako imenovane »zavezance«, ki so glede na svojo vlogo v digitalni družbi dolžni izvajati konkretne tehnične, organizacijske in kadrovske ukrepe. V tem kontekstu zakonodaja ne deluje le kot normativna zahteva, temveč vse bolj kot dejanski dejavnik oblikovanja kadrovskih strategij.

V sklopu RV6 smo tako želeli preveriti, ali sta status zavezanca po ZInfV-1 ali NIS2 in izvajanje dodatnih kadrovskih ukrepov na področju informacijske/kibernetske varnosti povezani veličini. Primerjali smo organizacije, ki so se identificirale kot zavezanci po ZInfV-1/NIS2 (pomembni ali bistveni subjekti), z organizacijami, ki tega statusa nimajo.

Za preverjanje povezanosti med statusom zavezanca in potrebo po izvajanju dodatnih kadrovskih ukrepov smo uporabili χ^2 test povezanosti. Rezultati, prikazani v tabeli 8, kažejo, da se je statistično značilna povezanost (p=0,022<0,05) pokazala le pri povečani potrebi po dodatnih znanjih in usposabljanjih obstoječih zaposlenih. To pomeni, da organizacije, ki spadajo med zavezance po ZInfV-1/NIS2, pogosteje občutijo potrebo po izvajanju ciljno usmerjenih internih izobraževanj za izboljšanje kompetenc obstoječega kadra. Da bi ugotovili moč povezanosti, smo izračunali še Cramérjev V, ki je enak 0,22 in dokazuje šibko do zmerno povezanost. Pri vseh ostalih navedenih potencialnih kadrovskih ukrepih (širitev ekipe, uvedba novih vlog, zunanje partnerstvo in okrepljena vloga vodstva) statistično značilne povezanosti nismo mogli potrditi. Na podlagi teh rezultatov lahko na RV6 odgovorimo le delno pritrdilno.

Za opažene vzorce obstajata vsaj dve razlagi. Prva je časovna komponenta: številne organizacije se zakonodaji šele prilagajajo in so še v začetni fazi uvajanja morebitnih dodatnih kadrovskih ukrepov. Druga razlaga je raznolikost v stopnji notranje zrelosti in upravljavske sposobnosti med organizacijami, kar vpliva na to, katere ukrepe so posamezne sposobne implementirati in katere ne.

Na tej osnovi lahko sklepamo, da zakonodaja v prvi fazi predvsem spodbuja kadrovske ukrepe, ki ne zahtevajo večjih sprememb organizacijske strukture, kot so dodatna interna usposabljanja. Vprašanje pa ostaja, ali bo zakonodajni pritisk dolgoročno spodbudil tudi širše organizacijske spremembe, kot so ustvarjanje novih varnostnih funkcij, sistematično načrtovanje kadrovskega razvoja in okrepljeno sodelovanje z zunanjimi strokovnjaki.

Z vidika oblikovanja politik to pomeni, da bi morala implementacija ZInfV-1 in NIS2 poleg nadzora nad skladnostjo vključevati tudi mehke ukrepe, kot so podpora vodstvom, svetovanje o kadrovski krepitvi ter usmerjanje organizacij v dolgoročno gradnjo internih zmogljivosti. Ob pričakovanem povečanju števila zavezancev bo ključno zagotoviti, da zakonodaja ne ostane zgolj formalna obveznost, temveč tudi vzvod za strateško upravljanje z znanji in kadri.

4 DISKUSIJA

Rezultati raziskave kažejo, da slovenske organizacije zaznavajo pomanjkanje kompetentnega kadra na področju informacijske/kibernetske varnosti kot resno in sistemsko oviro za dolgoročno digitalno odpornost. Povprečna ocena razpoložljivosti kadrov (2,74 na lestvici od 1 do 5) potrjuje ujemanje s svetovnimi trendi, kot jih navaja poročilo organizacije ISC² za leto 2024, kjer globalni primanjkljaj presega 4 milijone strokovnjakov [16]. Tudi Svetovni gospodarski forum (WEF) opozarja, da je pomanjkanje ustreznih

Tabela 8: **Rezultati χ^2 testa v sklopu analize RV6**

Potencialni dodatni kadrovski ukrep zaradi implementacije ZInfV-1 / NIS2	**Pearsonov χ^2 (df = 1)**	***p***	**Statistična značilnost**
Povečala se je potreba po dodatnem strokovnem kadru.	0,837	0,360	ne
Povečala se je potreba po dodatnih znanjih in usposabljanjih obstoječih zaposlenih.	**5,250**	**0,022**	**da**
Uvedli smo nove funkcije ali vloge (npr. CISO ipd.).	0,402	0,526	ne
Pogosteje sodelujemo z zunanjimi izvajalci.	0,402	0,526	ne
Okrepljena je bila vloga vodstva pri upravljanju informacijske/kibernetske varnosti.	0,007	0,935	ne

kadrov ena ključnih groženj kibernetski odpornosti na svetovni ravni [33]. Rezultati raziskave so pokazali, da pomanjkanje kadra bolj pesti javne organizacije kot pa zasebne ali mešane.

Poseben pomen ima ugotovitev, da organizacije, ki informacijsko/kibernetsko varnost obravnavajo kot strateško prioriteto, statistično značilno pogosteje zaznavajo pomanjkanje ustrezno usposobljenega in kompetentnega kadra, nakazuje na višjo stopnjo ozaveščenosti teh organizacij glede zahtev, ki jih postavlja učinkovito zagotavljanje varnosti. Takšne organizacije imajo praviloma bolje razvite procese, standarde in varnostne politike, zato tudi hitreje prepoznajo vrzeli v kadrovskih kompetencah. To pomeni, da je zaznavanje pomanjkanja kadra lahko tudi posledica višjih standardov in ambicij, ne zgolj objektivnega primanjkljaja, kar je pomembno upoštevati pri oblikovanju kadrovskih strategij in izobraževalnih programov. Slednje ugotovitve so povsem v skladu z izsledki v literaturi [21, 22].

Večdimenzionalna analiza ovir pri razvoju kompetenc na področju informacijske/kibernetske varnosti, ki vključuje tako strukturne kot organizacijske in sistemske dejavnike, potrjuje ugotovitve ENISA, ISACA in OECD, da se kompetenčne vrzeli ne pojavljajo le zaradi tržnega neravnotežja, temveč tudi zaradi pomanjkljive podpore vodstva, šibkih kadrovskih strategij ter slabe dostopnosti usposabljanj [23, 24, 34]. Rezultati faktorske analize so potrdili, da ovire nastopajo sočasno in v medsebojni odvisnosti, kar pomeni, da morajo biti rešitve prilagojene konkretnim tipom organizacij in sektorjem.

Analiza vpliva zakonodaje (ZInfV-1 in NIS2) na dodatne kadrovske ukrepe kaže, da je zakonodaja pomemben spodbujevalec, vendar trenutno vpliva predvsem na dodatna usposabljanja ne pa še na širše kadrovske premike. To je lahko posledica zgodnje faze implementacije, pomanjkanja institucionalne podpore ali dejstva, da številne organizacije še ne razpolagajo z notranjimi kapacitetami za prilagoditve. Primerjalne študije iz držav EU (npr. Finska, Nizozemska) kažejo, da so sistemski premiki mogoči predvsem tam, kjer zakonodajne zahteve spremljajo tudi spodbudne politike, javno sofinancirani programi in jasni kazalniki spremljanja učinkov [34, 35].

Menimo, da rezultati te raziskave predstavljajo dobro empirično podlago za oblikovanje nacionalnega kompetenčnega okvira, skladnega z ECSF, ki bi moral vključevati:

- razvoj standardov znanj in certifikatov na nacionalni ravni,
- oblikovanje spodbud za delodajalce v najbolj prizadetih sektorjih (npr. davčne olajšave za certificirana usposabljanja),
- vzpostavitev javno sofinanciranih programov kibernetskega izpopolnjevanja,
- vključitev kazalnikov kompetenčne razvitosti v nacionalne strategije (npr. Digitalna Slovenija, Nacionalni program kibernetske varnosti),
- boljše usklajevanje med akademsko sfero, gospodarstvom in državnimi organi (npr. preko javno-zasebnih partnerstev ali strateških svetov za kibernetsko odpornost).

Prav tako se odpira prostor za oblikovanje nacionalne podatkovne zbirke o stanju kadrovskih kapacitet na področju informacijske/kibernetske varnosti, ki bi omogočala redno spremljanje razkoraka med potrebami trga, izobraževalno ponudbo in dejansko zaposlenimi. Podoben pristop že razvijajo v nekaterih državah, kjer se kadrovski trendi spremljajo na podlagi centralnih kazalnikov in letnih poročil, kot na primer v okviru ameriške pobude Cybersecurity Workforce Data Initiative [36]. Takšna zbirka bi lahko služila kot podlaga za nadgradnjo obstoječih nacionalnih prizadevanj, saj so bile tudi v Sloveniji v zadnjih letih izvedene nekatere pomembne aktivnosti na področju kibernetske varnosti. Urad Republike Slovenije za informacijsko varnost (URSIV) je izdal *Priročnik kibernetske varnosti* [32], ki služi kot praktično vodilo za organizacije. Nacionalni odzivni center SI-CERT redno pripravlja letna poročila o incidentih [6], ki nudijo vpogled v aktualne grožnje in odzive. Državni svet RS je v svojih priporočilih [17] izpostavil potrebo po prilagoditvi izobraževalnega sistema realnim potrebam trga dela, medtem ko strateški dokument *Digitalna Slovenija 2030* opredeljuje krepitev kibernetske odpornosti kot eno od nacionalnih prioritet. Čeprav so ti ukrepi pomembni, ostajajo razpršeni in delno nepovezani, zato je oblikovanje enotnega nacionalnega kompetenčnega okvira še vedno nujno.

Za nadaljnje raziskave bi bilo smiselno izvesti longitudinalne študije, ki bi spremljale učinke zakonodaje in ukrepov skozi čas, ter razviti napovedne modele za potrebe po kompetencah, denimo s pomočjo simulacijskih tehnik, kot je sistemska dinamika. Tovrstni modeli bi omogočili tudi boljše strateško planiranje vlaganj in ciljno oblikovanje programov usposabljanja.

Raziskava ima nekaj omejitev, ki jih je treba upoštevati pri interpretaciji rezultatov. Vzorec, pridobljen prek strokovnih omrežij in partnerskih institucij, morda ni povsem reprezentativen za celotno populacijo slovenskih organizacij. Podatki temeljijo na samooceni, kar lahko vključuje subjektivne pristranskosti. Poleg tega so ugotovitve vezane na slovenski kontekst in časovno obdobje pred polno implementacijo zakonodajnih zahtev, kot je ZInfV-1 in NIS2, zato njihove pavšalne posplošitve na druge države ali kasnejša časovna obdobja niso povsem upravičene.

5 ZAKLJUČEK

Prispevek obravnava premalo raziskan a ključen vidik informacijske in kibernetske varnosti, kompetenčne vrzeli v slovenskih organizacijah. Rezultati empirične raziskave potrjujejo, da pomanjkanje usposobljenega kadra ni zgolj operativni problem posameznih organizacij, temveč odsev širših strateških, organizacijskih in sistemskih neravnovesij. Razkorak med potrebami trga, ponudbo izobraževalnega sistema in dejansko razpoložljivostjo kadra se kaže kot dolgoročna ovira za digitalno odpornost slovenskih organizacij.

Znanstveni doprinos članka je v konceptualni integraciji kompetenčnih potreb z regulativnim, organizacijskim in tržnim kontekstom. Na podlagi empiričnih podatkov članek ponuja večdimenzionalni vpogled v stanje kadrovskih kapacitet na področju informacijske/kibernetske varnosti v slovenskih organizacijah ter identificira ključne ovire in strateške razlike, ki vplivajo na zaznavo in obvladovanje kompetenčnih vrzeli. Ugotovitve potrjujejo, da so kompetenčne vrzeli v slovenskem prostoru večplastne, sistemsko pogojene in pogosto neodvisne od posameznih organizacij, zato zahtevajo usklajene odzive tako na ravni politike kot znotraj organizacij samih, vključno s sistematičnim načrtovanjem izobraževanja in usposabljanja na vseh ravneh.

Za oblikovalce politik rezultati predstavljajo pomembno podlago za razvoj nacionalnega kompetenčnega okvira, usklajenega z ECSF, ter pripravo sektorsko prilagojenih ukrepov tako od javno sofinanciranih programov usposabljanja do partnerstev med državo, gospodarstvom in akademskim okoljem. Nadaljnje raziskave naj se usmerijo v spremljanje dolgoročnih učinkov ukrepov, razvoj napovednih modelov ter sistemsko povezovanje empiričnih podatkov s strateškim načrtovanjem na državni ravni.

Trajnostna kibernetska odpornost bo v prihodnje mogoča le, če bo Slovenija svoje kompetenčne politike oblikovala na preverjenih podatkih o kadrovskih vrzelih, potrebah trga dela in učinkovitosti izobraževanj, ob jasnem sistemskem pristopu in dolgoročnem razvoju človeškega kapitala.

LITERATURA

[1] Uredba DORA – Digital Operational Resilience Act: regulativa za digitalno odpornost financ. (2025, 6. marec). iVarnost. https://ivarnost.si/dora-regulativa-za-digitalno-odpornost-financ/ (Dostopano dne: 6. avgust 2025)

[2] ENISA. (2023). Cybersecurity Threat Landscape 2023. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023 (Dostopano dne: 1. april 2025)

[3] CEN. (2024). European eCompetence Framework (eCF): An Introduction to the Standard and its Ecosystem (v2). https://www.researchgate.net/publication/375765291 (Dostopano dne: 1. april 2025)

[4] ENISA. (n.d.). European Cybersecurity Skills Framework (ECSF). https://www.enisa.europa.eu/topics/skills-and-competences/skills-development/european-cybersecurity-skills-framework-ecsf (Dostopano dne: 1. april 2025)

[5] Ruoslahti, H., Coburn, J., Trent, A., and Tikanmäki, I. (2021). "Cyber Skills Gaps – A Systematic Review of the Academic Literature", Connections: The Quarterly Journal, vol. 20, no. 2, pp. 33–45, 2021 https://doi.org/10.11610/Connections.20.2.02 (Dostopano dne: 1. april 2025)

[6] SI-CERT. (2025). Kibernetska varnost 2024 v številkah. https://www.cert.si/kibernetska-varnost-2024-v-stevilkah/ (Dostopano dne: 28. junij 2025)

[7] Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2021). Organizational science and cybersecurity: Abundant opportunities for research at the interface. Current Opinion in Psychology, 41, 80–85. https://doi.org/10.1016/j.copsyc.2021.04.005 (Dostopano dne: 13. junija 2025)

[8] Vlada RS. (2025). Zakon o informacijski varnosti (ZInfV-1). Uradni list RS, št. 40/2025. https://www.uradni-list.si/glasilo-uradni-list-rs/vsebina/2025-01-1571 (Dostopano dne: 20. junij 2025)

[9] Evropski parlament. (2023). Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji (NIS2). https://eur-lex.europa.eu/legal-content/SL/TXT/?uri=CELEX:32022L2555 (Dostopano dne: 20. junij 2025)

[10] Scholz, T., & Mayer, N. (2024). Towards a Research Agenda for the NIS2 Directive: Exploring Organisational and Compliance Challenges. arXiv preprint arXiv:2412.08084. https://arxiv.org/abs/2412.08084 (Dostopano dne: 11. junij 2025)

[11] Savin, A. (2024). NIS2 & Cybersecurity in Practice: Compliance Challenges. International In-house Counsel Journal, 17(69), 1–10. https://research.cbs.dk/en/publications/nis2-amp-cybersecurity-in-practice-compliance-challenges (Dostopano dne: 12. maj 2025)

[12] Ullah, F., Ye, X., Fatima, U., Akhtar, Z., Wu, Y., & Ahmad, H. (2025). What Skills Do Cyber Security Professionals Need? arXiv preprint arXiv:2502.13658. https://arxiv.org/abs/2502.13658 (Dostopano dne: 15. maj 2025)

[13] Kure, E., & Islam, N. (2022). Context-based and adaptive cybersecurity risk management framework. Risks, 11(6), 101.

https://www.mdpi.com/2227-9091/11/6/101 (Dostopano dne: 22. junij 2025)
[14] De Zan, T., & Di Franco, F. (2019). Cybersecurity skills development in the EU. ENISA – European Union Agency for Cybersecurity. https://millenniumedu.org/wp-content/uploads/2021/02/ENISA-Report-Cybersecurity-Skills-Development-in-the-EU.pdf (Dostopano dne: 22. junij 2025)
[15] OECD (2023), Building a Skilled Cyber Security Workforce in Five Countries: Insights from Australia, Canada, New Zealand, United Kingdom, and United States, OECD Skills Studies, OECD Publishing, Paris, https://doi.org/10.1787/5fd44e6c-en. (Dostopano dne: 22. junij 2025)
[16] ISC2. (2024). Cybersecurity Workforce Study 2024. https://edu.arrow.com/media/wtjfmszx/2024-isc2-wfs.pdf (Dostopano dne: 1. junij 2025)
[17] Državni svet RS. (2024). Kibernetska varnost zahteva odziven, realnim potrebam trga prilagojen izobraževalni sistem. Dostopno na: https://www.ds-rs.si/sl/novice/kibernetska-varnost-zahteva-odziven-realnim-potrebam-trga-prilagojen-izobrazevalni-sistem (Dostopano dne: 5. avgust 2025)
[18] BDO Global. (2024). Bridging the Cybersecurity Talent Gap: Augmenting human efforts with AI.https://www.bdo.si/getattachment/dc00d5b2-53ee-41a4-8013-6cdcc72e530e/Bridging-the-cybersecurity-talent-gap-TEDEN-4.pdf (Dostopano dne: 5. avgust 2025)
[19] Lesjak, D., Zwilling, M., & Klein, G. (2019). Cyber crime and cyber security awareness among students: A comparative study in Israel and Slovenia. Issues in Information Systems, 20(1), 80–87. https://doi.org/10.48009/1_iis_2019_80-87 https://iacis.org/iis/2019/1_iis_2019_80-87.pdf (Dostopano dne: 10. junij 2025)
[20] Markun, A., Kompetenčne potrebe slovenskih organizacij na področju kibernetske varnosti [magistrsko delo], Univerza v Mariboru, Fakulteta za organizacijske vede, 2025.
[21] Veale, M., & Brown, I. (2020). Cybersecurity. Internet Policy Review, 9(4). https://doi.org/10.14763/2020.4.1533 (Dostopano dne: 30. junij 2025)
[22] Uchendu, B., Nurse, J. R. C., Bada, M., & Furnell, S. (2021). Developing a cyber security culture: Current practices and future needs. arXiv preprint arXiv:2106.14701. https://arxiv.org/abs/2106.14701 (Dostopano dne: 1. julij 2025)
[23] Goupil, F., Laskov, P., Pekaric, I., Felderer, M., Dürr, A., & Thiesse, F. (2022). Towards understanding the skill gap in cybersecurity. Proceedings of ITiCSE '22. https://arxiv.org/abs/2204.13793 (Dostopano dne: 22. junij 2025)
[24] Ullah, F., Ye, X., Fatima, U., Akhtar, Z., Wu, Y., & Ahmad, H. (2025). What skills do cybersecurity professionals need? https://arxiv.org/abs/2502.13658 (Dostopano dne: 22. junij 2025)
[25] ENISA. (2022). European Cybersecurity Skills Framework – User Manual. https://www.enisa.europa.eu/sites/default/files/publications/European%20Cybersecurity%20Skills%20Framework%20User%20Manual.pdf (Dostopano dne: 22. junij 2025)
[26] National Institute of Standards and Technology – NIST. (2020). NICE Cybersecurity Workforce Framework (NIST SP 800-181 Rev. 1). https://doi.org/10.6028/NIST.SP.800-181r1 (Dostopano dne: 12. junij 2025)
[27] ENISA. (2020). Cybersecurity Skills Development in the EU. https://www.enisa.europa.eu/publications/cybersecurity-skills-development-in-the-eu (Dostopano dne: 12 junij 2025)
[28] Taherdoost, H. (2021). A Review on Risk Management in Information Systems: Risk Policy, Control and Fraud Detection. Electronics, 10(24), 3065. https://doi.org/10.3390/electronics10243065 (Dostopano dne: 26. junij 2025)
[29] Person, D., & Pareek, A. (2022). A qualitative study of human factors in cybersecurity: Beliefs, attitudes and behaviors. Cyberpsychology, Behavior, and Social Networking, 25(7), 450–456. https://www.liebertpub.com/doi/10.1089/cyber.2022.0191 (Dostopano dne: 3. julij 2025)
[30] Ruohonen, J. (2024). A Systematic Literature Review on the NIS2 Directive. arXiv preprint arXiv:2412.08084. https://arxiv.org/abs/2412.08084 (Dostopano dne: 3. julij 2025)
[31] National University Library. (2025). Partial Eta Squared – Statistics Resources. https://resources.nu.edu/statsresources/eta (Dostopano dne: 13. julij 2025)
[32] Urad Republike Slovenije za informacijsko varnost (URSIV). (2025). Priročnik kibernetske varnosti. https://www.gov.si/assets/vladne-sluzbe/URSIV/Datoteke/Prirocnik-kibernetske-varnosti.pdf (Dostopano dne: 12. junij 2025)
[33] World Economic Forum. (2024). Global Cybersecurity Outlook 2024. https://www.weforum.org/publications/global-cybersecurity-outlook-2024 (Dostopano dne: 22 junij 2025)
[34] OECD. (2024). Building a Skilled Cyber Security Workforce in Europe. OECD Skills Studies. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/02/building-a-skilled-cyber-security-workforce-in-europe_6abaf769/3673cd60-en.pdf (Dostopano dne: 12. julij 2025)
[35] Ministry of Transport and Communications of Finland. (2024). Digital skills and competence strategy for Finland 2023–2030. https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/165138/LVM_2024_5.pdf (Dostopano dne: 12. julij 2025)
[36] National Center for Science and Engineering Statistics. (2024). Cybersecurity Workforce Data Initiative. https://ncses.nsf.gov/initiatives/cybersecurity-workforce-data-initiative (Dostopano dne: 8. avgust 2025)

▪

Andreja Markun je magistrica organizatorka informatičarka, zaposlena na področju informacijske varnosti. V svoji raziskavi se ukvarja s sistemskimi pristopi k razvoju kibernetskih kompetenc, vplivom regulative na kadrovske ukrepe ter dolgoročno odpornostjo organizacij v digitalnem okolju.

▪

Alenka Brezavšček je izredna profesorica na Fakulteti za organizacijske vede Univerze v Mariboru, predstojnica Katedre za metodologijo. Doktorirala je na področju integralnega upravljanja kakovosti. Njeno raziskovalno delo vključuje operacijske raziskave, stohastične procese, zanesljivost in razpoložljivost sistemov, optimizacijo vzdrževanja ter informacijsko in kibernetsko varnost.

Izboljšanje učinkovitosti semaforiziranih križišč s simulacijami in strojnim učenjem

Šemso Hrnjičić, Uroš Rajkovič
Univerza v Mariboru, Fakulteta za organizacijske vede, Kidričeva cesta 55a, 4000 Kranj
semso.hrnjicic@gmail.com, uros.rajkovic@um.si

Izvleček

Razvoj simulacijskega okolja za proučevanje prometnih sistemov omogoča globlje razumevanje in boljše reševanje izzivov v prometu. V raziskavi smo se osredotočili na optimizacijo semaforiziranega križišča s ciljem izboljšanja njegove učinkovitosti in zmogljivosti. S pomočjo najsodobnejših orodij, kot sta Unity in Blender, smo ustvarili dinamičen model, ki lahko simulira različne prometne scenarije in se odziva na realno časovne spremembe v prometnem okolju. Zbiranje in analiza podatkov simulacije nam je omogočila, da natančno prilagodimo časovne cikle semaforjev in implementiramo inteligentne prometne nadzorne sisteme. Z integracijo naprednih tehnologij strojnega učenja smo razvili nevronske mreže, ki optimizirajo prometno signalizacijo in dramatično zmanjšajo čakalne čase. Rezultati naše raziskave kažejo občutne izboljšave v pretočnosti in varnosti prometa, kar dokazuje, da je pristop z uporabo simulacij in implementacijo simuliranih optimizacij ključen za prihodnje izboljšave v urbanem prometnem načrtovanju.

Ključne besede: simulacija križišča, spodbujevalno učenje, nevronske mreže, optimizacija

Improving the efficiency of signalized intersections with simulations and machine learning

Abstract

The development of a simulation environment for the study of transport systems enables a deeper understanding and a better solution to traffic challenges. In the research, we focused on the optimization of a traffic light intersection with the aim of improving its efficiency and performance. Using state-of-the-art tools such as Unity and Blender, we have created a dynamic model that can simulate various traffic scenarios and respond to real-time changes in the traffic environment. The collection and analysis of simulation data allowed us to precisely adjust traffic light cycles and implement intelligent traffic control systems. By integrating advanced machine learning technologies, we have developed neural networks that optimize traffic signals and dramatically reduce waiting times. The results of our research show significant improvements in traffic flow and safety, proving that the approach using simulations and the implementation of simulated optimizations is crucial for future improvements in urban traffic planning.

Keywords: Intersection simulation, reinforcement learning, neural network, optimisation

1 UVOD

Raziskovanje optimizacije pretočnosti prometa na prometnih križiščih z uporabo simulacijskih modelov je pomembno za razumevanje in izboljšanje pretočnosti prometa ter zmanjšanje zastojev. Semaforizirana križišča predstavljajo kompleksne sisteme, kjer je usklajevanje pretoka vozil ključnega pomena za preprečevanje prometnih zastojev in izboljšanje prometne varnosti. Simulacijski modeli lahko učinkovito ponazarjajo realne prometne razmere in pomagajo pri analizi različnih scenarijev.

Razvoj simulacijskega okolja za izboljšavo sema-

foriziranega križišča je aktualna tema zaradi naraščajoče urbanizacije in prometnih obremenitev, ki zahtevajo učinkovite rešitve za zmanjšanje zastojev, čakalnih časov in onesnaževanja. Simulacijska okolja omogočajo varno in stroškovno učinkovito testiranje različnih optimizacijskih pristopov, brez neposrednega poseganja v realni promet. Tako omogočajo izboljšanje pretočnosti prometa in podpirajo načrtovanje trajnostnih prometnih sistemov, hkrati pa zagotavljajo dragocene vpoglede za izboljšanje obstoječe prometne infrastrukture v mestih.

Optimizacija semaforiziranih križišč ni nič novega. Promet optimiziramo na različne načine in tudi drugi raziskovalci eksperimentirajo z optimizacijo s pomočjo strojnega učenja. Iz ene od relevantnih raziskav izhaja sledeče:

Eksperimentalni rezultati kažejo, da lahko sistemi s spodbujevalnim učenjem prekašajo številne prilagodljive sisteme. Eden od sistemov, TC-3, uporablja globalno komunikacijo med semaforji in lahko preseže delovanje drugih algoritmov, kadar promet ni zelo gost. Če je prometno omrežje nasičeno, ko povečujemo prometno obremenitev, sistemi s spodbujevalnim učenjem očitno presegajo fiksne krmilnike in tudi veliko profitirajo od sočasnega učenja. [1]

V primeru nepričakovanih zastojev (na primer zaradi nesreč) obveščeni potniki skrajšajo svoj potovalni čas z zamenjavo poti, vendar posledično alternativne poti postanejo polnejše, zaradi česar se lahko podaljšujejo potovalni časi za neobveščene voznike. [2]

Do danes so bile raziskane tako tradicionalne kot sodobne metode optimizacije semaforiziranih križišč, pri čemer raziskave z uporabo umetne inteligence ponujajo potencial za prilagodljivejše in učinkovitejše delovanje semaforiziranih križišč. Sodobne raziskave kažejo tudi na to, da boljši senzorji in vedno večja količina podatkov ne pomenijo vedno boljšo stopnjo izboljšave pretoka semaforiziranega križišča.

Rezultati kažejo, da podatki, zbrani iz tradicionalnih in vseprisotnih senzorjev, kot so detektorji zanke, zadostujejo za spodbujevalno učenje. Po modelu, oblikovanem v tej raziskavi, predstavitve stanja visoke ločljivosti, ki zahtevajo prefinjene senzorje, nudijo izboljšave le z zmanjšanjem zakasnitve za približno 10 %, brez razlike v čakalni vrsti ali pretoku. [3]

V okviru raziskave smo razvili simulacijski model semaforiziranega križišča z uporabo platforme Unity in simulirali pretok križišča z realnimi podatki. Nato smo analizirali simuliran pretok in uporabili tri različne metode optimizacije za izboljšanje učinkovitosti in natančnosti modela. V nadaljevanju bomo predstavili:

- vizualizacijo semaforiziranega križišča,
- podatke simulacije,
- uporabljene tehnike za optimizacijo semaforiziranega križišča in
- primerjavo rezultatov različnih metod optimizacije, da bi ocenil njihovo uspešnost.

Najprej bomo podrobneje predstavili vizualizacijo semaforiziranega križišča, nato bomo predstavili, kako delujejo vgrajeni senzorji, kako smo obdelali in uporabili pridobljene podatke, na koncu pa kako smo uporabili tehnike spodbujevalnega učenja za izboljšanje sistema. Prav tako bomo analizirali in primerjali rezultate različnih pristopov k optimizaciji križišča, kar nam bo dalo jasno sliko uspešnosti posameznih metod.

2 METODOLOGIJA

V naši raziskavi smo kot osnovni pristop uporabili načrtovanje in razvoj (Design Science Research, Hevner et al., 2004). V okviru tega pristopa razvijamo artefakt – simulacijski model semaforiziranega križišča – skozi tri zaporedne cikle:

- Cikel strogosti

V tej fazi smo izvedli temeljit pregled obstoječe literature in metod, ki se ukvarjajo s problematiko semaforiziranih križišč. Za izvedbo temeljitega pregleda literature smo opravili iskalni postopek v akademskih bazah ter pregledali druge vire (konferenčni zborniki, tehnična poročila, magistrske in doktorske naloge). Iskalne pojme smo oblikovali okoli ključnih tem (npr. *traffic signal optimization, traffic simulation, intersection modelling, adaptive traffic control, traffic light intersection, Unity simulation*), pregledali naslove in izvlečke, nato pa celotna besedila študij, ki so ustrezala našim kriterijem pregledali (študije, ki obravnavajo optimizacijo semaforiziranih križišč, modeliranje in simulacijo prometa, empirične meritve ali eksperimentalno vrednotenje). Ta postopek je zagotavljal pokritost teorije, metodologij in praktičnih primerov, relevantnih za naš raziskovalni cilj. Na podlagi te analize smo prepoznali pomembnost optimizacije semaforiziranih križišč in se odločili, da kot raziskovalni predmet izberemo semaforizirano križišče v Kranju.

- Cikel relevantnosti

Namen te faze je preveriti, ali ima optimizacija izbranega križišča praktično utemeljitev v realnem okolju. Pred izvedbo optimizacijskega postopka smo si zastavili ključno vprašanje: »Ali je izboljševanje delovanja semaforiziranega križišča smiselno?«. Z namenom odgovora na to vprašanje smo razvili simulacijski model, s katerim smo ocenili vpliv morebitnih sprememb na prometni pretok in varnost na križišču ter v njegovi okolici.

- Cikel razvoja

V tej fazi smo razvili in implementirali simulacijski model semaforiziranega križišča. Model smo izdelali v 3D okolju Unity, pri čemer smo uporabili empirično zbrane podatke – meritve pretoka na vseh vhodih križišča, izvedene v obdobju ene ure. Poleg funkcionalne simulacije smo zagotovili tudi vizualno predstavitev, da bi si lažje predstavljali stanje na križišču in njegovem neposrednem okolju. Na podlagi razvitega modela smo izvedli vrsto eksperimentov, kjer smo optimizirali križišče na tri različne načine. Primerjava eksperimentalnih rezultatov nam je omogočila oceno učinkovitosti posameznih optimizacijskih pristopov in določitev morebitnega profita izboljšav.

Z navedenim celovitim pristopom smo dosegli tako teoretično kot praktično podlago za nadaljnje raziskave in morebitno implementacijo optimizacij na izbranem semaforiziranem križišču.

3 REZULTATI

Za robustno povezavo simulacijskega modela z realnim stanjem smo izvedli empirično meritev pretoka vozil: enourno štetje vozil na vseh vhodih semaforiziranega križišča pri trgovskem centru Tuš Supermarket Planet Kranj (presečišče cest Cesta Boštjana Hladnika in Cesta Rudija Šeliga) je bilo izvedeno v soboto, 23. oktobra 2021. Pridobljene podatke smo uporabili za kalibracijo vhodnih pretokov in drugih parametrov modela ter kot osnovo za izvedbo eksperimentov in primerjavo rezultatov optimizacijskih scenarijev. Ta empirična podlaga zagotavlja, da so eksperimentalni scenariji zasnovani glede na dejanske prometne pogoje opazovanega križišča.

V tem poglavju predstavljamo ključne rezultate raziskave, ki zajemajo razvoj in uporabo simulacijskega modela izbranega semaforiziranega križišča ter vrednotenje učinkovitosti različnih optimizacijskih pristopov. Najprej podamo razvoj vizualnega dela raziskave, ki omogoča boljše razumevanje prometnih razmer in postavitve križišča. Nato opišemo postopek razvoja simulacijskega modela, vključno z uporabo empiričnih podatkov in tehničnimi vidiki implementacije. V zadnjem delu predstavimo rezultate optimizacijskih scenarijev, primerjamo njihove učinke ter ocenimo potencialne izboljšave prometnega toka in varnosti.

3.1 Vizualizacija

Vizualizacija je izjemno pomembna komponenta raziskave, ki olajša razumevanje problemov in omogoča boljše predstavljanje potrebnih sprememb in modifikacij. Za dosego slednjega cilja smo se odločili uporabiti programsko orodje Blender, ki nam je omogočilo natančno izdelavo tridimenzionalnega modela izbranega križišča. Po izdelavi smo model brez težav uvozili v program Unity, ki smo ga uporabili za nadaljnji razvoj simulacije.

Za bolj realistično upodobitev simulacijskega okolja smo v simulacijo vključili tudi satelitske posnetke območja, ki služijo kot ozadje za križišče. Dodali smo modele avtomobilov, ki predstavljajo raznolik promet, in modele semaforjev, ki regulirajo prometne tokove. Da bi dosegli še večjo verodostojnost, smo semaforjem dodali funkcionalne luči – zelene, rumene in rdeče, kar omogoča prikaz različnih faz prometne signalizacije.

Unity omogoča uvoz in sestavljanje sredstev, pisanje kode za interakcijo s predmeti, ustvarjanje ali uvoz animacij za uporabo z naprednim animacijskim sistemom in še veliko več. [4]

Vse te elemente lahko opazimo na sliki 1, ki prikazuje končni izgled vizualizacije križišča. Ta vizualizacija služi ne samo kot demonstracija funkcionalnosti modela, ampak tudi kot sredstvo za preverjanje, kako različni elementi koordinirano delujejo.

3.2 Razvoj simulacijskega modela

Za namen izvedbe simulacije našega semaforiziranega križišča smo razvili dve ključni entiteti, vsako s svojo specifično logiko in funkcionalnostjo, ki sta nujni za realistično in učinkovito modeliranje prometnih tokov.

Skripta mora biti pripeta na objekt v sceni, da ga Unity lahko uporabi. Skripte so napisane v posebnem jeziku, ki ga Unity razume. Prek tega jezika se lahko pogovarjamo z motorjem in mu dajemo navodila. Jezik, ki se uporablja v Unity, se imenuje C#. Vsi

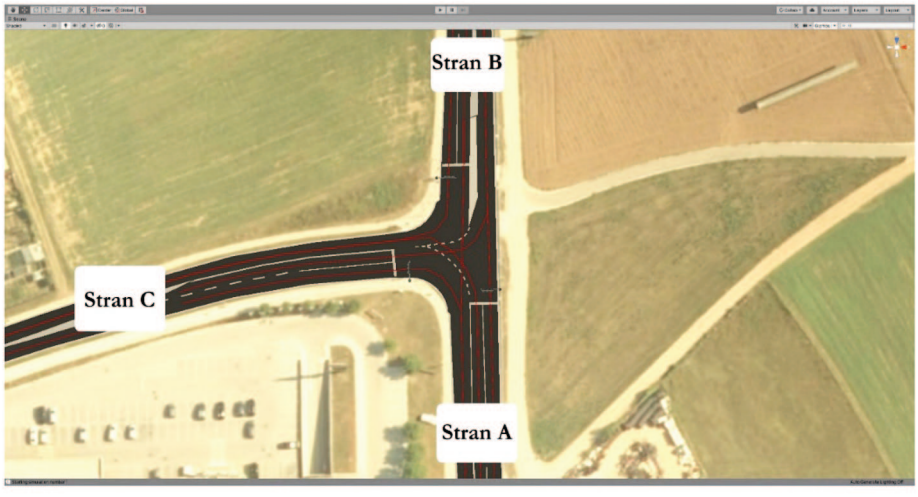
Slika 1: **Vizualizacija križišča**

jeziki, s katerimi Unity deluje, so objektno usmerjeni skriptni jeziki. Kot vsak jezik imajo skriptni jeziki sintakso ali dele govora, primarni deli pa se imenujejo spremenljivke, funkcije in razredi. [5]

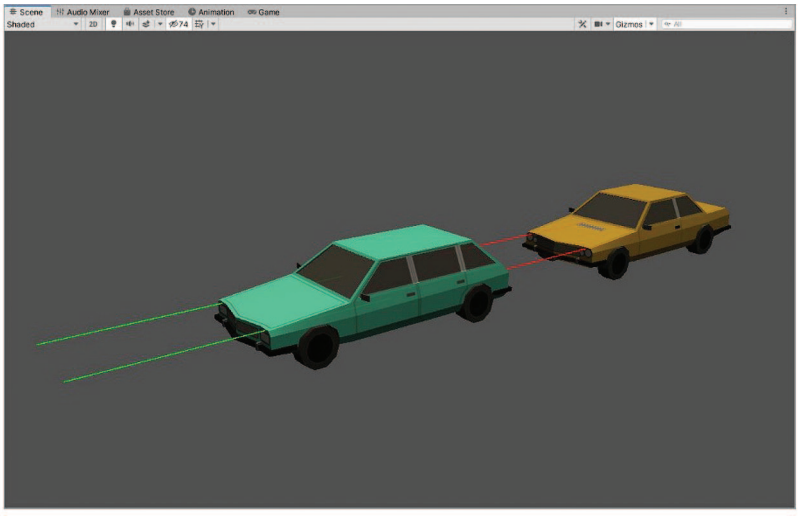
C# je preprost, sodoben, objektno usmerjen in tipno varen programski jezik. Ima svoje korenine v družini jezikov C in je znan predvsem programerjem C, C++ in Java. C# je ECMA International standardiziral kot standard ECMA-334, ISO/IEC pa kot standard ISO/IEC 23270. [6]

Prva entiteta je semaforizirano križišče, ki deluje kot nadzorna entiteta, ki ves čas simulacije skrbno spremlja čas in prometne razmere. Na podlagi predhodno določenih spremenljivk, kot so gostota prometa in posebne situacije na cesti, križišče dinamično določa, katera smer bo imela prednost. Sistem semaforjev je programiran tako, da maksimira pretočnost in minimizira čakalne čase, s čimer pripomore k večji varnosti in učinkovitosti na cesti.

Na sliki 2 je prikazan zračni pogled na izbrano križišče, ki nam daje jasno predstavo o njegovi strukturi in razporeditvi. Križišče je razdeljeno na tri različne sektorje: Stran A, Stran B in Stran C. Strani A in B predstavljata glavne, prednostne ceste, medtem ko je Stran C kategorizirana kot stranska cesta.



Slika 2: **Strani križišča**



Slika 3: **Vizualizacija senzorjev**

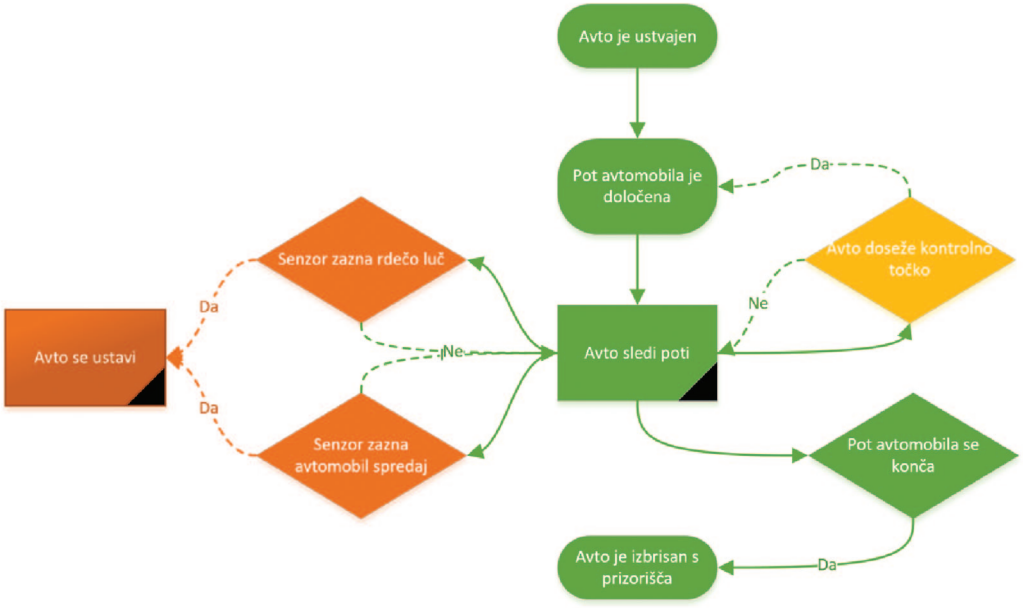
Druga entiteta je posamezen avtomobil. Vsak avtomobil v simulaciji predstavlja ločeno entiteto, ki se zaveda svoje lokacije in cilja. Avtomobili se vozijo proti križišču, kjer ob prihodu na določeno kontrolno točko sprejmejo odločitev o smeri nadaljevanja - levo, desno ali naravnost. Logika, ki usmerja odločitve avtomobilov, temelji na algoritmih, ki so bili razviti na podlagi zbranih podatkov o prometu. Ta logika omogoča avtomobilom, da reagirajo na spremenljive prometne razmere in semaforizacijo, kar zagotavlja pretočnost prometa in zmanjšuje tveganje za zastoje.

Da bi zagotovili, da vozila v simulaciji spoštujejo cestnoprometne predpise in se odzivajo na prometne razmere na realističen način, smo v modele vozil implementirali senzorje. Ti senzorji omogočajo zaznavanje drugih vozil, kontrolnih točk in prednostnih točk na cestišču. S tem smo vozilom omogočili, da se inteligentno odzivajo na spremembe v okolju, kot so spremembe v prometni luči ali nepredvidene ovire na cesti, kar povečuje realnost naše simulacije. Ta pristop ne samo izboljša natančnost simulacije, temveč tudi poveča njeno pedagoško vrednost pri demonstraciji, kako dinamični sistemi, kot so semaforizirana križišča, vplivajo na urbani promet.

Na sliki 3 je prikazan primer dveh avtomobilov, ki ilustrira delovanje vgrajenih senzorjev. Avtomobil ne zazna nobenih ovir pred seboj, kar je označeno z žarki senzorja zelene barve, ki ponazarjajo varno pot. Senzorji avtomobila na desni strani pa nasprotno zaznajo prisotnost drugega avtomobila neposredno pred seboj. Žarki senzorja se zato obarvajo rdeče, kar kaže na nevarnost trka ali potrebo po zmanjšanju hitrosti. Informacija o zaznani oviri se samodejno posreduje nadzornemu sistemu vozila, ki nato ustrezno prilagodi vedenje avtomobila, da ta izogne morebitni nevarnosti.

Diagram logike delovanja avtomobilov, ki je prikazan na sliki 4, podrobno opisuje procese, skozi katere avtomobil potuje od začetka do konca svoje poti v simuliranem okolju. Vsak avtomobil začne s specifičnim ciljem, do katerega je usmerjen z nizom vnaprej določenih kontrolnih točk. Ko avtomobil doseže kontrolno točko, prejme informacije o naslednjem cilju. Med potovanjem so avtomobili opremljeni s senzorji, ki nenehno ocenjujejo okoliško situacijo in omogočajo avtomobilu, da ustavi v treh specifičnih scenarijih: če zazna rdečo luč, če je neposredno pred njim drugo vozilo ali če mora zaviti in čaka na prednost nasproti vozečih vozil. Ko avtomobil doseže končni cilj, je iz scenarija odstranjen, da se ohrani optimalna zmogljivost simulacije in prepreči nepotrebna zasičenost prizorišča.

Za natančne analize prometnega toka smo merili gostoto prometa na tem križišču, ki je trajalo eno uro. V tem času smo zabeležili, da je skozi Stran A prešlo 690 vozil, kar jo uvršča kot najbolj obremenjeno stran križišča. Stran B je imela prav tako visok pretok z 646 vozili na uro, medtem ko je Stran C, kot manj prometna stranska cesta, zabeležila precej nižji prometni tok, s samo 120 vozili na uro. Te podatke prikažemo v tabeli 1, kjer je prikazano število avtomobilov, ki so prečkali križišče z vsake smeri v času ene ure. Takšna kvantitativna analiza prometa nam omogoča, da bolje razumemo dinamiko pretoka in vpliv razporeditve prometa na delovanje križišča.



Slika 4: **Logika delovanja avtomobila v simulaciji**

Tabela 1: **Podatki pretoka križišča**

	Število avtomobilov/h	Levo/h	Naprej/h	Desno/h	Levo v %	Naprej v %	Desno v %
A	690	108	582	0	16	84	0
B	646	0	564	82	0	87	13
C	120	84	0	36	70	0	30

Po zaključku razvoja našega simulacijskega modela smo se lotili uporabe zbranih podatkov za simulacijo prometnega toka na semaforiziranem križišču. Obdobje simulacije je trajalo eno uro. Da bi zagotovili zanesljivost naših rezultatov, smo vsako posebno stanje na križišču simulirali desetkrat, nato pa smo izvedli analizo povprečnih vrednosti, ki so bile zabeležene. Rezultate teh simulacij smo strnili v tabeli 2, kjer so povprečni rezultati prikazani v formatu ur, minut in sekund (hh:mm:ss). Posebno pozornost smo namenili analizi skupnih čakalnih časov avtomobilov za vsako smer posebej, da bi ugotovili, katera smer križišča povzroča najdaljše zastoje. Ugotovili smo, da avtomobili, ki prihajajo iz smeri A, v povprečju najdlje čakajo na semaforju, in sicer približno uro in 37 sekund.

Tabela 2: **Povprečni čakalni čas avtomobilov**

hh:mm:ss			
Čakalni čas A	Čakalni čas B	Čakalni čas C	Skupni čakalni čas
01:00:37	00:57:04	00:51:36	02:49:18

Slednji podatek je ključnega pomena za nadaljnje ukrepanje pri optimizaciji križišča, saj izpostavlja specifične izzive, s katerimi se srečujemo na najbolj obremenjeni smeri križišča. Razumevanje vzorcev čakanja nam omogoča ciljni pristop k izboljšavam načrtovanja semaforizacije in tako izboljšanje pretoka prometa na kritičnih točkah.

3.3 Optimizacija

V fazi optimizacije smo se osredotočili na tri glavne pristope za izboljšanje delovanja semaforiziranega križišča. Prvi pristop je vključeval prilagoditev časovnih intervalov semaforja. S pomočjo našega simulacijskega modela smo preizkusili različne kombinacije časov za prednostne in stranske ceste. Ta metoda nam je omogočila hitro in stroškovno učinkovito eksperimentiranje, kar je bistveno za iskanje optimalne nastavitve semaforjev, ki bi izboljšala pretočnost prometa.

Drugi pristop je bil implementacija senzorjev, ki omogočajo spremljanje trenutnih prometnih razmer v realnem času. S pomočjo teh senzorjev smo sema-

foriziranemu križišču omogočili, da dinamično prilagaja svoje delovanje glede na spremenljive prometne pogoje. To je pripomoglo k večji prilagodljivosti sistema in boljšemu odzivanju na nepričakovane spremembe v prometnih tokovih.

Tretji način optimizacije je vključeval uporabo strojnega učenja. Razvili smo model nevronske mreže s pomočjo odprtokodnega projekta ML-Agents in odprtokodnega okolja TensorFlow, ki je omogočil, da se naše simulacijsko križišče uči iz zbranih podatkov in samodejno prilagaja svoje delovanje z namenom izboljšanja pretočnosti in skrajšanja čakalnih časov.

Vse tri optimizacije smo temeljito preizkusili in skrbno dokumentirali rezultate. Povprečne vrednosti iz različnih simulacijskih scenarijev smo uporabili za analizo in primerjavo učinkovitosti posameznih pristopov. Na ta način smo lahko določili, katera metoda najbolj učinkovito izboljša prometno situacijo na križišču.

3.3.1 Strojno učenje

Strojno učenje uporabljamo kot tretji način optimizacije delovanja semaforiziranega križišča. Odločili smo se uporabiti paket ML-Agents, ki omogoča, da naš simulacijski model postane inteligenten agent, zmožen samostojnega učenja in odločanja.

Zbirka orodij ML-Agents je obojestransko koristna tako za razvijalce iger kot za raziskovalce umetne inteligence, saj zagotavlja osrednjo platformo, na kateri je mogoče oceniti napredek umetne inteligence v bogatih okoljih Unity in nato omogočiti dostop širši skupnosti raziskovalcev in razvijalcev iger. [7]

K navedenemu pristopamo s tehniko spodbujevalnega učenja. Spodbujevalno učenje je močno orodje, ki izhaja iz principov živalske in vedenjske psihologije, in ima ključno vlogo na mnogih področjih strojnega učenja. Ta pristop se osredotoča na interakcijo med agentom in okoljem, kjer agent prejema bodisi nagrade bodisi kazni, odvisno od učinka njegovih dejanj na okolje. V začetnih fazah učenja agent eksperimentira z različnimi strategijami, njegovo obnašanje pa se sčasoma oblikuje na podlagi povratnih informacij, ki jih prejme. To pomeni, da agent prejme nagrade, če njegova dejanja privedejo do pozitivnih izidov. Nagrade ga spodbujajo k ponovitvi uspešnih dejanj. Nasprotno, negativne nagrade ali kazni ga odvračajo od morebitnih škodljivih ali neučinkovitih dejanj.

Slika 5: **Elementi spodbujevalnega učenja**

Navedeni proces omogoča agentu, da se uči in prilagaja, kar povečuje njegovo sposobnost sprejemanja optimalnih odločitev v danih situacijah. Spodbujevalno učenje se uporablja v številnih aplikacijah, od iger, kjer se agenti učijo igrati zapletene igre na visoki ravni, do industrijskih aplikacij, kjer sistemi samodejno optimizirajo delovanje naprav za zmanjševanje porabe energije ali izboljšanje proizvodnje.

Glavni cilj našega učenja je minimiziranje čakalnih časov za vozila, kar je bistveno za izboljšanje učinkovitosti prometnega toka in zmanjšanje zastojev. Uvedba spodbujevalnega učenja ni le izvedbena prednost, ampak tudi inovativni pristop k prometni regulaciji, ki presega tradicionalne metode upravljanja semaforjev. Spodbujevalno učenje omogoča agentu, da iz iteracij učenja razvije strategije, ki optimizirajo dodeljevanje zelenih faz v realnem času glede na trenutne pogoje prometa.

Spodbujevalno učenje je eno najbolj vznemirljivih in tudi eno najstarejših področij strojnega učenja danes. Obstaja že od petdesetih let dvajsetega stoletja in je proizvedlo veliko zanimivih aplikacij, zlasti na področju iger (na primer TD-Gammon, Backgammon-playing program) in na področju nadzora strojev, vendar se je o teh aplikacijah redko pisalo na naslovnicah. Leta 2013 pa se je zgodila revolucija, ko so raziskovalci britanskega podjetja DeepMind predstavili sistem, ki bi se lahko naučil igrati skoraj katero koli igro konzole Atari in je sčasoma postal celo boljši od ljudi. Pri svojem delovanju uporablja zgolj neobdelane slike kot vhod brez predhodnega poznavanja pravil igre. [8]

Na sliki 6 prikazujemo, kako naš semafor (Agent), opremljen z mrežo senzorjev, nenehno spremlja stanje na križiščih (Okolje) in kako se na podlagi zbranih

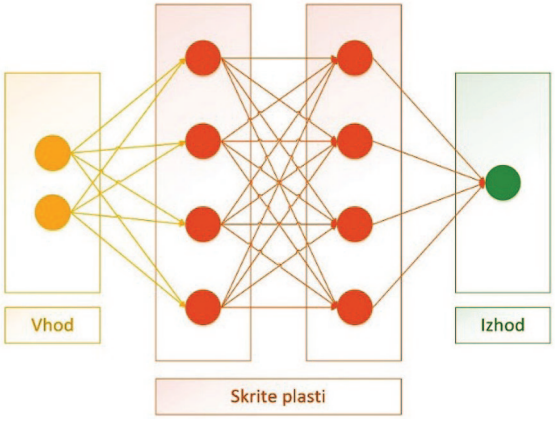
podatkov samostojno odloča, kateri smeri bo dodelil prednost. Povratne informacije, ki jih agent prejema od simulacijskega okolja, so oblikovane kot nagrade ali kazni. Te so neposredno povezane z izmerjenimi čakalnimi časi, kjer pozitivne nagrade stimulirajo tiste odločitve, ki skrajšajo čakalne dobe, medtem ko negativne kazni odvračajo od odločitev, ki vodijo v daljša čakanja. Ta sistem nagrajevanja in kaznovanja omogoča postopno izboljševanje strategij semaforizacije, s čimer povečujemo pretočnost in zmanjšujemo zastoje, kar ima za posledico izboljšano splošno učinkovitost križišča.

Slika 6: **Dinamika okolja in agenta**

Tako se skozi proces spodbujevalnega učenja naš model ne samo nauči odzivati na neposredne prometne izzive, temveč tudi predvideva in proaktivno upravlja prometne tokove, kar omogoča bolj tekoče in varnejše prometne pogoje na kritičnih urbanih točkah.

Na sliki 7 je prikazana končna konfiguracija nevronske mreže, ki bo uporabljena za dejansko delovanje v naši raziskavi. Ta mreža bo imela tri skrite plasti, pri čemer vsaka plast vsebuje 256 enot. Vizualna predstavitev modela jasno ločuje različne komponente: vhodne, skrite in izhodne plasti. Vhodna plast, označena z rumeno barvo, sprejema podatke iz okolja, ki so lahko različni prometni parametri, kot so gostota prometa, čas dneva, vremenske razmere in drugi relevantni dejavniki. Te vhodne podatke model uporabi za procesiranje v skritih plasteh nevronske mreže.

V modelu, kot je prikazan na sliki, so skrite plasti, ki so ključne za učenje in obdelavo vhodnih informacij, med vhodom in izhodom. Vsaka skrita plast vsebuje enote (nevrone), ki so prikazane kot rdeči krogi. Te enote delujejo kot procesorski elementi, ki težijo k preoblikovanju vhodnih podatkov v smiselne izhodne signale. V tem primeru imamo dve skriti plasti, kjer vsaka plast vključuje štiri enote. Ta konfiguracija omogoča mreži, da ujame in obdela kompleksne vzorce v podatkih, kar je bistveno za učinkovito odločanje o prometnih signalizacijah.



Slika 7: **Model nevronske mreže**

Z uporabo te konfiguracije nevronske mreže lahko pričakujemo izboljšanja v odzivanju križišč na spremenljive prometne pogoje, kar bo vodilo do

```yaml
default:
    trainer: ppo
    batch_size: 1024
    beta: 5.0e-3
    buffer_size: 10240
    epsilon: 0.2
    hidden_units: 128
    lambd: 0.95
    learning_rate: 3.0e-4
    learning_rate_schedule: linear
    max_steps: 5.0e5
    memory_size: 128
    normalize: false
    num_epoch: 3
    num_layers: 2
    time_horizon: 64
    sequence_length: 64
    summary_freq: 10000
    use_recurrent: false
    vis_encode_type: simple
    reward_signals:
        extrinsic:
            strength: 1.0
            gamma: 0.99

brain:
    batch_size: 10
    buffer_size: 100
    memory_size: 128

```

Slika 8: **Parametri nevronske mreže**

Tabela 2: **Razlaga parametrov [9]**

batch_size	Število izkušenj v vsaki ponovitvi gradientnega spuščanja. Ta mora biti vedno večkrat manjši od buffer_size. Če uporabljate neprekinjena dejanja, mora biti ta vrednost velika (približno 1000 sekund). Če uporabljate samo diskretna dejanja, mora biti ta vrednost manjša (približno 10 sekund).
buffer_size	PPO: število izkušenj, ki jih je treba zbrati pred posodobitvijo modela politike. Ustreza temu, koliko izkušenj je treba zbrati, preden se naučimo ali posodabljamo model. To bi moralo biti večkrat večje od batch_size. Običajno večji buffer_size ustreza stabilnejšim posodobitvam usposabljanja.
hidden_units	Število enot v skritih slojih nevronske mreže. Ustreza temu, koliko enot je v vsaki popolnoma povezani plasti nevronske mreže. Pri preprostih težavah, kjer je pravilno dejanje enostavna kombinacija opazovalnih vhodov, mora biti število majhno. Za težave, kjer je dejanje kompleksna interakcija med opazovanimi spremenljivkami, bi število moralo biti večje.
memory_size	Velikost pomnilnika, ki ga mora hraniti agent. Za uporabo LSTM usposabljanje zahteva zaporedje izkušenj namesto posameznih izkušenj. Ustreza velikosti množice števil, ki se uporabljajo za shranjevanje skritega stanja politike ponavljajoče se nevronske mreže. Ta vrednost mora biti večkratnik 2 in se mora prilagajati količinam informacij, za katere pričakujete, da si jih bo agent moral zapomniti, da lahko uspešno dokonča nalogo.
num_epoch	Število prehodov skozi medpomnilnik izkušenj pri izvajanju optimizacije gradientnega spuščanja. Večji, kot je batch_ size, bolj sprejemljivo je večje število tega parametra. Zmanjšanje tega bo zagotovilo stabilnejše posodobitve za ceno počasnejšega učenja.
num_layers	Število skritih plasti v nevronski mreži. Ustreza temu, koliko skritih plasti je prisotnih po vnosu opazovanja ali po CNN kodiranju vizualnega opazovanja. Za preproste težave bo manj plasti verjetno treniralo hitreje in učinkoviteje. Za kompleksnejše težave s krmiljenjem bo morda potrebnih več plasti.
sequence_length	Določa, kako dolga morajo biti zaporedja izkušenj med treningom. Upoštevajte, da če je ta številka premajhna, si agent ne bo mogel zapomniti stvari v daljšem časovnem obdobju. Če je to število preveliko, bo nevronska mreža potrebovala dlje, da se usposobi.

zmanjšanja čakalnih časov, izboljšanja pretočnosti prometa in povečanja splošne varnosti na cestah. Ta pristop predstavlja sodobno rešitev za izzive, s katerimi se srečujemo pri upravljanju urbanega prometa.

Na sliki 8 vidimo končne parametre za ustvarjanje naše nevronske mreže. Do prikazanih parametrov smo prišli tako, da smo vsako iteracijo nevronske mreže testirali v simulaciji in glede na rezultate smo izbrali optimalne parametre. Posamezni parametri so razloženi v tabeli

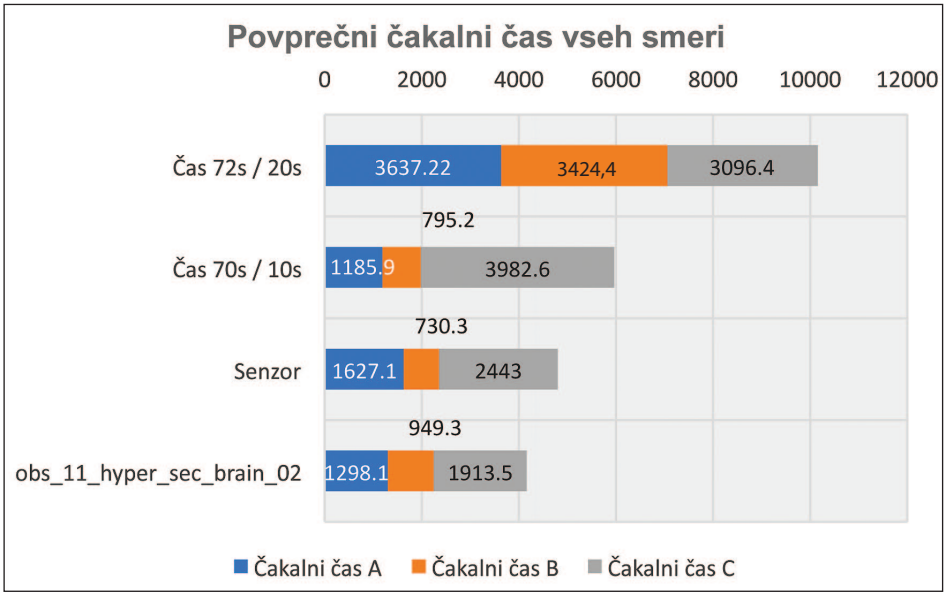
Ena komponenta učnih modelov s ogrodjem PyTorch je nastavitev vrednosti določenih atributov modela – hiperparametrov. Iskanje pravih vrednosti teh hiperparametrov lahko zahteva nekaj ponovitev. Posledično uporabljamo orodje za vizualizacijo, imenovano TensorBoard. Omogoča vizualizacijo določenih atributov agenta (na primer nagrada) skozi celotno usposabljanje, kar je lahko v pomoč tako pri gradnji intuicije za različne hiperparametre kot pri nastavljanju optimalnih vrednosti za vaše okolje. [7]

4 ANALIZA REZULTATOV OPTIMIZACIJE

Sedaj bomo pogledali rezultate vseh štirih stanj semaforiziranega križišča. Slika 9 ponuja vizualni pregled in primerjavo učinkov optimizacij na povprečne čakalne čase na križišču. Iz slike 9 so razvidne štiri vrstice, ki prikazujejo rezultate različnih stanj križišča:

1. Vrstica “Čas 72s / 20s” prikazuje izhodiščno stanje, kjer časi semaforjev niso bili spreminjani.
2. Vrstica “Čas 70s / 10s” odraža prvo optimizacijo, kjer smo spremenili čase semaforjev, kar je skrajšalo čakalne čase.
3. Vrstica “Senzor” prikazuje izboljšave, dosežene z uporabo senzorjev za dinamično prilagajanje časov semaforizacije glede na trenutne prometne razmere.
4. V zadnji vrstici, “obs_11_hyper_sec_brain_02”, so predstavljeni rezultati uporabe modela nevronske mreže za nadzor semaforiziranega križišča.

Ti rezultati potrjujejo učinkovitost sodobnih tehnologij in pristopov k upravljanju prometa na semaforiziranih križiščih. Optimizacija s pomočjo naprednih algoritmov strojnega učenja, kot je nevronska mreža, ponuja obetavne rešitve za izboljšanje prometne infrastrukture v urbanem okolju. Uporaba takšnih tehnologij ne samo izboljšuje pretočnost prometa in zmanjšuje čakalne čase, temveč tudi prispeva k večji varnosti, zmanjšanju stresa za voznike in splošnemu izboljšanju kakovosti bivanja v mestih.



Slika 9: **Rezultati simulacij vseh različnih stanj simulacije**

5 ZAKLJUČEK

V raziskavi smo optimizirali povprečni čakalni čas na izbranem semaforiziranem križišču. S pomočjo simulacijskega modela in strojnega učenja smo prišli do odgovora, na kakšen način in v kolikšni meri je mogoče optimizirati semaforizirano križišče. V zaključku naše raziskave je pomembno poudariti, da smo se med razvojem simulacijskega modela soočali z določenimi omejitvami. Osredotočili smo se izključno na analizo prometa na specifičnem križišču in v zelo omejenem časovnem okviru – za en dan in določeno uro. Kljub temu, da so rezultati pokazali značilne vzorce in omogočili določene optimizacije, moramo priznati, da je resnični svet bistveno bolj zapleten. Na prometne razmere nenehno vplivajo različni dejavniki, ki jih naš model trenutno še ne upošteva oziroma jih ne upošteva v celoti.

Analiza je pokazala, da so vse tri metode optimizacije znatno izboljšale pretočnost prometa na križišču:

- s prilagoditvijo časov semaforjev (Čas 70s / 10s) smo dosegli zmanjšanje skupnega čakalnega časa za približno 41 %,
- implementacija senzorjev, ki omogočajo prilagajanje semaforjev v realnem času, je zmanjšala čakalne čase za približno 53 %,
- najimpresivnejši rezultat je bil dosežen z uporabo nevronske mreže, ki je skupne čakalne čase zmanjšala za približno 59 %.

Zavedamo se, da so prometni sistemi dinamični in medsebojno povezani, zato je nujno, da naša naslednja faza razvoja vključuje razširitev simulacijskega modela na mrežo križišč. Vsako križišče v mestni mreži vpliva na delovanje sosednjih križišč, kar pomeni, da je treba za boljše razumevanje in optimizacijo prometnih tokov razviti model, ki lahko simulira in analizira več križišč hkrati. Tovrsten pristop bi nam omogočil bolj celostno razumevanje prometnih dinamik in vzorcev, kar bi posledično vodilo do učinkovitejših rešitev za zmanjšanje zastojev in izboljšanje pretočnosti.

Dolgoročno gledano je naš cilj razviti robustnejše in prilagodljive sisteme, ki se ne samo odzivajo na trenutne pogoje, ampak lahko predvidevajo in se proaktivno prilagajajo prihajajočim spremembam. To bo zahtevalo nadaljnje raziskave in razvoj v smeri vključitve naprednih tehnologij, kot sta umetna inteligenca in strojno učenje, ki lahko simulacijam prometa dodajo nove razsežnosti inteligence in predikativne moči.

V sorodni raziskavi je Wiering napisal:

V prihodnjem delu bi radi preizkusili svoje sisteme na bolj realističnih simulatorjih prometa, v katere želimo dodati tudi javni prevoz, ki bi moral imeti prednost, saj ima več potnikov. [1]

Prometne sisteme je mogoče optimizirati na različne načine in naša ratiskava je samo temelj za nadaljnje študije in razvoj na področju prometnega

inženiringa, s končnim ciljem ustvarjanja bolj odzivnih in inteligentnejših prometnih sistemov, ki bodo pripomogli k boljši mobilnosti, varnosti in kakovosti življenja v urbanem okolju.

6 LITERATURA

[1.] Wiering, M. (2000). Multi-Agent Reinforcement Learning for Traffic Light Control. University of Utrecht, Department of Computer Science

[2.] Wiering, M., van Veenen, J., Vreeken, J., & Koopman, A. (2004). Intelligent Traffic Light Control. Utrecht: institute of information and computing sciences, utrecht university.

[3.] Mohammad Noaeen, Atharva Naik, Liana Goodman, Jared Crebo, Taimoor Abrar, Zahra Shakeri Hossein Abad, Ana LC Bazzan, Behrouz Far (2022/8/1). Reinforcement learning in urban network traffic signal control: A systematic literature review. Expert Systems with Applications.

[4.] Tuliper, A. (1. Avgust 2014). Unity : Developing Your First Game with Unity and C#. MSDN Magazine, str. 36-37.

[5.] Unity Technologies. (26. Oktober 2020). Unity Documentation. Pridobljeno iz unity3d: https://docs.unity3d.com/Manual/index.html

[6.] Hejlsberg, A., Torgersen, M., Wiltamuth, S., & Golde, P. (2011). The C# Programming Language Fourth Edition. Boston: Addison-Wesley.

[7.] Unity Technologies. (5. Februar 2022). github.com/Unity-Technologies/ml-agents. Pridobljeno iz github.com/Unity-Technologies: https://github.com/Unity-Technologies/ml-agents

[8.] Géron, A. (2019). Hands-On Machine Learning with Scikit--Learn, Keras, and TensorFlow, 2nd Edition. Newton: O'Reilly Media, Inc.

[9.] Unity Technologies. (5. November 2021). Unity MLAgents Documentation. Pridobljeno iz ML Agents: https://docs.unity3d.com/Manual/com.unity.ml-agents.html

[10.] Blender. (4. Februar 2022). About - blender.org. Pridobljeno iz blender.org: https://www.blender.org/about/

▪

Šemso Hrnjičić je razvijalec programske opreme in svetovalec na področju preiskav letalskih nesreč in incidentov na Ministrstvu za obrambo Republike Slovenije. Trenutno deluje kot razvijalec v podjetju Endava, kjer sodeluje pri razvoju naprednih rešitev na področju mikroskopov za mednarodno podjetje. Njegova raziskovalna in strokovna področja vključujejo razvoj programske opreme, pametne sisteme in avtomatizacijo, simulacije ter uporabo umetne inteligence pri optimizaciji procesov. Posebej ga zanimajo aplikacije strojnega učenja, 3D simulacij in vizualizacij pri reševanju kompleksnih tehničnih in organizacijskih izzivov.

▪

Dr. Uroš Rajkovič je izredni profesor s področja informacijskih sistemov na Fakulteti za organizacijske vede Univerze v Mariboru. Njegova raziskovalna področja vključujejo umetno inteligenco in informacijske sisteme za podporo odločanju, s poudarkom na večkriterijskem modeliranju in optimizaciji procesov. Posebej ga zanimajo uporabe metod ekspertnih sistemov, simulacij ter naprednih algoritmov pri reševanju kompleksnih organizacijskih, tehničnih in družbenih problemov.

Iz Islovarja

Islovar je spletni terminološki slovar informatike, ki ga objavlja jezikovna sekcija Slovenskega društva INFORMATIKA na naslovu http://www.islovar.org. Slovar je javno dostopen za vpoglede in vnašanje novih izrazov.

3D-modelíranje -a s *(angl. 3D modeling)* izdelava 3D-modela z uporabo namenske programske opreme

3D-tískanje -a s *(angl. 3D-printing)* postopek izdelave tridimenzionalnih predmetov iz digitalnega modela s tiskalnikom; sin. aditivna proizvodnja

digitálno modelíranje -ega -a *(angl. digital modeling and fabrication)* proizvodnja, ki pri 3D-tiskanju uporablja 3D-modeliranje ali računalniško oblikovanje

modelíranje -a s *(angl. modeling)* postopek izdelave modela

modelírnik -a m *(angl. modeller)* namenska programska oprema, namenjena izdelavi 3D-modelov

podátkovni katalóg -ega -a m *(angl. data catalog)* podatkovni slovar, ki omogoča iskanje in poizvedovanje

podátkovni modél -ega -a m *(angl. data model)* model, ki opisuje entitete in povezave med njimi v računalniški obdelavi podatkov

simulácija -e ž *(angl. simulation)*
1. ponazoritev delovanja sistema
2. izvajanje eksperimenta z modelom

simulácijski modél -ega -a m *(angl. simulation model)* model, na katerega vpliva simulacijsko okolje in je namenjen uporabi v simulaciji

Izpitni centri ECDL

ECDL (European Computer Driving License), ki ga v Sloveniji imenujemo evropsko računalniško spričevalo, je standardni program usposabljanja uporabnikov, ki da zaposlenim potrebno znanje za delo s standardnimi računalniškimi programi na informatiziranem delovnem mestu, delodajalcem pa pomeni dokazilo o usposobljenosti. V Evropi je za uvajanje, usposabljanje in nadzor izvajanja ECDL pooblaščena ustanova ECDL Fundation, v Sloveniji pa je kot član CEPIS (Council of European Professional Informatics) to pravico pridobilo Slovensko društvo INFORMATIKA. V državah Evropske unije so pri uvajanju ECDL močno angažirane srednje in visoke šole, aktivni pa so tudi različni vladni resorji. Posebno pomembno je, da velja spričevalo v 148 državah, ki so vključene v program ECDL. Doslej je bilo v svetu v program certificiranja ECDL vključenih že preko 16 milijonov oseb, ki so uspešno opravile preko 80 milijonov izpitov in pridobile ustrezne certificate. V Sloveniji je bilo doslej v program certificiranja ECDL vključenih več kot 18.000 oseb in opravljenih več kot 92.000 izpitov. V Sloveniji sta akreditirana dva izpitna centra ECDL, ki imata izpostave po vsej državi.

Znanstveni prispevki

Kratki znanstveni prispevki

Informacije

ISSN 1318-1882