ELEKTROTEHNIŠKI VESTNIK 87(5): 251-259, 2020
IZVIRNI ZNANSTVENI ČLANEK

Vloga ponudnikov telekomunikacijskih storitev pri obvladovanju napadov DDoS

Kaja Prislan[1,*], **Kristina Stojchevska**[1, 2], **Anže Mihelič**[1, 3]

[1] *Univerza v Mariboru, Fakulteta za varnostne vede, Kotnikova ul. 8, 1000 Ljubljana, Slovenija*
[2] *T2 d.o.o, Verovškova ul. 64A, 1000 Ljubljana, Slovenija*
[3] *FernUniversität in Hagen, Universitätsstraße 47, 58097 Hagen, Nemčija*
* *E-pošta: kaja.prislan@fvv.uni-mb.si*

Povzetek. Napadi DDoS (napadi za porazdeljeno zavrnitev storitev) sodijo med najbolj razširjene kibernetske grožnje, ki pomenijo visoko tveganje za neprekinjeno delovanje informacijskih sistemov. Pomembno vlogo v sistemu odzivanja imajo upravljavci internetne infrastrukture, ki nadzirajo internetni promet. Pregled literature nakazuje na pomanjkanje znanstvenih raziskav o aktualnih izzivih in učinkovitih pristopih k soočanju z napadi DDoS, še zlasti skozi prizmo ponudnikov telekomunikacijskih storitev. Namen prispevka je proučiti trende na področju napadov DDoS in vlogo ponudnikov telekomunikacijskih storitev pri soočanju s tovrstno grožnjo. Skladno s tem smo izvedli raziskavo v obliki strukturiranih intervjujev s strokovnjaki, zaposlenimi pri največjih ponudnikih telekomunikacijskih storitev v Sloveniji. Rezultati kažejo, da se v Sloveniji ponudniki telekomunikacijskih storitev najpogosteje soočajo z volumetričnimi napadi DDoS manjšega obsega, med pogosto izpostavljene pa sodijo protokoli na transportnem sloju. Ponudniki telekomunikacijskih storitev ustrezno skrbijo za nadzor in omejevanje internetnega prometa, prav tako ponujajo dodatne storitve anti-DDoS, medtem ko naprednejših varnostnih mehanizmov še ne uporabljajo.

Ključne besede: napad DDoS, ponudniki telekomunikacijskih storitev, kibernetska varnost, zaznavanje, odzivanje

The role of telecommunication service providers in coping with DDoS attacks

DDoS attacks (distributed denial of service attacks) are among the most widespread cyber threats posing a high risk to a continuous operation of information systems. An important role in the response system is played by Internet infrastructure managers who control the Internet traffic. A literature review indicates a lack of scientific research on challenges and effective approaches in dealing with DDoS attacks, especially through the prism of telecommunications service providers. In the paper we study the trends in the field of DDoS attacks and the role of telecommunications service providers in dealing with this type of the threat. To determine the state of DDoS attacks in Slovenia and analyze the role of telecommunication service providers in responding to DDoS attacks, we conducted structured interviews among experts. The results show that telecommunication service providers in Slovenia most often face small-scale volumetric DDoS attacks exploiting transport layer protocols. Telecommunication service providers take due care to control and restrict the Internet traffic, when needed. They also provide additional anti-DDoS services but lack more advanced security mechanisms.

Keywords: DDoS attack, telecommunication service providers, cyber security, detection, response

1 UVOD

Pogostost in sofisticiranost kibernetskih napadov se je v zadnjih letih močno povečala, še zlasti v organizacijskem okolju [1]–[3]. Med najbolj razširjene kibernetske napade sodijo napadi za zavrnitev storitev (angl. *Denial of Service* – DoS). Napadi DoS so oblika kibernetske kriminalitete, ki napadejo računalnike ali omrežne vire s toliko prometa, da legitimnim uporabnikom spleta onemogočijo dostop do omrežnih virov [4]. Značilnost napada DoS je, da napadalec napade načrtovano žrtev (strežnik) in ji onemogoči pretok internetnega prometa oziroma storitev, ki so na voljo uporabnikom. Nadgradnja napadov DoS so napadi za porazdeljeno zavrnitev storitve (angl. *Distributed Denial of Service*), znani kot DDoS.

Kljub razširjenosti in aktualnosti tovrstne grožnje empiričnih raziskav, ki bi celostno proučile napade DDoS v Sloveniji in vlogo ponudnikov telekomunikacijskih storitev v sistemu, odzivanja ne zasledimo. Večina prispevkov, ki obravnavajo napade DDoS, je strokovnih, pri tem pa so pogosto teoretične narave (npr. [5], [6]) ali pa poročajo o pogostosti in razširjenosti kibernetskih napadov na globalni ravni (npr. [7]–[10]). Tudi na ravni Slovenije obstajajo poročila o razširjenosti napadov DDoS (npr. [1]), vendar temeljijo

Prejet 23. avgust, 2020
Odobren 29. oktober, 2020

izključno na prijavljenih incidentih, medtem ko ne dajejo vpogleda v značilnosti napadov DDoS ter trende na področju njihovega razvoja in obvladovanja. Strokovni prispevki pogosto vključujejo tudi analize varnostnih ukrepov. Med tovrstne sodi npr. poročilo o učinkovitosti zaščitnih ukrepov na osnovi analize 900 napadov DDoS med letoma 2015 in 2017, in sicer na področju bančništva, e-nakupovanja in telekomunikacij ter v drugih sektorjih [11].

Tako kot strokovna literatura tudi znanstvena (npr. [12]–[14]) ne ponuja odgovora o vlogi ponudnikov telekomunikacijskih storitev. Slednji predstavljajo prvo obrambno linijo pred napadi DDoS. V tem prispevku se bomo tako osredotočili na njihovo vlogo pri odkrivanju, preprečevanju in obvladovanju napadov DDoS. Z namenom ugotavljanja trenutnega stanja v Sloveniji smo izvedli strukturirane intervjuje s strokovnjaki za varnost, ki so zaposleni pri največjih slovenskih ponudnikih telekomunikacijskih storitev.

Prispevek je strukturiran, kot sledi. V naslednjem poglavju predstavimo napade DDoS, v tretjem poglavju predstavljamo varnostne ukrepe, povezane z napadi DDoS. V četrtem poglavju umestimo vlogo ponudnikov telekomunikacijskih storitev k obvladovanju napadov DDoS, v petem poglavju pa predstavimo metodologijo zbiranja podatkov. V šestem poglavju so predstavljeni rezultati, o katerih razpravljamo v sedmem poglavju. V zadnjem poglavju podajamo zaključek.

2 SPLOŠNO O NAPADIH DDOS

Napad DDoS je zlonamerni poskus prekinitve normalnega prometa ciljnega strežnika, storitve ali omrežja, tako da je okoliška infrastruktura preplavljena z internetnim prometom [5]. Je usklajen napad, ki poteka z uporabo velikega števila okuženih gostiteljev [15]. Tovrstni napadi svoj cilj uresničijo z uporabo več kompromitiranih računalniških sistemov kot virov napadalnega prometa, pri čemer je lahko tarča en sam spletni strežnik, lahko pa celotna internetna povezava določene organizacije [15]. Zlorabljene naprave lahko vključujejo računalnike ali druge omrežne vire, kot so naprave interneta stvari (angl. *Internet of Things* – IoT).

Napade DDoS poznamo v različnih oblikah, te so odvisne od tega, kaj predstavlja tarčo in kaj je cilj onemogočiti. Obstajajo različni pristopi k razvrščanju napadov DDoS. Po Kumarju [4] lahko napade DDoS na splošno razvrstimo v tri glavne kategorije: volumetrične napade (angl. *volumetric attacks*), napade na povezljivost (angl. *connection state attacks*) in napade aplikacijskega sloja (angl. *application-layer attacks*). Volumetrični napadi so usmerjeni v razpoložljivost virov z vbrizgavanjem velikega obsega določene vrste prometa. Napadi so običajno usmerjeni na spletne strani (zlasti na spletu, spletne igre na srečo), podjetniške internetne povezave, ponudnike gostovanja in ponudnike oblakov. Napadi na povezljivost povzročijo, da je protokol ciljnih virov prepoln oziroma nedosegljiv. Napadi navadno merijo na požarne zidove, sisteme za preprečevanje vdorov, požarne zidove spletnih aplikacij in podatkovne baze. Napadi aplikacijskega sloja so prikrite narave in se včasih imenujejo »nizki in počasni«, saj merijo na aplikacije kritične infrastrukture, npr. vlad, podjetij, bolnišnic [16].

Napad DDoS se navadno izvede v štirih korakih: v prvem koraku gre za skeniranje celotnega omrežja, za identifikacijo ranljivih naprav, vstopnih vrat, gostiteljev in podobno. V drugem koraku gre za najdbo ranljivega gostitelja, ki se ga okuži z zlonamerno programsko opremo. V tretjem koraku napadalec okuži gostitelje, da ustvarijo osnovo za učinkovit napad. V četrtem, zadnjem koraku okužene naprave sprožijo napad [15].

Sistemi oziroma naprave, ki jih napadalec okuži z zlonamerno programsko opremo, postanejo orodje za izvedbo napada. Takšne naprave imenujemo tudi »boti« oziroma »zombiji«. Omrežje, ki ga sestavljajo okužene naprave, se imenuje botnet. Ko je botnet vzpostavljen, lahko napadalec usmerja naprave z upravljanjem na daljavo, in sicer s pošiljanjem posodobljenih navodil vsakemu botu. Ukazi do vseh okuženih naprav ustvarijo pakete z veliko količino prometa in napadajo ciljni strežnik. Strežnik se ne more hitro odzvati na tako veliko količino paketov, kar pomeni, da s tem izčrpa svoje vire in se neha odzivati [17]. Ker je vsak bot na neki način »zakonita« naprava oziroma del interneta, je ločevanje med napadalnim prometom od običajnega precej zahtevno [5].

Napadalec lahko prek napada DDoS močno poslabša kakovost ali povsem prekine omrežno povezavo. V veliko primerih se izkorišča lažni IP. Napadalec v tem primeru ugotovi in posnema IP-naslov vira, ki pošilja podatke [18]. Glavni namen napada DDoS je, da žrtev ne more uporabljati omrežnega vira. V večini scenarijev se izvedejo napadi na spletne strežnike, centralno-procesne enote (CPU), pomnilnike in druge omrežne vire. Napad se lahko izvede tudi v oblačnem sistemu tako, da obremeni virtualne strežnike in bistveno zmanjša zmogljivost storitev v oblaku [19].

3 VARNOSTNI UKREPI

Zaradi pogostosti in destruktivnosti napadov DDoS so varnostni inženirji dejavno usmerjeni v razvoj zaščitnih mehanizmov [20]. Obstaja več razlogov, zakaj je napad DDoS težko zaznati in ublažiti. Vsak škodljivi paket je namreč sam po sebi legitimna transakcija. Legitimne transakcije je mogoče zlorabiti tako, da se izvajajo tako pogosto, dokler strežniku ne zmanjka zmogljivosti. Poleg tega ima vsak računalnik v napadu DDoS pogosto enkraten IP-naslov in poskuša v vsakem od svojih tisoč zahtevkov uporabiti drugačen ponarejeni IP-naslov in različne informacije v glavi, zato je težko identificirati in blokirati en sam vir napada [21].

Glede na to, da poznamo različne vrste napadov DDoS, se morajo tudi varnostni ukrepi temu prilagoditi. Za obrambo pred napadi DDoS na ravni aplikacije se uporabljajo orodja, kot so *Kill-Bots*, analize *Backscatter* in eksperimentalne ocene govornega nabora. Za zaščito

spletnih strežnikov pred napadi DDoS je učinkovito orodje *Kill-Bots* [22]. Z zagotavljanjem overjanja *Kill-Bots* uporablja grafične teste, ki se nekoliko razlikujejo od drugih sistemov z uporabo grafičnih testov. Ko *Kill-Bots* prepozna škodljive naprave (bote), grafične teste izključi in blokira njihov promet [22].

Naslednja je rešitev za napade na strežnike domenskih imen (angl. *Domain Name Server* – DNS). Rezultati kažejo, da pristop DNAME, ki ga predlaga Wang [23], predstavlja učinkovitejšo rešitev z manj lažnimi pozitivnimi rezultati na usmerjevalniku žrtve in naredi manj škode v omrežju zaradi proaktivnega obrambnega pristopa. DNAME signalizira direktivo o preusmeritvi domene rekurzivnim razreševalcem, ki svoj nadaljnji poizvedovalni promet preusmerijo na preusmeritvene domene [23].

Med pomembne korake za zaščito pred napadi DDoS prav tako sodijo: (a) razpršeni obrambni mehanizmi; (b) inteligentno upravljanje prometa; (c) zbiranje podrobnih informacij o napadu; (d) ocena napada; podpora za postopno uvajanje rešitev [20]. Poleg omenjenih se v literaturi omenjajo tudi druge metode za zaščito pred napadi DDoS, kot so: postavljanje pravilnih omejitev pretokov prometa, na osnovi katerih se lahko preprečijo morebitne zavrnitve legitimnega prometa [15]; usmerjanje paketov prek TCP-vrat [24]; uporaba varnosti prenosnega sloja (angl. *Secure Socket Layer* – SSL), ki je pogosta metoda spletnega šifriranja in se uporablja v protokolu HTTP [21]; in obramba *D-Ward*, ki je nameščena na mejnem usmerjevalniku z namenom, da bi zaznala napad [20].

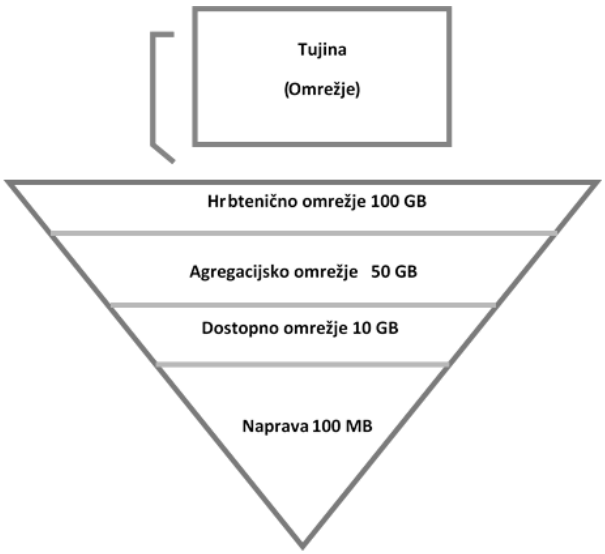
Navedeni ukrepi so večinoma zasnovani za nadzor in filtriranje prometa ter poskušajo slediti zlonamernemu IP-naslovu. Omenjeni procesi lahko močno prispevajo k učinkovitemu obvladovanju napadov DDoS. Napadov sicer ni mogoče odpraviti, mogoče pa jih je zmanjšati.

4 VLOGA PONUDNIKOV TELEKOMUNIKACIJSKIH STORITEV PRI OBVLADOVANJU NAPADOV DDOS

Telekomunikacijski sistemi so osnova digitalizacije in v sodobnem svetu zelo pomemben dejavnik pri vzpostavljanju celotnega omrežnega sistema. Ti so ključni vmesnik med uporabnikom in omrežjem ter kritična točka z vidika varnosti. Zaradi svoje vloge v omrežju jih umeščamo pod kritično infrastrukturo, saj lahko njihova odpoved ali oslabljeno delovanje povzroči veliko škodo uporabnikom in gospodarstvu ter nasploh vpliva na normalno delovanje države [25].

Najpogostejša kibernetska grožnja, s katero se soočajo ponudniki telekomunikacijskih storitev, so ravno napadi DDoS [17]. Poleg ustrezne zaščite lastne infrastrukture je njihova naloga tudi pomagati strankam, ki so tarča teh napadov [25].

Omrežje oziroma pot od ponudnika telekomunikacijske storitve do uporabnika si je mogoče predstavljati kot obrnjen trikotnik (slika 1). Prvi, najširši del predstavlja hrbtenično omrežje, ki ima dostop do interneta iz tujine s količino podatkov, na primer 100 GB. S hrbteničnega dela se omrežje seli proti naročniku in postaja manj zmogljivo oziroma ima slabše značilnosti, količina dostopnih podatkov tega sloja pa je 50 GB (agregacijsko omrežje). Zadnji, najmanj zmogljivi sloj predstavlja 10 GB dostopnega omrežja (to je tako imenovana centrala oziroma zadnji element omrežja do uporabnika). Iz tega sloja gre promet do stranke s količino, ki jo ima stranka naročeno. Če je stranka naročila na primer 100 Mbit/s in na teh 100 Mbit/s napadalec doda še 5 Gbit/s, usmerjevalnik zavrne vse, kar presega 100 MB/s in do stranke še naprej pošilja le 100 MB/s oziroma s tolikšno hitrostjo, kot jo ima stranka naročeno.



Slika 1: Shema pretoka internetnega prometa do uporabnika.

Obstajajo trije pristopi k obravnavanju napadov DDoS, ki jih uporablja vsak ponudnik telekomunikacijskih storitev: nadzor internetnega prometa (nadzor), odkrivanje in odzivanje [15]. Z nadzorom se spremljajo in zbirajo potrebne informacije o stanju omrežja na različnih točkah v omrežju. S pomočjo nadzora se lahko zaznajo določene anomalije ali nepravilnosti znotraj omrežja. Za pravočasno zaznavanje napadov DDoS je zelo pomembno, da se nadzira oziroma spremlja tako zunanji kot tudi notranji promet. V fazi odkrivanja ponudniki telekomunikacijskih storitev poskušajo prepoznati katerokoli zlorabo ali nepravilnost v delovanju omrežja. V tem koraku lahko tudi poskusijo ustaviti grožnjo, če je le mogoče. Običajen odziv ponudnika telekomunikacijskih storitev poteka z dvema osnovnima komponentama, tj. pasivno in aktivno komponento. Pasivna komponenta je sestavljena iz niza postopkov, ki vključujejo pregled konfiguracijskih datotek sistema za odkrivanje neprimernih nastavitev, pregled datotek z gesli za odkrivanje neprimernih gesel in pregled drugih sistemskih področij za odkrivanje nepravilnosti. Aktivna komponenta je sestavljena iz

drugega sklopa postopkov – odziva se na znane metode napada in ustvari sistemske odzive. Na sumljive dogodke se lahko odzove na več načinov, vključno s prikazom opozorila, beleženjem dogodka ali obveščanjem skrbnika [15].

Ponudniki telekomunikacijskih storitev prek svojih nadzornih centrov izvajajo 24-urni nadzor, spremljajo, kako poteka legalni promet in analizirajo nelegalnega. Pri napadih DDoS je razvidno, da gre za huda odstopanja pri pretoku prometa zaradi povečane količine prispelih podatkov. Ta anomalija se analizira z namenom, da se točno definira, za katero vrsto incidenta gre. Ob zaznavi napada pomagajo orodja, ki filtrirajo internetni promet. Nelegalni promet preusmerijo na drugo napravo za čiščenje. S tem lahko zaščitijo stranko in ublažijo ali celo povsem preprečijo napad [26]. Orodja za spremljanje so sposobna zagotoviti tudi statistiko, poročila in grafično predstavitev podatkov o internetnem prometu.

Pomembno orodje za odkrivanje potencialnih anomalij je paketni analizator ali »*sniffer*«, ki pri zbiranju podatkov analizira omrežje med različnimi omrežnimi napravami in končnimi uporabniškimi sistemi. Ko tokovi podatkov tečejo po omrežju, analizator zajame vsak paket in po potrebi dekodira surove podatke paketa ter prikaže vrednosti različnih polj v paketu in analizira njegovo vsebino v skladu z ustreznimi RFC (angl. *Requests for Comment*) ali drugimi specifikacijami. Med analizo lahko »*snifferji*« naletijo na pakete, ki ne bi smeli biti del podatkov, ali pakete, ki vsebujejo podatke o vdoru, virusih, napačnem vedenju in druge nepravilnosti [27].

5 VLOGA PONUDNIKOV TELEKOMUNIKACIJSKIH STORITEV PRI OBRAVNAVANJU NAPADOV DDOS V SLOVENIJI

Da bi pridobili vpogled v prakso soočanja z napadi DDoS v Sloveniji, smo izvedli kvalitativno raziskavo o vlogi ponudnikov telekomunikacijskih storitev pri obravnavanju napadov DDoS v Sloveniji. V raziskavi smo izvedli strukturirane intervjuje s strokovnjaki iz prakse na področju upravljanja informacijskih tehnologij in informacijske varnosti, ki so zaposleni v največjih telekomunikacijskih podjetjih v Sloveniji. Vprašanja so bila osredotočena na to, kako se ponudniki telekomunikacijskih storitev soočajo z napadi DDoS in kakšne so njihove izkušnje iz prakse: s kakšnimi metodami, orodji in mehanizmi odkrivajo napade DDoS, kateri varnostni ukrepi se uporabljajo in kako poteka sodelovanje s strankami v takih primerih.

5.1 Metoda

Za potrebe raziskave, ki je potekala v obliki intervjujev, smo pripravili vprašalnik, ki je vseboval 20 vprašanj odprtega tipa. Z intervjuji smo ugotavljali mnenja in izkušnje respondentov pri odkrivanju in preprečevanju napadov DDoS v Sloveniji. Vprašanja, zastavljena v intervjuju, smo oblikovali skladno z ugotovitvami iz teoretičnega dela, da bi preverili, kako se tovrstna spoznanja odražajo v praksi v slovenskem prostoru. Zaradi preglednosti so vprašanja s povzetki odgovorov predstavljena med rezultati (poglavje 6).

Podatki so bili zbrani z neposrednimi intervjuji, ki so bili posneti (avdioposnetek), odgovore respondentov pa smo nato transkriptirali. Na osnovi transkriptov smo primerjali odgovore ter iskali podobnosti in razlike v ugotovljenih stališčih. Rezultati so prestavljeni v povzeti in združeni obliki. Sodelovanje v intervjuju je bilo prostovoljno, respondentom pa smo zagotovili anonimnost pri objavi rezultatov. Pred izvedbo intervjujev smo od vseh respondentov pridobili soglasje za izvedbo intervjuja in obdelavo odgovorov. Intervjuvali smo sedem strokovnjakov iz prakse, ki so zaposleni na področju upravljanja informacijskih tehnologij in informacijske varnosti pri štirih različnih ponudnikih telekomunikacijskih storitev v Sloveniji. Intervjuji so bili izvedeni v obdobju od julija do avgusta 2019. Prvi intervju je bil izveden dne 25. 7. 2019, zadnji intervju pa dne 23. 8. 2019. Intervjuji so v povprečju trajali 35 minut, izvajali pa so se v poslovnih prostorih intervjuvane osebe.

5.2 Vzorec

Za izvajanje intervjuja smo izbrali namenski vzorec. Respondenti so bili izbrani na osnovi delovnega mesta. Ključno je bilo, da so respondenti zaposleni na področju upravljanja informacijskih tehnologij in informacijske varnosti pri ponudnikih telekomunikacijskih storitev v Sloveniji. Na osnovi omenjenih meril je bilo k sodelovanju skupaj povabljenih devet strokovnjakov, sedem se jih je odzvalo na vabilo (80-odstotna stopnja odzivnosti).

Vzorec vključuje sedem respondentov, pri čemer je bil z vsakim posebej opravljen individualni pogovor. Vsi respondenti so zaposleni v podjetjih za telekomunikacijske storitve. Intervjuji so bili opravljeni z:

- dvema specialistoma na področju informacijsko-komunikacijskih tehnologij,
- inženirjem za IT-sisteme in inženirjem za IP/MPLS,
- zaposlenim v 24-urnem nadzornem centru,
- vodjo centra za informacijsko varnost in
- direktorjem operativno-storitvenega centra.

Vsi respondenti imajo večletne izkušnje na področju upravljanja informacijskih tehnologij in informacijske varnosti z delovno dobo od 5 do 22 let v podjetjih za telekomunikacije (T2, A1, Telekom in Telemach). Starost respondentov je od 33 do 53 let, vsi respondenti so bili moškega spola z dokončano izobrazbo diplomiranega inženirja s področja elektrotehnike ali računalništva in informatike.

6 REZULTATI

V tem poglavju predstavljamo povzetke odgovorov respondentov na 20 vprašanj, na osnovi katerih so bili izvedeni intervjuji.

S kakšnimi kibernetskimi grožnjami se glede na vaše izkušnje najpogosteje soočajo ponudniki telekomunikacijskih storitev? Odgovori respondentov na to vprašanje so bili zelo enotni, vsi so namreč povedali, da se pri svojem delu najpogosteje soočajo z napadi DDoS, posebno volumetričnimi. Pogosti so še vdori v elektronske poštne nabiralnike, vdori v strežnike telefonije, »phishing« prevare ter neželena pošta, prestrezanje komunikacij, kraja podatkov in izsiljevanje.

Kako pogosti so po vašem mnenju napadi DDoS v Sloveniji? Pri tem vprašanju so respondenti poudarili, da je treba razlikovati med napadi DDoS večjega in manjšega obsega. Manjši napadi DDoS se lahko dogajajo na tedenski ravni, večji pa so zelo redki.

Iz katerih držav po vašem mnenju najpogosteje izvirajo/prihajajo napadi DDoS? Zakaj menite, da je tako? Respondenti so izrazili stališče, da je izvor napadov DDoS težko ugotoviti, saj so običajno visoko distribuirani, kar pomeni, da zlonamerni promet prihaja z različnih kontinentov hkrati. Če analiziramo vire, vidimo, da je omrežje botov dobro organizirana infrastruktura, ki omogoča napade DDoS. Zelo malo jih je iz »izoliranih virov«. Večji napadi DDoS so organizirani bodisi samostojno, kar pomeni, da oseba, ki to izvaja, že ima svojo infrastrukturo (določeno število uporabljenih končnih naprav, iz katerih se pošilja promet), ali pa, da se napad izvaja prek kupljene programske opreme za oblikovanje »botov«. Znano je tudi, da je napade DDoS mogoče naročiti na temnem spletu. Opazimo lahko, da glavnina prometa izvira iz največje prepustnosti v infrastrukturi, se pravi od tam, kjer je največ zmogljivosti virov, kot so Azija, ZDA, Velika Britanija, Francija, Rusija, Ukrajina in Afrika. Promet dejansko prihaja z vsega sveta, zato je težko reči, da je osredotočen na posamezno območje ali državo.

Kdo so po vašem mnenju najpogosteje storilci napadov DDoS in kakšni so njihovi motivi? Respondenti navajajo, da je zelo težko odkriti storilce in njihove vzgibe za taka dejanja. Navajajo pa, da so to lahko kriminalne združbe, konkurenca in državno podprte skupine, največkrat pa gre za skupine, ki se strokovno ukvarjajo z napadi DDoS, pisanjem in preverjanjem programov/skript. Motivi so različni, od premoženjske koristi, dokazovanja, kraje identitete, kraje podatkov in pridobivanja konkurenčne prednosti do onemogočanja delovanja kritične infrastrukture ali pridobivanja geopolitičnih prednosti.

Kdo so po vašem mnenju najpogostejša tarča napadov DDoS in zakaj? Respondenti so poudarili, da so to večinoma poslovne stranke v okviru bančništva, zavarovalnic, velikih institucij. Tarče so pogosto tudi individualni/fizični uporabniki, ki so odvisni od spletnih strani/storitev, posamezniki, ki se ukvarjajo s kriptovalutami itd.

Katere so glede na vaše izkušnje najpogostejše oblike napadov DDoS v Sloveniji? Ali menite, da se narava teh napadov razlikuje v primerjavi z izkušnjami v tujini? Zakaj da/ne? Pri tem vprašanju respondenti navajajo, da je najpogostejša oblika napada DDoS volumetrični napad. Redkeje zaznavamo napade DDoS, ki merijo na varnostne ali funkcionalne luknje v neki programski opremi. Navadno se s točno določeno količino zahtevkov povzroči prekomerna poraba, izčrpavanje virov. Promet je običajno v Mbit/s, Kbit/s, kar povzroči, da so tisti strežniki v ozadju, ki strežejo zahtevke, povsem zasedeni, storitev pa se na ta način onemogoči. Stranki, ki se obrne na ponudnika telekomunikacijskih storitev, se lahko pomaga, in sicer tako, da se ji blokira dohodni promet. To poteka na aplikacijskem sloju. Včasih je treba blokirati kakšen vir, ki pošilja množico DNS-zahtevkov ali NTP-zahtevkov, ki niso legitimni. Poleg navedenih zaznavajo tudi napade DDoS z izčrpanjem virov s ciljem onesposobitve IKT-opreme (IPS/IDS, požarne pregrade, WAF, strežnikov). Vsi respondenti so se strinjali, da je narava napadov DDoS v Sloveniji enaka oziroma podobna kot v tujini.

Kako veliko škodo po vašem mnenju povzročajo napadi DDoS? Respondenti navajajo, da je obseg škode zelo odvisen od tarče. Če gre za poslovno stranko, veliko korporacijo, banko in podobno, lahko onemogočene storitve za določen čas povzročijo ogromno škodo. Škoda je odvisna tudi od tega, koliko časa traja napad DDoS, torej koliko časa je stranka »odrezana« od interneta. Če gre za fizičnega uporabnika, je škoda navadno zelo majhna ali pa je sploh ni, odvisno od tega, s čim se uporabnik ukvarja, in od narave napada (z vidika velikosti in obsega).

Kateri deli omrežja so po vašem mnenju najpogosteje tarča napadov DDoS (protokoli, CPU, oprema ipd.)? Na to vprašanje so respondenti podali različne odgovore: protokoli UDP, strankin računalnik, usmerjevalnik (tega so omenili največkrat). Navedli so tudi, da se meri predvsem na točno določen IP-naslov. Pri poslovnih strankah merijo na strežnike, pri določenih pa tudi na aplikacije. Če gre za volumetrični napad DDoS, se najpogosteje meri na usmerjevalnik ali požarni zid, z namenom, da bi se zrušila povezava. Mogoči so tudi napadi na CPU, internetne povezave (seje), IPS/IDS, požarne pregrade in WAF.

Kako pogosto so po vašem mnenju tarča napadov DDoS fizične stranke? Na to vprašanje so respondenti ravno tako podali različne odgovore. Pet respondentov je kot najpogostejšo tarčo izpostavilo fizične stranke, dva respondenta pa menita, da so pravne osebe pogosteje žrtve napadov, saj so zaradi virov (finančnih in informacijskih), s katerimi razpolagajo, bolj zanimive za storilce.

Kakšno vlogo po vašem mnenju igrajo ponudniki telekomunikacijskih storitev pri odkrivanju in preprečevanju napadov DDoS, koliko so pomembni v teh primerih? Pri tem vprašanju so vsi respondenti izrazili enako stališče, in sicer, da ponudniki telekomunikacijskih storitev igrajo zelo pomembno

vlogo pri odkrivanju in preprečevanju napadov DDoS, saj so edini, ki prek nadzora zaznajo napad in lahko ukrepajo tako, da obvestijo stranko, zablokirajo njen promet in ji pomagajo oziroma svetujejo pri nadaljnjih korakih.

Na kakšen način ponudniki telekomunikacijskih storitev (s kakšnimi ukrepi, mehanizmi, orodji) glede na vaše izkušnje odkrivajo napade DDoS? Respondenti so pojasnili, da zaznavanje in blaženje napadov DDoS izvajajo z namensko programsko in strojno opremo. Večina dogodkov se ugotavlja prek 24-urnega nadzora omrežja. Vsak DDoS povzroča anomalijo v prometu, v številu sej, količini prometa itd. Torej vsak, ki izvaja nadzor, v primeru nenormalnega odstopa takoj razbere, da gre za napad. Napad DDoS nikoli ni običajen oziroma normalen promet, temveč je zmeraj drugačen, in zato obstajajo namenske naprave, ki odstopanja zaznavajo z analiziranjem prometa ter prometnih tokov med viri in žrtvami. Eden izmed znanih ukrepov je t. i. black holing, kar pomeni blokiranje dohodnega prometa v smeri proti stranki. Tukaj obstaja nekaj kolateralne škode. Za slovenski prostor je to še sprejemljivo, saj deluje do 99,5 odstotka natančno glede na to, da je večina napadov DDoS usmerjenih iz tujine v Slovenijo. Napadov znotraj Slovenije ali istega ponudnika skorajda ni. Drugi mehanizem je eno raven višje, to pa predstavlja t. i. data scraping in pomeni filtriranje dohodnega prometa. To sta dva mehanizma, s katerima ponudniki telekomunikacijskih storitev najpogosteje obravnavajo napade.

Kaj po vaših izkušnjah naredi ponudnik telekomunikacijskih storitev, ko zazna, da se izvaja napad DDoS? Kakšen je postopek/protokol odzivanja in kateri ukrepi se sprožijo? Respondenti so pojasnili, da mora ponudnik telekomunikacijskih storitev najprej zavarovati temeljno omrežje in storitve. Ob večjih napadih DDoS na končne uporabnike, npr. poslovne uporabnike, varnostno-operativni center kibernetske varnosti obvesti uporabnika, ki je tarča napadov DDoS, in skupaj poskusijo ublažiti napad. Hiter odziv in ustrezna podpora strokovnjakov, tako na strani ponudnika storitev kot uporabnika, sta ključna za minimiziranje škode napadov DDoS. Sicer pa so v sklopu sistemov, ki jih telekomunikacijski operaterji uporabljajo za upravljanje neprekinjenega poslovanja (SUNP) in vodenja varovanja informacij (SVVI), že definirani protokoli, vezani na razpoložljivost, celovitost in zaupnost komunikacij oziroma informacij.

Na kakšen način glede na vaše izkušnje ponudniki telekomunikacijskih storitev preprečujejo napade DDoS? Kakšni so varnostni ukrepi in mehanizmi? Respondenti navajajo, da je zelo težko preventivno ukrepati proti napadom DDoS, zlasti če govorimo o volumetričnih napadih. Obstajajo storitve (programska oprema), ki omogočajo filtriranje prometa. Storitev ni brezplačna, vsaka stranka pa jo lahko naroči. Obstaja še metoda t. i. »clean pipe« za filtriranje zlonamernega od legalnega internetnega prometa. Med preventivo umeščajo tudi nadzor nad omrežjem. Pri tem dodajajo, da je pomemben korak pri preventivi ozaveščanje strank o kibernetskih grožnjah.

Kaj lahko po vašem mnenju ponudnik telekomunikacijskih storitev stori, da zavaruje svoje stranke? Respondenti navajajo, da je težko nadzirati promet za vsako stranko posebej. Zato jih ozaveščajo, nadgrajujejo njihovo opremo, dejavno menjajo lastno opremo, izvajajo nadzor nad sumljivimi dogajanji. Ponudnik telekomunikacijskih storitev lahko za zaščito svojih uporabnikov ponudi preventivne storitve zaznavanja in blaženja napadov DDoS, ki niso osnovne storitve – pri tem uporabnike integrirajo v svoj celoviti sistem anti-DDoS, ki ga za vsakega uporabnika deloma prilagodijo, tudi licenčno, zato to ni osnovna storitev (je plačljiva).

Kakšna je po vaših izkušnjah škoda napadov DDoS za ponudnike telekomunikacijskih storitev in kakšna za stranko? V odgovorih na to vprašanje so respondenti izrazili različna stališča, nekateri so poudarili, da imajo lahko ponudniki telekomunikacijskih storitev večjo škodo, saj v primeru velikega napada DDoS lahko zablokirajo promet tudi drugim uporabnikom ter celo poškodujejo strežnike in infrastrukturo. Drugi so odgovorili, da je škoda večja za stranke, ker napadi DDoS običajno niso tako močni, da presežejo promet, s katerim razpolaga en ponudnik telekomunikacijskih storitev, zato ponudnik navadno nima velike škode. Če je ena fizična povezava prekinjena, jih imajo še vedno več v ozadju. Napad DDoS bi moral biti zelo obsežen, da bi ponudniku telekomunikacijskih storitev povzročil škodo. Več težav je bilo pred uporabo orodja za nadzor NFSIN. S tem orodjem lahko ugotovijo, na kateri IP-naslov dospeva več prometa ali pa več paketov. Respondenti so pojasnili še, da je bil v preteklosti (leta 2014) sicer zaznan tako velik napad, da so tudi operaterji občutili težavo, kar pomeni, da je napolnil hrbtenične povezave. V povprečju pa je škoda relativno majhna, saj imajo ponudniki veliko dostopnih točk do interneta prek številnih redundantnih povezav. Glavnino škode zatorej večinoma občuti naročnik, ki je običajno odvisen od le ene povezave do interneta prek svojega operaterja.

Kateri so po vašem mnenju najpomembnejši varnostni ukrepi, s katerimi bi stranke morale biti seznanjene, da se zaščitijo pred napadi DDoS? Kateri izmed teh ukrepov je po vašem mnenju najpomembnejši? Respondenti navajajo, da so za ustrezno zaščito pred napadi DDoS pomembni dovolj zmogljiva IKT-oprema, dovolj zmogljiva internetna povezava in uporaba storitve blaženja napadov DDoS. Za uspešno preventivno ukrepanje bi morali uporabniki telekomunikacijskih storitev poskrbeti, da je oprema pravilno konfigurirana; da je programska oprema redno posodobljena; ter da se za storitev in opremo izvede penetracijski test, s katerim se preveri, ali so na obeh straneh naredili vse za zaščito. Tako se lahko izognejo vdorom ali napadom DDoS za izkoriščanje ranljivosti na aplikacijskem sloju.

Na kakšen način glede na vaše izkušnje ponudniki telekomunikacijskih storitev obveščajo in seznanijo svoje stranke, kako poteka sodelovanje, ali stranke upoštevajo navodila in znanje, ki so ga prejeli? Navajajo, da je postopek tak, da nadzorni center ali podpora pokliče stranko in ji obrazloži, kaj se je zgodilo. Hkrati stranko obvestijo, da ji bodo onemogočili dostop do spleta za določeno časovno obdobje, če je treba. Stranko poskušajo seznaniti s to vrsto napada in ji svetujejo, naj se obrne na SI-CERT za več informacij.

Ali menite, da so stranke dobro seznanjene z varnostnimi ukrepi? Pri tem vprašanju so respondenti poudarili, da se soočajo z dvema vrstama odzivov. Poslovne stranke se nevarnosti navadno bolj zavedajo in so bolj ozaveščene ter ne nazadnje bolj tehnično usposobljene, zato določene ranljivosti odpravijo same. Pri fizičnih osebah oziroma navadnih uporabnikih pa je velikokrat težava nevednost, zato se pogosto ne odzovejo ustrezno oziroma ne upoštevajo navodil. Poslovne stranke so po njihovih izkušnjah bolj odzivne.

Ali menite, da ponudniki telekomunikacijskih storitev v Sloveniji ustrezno skrbijo za zaščito pred napadi DDoS? Kje so po vašem mnenju pomanjkljivosti in kaj bi lahko izboljšali? Respondenti navajajo, da ponudniki telekomunikacijskih storitev v Sloveniji zelo dobro skrbijo za svoje stranke ter da po potrebi zelo korektno in strokovno sodelujejo med seboj. Kot pomanjkljivosti navajajo predvsem pomanjkanje finančnih virov, kar jim onemogoča uporabo boljše in dražje opreme. Možnosti izboljšav naj bi bile v nadzoru, filtriranju prometa, zapiranju določenih vrat in podobnih tehničnih ukrepih.

Kako ocenjujete razvoj tovrstnih groženj v prihodnje in kakšna so vaša pričakovanja? Respondenti so izrazili stališče, da bo s širjenjem digitalizacije in selitve dejavnosti na splet naraščalo tudi število tovrstnih groženj. Vsi napadi, ki jih trenutno zaznavajo, so na IPv4, kjer so zaščite precej dobro urejene, zato je mogoče grožnjo hitro odkriti, jo omejiti in tudi odpraviti, s čimer zaščitijo uporabnike. Narašča pa uporaba IPv6, kjer so varnostni mehanizmi za zdaj nekoliko slabši, tudi požarne pregrade, ki skrbijo za blokade, so slabše konfigurirane. Težava je tudi, da napadalci ne potrebujejo posebnega znanja, saj je škodljivo programsko opremo, s katero se lahko izvede napad DDoS, na nelegalnem trgu mogoče dobiti po izjemno nizki ceni. Po mnenju respondentov pa je mogoče v prihodnje pričakovati tudi, da bodo na voljo enostavne aplikacije, ki bodo storilcem omogočile sprožitev napada zgolj z enim ukazom/klikom.

Povzamemo lahko, da so respondenti pri večini vprašanj delili enaka oziroma dokaj podobna stališča, zgolj pri nekaterih so se njihova mnenja razlikovala. To lahko pripišemo razlikam v izkušnjah in naravi dela.

7 RAZPRAVA

Na osnovi intervjujev s strokovnjaki iz prakse na področju upravljanja informacijskih tehnologij in informacijske varnosti, zaposlenimi pri ponudnikih telekomunikacijskih storitev, smo ugotovili, da se lahko napadi DDoS učinkovito zaznajo s pomočjo nadzora prometa, s katerim se spremlja kontinuiteta porabe internetnega prometa pri določeni stranki, in opazijo odstopanja oziroma povečanje količine prometa (»špice«). Po mnenju respondentov javnost oziroma uporabniki telekomunikacijskih storitev sicer še niso zadostno seznanjeni s problematiko napadov DDoS, zato je vloga telekomunikacijskih operaterjev pri zaznavanju in preventivi napadov še toliko bolj pomembna, kar potrjujeta tudi [15] in [25]. Tu navajajo, da imajo ponudniki telekomunikacijskih storitev velik vpliv in pomen pri odkrivanju in preprečevanju napadov DDoS, saj imajo pregled nad strankinim internetnim prometom in razpolagajo z določenimi orodji za nadzor in obvladovanje tovrstnih napadov. Tudi raziskava, izvedena v različnih industrijskih panogah o ukrepanju organizacij proti napadom DDoS [14], je pokazala, da se v praksi borba proti napadom DDoS večinoma prenaša na ponudnike internetnih storitev.

Rezultati nakazujejo, da uporaba varnostnih mehanizmov in načinov ukrepanja v primerih uresničenih volumetričnih napadov DDoS ne sledi razvojnim trendom. Čeprav se intenzivno razvijajo nove rešitve in se v praksi že uporabljajo napredne metode, jih slovenski ponudniki telekomunikacijskih storitev še ne uporabljajo. Investicije v nadgradnjo varnostnih mehanizmov, procesov in orodij so za zdaj močno omejene, primarno zaradi finančne zahtevnosti. Pretežno se ponudniki zato zanašajo na klasične pristope, kot sta spremljanje količine internetnega prometa in začasno blokiranje storitev, če je uporabnik žrtev napada DDoS. Kot pomembno lahko poudarimo ugotovitev, da so v Sloveniji pogostejši napadi na fizične uporabnike telekomunikacijskih storitev kot na poslovne uporabnike. Med najranljivejše sodijo predvsem tisti, ki se ukvarjajo z digitalnimi storitvami, kot so kriptovalute in igranje iger na spletu. Sočasno s tem ugotavljamo, da uporabniki niso dovolj ozaveščeni o problematiki napadov DDoS, preventivnih ukrepih pri uporabi spleta in načinih primernega odzivanja.

Ker so posledice napadov DDoS največje za uporabnike, ki nimajo zadostnega tehničnega znanja za preventivo napadov, je vloga ponudnikov telekomunikacijskih storitev pri preprečevanju in zaznavanju napadov še toliko večja. Trenutno njihovi varnostni sistemi zadostujejo za obvladovanje tovrstnih groženj, vendar bo s pričakovanim razvojem kibernetskih napadov v prihodnje treba zagotoviti nadgradnjo celotnih procesov pri zagotavljanju kibernetske varnosti, saj je naša raziskava pokazala, da potrebujejo boljša orodja oziroma procese. Zaenkrat so ustrezno pripravljeni zgolj na določene vrste napadov DDoS, kot so volumetrični. V prihodnje se bo treba osredotočiti na implementacijo in

testiranje novih metod. Pripraviti se je treba na širši prevzem IPv6-protokola, ki deluje drugače kot trenutno razširjeni IPv4-protokol. Ta je sicer že nekoliko zastarel, ampak bolj varen kot IPv6, saj ima dobro razvite varnostne mehanizme, ki jih IPv6 še nima. Splošna analiza trendov in razvoja sistemov anti-DDoS sicer kaže, da strokovna javnost investira v razvoj novih metod, algoritmov in drugih rešitev, ki pa za zdaj ostajajo v fazi preverjanja ali razvijanja. Vendar so to dobri predlogi z obetavnimi preliminarnimi rezultati, ki jih je zato treba spremljati in vanje nadalje vlagati, da bi se lahko dokončno vpeljali v prakso. Ne nazadnje pa je zelo pomembno tudi mednarodno sodelovanje tako držav in organizacij kot ponudnikov telekomunikacijskih storitev pri boju proti napadom DDoS, ki so večinoma mednarodne narave.

Na osnovi ugotovitev lahko poudarimo nekatere ključne izzive, ki jih je treba sprejeti v prihodnje. Prvi izziv je povezan z zmanjševanjem razširjenosti napadov DDoS. Četudi so na voljo naprednejše rešitve, uvajanje novih varnostnih ukrepov, mehanizmov in opreme za pravočasno odkrivanje napadov DDoS ne poteka ažurno, saj so storitve za zaščito drage in tako za marsikatero organizacijo, med drugim tudi za ponudnike telekomunikacijskih storitev, prevelika investicija. Trenutno so zato uporabniki večinoma omejeni le na 24-urni nadzor in filtriranje internetnega prometa. Drugi izziv je povezan z izboljšanjem splošne ozaveščenosti in pripravljenosti uporabnikov internetnih storitev na soočanje s tovrstnimi kibernetskimi grožnjami. V prihodnje bo v ta namen potreben razvoj učinkovitejših pristopov k sodelovanju med različnimi deležniki pri ozaveščanju in spodbujanju varno naravnanega pristopa k uporabi interneta. Sicer napadi zaenkrat na ravni Slovenije niso toliko ogrožajoči, saj ne povzročajo velike škode. Smiselno pa je upoštevati dejstvo, da se kibernetske grožnje stalno razvijajo, kibernetski prostor pa je globalen, zato lahko vplive splošnih trendov na področju razvoja kibernetskih napadov v določeni meri pričakujemo tudi v slovenskem prostoru. Tretji izziv je tako zagotavljanje fleksibilnosti na sistemski ravni v odzivanju na razvoj kibernetskih groženj.

7.1 Implikacije

Predstavljeni rezultati so tako rekoč uporabni z več vidikov. Prvič, ponudniki telekomunikacijskih storitev lahko na osnovi ugotovljenih pomanjkljivosti v obstoječih pristopih ter predstavljenih novostih na področju varnostnih ukrepov in pričakovanih izzivih v prihodnje načrtujejo izboljšave ter nadgradnje varnostnih ukrepov in mehanizmov. To je še zlasti pomembno pri pripravi na širšo uporabo IPv6, pri katerem se bodo pojavljala nova tveganja za zlorabe. Drugič, tudi drugi deležniki, ki se na različne načine ukvarjajo z upravljanjem kibernetskih groženj, lahko na osnovi rezultatov o naravi tovrstne grožnje in ranljivosti uporabnikov okrepijo in nadgradijo svoje programe ozaveščanja o preventivnem ukrepanju. Tretjič, za raziskovalno področje so rezultati dobra osnova za nadaljnje in podrobnejše raziskave, ki bi omogočile posploševanje rezultatov na območju Slovenije. Ne nazadnje pa so ugotovitve namenjene tudi splošnim uporabnikom spleta, saj omogočajo vpogled v implikacije napadov DDoS, načine njihovega zaznavanja in primerno ukrepanje, s katerim lahko izboljšajo samozaščitno vedenje.

7.2 Omejitve in nadaljnje delo

Naša raziskava ima določene omejitve, ki jih je pri interpretaciji rezultatov treba upoštevati. Omejitve so povezane predvsem z vzorčenjem in se kažejo pri izvedbi intervjujev. Vzorec ni bil naključen, temveč namenski, respondenti pa so prihajali iz omejenega nabora ponudnikov telekomunikacijskih storitev v Sloveniji. Skladno s tem, ugotovitev ne moremo posploševati na izkušnje vseh slovenskih operaterjev.

Ob upoštevanju stalnega razvoja kibernetskega prostora in s tem povezanih groženj je pomembno nadaljevati dejavno raziskovanje in proučevanje področja napadov DDoS. Smiselno nadaljnje delo bi vključevalo (a) študije primerov, ki bi vključevale sistematično analizo reprezentativnih vzorcev napadov DDoS v zaznavi več ponudnikov telekomunikacijskih storitev, da se ugotovi splošna razsežnost in dinamika tovrstne kibernetske grožnje v Sloveniji; (b) strukturirane raziskave, kot sta pregled in primerjava pristopov k obvladovanju napadov DDoS med reprezentativnim vzorcem ponudnikov telekomunikacijskih storitev v Sloveniji, da se ugotovi razlike in podobnosti ter spodbuja skupni razvoj; (c) analize odzivanja na napade DDoS v Sloveniji v primerjavi s tujimi praksami, da se ugotovi ključne pomanjkljivosti v obstoječih varnostnih sistemih; (d) identificiranje primerov dobrih praks reševanja napadov DDoS na strani upravljavcev kritične infrastrukture iz tujine, in sicer za iskanje potencialnih sistemskih rešitev v Sloveniji.

8 ZAKLJUČEK

Napadi DDoS so aktualna kibernetska grožnja tako za državne in gospodarske organizacije kot tudi za individualne uporabnike spleta. Razvoj grožnje je eksponenten, stalno se namreč pojavljajo novi inovativni načini izvajanja napadov, skladno s tem pa se razvijajo tudi metode in orodja za obrambo proti njim. V tem prispevku smo s pomočjo intervjujev s strokovnjaki iz prakse na področju upravljanja informacijskih tehnologij in informacijske varnosti ugotovili, kakšno vlogo imajo upravljavci internetne infrastrukture pri odkrivanju in preprečevanju napadov ter kako skrbijo za zaščito infrastrukture in uporabnikov. Z reševanjem opisanih izzivov in dejavnim raziskovalnim delom lahko v prihodnje zagotovimo učinkovitejše odzivanje ponudnikov telekomunikacijskih storitev. Pomembno pa je razumeti predvsem to, da upravljavci internetne infrastrukture ne morejo v celoti prevzeti odgovornosti za zaščito in preventivo. Sicer predstavljajo prvo obrambno linijo, vendar morajo za preprečitev napadov z

odgovorno uporabo spleta in upoštevanjem smernic, ki jih podajajo ponudniki telekomunikacijskih storitev in drugi deležniki na področju preprečevanja kibernetskih groženj, poskrbeti tudi uporabniki sami. Ne nazadnje pa je za skupen in usklajen razvoj ter iskanje sistemskih rešitev pomembno ohranjati in krepiti povezave med različnimi upravljavci internetne infrastrukture in drugimi subjekti, ki na nacionalni ravni delujejo na področju kibernetske varnosti.

LITERATURA

[1] SI-CERT, "Poročilo o omrežni varnosti za leti 2016–2017," 2018. [Online]. Available: https://www.cert.si/letna_porocila/porocilo-o-omrezni-varnosti-za-leti-2016-2017/.

[2] B. Ivanc in T. Klobučar, "Attack modeling in the critical infrastructure," *Elektroteh. Vestnik/Electrotechnical Rev.*, vol. 81, no. 5, pp. 285–292, 2014.

[3] D. Fujs, S. L. R. Vrhovec in D. Vavpotič, "Inovativni model za obvladovanje informacijskovarnostnih groženj pri uporabi informacijskih sistemov," *Elektroteh. Vestn.*, vol. 87, no. 3, pp. 109–116, 2020.

[4] A. Kumar, "DDOS Attacks-A Cyber threat and possible Solutions," *Isaca Journal*, 2013. .

[5] Cloudflare, "What is DDoS attack?," 2019. [Online]. Available: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-attack/?fbclid=IwAR1tTV6suHWJNgqqCK9iykcpfOS50iLqexQioYXBYJiyGaw_WPk_fHm2otE.

[6] Netscout, "Threat Intelligence Report 2H 2018: Dawn of the Terrorbit Era," 2018. [Online]. Available: https://www.netscout.com/threatreport/.

[7] ENISA, "Trust Services Security Incidents 2018: Annual report," 2019. [Online]. Available: https://www.enisa.europa.eu/publications/trust-services-security-incidents-2018.

[8] EUROPOL, "Internet organised crime threat assessment (IOCTA)," 2018. [Online]. Available: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-201.

[9] O. Kupreev, K. Badovskaya in A. Gutnikov, "DDoS attacks in Q1 2019. Kaspersky Lab report," 2019. [Online]. Available: https://securelist.com/DDoS-report-q1-2019/90792/.

[10] Nexusguard, "DDoS Threat Report 2019 Q3," 2019. [Online]. Available: https://www.nexusguard.com/threat-report-q3-2019.

[11] R. Gan, "MazeBolt Publishes First Ever State of DDoS Protection Report," *CISION PR newswire*, 2019. [Online]. Available: https://www.prnewswire.com/il/news-releases/mazebolt-publishes-first-ever-state-of-ddos-protection-report-803618725.html.

[12] A. Serrano Mamolar, Z. Pervez, Q. Wang in J. M. Alcaraz-Calero, "Towards the Detection of Mobile DDoS Attacks in 5G Multi-Tenant Networks," in *IEEE European Conference on Networks and Communications*, 2019, pp. 273–277.

[13] L. Zabrodina, D. Parfenov, I. Bolodurina, V. Torchin, and A. Zhigalov, "Development of a Model of Cyberattacks Identification Based on the Analysis of Device States in the Network of a Telecommunications Service Provider," in *2019 International Multi-Conference on Engineering, Computer and Information Sciences*, 2019, pp. 675–680.

[14] Y. Cao, Y. Gao, R. Tan, Q. Han in Z. Liu, "Understanding Internet DDoS Mitigation from Academic and Industrial Perspectives," *Inst. Electr. Electron. Eng.*, vol. 6, pp. 66641–66648, 2018.

[15] D. Kumar Bhattacharyya in J. Kumar Kalita, "DDoS Attacks Evolution, Detection, Prevention, Reaction, and Tolerance," *CRC press*, 2016.

[16] CISCO, "Cisco ASR 9000 vDDoS Protection," 2015. [Online]. Available: https://www.cisco.com/c/en/us/products/collateral/routers/asr-9000-series-aggregation-services-routers/solution-overview-c22-736143.pdf .

[17] M. Taghizadeh Manavi, "Defence mechanisms against Distributed Denial od Service attaks: A survey," *Comput. Electr. Eng.*, no. 72, 2018.

[18] E. Risteska in M. Boganovski, "Напад со преплавување со UDP пакети," in *Conference on Information Tehnologies for Young Researches (CITYR)*, 2012, pp. 47–53.

[19] V. R. Deshmukh in K. Devadkar, "Understanding DDoS attak and its effect in Cloud Environment," *Procedia Comput. Sci.*, no. 49, pp. 202–220, 2015.

[20] T. Usman, M. Yasir, A. Bessam in H. ManPyo, "Collaborative peer to peer defense mechanisem for DDoS attaks," *Procedia Comput. Sci.*, no. 5, pp. 157–164, 2011.

[21] Radware, "DDoS survival Handbook: The ultimate guide to everything you need to know about DDoS attacks," 2013. .

[22] I. S. Amiri in M. R. K. Soltanian, *Theoretical and Experimental Methods for Defending Against DDoS attacks*. Waltham: Elsevier, 2016.

[23] Z. Wang, "An elastic and resiliency defense against DDoS attacks on the critical DNS authoritative infrastructure," *J. Comput. Syst. Sci.*, no. 99, pp. 1–26, 2019.

[24] C. S. Yoo, "Wireless network neutrality: Technological challenges and policy implications," *Berkeley Technol. Law J.*, vol. 31, no. 2, pp. 1409–1460, 2016.

[25] A. M. Craciun, "Threats and risks to telecommunications systems," *Int. J. Inf. Secur. Cybercrime*, vol. 7, no. 1, pp. 23–31, 2018.

[26] netZentry, "Defending eBusinesses and Hosting Service Providers from DDOS Attacks: A netZentry Technology White Paper," 2006. [Online]. Available: https://www.tradepub.com/free-offer/protect-your-servers-from-ddos-attacks/w_aaaa1019?sr=hicat&_t=hicat:790.

[27] P. Shinde in J. T. Parvat, "DDoS Attack Analyzer: Using JPCAP and WinCap," *Procedia Comput. Sci.*, no. 79, pp. 781–784, 2016.

Kaja Prislan je leta 2016 doktorirala na Fakulteti za varnostne vede Univerze v Mariboru, kjer je zaposlena kot docentka za področje varnostnih ved. Njeni raziskovalni interesi vključujejo upravljanje informacijske varnosti v organizacijah, vedenjske vidike pri uporabi informacijskih tehnologij in varnost v (pametnih) skupnostih.

Kristina Stojchevska je leta 2020 magistrirala na Fakulteti za varnostne vede Univerze v Mariboru. Zaposlena je v podjetju T2 d. o. o. Njeni raziskovalni interesi vključujejo varnost omrežij in kibernetsko varnost.

Anže Mihelič je leta 2016 magistriral na Fakulteti za varnostne vede Univerze v Mariboru. Je doktorski kandidat na Fakulteti za računalništvo in informatiko ter Pravni fakulteti Univerze v Ljubljani. Kot asistent je zaposlen na Fakulteti za varnostne vede Univerze v Mariboru, kot raziskovalec pa na Fakulteti za matematiko in računalništvo na FernUniversität in Hagen. Njegovi raziskovalni interesi obsegajo tehnične, zasebnostne, pravne ter psihološke vidike informacijske in kibernetske varnosti.