Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Bakalářská práce

Obrana proti útoku distributed denial of service

Jiří Pátek

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jiří Pátek

Systémové inženýrství a informatika
Informatika

Název práce

Obrana proti útoku distributed denial of service

Název anglicky

Defense against Distributed Denial of Service Attack

Cíle práce

Hlavním cílem práce je analýza možností ochrany proti DDoS útokům. Dílčími cíli jsou:
- analýza různých technik útoků
- analýza praktické použitelnosti a efektivity metod obrany
- příklady řešení ochrany
- závěry a doporučení

Metodika

Práce je založena na studiu technik útoků DDoS a obrany proti nim. Bude provedena analýza typů útoků, jejich cíle a současné trendy. Bude provedeno zhodnocení přístupů k obraně proti těmto útokům. Na základě analýzy bude vyhodnoceno srovnání jejich efektivity proti nejběžnějším typům útoků. V závěru práce budou syntetizovány příklady řešení obrany proti DDoS útokům pro modelové subjekty.

Doporučený rozsah práce

40 – 50 stran

Klíčová slova

síťová bezpečnost, odepření přístupu, DDoS, botnet, počítačová kriminalita

---

Doporučené zdroje informací

BHATTACHARYYA, D. K. a KALITA, J. K. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance. Boca Raton: CRC Press, 2016. ISBN 978-1-4987-2964-2.

SOLTANIAN, M. R. K. a AMIRI, I.S. Theoretical and Experimental Methods for Defending Against DDoS Attacks. Waltham: Elsevier, 2016. ISBN 978-0-12-805391-1.

THAKKAR, D. Preventing Digital Extortion: Mitigate ransomware, DDoS, and other cyberextortion attacks. Birmingham: Packt, 2017. ISBN 978-1-78712-036-5.

Předběžný termín obhajoby

2020/21 ZS – PEF (únor 2021)

Vedoucí práce

Ing. Alexandr Vasilenko, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 4. 9. 2019

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 14. 10. 2019

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 29. 11. 2020

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Obrana proti útoku distributed denial of service" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 30.11.2020 _____

Poděkování

Rád bych touto cestou poděkoval Ing. Alexandru Vasilenkovi, Ph.D. za vedení této práce a své rodině za stálou podporu.

Obrana proti útoku distributed denial of service

Abstrakt

Tato bakalářská práce je zaměřena na problematiku útoků distributed denial of service (DDoS). Popisuje metody DDoS útoků, techniky obrany a současné trendy v obraně proti DDoS útokům. Práce analyzuje a srovnává typy systémů obrany proti útokům DDoS a porovnává vybrané specializované poskytovatele obrany proti DDoS. Práce popisuje vlastnosti systémů obrany proti DDoS a jejich význam pro pět modelových subjektů – banku, zpravodajský server, cloudové úložiště, nemocnici a on-line herní platformu. Výběr vhodného systému obrany je ukázán na fiktivním cloudovém úložišti. Práce ukazuje, jak volba systému obrany proti DDoS závisí na individuálních potřebách chráněného subjektu.

Klíčová slova: počítačová kriminalita, síťová bezpečnost, odepření přístupu, DDoS, botnet, Internet věcí, obrana proti DDoS

Defence against distributed denial of service attack

Abstract

This bachelor's thesis is focused on the problematics of Distributed Denial of Service attacks (DDoS). The thesis describes methods of DDoS attacks, techniques of defence against DDoS attacks and current trends in the defence against DDoS attacks. The thesis analyzes and compares types of systems of defence against DDoS attacks and compares selected specialized DDoS defence providers. The thesis describes attributes of the DDoS defence systems and their importance for five model subjects – a bank, a news server, a cloud storage, a hospital and an on-line gaming platform. Selection of the suitable DDoS defence system is described using a fictional cloud storage. The thesis shows how the choice of the DDoS defence system depends on invidual needs of the protected subject.

Keywords: cybercrime, network security, denial of service, DDoS, botnet, Internet of Things, defence against DDoS

Obsah

Seznam obrázků

Seznam tabulek

1. Úvod

Práce je zaměřena na problematiku útoků distributed denial of service (DDoS), jejich detekci a obranu proti nim. Útok DDoS je velmi populárním typem kybernetického útoku, a to především pro jeho jednoduchou implementaci a zároveň velkou efektivitu [1].

Běžná obrana pomocí síťových zařízení a tradičních metod obrany je důležitou součástí celkové bezpečnostní strategie, ale neposkytuje dostatečnou ochranu proti útoku DDoS. Konvenční metody obrany, typicky firewally, dokáží zabránit jednotlivým průnikům do sítě, ale nedokáží síť ochránit před přehlcením útokem DDoS [2]. Subjekty také často přecházejí na cloudová řešení, což může způsobit, že dosavadní obrana není proti potenciálnímu útoku DDoS dostatečná. Nedostatečná obrana před útoky DDoS může mít pro cílené subjekty značné následky [8]. Proto subjekty potřebují účelově vytvořený systém, který je schopný odhalit a odrazit různé typy DDoS útoků.

Počet a velikost DDoS útoků každým rokem roste, což po subjektech závislých na internetových službách vyžaduje neustálé rozšiřování a aktualizaci svých obranných systémů [3]. Napříč platformami se objevují nové a sofistikovanější varianty útoku DDoS, což vyžaduje výzkum a implementaci modernějších metod detekce a obrany k udržení kroku s útočníky.

2. Cíl práce a metodika

Cíl práce

Hlavním cílem práce je analýza možností ochrany proti DDoS útokům. Dílčími cíli jsou:

- analýza různých technik útoků,
- analýza praktické použitelnosti a efektivity metod obrany,
- příklady řešení ochrany,
- závěry a doporučení.

Metodika

Práce je založena na studiu technik útoků DDoS a obrany proti nim. Bude provedena analýza typů útoků, jejich cíle a současné trendy. Bude provedeno zhodnocení přístupů k obraně proti těmto útokům. Na základě analýzy bude vyhodnoceno srovnání jejich efektivity proti nejběžnějším typům útoků. V závěru práce budou syntetizovány příklady řešení obrany proti DDoS útokům pro modelové subjekty.

3. Teoretická východiska

3.1 Distributed Denial of Service

Distributed Denial of Service (DDoS) je koordinovaný počítačový útok, ve kterém se útočník snaží zahltit server, síť nebo počítač oběti požadavky za použití velkého množství počítačů [1]. Takto zahlcený systém poté může přestat fungovat pro legitimní požadavky klientů a může mít za následek i úplné zhroucení napadené sítě. Distribuovaná povaha útoku DDoS ho činí velice výkonným a obtížným pro identifikaci a odražení.

V počáteční fázi útoku útočník identifikuje potenciální zranitelnosti v jedné nebo více sítích, kde nainstaluje malware pro infikování co největšího množství počítačů. Takto infikované počítače útočník ovládá ze vzdálené lokace. V další fázi útočník využije infikované počítače k posílání požadavků na cílový server oběti. V závislosti na intenzitě vysílaných požadavků, počtu útočících infikovaných počítačů a schopnostech obrany oběti nastane poškození v síti oběti.

Hlavní důvody, které činí DDoS útok populárním typem útoku, jsou [1]:

- v internetové bezpečnosti existuje vysoká vzájemná provázanost,
- internetové zdroje jsou omezené,
- existuje mnoho nevědomě infikovaných zařízení, která mohou provádět útok proti serverům oběti,
- informace a zdroje, které mohou být použity pro potlačení hrozících útoků se většinou nesbírají,
- Internet používá jednoduché a přímočaré směrovací algoritmy,
- existují neshody v designu a rychlosti mezi různými částmi sítě,
- správa sítě je často zanedbávaná,
- sdílení zdrojů.

3.2 Motivace pro útoky DDoS

Existuje mnoho důvodů, proč se útočníci rozhodnou provést útok DDoS. Důvody jsou často finančně motivované, ale mohou být i nefinančně motivované.

3.2.1 Finanční motivace

Finanční zisk se řadí mezi nejčastější důvod útoku DDoS [3, 12]. Motivace za účelem finančního obohacení jsou [13]:

- vydírání – útočníci se snaží vydírat předem vybrané cíle a útok DDoS si zvolí jako prostředek jejich vydírání. Útočník zahájí proti předem vybranému cíli menší útok DDoS a pošle mu vyděračskou zprávu, která slibuje, že za finanční obnos nebude subjekt cílován dalšími většími útoky DDoS. Pokud se subjekt rozhodne zaplatit, tak mu hrozí, že si ho vyděrači označí za plátce a zaútočí v budoucnosti,
- odvrácení pozornosti od jiného typu útoku – útočníci nepožadují výkupné, ale použijí útok DDoS pro odvrácení pozornosti od jiného druhu kybernetického útoku,
- konkurenční boj – konkurenční firma se snaží prostřednictvím DDoS konkurentům omezit nebo přerušit poskytování služeb, poškodit reputaci a zvýhodnit tak svoji pozici na trhu.

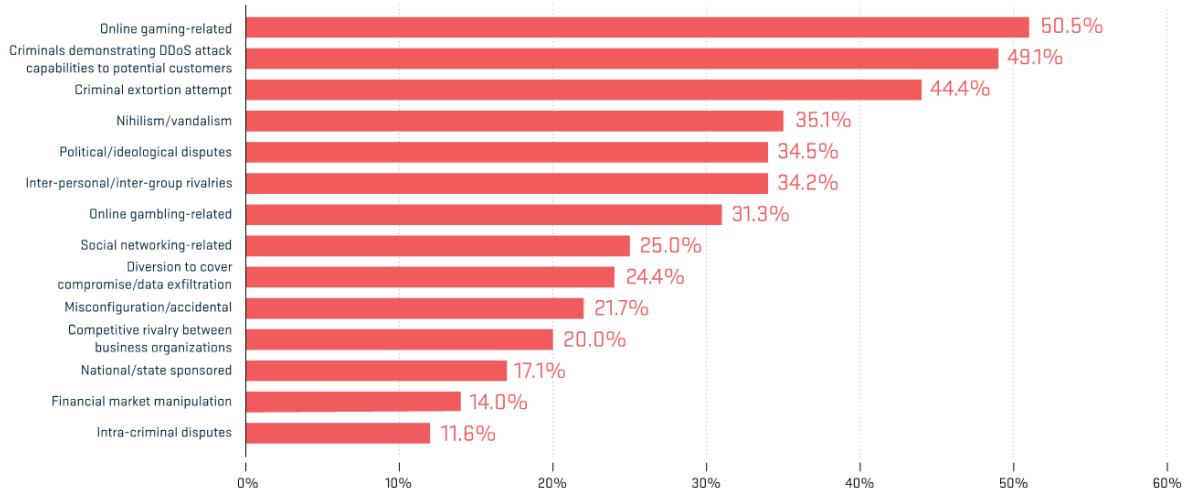
3.2.2 Nefinanční motivace

Některé útoky nejsou motivovány finančním ziskem. Motivace útoků, které jsou prováděny bez finančího obohacení, mohou být [3, 13]:

- pomsta – útoky DDoS prováděné bez finanční motivace jsou velmi často prováděné za účelem pomsty, a to jak bývalých zaměstnanců, tak nespokojených zákazníků nebo obchodních partnerů,
- podpora politické agendy nebo sociální změny – útok DDoS může být použit politickými, ideologickými nebo teroristickými skupinami pro digitální umlčení opozice,
- kybernetická válka mezi státy,
- zvýšení reputace útočníka,
- otestování síly útoku nebo odolnosti napadeného systému,
- neúmyslné útoky,
- žert pro pobavení nebo otestování vlastních schopností.

V roce 2018 firma Arbor Networks zabývající se prodejem síťových zabezpečení a síťového monitoringu vydala třináctou výroční zprávu o zabezpečení celosvětové

infrastruktury (13th Annual Worldwide Infrastructure Security Report, WISR) [14]. V části zprávy týkající se motivace útoků DDoS se dotazovala poskytovatelů služeb (poskytovatelé internetového připojení, poskytovatelé hostingů a datových center, poskytovatelé cloudových služeb, mobilní operátoři, poskytovatelé DNS služeb atd.) k označení nejčastějších motivací útoku za uplynulý rok 2017 (Obrázek 1). Na prvním místě je stejně jako předešlý rok považováno jako největší motivace online hraní, i přesto, že meziročně kleslo z 63% na 50%. Na druhém místě je demonstrace schopnosti útoku DDoS s 49%, která meziročně předstihla politickou a ideologickou motivaci. Vzestup demonstrací útoků je způsoben rostoucím množstvím subjektů, kteří poskytují útok DDoS jako službu k pronájmu. Na třetím místě je kriminální vydírání s 44%.



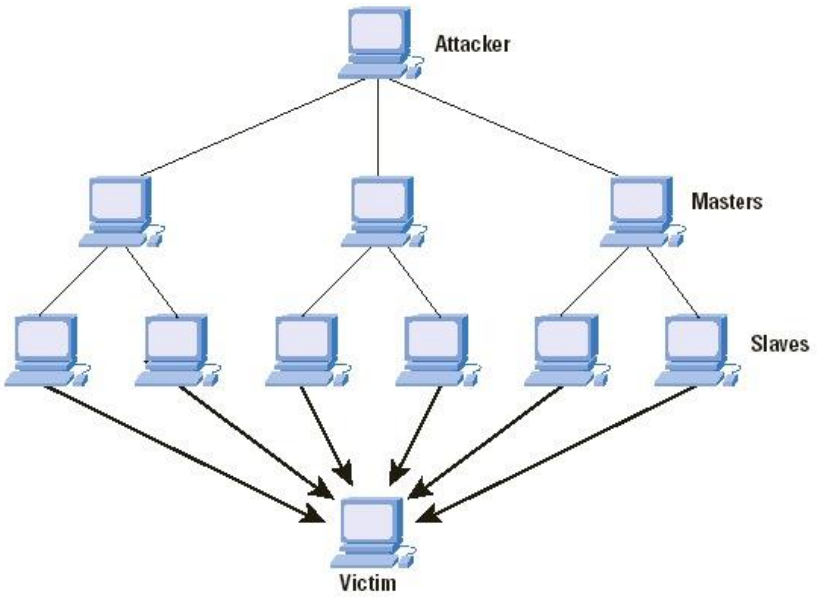
Obrázek 1 – Motivace útoků DDoS

3.3 Typický útok DDoS

Typický DDoS útok používá k provedení útoku velké množství infikovaných počítačů. Většina vlastníků infikovaných počítačů si není vědoma přítomnosti malwaru v jejich počítači. Infikované počítače se rozdělují na dva druhy [52]:

- master zombie – ovládané přímo útočníkem,
- slave zombie – řízeny automaticky master zombiemi.

Před zahájením útoku master zombie nečinně vyčkávají na příkaz k provedení útoku. Jakmile master zombie tento příkaz obdrží, rozešlou ho slave zombiím, které začnou provádět útok podle obdržených instrukcí. Hierarchické schéma útoku je zobrazeno na Obrázku 2.



Obrázek 2 – Schéma útoku DDoS

3.4 Technologie pro DDoS

Útočníci se snaží adaptovat různé moderní technologie, aby zvýšili efektivitu útoku DDoS. Jedná se například o botnety, využití zařízení Internetu věcí (IoT) a DDoS k pronájmu.

3.4.1 Botnet

Botnet je skupina zařízení připojených k Internetu, které jsou napadeny malwarem a ovládány vzdáleně vlastníkem botnetu [23]. Botnet je většinou navržen k provádění nezákonných anebo škodlivých úkonů jako jsou DDoS útoky, odesílání spamu, krádeže dat a jiné kyberzločiny. Botnety se většinou můžou samovolně rozšiřovat do okolních sítí pomocí trojských koní, zneužitím zranitelnosti webových stránek nebo zneužitím slabé ochrany autentizace. Počet zařízení v botnetu se typicky pohybuje od několika tisíců až po stovky tisíc.

3.4.2 Podvržení IP adresy

Při normální IP komunikaci obsahuje hlavička paketu zdrojovou IP adresu a cílovou IP adresu [24]. K podvržení IP adresy dojde tak, že škodlivý program vytvoří vlastní paket a nenastaví pravdivou zdrojovou IP adresu. Toho program dokáže docílit zneužitím raw IP

socketů, které umožní hlavičky paketů zpřístupnit programu a následně ji upravit. Existují tři základní možnosti jak vytvářet podvržené IP adresy [24].

První možností je, že útočník vytvoří náhodně generované zdrojové IP adresy. Tyto adresy jsou generovány náhodně z celého IP adresového prostoru (0.0.0.0 až 255.255.255.255). Tuto variantu generování IP adres lze použít, pokud útočník potřebuje velké množství paketů s podvrženou IP adresou a nepotřebuje zaručit doručení každého konkrétního paketu (některé z takto vytvoření podvržených zdrojových adresy se vytvoří neplatné nebo neroutovatelné). Tato metoda porovná zdrojovou adresu paketu s adresovým prostorem přiřazeným k zdrojové nebo cílové lokaci v závislosti na umístění filtrujícího routeru. Pakety, jejichž zdrojová IP adresa nepatří k zdrojové nebo cílové lokaci, jsou zahozeny. Obrana proti takto generovaným IP adresám je použití vstupního a výstupního filtrování na routeru. Aby však vstupní a výstupní filtrování paketů výrazně omezilo schopnost útočníků generovat podvržené IP adresy, muselo by být široce používáno.

Druhou možností je, že útočník zneužije konkrétní podsíť, ve které se nachází jeho oběť. Pokud se například oběť nachází v síti 192.168.1.0/24 a má přiřazenou konkrétní adresu z tohoto rozsahu, tak ji může útočník snadno podvrhnout za kteroukoliv jinou adresu z tohoto rozsahu. Takovému podvržení IP adresy lze zabránit tím, že správce sítě zakáže přiřazení MAC adresy k IP adrese všem kromě správce sítě. Takto podvržené pakety lze také filtrovat za použití vstupního a výstupního filtrování na routeru, ale pouze na úrovni dané podsítě.

Třetí možností je, že útočník podvrhne zdrojovou IP adresu oběti. Tato metoda se používá při útocích DDoS založených na reflektorech. Útoku lze předejít, pokud dochází k filtrování paketů routerem při výstupu ze zdrojové sítě nebo při vstupu do sítě poskytovatele internetového připojení.

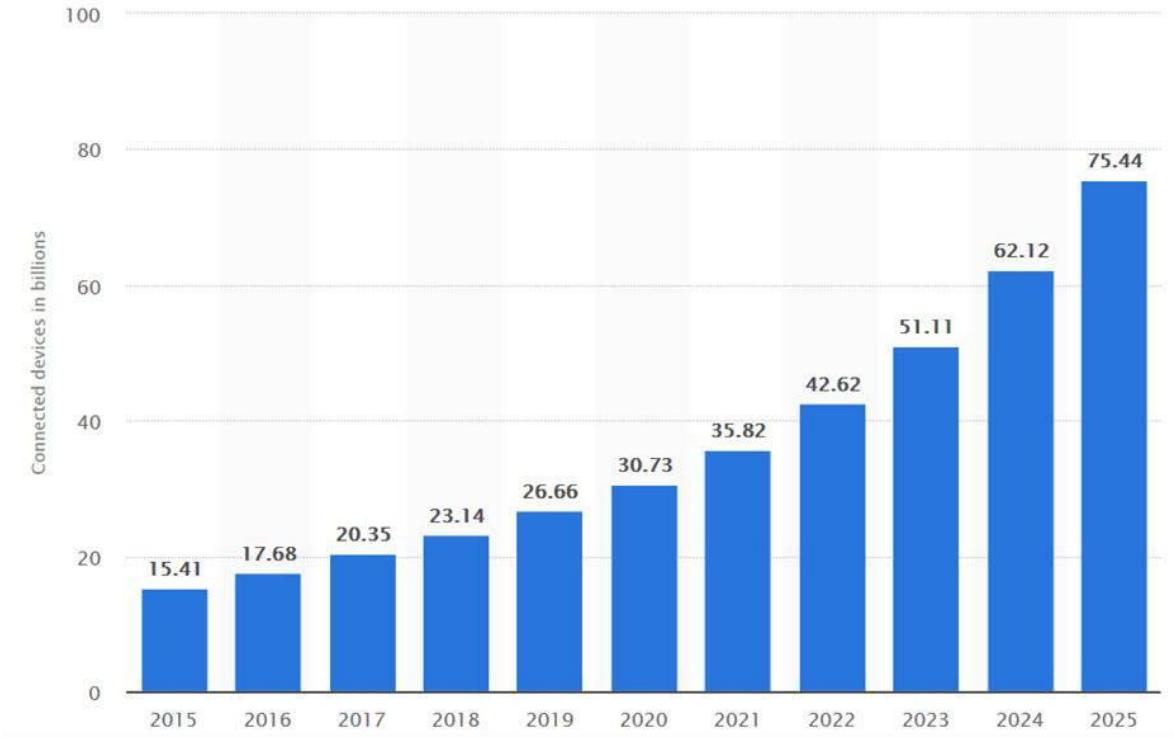
Použití podvržených IP adres není nutné pro úspěšný útok DDoS (vyjma útoku DDoS založeného na reflektorech), přesto se velmi často používá z následujících důvodů:

- skryje skutečnou identitu zombií,
- zhorší možnost vysledování útočníka,
- zabrání snadnějšímu filtrování paketů DDoS útoku.

3.4.3 Internet věcí

Internet věcí jsou zařízení připojená k Internetu za účelem výměny informací. Jedná se například o domácí spotřebiče, vozidla, kamery a různé senzory. Tyto zařízení je možné

zneužít k provedení útoku DDoS. Růst odvětví Internetu věcí je prudce rostoucí (Obrázek 3) [4].



Obrázek 3 – Počet připojených IoT zařízení (v mld.)

DDoS útoky pomocí IoT zařízení již proběhly. Výzkumníci z firmy Sucuri Security zabývající se internetovou bezpečností odhalili v roce 2016 botnet, který se skládá z více než 25000 bezpečnostních kamer připojených k internetu [5]. Tento botnet útočníci použili k DDoS útoku na webové stránky malého kamenného zlatnictví. Jednalo se o útok na 7. vrstvě pomocí HTTP flood. Útok byl atypický svojí dlouhou dobou trvání (několik dnů) a na vrcholu intenzity dosahoval až 50000 HTTP požadavků za sekundu. Tento kybernetický útok poukazuje na potenciál zneužití moderních technologií jako je IoT. Mnoho IoT zařízení se prodává bez ochrany heslem nebo jejich uživatelé často používají výchozí přednastavená hesla pro přístup na Internet, proto je pro útočníka snadné je zneužít.

3.4.4 DDoS k pronájmu

S rostoucím popularitou DDoS útoků vznikly subjekty, které poskytují DDoS útoky k pronájmu (DDoS Stressers, DDoS Booters) [6]. Uživatelé těchto služeb mají možnost

anonymně zaútočit na jakýkoliv cíl bez větších technických znalostí, zdrojů, přípravy, a za velmi nízkou cenu.

Nezákonnost DDoS útoků staví poskytovatele těchto služeb do složité situace, protože chtějí poskytovat DDoS útoky legálně. Proto někteří poskytovatelé nazývají DDoS službu jako zátěžový DDoS test a naznačují její použití k testování odolnosti vlastního serveru. Poskytovatelé však často neověřují identitu zákazníka ani to, zda je zákazník skutečně vlastníkem serveru, na kterém bude proveden testový zátěžový DDoS útok. Zákazník tak může použít DDoS útok na jakýkoliv cíl.

3.5 Následky útoku DDoS

Úspěšně provedený útok DDoS má za následek částečné nebo úplné zhroucení cíleného systému. Nejčastější následky jsou:

- nedostupnost poskytovaných služeb,
- ztráta produktivity,
- poškození značky nebo pověsti firmy,
- náklady na kybernetické zabezpečení do budoucnosti,
- finanční kompenzace zákazníků,
- právní následky,
- ztráta příjmů,
- náklady na vyšetření útoku,
- ztráta zákazníků,
- odchod zaměstnanců,
- finance na zaplacení požadavků útočníka,
- fluktuace ceny akcií,
- pokuty nebo penále od regulátora.

Ve zprávě WISR [14] se firma Arbor Networks dotazovala výzkumných a vzdělávacích institucí, finančních institucí, vládních institucí a technologických firem a dalších subjektů na četnosti útoků za rok 2017. 60% dotázaných subjektů bylo napadeno alespoň jedním útokem DDoS, přičemž 13% bylo napadeno 100 nebo více útoky za posledních 12 měsíců. Napadení 100 nebo více útoky se meziročně zvýšilo o více než 100%.

84% dotázaných napadených subjektů zažilo nejdelší délku útoku menší než 24 hodin, z toho 70% dotázaných zažilo nejdelší délku pod 7 hodin. 75% dotázaných subjektů uvedlo, že jsou schopny zmírnit dopady útoku DDoS za méně než 1 hodinu. 30% uvedlo používání okamžitého zmírnění dopadů pomocí místního (on-premise) řešení nebo cloudové služby. Pouze 3% subjektů uvedly, že nepoužívají žádný prostředek pro zmírnění dopadů útoků DDoS. To poukazuje na to, že potenciální následky DDoS útoku mohou být velmi vážné.

3.6 Historické DDoS útoky

K prvnímu útoku typu odepření přístupu (Denial of Service – DoS) došlo v roce 1974 třináctiletým studentem střední školy ve Spojených státech amerických [3]. Student použil příkaz external, který sloužil pro interakci s externími zařízeními připojenými k terminálům. Když byl ale příkaz external spuštěn na terminálu bez externích zařízení, tak způsobil zablokování terminálu a vyžadoval restartování pro zpětné nabytí funkčnosti. Tato zranitelnost byla vyřešena zákazem příkazu external ve výchozím nastavení.

V roce 1999 útočník použil nástroj Trinoo ke kolapsu počítačové sítě University of Minnesota na dva dny [3]. Trinoo byl jednoduchý program bez anonymních funkcí používaný k DDoS útokům. Obsluhoval síť infikovaných strojů nazvaných Masters a Daemons, které umožnily útočníkovi poslat DDoS instrukce pár Masters hostům, kteří poté dále předali instrukce Daemons hostům, kteří zahájili UDP flood útok.

Dalším populárním nástrojem používaným k DDoS útokům byl program Stacheldraht, který podporoval vzdálené aktualizace a podvržení IP. Program mohl také obsahovat nástroje pro sbírání a shromažďování statistik útoků.

3.6.1 Nejvýznamnější DDoS útoky [7]

Útok na Amazon, CNN, eBay, Dell, Yahoo (2000)

V únoru 2000 patnáctiletý hacker známý pod přezdívkou Mafiaboy odepřel přístup k několika webovým stránkám velkých společností včetně Amazonu, CNN, eBay, Dellu a Yahoo. Útok byl významný svojí dlouhou délkou trvání (více než jeden týden), nízkým věkem útočníka a způsobenými škodami, které byly odhadnuty na více než 1,2 miliardy USD [8].

Útok na estonské vládní systémy (2007)

V dubnu a květnu 2007 byly estonské vládní systémy a služby napadeny útokem DDoS [9]. Útok cílil na státní agentury, finanční instituce, banky a média. DDoS útoku předcházelo rozhodnutí estonské vlády přesunout sovětský památník druhé světové války z centra Tallinu, což vyvolalo protesty ruské vlády a nepokoje mezi ruskou etnickou menšinou v Estonsku. Estonské úřady obvinily z útoku Rusko, které útok popřelo. Následkem útoku Estonsko v roce 2008 zřídilo centrum kybernetické obrany NATO (NATO Cooperative Cyber Defence Centre of Excellence) a vyzvalo Evropskou unii, aby učinila kybernetické útoky trestným činem.

Útok na americké banky (2012)

V září a říjnu 2012 se stalo 6 největších amerických bank cílem DDoS útoku. Útok trval déle než tři dny a byl jedinečný v tom, že útočníci namísto jednoho soustředěného útoku použili řadu různých typů útoku, aby znesnadnili obranu a zjistili, který typ způsobuje největší škodu.

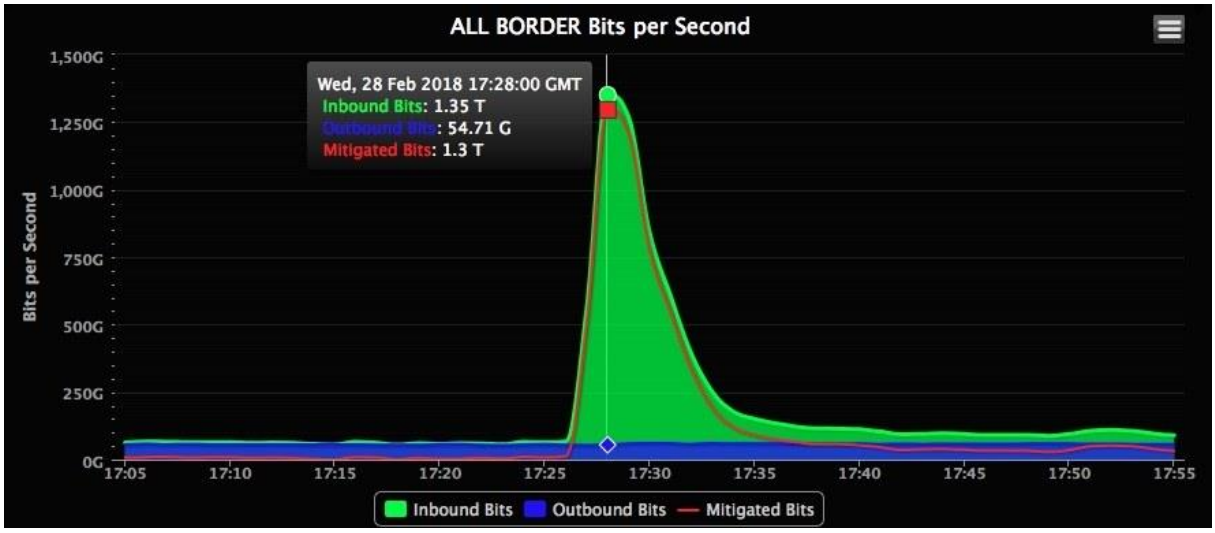
Útok na Dyn (2016)

V říjnu 2016 byl proveden DDoS útok na významného DNS poskytovatele Dyn. Útok znemožnil přístup na webové stránky více než 80 jeho zákazníků včetně stránek Airbnb, Amazonu, Spotify, Netflixu, PayPalu, Redditu a Twitteru. Útočníci vytvořili pomocí malwaru Mirai botnet s více než 100 000 IoT zařízeními [10]. Mirai hledá na internetu IoT zařízení, která běží na ARC procesoru (na ARC procesoru běží ořezaná verze linuxu, kterou často používají IoT zařízení). Pokud nalezené IoT zařízení používá výchozí uživatelské jméno a heslo, tak je botnet schopný je infikovat a přidat k botnetu. Útok způsobil údajnou škodu 110 milionů USD navzdory tomu, že byl odražen během jednoho dne.

Útok na GitHub (2018)

V únoru 2018 byl napaden GitHub (online služba využívaná programátory pro správu kódu) DDoS útokem. Tento útok byl druhý největší v historii na objem odeslaných dat a ve špičce dosáhl až 1,35 Tb/s (Obrázek 4). Navzdory skutečnosti, že útočníci vysílali

tak masivní objem dat, trval celý útok pouze 10 minut, protože společnost, kterou GitHub používal na ochranu proti DDoS útoku, ho byla schopná zastavit.



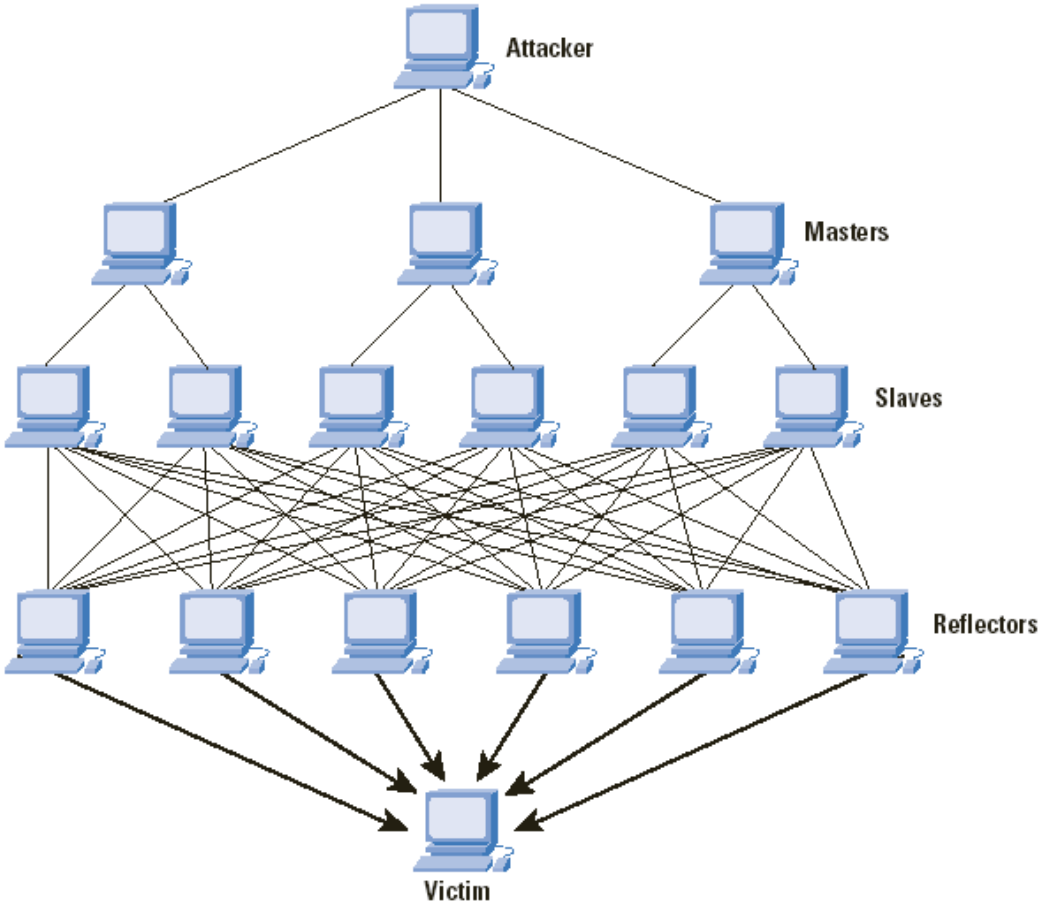
Obrázek 4 – DDoS útok na GitHub

3.7 Rozdělení DDoS útoků

DDoS útoky dělíme do několika kategorií podle různých kritérií – typu útoku, velikosti objemu útoku, dynamiky rychlosti útoku a cíle útoku [1].

3.7.1 Rozdělení podle typu útoku

Podle typu útoku jsou DDoS útoky rozděleny do dvou kategorií – na přímé útoky a na útoky založené na reflektorech (reflector-based). Při přímém útoku útočník používá k provedení útoku přímo zombie (viz kapitola 3.3 Typický útok DDoS). Naproti tomu DDoS útoky založené na reflektorech využívají k útoku mnoho legitimních serverů – reflektorů, na které útočník pošle požadavek s podvrženou zdrojovou IP adresou jeho oběti (Obrázek 5). Tyto servery poté na požadavek odpoví posláním zpráv, jejichž objem je typicky několikanásobně větší, než velikost původního požadavku. Útok, ve kterém je odpověď několikanásobně větší než velikost původního požadavku, se nazývá amplifikační útok.



Obrázek 5 – DDoS útok založený na reflektorech

3.7.2 Rozdělení podle velikosti objemu útoku

DDoS útoky jsou rozděleny podle objemu útoku na objemové a nízkoobjemové. Při objemovém útoku útočník používá k útoku velký objem paketů směrem k cíli. Objemový útok je nejběžnějším typem DDoS útoku.

Při nízkoobjemovém útoku útočník provede útok posíláním paketů nižší rychlostí, která více odpovídá legitimnímu síťovému provozu. Tento typ útoku se často například snaží vyčerpat výpočetní výkon oběti zasláním dotazů náročných na procesorový výkon.

3.7.3 Rozdělení podle dynamiky rychlosti útoku

Podle dynamiky rychlosti útoku se dělí DDoS útoky do 4 kategorií – s konstantní rychlostí, se zvyšující se rychlostí, pulzní útok a útok podskupiny.

Útok s konstantní rychlostí

Zombie po obdržení příkazu od útočníka začnou odesílat pakety konstantní rychlostí a objem útoku tak dosáhne svého maxima za velmi krátký časový úsek. Dosažená rychlost útoku je konstantní až do skončení útoku. Tento typ útoku způsobí rychlé a náhlé zaplavení sítě oběti.

Útok se zvyšující se rychlostí

Útočník postupně zvyšuje rychlost útoku směrem k cíli. Tento typ útoku se používá útočníkem pro pochopení reakce oběti na útok, aby se útočník mohl pokusit vyhnout detekčnímu systému oběti.

Pulzní útok

Útočník aktivuje zombie, které pravidelně v určených časových intervalech posílají pakety k cíli. Tento typ útoku se používá k zamaskování útoku detekčním systémem oběti.

Útok podskupiny

Útok podskupiny je založen na stejném principu jako pulzní útok s rozdílem, že zombie jsou rozděleny do skupin. Tyto skupiny jsou aktivovány a deaktivovány v různých kombinacích. Tento typ útoku se používá k dalšímu zamaskování útoku.

3.7.4 Rozdělení podle cíle útoku

DDoS útoky lze také rozdělit na přímé a nepřímé, podle toho, zda je útok cílen přímo na oběť nebo zda je cílen nepřímo na prostředníky, kteří poskutují oběti služby a jsou důležití pro správné fungování kritických systémů oběti. Jedná se například o poskytovatele webhostingu, cloudových služeb nebo platební brány.

3.8 Metody DDoS útoků

Existuje mnoho různých typů DDoS útoků, protože existuje mnoho různých síťových technologií, které lze potenciálně zneužít [15].

3.8.1 Přímé útoky

ICMP Flood

ICMP Flood útok se řadí mezi populární DDoS útoky. Útočník se snaží zahltit systémy oběti požadavky ICMP echo (příkazy ping, které se za běžných okolností používají k testování konektivity a latence mezi dvěma síťovými rozhraními) [16]. Útok se projeví zaplavením sítě oběti pomocí paketů s požadavkem, na které síť oběti odpoví úměrným množstvím paketů s odpovědí. Toto zatěžuje příchozí a odchozí přenosovou rychlost v síti a může dojít až k úplnému zahlcení sítě. K tomu, aby byl ICMP Flood útok účinný, potřebuje útočník větší přenosovou rychlost, než má k dispozici oběť.

HTTP Flood

HTTP Flood útok využívá zdánlivě legitimní HTTP požadavky a je často používán botnety, kteří cílí na webové servery nebo aplikace [17]. HTTP Flood útok nepoužívá podvržené pakety ani reflektory a k úspěšnému provedení útoku stačí menší přenosová rychlost než u většiny ostatních DDoS útoků. Tyto útoky však vyžadují hlubší porozumění cíli útoku a každý útok musí být vytvořen speciálně pro daný cíl. To má také za následek značné ztížení detekce a zmírnění dopadů takto provedených útoků.

Útok funguje tak, že útočník odesílá HTTP požadavky, které jsou buď typu GET, typu POST, nebo jejich kombinací. Požadavek GET se používá k načtení běžného statického obsahu, zatímco požadavek POST se používá pro přístup k dynamicky generovaným zdrojům. Útoky využívající požadavky POST bývají více efektivní, protože více zatěžují serverové zdroje než požadavky GET, neboť mohou obsahovat parametry, které spouštějí náročné zpracování na straně serveru. Na druhou stranu útoky s použitím požadavků GET jsou jednoduší a lépe škálovatelné při použití botnetu.

Fragmentovaný HTTP Flood

Fragmentovaný HTTP Flood útok funguje na stejném principu jako HTTP Flood s tím rozdílem, že HTTP pakety jsou před odesláním rozděleny na co nejmenší části. Pokud se cílový server pokusí zpětně sestavit tyto fragmentované pakety, mohou se mu vyčerpat všechny prostředky a může dojít k odepření poskytované služby.

HTTP Flood s jedním požadavkem

HTTP Flood útok s jedním požadavkem odesílá menší množství paketů, které obsahují velký počet požadavků. Útočník je tak schopen přetížit server oběti za použití malého počtu odeslaných paketů. Vzhledem k malé přenosové rychlosti útoku je tento typ útoku obtížněji detekován obrannými systémy oběti.

Rekurzivní HTTP GET Flood

Rekurzivní HTTP GET Flood útok si vyžádá webovou aplikaci oběti, poté analyzuje odpovědi a pomocí rekurze požaduje načíst každý objekt na dané webové aplikaci. Útok se maskuje jako legitimní uživatelé, kteří se pohybují po webové aplikaci.

SYN Flood

SYN Flood útok využívá TCP protokol a třícestný handshake [18]. Útočník odesílá TCP požadavky na připojení rychleji, než je jsou systémy oběti schopné zpracovat, čímž dojde ke spotřebě zdrojů daných systémů, což má za následek zpomalení nebo odepření služby legitimním uživatelům.

Pokud chce klient navázat spojení se serverem pomocí TCP, následný legitimní pokus o navázání spojení pomocí třícestného handshaku probíhá takto:

- klient vyžádá spojení zasláním zprávy SYN (synchronizace) serveru,
- server potvrdí navázání spojení odesláním zprávy SYN-ACK (potvrzení synchronizace) zpět klientovi,
- klient odpoví zprávou ACK (potvrzení) a naváže spojení.

Při útoku SYN Flood útočník pošle opakovaně pakety SYN na každý port cíleného serveru. Server následně na každý takový paket odpoví odesláním zprávy SYN-ACK z každého otevřeného portu. Odpověď serveru útočník následně ignoruje nebo ani nepřijme (při použití falešné IP adresy). Server určitou dobu čeká na odpověď klienta a během této doby má otevřené spojení, které nemůže ukončit. Před uplynutím této doby dorazí od útočníka další paket SYN. Toto ponechá všechna spojení napůl otevřené a následně vyčerpá všechny prostředky serveru.

SYN-ACK Flood

Při útoku SYN-ACK Flood je na server oběti posláno velké množství paketů typu SYN-ACK [21]. Tyto pakety nejsou součástí žádné probíhající relace na serveru, slouží pouze k narušení chodu serveru. Nelegitimní pakety SYN-ACK vypadají podobně jako legitimní a pouze neobsahují hlavní datovou část. Útok cílí na zařízení, která zpracují každý paket, který obdrží.

UPD Flood

UDP Flood útok cílí na náhodné porty serveru oběti a k útoku využívá datagramy UDP [19]. UDP Flood útok často využívá podvržené IP adresy datagramů, aby se vracející pakety nevrátily útočníkovi a pro větší anonymizaci útoku.

UDP datagram je síťový protokol, který nenavazuje spojení pomocí handshaku, což může mít za následek, že kdokoliv může odeslat velký objem datagramů na kterýkoliv server. Poté, co napadený hostitel přijme tyto datagramy, zkontroluje, jestli aplikace spojená s těmito datagramy na tomto portu naslouchá. Zjistí, že žádná aplikace nenaslouchá, a tak odešle zpět návratový ICMP paket s touto informací (Destination Unreachable). Když hostitel přijímá velké množství UDP datagramů a odesílá ICMP pakety, tak se systém může stát přetíženým a může přestat reagovat na legitimní požadavky.

IP Null

Legitimní pakety IPv4 v hlavičce obsahují informace o protokolu, který používají na transportní vrstvě. Při IP Null útoku útočník nastaví hodnoty hlaviček IPv4 paketů na hodnotu 0 [20]. Nastavenou hodnotu 0 v hlavičce paketu mohou routery a firewally vyhodnotit jako nezařazený paket a můžou ho poslat dál do sítě. Velké množství takových paketů může spotřebovat zdroje serveru a způsobit tak jeho selhání a nedostupnost.

3.8.2 Útoky založené na reflektorech

DNS Flood

Útok DNS Flood zneužívá servery Domain Name Service (DNS), které se při legitimním použití využívají k převodu doménových jmen na IP adresu [27]. Útočník pošle

požadavek s podvrženou IP adresou oběti na co největší množství DNS serverů, které poté odešlou pakety s odpovědí na podvrženou IP adresu oběti. Útok jde amplifikovat pomocí rozšíření protokolu EDNS0 DNS, který umožní velké zprávy DNS, nebo pomocí kryptografického rozšíření zabezpečení DNSSEC. Míra amplifikace dosahuje až sedmdesátinásobku požadavku útočníka.

SNMP Flood

Útok SNMP Flood využívá protokol Simple Network Management Protocol (SNMP), který se při legitimním použití používá pro konfiguraci a shromažďování informací síťových zařízení [22]. Útočník pošle velké množství SNMP dotazů s podvrženou IP adresou oběti na připojená zařízení, která na ně následně odpoví. SNMP útok využívá amplifikaci s mírou amplifikace až 1700.

Memcached reflektory

Memcached reflection využívá systém memcaching, který se používá pro ukládání do paměti cache k urychlení webových stránek používajících databáze [11]. Útočník podvrhne IP adresu oběti a pošle žádost několika memcached serverům. Tyto servery poté posílají odpovědi do cíle, který je uveden v podvržené zdrojové IP adrese. Tato metoda může zvětšit původní objem útoku až 51200x – například 15 B požadavek na memcached server může vyvolat až 750 kB odpověd na cíl.

NTP Flood

Útok NTP Flood zneužívá veřejně přístupné servery, které používají protokol NTP (Network Time Protocol) [25]. Protokol NTP používá k přenosu protokol UDP a při legitimním použití se využívá pro synchronizaci hodin na zařízeních připojených k Internetu. Starší verze poskytují monitorovací službu, která umožnuje administrátorům načíst seznam posledních 600 hostů připojených k serveru. Útočník zneužije monitorovací službu tím, že opakovaně zašle požadavek na získání seznamu se 600 hosty a IP adresu cíle podvrhne za IP adresu oběti. Amplifikace NTP Flood útoku má míru až 557.

SSDP Flood

Útok SSDP Flood používá protokol SSDP (Simple Service Discovery Protocol) a zneužívá síťové protokoly UPnP (Universal Plug and Play) [26]. Protokol SSDP se za běžných okolností používá k vzájemnému zjišťování PnP (Plug and Play) zařízení připojených k síti.

V prvním kroku útočník vyhledá všechna PnP zařízení v dané síti, která lze použít jako reflektory. Poté útočník vytvoří UDP datagram s podvrženou IP adresou oběti. Poté útočník pomocí botnetu odešle vytvořený UDP datagram ke každému nalezenému PnP zařízení. Každé PnP zařízení, které obdrží UDP datagram, odešle odpověď na cíl. Míra amplifikace SSDP Flood útoku je až 30.

3.9 Obrana proti DDoS útoku

Při napadení sofistikovaným DDoS útokem nemusí být stávající obranné mechanismy schopny tento útok v reálném čase efektivně potlačit [1]. Zvolené řešení obrany by mělo včasně detekovat útok s co nejmenším výskytem falešně pozitivních detekcí, být plně funkční s velkým provozem v síti, dosahovat velké míry úspěšnosti při zajištění bezpečnosti sítě a zajistit, aby legitimní uživatelé měli v případě napadení stálý přístup k síti a nedošlo k signifikantnímu zpomalení sítě [45].

Kvalitní řešení obrany by mělo rychle a přesně reagovat na útok a zachovat funkčnost i v případě velkého nárůstu nelegitimního provozu. Systém obrany by také měl obsahovat některou z metod IP tracebacku využívaných pro identifikaci původu paketu. Zvolená metoda IP tracebacku by měla být rychlá, přesná a efektivní i v případě DDoS útoku s velkým množstvím nelegitimního provozu.

Obecný systém obrany proti DDoS útoku se skládá ze tří základních modulů – monitorovací modul, detekční modul a reakční modul [1].

3.9.1 Monitorovací modul

Monitorovací modul sleduje a kontroluje používané služby a probíhající aktivity na různých místech v síti [1]. Tento modul také identifikuje neautorizované aktivity a neobvyklé chování v síti. Příčinou neobvyklého chování je buď pokus o zneužití a napadení sítě, nebo síťové anomálie.

3.9.2 Detekční modul

Detekční modul na základě informací získaných z monitorovacího modulu vytváří hlášení pro reakční modul a administrátora sítě [1]. Hlavní funkcí detekčního modulu je shromažďování dat z různých míst v síti, jejich následná analýza, analýza informací o síťovém provozu a identifikace pokusů o narušení bezpečnosti. Na základě analýzy detekuje útoky a podezřelé incidenty a podává hlášení při jejich výskytu.

3.9.3 Reakční modul

Reakční modul se skládá z pasivní a aktivní části. Pasivní část kontroluje konfigurační soubory systému a další oblasti systému s úkolem zjištit porušení nastavené bezpečnostní politiky sítě. Aktivní část reaguje na detekované útoky. Na neobvyklé chování může odpovídat různými způsoby, například vytvořením protokolu události (event log), zobrazením výstrahy, upozorněním administrátora nebo spuštěním obranných procedur systému.

3.10 Taxonomie systémů obrany proti DDoS útokům

3.10.1 Taxonomie podle struktury řízení

Struktura řízení je uspořádání dílčích podsystémů a jejich vzájemného propojení a komunikace. Podle struktury řízení se systémy obrany proti DDoS útokům dělí do tří základních kategorií – centralizované, hierarchické a distribuované [1].

Centralizovaný systém obrany

Centralizovaný systém obrany proti DDoS útokům používá lokální detekční moduly, které vytvářejí výstrahy a odesílají je na centrální server [28]. Centrální server přijímá a vyhodnocuje souvztažnosti mezi výstrahami a analyzuje je. Přesné rozhodnutí se vykonává na centrálním serveru na základě analýzy všech obdržených výstrah ze všech lokálních detekčních modulů. Centrální server musí být schopen zpracovat velké množství provozu za krátký časový úsek, aby nedošlo k přetížení a následnému kolapsu celého centralizovaného systému obrany.

Hierarchický systém obrany

Hierarchický systém obrany je rozdělen do několika dílčích podsystémů různých úrovní. Tyto podsystémy obdobně jako detekční moduly centralizovaného systému obrany vytvářejí výstrahy [1]. Podsystémy na nejnižší úrovni vytvářejí výstrahy a odesílají je podsystémům na vyšší úrovni. Podsystémy na vyšší úrovni také vytvářejí výstrahy a poté vyhodnotí jejich souvztažnost s obdrženými výstrahami z nižší úrovně. Takto vyhodnocené výstrahy jsou poté poslány do vyšší úrovně pro další analýzu. Nejvyšší úroveň obsahuje centrální jednotku.

Distribuovaný systém obrany

Distribuovaný systém obrany se skládá z plně autonomních systémů s distribuovanou kontrolou řízení [28]. Distribuovaný systém nepoužívá žádnou centrální jednotku. Všechny autonomní systémy mají vlastní části, které spolu navzájem komunikují. Selhání jednoho autonomního systému způsobí kolaps obrany pouze konkrétní části sítě.

3.10.2 Taxonomie systémů obrany podle umístění

Systém obrany může být umístěn ve třech různých sítích – v cílové síti, ve zdrojové síti nebo v propojovací síti [1]. Cílová síť je síť chráněného subjektu – ten poskytuje anebo využívá internetové služby a zároveň může být cílem DDoS útoku. Zdrojová síť je příjemcem i odesílatelem legitimního provozu. Zároveň z ní může být prováděn DDoS útok. Propojovací síť leží mezi zdrojovou a cílovou sítí a slouží pro přenos dat mezi nimi.

Umístění v cílové síti

Systém obrany umístěný v cílové síti je realizován především pomocí routerů pod přímou nebo nepřímou kontrolou cílového subjektu.

Umístění ve zdrojové síti

Systém obrany umístěný ve zdrojové síti brání potenciálním útočníkům v účasti na DDoS útoku. Detekuje a následně zahazuje pakety účastnící se DDoS útoku. Výhoda je detekce útoku a filtrování paketů předtím, než jsou směrovány do Internetu. Mechanismy

zodpovědné za reakci proti útoku musí být tolerantní a selektivní kvůli minimalizaci poškození legitimního provozu falešně pozitivními detekcemi [29].

Umístění v propojovací síti

Systém obrany umístěný v propojovací síti je navržen tak, aby překonal omezení obrany v cílové a zdrojové síti. Problém tohoto systému obrany je nasazení a zavedení, protože není jasné, kdo by zaplatil výdaje spojené s tímto systémem [49]. Aby se dosáhla co největší přesnost detekce DDoS útoku, tak musí být detekční systém obsažen v co největším počtu okrajových routerů v Internetu, jinak může dojít k selhání detekčních mechanismů [1].

3.11 Detekce DDoS útoků

Detekce DDoS útoků se dělí na dvě hlavní kategorie – detekce zneužití a detekce anomálií. Detekce zneužití hledá předem nadefinované vzory útoků v síťovém provozu k detekování známých DDoS útoků. Detekce anomálií hledá neobvyklé vzorce chování a dokáže detekovat i dosud neznámé typy útoků.

3.11.1 Detekce zneužití

Při detekci zneužití se nadefinuje abnormální chování v síťovém provozu a všechno ostatní chování se považuje za normální [1]. Detekce zneužití detekuje pouze známé útoky DDoS pomocí předem nadefinovaných charakteristik těchto útoků. Přesnost detekčního systému závisí na množství a kvalitě zpracování dat z předešlých útoků. Abnormální chování je možné definovat například signaturami, pravidly v expertním systému nebo aktivitami ve State-Transition systému. Hlavní výhodou tohoto typu detekce je vysoká úspešnost detekce známých útoků a nízký počet falešně pozitivních detekcí. Nevýhodou je, že detekce zneužití nedokáže detekovat dosud neznámé typy útoků – pokud útočník použije nový typ DDoS útoku, který nesplňuje předem nadefinované charakteristiky, systém detekce selže.

Detekce DDoS útoků založená na signaturách

Detekce založená na signaturách má v databázi uložené vzory DDoS útoků zvaných signatury. Signatura je záznam, který obsahuje zdrojovou a cílovou IP adresu, číslo portu

a případně klíčová slova z uživatelských dat paketu [50]. Síťový provoz se porovnává s těmito předem nadefinovanými vzory a pokud najde shodu, tak vygeneruje výstrahu. To je efektivní pouze pokud jsou signatury daného útoku uložené v databázi, proto se v případě nového nebo známého modifikovaného útoku výstraha nevyvolá a systém útok nedetekuje [51]. Proto je nutné databázi signatur v případě objevení nového typu DDoS útoku aktualizovat.

Detekce DDoS útoků založená na expertních systémech

Detekce založená na expertních systémech používá k odhalení útoků předem vytvořenou sadu pravidel, která popisují útoky. Pravidla vytvářejí experti analýzou již uskutečněných útoků. Expertní systémy také obsahují znalosti z předešlých narušení, známých zranitelností systému a informace o implementované bezpečnostní politice [46]. Síťový provoz se porovnává s vytvořenými pravidly k odhalení útoku.

Detekce DDoS útoků založená na State-Transition technikách

State-Transition techniky nahlíží na DDoS útoky jako na sekvenci aktivit [34]. Detekovaná aktivita nebo skupina aktivit může způsobit přechod z jednoho stavu do jiného. Napadení útokem je detekováno pokud se systém dostane do stavu označeného jako ohrožený stavu systému.

3.11.2 Detekce anomálií

Velká část chování v síťovém provozu je normální s malým množstvím abnormálního chování. Abnormální chování může představovat potenciální útok. Toto chování lze nalézt porovnáním logů a datasetů síťového provozu s vzorci předcházejících známých abnormálních chování. Kvůli velkému množství, různorodosti a neustálému růstu těchto logů a datasetů se vzory abnormálního chování velmi těžko hledají konvenčními metodami. V takovýchto situacích může být velmi výhodné implementovat některou z metod detekce anomálií.

Detekce anomálií funguje opačným způsobem než detekce zneužití, kde se předem nadefinuje normální chování v síťovém provozu a všechno ostatní chování se považuje jako abnormální. Hlavní výhodou detekce anomálií je schopnost detekovat i dosud neznámé typy útoků.

Detekce DDoS útoků založená na statistických přístupech

Statistický přístup detekce zjišťuje, zda se pozorované chování významně liší od očekávaného chování [47]. K tomu se používají statistické metody k vytvoření normálního profilu a statistické testy na zjištění, zda se pozorované aktivity výrazně odchylují od nastaveného normálního profilu. Na základě míry odchýlení je detekčním systémem přiřazena hodnota této abnomální aktivitě. Jakmile tato hodnota překročí předem určený limit, systém vyhlásí alarm.

Detekce DDoS útoků založená na strojovém učení

Strojové učení je schopnost systému se průběžně učit a zlepšovat v činnosti nebo skupině činností. Metody strojového učení se zlepšují v daných činnostech na základě předchozích výsledků – mění svoji strategii na základě nově získaných informací [48].

Detekce DDoS útoků založená na strojovém učení má za cíl vytvořit platné a smysluplné vzorce z datového souboru, který obsahuje různá data týkající se síťového provozu, pomocí algoritmu strojového učení [30]. Algoritmus strojového učení se pokouší rozeznat různé vzory z datového souboru k učinění rozhodnutí nebo předpovědi i v případě, kdy dostane nová nebo dosud neznámá data.

Detekce DDoS útoků založená na fuzzy logice

Detekce DDoS útoků založená na fuzzy logice používá fuzzy logiku – speciální logiku, která nabývá jakéhokoliv reálného čísla mezi 0 a 1 včetně [35]. Fuzzy logiku lze použít při detekci DDoS útoků, protože je vyhodnocován velký počet nejasných a neúplných parametrů (doba využití procesoru, rychlost aktivity, interval připojení) [34].

3.12 Prevence DDoS útoků

K prevenci útoků se nasazuje systém prevence průniků (Intrusion Prevention System – IPS), který v reálném čase blokuje detekované útoky [1, 31].

Mezi hlavní činnosti IPS patří spouštění alarmů, zahazování škodlivých paketů, resetování připojení a blokování provozu z daných IP adres. Pro efektivní zastavení útoku se musí včas detekovat zdroje útoku a poté zahájit příslušné kroky k identifikaci těchto zdrojů. Koordinovaná povaha DDoS útoku a decentralizovaná povaha Internetu spolu

s častým použitím podvržených IP adres dělají identifikaci zdrojů útoku v reálném čase značně obtížnou.

3.12.1 IP Traceback

Metody IP Traceback jsou používány pro identifikaci původu paketu [32]. IP Traceback se neomezuje pouze na pakety pocházející z DDoS útoků a může sloužit na identifikaci jakéhokoliv zdroje paketu na Internetu [37]. Přesná identifikace zdroje paketu je často složitá, protože zdrojová IP adresa v paketech pocházejících z DDoS útoku je mnohdy podvržená. Zdrojem paketů při DDoS útoku není často sám útočník, ale zombie, reflektor nebo jiné zařízení napadené a ovládané útočníkem.

Efektivní metoda IP Traceback by měla splňovat následující požadavky:

- minimalizovat zapojení poskytovatelů internetových služeb (ISP) – při přílišném zapojení ISP do IP Tracebacku může proces trvat delší dobu a může být potřeba větší množství zdrojů,
- minimalizovat počet paketů potřebných k provedení IP Tracebacku – zdroje útoku by měly být identifikovány ihned poté, co se detekuje útok, za použití co nejmenšího počtu paketů,
- minimalizovat režijní náklady – síťová zařízení budou vykazovat větší režijní náklady na zpracování toku paketů a výpočty různých statistických parametrů,
- minimalizovat využití paměti – síťová zařízení budou vykazovat větší zaplnění paměti kvůli ukládání informací pro IP Traceback,
- snadnou implementaci,
- škálovatelnost – metoda IP Traceback by měla být škálovatelná nezávisle na výrobcích a prodejcích síťových zařízení,
- minimalizovat režii na přenos dat – IP Traceback bude potřebovat další přenos dat a měla by se předpokládat reálná přenosová rychlost při implementaci,
- maximalizovat schopnost určení původu paketu pro co nejvíce různých typů útoků – mnoho metod IP Traceback nefunguje proti všem typům útoků.

Link Testing

Link Testing zpětně sleduje tok dat od oběti k útočníkovi. Pro úspěšné zjištění zdroje je nutné, aby DDoS útok zůstal aktivní po celou dobu sledování – tato metoda nefunguje

na jakkoliv přerušovaný DDoS útok (například metody DDoS založené na pulzním útoku). Mezi hlavní metody Link Testing patří Input Debugging a Controlled Flooding.

Při Input Debugging metodě je nejprve detekován útok a vytvořena signatura útoku, se kterou se poté porovnají všechny příchozí pakety. Pomocí porovnání signatur a paketů se postupně identifikují následující odpovídající routery, ze kterých byly směrovány pakety DDoS útoku, dokud není identifikován prvotní zdroj útoku.

Metoda Controlled Flooding testuje příchozí spojení oběti opakovaným zaplavováním každého takového spojení velkým množstvím dat. Sledováním změny v počtu přijatých paketů oběti lze identifikovat, z jakého spojení přicházejí pakety DDoS útoku. Toto je aplikováno na následující routery, dokud není identifikován prvotní zdroj útoku.

Packet Marking

Packet Marking je jedna z nejběžnějších a nejvýznamnějších metod IP Tracebacku. Tato metoda používá hlavičku IP paketu, kam ukládá auditní stopu. Mezi hlavní metody Packet Marking patří pravděpodobnostní Packet Marking a deterministický Packet Marking.

Pravděpodobnostní Packet Marking označí s určenou pravděpodobností přijatý paket (například 0,01). K takto označeným paketům uloží informaci o počtu routerů, kterými paket procházel. Tato informace se použije při následné rekonstrukci cesty paketu. Pro úspěšné nalezení zdroje paketu je potřeba dostatečné množství paketů, ale není potřeba znát topologii sítě. Tato metoda vykazuje velký počet falešně pozitivních výsledků.

Deterministický Packet Marking označí každý paket, který prochází prvním vstupním routerem. K takto označeným paketům uloží informaci o IP adrese tohoto routeru. IP adresa je rozdělená na dvě části a každá z těchto částí je náhodně zaznamenána do každého příchozího paketu. Celá IP adresa se zpětně získá, když oběť útoku získá obě části IP adresy pocházející ze stejného routeru. Deterministický Packet Marking bude hlásit falešně pozitivní zdrojovou IP adresu, pokud ji útočník podvrhl.

ICMP Traceback

ICMP Traceback s velmi malou pravděpodobností (například 0,00005) označí odesílaný paket a společně s ním odešle speciální ICMP zprávu, která obsahuje údaje

o sousedních routerech, kterými paket prochází. Takto označený odeslaný paket obsahuje autentizační pole, které chrání IP adresu před podvržením. Z ICMP zpráv lze sestavit cestu paketu a zjistit tak zdrojovou IP adresu.

IP Logging

IP Logging ukládá krátké informace o paketu jako je signatura a hlavička paketu do všech nebo některých routerů. Pokud oběť detekuje DDoS útok, tak vyžádá od nadřazeného routeru informace o tomto paketu. Po poskytnutí informací se proces zopakuje s dalším nadřazeným routerem, dokud není nalezena zdrojová IP adresa.

3.12.2 Metody filtrování paketů

Filtrování paketů síťového provozu chrání zdroje sítě před DDoS útoky.

Vstupní a výstupní filtrování

Filtrování paketů je základní mechanismus ochrany, který na základě přednastavených pravidel kontroluje a filtruje síťový provoz. Například porovnává zdrojovou IP adresu obdrženého paketu s rozsahem IP adres přiřazeným v jeho zdrojové nebo cílové síti, podle umístění daného routeru, který provádí filtrování [24]. Pakety, které se neshodují, považuje za podvržené a zahodí je. Mechanismus filtrování lze také aplikovat na čísla portů, typy protokolů a na další parametry. Vstupní filtrování paketů (Ingress Filtering) je filtrování paketů přicházejících do sítě. Výstupní filtrování paketů (Egress Filtering) je filtrování paketů odcházejících ze sítě.

Řízení rychlosti provozu

Řízení rychlosti síťového provozu je omezení nebo zpoždění rychlosti příchozích paketů podle předem nastavených kritérií. Mechanismus řízení rychlosti je navržen tak, aby legitimní provoz byl co nejméně ovlivněn. Při případném DDoS útoku nevznikají řízením rychlosti provozu žádné další režijní náklady na požadované zdroje.

Hloubková inspekce paketů

Hloubková inspekce paketů (Deep Packet Inspection – DPI) je vylepšený mechanismus filtrování paketů v reálném čase [33]. DPI se používá pro lokalizování,

detekování, kategorizování, blokování nebo přesměrování paketů, které splňují přednastavená pravidla. Na rozdíl od běžného filtrování paketů, které vyhodnocuje pouze hlavičku paketu, DPI vyhodnocuje i datovou část paketu. Velkou nevýhodou DPI je nemožnost vyhodnocovat datový obsah paketů, které jsou zašifrované – tím je jeho efektivita omezena.

4. Praktická část

4.1 Srovnání systémů obrany proti DDoS útokům

Systémy obrany proti útoku DDoS lze porovnávat na základě různých parametrů. Různé zaměřené subjekty považují za důležité rozdílné parametry. Mezi hlavní parametry patří [28]:

- Náročnost konfigurace – představuje míru časové a znalostní náročnosti potřebné pro dané nastavení systému obrany.
- Náročnost implementace – udává míru obtížnosti zavedení systému obrany.
- Nákladnost – představuje celkové náklady na implementaci a dlouhodobou údržbu systému.
- Přesnost detekce útoků – schopnost systému obrany správně identifikovat DDoS útok. Přesnost závisí na množství falešně pozitivních a falešně negativních detekcí.
- Robustnost – představuje schopnost systému odrazit útok DDoS.
- Škálovatelnost – schopnost systému zvýšit obranu v případě potřeby. Může se jednat jak o kvantitativní, tak i o kvalitativní navýšení.
- Omezení uživatelů – představuje omezení legitimních požadavků uživatelů.

4.1.1 Porovnání systémů obrany podle struktury řízení

Systémy obrany proti DDoS útokům se rozdělují podle struktury řízení na tři hlavní typy – centralizovaný, hierarchický a distribuovaný, které byly představeny v kapitole 3.10.1. Základní vlastnosti těchto typů jsou porovnány v Tabulce 1.

Tabulka 1 – Porovnání systémů obrany podle struktury řízení [28]

Vlastnost	**Centralizovaný**	**Hierarchický**	**Distribuovaný**
Náročnost implementace	nízká	střední	vysoká
Náročnost konfigurace	nízká	střední	vysoká
Nákladnost	nízká	střední	vysoká
Přesnost detekce útoku	nízká	nízká	vysoká
Robustnost	nízká	střední	vysoká
Škálovatelnost	nízká	střední	vysoká

Centralizovaný systém obrany

Centralizovaný systém obrany může být implementován v cílové síti nebo ve zdrojové síti. Hlavní výhodou centralizovaného systému je finančně méně nákladné zavedení a údržba v porovnání s ostatními systémy obrany. Systém je také snadno konfigurovatelný a je jednoduché obnovit jeho funkčnost v případě kolapsu. Centrální server systému musí být navržen tak, aby byl schopný zpracovat velké množství dat za krátké časové období. Funkčnost systému tedy záleží na velikosti útoku – systém může selhat, pokud má DDoS útok velkou přenosovou rychlost. U centralizovaného systému selhání jakékoliv jeho části vede ke kolapsu celého systému.

Hierarchický systém obrany

Hierarchický systém obrany může být implementován v cílové síti nebo ve zdrojové síti. Hlavní výhodou hierarchického systému je větší škálovatelnost (snadnější přidaní dalších modulů) a robustnější obrana oproti centralizovanému systému – pokud dojde k selhání podsystému na nižší úrovni, tak nedojde ke kolapsu celého systému, ale pouze konkrétní části. Pokud ale dojde k selhání centrální jednotky, tak systém zkolabuje celý.

Distribuovaný systém obrany

Distribuovaný systém obrany je implementován především v propojovacích sítích. Hlavní výhoda distribuovaného systému je lepší škálovatelnost díky absenci centrální jednotky. Distribuovaný systém má nižší přesnost detekce DDoS útoků, protože nemá úplné informace o topologii sítě. Konfigurace distribuovaného systému je náročnější oproti centralizovanému systému, protože každý autonomní systém vyžaduje individuální nastavení. Distribuovaný systém obrany je velmi náročný na implementaci kvůli jeho decentralizovanému umístění na různých místech v síti.

4.1.2 Porovnání systémů obrany podle umístění

Systémy obrany proti DDoS útokům se rozdělují podle umístění na tři hlavní typy – v cílové síti, ve zdrojové síti a v propojovací síti, které byly představeny v kapitole 3.10.2. Základní vlastnosti těchto typů jsou porovnány v Tabulce 2.

Tabulka 2 – Porovnání systémů obrany podle umístění [36]

Vlastnost	**V cílové síti**	**Ve zdrojové síti**	**V propojovací síti**
Náročnost implementace	nízká	vysoká	vysoká
Náročnost konfigurace	nízká	nízká	vysoká
Nákladnost	nízká	nízká	vysoká
Přesnost detekce útoku	vysoká	nízká	střední
Robustnost	nízká	nízká	vysoká
Omezení uživatelů	nízké	vysoké	střední

Systém obrany umístěný v cílové síti

Systém obrany umístěný v cílové síti je implementován prostřednictvím routerů v cílové síti. Systém obrany v cílové síti dosahuje větší míře detekce útoku oproti ostatním umístěním. Útok je ale detekován až když se dostane do sítě oběti – obrana proti útoku je nespolehlivá, protože klienti v této síti již mohou být útokem ovlivněni. Nevýhody tohoto umístění jsou větší pravděpodobnost výskytu vedlejších škod na legitimním provozu a selhání systému při velmi vysoké přenosové rychlosti útoku DDoS.

Systém obrany umístěný ve zdrojové síti

Systém obrany umístěný ve zdrojové síti je implementován prostřednictvím routerů ve zdrojové síti. Výhoda tohoto umístění je možnost zastavení nelegitimního provozu předtím, než dorazí do cílové sítě, a redukce kolize předtím, než se nelegitimní provoz smíchá s legitimním provozem. Metody IP trackback v tomto umístění dosahují velmi vysoké přesnosti. Detekce DDoS útoků je méně spolehlivá, pokud má útok mnoho útočících hostů s podobným chováním jako při běžném provozu. Nasazení ve zdrojové síti je velmi složité, protože místo umístění systému obrany není v síti chráněného subjektu. Další nevýhodou je, že tento systém obrany zavádí síť, která nemá žádný podstatný přínos pro své klienty, a může tak docházet k vedlejším škodám na legitimním provozu. Systém detekuje útoky a filtruje pakety předtím, než jsou směrovány do Internetu a má schopnost detekovat a zastavit útok v počáteční fázi. Toto umístění zabraňuje zahlcení zdrojové i propojovací sítě.

Systém obrany umístěný v propojovací síti

Systém obrany umístěný v propojovací síti je implementován především prostřednictvím routerů v propojovací síti. Výhoda tohoto systému je detekce útoků a filtrace paketů předtím, než jsou dále směrovány do cílové sítě. Systém je oproti systému obrany umístěném v cílové síti méně náchylný proti DDoS útokům s velkou přenosovou rychlostí. Úplná reálná implementace však není v praxi možná, protože by vyžadovala přenastavení velkého množství routerů v Internetu. Vzniklé režijní náklady jsou velmi vysoké především kvůli velkému rozsahu sítě.

4.1.3 Porovnání systémů obrany podle metody detekce DDoS útoku

Systémy obrany proti DDoS útokům se rozdělují podle metody detekce DDoS útoku na dva hlavní typy – detekce zneužití a detekce anomálií, které byly představeny v kapitole 3.11. Základní vlastnosti těchto typů jsou porovnány v Tabulce 3.

Tabulka 3 – Porovnání systémů obrany podle metody detekce DDoS útoku [34]

Vlastnost	Detekce zneužití	Detekce anomálií
Náročnost konfigurace	nízká	vysoká
Robustnost	nízká	vysoká
Omezení uživatelů	nízké	vysoké

Detekce zneužití

Metody založené na detekci zneužití vykazují vysokou účinnost detekce pro známé DDoS útoky, nedetekují však typy DDoS útoků, jejichž vzorce chování dosud nebyly přidány do databáze útoků. Proto je nutné při objevení nového typu DDoS útoku aktualizovat databázi vzorců útoků. Oproti metodám detekce anomálií jsou metody detekce zneužití spolehlivější a mají menší pravděpodobnost falešně pozitivních detekcí. Na vytvoření a následné aktualizace efektivní metody detekce zneužití je potřeba podrobně analyzovat historické útoky a využít tým specializovaných odborníků. Složitost systému roste se zvyšujícím se počtem nadefinovaných vzorů útoků.

Detekce anomálií

Metody detekce anomálií oproti metodám detekce zneužití detekují známé i dosud neznámé typy útoků, dosahují ale většího množství falešně pozitivních detekcí. K plně účinnému provozu je potřeba vhodně nastavit parametry normálního chování.

4.2 Poskytovatelé obrany proti DDoS útoku

Subjekty často nepoužívají vlastní řešení obrany proti DDoS útokům a preferují řešení specializovaného poskytovatele obrany proti DDoS útoku. Mezi hlavní výhody tohoto řešení patří:

- zpravidla nižší cena,
- snadnější implementace a lepší škálovatelnost,
- není potřeba najímat a školit vlastní pracovníky včetně zkušených odborníků na DDoS problematiku,
- softwarové řešení obrany bude poskytnuto poskytovatelem obrany, a to často včetně specializovaného hardwaru,
- menší subjekty si nemohou dovolit implementovat vlastní řešení obrany z důvodu nedostatku zdrojů – specializovaný poskytovatel obrany je jejich jediná možnost, jak se DDoS útokům efektivně bránit,
- předání řízení a kontroly mimo působiště subjektu externímu poskytovateli,
- možnost implementovat moderní technické a technologické řešení obrany,
- přenesení části zodpovědnosti a rizik na poskytovatele obrany,
- umožnuje subjektu se plně zaměřit na jeho oblast činnosti,
- velký výběr specializovaných poskytovatelů obrany – velké množství poskytovatelů nabízí různá řešení obrany.

Mezi hlavní nevýhody patří:

- ztráta vlastní kontroly nad daným řešením obrany,
- plná závislost na cizím řešení obrany,
- dochází pouze k pronájmu služby po určitou dobu – nedochází k žádnému vlastnímu rozvoji DDoS obrany uvnitř subjektu,
- větší hrozba zneužití nebo odcizení informací – je žádná nebo minimální možnost kontroly pracovníků poskytovatele obrany,

- snížená možnost kontroly kvality poskytované služby.

Existuje mnoho specializovaných poskytovatelů externí obrany proti útoku DDoS, například:

Akamai [39]

Firma Akamai je jedna z největších a nejzavedenějších firem na trhu v oblasti síťové bezpečnosti. Nabízí obranu proti DDoS útokům pod názvem Kona DDoS Defender. Kona DDoS Defender využívá vlastní platformu pro zajištění vysoké škálovatelnosti a operaceschopnosti v případě útoku. Je schopná zastavit DDoS útoky ještě před jejich dosažením cílové sítě zákazníka. Akamai má k dispozici tým odborníků zaměřených na síťovou bezpečnost k dispozici nepřetržitě 24 hodin denně. Klienti mají možnost v případě probíhajícího DDoS útoku tento tým kontaktovat a požádat o pohotovostní ochranu.

Sucuri [40]

Firma Sucuri nabízí obranu proti DDoS útokům jako součást kompletní služby pro zabezpečení webu společně s monitoringem síťového provozu, detekcí a ochranou proti útokům. Sucuri nabízí 3 základní plány obrany s cenou od 199,99 do 499,99 USD ročně lišící se poskytovanými službami. Pro náročné zákazníky nabízí vlastní plán řešení obrany implementovaný na míru. Sucuri automaticky blokuje nelegitimní data bez ovlivnění legitimního provozu. Obrana využívá strojové učení a je schopna blokovat útoky na 3., 4. a 7. síťové vrstvě.

Netscout [41]

Firma Netscout poskytuje automatickou víceúrovňovou ochranu před DDoS útoky. Ochrana je integrovaná spolu s cloudovým řešením a poskytuje kompletní ochranu před všemi typy útoků. Toto řešení obrany je schopno odstranit až 11 Tb/s nelegitimního provozu při zachování legitimního provozu. Architektura je škálovatelná a vhodná pro implementaci v cloudových systémech. Řešení v reálném čase průběžně informuje o aktuálním stavu systému a historická data odesílá ke zpětnému vyhodnocení.

Cloudflare [42]

Firma Cloudflare nabízí cloudovou obranu proti DDoS útokům. Cloudflare disponuje sítí s přenosovou rychlostí 42 Tb/s a průměrně blokuje 72 miliard hrozeb denně. Blokuje DDoS útoky na 3., 4. a 7. síťové vrstvě. Obrana se skládá z více než 190 datacenter, na které je přesměrován nelegitimní provoz v případě napadení objemovým DDoS útokem. Proti nízkoobjemovým DDoS útokům Cloudflare používá metody řízení rychlosti provozu. Proaktivní obranné systémy používají strojové učení. Pro nekomerční využití nabízí Cloudflare základní ochranný plán zdarma.

StackPath [43]

Firma StackPath poskytuje kompletní systém obrany proti DDoS útokům. Systém funguje proti útokům na 3., 4. a 7. síťové vrstvě, kde využívá algoritmy chování pro detekci a zablokování objemových DDoS útoků. Sofistikované DDoS útoky na 7. síťové vrstvě je schopen webový aplikační firewall detekovat a zastavit během jedné sekundy. Na zastavení útoků používá vlastní globální síť s celkovou kapacitou 65 Tb/s. Také detekuje infiltrované zombie pomocí validačních metod. Zákazníci mají přístup k datům a statistikám v reálném čase k analýze útoků a vytvoření vlastní bezpečnostní politiky a úpravě síťových zásad a pravidel.

Radware [44]

Firma Radware nabízí jak hardwarové řešení, tak i softwarové řešení obrany. Hardwarové řešení je dedikované zařízení určené pro prevenci a ochranu proti DDoS útokům. Zařízení pracuje v reálném čase a poskytuje automatizovanou obranu proti různým typům DDoS útoků včetně nových a dosud neznámých útoků. Softwarové řešení se skládá ze skupiny bezpečnostních odboníků (Emergency Response Team – ERT), která se zabývá výzkumem bezpečnostních hrozeb a poskytuje podporu pro celou řadu hrozeb včetně DDoS útoků. ERT analyzuje populární i nové útoky a poskytuje zákazníkům odborné znalosti, osvědčené postupy a znalosti hrozeb, útočných nástrojů, zpravodajských a zmírňujících technologií. ERT umožňuje subjektům rozšířit svá současná řešení obrany.

4.3 Obrana proti DDoS útokům pro modelové subjekty

Zajištění obrany proti DDoS útoku je potřebné pro mnohé subjekty, které využívají internetové služby. Mezi tyto subjekty patří například soukromé společnosti, akciové společnosti, školy, státní organizace, neziskové organizace a soukromé servery. Různé subjekty požadují různé vlastnosti systému obrany proti DDoS útokům, proto jsou pro ně vhodná odlišná řešení obrany.

4.3.1 Banka

Hlavní služba závisející na Internetu je internetové bankovnictví. Internetové bankovnictví je rozhraní mezi bankou a jejími klienty. Využívá se pro správu finančních prostředků a provádění finančních transakcí. Nejdůležitější je bezpečnost a integrita bankovního systému a stálá dostupnost bankovních služeb. Výpadky jsou pro klienty nepříjemné, protože mohou způsobit mnoho problémů (například nemožnost splatit závazky).

Hrozba DDoS útoku na banky je vysoká, protože finanční sektor je cílem DDoS útoku v 42% za rok 2017 [14]. Úspěšný DDoS útok může bance způsobit finanční ztráty i dlouhodobé problémy (ztráta reputace, odliv klientů).

Pro banku je důležité mít kontrolu nad systémem obrany proti DDoS. Přenechání kontroly externímu poskytovateli je bezpečnostním rizikem a banka musí důkladně zvážit hrozbu zneužití dat. Proto je vhodné implementovat vlastní řešení obrany proti DDoS útoku. Nejdůležitější vlastnosti systému obrany pro banku jsou robustnost, přesnost detekce útoků a spolehlivost. Proto je možné doporučit implementaci distribuovaného systému obrany nasazeném v síti banky. Robustní systém by měl detekovat anomálie, což umožní obranu i proti novým typům DDoS útoků.

4.3.2 Zpravodajský server

Hlavní funkcí zpravodajských serverů je poskytování aktuálních a nepřetržitých multimediálních zpravodajských služeb. Pro zákazníky je důležitá stálá dostupnost služby.

Motivace za DDoS útoky na zpravodajské servery může být jak finančního, tak i nefinančního charakteru (například politického). Ve vysoce konkurenčním prostředí mohou časté (i krátkodobé) výpadky poskytované služby vést ke ztrátě zákazníků.

Na obranu proti DDoS útoku lze zvolit řešení poskytované firmou Sucuri. Firma Sucuri nabízí finančně dostupné řešení ochrany, které lze v případě potřeby snadno rozšířit. Řešení ochrany navíc není určené pouze proti DDoS útokům, ale obsahuje i pravidelné antimalwarové kontroly, odstraňování malwaru a vlastní firewall. Nejlevnější řešení obrany od firmy Sucuri stojí 199,99 USD ročně.

Pokud zpravodajský server implementuje vlastní řešení obrany, je vhodné vybrat řešení, které je jednoduché na implementaci a konfiguraci a není příliš nákladné. Proto je nejlepší implementovat centralizovaný systém nasazený ve vlastní síti. Omezení uživatelů systémem obrany by mělo být nízké, protože zpravodajský server je často uživateli frekventovaně navštěvován a jejich omezení v podobě například delšího čekání na načtení webové stránky je nežádoucí. Proto je vhodnější využít systém obrany proti DDoS založený na detekci zneužití.

4.3.3 Cloudové úložiště

Cloudové úložiště poskytuje pro zákazníky virtuální úložný prostor. Pro zákazníky je důležitá nejen neustálá dostupnost služby, ale také vysoká přenosová rychlost a možnost přistupovat ke cloudovém uložišti odkudkoliv pomocí Internetu. DDoS útoky jsou nebezpečné pro cloudové úložiště tím, že sníží nebo úplně zablokují přenosovou kapacitu a učiní přístup ke cloudovému úložišti nemožný. Následkem je kolísavá kvalita nabízených služeb a odchod zákazníků, případně i nutnost finanční kompenzace.

Systém obrany musí mít dostatečnou datovou propustnost, aby nedocházelo k omezení zákazníků. Velkou výhodou systému je možnost škálovatelnosti – ta v případě potřeby umožní zvýšení datové propustnosti sytému obrany.

Vhodným řešením je obrana firmy Cloudflare, která je vhodná pro implementaci v cloudových systémech díky velké propustnosti provozu a nadprůměrným možnostem škálování. Pro menší cloudové úložiště lze využít řešení firmy Netscout, které je dostatečné pro systémy, kterým stačí menší datová propustnost.

Alternativní možností je implementovat vlastní řešení. Hlavní výhodou vlastního řešení je implementace na míru podle architektury cloudu. Pro cloudové uložiště je důležité nízké omezení uživatelů a škálovatelnost kvůli případnému rozšiřování. Proto je vhodné zvolit distribuovaný systém obrany nasazený v cílové síti s využitím detekce zneužití.

4.3.4 Nemocnice

Nemocnice potřebuje přístup k Internetu kvůli komunikaci se vzdálenými pracovišti (například laboratořemi) a informačním systémům pro lékaře i klienty. Nemocniční přístroje mohou být součástí Internetu věcí, což je vystavuje zvýšenému nebezpečí kybernetického útoku.

Nemocnice jsou pro útočníky výhodný cíl DDoS útoku, protože se jedná o část kritické infrastruktury státu, jejíž výpadek či omezení funkčnosti může mít závažný dopad na zdraví obyvatel. DDoS útok může značně omezit běžný provoz nemocnice po dobu trvání útoku. DDoS útok na nemocnici může být také často doprovázen jiným typem útoku, který může cílit na odcizení citlivých dat o zdravotním stavu pacientů – tato data mají na internetovém černém trhu vyšší finanční hodnotu než je hodnota přístupových hesel nebo informací o platebních kartách [38].

Vzhledem k tomu, že internetové služby, které nemocnice poskytuje, nejsou její hlavní činností, je výhodné přenechat obranu proti DDoS útokům externím poskytovatelům. Pro účely nemocnice lze doporučit řešení obrany firmy Akamai s názvem Kona DDoS Defender. Kona DDoS Defender poskytuje dostatečnou možnost škálovatelnosti a velkou výhodou je v případě napadení DDoS útokem možnost kontaktovat jejich tým odborníků a vyžádat si pohotovostní ochranu.

Při implementaci vlastního řešení obrany je vhodné nasadit distribuovaný systém s detekcí anomálií – takový systém je robustní a má šanci detekovat sofistikované útoky, kterými může být nemocnice cílena například za účelem vydírání.

4.3.5 On-line herní platforma

Platforma umožňuje hraní her přes Internet – vyhledávání spoluhráčů a protivníků, realizaci hry na herním serveru a komunikaci mezi hráči. Pro hráče je důležitá dostupnost služby a také její kvalita (pro mnohé hry je například důležitá nízká latence).

On-line herní průmysl je častým cílem DDoS útoků, proto by subjekty neměly obranu podceňovat. Hrozí především útoky s nefinanční motivací. Krátkodobé výpadky služby způsobí nevoli hráčů, což může vést k finančním ztrátám. Dlouhodobé výpadky mohou způsobit odchod hráčů ke konkurenci.

Na obranu proti DDoS útokům je vhodné využít externího poskytovatele, protože investice do vlastního řešení obrany je pro herní společnosti většinou nedostupná. Vhodné

řešení nabízí firma G-Core-Labs, protože poskytuje ochranu proti DDoS útokům dedikovanou přímo pro herní servery [53].

Pokud chce subjekt zavést vlastní řešení obrany, je vhodné implementovat například centralizovaný systém v cílové síti s detekcí zneužití. Jeho výhodou je nízká nákladnost a hráči jím nejsou nadměrně omezováni.

4.4 Obrana proti útokům DDoS pro fiktivní subjekt

V předchozí kapitole jsou popsány možnosti obrany proti DDoS pro modelové subjekty, ale výběr optimálního systému obrany vždy závisí na konkrétních požadavcích a specifikacích daného subjektu. Proto je vhodné ukázat výběr systému obrany na konkrétním příkladu. Jako subjekt byla zvolena fiktivní společnost poskytující cloudové úložiště specializované na soubory zvukového designu. V tomto cloudovém úložišti jsou uloženy soubory ve zvukovém formátu – typicky s bezztrátovou kompresí (například formáty wav, aiff, flac). Cloud obsahuje řádově statisíce souborů a tisíce aktivních uživatelů. Požadavky a očekávání subjektu na systém obrany jsou:

- datová propustnost alespoň 1 GB/s,
- nízká finanční nákladnost – velmi důležité,
- jednoduchá implementace a konfigurace – důležité,
- nízké omezení uživatelů – méně důležité,
- subjekt neočekává výraznou změnu počtu uživatelů ani potřebné datové propustnosti.

Na základě požadavků subjektu byly přiřazeny jednotlivým vlastnostem systémů obrany váhy v rozsahu od 0 do 1, které vyjadřují jejich relativní důležitost (0 je nejnižší, 1 nejvyšší). Váhy jsou uvedeny v Tabulce 4, byly stanoveny tak, aby rovnoměrně pokrývaly interval od 0 do 1 v závislosti na důležitosti vlastností systému pro daný subjekt. Nákladnost má nejvyšší váhu 1, protože finančně nenáročné řešení je pro subjekt velmi důležité. Pro subjekt je dále důležitá nízká náročnost konfigurace a implementace systému. Proto je těmto vlastnostem přiřazena váha 0,8. Další v pořadí důležitosti je výše omezení uživatelů – pro něj je zvolena váha 0,6. Přesnost detekce útoků a robustnost jsou pro subjekt málo důležité, proto jim je přiřazena váha 0,4. Škálovatelnost má nejnižší váhu 0,2, protože subjekt v budoucnosti neočekává výraznou změnu potřebné datové propustnosti.

První možností je implementace vlastního řešení obrany. Při rozhodování s výběrem vhodného řešení může pomoci Tabulka 4. V posledních dvou řádcích tabulky je skóre jednotlivých typů systémů obrany, což vyjadřuje jejich relativní vhodnost pro dané cloudové úložiště. Pro výpočet skóre byl zvolen vážený součet hodnot všech vlastností, slovní hodnoty jednotlivých vlastností z kapitoly 4.1 jsou nahrazeny čísly (0 – nejhorší, 2 – nejlepší). V předposledním řádku Tabulky 4 je absolutní skóre, v posledním řádku je relativní skóre (absolutní skóre pro každou kategorii rozdělení metod obrany přeškálované do intervalu 0 až 1).

Tabulka 4 – Hodnocení typů systémů obrany pro fiktivní subjekt

Vlastnost	**Váha**	**Podle struktury řízení**			**Podle umístění**			**Podle metody detekce**	
		Centr.	Hier.	Distr.	Cíl.	Zdroj.	Prop.	Zneužití	Anomálie
Náročnost konfigurace	0,8	2	1	0	2	2	0	2	0
Náročnost implementace	0,8	2	1	0	2	0	0	–	–
Nákladnost	1	2	1	0	2	2	0	–	–
Přesnost detekce útoků	0,4	0	0	2	2	0	1	–	–
Robustnost	0,4	0	1	2	0	0	2	0	2
Škálovatelnost	0,2	0	1	2	–	–	–	–	–
Omezení uživatelů	0,6	–	–	–	2	0	1	2	0
Skóre		**5,2**	**3,2**	**2**	**7,2**	**3,6**	**1,8**	**2,8**	**0,8**
Relativní skóre		**1**	**0,375**	**0**	**1**	**0,333**	**0**	**1**	**0**

Nejvhodnější systém je ten, který má nejvyšší skóre v každé kategorii rozdělení metod obrany. Pro dané cloudové úložiště je tedy nejvhodnější centrálně řízený systém umístěný v cílové síti využívající detekci zneužití.

Alternativní možností je využít specializovaného poskytovatele obrany proti útoku DDoS. To se pro tento subjekt jeví jako lepší řešení – zejména kvůli požadavku subjektu na nízkou finanční nákladnost a jednoduchou implementaci a konfiguraci. Lze využít například poskytovatele Cloudflare, který nabízí plán Pro od 20 USD měsíčně.

5. Výsledky a diskuze

V bakalářské práci jsou popsány a porovnány různé typy systémů obrany proti DDoS útoku. Každý systém obrany má odlišné vlastnosti, výhody a nevýhody. Souhrnná efektivita systému nejde přesně vyčíslit, protože záleží nejen na konkrétní implementaci daného systému obrany, ale i na parametrech chráněného systému.

Výběr vhodného systému obrany proti DDoS útoku závisí na tom, jaké internetové služby subjekt využívá a poskytuje a na tom, jak nebezpečné DDoS útoky pro něj mohou být. Každý subjekt, kterému hrozí DDoS útok, by měl provést analýzu těchto faktorů a podle toho implementovat adekvátní plán obrany. Je také třeba počítat s negativními dopady obranného systému. Například příliš velké omezení uživatelů systémem obrany může způsobit jejich odchod – to může subjektu způsobit vyšší finanční ztrátu než potenciální hrozba DDoS útoku. Je také důležité vyčlenit prostředky na údržbu, aktualizaci a případné rozšiřování systému.

Subjekt může zavést vlastní řešení obrany nebo použít řešení od externího poskytovatele obrany. Obě varianty mají svá úskalí. Zavedení vlastního řešení obrany je finančně, technologicky a časově náročné, ale subjekt má nad systémem obrany plnou kontrolu. Využití externího poskytovatele je pro většinu subjektů dostupnější a jednodušší, na trhu však působí mnoho poskytovatelů a je obtížné vybrat nejvhodnějšího. Účinnost systémů jednotlivých poskytovatelů nelze z veřejně dostupných informací zjistit, proto je nemožné nabídky poskytovatelů zcela relevantně porovnat.

6. Závěr

V práci jsou představeny, popsány a porovnány různé možnosti obrany proti DDoS útoku. Ukázalo se, že žádná z popsaných možností není univerzálně nejlepší – každá má jiné vlastnosti, přednosti a slabiny. Při nasazování systému proti DDoS útoku je nutné analyzovat potřeby a požadavky chráněného subjektu a vytvořit co nejoptimálnější plán obrany. Obrana se realizuje buď využitím specializovaného poskytovatele obrany proti DDoS, nebo implementací vlastního řešení.

Při používání systému obrany proti DDoS útoku je nutné průběžně kontrolovat a vyhodnocovat jeho efektivitu a podle potřeby systém rozšířit, vylepšit nebo implementovat jiný systém.

Od počátku Internetu roste množství a diverzita internetových služeb a jejich význam a využití pro společnost. Společně s růstem Internetu se však zvyšuje i kyberkriminalita, jejíž významnou částí je útok DDoS. Je pravděpodobné, že tento trend bude pokračovat i v budoucnosti. Počet DDoS útoků bude narůstat, jejich síla poroste, budou se využívat nové technologie a vzniknou nové typy útoků. Stávající metody obrany proti DDoS útokům budou překonány, a proto je potřeba je neustále vylepšovat a vyvíjet metody nové.

7. Seznam použitých zdrojů

[1] BHATTACHARYYA, D. K. a KALITA, J. K. DDoS Attacks: Evolution, Detection, Prevention, Reaction, and Tolerance. Boca Raton: CRC Press, 2016. ISBN 978-1-4987-2964-2.

[2] GRYGAŘÍKOVÁ, Michaela. *Anti-DDoS ochrana aneb Proč jen firewall nestačí* [online]. 09. 09. 2019 [cit. 2020-11-03]. Dostupné z: https://www.master.cz/blog/anti-ddos-ochrana-proc-firewall-nestaci/

[3] RADWARE. *Radware's DDoS Handbook: The Ultimate Guide to Everything You Need to Know about DDoS Attacks.* Radware, 2013.

[4] BUSTAMANTE, Jaleesa. IoT Statistics. *IPropertyManagement* [online]. [cit. 2019-12-04]. Dostupné z: https://ipropertymanagement.com/iot-statistics

[5] CID, Daniel. Large CCTV Botnet Leveraged in DDoS Attacks. *Sucuri Blog* [online]. [cit. 2019-12-04]. Dostupné z: https://blog.sucuri.net/2016/06/large-cctv-botnet-leveraged-ddos-attacks.html

[6] Booters, Stressers and DDoSers. *Imperva* [online]. [cit. 2019-12-06]. Dostupné z: https://www.imperva.com/learn/application-security/booters-stressers-ddosers/

[7] STRAWBRIDGE, Geraldine. 10 Biggest DDoS Attacks and how your organisation can learn from them. *MetaCompliance* [online]. May 28, 2019 [cit. 2019-12-13]. Dostupné z: https://www.metacompliance.com/blog/10-biggest-ddos-attacks-and-how-your-organisation-can-learn-from-them/

[8] NICCOLAI, James. Analyst puts hacker damage at $1.2 billion and rising. *InfoWorld* [online]. February 10, 2000 [cit. 2019-12-13]. Dostupné z: https://web.archive.org/web/20071112081103/http://www.infoworld.com/articles/ic/xml/00/02/10/000210icyankees.html

[9] A look at Estonia's cyber attack in 2007. *NBC News* [online]. 7/8/2009 [cit. 2019-12-13]. Dostupné z: http://www.nbcnews.com/id/31801246/ns/technology_and_science-security/t/look-estonias-cyber-attack/

[10] *What is the Mirai Botnet?* [online]. [cit. 2019-12-14]. Dostupné z: https://www.cloudflare.com/learning/ddos/glossary/mirai-botnet/

[11] JEFFREY, Cal. GitHub falls victim to largest DDoS attack ever recorded. *TechSpot* [online]. March 1, 2018 [cit. 2019-12-14]. Dostupné z: https://www.techspot.com/news/73522-github-hit-massive-ddos-attack.html

[12] ENNIS, Dan. DDoS Attacks: 3 Common Motivations. *Trusted Knight* [online]. 13.12.2016 [cit. 2019-12-20]. Dostupné z: https://www.trustedknight.com/ddos-attacks-3-common-motivations/

[13] SPACEY, John. The 5 Motives for DDoS Attack. *Simplicable* [online]. March 14, 2011 [cit. 2019-12-20]. Dostupné z: https://arch.simplicable.com/arch/new/the-5-motives-for-ddos-attack

[14] *13th Worldwide Infrastructure Security Report* [online]. 2018 [cit. 2019-12-26]. Dostupné z: https://www.itnewsafrica.com/2018/02/arbor-networks-13th-annual-worldwide-infrastructure-security-report-revealed/

[15] 35 Types of DDoS Attacks Explained. *JavaPipe* [online]. [cit. 2020-01-14]. Dostupné z: https://javapipe.com/blog/ddos-types/

[16] Ping flood (ICMP flood). *Imperva* [online]. [cit. 2020-01-14]. Dostupné z: https://www.imperva.com/learn/application-security/ping-icmp-flood/

[17] HTTP Flood. *Imperva* [online]. [cit. 2020-01-14]. Dostupné z: https://www.imperva.com/learn/application-security/http-flood/

[18] TCP SYN Flood. *Imperva* [online]. [cit. 2020-01-17]. Dostupné z: https://www.imperva.com/learn/application-security/syn-flood/

[19] UDP Flood. *Imperva* [online]. [cit. 2020-01-17]. Dostupné z: https://www.imperva.com/learn/application-security/udp-flood/

[20] IP Null Attack. *DDoS-GUARD* [online]. [cit. 2020-01-18]. Dostupné z: https://ddos-guard.net/en/terminology/attack_type/ip-null-attack

[21] What Is an ACK Flood DDoS Attack? | Types of DDoS Attacks. *Cloudflare* [online]. [cit. 2020-01-20]. Dostupné z: https://www.cloudflare.com/learning/ddos/what-is-an-ack-flood/

[22] SNMP Reflection/Amplification. *Imperva* [online]. [cit. 2020-01-22]. Dostupné z: https://www.imperva.com/learn/application-security/snmp-reflection/

[23] What is a Botnet? *Cloudflare* [online]. [cit. 2020-01-24]. Dostupné z: https://www.cloudflare.com/learning/ddos/what-is-a-ddos-botnet/

[24] MIRKOVIC, Jelena, Sven DIETRICH, David DITTRICH a Peter REIHER. *Internet Denial of Service: Attack and Defense Mechanisms*. Prentice Hall, 2005. ISBN 978-0-1327-0454-0.

[25] NTP Flood: Amped and Dangerous. *Imperva* [online]. [cit. 2020-02-01]. Dostupné z: https://www.imperva.com/blog/ntp-flood-explained/

[26] What is a SSDP DDoS Attack? *Cloudflare* [online]. [cit. 2020-02-01]. Dostupné z: https://www.cloudflare.com/learning/ddos/ssdp-ddos-attack/
[27] DNS Amplification. *Imperva* [online]. [cit. 2020-02-01]. Dostupné z: https://www.imperva.com/learn/application-security/dns-amplification/
[28] SINGH, Karanbir, Kanwalvir Singh DHINDSA a Bharat BHUSHAN. Distributed Defense: An Edge over Centralized Defense against DDos Attacks. *I. J. Computer Network and Information Security* [online]. 2017 [cit. 2020-02-09]. DOI: 10.5815/ijcnis.2017.03.05. Dostupné z: 10.5815/ijcnis.2017.03.05
[29] MIRKOVIC, J., G. PRIER a P. REIHER. Source-end DDoS defense. In: *Second IEEE International Symposium on Network Computing and Applications.* Cambridge, MA, USA: NCA 2003, 2003, s. 171-178. DOI: 10.1109/NCA.2003.1201153. ISBN 0-7695-1938-5.
[30] BHATTACHARYYA, Dhruba Kumar a Jugal Kumar KALITA. *Network Anomaly Detection: A Machine Learning Perspective* [online]. CRC Press, 2014 [cit. 2020-02-13]. ISBN 978-1-4665-8209-5. Dostupné z: https://dlscrib.com/network-anomaly-detection-a-machine-learning-perspective_5869c3aa6454a7453035c079_pdf.html
[31] FUCHSBERGER, Andreas. Intrusion detection systems and intrusion prevention systems. *Information Security Technical Report.* 2005, 134-139. DOI: 10.1016/j.istr.2005.08.001.
[32] CUSACK, Brian, Zhuang TIAN a Ar Kar KYAW. In: *Interoperability, Safety and Security in IoT: Second International Conference, InterIoT 2016 and Third International Conference, SaSeIoT 2016, Paris, France, October 26-27, 2016, Revised Selected Papers.* 2016. DOI: 10.1007/978-3-319-52727-7_14. ISBN 978-3-319-52726-0. ISSN 1867-8211.
[33] BROOK, Chris. What is Deep Packet Inspection? How It Works, Use Cases for DPI, and More. *Digital Guardian* [online]. December 5, 2018 [cit. 2020-02-15]. Dostupné z: https://digitalguardian.com/blog/what-deep-packet-inspection-how-it-works-use-cases-dpi-and-more
[34] KAUR, Parneet, Manish KUMAR a Abhinav BHANDARI. A review of detection approaches for distributed denial of service attacks. In: *Systems Science & Control Engineering.* 5th. Informa, 2017, s. 301-320. DOI: 10.1080/21642583.2017.1331768. ISSN 2164-2583.
[35] NOVÁK, Vilém, Irina PERFILJEVA a Jiří MOČKOŘ. *Mathematical Principles of Fuzzy Logic*. Springer, 1999. ISBN 978-0-792-38595-0.

[36] PRASAD, K. Munivara, A. Rama Mohan REDDY a K.Venugopal RAO. DoS and DDoS Attacks: Defense, Detection and Traceback Mechanisms -A Survey. *Global Journal of Computer Science and Technology: E Network, Web & Security* [online]. 2014, **14**(7) [cit. 2020-02-21]. ISSN 0975-4172. Dostupné z: https://globaljournals.org/GJCST_Volume14/3-DoS-and-DDoS-Attacks-Defense-Detection.pdf

[37] MURUGESAN, Viji, Mercy SHALINIE a Nithya NEETHIMANI. A Brief Survey of IP Traceback Methodologies. *Acta Polytechnica Hungarica*. 2014, **11.**, 197-216.

[38] TAYLOR, Mark. Healthcare is in Cybercriminals' Crosshairs. *Radware Blog* [online]. August 6, 2019 [cit. 2020-02-28]. Dostupné z: https://blog.radware.com/security/ddosattacks/2019/08/healthcare-is-in-cybercriminals-crosshairs/

[39] *Akamai* [online]. [cit. 2020-03-03]. Dostupné z: https://www.akamai.com/

[40] *Sucuri* [online]. [cit. 2020-03-03]. Dostupné z: https://sucuri.net/

[41] *Netscout* [online]. [cit. 2020-03-03]. Dostupné z: https://www.netscout.com/

[42] *Cloudflare* [online]. [cit. 2020-03-06]. Dostupné z: https://www.cloudflare.com/

[43] *StackPath* [online]. [cit. 2020-03-07]. Dostupné z: https://www.stackpath.com/

[44] *Radware* [online]. [cit. 2020-03-07]. Dostupné z: https://www.radware.com/

[45] KOTEY, Seth Djane, Eric Tutu TCHAO a James Dzisi GADZE. On Distributed Denial of Service Current Defense Schemes. *Technologies* [online]. 2019 [cit. 2020-08-23]. DOI: 10.3390/technologies7010019. Dostupné z: 10.3390/technologies7010019

[46] GYANCHANDANI, Manasi, J.L. RANA a R.N. YADAV. Taxonomy of Anomaly Based Intrusion Detection System: A Review. *International Journal of Scientific and Research Publications* [online]. 2012, 2012, **2**(12) [cit. 2020-08-26]. ISSN 2250-3153. Dostupné z: http://www.ijsrp.org/research-paper-1212/ijsrp-p1232.pdf

[47] QAYYUM, A., M.H. ISLAM a M. JAMIL. Taxonomy of statistical based anomaly detection techniques for intrusion detection. *Proceedings of the IEEE Symposium on Emerging Technologies* [online]. 2005 [cit. 2020-08-27]. DOI: 10.1109/ICET.2005.1558893. ISBN 0-7803-9247-7. Dostupné z: https://ieeexplore.ieee.org/document/1558893

[48] PATCHA, Animesh a Jung-Min PARK. An overview of anomaly detection techniques: Existing solutions and latest technological trends. *Computer Networks* [online].

2007, **51**(12) [cit. 2020-08-27]. DOI: 10.1016/j.comnet.2007.02.001. Dostupné z: https://www.sciencedirect.com/science/article/abs/pii/S138912860700062X
[49] REIHER, Peter a Jelena MIRKOVIC. A taxonomy of DDoS attack and DDoS Defense mechanisms. *ACM SIGCOMM Computer Communication Review*. 2004. Dostupné z: doi:10.1145/997150.997156
[50] XIA, T., G. G. QU, S. HARIRI a M. YOUSIF. An efficient network intrusion detection method based on information theory and genetic algorithm. *PCCC 2005. 24th IEEE International Performance, Computing, and Communications Conference, 2005.* [online]. [cit. 2020-10-02]. ISSN 2374-9628. Dostupné z: doi:10.1109/PCCC.2005.1460505
[51] CHAUHAN, A., G. MISHRA a G. KUMAR. Survey on Data Mining Techniques in Intrusion Detection. *International Journal of Scientific & Engineering Research* [online]. 2011, **2**(7) [cit. 2020-10-02]. ISSN 2229-5518.
[52] THAKKAR, D. Preventing Digital Extortion: Mitigate ransomware, DDoS, and other cyberextortion attacks. Birmingham: Packt, 2017. ISBN 978-1-78712-036-5.
[53] GAME SERVER DDOS PROTECTION. *G-Core Labs* [online]. [cit. 2020-11-04]. Dostupné z: https://gcorelabs.com/ddos-protection-for-game-servers/

Obrázky

[Obrázek 1] 13th Worldwide infrastructure Security Report. In: *Netscout* [online]. 2018 [cit. 2019-11-19]. Dostupné z: https://pages.arbornetworks.com/rs/082-KNA-087/images/13th_Worldwide_Infrastructure_Security_Report.pdf
[Obrázek 2] Ataque Smurf. In: *Wikipedia* [online]. [cit. 2019-11-25]. Dostupné z: https://commons.wikimedia.org/wiki/File:Ataque_Smurf.jpg
[Obrázek 3] Internet of Things Statistics. In: *IoTech* [online]. [cit. 2019-11-28]. Dostupné z: https://www.the-iot.co.uk/news/internet-of-things-statistics/
[Obrázek 4] GitHub Survived the Biggest DDoS Attack Ever Recorded. In: *WIRED* [online]. 03.01.2018 [cit. 2019-12-10]. Dostupné z: https://www.wired.com/story/github-ddos-memcached/
[Obrázek 5] Abuse of Open Network Service in Distributed Reflection Denial of Service (DRDoS) Attack. In: *HKCERT* [online]. 24.2.2014 [cit. 2020-12-19]. Dostupné z: https://www.hkcert.org/my_url/blog/14022401