Gymnázium a ZUŠ Šlapanice, příspěvková organizace

DDoS útoky a bezpečnost na internetu

Brno

2022/2023

Vojtěch Zima

ROČNÍKOVÁ PRÁCE

Obor: Informatika

DDoS útoky a bezpečnost na internetu

DDoS attacks and security on the Internet

Gymnázium a ZUŠ Šlapanice, příspěvková organizace

VEDOUCÍ PRÁCE:

Mgr. Ondrůšek Roman

AUTOR:

Zima Vojtěch

Brno

2022–2023

Prohlášení

Prohlašuji, že jsem tuto ročníkovou práci vypracoval samostatně s použitím uvedené literatury a pramenů.

V ..... dne ....

podpis

Poděkování

Rád bych zde poděkoval všem lidem, kteří mi pomohli při tvorbě této ročníkové práce, především pak vedoucímu práce Mgr. Romanu Ondrůškovi.

Anotace

Práce se zabývá DDoS útoky a bezpečností uživatele na Internetu. V teoretické části jsou rozebrána témata jako networking, typy DDoS útoků a jejich dopady na společnost. Praktická část navazuje na teoretickou a doplňuje ji návodem na způsoby ochrany proti DDoS útokům. Na konci práce jsou uvedeny závěry, seznam použitých pramenů s časovým razítkem a příloha.

Abstract

The work deals with DDoS attacks and user security on the Internet. The theoretical part discusses topics such as networking, types of DDoS attacks, and their impact on society. The practical part follows from the theoretical part and supplements it with instructions on how to protect against DDoS attacks. At the end of the thesis, there are conclusions, a list of used sources with a time stamp, and an appendix.

Klíčová slova

DDoS útoky, bezpečnost na Internetu, Gymnázium a ZUŠ Šlapanice

Keywords

DDoS attacks, security on the Internet, Gymnázium a ZUŠ Šlapanice

Obsah

Úvod

Pojem DDoS attack nebo také DDoS útok rezonuje v naší společnosti čím dál tím častěji, avšak většina lidí ani neví, o co se jedná. Občas také mívají mylnou představu a často zaměňují tento kybernetický útok[1] za hackerské útoky jiným typem malwaru[2]. Cílem této ročníkové práce je zmapovat povědomí lidí o tomto tématu napříč zájmovými oblastmi prostřednictvím dotazníku, ale také vytvořit přehledný návod pro vyvarování a ubránění se těmto útokům, který zároveň pomůže každému ke zvýšení své bezpečnosti na internetu.

[1] Kyber(netický) útok[2] je útok v počítačové síti, jehož účelem je například narušení infrastruktury sítě, osobních počítačů…

[2] Malware[3] je škodlivý program vytvořený za účelem zneužití zařízení uživatele ve prospěch neoprávněné osoby (útočníka). Vychází jako zkratka z anglického *malicious software*.

Obecná charakteristika, označení pojmů

Abychom věděli, jak se zabezpečit proti DDoS útokům, je nejdříve důležité pochopit jejich princip, který je úzce spojen se samotným fungování internetu. V následujících kapitolách se proto dozvíte důležité pojmy, které zde v celé práci budeme hojně využívat.

DoS útok

Za DoS attack nebo také DoS útok se označuje útok za účelem zmatení, přehlcení nebo vypnutí cílového bodu, jímž může být jak počítač, tak proces nebo server, pomocí zasílání obrovského množství požadavků. Principem všech těchto kybernetických útoků je využití různých funkcí internetu, které potřebuje sám o sobě k fungování (například: ping, TCP požadavky), probíhajících za normálních podmínek neustále, a za které se snaží útočník skrýt a vydávat se tak za pouze velký nátlak obyčejných uživatelů, nikoliv uměle vytvořených požadavků počítačem. Protože však existují různé zabezpečovací systémy (například firewall) nebo služby jako Cloudflare, o kterých se dozvíte více dále v práci, tento DoS útok může být jednoduše odhalen a úspěšně zablokován společně s dalšími podobně vypadajícími požadavky (jinými slovy s požadavky, které jsou součástí DoS útoku). Z tohoto důvodu se útočníci snaží využívat sofistikovanějších požadavků, které však neposílají z jednoho počítače, nýbrž z celé sítě počítačů, aby tím zvýšili právě svoji úspěšnost. Takovémuto útok se pak přezdívá DDoS útok.[1][4]

DDoS útok

Pojem DDoS útok vychází z anglického výrazu Distributed Denial-of-Service attack (v překladu z angličtiny: distribuované odepření služby). Jedná se v podstatě pouze o komplexnější DoS attack, který však v dnešním světě představuje velkou hrozbu. Mnohem větší hrozbu než DoS útok. Jediným rozdílem mezi DoS a DDoS útokem je ten, že DoS útok, na rozdíl od DDoS

útoku, vykonává pouze jedno zařízení. V případě DDoS útoku požadavky posílá více zařízení současně, většinou nezávisle na sobě. V extrémních případech se může jednat klidně o řádově tisíce až miliony zařízení. Pro různé typy ochran proti těmto útokům se pak mnohem hůře rozlišuje, jaké požadavky přichází od normálního uživatele a jaké přichází od útočného zařízení. Samotná myšlenka využití více zařízení znamená více síly a více požadavků pro zpracování cílovým zařízením. Tím dojde k velkému využití šířky pásma sítě[3], ale také zmatení, zpomalení nebo dokonce zhavarování procesu nebo samotného cílového zařízení. Takováto síť počítačů, které posílají požadavky se stejným cílem proti stejnému koncovému zařízení, se označuje pojmem *botnet*. Zařízení v této síti mohou být buď úmyslně, nebo neúmyslně. V druhém případu se pak jedná o „zombie zařízení" čekající na instrukce od samotného útočníka. Útočník svůj *botnet* může vytvořit několika způsoby. Jedním je využití například služeb na internetu, které mají po celém světě rozmístěná zařízení kdykoliv připravená spustit DDoS útok. Pokud však útočník chce dosáhnout větších dopadů, zpravidla si volí cestu tvorby vlastního *botnetu*. V takovém případě si pak útočník může vytvořit vlastní malware, který bude vyčkávat na útočníkův rozkaz ke spuštění DDoS útoku (z hlediska infikovaného zařízení pak DoS útoku). Samotné „zombie zařízení" pak je infikováno a po spuštění DDoS útoku útočníkem si ani nemusí jak zařízení, tak uživatel všimnout, že je součástí *botnetu* a fakticky se z něj stává také útočník, přestože nevědomky.

Samotné DDoS útoky jsou velice časté, jelikož jejich tvorba je v některých případech až tak primitivní, že by ji mohl zvládnout člověk i s nulovými zkušenostmi. Takovéto útoky však nemívají globální či nijak výrazný drastický dopad.[5][9]

Motivace útočníků může být různá; od záměrného poškození konkurence až po čistě pro radost nebo prostě jen tak z nudy, což pro většinu lidí je tak všechno, co za DDoS útoky vidí. Kvůli tomu je však důležité také zmínit, že DDoS útoky si mohou objednat i firmy, když chtějí například vyzkoušet své nové ochranné

3 Šířka pásma určuje maximální kapacitu přenosu dat v síti. Pokud dojde k jejímu velkému využití, bude to mít za následek zpomalení sítě.[8]

systémy a připravit se tím tak na možné nebezpečí, které by mohlo přijít někdy v budoucnu.

Networking

Před tím, než se dostaneme k samotným typům DDoS útoků a jejich dopadům, je nutno pro lepší orientaci pochopit základní princip komunikace mezi zařízeními, který platí jak pro Internet, tak i lokální sítě.

Historie

Myšlenka propojení počítačů mezi sebou se objevila ve Spojených státech amerických někdy v 60. letech 20. století. Přišli s ní dva počítačoví inženýři Joseph Carl Robnett Licklider a Robert William Taylor. Těm se podařilo ve spolupráci s dalšími lidmi vytvořit v roce 1969 první počítačovou síť známou pod názvem ARPANET, která byla původně určena pouze pro vybrané univerzity a výzkumné ústavy z pár zemí světa[4]. Ta dala světu první podklad pro vznik Internetu. Revoluční zde byla idea *packet switching*, kterou využíváme dodnes. Funguje na principu shromažďování dat do packetů[5] a jejich následný přes pomocí fyzické vrstvy definované v OSI modelu[13]. Česky by se dal tento pojem přeložit jako přepojování paketů.[11]

V průběhu let se vytvořilo několik rozdílných principů sítí, které však navzájem nemohly komunikovat. Na vytvoření společného způsobu přenosu dat začala pracovat americká agentura DARPA. Ve spolupráci s dalšími organizacemi a univerzitami vytvořila protokol TCP/IP. Podobný záměr měla i společnost ISO[6], která také vytvořila vlastní protokol. Kvůli tomu proběhla debata trvající cirka 30 let známá pod názvem Válka protokolů, v níž zvítězil TCP/IP.[12]

---

[4] Mezi tyto země patřily: Spojené státy americké, Spojené království Velké Británie a Severního Irska a Norské království.

[5] Packet je soubor informací, které jsou společně s dalšími packety součástí jedné velké zprávy. Když je poslán požadavek skrz Internet, je rozdělen do více takovýchto packetů, které se spojí zase v jednu zprávu v cílovém zařízení.

[6] International Organization for Standardization, zkráceně ISO, je organizace starající se o vytváření mezinárodních standardů.[14]

TCP/IP model

Internet protocol suite, znám také pod přezdívkou TCP/IP, je referenční model systému komunikace mezi zařízeními. Jedná se vlastně o sadu pravidel (protokolů), které byly vytvořeny za účelem upřesnění a popsání funkcí komunikace počítačů mezi sebou. Tento model vyhrál ve Válce protokolů a stal se tak hlavní složkou Internetu. TCP/IP se skládá ze čtyř abstraktních vrstev, přičemž každá z nich obsahuje protokoly určující průběh manipulace s daty.[6]

Obrázek 1 – Grafické znázornění TCP/IP modelu

OSI model

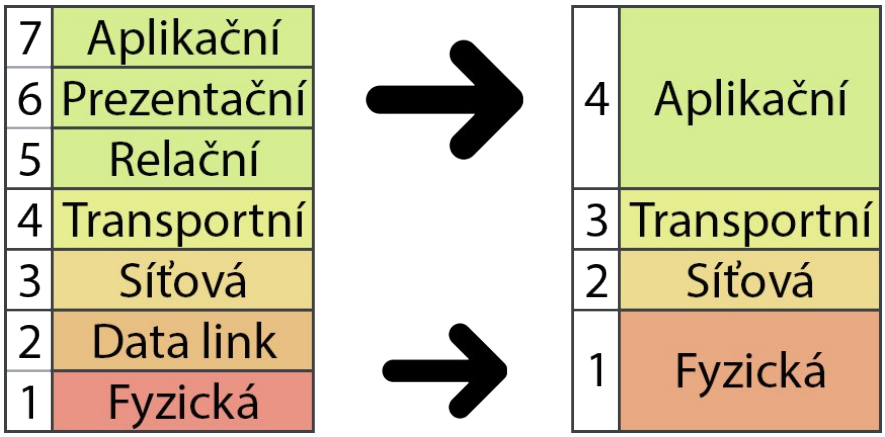
Open Systems Interconnection model, zkráceně OSI model, je stejný jako TCP/IP. Liší se pouze v počtu abstraktních vrstev, kterých má OSI model sedm.

Obrázek 2 – Grafické znázornění OSI modelu

Aplikační neboli sedmá vrstva se nachází v OSI modelu úplně nahoře. Je zodpovědná za komunikaci přímo se softwarem skrz zařízení, které posílá požadavky směrem ze nebo do sítě. V TCP/IP modelu pak zastává i prezentační a relační vrstvu, které mají na starost definovat typ, šifrování a relaci (*session*). Hlavními protokoly na sedmé vrstvě jsou HTTPS, FTP a DNS[10].

Transportní, neboli čtvrtá vrstva OSI modelu, pak určuje protokol, který bude využit k následnému transportu. Nejvýznamnější protokoly jsou zde TCP a UDP[10].

Vrstvy z OSI modelu by se však daly seskupit tak, že se bude jednat o TCP/IP model.



Obrázek 3 – Ukázka OSI modelu zobrazeného do TCP/IP modelu

Z *obrázku 3* tedy vyplývá, že když se bavíme o sedmé aplikační vrstvě OSI modelu, v praxi odkazujeme na čtvrtou vrstvu TCP/IP modelu.

Díky faktu, že se dříve věřilo, že ve Válce protokolů vyhraje právě OSI model, se lidé začali učit právě tento protokol. Protože se tak však nestalo a ujal se model TCP/IP, lidé dodnes používají vrstvy z OSI modelu jako referenci na vrstvy v TCP/IP modelu. Proto v rámci této práce se zde bude vyskytovat analogie z OSI modelu pro popisování TCP/IP modelu.

Jak modely fungují?

Oba dva komunikační protokoly pracují na stejném principu. Umožňují dorozumívat se se zařízením se stejným referenčním modelem[7] na stejné vrstvě. Tyto vrstvy se zkráceně zapisují jako L*N*, kde *N* je číslo vrstvy v OSI modelu.

Samotný princip obecného fungování referenčního modelu je následovný:

1. Vezmou se data z vyšší vrstvy (poprvé ze sedmé vrstvy) s protokolem odpovídajícím formátu dat na dané vrstvě, kterou obě dvě zařízení, komunikující mezi sebou, podporují a pošlou se o vrstvu níž.
2. Na nižší vrstvě se k předaným datům přidá („přilepí“ nebo „obalí“)“ informace odpovídající dané vrstvě. Jedná se především o informace o využitém protokolu danou vrstvou.

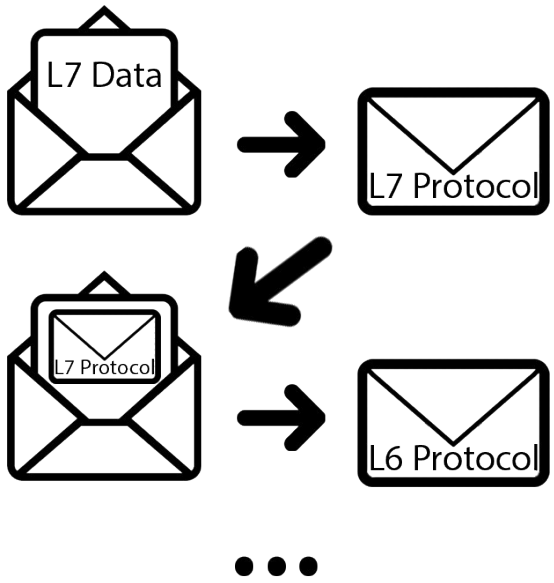
Toto vrstvení informací na sebe se odborně nazývá *encapsulation*[8]. Tento proces se pak opakuje, až dojde k první (fyzické) vrstvě, která pošle data skrz router přes Internet až do cílového zařízení. To přijme data v podobě, ve které byla poslána a opakuje se proces na OSI modelu v opačném směru.

1. Cílové zařízení přijme data a zpracuje je na první vrstvě. Zpracování spočívá v převzetí posledních a odebrání naposledy přidaných informací, čili informací náležejících první vrstvě.
2. Následně se zbylá data pošlou o vrstvu výš.

[7] V případě Internetu se jedná o TCP/IP model.
[8] *Encapsulation* se do češtiny překládá jako zapouzdření.

Tento proces se opakuje do té doby, než data dojdou k finální vrstvě, na které byl požadavek vytvořen odesílajícím zařízením. Tomuto postupnému odvrstvení informací se odborně říká *de-encapsulation*[9].

Samotnou *enkapsulaci* si lze představit jako vkládání obálky do jiné obálky. Data na sedmé (aplikační) vrstvě si můžeme představit jako dopis, který umístíme do obálky. Do záhlaví této obálky napíšeme informace o protokolu této vrstvy. Na vrstvě níž se pak vytvoří nová obálka, jejíž obsah bude tvořit obálka vytvořená ve vrstvě výš a do záhlaví takto nově vytvořené obálky se umístí informace o protokolu z dané vrstvy.[7]



Obrázek 4 – *Enkapsulace* vysvětlena pomocí obálek

Typy DDoS útoků

DDoS útoků existuje celá řada, která jde rozdělit do několika skupin podle určitých aspektů, jako je způsob útoku, jeho komplexnost, cíl apod. V rámci základního rozdělení se rozdělují takto[9][26][27][28]:

[9] *De-encapsulation* je anglický výraz a jedná se o opak zapouzdření (*enkapsulace*).

- **Objemové** (Volumetric, high-volume) – Tyto útoky pracují na principu vytváření a posílání velkého množství požadavků, které cílí na využití šířky pásma sítě – tím dojde k přehlcení a odmítnutí služby.
- **Protokolové** (Protocol) – Tyto útoky fungují převážně na L3 a L4 (třetí a čtvrté vrstvě OSI modelu) proti procesním zařízením v síti. Snaží se ho zahltit.
- **Aplikační** (Application) – Tyto útoky, jak už název napovídá, působí na L7 (sedmé aplikační vrstvě OSI modelu). Útočí převážně na procesní zařízení a většinou se jedná o komplexnější DDoS útoky, ve kterých jde v podstatě o vytvoření jednoduchého požadavku, který server zpracovává delší dobu a využívá tím tak kapacitu svých omezených zdrojů, jakými jsou například RAM.

Jedněmi z nejčastějších útoků pak jsou[26][27]:

- **UDP nebo ICMP flood** – Jedná se o časté objemové útoky, jejichž princip spočívá v zahlcení sítě požadavky, které nutí cíl posílat odpovědi ve formě, zdali je dostupný, jakou má latenci[10] apod. Kvůli své jednoduchosti jsou však lehce detekovatelné.
- **SYN flood** – Je označení pro DDoS útok založený na posílání SYN požadavků jako součást *three-way handshake*[11], který je nutný k ustálení komunikace skrz TCP protokol.
- **HTTP flood** – Je jeden z nejčastějších aplikačních DDoS útoků, který, jak název napovídá, cílí na webové servery pomocí HTTP protokolu. Bývají zkonstruovány tak, aby vypadaly jako normální uživatel Internetu, přičemž však mají úplně jiný úmysl. Tím se stávají hůře odlišitelnými od normálních lidí. Jejich účelem je využití co nejvíce výkonu webového serveru.

[10] Latence neboli odezva je čas, za kterou doputuje požadavek mezi dvěma zařízeními.

[11] Three-way handshake (z angličtiny; česky „třícestné podání ruky“); způsob ustalování komunikace u TCP protokolu. Postup ustálení: 1. uživatel pošle SYN request, 2. server ho obdrží, pošle SYN ACK request, 3. uživatel potvrdí odesláním ACK požadavku. Teprve pak může probíhat komunikace skrz TCP protokol.

- **DNS amplification** – Funguje na principu, že útočník pošle na *DNS resolver*[12] požadavek s falešnou IP adresou (IP adresou cíle) a podněcuje ho k poslání DNS odpovědi právě na ni.[29]

Četnost a dopad DDoS útoků

Na rozdíl od dopadů DDoS útoku, které lze určit a popsat jednoduše, DDoS útoky jako takové nelze nijak s přesností kontrolovat. Je to z důvodu, že tyto útoky jsou v podstatě soubory požadavků, které se přeposílají přes Internet stejně jako miliony dalších. Proto rozpoznat je bývá velice těžké, dokud nemají větší (detekovatelný) dopad. Avšak tím nejlepším způsobem, jak je můžeme zachytit, je pomocí výkazů služeb, které si různé firmy najímají pro svoji DDoS ochranu. Tyto služby pak mohou ve svých datech vidět špici v grafu, který zaznamenává počet přijatých požadavků. Protože jsou služby rozšířené, tak jejich data jsou více komplexnější a tím pádem i přesnější.

Dle mezinárodní korporace Link11[13], která právě poskytuje takováto data, počet samotných (větších – detekovatelných) DDoS útoků v roce 2021 oproti roku 2020 vzrostl o 41 % na přibližně 70,5 miliónů, což po uvážení začátku pandemie *SARS-CoV-2*[14] není nic překvapivého. Tím se jedná o další zvýšení v řádech několika minulých let. Největším útok, jenž byl zaznamenán, se stal útok o přenosové rychlosti až 4,5 Tbps (terabitů za sekundu). Nejčastěji se pak objevují objemové DDoS útoky společně s RDDoS útoky[15], kterých v poslední době rapidně přibývá. Pomocí nich útočníci již dostali dohromady kolem 4,5 miliónů USD (amerických dolarů) ze společností ze Severní Ameriky.

Jedním z nejdrastičtějších dopadů DDoS útoků pak v roce 2021 byly rozsáhlé *blackouty*[16], kde více jak 700 000 domácností v Karibiku přišlo o připojení k elektrické energii mezi zářím a listopadem. V pondělí 13. září 2021 se

[12] DNS Resolver je server v síti Internet, který konvertuje domény do IP adres a naopak.
[13] Link11; služba dostupná na URL adrese *https://www.link11.com/*[30]
[14] SARS-CoV-2, znám také jako COVID-19 nebo jen covid.
[15] RDDoS (Ransom DDoS) útok je jakýkoliv DDoS útok, který cílí na vyplacení peněz útočníkovi.
[16] Blackout je označení pro hromadný výpadek elektrické energie v určitém regionu.

důsledkem rozsáhlého DDoS útoku stala nedostupnost bankovních, meteorologických, poštovních a policejních služeb na Novém Zélandu, přičemž problémy s bankovnictvím pokračovaly ještě několik dalších dní.

Vedlejší účinky DDoS útoků

DDoS útoky bývají často společností právem odsuzovány jako čistě negativní záležitost. Málo kdo si však ještě uvědomuje jejich vedlejší účinky, které jsou stejně, jako samotný útok, převážně negativní.

Hlavním takovým efektem, který ještě bývá známý, je plýtvání elektřinou. Samotný útok je nejen náročné spustit, ale také držet v chodu. Problém ale nastává i na druhé straně. Když se DDoS útok dostává ke svému cíli, tak server na koncovém bodě začne pracovat na plný výkon, což nejen spotřebovává zbytečně elektřinu, která by se dala ušetřit, ale ubírá také na životnosti komponentů.

Mezi ty méně známé účinky, které však ovlivňují negativně i běžné uživatele, patří převážně zpomalení rychlosti internetu. Dochází k tomu, protože počítače, které jsou součástí *botnetu*, posílají požadavky skrz datacentrum jejich poskytovatele internetu (Vodafone, UPC, O2 apod.). Tím využívají jeho *bandwidth*[17], který pak nemusí stíhat zpracovávat požadavky ostatních uživatelů, kteří s tímto DDoS útokem nemají nic společného.

Všechny výše zmíněné vedlejší účinky pak mají za následek zbytečné plýtvání peněz a zátěž životního prostředí. Firmy jsou pak zároveň nuceny, v rámci investice do budoucna, zbytečně platit například za různé ochrany, které by, kdyby DDoS útoky neexistovaly, nemusely řešit.

[17] Bandwidth (česky šířka pásma) určuje maximální přenosovou rychlost sítě[8].

Legislativa České a Slovenské republiky

V této kapitole, jak už její název napovídá, se zaměříme na zákony v České a Slovenské republice, které se vážou na kyberkriminalitu a s tím spojené DDoS útoky. Jedná se o kriminalitu v kybernetickém prostoru[18][15]. Tato část byla postupně začleňována do trestního zákoníku České republiky na základě rámcových úmluv Evropské unie z roku 2005 a následně v roce 2013, kdy byla uvedena v platnost Úmluva o počítačové kriminalitě a směrnice Evropského parlamentu a Rady č. 2013/40/EU ze dne 12. 3. 2013, která již vyžadovala trestní postih[16].

Paradoxně i po všech těchto opatřeních, doteď bohužel neexistuje zákon v České republice přímo popisující problematiku DDoS útoků. To, dle advokáta Jakuba Šťastného, potvrzuje i fakt, že: *„příslušné orgány řešící trestní činnost tuto skutečnost často odkládají, protože se prý nejedná o trestný čin.“*[17].

Jediný zákon, který klasifikuje nepřímo tuto problematiku, je § 230 odstavec 2. písm. b Trestního zákoníku České republiky (dále jen ČR):

„Kdo zasáhne do počítačového systému nebo nosiče informací tím, že data uložená v počítačovém systému nebo na nosiči informací neoprávněně vymaže nebo jinak zničí, poškodí, změní, potlačí, sníží jejich kvalitu nebo je učiní neupotřebitelnými, bude potrestán odnětím svobody až na tři léta, zákazem činnosti nebo propadnutím věci.“[18]

Zákon zde pojednává pouze o potlačení dat nebo učinění je neupotřebitelnými. To jsou klíčová slova, která zde hrají roli. DDoS útok ale na druhou stranu pouze znepřístupňuje data uživatelům, kterým jsou posílána v rámci dlouhého cyklu skrz síť. Pokud by si tato data však chtěli zobrazit přímo jako soubor například v FTP serveru, neměl by to být z tohoto hlediska žádný problém. Kvůli těmto faktům je toto velice sporné téma.

[18] Kybernetický prostor je virtuální prostor počítačů a počítačových sítí, který není omezen hranicemi států.

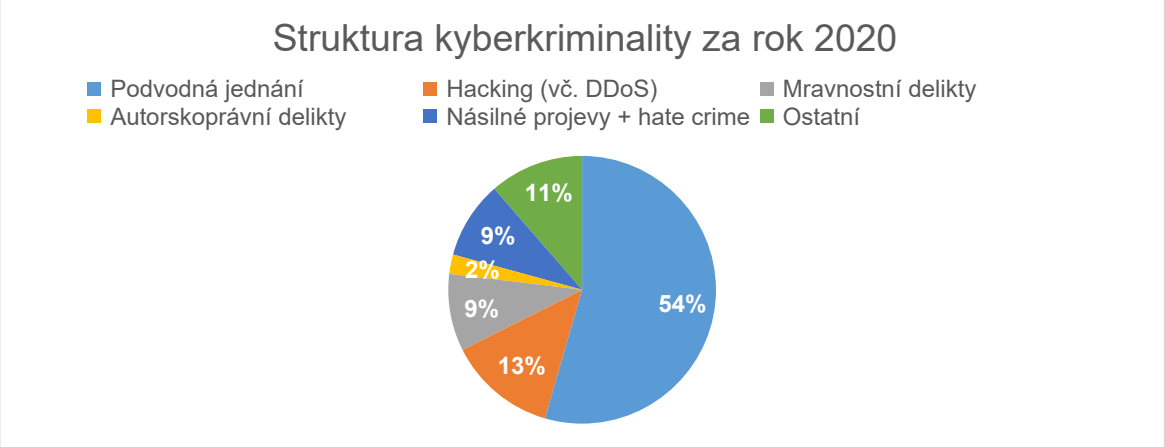
Lépe definován je zákon § 274a odstavec 1. písm. a Trestního zákoníku Slovenské republiky (dále jen SR):

„Kto obmedzí alebo preruší fungovanie počítačového systému alebo jeho časti neoprávneným vkladaním, prenášaním, poškodením, vymazaním, zhoršením kvality, pozmenením, potlačením alebo zneprístupnením počítačových údajov, potrestá sa odňatím slobody na šesť mesiacov až tri roky.“[19]

Zde, na rozdíl od českého zákona zmíněného výše, se objevuje fráze přerušení fungování samotného počítačového systému, které popisují DDoS útok v mnohem větším měřítku.

Z obou dvou zákonů vyplývá, že podílení se nebo provozování DDoS útoků bez souhlasu cílového zařízení je trestný čin. Mají také jeden velký nedostatek – neřeší, kdo přesně má nést zodpovědnost. V takovém případě v konečném důsledku jsou na vině i lidé, jejichž zařízení bylo nevědomě zneužito ve prospěch hlavního útočníka.

Ačkoliv se v poslední době počet trestných činů spáchaných v kyberprostoru neustále zvyšuje, DDoS útoky nejsou ani zdaleka nejpočetnější skupinou19. Proto je patrné, že se pravděpodobně brzké změny, dle mého názoru, v legislativě pravděpodobně nedočkáme.



Obrázek 5 – Struktura kyberkriminality za rok 2020[20]

[19] Vyplývá z dat Policie ČR k 1. 1. 2020.
[20] Vyplývá z dat časopisu Bezpečnostní teorie a praxe 1/2022[31].

Bezpečnost na Internetu

Teď, když jste se o DDoS útocích dozvěděli všechny podstatné informace, je na čase se podívat na to, jak se takovým útokům nejlépe vyvarovat, popřípadě se jim ubránit. Aby vůbec mohlo dojít ke spuštění DDoS útoku, útočník musí definovat cílové zařízení pomocí IP adresy. Internet pro navazování komunikace mezi dvěma zařízeními používá IP adresu[21], což je 32bitové číslo nebo 128bitové číslo[20], které je unikátní a je přiřazeno každému zařízení připojenému na Internet. Ve chvíli, když si chcete zobrazit například webovou stránku, posíláte tím i svoji IP adresu, aby stránka věděla, kam má poslat svoji odpověď.

Jak se nestát cílem DDoS útoku?

Jak už jste z předchozí kapitoly jistě pochopili, nedílnou součástí prevence proti DDoS útokům je uchovávání své IP adresy v co největší tajnosti. Pokud totiž útočník nebude znát vaši IP adresu, nebude moci DDoS útok spustit. Mimo jiné pomocí IP adresy lze také zjistit místo přibližné lokace zařízení, čehož by se dalo jednoduše zneužít.

Protože IP adresa je nezbytná v komunikaci skrz Internet, může se na první pohled zdát, že není jiné cesty než chodit na webové stránky, kterým věříte, že nezneužijí vaši IP adresu. Opak je však pravdou – existuje několik způsobů, jak při používání Internetu zůstat více anonymní.

Virtual Private Network (VPN)

Nejlepším způsobem, jak uchovat svoji IP adresu před okolním světem v tajnosti je využití VPN služeb[22] nebo vytvoření vlastní VPN sítě. VPN je zkratka z angličtiny, která znamená virtuální privátní síť. Všechny tyto sítě fungují na principu přeposílání požadavků (requests) skrz VPN servery. Cesta

[21] Zkratka IP vychází z anglického výrazu Internet Protocol.
[22] VPN služba je internetová služba poskytující připojení a využívání VPN serverů služby.

jednoho požadavku pro zobrazení webové stránky pak může vypadat následovně:

1. Uživatel pošle skrz webový prohlížeč (a všechny vrstvy OSI modelu) požadavek, který směřuje na URL adresu[23] *http://example.com/*.
2. Požadavek je poslán poskytovateli internetového připojení, který zde funguje pouze jako přeposílatel.
3. Tento požadavek je pak, pomocí aplikace starající se o připojení na VPN server, poupraven a poslán na VPN server.
4. VPN server požadavek zpracuje a přepošle ho na původní URL adresu *http://example.com/*.
5. Webový server, který tento požadavek přijme, ho zpracuje a pošle zpět odpověď ve formě stránky.

Zajímavá situace však nastává v pátém bodě. Webový server totiž ve skutečnosti neposílá odpověď (response) přímo uživateli, ale VPN serveru, který ho přeposílá dále poskytovateli internetu atd. Z toho vyplývá, že webový server nevidí (neposílá odpověď) ve skutečnosti IP adresu uživatele, ale pouze VPN serveru, který může být klidně tisíce kilometrů vzdálen od samotného zařízení uživatele. To má za výhody jak zachování větší anonymity, tak například zpřístupnění obsahu dostupného pouze pro určité země, protože stránka komunikuje s VPN serverem v domnění, že se jedná o uživatele ve státě, kde se nachází VPN server. Kromě těchto funkcí VPN služby také nabízí funkce jako jsou *kill switch*[24], *port forwarding, šifrování dat* a mnohé další, pomocí kterých jsou IP adresa a data uživatele více chráněna.

Z uživatelského hlediska jsou VPN služby dle mého názoru jedním z nejlepších, avšak ne tak častých řešení. Jejich nastavení zpravidla spočívá pouze v nainstalování aplikace a jejich používání většinou nijak výrazně neovlivňuje rychlost odezvy[25]. Jedinou nevýhodou je, že tyto služby bývají většinou placené, ale najdou se i nějaké bezplatné. U těch je ale třeba se mít na pozoru, protože

[23] URL adresa je cesta ve formě textu sloužící k odkazování na obsah dostupný na Internetu.[24]

[24] Kill switch je funkce, která zajišťuje vypnutí internetového připojení při výpadku spojení, aby nedošlo k nechtěnému odhalení IP adresy uživatele.[22]

[25] Jedná se o informaci z mé zkušenosti, která se však mění společně s výběrem VPN služby.

u drtivé většiny z nich lze narazit na poskytování informací o uživatelově historii, informacích a podobně třetím stranám, což úplně podkopává význam VPN služeb jako takových. V takovém případě je lepší danou VPN službu ani nepoužívat.

Pokud to s udržením anonymity myslíte vážně, mohu doporučit známé VPN služby jako například *Nord VPN*, *Surfshark VPN* a *Proton VPN*. Všechny z nich disponují ochrannými prvky zmíněnými výše. Pokud však za tyto služby nechcete moc utrácet, ale zároveň chcete udělat alespoň něco pro zvýšení Vaší bezpečnosti, mohu doporučit službu *Proton VPN*, která obsahuje kromě té placené i neplacenou verzi zdarma. Najdete zde však pouze výběr z VPN serverů ze tří států a funkci *kill switch*, což ale oproti ostatním nabídkám na trhu je více než dostačující. Samozřejmě ani jedna z mnou doporučených VPN služeb neposkytuje informace o uživateli třetím stranám.

Proxy server

Jako další prostředek k uchování IP adresy v tajnosti je možnost použití proxy serveru. Ten funguje na podobném principu jako VPN servery (přeposílání požadavků skrz server tomu určený), avšak bez funkcí jako *kill switch* apod. Jeho hlavní přednost je však ta, že na rozdíl od VPN služeb má možnost přeposílat pouze určitý *traffic*[26]. Jinými slovy proxy server může využívat pouze nějaký program místo celého počítače. Navíc také umožňuje cyklení více proxy serverů na sebe, takže místo toho, aby data putovala pouze k jednomu proxy serveru a pak přímo na cílové zařízení požadavku, tak putuje přes více proxy serverů. Tím se docílí lepšího zabezpečení, protože kdyby někdo chtěl zjišťovat původce požadavku, musel by projít přes všechny proxy servery pozpátku. Kromě toho ani samotný proxy server (kromě toho prvního) neví, z jakého původního zařízení byl požadavek poslán. Protože se nejedná o úplně jednoduchou věc na nastavení, které nemá takový potenciál pro normální lidi, tak jsou proxy servery používány převážně programátory, správci sítí apod.

[26] Traffic je označení pro data, která jsou přenášena skrz síť.

The Onion Router (TOR)

Pro získání větší anonymity při prohlížení webových stránek lze využít webový prohlížeč The Onion Router Browser (zkráceně TOR Browser nebo TOR prohlížeč). Ten je znám především ve společnosti spíše díky tomu, že poskytuje možnost zobrazovat stránky s doménou končící na *.onion*[27]. Snaží se chránit uživatelovu komunikaci a tím i jeho IP adresu pomocí komplikovaného systému přeposílání požadavků skrz zařízení připojené do sítě TORu. Zjednodušeně by se tento proces dal shrnout do pár kroků; vytvoření tzv. *randez-vous point* (místo setkání) a následném zobrazení stránky uživatelem na tomto „místě". Celý tento systém doprovází ještě spousta hesel, šifrování a dalších zabezpečovacích věcí, které zajišťují uživateli téměř absolutní anonymitu.

Ovšem TOR prohlížeč má své jedno velké negativum, a to, že je díky svému spletitému systému značně pomalejší než ostatní normální prohlížeče. Proto bych ho nedoporučoval používat na denní bázi místo normálních prohlížečů[28], ale spíše u podezřelých odkazů nebo u stránek, které ve vás vzbuzují negativní dojem.

Dynamická IP adresa

Další možností, jak zůstat na Internetu více anonymní, je obstarání si dynamické IP adresy například do domácí sítě od poskytovatele Internetu. Jedná se vlastně o IP adresu, která se však mění po každém připojení na Internet, a kterou síti přiřazuje DHCP[29] server. Přestože takováto příležitost zní lákavě, má i několik nevýhod. Nemohou ji například používat hostingy (protože tam je funkce měnící IP adresy nepřípustná), sítě s potřebou využití vzdáleného přístupu, a také síti hrozí možnost selhání způsobená třeba nefunkčností DHCP serverů – tím se stává méně spolehlivá.[23]

[27] Jinými slovy webové stránky na darkwebu.
[28] Například Brave, Google Chrome, Mozila Firefox, Edge, Opera a mnohé další.
[29] DHCP je zkratka vycházející z anglického výrazu pro Dynamic Host Configuration Protocol.[23]

Pokud se tedy chystáte rozhodnout, zohledněte všechny nároky, které budete mít na svoji budoucí síť. Jestli se bojíte složitého nastavování a nebudete potřebovat se připojit na svoji síť zvenčí, dynamická IP adresa je pro vás lepší volbou. V opačném případě pak použijte raději IP adresu statickou.

Jak se nezúčastnit botnetu?

Pokud jste již zvládli základy obrany proti DDoS útoku, aby se z vás nestal cíl DDoS útoku, je načase zjistit, jak se nestát jeho součástí a nenapomáhat tím tak útočníkům v nelegální činnosti. Hlavní příčinou, proč se z počítačů[30] stávají „zombie zařízení“, je škodlivý software (malware). Pokud již je počítač infikován a vyčkává na příkaz od útočníka, je těžké tento malware odhalit. Z toho důvodu je důležitá prevence, která spočívá především v opatrnosti při čtení emailů, otevírání webových stránek, rozklikávání podezřelých URL odkazů a podobně, které mají za úkol spustit kód na vašem počítači, který se postará o vytvoření brány mezi vámi a útočníkem.

Nelegální stahování

Jednou z neúspěšnějších možností rozšiřování malwaru je ho zakomponovat společně s nějakým obsahem, který se zveřejňuje převážně na stránkách určených pro sdílení souborů. Takovou může být třeba v České a Slovenské republice stránka Ulož.to nebo v zahraničí známý MediaFire. Obsahem většinou bývá nějaký nelegální obsah jako třeba cracknuté programy[31] a seriály, které je uživatel posléze nucen otevřít a tím si tak může dobrovolně infikovat zařízení.

Pokud již malware ve svém zařízení máte, je těžké ho identifikovat, dokud se neprojeví. Doporučit mohu například antivirový software a využít možnost prohlédnutí (skenování) počítače. Pokud vám nějaký malware najde, většinou

[30] V této kapitole je počítačem myšleno zařízení, které má přístup k Internetu.

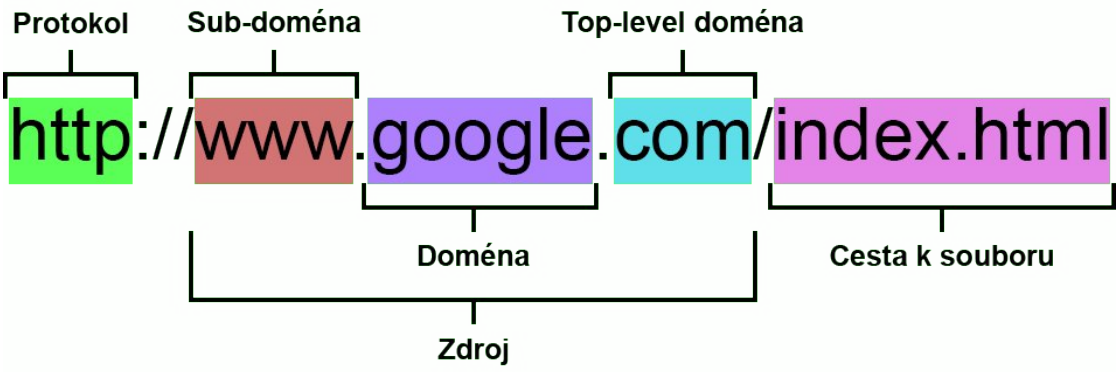
[31] Cracknutý program je software, který byl upraven bez patřičného povolení. Příkladem mohou být free verze placených programů, které nepochází od výrobce.

program nabídne možnost se ho zbavit. Tato funkce však nemusí fungovat stoprocentně. Nejlepším způsobem pro zbavení se malwaru je si reinstalovat (znovu nainstalovat) váš operační systém, avšak tuto možnost bych zvážil až jako poslední, jelikož se nejedná o úplně lehké a časově nenáročné řešení.

Phishing e-maily

Jedná se o emaily, které jsou vytvořeny za účelem podvodných činností. Aby se však ale z nich mohl malware přesunout na Váš počítač, musí být provedena nějaká akce. Ta je zde přítomna buď jako nějaký soubor, nebo častěji ve formě nějakého odkazu, na který se vás email snaží nutit kliknout. Na tyto emaily je potřeba si dávat pozor, protože se většinou vydávají za jinou identitu, které důvěřujeme (například banka, pošta apod.) a snaží se tím tak zmást svůj cíl (uživatele) a docílit tak tím akce požadované útočníkem (kliknutí na odkaz, stažení souboru, zadání hesla…).

Obecně nelze vytvořit přesný návod, podle jakého lze takovýto email rozpoznat. Nejlepší způsob na ochranu bývá selský rozum. Pokud vám například přijde email od banky, se kterou jste doteď neměli nic společného, nebo email bude psán lámanou češtinou, tak se s největší pravděpodobností bude jednat o podvod. Pokud byste v takovémto uvažování neuspěli, je dobré se naučit, jak vypadá podezřelý hypertextový odkaz, na který většina phishingových emailů odkazuje.



Obrázek 7 – URL adresa a její části

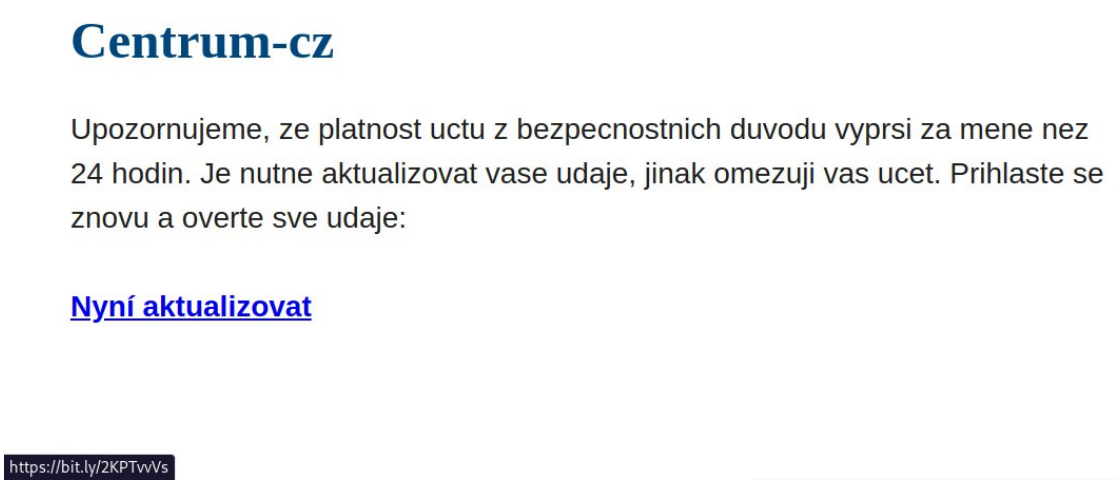
Pochybný hypertextový odkaz většinou mívá některé z těchto aspektů:

- **Přeházená písmenka** – Je důležité si zkontrolovat, zdali odkaz, na který klikáme opravdu odkazuje na danou stránku. Občas se totiž stává, že útočník záměrně přehodí, nahradí nebo klidně vypustí jedno písmenko. Takový link[32] pak může vypadat jako *https://goolge.com/* místo *https://google.com/* na který by měl směřovat. Další příklady: *http://games-survival.net/* místo *http://games.survival.net/*, *https://hpixel.tv/* místo *https://hypixel.tv/* apod.
- **Jiná top-level doména** – Další způsob, který bývá aplikován na podvodné URL adresy je změna *top-level* domény[33]. Příkladem takové URL adresy je například *http://youtube.tk* nebo *https://youtube.cum* místo *https://youtube.com/*.
- **Vypadá v pořádku** – I když se zdá, že link je naprosto v pořádku, v HTML[34] (případně společně s JS[35]) totiž zobrazený text odkazu nemusí odpovídat adrese, na kterou uživatele přesměrovává. Z toho důvodu je důležité si zkontrolovat, kam doopravdy odkazuje. Toho se dá u moderních prohlížečů docílit tím, že přejedete myší[36] nad odkaz a nekliknete na něj. Po chvíli se vám v pravém dolním nebo v levém dolním rohu ukáže reálná URL adresa. Pokud se Vám však neukáže nic, znamená to, že přesměrování probíhá pomocí Java Scriptu. V takovém případě je dobré kliknout na odkaz pravým tlačítkem myši a zvolit možnost prozkoumat, kde můžete ale nemusíte vidět reálný odkaz.

URL odkaz také pak nemusí být jen jako součást nějakého textového odkazu, ale může vás přesměrovat i po kliknutí například na nějakou reklamu, obrázek, formulář apod. Proto při používání Internetu se snažte být ostražití a důslední a vždy kontrolujte, na co klikáte.

---

[32] Link je označení pro hypertextový odkaz.
[33] Viz *obrázek 6*.
[34] HTML (Hyper Text Markup Language) je jazyk, ve kterém se zobrazují webové stránky.
[35] JS (Java Script) je programovací jazyk, který umožňuje pracovat se vstupem uživatele na webových stránkách.
[36] Platí pro počítače s GUI (grafickým rozhraním), které podporují vstup uživatele pomocí myši.



Obrázek 8 – Příklad phishing e-mailu

Obrázek 9 – Příklad phishing e-mailu

Stahování souborů z Internetu

Pokud stahujete nějaké soubory z Internetu (včetně příloh e-mailů), u kterých nevíte, odkud pocházejí, je důležité se mít na pozoru. Do hodně typů souborů lze totiž zakomponovat *executable* kód[37]. Takovými bývají například soubory typu *.exe*, *.pfd*, *.scr*, *.bat*, a podobně. Tyto a další přípony se na sebe ještě dají cyklit, takže výsledná přípona může vypadat například *.docx.scr* (Executable Microsoft Word dokument). Proto obecně platí *nedůvěřuj a prověřuj*. Pokud už si takový soubor musíte stáhnout a nevěříte zdroji, doporučuji si ho alespoň zkontrolovat antivirem nebo jinými dostupnými bezpečnostními službami.

Náhodné disky

Určitě znáte takový ten pocit, když doma najdete nějaký starý flash disk a zapojíte ho do počítače, abyste se podívali, co za poklady skrývá. Toto však nikdy nedělejte u jakýchkoliv disků, u kterých si nejste jisti původem. Pokud například najdete takovou flashku[38] nebo zařízení na veřejnosti, které vypadá jako flashka, rozhodně ji do počítače nezapojujte. Může totiž obsahovat již zmíněné *executable* soubory, nebo se o flash disk vůbec nemusí jednat. Existují totiž zařízení, která jsou zakamuflovaná, aby vypadala jako flashky, ale ve skutečnosti se může jednat o počítač, který se po zapojení do vašeho zařízení může tvářit jako vstup uživatele a splnit tím svůj účel ve formě nainstalování souborů, zaktivování škodlivého kódu apod.

Jak poznám, že jsem obětí DDoS útoku a co dělat?

Ze začátku je důležité zmínit, že neexistuje přesný návod na to, jak se ubránit proti DDoS útoku, protože technologie se pořád vyvíjí. Tím pádem žádná síť není stoprocentně chráněna. Pokud jste obětí DDoS útoku, nebo jakožto součást

[37] *Executable* kód je kód, který lze zaktivovat. Například při otevření souboru.
[38] Flashka je zkrácený hovorový výraz pro flash disk.

botnetu posíláte požadavky na útočníkův cíl, poznáte to prakticky docela snadno. Může vám selhat internetové připojení, zatížení komponentů (procesoru, grafické karty…) může rapidně z ničeho nic narůst a podobně. Ve chvíli, kdy již na vás někdo útočí pomocí DDoS útoku, nejlepším možným řešením je odpojení se z Internetu. Pokud Vám však jde o to zůstat co nejdéle online[39], nejlepší je udělat to, co byste udělali pro prevenci proti těmto útokům.

Firewall

Prevence spočívá převážně v dobře nastaveném filtru na příchozí a odchozí požadavky – firewallu. Ten může být jak hardwarový ve formě zařízení, tak softwarový ve formě programu. Tvoří jakousi pomyslnou bariéru mezi vámi (respektive vaším zařízením) a vnějším světem. Je založen na bázi pravidel, podle kterých následně vyhodnocuje, zdali požadavek vpustí nebo vypustí z/do sítě, nebo v případě softwarového firewallu požadavky mezi porty a programy. Firewallů existuje více typů podle toho, na jaké vrstvě OSI modelu pracují. Nemusejí totiž vyhodnocovat jen požadavky na bázi toho, z jaké IP adresy a na jaký port přicházejí, ale mohou vyhodnocovat také například na L7 (sedmé úrovni OSI modelu), kde posuzují, zdali je HTTP požadavek způsobilý či nikoliv. Firewall pak nemusí být jen jako součást osobního počítače/serveru, ale mají ho i další zařízení v síti jako například routery.[25]

Ostatní

Další možností, jak se bránit proti DDoS útokům, je možnost využití zabezpečovacích služeb jako Cloudflare, TCP Shield, Link 11 apod. Pokud máte svá data uložena na cloudu, tak máte již sérii zabezpečení, které s sebou přináší právě cloud. Může se jednat jak o firewally, služby třetích stran atd. Jestliže však máte data uložena ve vlastní síti a bojíte se dopadů DDoS útoků, můžete využít záložních zařízení, která budete mít normálně zapojená v síti a v případě výpadku jednoho typu zařízení vám budou pořád fungovat další zbylá.

[39] Online znamená, aby zařízení bylo připojené k Internetu, a odpovídalo.

Například máte server, který je napojený na dva firewally. Když jeden zhavaruje, pořád vám zbude jeden. Takováto verze ochrany je však náročnější na nastavení, takže pokud nejste síťový inženýr, budete si muset na tuto práci někoho najmout.

Společnost a její pohled na DDoS útoky

V rámci této ročníkové práce jsem vytvořil i dotazník (viz *Příloha 1*), abych zmapoval povědomí lidí o DDoS útocích a bezpečnosti na Internetu. Některé závěry jsou již využity různě v práci. V následujícím textu budou pro lepší orientaci použity zkratky LSIT (lidé se zájmem o IT) a LBIT (lidé bez zájmu o IT). Dohromady na dotazník odpovědělo 141 lidí. Polovina všech respondentů pak byla ve věku mezi 15 a 17 lety, přičemž BSIT bylo přibližně stejně jako LBIT.

Z *otázky č. 1* dle očekávání vyplynulo, že obecně LSIT vědí o DDoS útocích více, než LBIT. Ovšem přibližně 2/3 LSIT si už nejsou jistí, případně se nevyznají ve větších detailech a zákoutích tohoto tématu (viz *otázka č. 12* a *obrázek 9*).

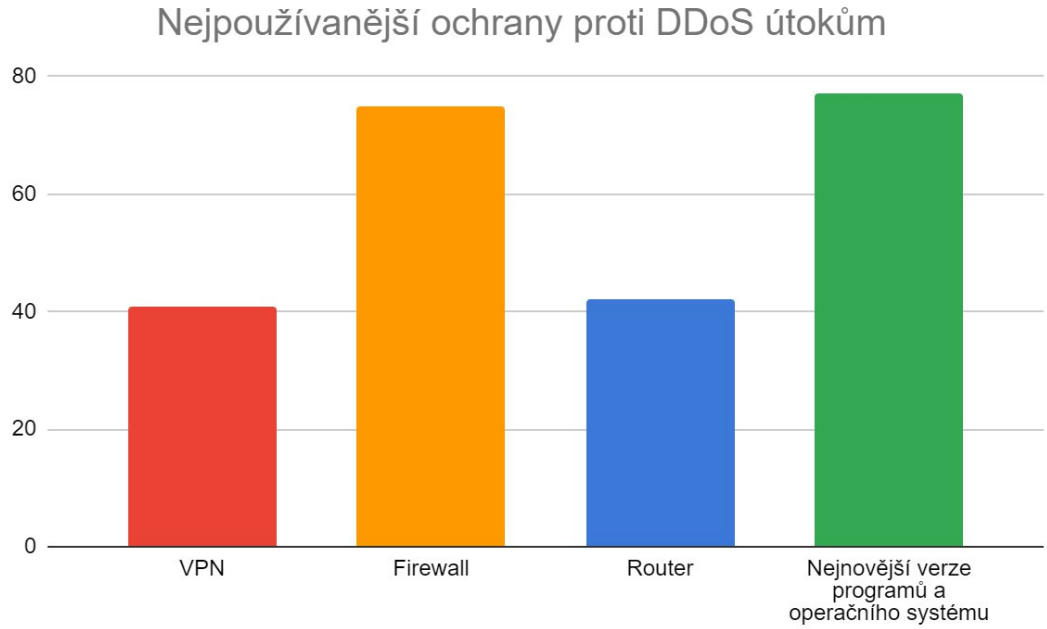
Obrázek 10 – Graf odpovědí LSIT na *otázku č. 12*

K překvapivému výsledku se dostalo shrnutí odpovědí u *otázky 15 „Vidíte DDoS útoky jako čistě negativní záležitost?“* Moje původní očekávání bylo, že alespoň 90 procent dotázaných odpoví kladně, avšak ve výsledku toto téma jako čistě negativní nevnímá 41,8 % všech dotázaných, čemuž odporuje *otázka č. 7*. Zde

27 lidí zde odpovědělo pouze odpovědí „Záměrné poškození“, dále 94 lidí tuto odpověď uvedlo společně s dalšími.

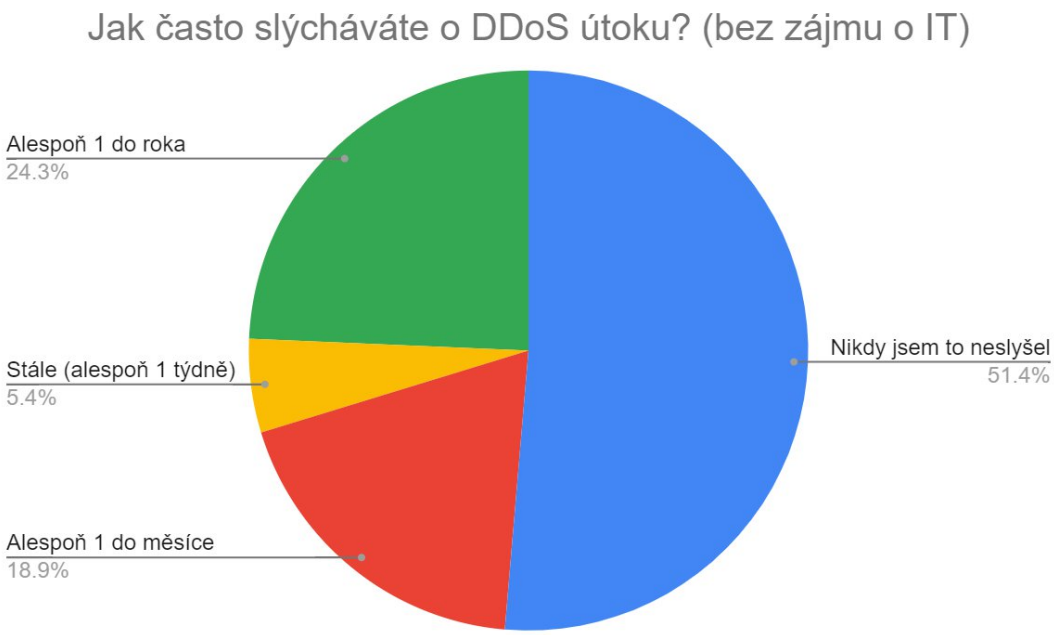
Lidé se o tomto tématu dozvídají převážně z konverzace s ostatními lidmi nebo ze zpravodajských portálů a sociálních sítí, jak vyplývá z *otázky č. 3*. Mylnou představu má více než polovina LBIT, kteří DDoS útoky vidí spíše jako vzácnější jev, který se nevyskytuje tak často. Tento fakt se vyplnil dle očekávání a potvrzuje moji vizi uvedenou v úvodu práce.

U *otázky č. 11 „Myslíte si, že je toto téma důležité rozebírat?“* třetina dotázaných pak odpověděla, že je jim to jedno, jestli se o tomto tématu budou nebo nebudou bavit. Zbytek se pak více méně shodoval v tom, že je důležité se o tomto tématu bavit, přičemž nejčastější příčinou bylo zvýšení bezpečnosti uživatelů, jak už ze strany oběti, tak hlavně ze strany ochrany před zapojením do botnetu. Pouhá 2 % dotázaných pak odpověděla, že to není důležité a argumenty u nich byly převážně o tom, že je velice nepravděpodobné, že by se stali (nebo stala??? TODO) cíli DDoS útoků. Nejčastější ochranou u lidí pak bývá firewall na úkor VPN služeb (viz *otázka č. 10* a *obrázek 10*).



Obrázek 11 – Graf odpovědí na *otázku č. 10*

Zajímavé mi přišlo, že přibližně polovina LBIT o DDoS útocích nikdy neslyšela (viz *otázka č. 2*), přestože, dle mého názoru, bylo v době počátku války mezi Ukrajinou a Ruskem v roce 2022 vysoce medializované.



Obrázek 12 – Graf odpovědí na otázku *č. 2*

Závěr

V ročníkové práci jsem se snažil převážně zmapovat problematiku DDoS útoků a vytvořit přehledný návod, jak se jim vyvarovat. Zde jsem se věnoval většině nejznámějších postupů. Z důvodu omezeného rozsahu práce jsem u většiny z nich však nezacházel do velkých podrobností. Do práce jsem přidal i kapitoly, které přímo nesouvisí s tématem práce, avšak pro pochopení samotného tématu je důležité znát několik aspektů, jako třeba fungování Internetu, OSI modelu apod. V práci jsou použity výsledky z průzkumu, který jsem dělal z důvodu zmapování povědomí společnosti o DDoS útocích a bezpečnosti na Internetu. Nepodařilo se mi však rozšířit dotazník i mezi jiné věkové skupiny než mé vrstevníky, pravděpodobně z důvodu nezájmu o toto téma. Proto v této práci jsou výsledky použity spíše jako doplnění k různým informacím.

Použité zdroje

[1] POWERCERT, Animated Videos. YouTube. YouTube [online]. United States of America, 2017, 26. 11. 2017 [cit. 2022-09-26].
Dostupné z: https://www.youtube.com/watch?v=ilhGh9CEIwM

[2] Cyberattack. Wikipedia [online]. last edited on 31 July 2022, at 19:22 (UTC) [cit. 2022-09-26].
Dostupné z: https://en.wikipedia.org/wiki/Cyberattack

[3] Malware. Wikipedia [online]. naposledy editováno 12. 7. 2022 v 16:34 [cit. 2022-09-26]. Dostupné z: https://cs.wikipedia.org/wiki/Malware

[4] Denial-of-service attack. Wikipedia [online]. last edited on 26 September 2022, at 14:15 (UTC) [cit. 2022-09-26].
Dostupné z: https://en.wikipedia.org/wiki/Denial-of-service_attack

[5] CHUCK, Network. I bought a DDoS attack on the DARK WEB (don't do this). YouTube [online]. United States of America, 3. 10. 2020 [cit. 2022-10-24].
Dostupné z: https://www.youtube.com/watch?v=eZYtnzODpW4

[6] CHUCK, Network. What is TCP/IP and OSI? // FREE CCNA // EP 3. YouTube [online]. United States of America, 6. 8. 2020 [cit. 2022-10-24].
Dostupné z: https://www.youtube.com/watch?v=CRdL1PcherM

[7] CHUCK, Network. REAL LIFE example!! (TCP/IP and OSI layers) // FREE CCNA // EP 4. YouTube [online]. United States of America, 6. 8. 2020 [cit. 2022-10-24].
Dostupné z: https://www.youtube.com/watch?v=3kfO61Mensg

[8] Network Bandwdith. SolarWinds [online]. United States of America [cit. 2022-10-29]. Dostupné z: https://www.solarwinds.com/resources/it-glossary/network-bandwidth

[9] What is DDoS Attack?. Microsoft Security [online]. United States of America [cit. 2022-10-29]. Dostupné z: https://www.microsoft.com/en-us/security/business/security-101/what-is-a-ddos-attack

[10] OSI model. Wikipedia [online]. last edited on 25 September 2022, at 04:01 (UTC) [cit. 2022-10-30].
Dostupné z: https://en.wikipedia.org/wiki/OSI_model

[11] ARPANET. Wikipedia [online]. last edited on 19 September 2022, at 07:34 (UTC) [cit. 2022-10-30]. Dostupné z: https://en.wikipedia.org/wiki/ARPANET

[12] Packet Switching. Avi Networks [online]. United States of America [cit. 2022-10-30]. Dostupné z: https://avinetworks.com/glossary/packet-switching/

[13] Protocol Wars. Wikipedia [online]. last edited on 30 October 2022, at 18:23 (UTC) [cit. 2022-10-30].
Dostupné z: https://en.wikipedia.org/wiki/Protocol_Wars

[14] ISO. About us. ISO [online]. Switzerland [cit. 2022-10-30].
Dostupné z: https://www.iso.org/about-us.html

[15] Kyberkriminalita. Policie České republiky [online]. Czech republic [cit. 2022-11-19].
Dostupné z: https://www.policie.cz/clanek/kyberkriminalita.aspx

[16] Nejčastější projevy kybernetické kriminality s odkazem na trestní zákoník. Policie České republiky [online]. Czech republic [cit. 2022-11-19].
Dostupné z: https://www.policie.cz/clanek/nejcastejsi-projevy-kyberneticke-kriminality-s-odkazem-na-trestni-zakonik.aspx

[17] ŠŤASTNÝ, Jakub. Trestní postih DoS/DDoS útoků. Šťastný - advokát [online]. Czech republic, 2020, 25. 5. 2020 [cit. 2022-11-19].
Dostupné z: http://stastny-advokat.cz/cz/blog/trestni-postih-dos-ddos-utoku/

[18] ČESKO. § 230 odst. 2 písm. b) zákona č. 40/2009 Sb., trestní zákoník – znění od 1. 9. 2022. In: *Zákony pro lidi.cz* [online]. © AION CS 2010–2022 [cit. 19. 11. 2022]. Dostupné z: https://www.zakonyprolidi.cz/cs/2009-40#p230-2-b

[19] SLOVENSKO. § 247a ods. 1 písm. a) zákona č. 300/2005 Z. z. trestný zákon - znenie účinné od 17.07.2022. In *Zákony pre ludi.sk* [online]. [cit. 19. 11. 2022]. Dostupné z https://www.zakonypreludi.sk/zz/2005-300/znenie-20220717#p247a-1-a

[20] IP address. Wikipedia [online]. last edited on 31 October 2022, at 19:55 (UTC) [cit. 2022-12-13].
Dostupné z: https://en.wikipedia.org/wiki/IP_address

[21] NORDSEC LTD. 25 Benefits of a VPN (Virtual Private Network). NordVPN [online]. United Kingdom [cit. 2022-12-18].
Dostupné z: https://nordvpn.com/features/

[22] SURFSHARK B.V. Surfshark VPN Features. Surfshark [online]. Netherlands [cit. 2022-12-18]. Dostupné z: https://surfshark.com/features

[23] GILLIS, Alexander. TECHTARGET. What is a Dynamic IP Address?. TechTarget [online]. United States of America, last updated in March 2020 [cit. 2022-12-23].
Dostupné z: https://www.techtarget.com/whatis/definition/dynamic-IP-address

[24] URL. Wikipedia [online]. last edited on 16 December 2022, at 01:06 (UTC) [cit. 2022-12-23]. Dostupné z: https://en.wikipedia.org/wiki/URL

[25] FORCEPOINT. What is a Firewall?. FORCEPOINT. Forcepoint [online]. United States of America [cit. 2022-12-25].
Dostupné z: https://www.forcepoint.com/cyber-edu/firewall

[26] EDUCBA. Types of ddos Attack. EDUCBA. EDUCBA [online]. India [cit. 2022-12-25]. Dostupné z: https://www.educba.com/types-of-ddos-attack/

[27] AT&T CYBERSECURITY. The 3 Types of DDoS Attacks Explained. AT&T CYBERSECURITY. AT&T Cybersecurity [online]. United States of America [cit. 2022-12-25]. Dostupné z: https://cybersecurity.att.com/blogs/security-essentials/types-of-ddos-attacks-explained

[28] VODAFONE. DDoS. VODAFONE. Vodafone [online]. Qatar [cit. 2022-12-28].
Dostupné z: https://www.vodafone.qa/en/business/services/security/ddos

[29] IMPERVA. What is DNS Amplification. IMPERVA. Imperva [online]. United States of America [cit. 2022-12-28].
Dostupné z: https://www.imperva.com/learn/ddos/dns-amplification/

[30] LINK11. DDoS Report 2021. Link11 [online]. 2021, 9. 10. 2021 [cit. 2022-12-28].
Dostupné z: https://www.link11.com/en/downloads/ddos-report-full-year-2021/

[31] Počítačová mravnostní kriminalita. Věda Policejní akademie: Bezpečnostní teorie a praxe [online]. Czech republic, 2022, 1. 1. 2022 [cit. 2023-01-01]. Dostupné z: https://veda.polac.cz/wp-content/uploads/2022/04/Pocitacova-mravnostni-kriminalita-%E2%80%93-kybergrooming.pdf

Obrázky

Všechny obrázky použité v práci jsou výhradním dílem autora, které byly dělány čistě ze znalostí autora, některé dle předloh uvedených níže:

[01] Logo Gymnázia Šlapanice. In: Gymnázium a ZUŠ Šlapanice [online]. [cit. 2022-09-26].
Dostupné z: https://gslapanice.cz/sites/default/files/inline-images/logo_gs_mody_prechod_na_pruhledne_1.png

[02] Router Icon. In: ClipArt Best [online]. [cit. 2022-10-30].
Dostupné z: http://www.clipartbest.com/clipart-4ibL66qrT

[03] Computer Icon. In: Vecteezy [online]. [cit. 2022-10-30]. Dostupné z: https://www.vecteezy.com/vector-art/648392-computer-icon-symbol-sign

[04] Mail Envelope Opened Symbol. In: OnlineWebFonts [online]. [cit. 2022-10-30]. Dostupné z: https://www.onlinewebfonts.com/icon/56743

[05] Mail Symbol. In: Multimediaitflah [online]. [cit. 2022-10-30]. Dostupné z: https://multimediaitflah.blogspot.com/2021/04/mail-symbol-message-clipart-mail-symbol.html

Přílohy

Příloha 1 – Dotazník

Součástí práce jsou závěry z dotazníku, který byl vytvořen pomocí webové aplikace Google Forms. *Příloha 1* je pouze přepisem, který zanechává hierarchickou a funkcionální strukturu.

Otázky, které jsou psány **tučně** se zobrazily každému uživateli nezávisle na jeho odpovědi. Z výběru možností označených • (černým vyplněným kruhem) jde vybrat pouze jedna možnost. Z výběru možností označených ○ (černou kružnicí) lze vybrat libovolný počet možností. Otázky, které jsou psány ***tučně a kurzívou*** se zobrazí uživateli pouze v závislosti, zdali odpověděl spíše kladně na otázku. U otázek, kde nejsou vypsány možnosti, dotázaní odpovídali svými slovy[40].

1. **Co je to DDoS útok?**
   - Přesně vím, o co se jedná
   - Vím, ale jen zhruba
   - Nejsem si moc jistý/jistá
   - Nemám ponětí, o co se jedná
2. **Jak často o DDoS útoku slýcháváte?**
   - Stále (alespoň 1 týdně)
   - Občas (alespoň 1 do měsíce)
   - Téměř vůbec (alespoň 1 do roka)
   - Nikdy jsem o tom neslyšel/a
3. **Z jakých zdrojů se k Vám tyto informace dostávají?**
   - Televizní noviny, televizní reportáž…
   - Noviny, časopisy
   - Konverzace (například předání informace od kamaráda)
   - Zpravodajské portály (například článek na Internetu)

[40] Jednalo se o otevřenou otázku, kde respondenti mohli uvést jakoukoliv odpověď ve formě textu.

- Sociální sítě

4. Jak často si myslíte, že se DDoS útoky dějí? (Napište Váš odhad počtu útoků, které proběhnou v celém světě za 24 hodin.)

- Edukativní důvody
- Pro zábavu, z nudy…
- Záměrné poškození (nedostupnost webové stránky, selhání serveru…)
- Testování ochran proti DDoS útokům (protože si to firma objednala)
- Jiné…

5. Myslíte, že je provozování DDoS útoků legální v ČR/SR?

- Ano
- Ne
- Jiné…

6. Jak se projeví, že je vaše zařízení cílem DDoS útoku?

- Vím
- Nejsem si jistý/jistá
- Nevím

7. Vyberte projevy DDoS útoku, které znáte:

- Zpomalení internetového připojení
- Výpadek internetového připojení
- Zpomalení zařízení
- Jiné…

8. Byl/a jste někdy původcem DDoS útoku? (Z pozice hlavního útočníka/útočnice — dělali jste ho záměrně.)

- Ano
    1. ***Za jakým účelem jste provozovali DDoS útok?***
        - Edukativní účely
        - Pro zábavu, z nudy…
        - Záměrné poškození (nedostupnost webové stránky, selhání serveru…)
        - Testování ochran proti DDoS útokům (protože si to firma objednala)
        - Jiné…

2. ***Jakých prostředků jste využili?***
    - Webové stránky
    - Pre-build software (program od někoho jiného — například na GitHubu)
    - Vlastní zdroje
    - Jiné…
- Ne

9. Víte, jak se DDoS útoku bránit?

- Ano
    1. ***Jaké znáte možnosti obrany proti DDoS útoku?***
        - Firewall
        - Zabezpečovací služby (například Cloudflare, Link11, TCP Shield…)
        - Prevence (nastavení routeru, používání VPN…)
        - Jiné…
- Nejsem si jistý/jistá
- Ne

10. Vyberte všechny možnosti, které používáte k ochraně:

- Dobře nastavený firewall
- Nejnovější verze programů a operačního systému
- Nastavenou konfiguraci routeru
- Používání VPN služeb
- Jiné…

11. Myslíte si, že je toto téma důležité rozebírat?

- Ano
    1. ***Proč ano?***
- Ne
    1. ***Proč ne?***
- Je mi to jedno…

12. Znáte nějaké typy DDoS útoků?

- Ano
    1. ***Vyberte, které typy DDoS útoků jste znali:***
        - RDDoS

- ICMP flood
- SYN flood
- HTTP flood
- Jiné…

- Nejsem si jistý/jistá
- Ne

13. Dokázali byste rozdělit DDoS útoky podle vrstev OSI modelu?

- Ano
- Nejsem si jistý/jistá
- Spíše ne
- Ne

14. Jaké znáte vedlejší efekty DDoS útoků?

- Plýtvání elektřiny
- Zpomalování internetu uživatelům, kteří s tím nemají nic společného (využívání bandwidth)
- Plýtvání peněz
- Jiné…

15. Vidíte DDoS útoky jako čistě negativní záležitost?

- Ano
- Ne

16. Zajímáte se o IT?

- Ano
- Ne

17. Jaký je Váš věk?

- Méně než 8 let
- 8 — 11 let
- 12 — 15 let
- 15 — 17 let
- 18 — 22 let
- 23 — 36 let
- 37 — 57 let

- 58 — 77 let
- Více než 78 let

18. Vyberte školy, které studujete nebo jste vystudoval/a:

- Základní škola
- Střední škola se zaměřením na IT
- Střední škola s jiným zaměřením (než IT)
- Gymnázium všeobecné
- Gymnázium se zaměřením na IT
- Gymnázium s jiným zaměřením (než IT)
- Vyšší odborná škola se zaměřením na IT
- Vyšší odborná škola s jiným zaměřením (než IT) (včetně konzervatoře)
- Vysoká škola
- Zahraniční studium
- Jiné…

19. V jaké zemi přebýváte?

- Česká republika
- Slovenská republika
- Jiné…

20. Chcete něco dodat?