FAKULTA INFORMAČNÍCH TECHNOLOGIÍ ČVUT V PRAZE

Zadání bakalářské práce

Název:	Analýza nejčastěji používaných síťových útoků a jejich mitigace
Student:	Stanislava Blaňková
Vedoucí:	Ing. Alexandru Moucha, Ph.D.
Studijní program:	Informatika
Obor / specializace:	Bezpečnost a informační technologie
Katedra:	Katedra počítačových systémů
Platnost zadání:	do konce letního semestru 2021/2022

Pokyny pro vypracování

Vytvořte komplexní analýzu nejznámějších útoků na firemní sítě. U těchto síťových útoků zdokumentujte související procesy a metody jejich detekce a mitigace, zaměřte se na technologie a zařízení Cisco.

Elektronicky schválil/a prof. Ing. Pavel Tvrdík, CSc. dne 18. prosince 2020 v Praze.

FAKULTA
INFORMAČNÍCH
TECHNOLOGIÍ
ČVUT V PRAZE

Bakalářská práce

Analýza nejčastěji používaných síťových útoků a jejich mitigace

Stanislava Blaňková

Katedra počítačových systémů
Vedoucí práce: Ing. Alexandru Moucha, Ph.D.

13. května 2021

Poděkování

Děkuji Ing. Alexandru Mouchovi, Ph.D. za jeho vedení a cenné rady, které přicházely ve správných chvílích. Aleně B. a Janu Ř. děkuji za veškerou jejich podporu. Velice si Vás všech vážím.

Prohlášení

Prohlašuji, že jsem předloženou práci vypracovala samostatně a že jsem uvedla veškeré použité informační zdroje v souladu s Metodickým pokynem o dodržování etických principů při přípravě vysokoškolských závěrečných prací.

Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona, ve znění pozdějších předpisů. V souladu s ust. § 2373 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů, tímto uděluji nevýhradní oprávnění (licenci) k užití této mojí práce, a to včetně všech počítačových programů, jež jsou její součástí či přílohou a veškeré jejich dokumentace (dále souhrnně jen „Dílo"), a to všem osobám, které si přejí Dílo užít. Tyto osoby jsou oprávněny Dílo užít jakýmkoli způsobem, který nesnižuje hodnotu Díla a za jakýmkoli účelem (včetně užití k výdělečným účelům). Toto oprávnění je časově, teritoriálně i množstevně neomezené. Každá osoba, která využije výše uvedenou licenci, se však zavazuje udělit ke každému dílu, které vznikne (byť jen zčásti) na základě Díla, úpravou Díla, spojením Díla s jiným dílem, zařazením Díla do díla souborného či zpracováním Díla (včetně překladu) licenci alespoň ve výše uvedeném rozsahu a zároveň zpřístupnit zdrojový kód takového díla alespoň srovnatelným způsobem a ve srovnatelném rozsahu, jako je zpřístupněn zdrojový kód Díla.

V Praze dne 13. května 2021 . . . . . .

Odkaz na tuto práci

Blaňková, Stanislava. *Analýza nejčastěji používaných síťových útoků a jejich mitigace*. Bakalářská práce. Praha: České vysoké učení technické v Praze, Fakulta informačních technologií, 2021.

Abstrakt

Bakalářská práce se zabývá analýzou nejčastějších síťových útoků a popisem jejich mitigace, zaměřuje se na území České republiky. Na začátku je vymezena základní terminologie a na jejím základě je následně proveden průzkum výskytu bezpečnostních incidentů v letech 2017 až 2020. Průzkum je interpretován v prostředí síťových útoků na základě taxonomie incidentů a ve spolupráci s odborníky z Národního úřadu pro kybernetickou a informační bezpečnost. Vyplynuvší útoky: skenování portů, otrava mezipaměti DNS a DDoS útok, jsou následně detailně rozebrány, tzn. je uveden jejich princip a popsána jejich taxonomie. Útoky jsou navíc vždy analyzovány i v kontextu bezpečnostních incidentů a zasazeny do terminologie představené v počátku práce.

Následně je pro tyto útoky představeno účinné řešení, jak metodické, tak procesní (s výjimkou DDoS útoku, ten je řešen pouze metodicky). Řešení detailně popisuje způsoby mitigace analyzovaných útoků, zaměřuje se na technologická řešení: Cisco ASA, Cisco FMC, DNSSEC. V příloze je navíc uveden příklad postupu základní bezpečnostní konfigurace Cisco ASA firewallu a postup nastavení detekce port skenů na technologii Cisco FMC. Přílożené konfigurační postupy jsou v práci řádně okomentovány.

Klíčová slova analýza síťových útoků, průzkum výskytu, oblast ČR, skenování portů, otrava mezipaměti DNS, DDoS, metody mitigace, Cisco ASA, Cisco FMC, DNSSEC

Abstract

The bachelor thesis deals with an analysis of the most common network attacks and a description of their mitigation, focusing on the territory of the Czech Republic. At the beginning, the basic terminology is defined and on its basis, a survey of the occurrence of security incidents in the years 2017 to 2020 is subsequently performed. The survey is interpreted in the context of network attacks based on the taxonomy of incidents and in cooperation with experts from the National Office for Cyber and Information Security. The resulting attacks: port scanning, DNS cache poisoning and DDoS attack, are then analyzed in detail, ie. their principle is given and their taxonomy is described. In addition, attacks are always analyzed in the context of security incidents and embedded in the terminology introduced at the beginning of the work.

Subsequently, an effective solution, both methodological and procedural, is presented for these attacks. The solution presents methods of detection and prevention of analyzed attacks focuses on technological solutions: Cisco Cisco ASA, Cisco FMC, DNSSEC. In addition, the appendix provides an example of the basic Cisco ASA firewall security configuration procedure and the procedure for setting up port scan detection on Cisco FMC technology. The attached configuration procedures are properly commented in the work.

Keywords network attack analysis, occurrence survey, Czech Republic area, port scanning, DNS cache poisoning, DDoS, mitigation methods, Cisco ASA, Cisco FMC, DNSSEC

Obsah

Seznam obrázků

Úvod

V kontextu dnešní doby se stále zvyšují nároky na zabezpečení síťové infrastruktury. Pro některé menší a středně veliké firmy (či státní podniky) to může představovat významné náklady, které zvláště v krizové době mohou být velkou překážkou pro realizaci bezpečné sítě.

Cílem práce je seznámit čtenáře s tím, jaké jsou současné nejběžnější útoky využívající či cílící na síťovou infrastrukturu společností v České republice a přiblížit tak čtenáři problematiku síťové bezpečnosti. Práce rovněž představuje metody a procesy zmírnění dopadů těchto útoků, může tedy posloužit dalším společnostem a jejich technickým zaměstnancům jako odrazový můstek pro vytvoření kvalitního síťového zabezpečení a jako zdroj užitečných informací pro bezpečné nastavení síťových zařízení. Konkrétně se práce zaměřuje na technologická řešení společnosti Cisco.

Téma jsem si zvolila jednak, protože by to dle mého názoru mohlo některým společnostem pomoci při rozvoji bezpečnosti jejich sítě, jednak z důvodu, že jsem postrádala v literatuře takto geograficky vymezenou práci.

Samozřejmě není v možnostech práce poskytnout kompletní návod, jak vytvořit stoprocentně bezpečnou síť - to si práce za cíl neklade. Nicméně pokrytí alespoň nejčastějších útoků, může mít poměrně dobrý efekt a velice příznivý přínos. Také by dle mého názoru geograficky vymezený pohled mohl být užitečný a inspirativní pro další zkoumání.

Práce se skládá ze dvou hlavních kapitol: *Analýza* a *Mitigace*.

V první kapitole práce shrnuje potřebnou terminologii, dále popisuje postup průzumu výskytu síťových útoků v ČR, předkládá a interpretuje jeho výsledky a nakonec detailně rozebírá nejpodstatnější útoky vyplývající z tohoto průzkumu.

Druhá kapitola se zaměřuje na obranu sítě vůči analyzovaným útokům. Opět se pro začátek nabízí úvod do používané terminologie, ta se zaměřuje na vysvětlení a popis technologií, které je možné využít k detekci a ke zmírnění dopadu útoků. Podkapitola shrnuje také přehled a stručný popis Cisco tech-

nologií. Pro dříve analyzované útoky jsou představena konkrétní metodická řešení zmírnění jejich dopadů a způsoby, jak je možné nastavit Cisco technologie tak, aby síť proti útokům, co nejlépe ochránily.

Kapitola 1

Cíl práce

Hlavním cílem bakalářské práce je vytvoření komplexní analýzy síťových útoků, se kterými se dnes běžně setkávají firmy na území ČR, a popsání způsobů jejich detekce a mitigace.

Cílem analytické části je dohledání nejčastějších síťových útoků na našem území a jejich následná detailní analýza. K tomu je potřeba vymezení základní terminologie, dohledání často zmiňovaných útoků v současné literatuře a průzkum toho, jaké z těchto útoků (a jestli vůbec) jsou na našem území evidovány. V závěru průzkumu budou vybrány útoky k analýze, výběr bude náležitě okomentován. Vybrané útoky budou detailně vysvětleny s ohledem na jejich princip a klasifikaci.

Druhá část práce cílí především na vysvětlení způsobů detekce a mitigace výše zmíněných útoků. Napřed bude vytvořen přehled technologií a základní terminologie. Poté budou rozebrány metody a procesy detekce a mitigace vybraných útoků z analytické části. Celá tato část se zaměří na Cisco technologie.

Kapitola 2

Analýza

Cílem této kapitoly je identifikace a analýza nejčastěji se vyskytujících síťových útoků na území ČR.

Na úvod kapitola definuje základní pojmy potřebné pro průzkum, v hlavní části se zabývá průzkumem samotným a analýzou útoků, které z něj vyplývají.

2.1 Terminologický základ

Podstatným pro další práci je pojem *síťový útok*. Než se dostaneme k zavedení kýženého pojmu, napřed bude potřeba definovat několik málo pomocných pojmů.

Z Kolouchova a Baštova díla [1] je zjevné, že hlavním cílem kybernetické bezpečnosti je zajistit *důvěrnost*, *integritu* a *dostupnost*, jak informací samotných, tak i informačního systému a jeho prvků. Citujme tedy z doporučení ITU-T X.800 [2] (překlad Lórencz [3]) definice následujících tří pojmů:

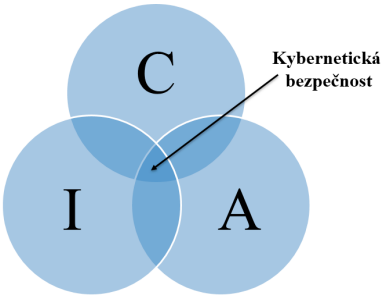
Definice 2.1.1 *„**Důvěrnost** je vlastnost, která zaručuje, že informace nebude dostupná neautorizovanému subjektu.“*

Definice 2.1.2 *„**Integrita**[1] je vlastnost, která zaručuje úplnost a přesnost zpracované, resp. přenášené informace.“*

Definice 2.1.3 *„**Dostupnost** je vlastnost, která zaručuje, že informace bude dostupná autorizovanému subjektu.“*

Tyto vlastnosti se označují [1] jako *CIA triáda* (z angl. ***C**onfidentiality, **I**negrity* a ***A**vailability*). Můžeme říct, že triáda tvoří jádro kybernetické bezpečnosti, a tedy útokem na některou z výše uvedených vlastností dojde k narušení bezpečnosti informačního systému.

[1] též překládáno dle [1] jako **celistvost**



Obrázek 2.1: CIA a kybernetická bezpečnost [1]

Definice 2.1.4 *„**Kybernetický útok** lze definovat jako jednání útočníka či skupiny útočníků, které využívá informační a komunikační technologie k útoku na jinou informační a komunikační infrastrukturu, ať už s cílem narušit **dostupnost, důvěrnost** nebo **integritu** dat.“ [1]*

Přičemž *data* jsou v jistém smyslu pojem nadřazený k pojmu *informace*. Chápejme tedy, že informace se typicky skládá z nějakých dat, ale data samotná nemusejí být celistvou informací.

A konečně, podmnožinou kybernetických útoků jsou *útoky síťové*, resp. *útoky na počítačovou síť* (z angl. *computer network attacks*).

Definice 2.1.5 ***Síťový útok**, resp. **útok na počítačovou síť**, definujeme jako „činnosti prováděné za pomoci počítačových sítí vedoucí k narušení, popření, degradaci nebo zničení informací uložených v počítačích a počítačových sítích, nebo počítačů a sítích samotných.“ [4] (překlad autorky)*

Kritéria pro vymezení této podmnožiny nemají přesné hranice, a to především díky možným překryvům síťové a počítačové bezpečnosti, ke kterým dle Lórencze [3] dochází. Výše uvedené *„narušení, popření, degradace“* a *„zničení“* informací je z podstaty věci (v kontextu kybernetické bezpečnosti) chápáno jako útok na triádu CIA. Definice však zúžuje prostředky i cíl útoku, proto je možné mluvit o podmnožinovém vztahu předešlých dvou pojmů.

Nicméně se stále jedná o velice rozsáhlou oblast, kterou je (dle domluvy s vedoucím práce) potřeba kvůli omezenému rozsahu práce zúžit, a proto pro účely práce použijeme následující definici.

Definice 2.1.6 *„Kybernetický útok, cílící na síťovou infrastrukturu nebo síťový provoz, který je možné detekovat nazveme **síťovým útokem**.“ [5]*

Takto zostříme hranici mezi síťovou a počítačovou bezpečností. Vyloučíme tím z práce například rozsáhlou kategorii *škodlivých virů* posílaných po síti, které cílí na koncová zařízení a další útoky, které by běžně spadaly do oblasti počítačové bezpečnosti, pokud by nebyly přenášeny po síti.

V neposlední řadě je potřeba porozumět pojmu *bezpečnostní incident* a pochopit jeho odlišnosti od kybernetického útoku. Vyjdeme ze zákona[2] o kybernetické bezpečnosti.

Definice 2.1.7 ***Bezpečnostní incident*** *definujeme jako „narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.“*

Neboli, *bezpečnostní* incident je událost, při které došlo k narušení *triády CIA*. Rozdílem oproti kybernetickému útoku je ten, že útok je cílený a úmyslný. Tedy útočník vědomě narušuje bezpečnost. Kdežto u bezpečnostního incidentu může jít i o neúmyslné narušení či o nedbalost. Dále je důležité poznamenat, že *kybernetická bezpečnostní událost* se od *bezpečnostního incidentu* liší tím, že na základě ní pouze *může* dojít k narušení bezpečnosti, kdežto při incidentu k tomuto narušení *již došlo*. Ona událost má tedy potenciál stát se bezpečnostním incidentem, ale dojít k tomu nutně nemusí.

A nakonec pro úplnost uveďme poslední čtyři související termíny, které můžeme použít pro kategorizaci a popis útoků. Tyto termíny později poslouží při analýze útoků.

Zaprvé rozlišujeme útoky na *pasivní* a *aktivní*.

Definice 2.1.8 ***Pasivní útok*** *je útok, při kterém se útočník „pokouší získat nebo využít informace ze systému, ale nijak se nepokouší ovlivnit prostředky tohoto systému.“ [6] (překlad autorky)*

Definice 2.1.9 ***Aktivní útok*** *je útok, při kterém se útočník „pokouší měnit systémové prostředky nebo ovlivnit jejich funkčnost.“ [6] (překlad autorky)*

Lórencz [3] ve svých přednáškách zmiňuje, že pasivní útoky se jen těžko detekují. Zakládají se na monitorování či odposlechu datového provozu, čímž dochází k narušení důvěrnosti dat, ale data nejsou nijak modifikována či znepřístupněna autorizovaným subjektům. Takovými nezřetelnými projevy útoků se jejich detekce pochopitelně znesnadňuje. Naproti tomu aktivní útoky se vzhledem ke své povaze detekují mnohem snadněji, projevují se totiž rychleji a mají evidentní účinky. Tyto útoky můžeme dělit na útoky využívající předstírání identity, útok opakováním, modifikace zprávy nebo útoky typu odmítnutí služby.

Za druhé můžeme rozlišovat útoky podle toho odkud jsou iniciovány, tedy podle toho zda útočíme *zevnitř* bezpečnostního perimetru nebo *zvnějšku*.

Definice 2.1.10 ***Vnitřní útok*** *(z angl. „inside attack“) je útok, který je„iniciovaný entitou (tzv. „insider“) uvnitř bezpečnostního perimetru, tedy entita*

[2] § 7 odst. 2 zákona č. 181/2014 Sb. o kybernetické bezpečnosti

***je oprávněná** k přístupu k systémovým prostředkům, ale používá je **nepovoleným způsobem**.“ [6] (překlad autorky)*

Definice 2.1.11 ***Vnější útok** (z angl. „outside attack“) je útok, který je „iniciovaný zvnějšku perimetru uživatelem (tzv. „outsider“), který **není oprávněný** k přístupu k systémovým prostředkům nebo má **nelegitimní** přístup.“ [6] (překlad autorky)*

Jinými slovy, v kontextu *útoků na síťovou infrastrukturu*, k útoku *zevnitř sítě* dochází uvnitř perimetru sítě, tj. ze zařízení , které má oprávněný přístup k síti nebo je v ní přímo fyzicky umístěno. Naproti tomu útok *zvnějšku sítě* chápeme jako útok na perimetr sítě, protože útočník není v síti, útočí buďto na zmíněný perimetr nebo se skrz něj pokouší do sítě proniknout.

2.2 Průzkum výskytu útoků

Původním cílem průzkumu bylo zmapovat přímo četnost *síťových útoků*, mířených na subjekty vyskytující se na území ČR. Ovšem při prohledání dostupných zdrojů (databáze ČSÚ, statistické databáze knihovny ČVUT, data poskytovaná národním a vládním CERT týmem, komunikace s NÚKIB [7]), bylo nutné dojít k závěru, že žádná statistická data zaměřující se konkrétně na tuto problematiku neexistují. Stejně tak je tomu v případě evidence *kybernetických útoků*, kde snaha dohledat tuto evidenci byla dalším logickým krokem průzkumu.

Úspěch přišel až v případě statistik týkajících se *bezpečnostních incidentů*. Proto byl průzkum dále rozšířen, bylo nutné zvětšit jeho záběr na data vázaná k incidentům. A protože úmyslně zaviněné bezpečnostní incidenty se překrývají s kybernetickými útoky, potažmo síťovými útoky, mohou být nalezená data použita pro potřeby průzkumu.

Původní cíl tímto tedy neopouštíme, ale průzkum bude o něco méně přímý, vzhledem k tomu, že data evidovaná v rámci bezpečnostních incidentů se musejí vhodně interpretovat a převést do prostředí síťových útoků, se kterými mají překryv. Průzkum tedy vymezme takto:

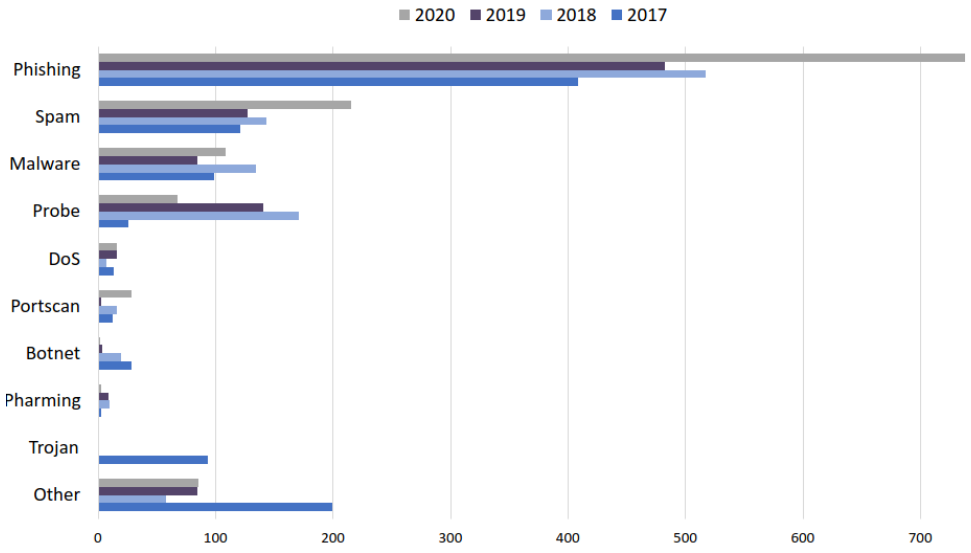
- oblast: ČR,
- časový rozsah, v letech: 2017, 2018, 2019, 2020
- zdroje dat: výroční zprávy národního a vládního CERT týmu, přímá komunikace s vládním CERT týmem (tj. NÚKIB)

Česká republika, tj. všichni uživatelé a všechny provozované sítě na jejím území, spadá dle [9] do pole působnosti národního CERT týmu (tj. CSIRT.CZ, jehož provozovatelem je sdružení CZ.NIC). Národní CERT spolupracuje s dalšími 25 bezpečnostními [10] týmy na našem území. S těmito týmy sdílí data

a koordinuje řešení incidentů. Ke zmíněným týmům se řadí i vládní CERT (tj. GOVCERT.CZ, tedy NÚKIB). Vládní CERT má ze zákona speciální roli, zaměřuje se především na regulované subjekty napříč republikou, kterým zákon uděluje povinnost[3] hlášení bezpečnostních incidentů. Data od těchto dvou týmů tedy pokrývají dostatečný vzorek pro průzkum výskytu incidentů v České republice.

Dle informací z NÚKIB [11] se národní a vládní CERT tým řídí při evidenci bezpečnostních incidentů stejnou taxonomií (ENISA[4]) tak, aby data byla v rámci CERT týmů konzistentní. Také však dochází k prohloubení stávající evidence útoků, ta se v posledních letech rozšiřuje na základě matice[5] organizace Mittre, čímž dochází k podrobnější evidenci jednotlivých útočných metod použitých v rámci bezpečnostních incidentů. Data podle této nové taxonomie jsou však dostupná pouze za poslední rok a půl, proto průzkum vyjde ze starší taxonomie, jejíž data jsou dostupná v širším časovém horizontu.

Souhrná data, vycházející z výročních zpráv [12], [13], [14], [15] národního CERT týmu z let 2017-2020, jsou následující:



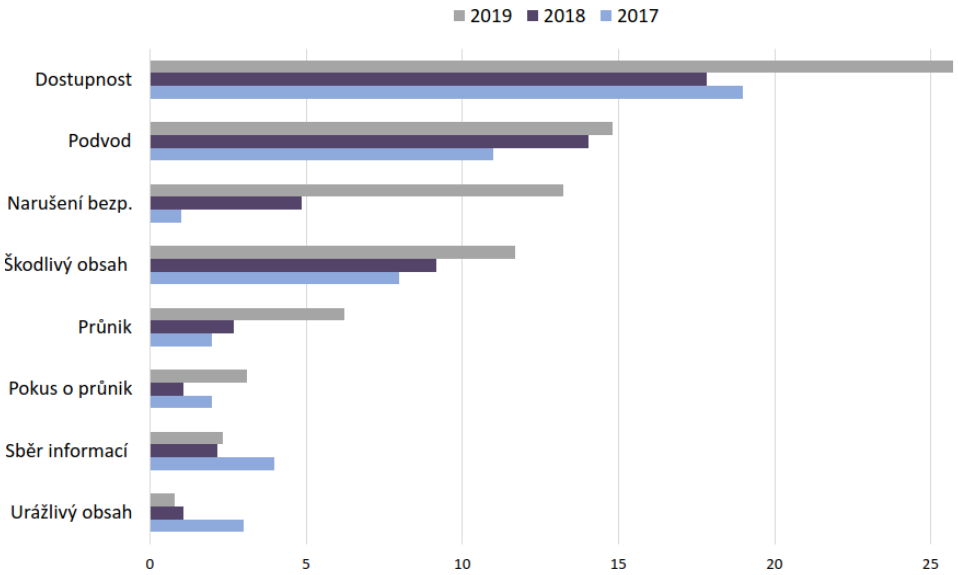
Obrázek 2.2: Evidované bezpečnostní incidenty (národní CERT)

Druhý graf ilustruje data vládního CERT týmu, vychází z výročních zpráv z let 2017-2019 [16], [17], [18] (zpráva z roku 2020 zatím není dostupná):

[3] dle § 8 odst. 1 zákona č. 181/2014 Sb. o kybernetické bezpečnosti

[4] `https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy`

[5] viz `https://attack.mitre.org/matrices/enterprise/`



Obrázek 2.3: Evidované bezpečnostní incidenty (vládní CERT)

Data uvádí absolutní počty všech řešených incidentů ve vybraných kategoriích (zdrojové tabulky viz příloha B). V grafu národního CERT je vynechaná kategorie *Virus*, která za dané roky měla nulový výskyt a též ktegorie *Sensor Network*, která dle popisu [19] není vyhodnocována jako incident. Dále je pak v grafu vládního CERT z původních dat vynechaná kategorie *Administrativní*, která nespadá do oblasti kybernetických útoků.

Je důležité zmínit, že se dle informací [11] typicky eviduje nejzávažnější dosažená fáze útoku. Je tedy běžné, že například pokud dojde ke skenování sítě, pokusu o průnik do sítě a následnému úspěšnému průniku, bude evidován pouze incident v kategorii *Průnik*, ale už nebude neevidován incident v kategoriích *Sběr informací* a *Pokus o průnik*.

Jednotlivé kategorie je možné na sebe namapovat dle příslušných popisů [19] [20] takto (s tím, že levé pojmy jsou obsáhlejší než pojmy vpravo):

- Dostupnost $\approx DoS$
- Podvod $\approx Phishing, Pharming$
- Narušení bezpečnosti
- Škodlivý obsah $\approx Malware, Trojan, Virus$
- Průnik $\approx Botnet$
- Pokus o průnik

- Sběr informací ≈ *Probe*[6], *Portscan*[7]
- Urážlivý obsah ≈ *Spam*

Cílem následujících odstavců je okomentovat jednotlivé kategorie vzhledem k získaným datům a propojit je se síťovými útoky dle informací z NÚKIB a z infromací dostupných z popisů kategorií incidentů.

Dostupnost je nejpočetněji zastoupená kategorie incidentů v datech vládního týmu. Řadí se sem veškeré *DoS útoky* a mezi nejčastější síťové útoky na dostupnost patří dle NÚKIB [21] *DDoS útoky*. Na národní úrovni již tato kategorie nevykazuje tak častý trend, ale stále zastává pozici v poměrně vysokých příčkách, dle popisu kategorie [19] sem často spadají hlášení týkající se IP adres, které k DoS útoku byly zneužity.

U podvodných metod útoků je jednoznačně nejtypičtějším útokem *Phishing*, jak na vládní [21], tak na národní úrovni, kde se nachází na prvním místě. Dál do podvodných metod patří útoky využívající předstírání identity, na národní úrovni se eviduje kategorie *Pharming*, ta je z hlediska této práce zajímavější než phishing, protože dle [19] využívá nejčastji metodu síťového útoku *otravy mezipaměti DNS*[8]. Pharming je se svou četností až na osmé pozici evidence národního týmu.

Narušení bezpečnosti je kategorie, ve které dle vládního CERT [21] dochází nejčastěji k exfiltraci dat nebo k úniku přihlašovacích údajů. Z pohledu síťových útoků sem dle [20] patří odposlouchávání a rozsáhlá kategorie *Spoofing útoků*. Jedná se o třetí nejpočetnější kategorii v evidovaných datech vládního týmu v roce 2019.

Škodlivý obsah se v průběhu posledních tří let objevuje ve vládních datech na třetí a čtvrté pozici, jde o početně zastoupenou kategorii. Na vládní úrovni do této kategorie patří *Malware*, *Virus* a *Trojan*. Z toho nejčastější je *Malware*, který je za rok 2020 na třetím místě, v předešlých letech se objevuje ale i na nižších pozicích. V případě, že škodlivé kódy používají nějaký síťový útok, nedochází dle Sikory [7] k evidenci těchto metod, protože nejsou v rámci šetření incidentu podstatné. Sikora, ale píše, že malware může metody síťových útoků využívat.

Průnik a pokus o průnik obsazují v letech 2019-2020 čtvrtou a pátou pozici, přičemž kategorie *Průnik* má rostoucí tendenci. Z pohledu sítí se dle Sikory [21] nejčastěji jedná o prolomení (resp. pokus o prolomení) hesla uživatelského účtu nebo o exploitaci zranitelnosti (resp. pokus o exploitaci). Z vládních dat sem dle taxonomie [20] spadá kategorie *Botnet*, ve které se evidují zařízení zneužita k DoS nebo DDoS útokům. Četnost incidentů v kategorii *Botnet* v průběhu let 2017-2020 klesala.

[6] česky prozkoumávání/sondování
[7] česky port sken
[8] angl. *DNS cache poisioning*

Sběr informací je za poslední rok až na předposlední pozici, v minulých letech se však pohyboval ve vyšších pozicích. V rámci síťových útoků sem dle popisu [20] řadíme skenování (např. portů, zranitelností). Dle Sikory [7] skenování příchozí z veřejné sítě nemá smysl nijak evidovat; pokud jde pak o incidenty ve vnitřní síti, je zmapování infrastruktury nutnost pro další postup útoku. Dle rozhovoru [11] je při postupu útoku do další fáze evidována pokročilejší fáze útoku, proto může být v této kategorii zdánlivě méně výskytů, ačkoli fakticky je skenování velmi častá záležitost. Četnost evidovaných incidentů v kategorii *Portscan* v národních datech se v roce 2020 významně navýšila a nachází se tak na páté nejvýznamnější pozici.

Urážlivý obsah je v datech vládní úrovně na posledním místě v počtu hlášených incidentů a v uvedených letech má klesající tendenci. Dle [21] se typicky jedná o SPAM. V datech národního týmu jsou data v této kategorii v posledním roce na druhé pozici, v minulých letech však byla na pozicích nižších.

Dle Sikory [7] je běžnou technikou síťových útoků také *podvržení IP adresy*[9]. Tato metoda se využívá ke skrytí identity útočníka.

2.2.1 Výsledek

V úvahu přicházeli dvě možnosti postupu. První možností bylo zpracování analýzy útoků „do šířky“ (tzn. rozebrat větší množství útoků povrchově). Tento postup by byl výhodný z hlediska přínosu kapitoly *Mitigace*, která by tak souhrně popsala zmírnění většího množství útoků. Druhou možností bylo zpracování útoků „do hloubky“ (tzn. rozebrat menší množství útoků s větším detailem) , které pro změnu umožní pojmout téma natolik odborně, jak si to vyžaduje psaní bakalářské práce. Vzhledem k povaze práce byl tedy zvolen druhý postup. Vybrané síťové útoky určené pro další rozbor jsou následující:

- Skenování portů
- Otrava mezipaměti DNS
- DDoS útok

Skenování portů je dle průzkumu častou metodou a bylo vybráno, protože se jedná o první článek možného řetězce útoků a zdá se být logické mitigovat útoky již v této fázi. Další zvolenou útočnou metodou je *otrava mezipaměti DNS*. Jedná se o útok, který může být využit například škodlivými kódy nebo při pharmingu. Navíc jde dle [8] o stále aktuální hrozbu. A jako poslední byl vybrán *DDoS útok*, který je dle informací nejčastěji řešeným útokem vládního CERT týmu, jehož data odpovídají dle [16] společnostem se špatným síťovým zabezpečením v důsledku podfinancování. Proto byl s ohledem na tento fakt a zamýšlený přínos práce vybrán poslední analyzovaný útok takto.

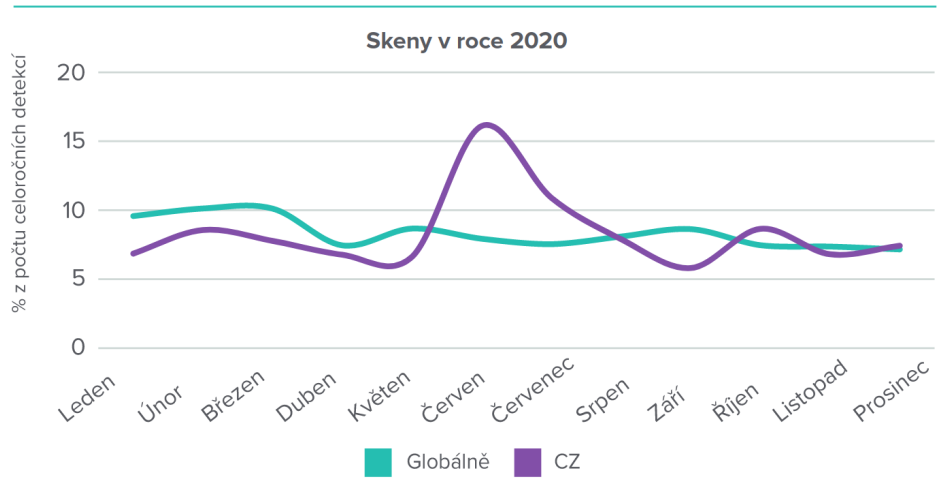
[9] angl. *IP address spoofing*

2.3 Analýza útoků

V úvodu následujících podkapitol je vždy každý útok propojen s kontextem bezpečnostních incidentů a s průzkumem představeným v předchozí kapitole. Hlavní částí je rozbor principu jednotlivých útoků a představení a vysvětlení taxnomoií útoků. Dále jsou vysvětleny některé podtypy daných útoků vyplývající z předešlé přestavené taxonomie. V závěru každé podkapitoly jsou útoky interpretovány v kontextu terminologie vysvětlené v kapitole 2.1.

2.3.1 Skenování portů

Port sken je ve zdroji [22] řazen mezi takzvané *průzkumné útoky*[10], jejichž cílem je sběr informací. V rámci bezpečnostních incidentů řadíme skenování portů do kategorií *Sběr informací, Port sken* a *Probe* (tj. sondování). Dle předchozího průzkumu se jedná se o jeden z nějčastějších útoků na síťovou infrastrukturu. Společnost ALEF uvádí ve svém reportu [23] následující průběh detekce skenů v roce 2020:



Obrázek 2.4: Detekce skenů v roce 2020 [23]

Průběh je dle [24] popisu v reportu podobný průběhu z roku 2019, kde dochází na úrovni České republiky v letních měsících k obdobným špičkám (přibližně o měsíc později, tj. v červenci a listopadu). Trendy detekovaných skenů se v roce 2019 v druhé polovině roku překrývají s trendy v detekci škodlivého kódu. ALEF zde uvádí možnou souvislost s malware kampaněmi cílícími na systémy dostupné z internetu, jejichž zranitelnosti byly odhalené

[10] angl. *Reconnaissance Attacks*

právě skenováním. Je evidentní, že skenování je prvopočátkem velkého množství útoků, proto je potřeba zabývat se jeho detekcí a mitigací.

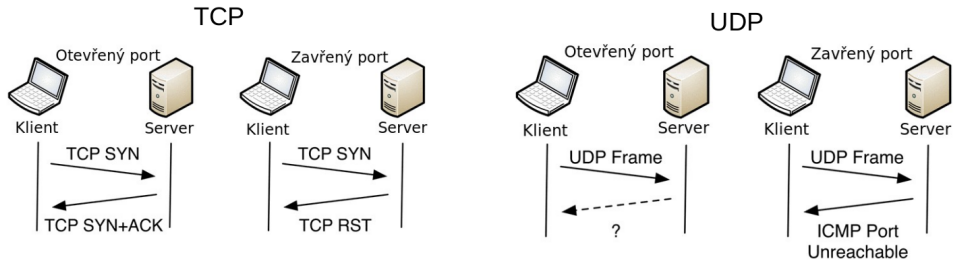
NIST ve svém glosáři uvádí odkazy na následující definice:

Definice 2.3.1 ***Skenování portů***[11] *definujeme jako „použití programu ke vzdálenému určení otevřených portů systému.“ [25] (překlad autorky)*

Definice 2.3.2 ***„Port skener***[12] *je program, který dokáže zjistit, které porty v systému jsou otevřené.“[26] (překlad autorky)*

Jinými slovy, port sken za pomoci port skeneru zjišťuje jaké služby (tj. porty) jsou dostupné (tedy mohou přijímat a odesílat data) v daném rozsahu IP adres v systému. Tyto služby mohou mít zranitelnosti, které je útočník schopen zneužít, pokud se službou může komunikovat. Existuje mnoho druhů port skenerů, jeden z nejběžnějších je např. nástroj *nmap*.

Základním členěním port skenů, které je napříč léty v literatuře [27], [28], [29] k vidění, je rozlišení na *TCP* a *UDP skeny*. Podle toho, zda port sken určuje dostupnost služeb (resp. portů) uskutečnujících spojení pomocí transportního protokolu TCP nebo UDP. Každý z těchto protokolů má své specifické vlastnosti a na jejich základě se skeny od sebe liší. Protože TCP protokol je tzv. *connection-oriented*, dochází při navázání spojení se službou k výměně specifických packetů v podobě známého *three-way handshake*. Naproti tomu UDP je tzv. *connectionless*, to znamená, že nedochází k potvrzení navázaného spojení a rovnou je odeslána odpověď na přijatý packet. Z pohledu port skenů je toto podstatné, protože podle reakce při pokusu o navázání komunikace je možné zjistit, zda je daná služba dostupná či nikoli. Rozdíl ilustruje obrázek 2.4., na kterém je vidět reakce serveru na klientův požadavek.



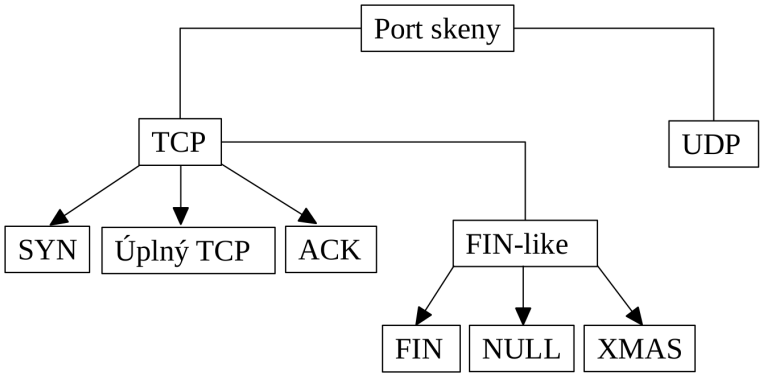
Obrázek 2.5: TCP a UDP porty reagují odlišně na doručený packet v závislosti na tom, zda je port otevřený nebo zavřený [28] (překlad autorky)

Pro znázorněný TCP sken (zde konkrétně SYN sken, který bude podrobněji vysvětlen na další straně) je reakce indikující otevřený port přijetí SYN/ACK

[11] angl. *Port scanning*
[12] angl. *Port scanner*

packetu odeslaného serverem (tj. běžná odpověď v rámci *three-way handshake*). Pakliže je port serveru zavřený dorazí packet s příznakem RST (tj. reset připojení[13]). V případě UDP komunikace začne server při přijetí packetu na otevřeném portu okamžitě komunikovat a odešle požadovaná data zpět klientovi, v případě zavřeného portu dojde k zaslání zprávy specializovaným protokolem ICMP, tato zpráva nese informaci o nedosažitelném portu[14]. Z tohoto chování komunikačních protokolů je tedy nepochybně možné vydedukovat dostupnost či nedostupnost služeb na daných portech.

Na základě informací z dostupné literatury [22], [27], [29], [30], [31], [32] byl vytvořen přehled základních zmiňovaných technik port skenů. Tyto metody můžeme pro přehlednost znázornit následujícím schématem (inspirovaným výše zmíněnými zdroji):



Obrázek 2.6: Základní členění port skenů

Veškeré popsané metody skenů jsou typicky implementovány na úrovni skenerů, které umožňují tyto metody jednoduše použít. V následujících odstavcích detailně zanalyzujeme tyto metody, práce přitom vyjde z výše zmíněné literatury, především z nejnovějších manuálových stránek programu *nmap* [32]. Na úvod zmiňme, že nástroj *nmap* definuje šest možných stavů portu: *open*, *closed*, *filtered*, *unfiltered*, *open|filtered* a *closed|filtered*.

Implementace *SYN skenu* využívá techniku zaslání synchronizačního packetu s TCP příznakem[15] SYN (tj. první krok *three-way hanshake*), který na straně serveru vyvolá následující reakci na základě toho, zda je daný port serveru:

- otevřený: odešle server klientovi SYN/ACK packet (tj. druhý krok *three-way hanshake*), stav portu je skenerem určen jako *open*,
- zavřený: odešle klientovi packet s RST příznakem, stav portu je skenerem určen jako *closed*,

[13] angl. *reset the connection*
[14] angl. *port unreachable*
[15] angl. *flag*

- filtrovaný: klientovi nedorazí žádná odpověď nebo chybová zpráva realizovaná ICMP protokolem (typicky může být odpověď serveru filtrována firewallem nebo routerem) a nemůže proto určit zda je port otevřený nebo zavřený, stav portu je proto skenerem určen jako *filtered*.

Po proběhnutí této výměny klient, ze kterého je realizován sken, zašle dle [27] ve všech popsaných případech packet s RST příznakem, proto ani v případě otevřeného portu nedojde k úplnému navázání spojení (sken nezrealizuje poslední krok *three-way hanshake*, tj. odeslání packetu s příznakem ACK). Nedorazí-li žádná odpověď dle [32] skener několikrát opakuje proces, aby vyloučil přenosové chyby, čímž dojde k dramatickému zpomalení skenu.

Naproti tomu dle [27] *úplný TCP sken*[16] se pokouší *three-way hanshake* provést kompletně, ovšem na vyšší úrovni pomocí systémového volání *connect()*. Pokud je tedy port otevřený dojde k navázání spojení, zavřený port je indikován neuskutečněním spojení (tzn. systémové volání je vykonáno s návratovou hodnotou -1). Určení dostupnosti portu probíhá tedy z pohledu odeslaných a přijatých packetů velice podobně jako v předchozím případě, rozdílným momentem je dokončení *three-way hanshake*, při kterém dle [32] typicky dochází k zalogování spojení v systému. Proto pokud je to možné je doporučeno použít SYN sken, k jeho použití musí mít ovšem uživatel potřebná oprávnění pro manipulaci s packety.

ACK sken dle zdroje [31] necílí na určení otevřenosti či uzavřenosti portů, ale soustředí se na zjištění informace, zda jsou porty filtrované či nikoli a je možné pomocí něj určit přítomnost firewallu (popřípadě blíže určit jeho nastavená pravidla). Stejnou informaci potvrzuje i dokumentace [32] nástroje *nmap*. ACK sken zasílá packet s nastaveným ACK příznakem a dokáže z odpovědi serveru určit, je-li port:

- filtrovaný: pokud nedorazí žádná odpověď nebo chybová zpráva protokolu ICMP, stav portu je skenerem určen jako *filtered*,
- nefiltrovaný: v případě, že server odpoví packetem s RST příznakem, stav portu je určen jako *unfiltered*.

Pod pojmem *FIN-like skeny* práce označuje skeny, které fungují na stejném principiálním základu jako FIN sken, jediné v čem se liší je nastavení příznaků v odesílaném packetu. Dokumentace *nmap* [32] píše, že *NULL sken* odesílá packet bez jakýchkoliv nastavených příznaků, *FIN sken* odesílá packet pouze s FIN příznakem a *XMAS sken* pro změnu nastaví packetu hned tři příznaky: FIN, PSH a URG. (Obecně stejného efektu docílí všechny kombinace příznaků, které neobsahují žádný z příznaků SYN, RST nebo ACK). Vyhodnocení stavu portů je pro všechny *FIN-like skeny* totožné, port je vyhodnocen jako:

[16] v anglicky psané literatuře označován jako *full-TCP connection scan* nebo jako *TCP connect scan*

- zavřený: pokud server odpoví packetem s RST příznakem, pak je stav portu vyhodnocen jako *closed*,
- otevřený nebo filtrovaný: v případě, že nedorazí žádná odpověď může být port v jednom z těchto dvou stavů, tedy je vyhodnocen skenerem jako *open|filtered*,
- filtrovaný: skener s jistotou vyhodnotí port jako filtrovaný v případě, že dorazí jako odpověď serveru chybová zpráva ICMP indikující nedosažitelný port, skener tento port označí jako *filtered*.

Zdroj [27] pojmenovává tyto druhy skenů jako tzv. *tajné skeny*[17]. Tyto skeny umožňují dle [31] proniknout některými ochranami, dokumentace *nmap* [32] zmiňuje, že mohou proniknout skrze určité nestavové firewally nebo filtrující routery. Nicméně existuje mnoho moderních IDS produktů (mimo jiné jde i o Cisco zařízení), které je možné nastavit tak, aby *FIN-like* skeny detekovali.

Pro úplnost ještě jednou krátce a uceleně zopakujme fungování *UDP skenu*, ten dle [32] reaguje následovně:

- zavřený: pokud je doručena ICMP chybová zpráva o nedosažitelném portu ze strany serveru, je stav portu vyhodnocen jako *closed*,
- otevřený: pokud ze strany serveru dorazí UDP packet (tj. dojde ke standardní komunikaci ze strany serveru), port je vyhodnocen skenerem jako *open*,
- otevřený nebo filtrovaný: pokud nedorazí žádná odpověď ani po opakovaném zaslání packetu, skener není schopen určit zda je port otevřený nebo filtrovaný a vyhodnotí ho proto jako *open|filtered*.

Dalším podstatným dělením zmiňovaným v literatuře [30], je rozdělení skenů podle Yegneswarana [33], který dělí skeny na *horizontální*, *vertikální*, *koordinované*[18] a *tajné skeny*. Jejich popisy jsou ve zkratce uvedeny v následujícím odstavci.

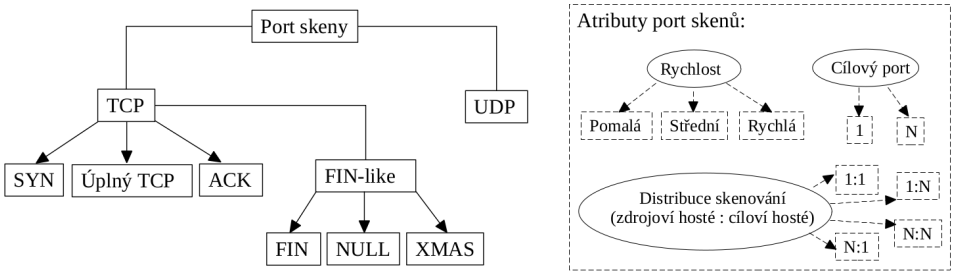
Vertikální skeny jsou uskutečňovány z *jedné* zdrojové IP adresy a směřují na *jednu* cílovou adresu, zaměřují se na *více* cílových portů. Horizontální skeny se realizují z *jedné* zdrojové IP adresy a směřují na *více* cílových IP adres, cílí na *jeden* port. Zdrojem koordinovaných skenů je *více* IP adres, stejně tak je cílem *více* IP adres a *více* cílových portů. Tajné skeny jsou vertikální a horizontální skeny, které se pokouší vyhnout detekci za pomoci změn časového rámce.

Barnett a Irwin [30], na základě Yegneswaranova dělení, vytváří novou taxonomii síťových skenů (viz Příloha C, obrázek C.1), a navíc doplňují původní

[17] angl. *stealth scans*

[18] nazývané také jako *distribuované*

klasifikaci (viz Příloha C, obrázek C.2) o následující atributy[19]: *skenovací rychlost*, *distribuci skenování* a *cílový port*. Na základě toho bylo v rámci práce vytvořeno následující schéma. Toto schéma (obrázek 2.7) rozšiřuje původní vypracovaný přehled základních technik port skenů (obrázek 2.6) o atributy dle taxonomie [30].



Obrázek 2.7: Přehled základních technik port skenů a jejich klasifikace

Atribut *Distribuce skenování* určuje počet IP adres využitých útočníkem ku počtu skenovaných cílových IP adres. Mohou nastat celkem čtyři varianty: 1:1, 1:N, N:1, N:N, kde $N \geq 2$. Přičemž nejčastější dle [30] bývá varianta 1:1 (viz *vertikální skeny*) a 1:N (viz *horizontální skeny*). Vyjímečná je kombinace N:1. Atribut *Rychlost* určuje dle [30] tři základní kategorie, sken může být pomalý, střední a rychlý. Pomalé skeny se složitěji odhalují, tuto rychlost využívají *tajné skeny*. Dále atribut *Cílový port*, v rámci TCP a UDP skenů, určuje dle [30] počet portů, na které je sken cílený. Může jít pouze o jeden cílový port (viz *horizontální skeny*), ale i o větší počet cílových portů (viz *vertikální skeny*). Skeny s distribucí skenování N:1 nebo N:N s N cílovými porty jsou pak výše zmiňované *koordinované skeny*. Atributy ovšem umožňují popsat větší množství kategorií než původní dělení dle Yegneswarana.

Na konec analýzy zasaďme skenování do terminologie uvedené v kapitole 2.1 a shrňme předpoklady pro jeho vykonání. Skenování portů je *aktivní* síťový útok, protože aktivně komunikuje s cílovým systémem, čímž ho ovlivňuje a v některých extrémech může dojít dle [27] dokonce k ovlivnění jeho funkčnosti. Sken portů může být dále klasifikován jako *vnitřní* útok, ale i jako *vnější* útok na síť podle toho, zda se útočící stroj nachází uvnitř sítě nebo zda je za jejím perimetrem. Nutným předpokladem útoku je znalost cílových IP adres (ty je možné zjistit různými způsoby například síťovými skeny jako je *ping sken*, ale je také možné se k informaci o rozsahu IP adres dostat na základě uniklých dat společnosti). A na konec potřebuje mít útočné zařízení k dispozici skenovací softwarový nástroj, tzv. port skener, a dostatečná

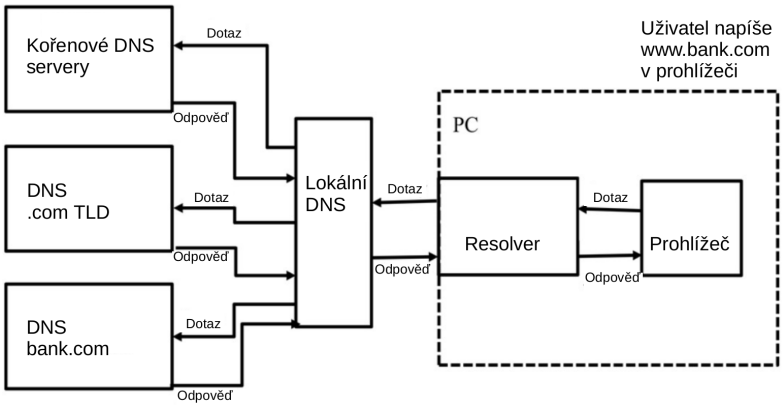
[19]Význam atributů je okomentován pod schématem 2.7.

oprávnění pro jeho použití, tj. pro manipulaci se síťovými packety nebo pro použití sytémových volání.

2.3.2 Otrava mezipaměti DNS

Z průzkumu 2.2 přímo plyne spojitost útoku *otravy mezipaměti DNS*, též známého pod názvem *podvržení DNS*[20], s kategoriemi incidentů *Pharming* a *Malware*. Kategorie malware je přitom hned třetí nejpočetnější kategorie hlášených incidentů v datech národního CERT týmu. Dále poznamenejme, že útok ve vládních datech spadá do kategorie *Škodlivý obsah*, která se v roce 2019 vyskytla v řešených incidentech jako čtvrtá nejpočetnější kategorie, v letech 2017 a 2018 dokonce třetí. Kromě toho podvržení DNS je také možné řadit do kategorie tzv. *spoofing útoků*, které jsou dle průzkumu hojně využívany v kategorii incidentů *Narušení bezpečnosti*, ta se v roce 2019 umístila na třetí pozici. *Otrava mezipaměti DNS* je tedy poměrně komplexně zastoupena v mnoha kategoriích incidentů a dle průzkumu se jedná o častý a stále aktuální útok. Studie [34] z roku 2017 navíc dochází k zjištění, že „...více než 92 % internetových resolvovacích platforem DNS je náchylných k injekci záznamů a mohou být trvale otráveny."[21] (překlad autorky)

Je známo, že na základě DNS[22] protokolu jsme schopni v rámci celosvětové internetové sítě překládat lidsky čitelné alfabeticky zadané doménové adresy na strojově srozumitelné numrické IP adresy. Vzhledem k tomu, že použití DNS protokolu je rozšířené po celém světě, mohou být jeho zranitelnosti kritické. Pro další analýzu útoku je podstatné pochopení DNS, uveďme tedy jeho základní architekturu (viz obrázek 2.8) a popišme ji.



Obrázek 2.8: Architektura DNS systému[45] (překlad autorky)

[20] z angl. *DNS spoofing*

[21] z angl.: „more than 92 percent of the Internet's DNS resolution platforms are vulnerable to records injection and can be persistently poisoned."

[22] z angl. *Domain name system*

Architektura DNS má dle [45], [46] dvě hlavní komponenty: *jmenné servery*[23] (neboli DNS servery) a klientský PC s *resolverem*. Jmenné servery jsou databáze, které mají uložené záznamy. Záznam je překlad z tzv. *hostname* na IP adresu. Resolvery mají roli rozhraní mezi klientem a jmenným serverem. Pokud server nějaký záznam nemá dotáže se resolver lokálního DNS serveru, zda má překlad on. Při úspěchu předá DNS server překlad resolveru, v opačném případě postupuje dále v hledání, dle předepsaného algoritmu (postupuje se hierarchicky). Každý DNS resolver má svojí vlastní *lokální mezipaměť*[24], do které si ukládá nedávno hledané dotazy klienta, pro urychlení dalších dotazů.

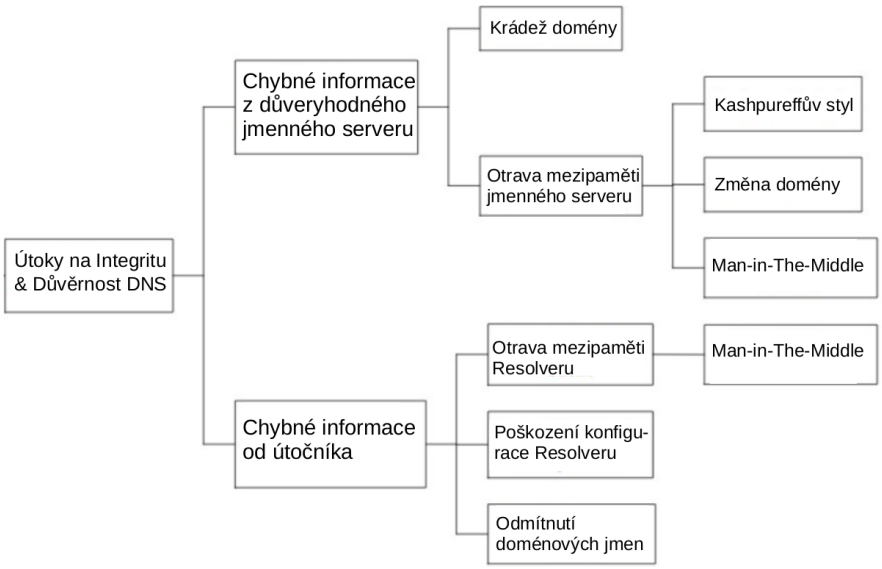
Primárním cílem *otravy mezipaměti DNS* je podat dotazujícímu serveru odpověď s nesprávným překladem *hostname*, tento překladový záznam bude odkazovat na IP adresu útočníka namísto správné IP adresy. Existuje více útočných způsobů, jak toho docílit. Zdroj [34] úvádí k roku 2017 souhrn útoků cílících na *otravu mezipaměti DNS*, jde o následující útoky: [35], [36], [37], [38], [39], [40], [41], [42] a práce doplňuje k tomuto přehledu odkaz na nedávný nový útok [43]. Přičemž jako klasické principy otravy mezipaměti DNS bývají označovány, tzv. *narozeninový útok*[35] a na něm založený *Kaminskyho exploit* [36].

Narozeninový útok se zakládá na neověření identity serverové odpovědi v rámci DNS protokolu. Po dotazu klienta na daný *hostname*, prohledá lokální DNS server své uložené záznamy a mezipaměť. V případě, že pro *hostname* nenajde záznam, zašle dotaz kořenovému serveru, který má uvedený ve své konfiguraci. Poté čeká na odpoveď, po doručení odpovědi se dle [44] ověří následující údaje: zdrojová IP adresa, cílový port, dotazová sekce[25] a ID transakce, tzv. TXID. Žádný z těchto údajů však nezaručuje, že zpráva pochází z kořenového serveru a údaje nebyly podvrženy. Dle [44] je možné všechny údaje kromě TXID odhadnout, a útočník dokáže snadno vytvořit DNS odpověď s odpovídajícími údaji. Co se týče TXID, jde o 16 bitové číslo, má tedy pouze 16 bitů entropie, útočník tedy v průměru potřebuje 2^8 pokusů, aby číslo uhádl. Vygenerovat 2^8 odpovědí (každou s jiným TXID) a zaslat je serveru oběti, je pro útočníka výpočetně zvládnutelný úkol. Zašle tedy tyto odpovědi. Poslední podmínkou úspěšného útoku je podvržení odpovědi lokálnímu serveru dříve než dorazí nepodvržená odpověď původně dotazovaného autoritativního serveru. Povede-li se to, v mezipaměti lokálního serveru se uloží *otrávený* záznam a útok je hotov. Kaminsky tento útok ještě dále rozšiřuje o možnost přinutit resolver oběti o iniciování dotazu na autoritativní server dle útočníkova výbě-ru.

Nyní pomocí schématu (obrázek 2.9) klasifikujme *útoky otravou mezipaměti DNS* v kontextu *Útoků na integritu a důvěrnost DNS*. Uvedené schéma

[23] z angl. *Name servers*
[24] z angl. *local cache*
[25] z angl. *query section*

je výřezem z původní taxonomie dle Chatzise [47], který se zabývá útoky na DNS v obecnější rovině než tato práce. Celá jeho taxonomie je uvedena v příloze D, obrázek D.1.



Obrázek 2.9: Taxonomie útoků na integritu a důvěrnost DNS [47] (překlad autorky)

Z kategorií viditelných ve schématu se analyzovaného útoku týká kategorie *Otrava mezipaměti jmenného serveru* a její podkategorie *Man-in-The-Middle*. Jedná se o kategorii, ve které klient získá chybný DNS záznam přímo od svého důvěryhodného DNS serveru. Vzhledem k hierarchické povaze protokolu DNS, nemusí být nutně otrávena mezipaměť prvního dotazovaného serveru, ale klidně se může jednat o server, který se vyskytne až později v řetězci dotazů.

Ke konci kapitoly ještě uveďme klasifikaci útoku *podvržení DNS* podle terminologie 2.1. Analyzovaný útok je *aktivní*, protože ovlivňuje systém a následně i přesměrovává klientovu komunikaci, pomocí podvrženého záznamu v mezipaměti. Může jít jak o *vnitřní*, tak o *vnější* útok. Záleží na tom, kde v síti se útočník nachází. Pokud je v lokální síti a napadá lokální DNS, jde o *vnitřní útok*, v případě napadení autoritativních serverů lokálního DNS se může jevit jako *vnější útok*. V rámci CIA triády útok zasahuje vlastnost *integritu*, tím že zfalšuje záznam a klient, tak dostává změněnou a neúplnou informaci. Následným přesměrováním na útočníkovi stránky může posléze dojít i k narušení *důvěrnosti*.

2.3.3 DDoS útok

Distribuovaná odmítnutí služby, neboli DDoS útoky, jsou v posledních letech dle průzkumu nejčastějším trendem mířícím na české subjekty spadající do pole působnosti vládního CERT týmu. DDoS se řadí do kategorie incidentů *Dostupnost*, má však také spojitost s kategorií incidentů *Botnet* a *DoS*, ta dle průzkumu také zastává významnou roli na naší národní scéně. Úzká souvislost těchto kategorií je mimo jiné v kapitole 2.3.3 vysvětlena.

Zavěďme potřebné definice, jež jsou odkazovány z glosáře NIST.

Definice 2.3.3 ***Odmítnutí služby**, tzv. **DoS útok**[26], je definován jako „zabránění **autorizovanému** přístupu k systémovým prostředkům nebo zpoždění systémových operací a funkcí.“ [25] (překlad autorky)*

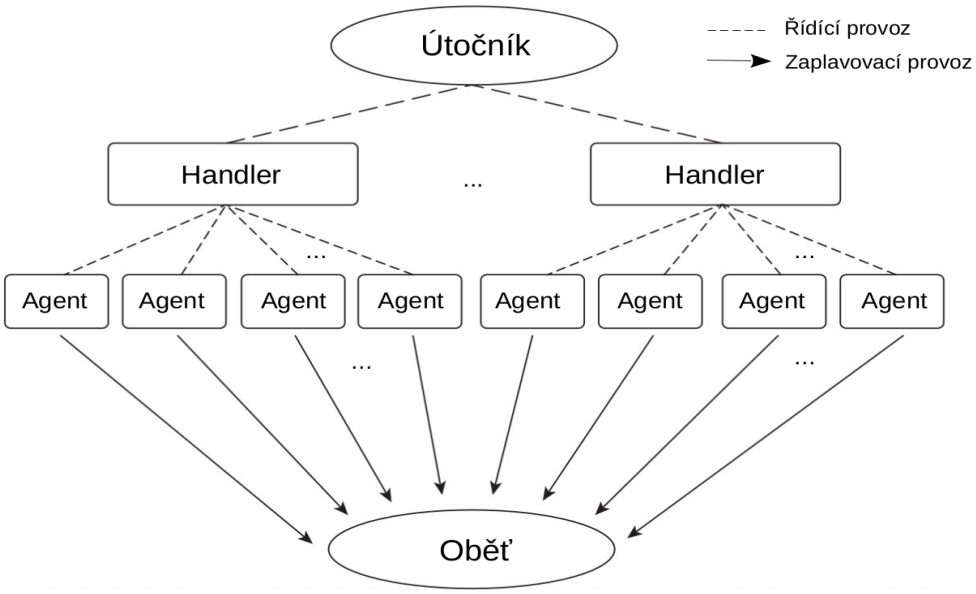
Definice 2.3.4 ***Distribuované odmítnutí služby**, tzv. **DDoS útok**[27], je definován jako „technika DoS útoku, která k útoku využívá velké množství zařízení.“ [48] (překlad autorky)*

Tedy v obou případech útoku, útočník omezuje uživateli přístup na cílový systém. Útoky se liší pouze v multiplicitě útočných strojů. Z toho je evidentní souvislost těchto dvou útoků, a proto DDoS může využívat stejných technik jako DoS útok, akorát tyto metody bude provádět vzdáleně pomocí více zařízení, nad kterými má kontrolu. Zařízení, která útočník ovládá dohromady vytváří tzv. *botnet*, což je síť infikovaných zařízení, která jsou zneužita pro DDoS útok. Kategorie incidentů *Botnet* a *DoS* dle vysvětlení [19] typicky evidují tato infikovaná zařízení. Odtud plyne souvislost DDoS útoků se zmíněnými kategoriemi.

Analyzujme obecnou strategii DDoS útoku, vyjdeme z obrázku 2.10, který zaznamenává stavební prvky celého útoku. V architektuře útoku (obrázek 2.10) je možné vidět čtyři druhy objektů připojených v síti a dva druhy provozu (*řídící* a *zaplavovací*[28]). Význam objektů *útočník* a *oběť* je zřejmý, není nutné je vysvětlovat. Objekt *handler*[29] je dle [50] nakžené zařízení, které je schopné ovládat další napadená zařízení tzv. *agenty*[30] a na příkaz útočníka je řídí při útoku. Agent je taktéž nakažené zařízení, na němž běží speciální program, který na příkaz handler objektu generuje útočná data ve chvíli útoku. Útočník typicky ovládá větší množství handler zařízení, a ta ovládají mnoho agentů. V konečném důsledku jsou agent zařízení vlastně strůjci jednotlivých DoS útoků, ze kterých se DDoS skládá. *Řídící provoz* je pak provoz, kterým se doručují příkazy jednotlivým strojům, ať už mezi útočníkem a handler zařízeními nebo mezi handlery a agenty. *Zaplavovacím provozem* se pak myslí

[26] z angl. *Denial-of-Service*
[27] z angl. *Distributed Denial-of-Service*
[28] z angl. *Flood Traffic*
[29] nazýván také jako *Master*
[30] nazýván také jako *Zombie*

velké množství útočných dat vysílaných na adresu zařízení oběti. Tato architektura mimo jiné umožňuje útočníkovi maskovat svou identitu.



Obrázek 2.10: Architektura DDoS útoku [22], [50] (překlad autorky)

Strategii DDoS útoku je dle [50] možné shrnout do čtyř kroků:

1. Výběr agentů: Aby útočník mohl zařízení zneužít a získat k němu přístup, musí být zařízení zranitelné. Může jít o sowftwarovou zranitelnost nebo např. o zařízení se slabým heslem a možností vzdáleného přístupu, způsobů je mnoho. Také je pro útočníka výhodné soustředit se na zařízení, která mají možnost vygenerovat silný datový tok.

2. Kompromitace: V tomto kroce útočník napadne vybraná zařízení a nainstaluje na ně speciální útočný kód. Kód se musí chovat nenápadně, aby byla, co nejmenší pravděpodobnost, že bude objeven a deaktivován. Speciální program určený pro handler zařízení je schopen řídit mnoho agentů, jejich programy jsou pro změnu specializované na generování objemného proudu dat, který ve chvíli útoku směřují na oběť.

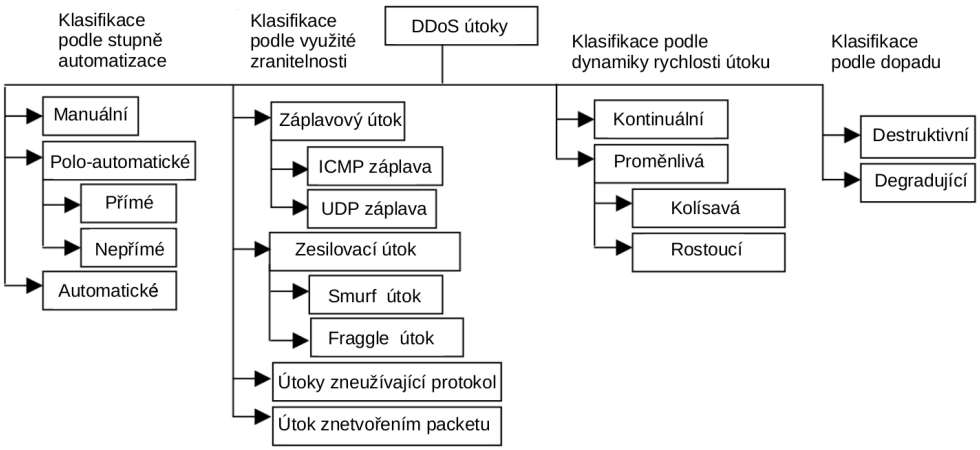
3. Komunikace: Hlavním cílem komunikace je zjištění, kdy jsou handler a agent zařízení aktivní, čímž je možné určit, kdy je optimální útok realizovat. Jak je znázorněno na obrázku 2.10, útočník může komunikovat s větším počtem handler zařízení. Zároveň je každý agent ovládán jedním nebo i více handler objekty, to už záleží na konkrétních realizacích DDoS útoku. Komunikace probíhá pomocí standardních komunikačních protokolů jako je TCP, UDP a ICMP.

4. Útok: Útok je krok, ve kterém vydá útočník příkaz příslušným handler

zařízením, ta zaktivují agenty, kteří útok vykonají. Útočník může při příkazu nastavit různé parametry útoku jako například dobu trvání, cílový port, TTL packetů a další. Vhodné nastavení těchto parametrů může znesnadnit detekci útoku.

První krok je zpočátku prováděn manuálně, později je však možné proces automatizovat a různými skenovacími technikami objevovat další zranitelné stroje, které je možné zneužít. Stejně tak již kompromitované stroje mohou kód tzv. *samo-propagovat*[31] pomocí automatizovaných nástrojů. DDoS útok je mimo jiné možné klasifikovat právě podle stupně automatizace, čímž se dostáváme ke klasifikaci DDoS útoků.

Z díla [49] vyplývá, že DDoS je možné uskutečnit na jakékoli vrstvě, kterou popisuje ISO/OSI model. Je tedy evidentní obrovská komplexnost DDoS útoků a proto není možné v rámci práce popsat veškéré druhy těchto útoků. Práce tedy detailně popisuje základní klasifikaci DDoS útoků a krátce vysvětluje některé jeho druhy. Práce se řídí klasifikací dle Douligerise a Mitrokotsaové [50] (obrázek 2.11). Je vhodné zmínit, že hojně citována je i klasifikace dle Mirkovicové a Reihera [51] pro úplnost je i jimi představená klasifikace DDoS útoku přiložena v závěru dokumentu (Příloha E, obrázek E.1).



Obrázek 2.11: Klasifikace DDoS útoků [50] (překlad autorky)

Ve schématu můžeme [51] pozorovat čtyři kategorie, podle nichž se DDoS útoky klasifikují. Schéma má dvě úrovně, v první úrovni jsou útoky klasifikovány podle stupně automatizace, využité zranitelnosti, dynamiky rychlosti a dle dopadu. Druhá úroveň reprezentuje charakteristické rozdělení podkategorií první úrovně.

Podle *stupně automatizace* klasifikujeme distribuované útoky na *manuální*, *polo-automatické* a na *automatické*. Plně manuální útoky jsou nyní spíše his-

[31] z angl. *self-propagation*

torií. Kroky jako vzdálené skenování, exploitace zranitelnosti a instalace škodlivého kódu byly brzy automatizovány pomocí skriptů, které využívají poloautomatické a automatické DDoS útoky ke kompromitaci handler a agent zařízení. Typ útoku, adresa oběti a počátek útoku musí být v případě poloautomatických útoků specifikované útočníkem na handler zařízeních. Podkategorie polo-automatických útoků se dále dělí na útoky s *přímou* a *nepřímou* komunikací, v případě přímé komunikace musí agent a handler zařízení znát svou vzájemnou identitu, aby stroje mohly komunikovat. To je veliká nevýhoda, protože odhalením jednoho stroje je možné odhalit celý *botnet*. Útoky s nepřímou komunikací přesměrovávají svou komunikaci tak, aby bylo toto odhalení těžší. *Automatické* DDoS útoky mají naproti tomu veškeré informace potřebné k útoku předprogramované v již nainstalovaném kódu handler a agent strojů, a tím se snižuje riziko odhalení identity útočníka.

Podle *využité zranitelnosti*[32] rozlišujeme DDoS využívající *záplavové útoky*[33], *zesilovací*[34], *útoky zneužívající protokol*[35] a *útoky znetvořující packety*[36]. Záplavové útoky fungují na principu zasílání velkého objemu dat, čímž vytíží šířku pásma[37] sítě oběti. Typickými příklady útoku je UDP záplava[38] nebo ICMP záplava[39]. Zesilovací útoky pro změnu zneužívají vlastností síťových zařízení k zasílání *broadcast* zpráv, čímž zahltí systém oběti. Známými zesilujícími útoky jsou například *Smurf útok*, který používá k odrazu ICMP dotazů DNS servery jako zesílující reflektory, a *Fraggle útok*, ten je téměř stejný jako *Smurf útok*. Liší se v tom, že namísto ICMP protokolu používá k zasílání zpráv transportní protokol UDP a může způsobit větší škody. Nakonec zmiňme poslední dvě podkategorie: Zaprvé *útoky zneužívající protokol*, ty typicky cílí na nějakou zranitelnou vlastnost implementace protokolu. Známým příkladem je SYN záplava, která cílí na implementaci *three-way-handshake* TCP protokolu, při otevření spojení SYN packetem se na straně oběti v momentě přijetí packetu a odeslání odpovědi v podobě ACK/SYN packetu alokuje malé množství paměti. Útočník tedy při otevření velkého množství spojení pomocí SYN packetů vyčerpá zdroje systému. A za druhé *Útoky znetvořením packetu*, ty pro změnu pozmění nekorektně IP packet a odešlou ho oběti, což může mít za následek pád systému oběti.

Podle *dynamiky rychlosti útoku* dělíme DDoS útoky na tzv. *Kontinuální* a *Proměnlivé*. Kontinuální útoky mají v průběhu času útoku stále konstantní sílu, působí od začátku maximální silou a jejich účinek je velice rychlý. Útoky s proměnlivou rychlostí v čase mění sílu útoku, ta může buďto postupně

[32] z angl. *exploited vulnerability*
[33] z angl. *Flood attacks*
[34] z angl. *Amplification attacks*
[35] z angl. *Protocol Exploit attacks*
[36] z angl. *Malformed Packet attacks*
[37] angl. *bandwidth*
[38] z angl. *UDP flood*
[39] z angl. *ICMP flood*

růst a tak vyčerpat zdroje oběti, nebo může být *kolísavá* a doléhat na oběť ve vlnách. Změny rychlosti útoku se využívají k prodloužení času detekce nebo k vyhnutí se detekci na základě úpravy síly útoku podle aktivity oběti.

A nakonec schéma 2.11 uvádí klasifikaci podle *dopadu*, která obsahuje dvě podkategorie. *Destruktivní* podkategorie cílí na kompletní odepření přístupu ke službě autorizovaným klientům. Kdežto *degradující* útok pouze vytíží velkou část prostředků oběti, čímž samozřejmě dojde k velkým škodám na straně oběti, které jsou umocněny dlouhou dobou detekce útoku, jenž je pro útok typická.

Kvůli těsné souvislosti DoS a DDoS útoků krátce nastiňme klasifikaci DoS útoků. DoS útok je dle [50] možné klasifikovat v pěti kategoriích na útoky na *úrovni síťových zařízení*, *úrovni operačního systému* nebo na *aplikační úrovni*, další kategorie jsou útoky založené na principu *datové záplavy*[40] a *útoky na vlastnosti protokolu*. První kategorie využívá chyby a zranitelnosti síťových zařízení nebo cílí na vyčerpání zdrojů síťového hardware. Druhá a třetí kategorie mají jasný význam, cílí na chyby a zranitelnosti operačního systému nebo aplikací. Čtvrtá kategorie funguje na principu zasílání obrovského objemu dat, čímž oběť zahltí. Patá kategorie dle zdroje využívá standardních vlastností různých protokolů. Uvádí se také, že v několika typech útoků z paté kategoie se cílí přímo na DNS, přičemž mnoho těchto typů útočí konkrétně na mezipaměť DNS.

Na závěr analýzy opět shrňme DDoS útoky v kontextu terminologie kapitoly 2.1 a uvěďme stručně jeho předpoklady. Z předchozího textu naprosto evidentně vyplývá, že distribuované DoS útoky jsou *aktivní útoky*. Útočí na síť typicky *zvnějšku*, jedná se tedy standardně o *vnější útoky*, technicky je však možné uskutečnit je i uvnitř sítě jako tzv. *vnitřní útoky*. Pro vznik útoku bývá potřebné exploitovat větší počet zařízení, které jsou následně zneužity k DoS útoku. Základním předpokladem je tedy vytvoření *botnetu*, tj. síť zranitelných (a v důsledku toho kompromitovaných) zařízení. Napadení těchto zařízení z logiky věci předchází skenování těchto strojů kvůli nalezení jejich zranitelností. Co se týče vlastností CIA triády, je v rámci útoku napadena především vlastnost *dostupnost*, nicméně v rámci kompromitace zařízení dochází nepochybně i k narušení *důvěrnosti* systému a nakonec v rámci některých typů útoku (např. DDoS pomocí zesílení skrze DNS) je útokem narušena i *intergrita* informací v systému.

[40] z angl. *data flood*

Kapitola 3

Mitigace

3.1 Technologická terminologie

Základními bezpečnostními síťovými prvky, které je potřeba v rámci práce představit, jsou *Firewall*, *Systém detekce průniku (IDS)* a *Systém prevence průniku* (*IPS*)[41]. Zaveďme tedy jejich definice.

Definice 3.1.1 ***Firewall*** *je „mezisíťová brána, která omezuje přenos datové komunikace* ***do*** *a* ***z*** *jedné z připojených sítí (o této síti se říká, že je tzv. „uvnitř“ brány firewall), čímž chrání systémové zdroje této sítě před hrozbami z druhé připojené sítě (tedy té, o které se říká, že je tzv. „venku“ za bránou firewall).“ [6] (překlad autorky)*

Neboli firewall je vlastně ochraný štít firemní sítě, který umí filtrovat příchozí i odchozí komunikaci, čímž chrání před nepovoleným provozem mezi vnější a vnitřní sítí. Na firewallu je možné nastavit různá pravidla, která povolí nebo zakáží provoz dle potřeb společnosti, těmto pravidlům se říká ACLs[42].

Dále institut NIST definuje:

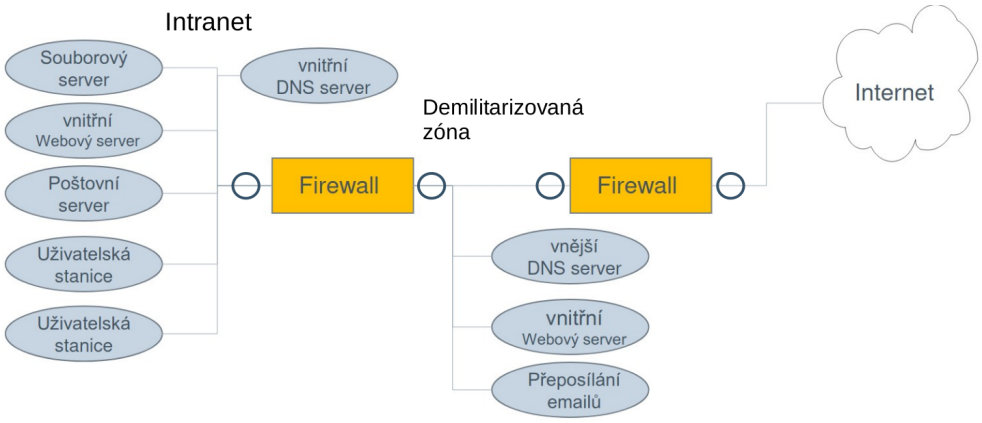
Definice 3.1.2 ***Systém detekce průniku****, neboli* ***IDS***[43]*, je „softwarová aplikace, kterou lze implementovat na hostujících operačních systémech nebo jako síťová zařízení k monitorování aktivity spojené s průnikem do systému nebo jeho zneužitím.“ [53] (překlad autorky)*

Definice 3.1.3 ***Systém prevence průniku***[44]*, neboli* ***IPS***[45]*, je „software, který má všechny funkce systému detekce průniku a může se navíc pokusit zastavit možné incidenty.“ [54] (překlad autorky)*

[41] také nazýván jako *Systém detekce a prevence průniku*, neboli IDPS
[42] z angl. *Access Control Lists*
[43] z angl. *Intrusion detecton system*
[44] také nazýván jako *Systém detekce a prevence průniku*, neboli IDPS
[45] z angl. *Intrusion prevention system*

Z definic je evidentní překryv systémů detekce a prevence, IPS tedy může zastoupit IDS. Tyto systémy je možné realizovat jako samostatná síťová zařízení, ale je také možné použít jejich aplikační řešení. Podle toho zdroj [55] dělí IDS na tzv. *network-based* a *host-based*, zkráceně NIDS a HIDS. Přičemž NIDS využívá k prohledávání datového toku síťovou kartu v promiskuitním módu, typicky se provoz zrcadlí pomocí span portu přepínače[46], aby IDS nestál v cestě provozu. Naproti tomu HIDS je čistě sowftwarové řešení a narozdíl od NIDS se typicky umisťuje na více hostů v síti namísto, aby bylo umístěno jen na pár klíčových místech sítě (jak je to u NIDS). Systém IPS funguje velice podobně jako NIDS, s tím rozdílem, že může aktivně zasahovat do provozu a blokovat ho. IPS systémy rovněž fungují velice podobně jako firewall až na to, že se řídí při filtrování provozu pomocí shody s tzv. signaturami, kdežto firewall běžně blokuje provoz na základě IP adres a portů. Dle [52] může IPS také provoz blokovat tak, že zašle pokyn firewallu, který vygeneruje nebo aktivuje potřebné pravidlo na základě instrukcí.

Ukažme, kde v síti je NIDS a IPS možné umístit. V obrázku 3.1 je znázorněna architektura běžné firemní sítě [52], tmavomodrými kolečky jsou pak vyznačena možná umístění NIDS nebo IPS systémů na základě informací z díla [55].



Obrázek 3.1: Běžná architektura firemní sítě [52]

Konkrétní umístění IDS/IPS systémů záleží na individuálních potřebách každé firmy, typicky se rozhoduje podle toho, které části sítě jsou pro společnost nejcennější, a nebo podle toho, jak vysoká je pravděpodobnost útoku na ně.

Nakonec krátce zmiňme *DNSSEC*, neboli *bezpečnostní rozšíření DNS*[47]. Toto rozšíření umožňuje dle [70] využití asymetrické kryptografie pro autenti-

[46] angl. *switch*
[47] angl. *DNS security extension*

fikaci komunikace v rámci DNS protokolu, čímž pomáhá tento letitý protokol zabezpečit. Příkladný proces jeho nastavení je uveden v podkapitole 3.1.2.

3.1.1 Cisco technologie

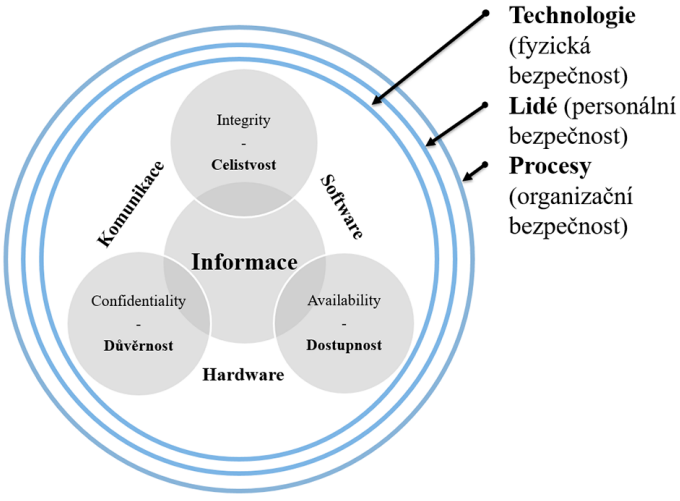
Nyní představme konkrétní nabízená Cisco řešení pro malé a středně velké podniky. Dle [67] se jako řešení nabízí:

- Cisco ASA[48]
- Cisco ASA s FirePOWER
- FTD (FirePower Threat Defense)
- FMC (FirePOWER Management Center)

Samostatné ASA zařízení, tj. bez Firepower modulu (první bod), je firewall. Zbylá tři řešení (druhý až čtvrtý bod) mohou vystupovat, jak v roli firewallu, tak jako IDS a IPS. Veškeré konfigurační příručky k těmto technologiím jsou dostupné ze zdroje [68].

3.2 Metody a procesy mitigace útoků

Obrázek 3.2 navazuje na úvodní obrázek 2.1 a rozšiřuje ho o modré bezpečnostní prstence: Technologie, Lidé a Procesy.



Obrázek 3.2: Vrstvy zabezpečení [1]

[48] z angl. *Adaptive Security Appliance*

V této kapitole (v podkapitolách 3.2.1, 3.2.2 a 3.2.3) si představíme konkrétní metody a procesy mitigace předešlých analyzovaných síťových útoků. Popíšeme tedy pouze technologickou vrstvu zabezpečení. Nicméně bez-pečnou síť není možné vytvořit jen pomocí technologií, obrázek 3.2 se snaží decentně zdůraznit, že bezpečnost systému je možné zajistit pouze ve vrstvách, žádná vrstva není dokonalá a pouze jejich kombinací docílíme dobrých výsledků.

Co se týče rozebírané vrstvy technologií, i zde je vhodné využívat pravidlo zabezpečení na více úrovních. Selže-li jedna technologie, může útok zachytit technologie druhá. Ačkoli práce popisuje především síťové bezpečnostní síťové prvky jako je firewall, IDS a IPS, existují i další bezpečnostní technologie a postupy. Může jít o různá antivirová řešení, SIEM[49], SDN[50]. Rovněž klíčovou roli v bezpečnosti sítě hraje vhodně navržená topologie, či segmentace sítě. Také se technologie dají různě kombinovat. Popis všech těchto postupů ovšem není reálné v textu práce pojmout.

3.2.1 Skenování portů

Fesl [52] ve své přednášce uvádí jako účinné metody obrany proti skenování portů použití technologií firewall, IDS a IPS. Přičemž zmiňuje obecné pravidlo pro správce firewallů: „Povol to nejnutnější a zbytek zakaž."

To z pohledu portů znamená, že je potřeba zakázat veškeré služby, které nejsou potřebné. To je možné realizovat na firewall zařízeních (pomocí ACLs), ale i pomocí IPS systémů (případně i pomocí IDS, které zašle zprávu administrátorovi, který nastaví pravidlo na firewallu manuálně). Tím, že budeme provoz filtrovat, snížíme množství informací, ke kterým bude mít útočník přístup nebo úplně zablokujeme útočníkovu komunikaci při pokusu o průnik do interní sítě.

První technologií, jejíž procesy detekce a mitigace rozebereme je:

- Cisco ASA

ASA je firewallové řešení společnosti Cisco. Popíšeme dle [22] proces základního nastavení zařízení a princip nastavení bezpečnostních politik a přístupových pravidel, kterými se dá provoz blokovat. V závěru vysvětlíme princip ACLs. Vyjasníme, jak se vše vztahuje ke skenování portů.

Základní nastavení ASA firewallu je při nasazení nutné provést pomocí příkazové řádky, neboli CLI. Podrobný návod je vložen v příloze F (obrázek F.1, F.2). Tento návod ukazuje, jak aktivovat možnost přihlášení pomocí grafického rozhraní ASDM[51]. Dál ukazuje, jak nastavit zařízení, z něhož bude připojení povolené a nakonec předvádí, jak na firewallu vytvořit uživatele s administrátorskými právy. Po nastavení potřebných bezpečnostních levelů[52] (viz

[49] Security Information and Event Management
[50] Software-defined networking
[51] z angl. *Adaptive Security Device Manager*
[52] z angl. *security levels*

příloha F, obrázek F.3) pomocí, kterých Cisco ASA kontroluje připojení mezi jednotlivými rozhraními zařízení, je možné se pod vytvrořeným uživatelem přihlásit do ASDM.

Nyní je možné nastavovat v grafickém ASDM *bezpečnostní politiky* (příloha F, obrázek F.4), které se konfigurují pomocí přístupových pravidel[53]. Defaultní nastavení rozhraní povoluje provoz z vyšších bezpečnostních levelů do nižších, provoz z nižš-ích levelů do vyšších zakazuje. Navíc je ve výchozím nastavení také zakázán provoz mezi dvěma rozhraními na stejném levelu. V rámci bezpečnostních politik a pravidel je navíc možné vytvářet pomocné *objektové skupiny*[54] (příloha F, obrázek F.5), které se využívají při nastavování přístupových pravidel. Objekty reprezentují: *sítě*, *individiuální hosty*, *skupiny služeb* nebo *zdroje*[55]. Použití objektu v pravidle je rovněž v obrázku F.5.

Politiky se dají také vytvářet pomocí tzv. *class map* (ty využívají ACLs), *policy map* a *servisních politik*[56] v MPF[57]. V příloze je vložen příkladný postup (příloha F obrázek F.6) použití všech těchto komponet implementujích politiky v MPF.

V rámci popisu procesů první technologie zmiňme princip ACLs [69]. ACLs jsou pravidla, která filtrují IP packety na základě: zdrojové adresy, cílové adresy, typu packetu (a jakékoli kombinace těchto možností). Na IP packet se tedy aplikuje sada tzv. `permit` a `deny` podmínek. Na základě toho firewall (případně router), buďto IP packet blokuje nebo ho směruje dál na místo určení. Podmínky se vyhodncují skvenčně a jamkile se najde první shoda, proces vyhodnocování těchto podmínek končí a postupuje se podle této shody. Jinými slovy pokud bychom na začátku podmínek vložili příkaz: `deny any any`, zablokujeme veškerý provoz a jakékoli další podmínky se nevyhodnotí. Návod na konfiguraci [69] běžně používaných IP ACLs je k nahlédnutí ve zmíněném zdroji, který rozebírá nastavení typů ACL: *standard* a *extended*. Doktor Moucha [56] také zmiňuje *reflexivní* ACL, které na základě komunikace z vnitřku sítě povolují vnější komunikaci na portech, na které je odpovídáno pouze v reakci na komunikaci iniciovanou zevnitř sítě. O reflexivních a dalších typech ACL je možné se dočíst více například zde [57].

Další funkcionalitou ASA je dle [59] tzv. *detekce hrozeb*[58], ačkoli se sice nejedná o plnohodnotnou náhradu IDS/IPS, jde o další bezpečnostní vrstvu, která může administrátorovi pomoci detekovat hrozby. Tuto funkcionalitu se hodí využít v prostředích, kde není IDS/IPS řešení dostupné (dle konfigurační příručky [60] mohou být však aplikovány i obě dvě tyto ochrany najednou).

[53] z angl. *access rules*
[54] angl. *object groups*
[55] angl. *Resources*
[56] angl. *service policies*
[57] z angl. *Modular Policy Framework*
[58] angl. *Threat detection*

A nakonec má ASA firewallu je možnost připojit tzv. IPS module. Příklad tohoto propojení a jeho konfugurace je k nalezení v [58]. Díky připojení tohoto modulu je možné realizovat detekční a preventivní opatření a blokovat, na základě zjištění IPS, provoz vyhodnocený jako nebezpečný.

Tím se dostáváme k samotným IPS systémům. Jak již bylo zmíněno v podkapitole 3.1.1, tyto systémy jsou implementovány následujícími Cisco technologiemi: ASA s FirePOWER, FTD nebo FMC. Pro procesní ukázku byl v rámci práce zvolen FMC [61] jako zástupce těchto IPS systémů, popišme si tedy tuto technologii.

- FMC (FirePOWER Management Center)

Nebudeme se nyní již zabývat základním nastavením, to je možné najít v aktuálních příručkách [62], [63]. Okomentujme postup nastavení detekce port skenů (viz příloha G, obrázek G.1) dle příručky [64], ve kterém je ukázána aktivace detekce skenování portů. V rámci nastavení je na výběr z detekce TCP nebo UDP skenů. Dál je možné specifikovat konkrétní podtypy těchto skenů. Cisco eviduje následující kategorie: „*Portscan Detection*“, „*Port Sweep*“, „*Decoy Portscan*“ a „*Distributed Portscan*“. Tyto podtypy skenů pokrývají členění analyzované v kapitole 2.3.1, jejich detailní popis je v příručce. Dál je potřeba nastavit úroveň citlivosti, tzv. „*Sensitivity level*“, na výběr jsou tři úrovně: „*Low*“, „*Medium*“ a „*High*“, volíme dle potřeb společnosti. Je také zvolit vybraná zařízení, kterých se detekce bude týkat, případně nastavit, kterých zařízeních se detekce dotýkat nemá.

Shrňme tedy v čem spočívá mitigace port skenů pomocí zmíněných technologií. Dle [56] jsou možnosti ochrany následující: je-li port sken z jedné zdrojové IP adresy a kontroluje dostupnost portů predikovatelným způsobem, je možné blokovat přístup této adresy na úrovni firewallu pomocí ACLs; jsou-li skeny sofistikovanější (distribuované z více zdrojových IP adres a kontrolují dostupnost portů pseudonáhodně) je řešením blokovat veškeré nevyužívané porty a navíc použít reflexivní ACLs.

Na závěr zmiňme, že je důležité dle [67] dát si pozor na to, aby prevenční systémy v síti nemohly být útočníky zneužity k DoS útokům. To je myšleno v tom smyslu, že útočník umí podvrhnout zdrojovou IP adresu v packetu a tudíž by mohl předstírat skenovací útok z adresy, které by chtěl zamezit přístup ke službám. (Toto pravdilo platí nejen pro skenování portů, ale i pro mitigaci DDoS útoků, která je svým způsobem podobné povahy jako port sken.) Z těchto důvodů bylo v rámci mitigace představeno pouze detekční řešení na IPS systému, tak aby výsledná rozhodnutí o blokaci potenciálně škodlivého provozu byla v režii administrátora a nebyla zneužita k dalšímu útoku.

3.2.2 Otrava mezipaměti DNS

Zdroje [8], [56], [65], [66] (a další) se jednoznačně shodují, že učinnou ochranou metodou proti *otravě mezipaměti DNS* je správně nakonfigurovaný DNSSEC. Problémem při konfiguraci mohou být například slabé vygenerované klíče na základě nedostatečně silného zdroje náhodných dat s vysokou entropií.

DNSSEC je [70] založený na principu řetězce důvěry, který mezi sebou jednotlivé DNS servery vybudují pomocí vygenerování asymetrických klíčů, jimiž následně zabezpečují komunikaci. V případě lokálního servru je tedy postup následující: DNS server vygeneruje pro svou zónu dostatečně silný soukromý a veřejný klíč, veřejný klíč publikuje pomocí autoritativního serveru a soukromým klíčem pak podepíše své technické údaje, které DNS při komunikaci zasílá spolu s odpovědí nebo dotazem. Příjemce si pak může technické informace dešifrovat pomocí veřejného klíče a tím ověří identitu DNS serveru. Obdobný proces nastavení probíhá i u autoritatívního serveru, který provede stejnou výměnu se svým nadřazeným serverem a tak to pokračuje dále až ke kořenovým serverům. Tím je vytvořen potřebný řetězec důvěry.

Popišme v následujících odstavcích dle [71] proces vygenerování klíčů DNS zóny a umístění veřejného klíče do nadřazené zóny. Ilustrativní příklad nastavení DNSSEC je proveden na serveru BIND verze 9.9, prakticky půjde o nastavení na Debian Jessie s nainstalovaným balíčkem `bind9`. BIND sever v příkladu slouží jako autorativní server pro doménu `example.com`, konfigurační soubor `/etc/bind/named.conf.local` s definicí zóny vypadá tedy následovně:

```
zone "example.com" {
    type master;
    file "/etc/bind/example.com";
};
```

První krok našeho nastavení je kontrola zdroje entropie. V našem případě nástroje využívají pro generování náhodných čísel `/dev/random`, ten v případě nedostatečné entropie blokuje generování náhodných dat. Pomocí následujícího příkazu můžeme zkontrolovat objem vyráběných náhodných dat:

```
pv -nb /dev/random > /dev/null
```

Vypisuje-li se po zadání příkazu stále stejná hodnota, jedná se o signál nedostatečné entropie a zdroj entropie je nutné upravit. To je možné provést například instalací démon procesu *haveged*, takto: `apt-get install haveged`. Tento démon navýší entropii nástroje `/dev/random` a ten začne generovat data. Opakováním předešlého příkazu `pv` si můžeme ověřit, že objem vygenerovaných dat se každou vteřinou navyšuje. O dalších dostupných zdrojích entropie a jejich kvalitě je možné se dočíst například v práci [72].

Provedeme d*ruhý krok*, v terminálu vygenerujeme klíče pro podpis a ověření původu dat a povolíme serveru BIND práva, tak aby je mohl upravovat a číst.

```
# mkdir /etc/bind/keys
# cd /etc/bind/keys
# dnssec-keygen -a ECDSAP256SHA256 -fK example.com
Generating key pair.
Kexample.com.+013+32462
# chmod g+r K*.private
```

V tomto příkladě je využitý šifrovací algoritmus založený na použití eliptických křivek, tedy `ECDSA P-256`, v kombinaci s hashovací funkcí `SHA256`, který je v rámci DNSSEC podporován. Tato šifra je dle aktuálního RFC 8624 [73], založeného na doporučení dle autority IANA, silná a její použití je v pořádku. Vygenerované klíče jsou uloženy v adresáři`/etc/bind/keys`.

Ve třetím kroce je nutné aktivovat možnost tzv. *inline podepisování*. Předtím je potřeba vytvořit symbolický odkaz na zónový soubor, ve kterém bude mít BIND právo zápisu, takto: `ln -s /etc/bind/example.com /var/cache/bind`

Inline podepisování v konfiguračním souboru zóny aktivujeme následovně:

```
zone "example.com" {
    type master;
    file "example.com";
    inline-signing yes;
    auto-dnssec maintain;
    key-directory "/etc/bind/keys";
};
```

Po zadání příkazu `rndc reload` se během chvíle provede podpis zóny.

Posledním krokem je předání veřejného klíče nadřazenému serveru. To je v tomto konkrétním případě provedeno příkzem:

```
# dnssec-dsfromkey /etc/bind/keys/Kexample.com.+013+32462
```

Více detailních informací a možností nastavení je v aktuální příručce [74] DNSSEC pro nejpoužívanější serverové DNS řešení BIND 9.

3.2.3 DDoS útok

Detekce a mitigace DDoS útoků je dle [51], [50], [56], [67] velice náročný problém, s nímž se potýkájí sítě po celém světě. Z podstaty účelu a vlastností

samotného Internetu, je umožněna ohromná síla útoku a zároveň jeho dobré maskování. Díky technikám jako je *podvržení IP adresy*[59] nebo přesměrování provozu, je tak opravdová identita útočníka těžko dohledatelná. Protože DDoS je natolik komplexní útok, je reálné ho v některých podobách detekovat a účinně řešit, nicméně existují jeho formy, které zkrátka řešit nelze a pouze dochází k přesouvání problému (směrem co nejblíže k útočníkovi). Takovým útokem může být například DDoS mířený na vyčerpání šířky pásma, ta bude mít v lepších případech přenosovou rychlost 1 Gb/s, útočník je ovšem schopný vygenerovat řádově Tb/s a tím pásmo úplně zahltit. Kromě takových útoků však existují i DDoS útoky zneužívající například konkrétní zranitelnosti a nastavení systému. Mitigace takových útoků je možná, ale je hodně specifická pro různé případy útoků. Z důvodu této komplexnosti a variability útoku si v této podkapitole popíšeme pouze metody mitigace DDoS útoků, procesní řešení jsou v tomto případě příliš závislá na konkrétních útocích, individuálních potřebách sítě a na síťové topologii.

Douligeris a Mitrokotsa ve své práci [50] klasifikují metody obrany vůči DDoS útokům a uvádí způsoby prevence útoku ještě před jeho vznikem. Tyto metody jsou: *využívání globálně koordinovaných filtrů, deaktivace nepoužívaných služeb*[60]*, aplikování bezpeč-nostních záplat, deaktivace IP broadcastů, vyvažování zátěže*[61] nebo využití tzv. *honeypotů*, které slouží jako návnada pro útočníka. Dále dílo zmiňuje existenci detekčních metod, založených na *detekci anomálií* v systému nebo na *detekci zneužití*[62] systému. Celá klasifikace je přiložena v příloze H (obrázek H.1). Zajímavou kategorií, kterou práce mimo jiné zmiňuje je mitigace DDoS útoku pomocí tzv. *odolnosti proti chybám*[63], to znamená, že síť je vystavena natolik robustně, že při přetížení jednoho spojení, může zprostředkovat přístup klientům skrze duplicitní síťové propojení. Síť se může takto duplikovat na úrovni hardwaru, softwaru i systému. Z podstaty věci jde ovšem o poměrně nákladné řešení, tato strategie se tedy používá pro nejkritičtější síťové infrastruktury. Příkladem využití této metody v České republice je realizace projektu Fénix, který dle [17] sdružuje sítě poskytovatelů síťového připojení, neboli ISP, a dalších provozovatelů. V případě přetížení některého z uzlů sítě projektu Fénix je provoz přesměrován na ostatní přípojky, čímž se zachová dostupnost významných služeb.

Navažme na poslední uvedenou metodu přednáškou doktora Fesla [52]. Ten ve svých slidech uvádí IPS systémy jako účinnou ochranu proti DDoS útokům. Tyto systémy mohou mitigovat nejen útoky na konkrétní stanice, ale i útoky na zmiňovanou šířku pásma. Základem realizace tohoto řešení při útoku na síť zákazníka, je komunikace s poskytovatelem (ISP). Zákazníkova bezpečnostní zařízení po detekci útoku cíleného na určitou IP adresu ve vnitřní síti, zašlou

[59] angl. *IP address spoofing*
[60] viz popis možností nastavení ACLs v kapitole 3.2.1
[61] angl. *Load Balancing*
[62] angl. Misuse detection
[63] angl. *Fault tolerance*

síťovému zařízení poskytovatele informaci o útoku pomocí BGP FlowSpec protokolu. Poskytovatel na základě této zprávy na hranicích své sítě zablokuje provoz směřovaný na atakovanou IP adresu. Tím se tedy vnitřní síť uchrání od útoku, nicméně je problém svým způsobem přesunut na poskytovatele. Měl-li by útočník dostatečně velkou výpočetní sílu, mohl by ochromit i poskytovatele. Na konec zmiňme, že v rámci mitigace útoků na šířku pásma na úrovni firmy, je dle [67] podstatné neblokovat pomocí IPS systémů provoz před tzv. úzkým hrdlem, které se nachází mezi perimetrem firemní sítě a hraničním směrovačem poskytovatele, pomocí nejž je firma spojena s jeho sítí. Tento požadavek Feslovo řešení splňuje, protože deleguje problém až za zmíněné úzké hrdlo. Řešení dle Feslových přednášek je tedy možné považovat za účinné.

Závěr

Práce se zabývala nejčastějšími síťovými útoky na území České republiky, jejich analýzou a popisem jejich mitigace. Cílem bylo vytvořit komplexní analýzu těchto útoků a zdokumentovat metody a procesy jejich mitigace. Práce se skládá ze tří logických celků: průzkum výskytu, analýza a mitigace útoků. Průzkum útoků se zaměřuje na evidenci útoků v ČR. V této části došla práce k závěru, že evidence útoků v prostředí ČR není vedena, proto vyšla z evidence bezpečnostních incidentů českého národního a vládního CERT týmu. Interpretací dat získaných v průzkumu, došlo k výběru tří síťových útoků: skenování portů, otrava mezipaměti DNS a DDoS útok. Tyto útoky byly v další části práce zanalyzovány, analýza se soustředila na detailní popis principu útoků a na představení klasifikace útoků. Zároveň byly útoky v rámci analýzy zasazeny do kontextu bezpečnostních incidentů. V poslední části práce jsou představeny bezpeč-nostní technologie firewall, IDS, IPS, práce také uvádí konkrétní Cisco technologie: ASA, ASA s FirePOWER, FTD (FirePOWER Threat Defense) a FMC (FirePOWER Management Center). Metody mitigace jsou úspěšně představeny pro všechny útoky. Následuje popis procesů mitigacace pro útoky: skenování portů a otrava mezipaměti DNS. V rámci DDoS útoku procesy nejsou zdokumentovány, protože jsou příliš specifické pro konkrétní situace a firemní sítě. Proces mitgace skenování portů je ilustrován pomocí technologií ASA (tj. firewall) a FMC (tj. IDS a IPS systém). Práce přikládá (příloha F,G) dohledané postupy nastavení těchto technologií, postupy ve svém textu řádně komentuje. V souvislosti s ASA firewallem jsou rovněž detailně vysvětleny postupy nastavení pravidel pomocí tzv. ACLs. Dalším dokumentovaným procesem v rámci mitigace otravy mezipaměti DNS je nastavení podpisu zóny a napojení lokálního DNS do řetězce důvěry za použití protokolu DNSSEC, proces je předveden na implementaci DNS serveru BIND.

Literatura

[1] KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity* [online]. Praha: CZ.NIC, z.s.p.o., 2019 [cit. 2021-04-08]. CZ.NIC. ISBN 978-80-88168-34-8. Dostupné z: `https://knihy.nic.cz/files/edice/cybersecurity.pdf`

[2] INTERNATIONAL TELECOMMUNICATION UNION. *ITU-T Recommendations: Security architecture for Open Systems Interconnection for CCITT applications* [online]. 1991-03-22. Ženeva, 1991 [cit. 2021-02-23]. Dostupné z: `https://www.itu.int/ITU-T/recommendations/rec.aspx?id=3102`

[3] LÓRENCZ, Róbert. Bezpečnost: 12. Informační bezpečnost [přednáška]. In: *courses. fit.cvut.cz* [online]. Praha: Katedra informačních bezpečnosti, ČVUT v Praze, 2020. [cit. 2021-02-23]. Dostupné z: `https://courses.fit.cvut.cz/BI-BEZ/media/lectures/bez12.pdf`

[4] Computer network attack (CNA). In: *CNSSI, Committee on National Security Systems (CNSS) Glossary* [online]. Committee on National Security Systems, No. 4009, 2015. [cit. 2021-04-09]. Dostupné z: `https://www.cnss.gov/CNSS/issuances/Instructions.cfm`

[5] MOUCHA, Alexandru, vedoucí práce, zaměstnanec Fakulty informačních technologií, ČVUT v Praze [telefonický rozhovor]. 2021-03-12.

[6] SHIREY, R. *RFC 4949 - Internet Security Glossary, Version 2* [online]. The IETF Trust, 2007 [cit. 2021-02-23]. Dostupné z: `https://www.rfc-editor.org/rfc/rfc4949.txt` 10.17487/RFC4949

[7] SIKORA, Vojtěch, zaměstnanec NÚKIB. *Re: FIT ČVUT - dotaz ke statistickým datům* [elektronická pošta]. Message to: blanksta@fit.cvut.cz. 2021-03-24 9:36 [cit. 2021-04-16].

[8] CALETKA, Ondřej. Smutné DNS: nový způsob otrávení keše umožňuje podvrhnout údaje. *Root.cz: Bezpečnost* [online]. ROOT.CZ, 2020 [cit.

2021-5-4]. Dostupné z: https://www.root.cz/clanky/smutne-dns-novy-zpusob-otraveni-kese-umoznuje-podvrhnout-udaje/

[9] *O týmu CSIRT.CZ* [online]. Národní CSIRT České republiky [cit. 2021-4-25]. Dostupné z: https://csirt.cz/cs/o-nas/https://csirt.cz/cs/o-nas/

[10] *Spolupráce: Bezpečnostní týmy v České republice* [online]. Národní CSIRT České republiky [cit. 2021-4-25]. Dostupné z: https://csirt.cz/cs/o-nas/spoluprace/

[11] SIKORA, Vojtěch, zaměstnanec NÚKIB [videohovor]. 2021-04-21.

[12] CZ.NIC. *Zpráva o činnosti CSIRT.CZ (národního CSIRT ČR) za rok 2020* [online]. Praha: CZ.NIC, z.s.p.o., 2021 [cit. 2021-04-23]. Dostupné z: https://www.csirt.cz/media/filer_public/c1/64/c1642df8-32f0-4976-9062-ac259f7a43b4/210304_csirt_vyrocni_zprava_2020.pdf

[13] CZ.NIC. *Zpráva o činnosti CSIRT.CZ (národního CSIRT ČR) za rok 2019* [online]. Praha: CZ.NIC, z.s.p.o., 2020 [cit. 2021-04-23]. Dostupné z: https://www.csirt.cz/media/filer_public/b7/74/b7745b25-45e0-4a13-92ff-154f784662e8/csirt_zprava_2019.pdf

[14] CZ.NIC. *Zpráva o činnosti CSIRT.CZ (národního CSIRT ČR) za rok 2018* [online]. Praha: CZ.NIC, z.s.p.o., 2019 [cit. 2021-04-23]. Dostupné z: https://www.csirt.cz/media/filer_public/4e/dc/4edc3bff-5750-4527-82dc-3f155f578158/csirt_zprava_2018.pdf

[15] CZ.NIC. *Zpráva o činnosti CSIRT.CZ (národního CSIRT ČR) za rok 2017* [online]. Praha: CZ.NIC, z.s.p.o., 2018 [cit. 2021-04-23]. Dostupné z: https://www.csirt.cz/media/filer_public/4b/4d/4b4da98a-d851-44fe-bdef-6d7759b59ea6/csirt_zprava_2017.pdf

[16] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, P.O. *Zpráva o stavu kybernetické bezpečnosti za rok 2019* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, P.O., 2020 [cit. 2021-04-23]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/NUKIB_ZSKB_2019.pdf

[17] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, P.O. *Zpráva o stavu kybernetické bezpečnosti za rok 2018* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, P.O., 2019 [cit. 2021-04-23]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2018-cz.pdf

[18] NÁRODNÍ ÚŘAD PRO KYBERNETICKOU A INFORMAČNÍ BEZPEČNOST, P.O. *Zpráva o stavu kybernetické bezpečnosti za rok 2017* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, P.O., 2018 [cit. 2021-04-23]. Dostupné z: https://www.nukib.cz/download/publikace/zpravy_o_stavu/zprava-o-stavu-kyberneticke-bezpecnosti-cr-2017.pdf

[19] *Typy řešených incidentů* [online]. Národní CSIRT České republiky [cit. 2021-4-25]. Dostupné z: https://www.csirt.cz/cs/typy-resenych-incidentu/

[20] ENISA. *Reference Incident Classification Taxonomy: Starting Point – ecsirt.net taxonomy* [online]. [cit. 2021-4-25]. Dostupné z: https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy

[21] SIKORA, Vojtěch, zaměstnanec NÚKIB. *Re: FIT ČVUT - dotaz ke statistickým datům* [elektronická pošta]. Message to: blanksta@fit.cvut.cz. 2021-04-21 20:00 [cit. 2021-04-25].

[22] MCMILLAN, Troy. *CCNA security study guide: exam 210-260* [online]. 2nd ed. Indianapolis, Indiana: Sybex, 2018 [cit. 2021-04-08]. ISBN 978-1-119-40993-9. Dostupné z: https://ebookcentral.proquest.com/lib/cvut/detail.action?docID=5215616

[23] ALEF DISTRIBUTION CZ, S.R.O. *SECURITY report 2021* [online]. Praha: ALEF Distribution CZ, 2021 [cit. 2021-5-4]. Dostupné z: https://www.alef.com/alefnula/content/mediagallery/alef_system/file/article/file/2134.pdf

[24] ALEF DISTRIBUTION CZ, S.R.O. *SECURITY report 2020* [online]. Praha: ALEF Distribution CZ, 2020 [cit. 2021-5-4]. Dostupné z: https://www.alef.com/alefnula/content/mediagallery/alef_system/file/article/file/2059.pdf

[25] STOUFFER, Keith, Victoria PILLITTERI, Suzanne LIGHTMAN, Marshall ABRAMS a Adam HAHN. *NIST Special Publication 800-82: Guide to industrial control systems (ICS) security* [online]. Rev. 2. Gaithersburg: National Institute of Standards and Technology, 2015, s.B-11 [cit. 2021-4-30]. Dostupné z doi: http://dx.doi.org/10.6028/NIST.SP.800-82r2

[26] SCARFONE, Karen, Murugiah SOUPPAYA, Amanda CODY a Angela OREBAUGH. *Recommendations of the National Institute of Standards and Technology: Technical Guide to Information Security Testing and Assessment* [online]. Gaithersburg: National Institute of Standards and Technology, 2008, s.F-2 [cit. 2021-4-30]. Dostupné z: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-115.pdf

[27] DE VIVO, Marco, Eddy CARRASCO, Germinal ISERN a Gabriela O. DE VIVO. A review of port scanning techniques. *SIGCOMM Comput. Commun.* [online]. New York, NY, USA: Association for Computing Machinery, 1999, Rev. 29(2), 41–48 [cit. 2021-5-3]. ISSN 0146-4833. Dostupné z doi: https://doi.org/10.1145/505733.505737

[28] GHIETTE, V., N. BLENN a C. DOERR. Remote Identification of Port Scan Toolchains. In: *2016 8th IFIP International Conference on New Technologies, Mobility and Security (NTMS)* [online]. Larnaca, Cyprus: IEEE, 2016, 1-5 [cit. 2021-05-03]. ISSN 2157-4960. ISBN: 978-1-5090-2914-3. Dostupné doi: https://doi.org/10.1109/NTMS.2016.7792471

[29] HUSSEIN, Majed, Hassan N. NOURA, Ola SALMAN, Ali CHEHAB a Raphaël COUTURIER. Efficient and Secure Statistical Port Scan Detection Scheme. In: *International Conference on Mobile, Secure, and Programmable Networking* [online]. Cham: Springer, 2020, s. 72-88 [cit. 2021-5-3]. ISBN 978-3-030-67550-9. Dostupné z doi: https://doi.org/10.1007/978-3-030-67550-9_6

[30] BARNETT, Richard J a Barry IRWIN. Towards a taxonomy of network scanning techniques. In: *The 2008 annual research conference of the South African Institute of Computer Scientists and Information Technologists on IT research in developing countries: riding the wave of technology (SAICSIT '08)* [online]. New York, NY, USA: Association for Computing Machinery, 2008 [cit. 2021-05-03]. Dostupné z doi: https://doi.org/10.1145/1456659.1456660

[31] ANANIN, E. V., A. V. NIKISHOVA a I. S. KOZHEVNIKOVA. Port scanning detection based on anomalies. In: *2017 Dynamics of Systems, Mechanisms and Machines (Dynamics)* [online]. Omsk: IEEE, 2017 [cit. 2021-05-04]. ISBN 978-1-5386-1820-2. Dostupné z doi: https://doi.org/10.1109/Dynamics.2017.8239427

[32] NMAP(1) Nmap Reference Guide. *Linux man pages: Section 1* [online]. 2020 [cit. 2021-05-05]. Dostupné z: https://man7.org/linux/man-pages/man1/nmap.1.html

[33] YEGNESWARAN, Vinod, Paul BARFORD a Johannes ULLRICH. Internet intrusions: global characteristics and prevalence. In: *Proceedings of the 2003 ACM SIGMETRICS international conference on Measurement and modeling of computer systems (SIGMETRICS '03)* [online]. New York, NY, USA: ssociation for Computing Machinery, 2003, s. 138–147 [cit. 2021-5-5]. Dostupné z doi: https://doi.org/10.1145/781027.781045

[34] KLEIN, Amit, Shulman HAYA a Waidner MICHAEL. Internet-wide study of DNS cache injections. In: *IEEE INFOCOM 2017 - IEEE Conference on Computer Communications* [online]. Atlanta, GA, USA: IEEE,

2017, s. 1-9 [cit. 2021-05-09]. ISBN 978-1-5090-5336-0. Dostupné z doi: https://doi.org/10.1109/INFOCOM.2017.8057202

[35] STEWART, Joe. *DNS cache poisoning-the next generation* [online]. 2003 [cit. 2021-05-10]. Dostupné z: https://www.thefengs.com/wuchang/courses/old_courses/cs510netsec_fall2005/summaries/10.pdf

[36] KAMINSKY, Dan. In: *Black ops 2008* [online]. Black Hat USA, 2008 [cit. 2021-5-10]. Dostupné z: http://kurser.lobner.dk/dDist/DMK_BO2K8.pdf

[37] HERZBERG, Amir a Haya SHULMAN. Security of Patched DNS. In: *Foresti S., Yung M., Martinelli F. (eds) Computer Security – ESORICS 2012. ESORICS 2012* [online]. Springer, Berlin, Heidelberg, 2012, s. 271-288 [cit. 2021-5-10]. ISBN 978-3-642-33167-1. Dostupné z doi: https://doi.org/10.1007/978-3-642-33167-1_16

[38] SHULMAN, Haya a Michael WAIDNER. Towards Security of Internet Naming Infrastructure. In: *Pernul G., Y A Ryan P., Weippl E. (eds) Computer Security – ESORICS 2015. ESORICS 2015* [online]. Cham: Springer, 2015, s. 3-22 [cit. 2021-5-10]. ISBN 978-3-319-24174-6. Dostupné z doi: https://doi.org/10.1007/978-3-319-24174-6_1

[39] SHULMAN, Haya a Michael WAIDNER. Fragmentation considered leaking: port inference for dns poisoning. In: *Boureanu I., Owesarski P., Vaudenay S. (eds) Applied Cryptography and Network Security. ACNS 2014.* [online]. Cham: Springer, 2014, s. 531-548 [cit. 2021-5-10]. ISBN 978-3-319-07536-5. Dostupné z doi: https://doi.org/10.1007/978-3-319-07536-5_31

[40] HERZBERG, Amir a Haya SHULMAN. Vulnerable delegation of DNS resolution. In: *Crampton J., Jajodia S., Mayes K. (eds) Computer Security – ESORICS 2013. ESORICS 2013* [online]. Berlin, Heidelberg: Springer, 2013 [cit. 2021-5-10]. ISBN 978-3-642-40203-6. Dostupné z doi: https://doi.org/10.1007/978-3-642-40203-6_13

[41] HERZBERG, Amir a Haya SHULMAN. Socket overloading for fun and cache-poisoning. In: *Proceedings of the 29th Annual Computer Security Applications Conference (ACSAC '13)* [online]. New York, NY, USA: Association for Computing Machinery, 2013, s. 189–198 [cit. 2021-5-10]. ISBN 9781450320153. Dostupné z doi: https://doi.org/10.1145/2523649.2523662

[42] HERZBERG, Amir a Haya SHULMAN. Fragmentation considered poisonous, or: One-domain-to-rule-them-all. org. In: *2013 IEEE Conference on Communications and Network Security (CNS)* [online]. National Harbor, MD, USA: IEEE, s. 224-232 [cit. 2021-5-10]. ISBN 978-1-4799-0895-0. Dostupné z doi: https://doi.org/10.1109/CNS.2013.6682711

[43] KEYU, Man, Zhiyun QIAN, Xiaofeng ZHENG, Youjun HUANG a Haixin DUAN. DNS Cache Poisoning Attack Reloaded: Revolutions with Side Channels. In: *Proceedings of the 2020 ACM SIGSAC Conference on Computer and Communications Security (CCS '20)* [online]. New York, NY, USA: Association for Computing Machinery, 2020, s. 1337–1350 [cit. 2021-05-09]. Dostupné z doi: https://doi.org/10.1145/3372297.3417280

[44] SON, Sooel a Vitaly SHMATIKOV. The hitchhiker's guide to DNS cache poisoning. In: *Jajodia S., Zhou J. (eds) Security and Privacy in Communication Networks. SecureComm 2010* [online]. Berlin, Heidelberg: Springer, 2010, s. 466-483 [cit. 2021-5-10]. ISBN 978-3-642-16161-2. Dostupné z doi: https://doi.org/10.1007/978-3-642-16161-2_27

[45] DISSANAYAKE, I. M. M. DNS Cache Poisoning: A Review on its Technique and Countermeasures. In: *2018 National Information Technology Conference (NITC)* [online]. Colombo, Sri Lanka: IEEE, 2018, s. 1-6 [cit. 2021-05-09]. ISBN 978-1-5386-9136-6. ISSN 2279-3895. Dostupné z doi: https://doi.org/10.1109/NITC.2018.8550085

[46] AGARWAL, S., S. PRAMANICK, N. BHANDARI a G. USHA. A Case Study Solution to DNS Cache Poisoning Attacks. *(IJARBEST) International Journal of Advanced Research in Basic Engineering Sciences and Technology* [online]. 2017, vol.3(36) [cit. 2021-05-09].Dostupné z: https://www.ijarbest.com/conference/spcl36/1205

[47] CHATZIS, Nikolaos. Motivation for Behaviour-Based DNS Security: A Taxonomy of DNS-Related Internet Threats. In: *The International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007)* [online]. Valencia, Spain: IEEE, 2007, s. 36-41 [cit. 2021-05-09]. Dostupné z doi: https://doi.org/10.1109/SECUREWARE.2007.4385307

[48] REGENSCHEID, Andrew R. a Geoff BEIER. *NISTIR 7711: Security Best Practices for the Electronic Transmission of Election Materials for UOCAVA Voters* [online]. Gaithersburg: National Institute of Standards and Technology, 2011, s.67 [cit. 2021-05-05]. Dostupné z: https://doi.org/10.6028/NIST.IR.7711

[49] NAGESH, K., R. SUMATHY, P. DEVAKUMAR a K. SATHIYAMURTHY. A Survey on Denial of Service Attacks and Preclusions. In: *Proceedings of the International Conference on Informatics and Analytics (ICIA-16)* [online]. New York, NY, USA: Association for Computing Machinery, 2016, Article 118, 1–10 [cit. 2021-05-07]. Dostupné z doi: https://doi.org/10.1145/2980258.2982110

[50] DOULIGERIS, Christos a Aikaterini MITROKOTSA. DDoS attacks and defense mechanisms: classification and state-of-the-art. *Computer Networks*

[online]. Issue 5. 2004, (44), 643-666 [cit. 2021-05-07]. ISSN 1389-1286. Dostupné z doi: https://doi.org/10.1016/j.comnet.2003.10.003

[51] MIRKOVIC, Jelena a Peter REIHER. A Taxonomy of DDoS Attack and DDoS Defense Mechanisms2004. *SIGCOMM Comput. Commun.* [online]. New York, NY, USA: Association for Computing Machinery, 2004, duben 2005, Rev. 34(2) [cit. 2021-05-08]. ISSN 0146-4833. Dostupné z doi: https://doi.org/10.1145/997150.997156

[52] FESL, Jan. Počítačové sítě: Přednáška č. 8 - Bezpečnost v počítačových sítích [přednáška]. In: *courses. fit.cvut.cz* [online]. Praha: Katedra počítačových systémů, ČVUT v Praze, 2020. [cit. 2021-05-05]. Dostupné z: https://courses.fit.cvut.cz/BI-PSI/media/lectures/P_8.pdf

[53] GRANCE, Tim, Joan HASH, Steven PECK, Jonathan SMITH a Karen KOROW-DIKS. *Security Guide for Interconnecting Information Technology Systems: Recommendations of the National Institute of Standards and Technology* [online]. Gaithersburg: National Institute of Standards and Technology, 2002, s.D-2 [cit. 2021-05-05]. Dostupné z doi: https://doi.org/10.6028/NIST.SP.800-47

[54] SCARFONE, Karen a Peter MELL. *Guide to Intrusion Detection and Prevention Systems (IDPS): Recommendations of the National Institute of Standards and Technology* [online]. Gaithersburg: National Institute of Standards and Technology, 2007, s.A-2 [cit. 2021-05-05]. Dostupné z doi: https://doi.org/10.6028/NIST.SP.800-94

[55] BROTHERSTON, Lee a Amanda BERLIN. *Defensive Security Handbook: Best Practices for Securing Infrastructure*. Sebastopol: O'Reilly Media, 2017, s. 215-223. ISBN 9781491960387.

[56] MOUCHA, Alexandru, vedoucí práce, zaměstnanec Fakulty informačních technologií, ČVUT v Praze *Re: BP - dotaz na technologie* [elektronická pošta]. Message to: blanksta@fit.cvut.cz. 2021-05-06 4:49 PM [cit. 2021-05-11].

[57] *Configuring IP Access Lists: Reflexive ACLs* [online]. Cisco Systems, Inc., 2007 [cit. 2021-5-12]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/security/ios-firewall/23602-confaccesslists.html#reflexacl

[58] *Cisco ASA IPS Module Quick Start Guide* [online]. Cisco Systems, Inc., 2012 [cit. 2021-5-12]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/security/asa/quick_start/ips/ips_qsg.html#wp38566

[59] *ASA Threat Detection Functionality and Configuration* [online]. Cisco Systems, Inc., 2015 [cit. 2021-5-12]. Dostupné z: https://

www.cisco.com/c/en/us/support/docs/security/asa-5500-x-series-next-generation-firewalls/113685-asa-threat-detection.html

[60] *CLI Book 2: Cisco ASA Series Firewall CLI Configuration Guide, 9.6: Detecting Threats* [online]. Cisco Systems, Inc., 2020 [cit. 2021-5-12]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/security/asa/asa96/configuration/firewall/asa-96-firewall-config/conns-threat.html#ID-2132-00000007

[61] *Configuration Guides: Firepower Management Center (for ASA with Firepower Services and Firepower Threat Defense)* [online]. Cisco Systems, Inc. [cit. 2021-5-12]. Dostupné z: https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html#anchor807

[62] *Firepower Management Center Configuration Guide, Version 6.7: Classic Device Management Basics* [online]. Cisco Systems, Inc., 2021 [cit. 2021-5-12]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/classic_device_management_basics.html

[63] *Firepower Management Center Configuration Guide, Version 6.7: IPS Device Deployments and Configuration* [online]. Cisco Systems, Inc., 2021 [cit. 2021-5-12]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/ips_device_deployments_and_configuration.html

[64] *Firepower Management Center Configuration Guide, Version 6.7: Detecting Specific Threats: Portscan Detection* [online]. Cisco Systems, Inc., 2021 [cit. 2021-5-12]. Dostupné z: https://www.cisco.com/c/en/us/td/docs/security/firepower/670/configuration/guide/fpmc-config-guide-v67/detecting_specific_threats.html#ID-2236-000000a6

[65] DOSTÁL, Jiří, Alexandru MOUCHA. Síťová a systémová bezpečnost: Počítačové sítě [přednáška]. In: *courses. fit.cvut.cz* [online]. Praha: Katedra informační bezpečnosti, ČVUT v Praze, 2020. [cit. 2021-05-11]. Dostupné z: https://courses.fit.cvut.cz/BI-SSB/media/lectures/new/BI-SSB_03_Pocitacove_site.pdf

[66] STEINHOFF, U., A. WIESMAIER a R. ARAÚJO. The state of the art in DNS spoofing. In: *Proc. 4th Intl. Conf. Applied Cryptography and Network Security (ACNS)* [online]. Germany, 2006 [cit. 2021-5-11]. Dostupné z: https://www.wiesmaier.de/publications/reviewed/200606_ACNS06_The_State_of_the_Art_in_DNS_Spoofing.pdf

[67] MOUCHA, Alexandru, vedoucí práce, zaměstnanec Fakulty informačních technologií, ČVUT v Praze [telefonický rozhovor]. 2021-05-10.

[68] *Configuration Guides* [online]. Cisco Systems, Inc. [cit. 2021-5-12]. Dostupné z: https://www.cisco.com/c/en/us/support/security/asa-firepower-services/products-installation-and-configuration-guides-list.html#_top

[69] *Configure Commonly Used IP ACLs* [online]. Cisco Systems, Inc., 2020 [cit. 2021-5-12]. Dostupné z: https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html

[70] *Jak funguje DNSSEC* [online]. CZ.NIC, Z. S. P. O. Praha: CZ.NIC, z.s.p.o., 2008 [cit. 2021-5-11]. Dostupné z: https://www.nic.cz/page/444/jak-funguje-dnssec/

[71] CALETKA, Ondřej. DNSSEC s BIND 9.9 snadno a rychle. *Root.cz: Bezpečnost* [online]. ROOT.CZ, 2016 [cit. 2021-05-11]. Dostupné z: https://www.root.cz/clanky/dnssec-s-bind-9-9-snadno-a-rychle/

[72] FARKAS, Marek. *Dostupné zdroje entropie a jejich kvalita v systémech Linux a Windows* [online]. Pardubice, 2014. Univerzita Pardubice, Fakulta elektrotechniky a informatiky. Dostupné z: https://dk.upce.cz/handle/10195/60838

[73] WOUTERS, P. a O. SURY. *RFC 8624: Algorithm Implementation Requirements and Usage Guidance for DNSSEC, June 2019* [online]. [cit. 2021-5-12]. ISSN 2070-1721. Dostupné z doi: https://doi.org/10.17487/RFC8624

[74] *DNSSEC Guide* [online]. Internet Systems Consortium, Inc., 2021 [cit. 2021-5-12]. Dostupné z: https://bind9.readthedocs.io/en/latest/dnssec-guide.html

Příloha **A**

Seznam použitých zkratek

CERT z angl. *Computer Emergency Response Team*

CIA z angl. *Confidentiality, Inegrity, Availability*

ČSÚ Český statistický úřad

ČVÚT České vysoké učení technické v Praze

DDoS z angl. *Distributed Denial-of-Service*

DoS z angl. *Denial-of-Service*

ISP z angl. *Internet service provider*

NIST National Institute of Standards and Technology

NÚKIB Národní úřad pro kybernetickou a informační bezpečnost

TCP z angl. *Transmission Control Protocol*

TTL z angl. *Time to live*

UDP z angl. *User Datagram Protocol*

Příloha B

Data k vypracovaným grafům

Obr. 2.2 - Evidované bezpečnostní incidenty (národní CERT):

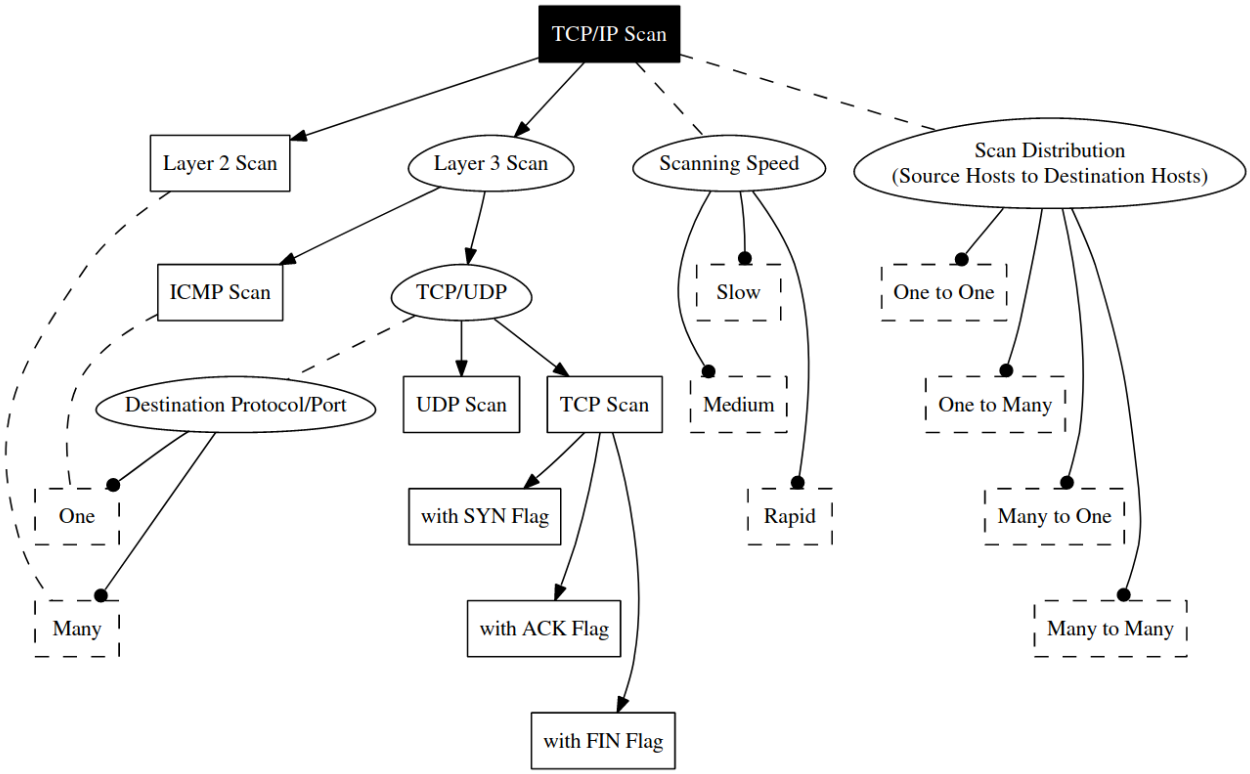
Ev. kategorie incidentu	Počet v roce 2017	Počet v roce 2018	Počet v roce 2019	Počet v roce 2020
Phishing	409	518	483	738
Spam	121	144	128	216
Malware	99	135	85	109
Probe	26	171	141	68
DoS	14	7	16	16
Portscan	13	16	3	29
Botnet	29	20	4	2
Trojan	94	0	0	0
Virus	0	0	0	0
Other	200	58	85	86

Obr. 2.3 - Evidované bezpečnostní incidenty (vládní CERT):

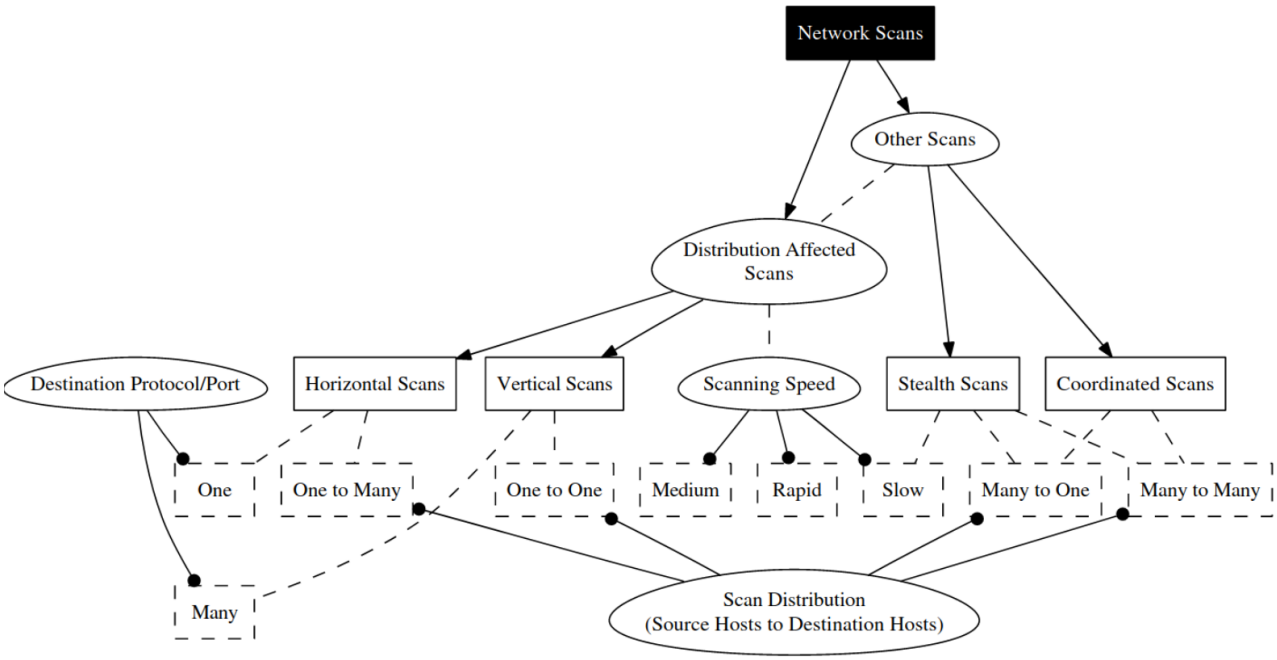
Ev. kategorie incidentu	Počet v roce 2017	Počet v roce 2018	Počet v roce 2019	Počet v roce 2020
Dostupnost	19	$17.82 \doteq 18$	$25.74 \doteq 26$	-
Podvod	11	$14.04 \doteq 14$	$14.82 \doteq 15$	-
Narušení bezpečnosti	1	$4.86 \doteq 5$	$13.26 \doteq 13$	-
Škodlivý obsah	8	$9.18 \doteq 9$	$11.7 \doteq 12$	-
Průnik	2	$2.7 \doteq 3$	$6.24 \doteq 6$	-
Pokus o průnik	2	$1.08 \doteq 1$	$3.12 \doteq 3$	-
Sběr informací	4	$2.16 \doteq 2$	$2.34 \doteq 2$	-
Urážlivý obsah	3	$1.08 \doteq 1$	$0.78 \doteq 1$	-

Příloha C

Taxonomie technik síťového skenování dle Barnetta a Irwina



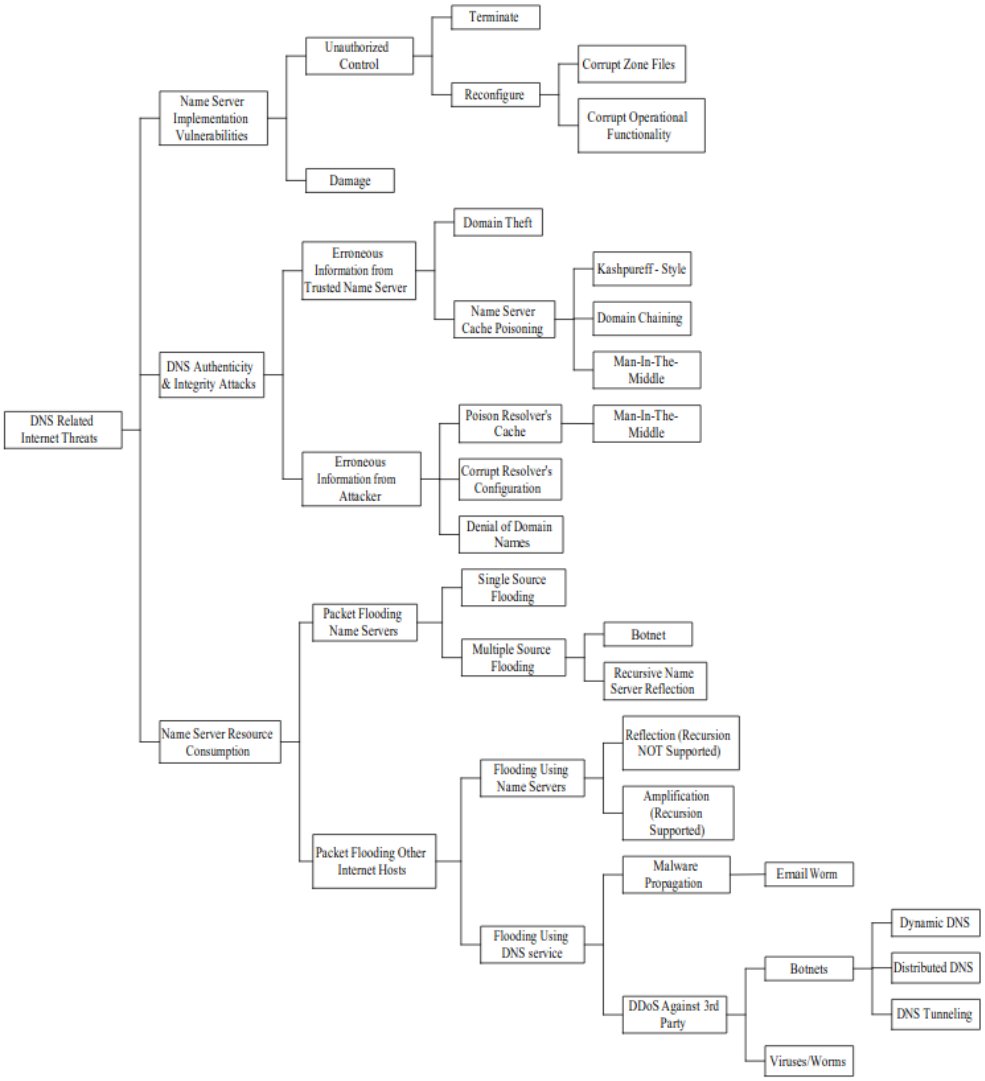
Obrázek C.1: Taxonomie technik síťového skenování [30] (překlad autorky)



Obrázek C.2: Původní členění [33] doplněné o atributy [30] (překlad autorky)

Příloha D

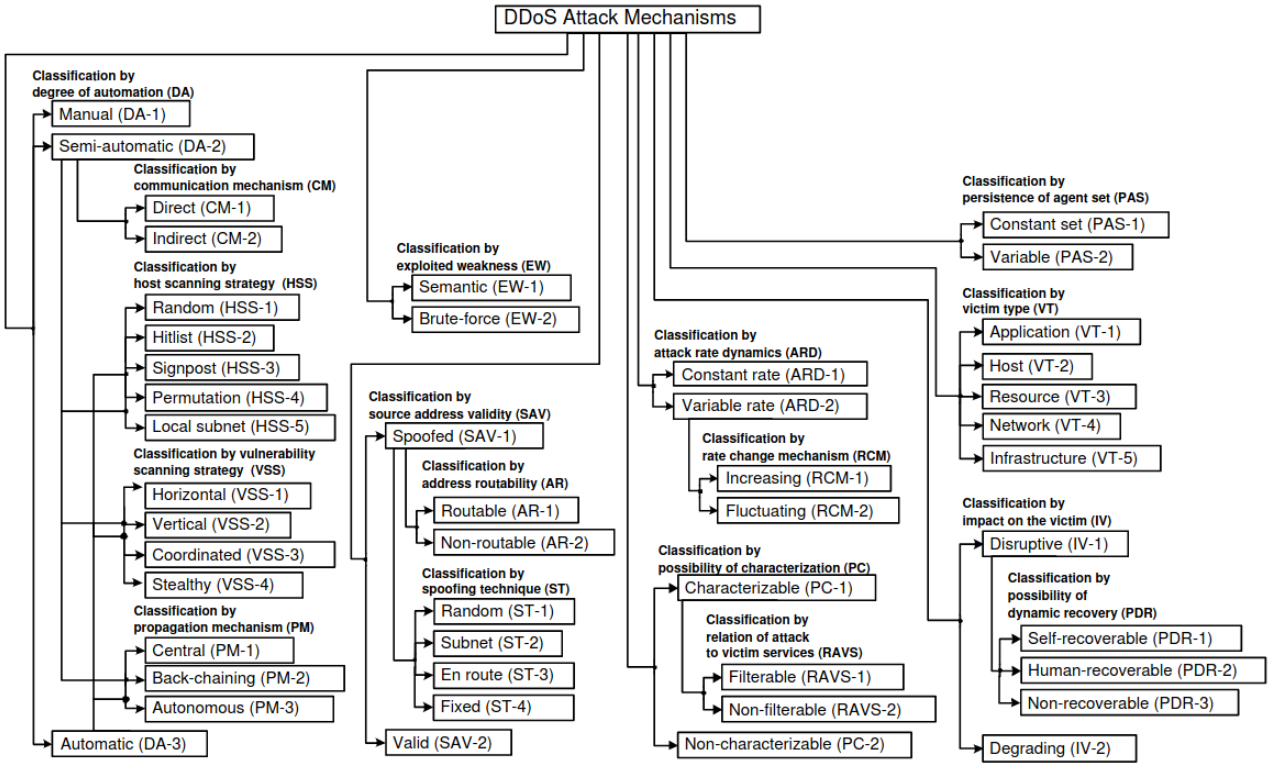
Taxonomie Internetových hrozeb souvisejících s DNS dle Chatzise



Obrázek D.1: Taxonomie Internetových hrozeb souvisejících s DNS [47] (překlad autorky)

Příloha E

Taxonomie mechanismů DDoS útoku dle Mirkovicové a Reithera



Obrázek E.1: Taxonomie mechanismů DDoS útoku [51] (překlad autorky)

Příloha F

Procesy základní bezpečnostní konfigurace Cisco ASA firewallu

Initial Configuration of the ASA

In this procedure, you will configure the interfaces of the ASA with IP addresses, subnet masks, and security levels. Finally, you will enable those interfaces.

1. Connect to the ASA using a console cable.
2. Enter interface configuration mode for the external (Internet facing) interface.

```
asa70(config)#int Gi0/1
asa70(config-if)#
```

3. Configure an IP address and subnet mask for the interface.

```
asa70(config-if)#ip address 201.16.5.5 255.255.255.0
```

4. Give the interface a name. In this case, name it *outside*.

```
asa70(config-if)#nameif outside
```

5. Enable the interface.

```
asa70(config-if)#no shutdown
```

6. Using the same commands configure and enable two other interfaces, naming the interface leading to the DMZ as *dmz* and the interface leading to the private network (the LAN) *inside*.

```
asa70(config)#int gi0/2
asa70(configif)#ip address 172.168.5.5 255.255.255.0
asa70(configif)#nameif dmz
asa70(configif)#no shutdown
asa70(config)#int gi0/3
```

Obrázek F.1: Počáteční konfigurace ASA (kroky 1-6) [22] (překlad autorky)

```
asa70(configif)#ip address 192.168.5.5 255.255.255.0
asa70(configif)#nameif inside
asa70(configif)#no shutdown
```

7. Now we need to enable the HTTP server on the ASA, which is required to connect to the device using the ASDM.

```
asa70(config)#http server enable
```

8. Now we will define an IP address on the inside network that will be allowed to connect to the ASA using either SSH or HTTP to manage the ASA.

```
asa70(config)#http 192.168.5.20 255.555.255.255 inside
asa70(config)#ssh 192.168.5.20 255.555.255.255 inside
```

9. Finally we'll create a local account on the ASA for the technician who will connect using HTTP or SSH and enable local authentication on the ASA. The username will be *Bob* and the password *passbob*. Give him level 15 (admin) access.

```
asa70(config)#username bob password passbob encrypted privilege 15
```

10. Normally at this point one would also configure a security level. We will do that in the next exercise after we discuss security levels.

Obrázek F.2: Počáteční konfigurace ASA (kroky 7-10) [22] (překlad autorky)

Setting Security Levels

In this procedure, you will configure the interfaces of the ASA security levels reflecting the relative trustworthiness of the inside, outside, and dmz interfaces. The interfaces in this procedure align with the last procedure, NOT with Figure 15.5, which is a different example.

1. Enter interface configuration mode for the inside, outside, and dmz interfaces and assign the security levels 100, 50, and 0 respectively.

```
asa70(config)#int gi0/3
asa70(config)#security-level 100
asa70(config)#int gi0/2
asa70(config)#security-level 50
asa70(config)#int gi0/3
asa70(config)#security-level 0
```

At this point you should be able to connect to the ASA using the ASDM as Bob from the machine at 192.168.5.20.

Obrázek F.3: Nastavení úrovní zabezpečení [22] (překlad autorky)

Creating Interface Access Rules in ASDM

In this procedure, you will configure two interface access rules in the ASDM. The ASA you manage has three interfaces that you have labeled inside (LAN), outside (Internet), and dmz. The security levels you have assigned are 100, 0, and 50 respectively. Currently the only rules in place are the global default rules discussed in the first set of bullet points in the section "Interface Access Rules" earlier in this section.

You need to configure the following rules:

- Allow only HTTP access from the outside interface to the dmz.
- Allow only HTTP from the inside to the dmz.

1. Connect to the ASA with the ASDM.
2. Navigate to Configuration ➢ Firewall ➢ Access Rules.
3. Click Add, and choose Add Access Rule.
4. We will first create the rule allowing only HTTP access from the outside interface to the dmz. In the Add Access Rule dialog box, select outside as the interface on which to apply the rule. In the Action section, select the Permit radio button. In the drop-down box for source IP address, select ANY. In the drop-down box for destination IP address, select ANY. In the Service box, type or select HTTP. Click OK. On the ASDM main page, click Apply.
5. Click Add, and choose Add Access Rule.
6. We will next create the rule allowing only HTTP access from the inside interface to the dmz. In the Add Access Rule dialog box, select inside as the interface on which to apply the rule. In the Action section, select the Permit radio button. In the drop-down box for source IP address, select ANY. In the drop-down box for destination IP address, select ANY. In the Service box, type or select HTTP. Click OK. On the ASDM main page, click Apply.

The configuration is now complete.

Obrázek F.4: Vytváření *přístupových pravidel* rozhraní v ASDM [22] (překlad autorky)

Creating and Using Objects in an Access Rule

In this procedure, you will create three objects and use them in an access rule. You need to allow HTTP traffic from the 192.168.5.0/24 network inside the LAN to a web server with the IP address of 201.3.3.3 in the DMZ. Therefore, you will

- Create a network object to represent the 192.168.5.0/24 network
- Create a service object to represent HTTP
- Create a host object to represent the server at 201.3.3.3
- Link these objects in an access rule and apply it to the inside interface

Note: interface objects have been created and named inside, outside, and dmz with security levels of 100, 0, and 50.

1. Connect to the ASA with the ASDM.
2. Navigate to Configuration ➢ Firewall ➢ Objects ➢ Network Objects/Groups.
3. Select Add, then Network Object.
4. In the Name field, enter HTTP_group_internal.
5. In the IP address and network mask sections, enter 192.168.5.0 and 255.255.255.0. Then select OK.
6. Select Add, then Network Objects/Groups.
7. In the Name field, enter DMZ_web.
8. In the IP address section, enter 201.3.3.3. Then select OK.
9. Select Object, then Service Objects/Groups and finally Add Service Group.
10. In the Add Service Group dialog box, enter a name for DMZ_services.
11. In the Existing service group section, select TCP-HTTP and TCP-HTTPS and select Add. Then click OK.
12. In the main ASDM window, select Apply to create the objects.
13. Navigate to Configuration ➢ Firewall ➢ Access Rules.
14. Click Add, and choose Add Access Rule.
15. In the Add Access Rule dialog box, select inside as the interface on which to apply the rule. In the Action section, select the Permit radio button. In the drop-down box for source IP address, select the object you created called HTTP_group_internal. In the drop-down box for destination IP address, select the object you created called DMZ_web. In the Service box, select the object you created called DMZ_services. Click OK. On the ASDM main page, click Apply.

The configuration is now complete.

Obrázek F.5: Vytváření a používání objektů v *přístupovém pravidle* [22] (překlad autorky)

Configuring Default Cisco Modular Policy Framework (MPF)

In this exercise, you will create a new policy by creating a class map that identifies Telnet as the traffic and a policy-map that identifies an action of deny and apply the two to all interfaces with a service policy.

1. Connect to the ASA with the ASDM.
2. Navigate to Configuration ➢ Firewall ➢ Service Policy Rules and click Add, then Service Policy rule.
3. Name the service policy *No_telnet* and select the Global radio button (which applies it to all interfaces). Click Next.
4. In the Traffic Class Criteria dialog box, select Create A New Traffic Class. Name the class *Telnet_deny*.
5. In the Traffic Match Criteria section, check the box for TCP Or UDP Destination Port and select Next.
6. In the service field of the next box enter **TCP/23** in both the Source and Destination fields. Click Next.
7. Select Finish. The configuration is complete.

Obrázek F.6: Konfigurace Výchozí Cisco *Modular Policy Framework* (MPF) [22] (překlad autorky)

Příloha G

Proces konfigurace detekce port skenu pomocí Cisco FMC

Configuring Portscan Detection

The portscan detection configuration options allow you to finely tune how the portscan detector reports scan activity.

The system builds a separate network map for each leaf domain. In a multidomain deployment, using literal IP addresses to constrain this configuration can have unexpected results. Using override-enabled objects allows descendant domain administrators to tailor Global configurations to their local environments.

Procedure

Step 1 Choose **Policies** > **Access Control**, then click **Network Analysis Policy** or **Policies** > **Access Control** > **Intrusion**, then click **Network Analysis Policy**.

Note If your custom user role limits access to the first path listed here, use the second path to access the policy.

Step 2 Click **Edit** (✎) next to the policy you want to edit.

If **View** (👁) appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

Step 3 Click **Settings**.

Step 4 If **Portscan Detection** under **Specific Threat Detection** is disabled, click **Enabled**.

Step 5 Click **Edit** (✎) next to **Portscan Detection**.

Step 6 In the **Protocol** field, specify protocols to enable.

Note You must ensure TCP stream processing is enabled to detect scans over TCP, and that UDP stream processing is enabled to detect scans over UDP.

Step 7 In the **Scan Type** field, specify portscan types you want to detect.

Step 8 Choose a level from the **Sensitivity Level** list; see Portscan Types, Protocols, and Filtered Sensitivity Levels, on page 4.

Step 9 If you want to monitor specific hosts for signs of portscan activity, enter the host IP address in the **Watch IP** field.

You can specify a single IP address or address block, or a comma-separated lists of either or both. Leave the field blank to watch all network traffic.

Step 10 If you want to ignore hosts as scanners, enter the host IP address in the **Ignore Scanners** field.
You can specify a single IP address or address block, or a comma-separated lists of either or both.

Step 11 If you want to ignore hosts as targets of a scan, enter the host IP address in the **Ignore Scanned** field.

You can specify a single IP address or address block, or a comma-separated lists of either or both.

Tip Use the **Ignore Scanners** and **Ignore Scanned** fields to indicate hosts on your network that are especially active. You may need to modify this list of hosts over time.

Step 12 If you want to discontinue monitoring of sessions picked up in mid-stream, clear the **Detect Ack Scans** check box.

Note Detection of mid-stream sessions helps to identify ACK scans, but may cause false events, particularly on networks with heavy traffic and dropped packets.

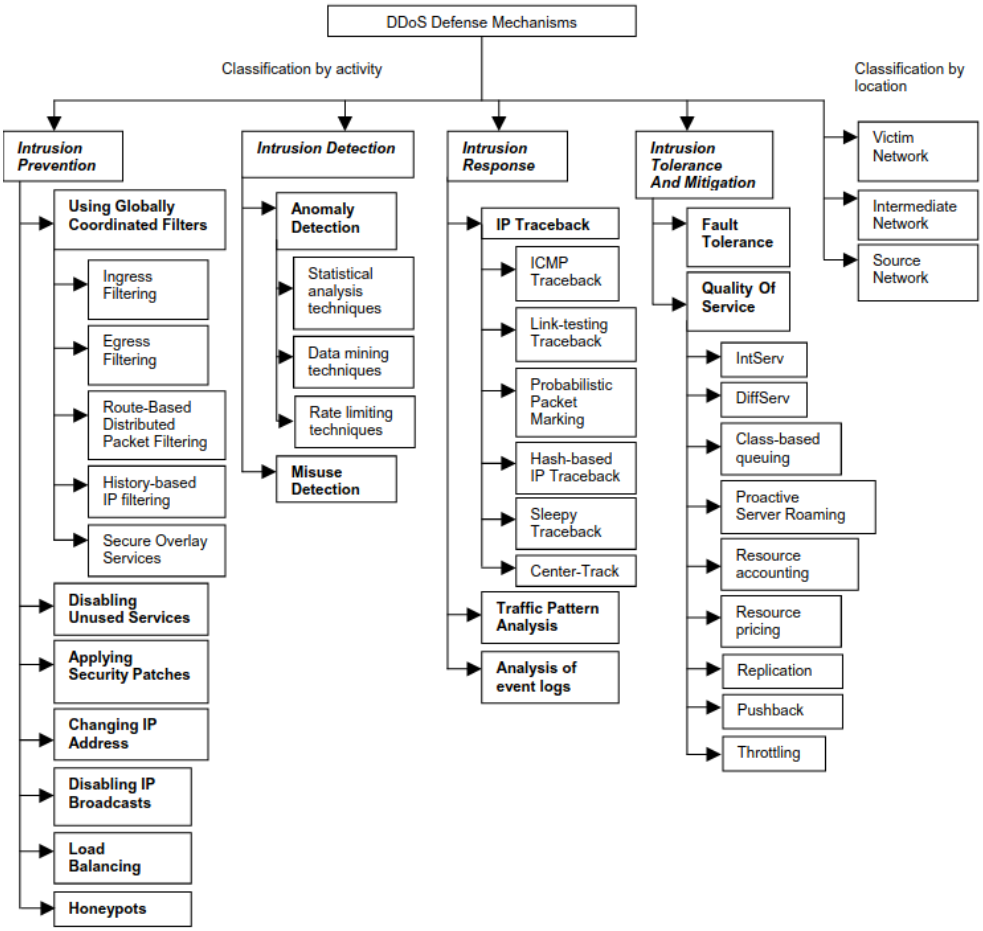
Step 13 To save changes you made in this policy since the last policy commit, click **Policy Information**, then click **Commit Changes**.

If you leave the policy without committing changes, changes since the last commit are discarded if you edit a different policy.

Obrázek G.1: Nastavení detekce port skenu [64] (překlad autorky)

Příloha H

Klasifikace metod ochrany proti DDoS útoku



Obrázek H.1: Klasifikace metod ochrany proti DDoS útoku[50] (překlad autorky)

Příloha I

Obsah přiloženého CD

- `ctiMe.txt` ..... stručný popis obsahu CD
- `src`
  - `thesis` ..... zdrojová forma práce ve formátu LaTeX
- `text` ..... text práce
  - `thesis.pdf` ..... text práce ve formátu PDF
- `ZIP` ..... archiv přiložených souborů