ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE

FAKULTA
BIOMEDICÍNSKÉHO
INŽENÝRSTVÍ

BAKALÁŘSKÁ PRÁCE

2020

MICHAL
ŠTUSÁK

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta biomedicínského inženýrství

Katedra zdravotnických oborů a ochrany obyvatelstva

Kybernetické hrozby proti kritické informační infrastruktuře v ČR

Cyber Threats against Critical Information Infrastructure of the Czech Republic

Bakalářská práce

Studijní program: Ochrana obyvatelstva
Studijní obor: Plánování a řízení krizových situací

Vedoucí práce: doc. RNDr. Josef Požár, CSc., dr. h. c.

Michal Štusák

Kladno, květen 2020

ČVUT
ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

I. OSOBNÍ A STUDIJNÍ ÚDAJE

Příjmení:	**Štusák**	Jméno:	**Michal**	Osobní číslo:	**34537**
Fakulta:	**Fakulta biomedicínského inženýrství**				
Garantující katedra:	**Katedra zdravotnických oborů a ochrany obyvatelstva**				
Studijní program:	**Ochrana obyvatelstva**				
Studijní obor:	**Plánování a řízení krizových situací**				

II. ÚDAJE K BAKALÁŘSKÉ PRÁCI

Název bakalářské práce:

Kybernetické hrozby proti kritické informační infrastruktuře v ČR

Název bakalářské práce anglicky:

Cyber Threats against Critical Information Infrastructure of the Czech Republic

Pokyny pro vypracování:

Předmětem bakalářské práce bude popis a analýza stavu kybernetických hrozeb v České republice se zaměřením na kritickou informační infrastrukturu. V teoretické části budou vymezeny základní pojmy kybernetické bezpečnosti a kritické informační infrastruktury. Dále budou uvedeny subjekty podílející se na zajištění kybernetické bezpečnosti České republiky. V praktické části budou popsány a analyzovány jednotlivé kybernetické hrozby. Dále bude proveden rozbor kybernetických hrozeb Distributed denial-of-service (DDoS) útoků a jejich dopad na kritickou informační infrastrukturu a navržen způsob ochrany proti těmto hrozbám.

Seznam doporučené literatury:

[1] KOLOUCH, Jan, BAŠTA, Pavel, CyberSecurity, Praha: CZ.NIC, 2019, ISBN 978-80-88168-31-7
[2] HROMADA, Martin, HRŮZA, Petr, KADERKA, Josef a kol., Kybernetická bezpečnost: teorie a praxe, Praha: Powerprint, 2015, ISBN 978-80-87994-72-6
[3] POŽÁR, Josef, Základy teorie informační bezpečnosti, Praha: Vydavatelství PA ČR, 2007, ISBN 978-80-7251-250-8
[4] SMEJKAL, Vladimír, Kybernetická kriminalita, Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, 636 s., ISBN 978-80-7380-501-2
[5] KOLOUCH, Jan, CyberCrime, Praha: CZ.NIC, 2016, ISBN 978-80- 88168-15-7

Jméno a příjmení vedoucí(ho) bakalářské práce:

doc. RNDr. Josef Požár, CSc.

Jméno a příjmení konzultanta(ky) bakalářské práce:

Datum zadání bakalářské práce: **17.02.2020**
Platnost zadání bakalářské práce: **19.09.2021**

prof. MUDr. Leoš Navrátil, CSc., MBA, dr.h.c.
podpis vedoucí(ho) katedry

prof. MUDr. Ivan Dylevský, DrSc.
podpis děkana(ky)

Prohlášení

Prohlašuji, že jsem bakalářskou práci s názvem Kybernetické hrozby proti kritické informační infrastruktuře v ČR vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

Nemám závažný důvod proti užití tohoto školního díla ve smyslu § 60 zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů.

V Kladně dne 01.04.2020

…….
podpis

Poděkování

Touto cestou bych rád poděkoval svému vedoucímu práce doc. RNDr. Josefu Požárovi, CSc., dr. h. c. za jeho podporu, trpělivost, cenné rady, připomínky i konstruktivní kritiku. Zároveň bych chtěl poděkovat vlastní rodině za trpělivost a podporu.

Abstrakt

Předmětem bakalářské práce je popis a analýza stavu kybernetických hrozeb v České republice se zaměřením na kritickou informační infrastrukturu. V teoretické části jsou vymezeny základní pojmy kybernetické bezpečnosti a kritické informační infrastruktury. Dále jsou uvedeny subjekty podílející se na zajištění kybernetické bezpečnosti České republiky.

V praktické části jsou popsány a analyzovány jednotlivé kybernetické hrozby. Detailní rozbor pak je proveden ke kybernetické hrozbě Distributed denial-of-service (DDoS) útoku a jeho dopadu na kritickou informační infrastrukturu. Následně je navržen způsob ochrany proti této hrozbě.

Klíčová slova

DDoS; kybernetická hrozba; kritická informační infrastruktura; kybernetická bezpečnost; kyberprostor.

Abstract

The subject of the bachelor thesis is a description and analysis of the state of cyber threats in the Czech Republic with a focus on critical information infrastructure. The theoretical part defines the basic concepts of cyber security and critical information infrastructure. The following are the entities involved in ensuring the cyber security of the Czech Republic.

The practical part describes and analyzes the individual cyber threats. A detailed analysis is then performed on the cyber threat of a Distributed denial-of-service (DDoS) attack and its impact on critical information infrastructure. Subsequently, a method of protection against this threat is proposed.

Keywords

DDoS; Cyber Threat; Critical Information Infrastructure; Cyber Security; Cyberspace.

Obsah

1 Úvod 11

2 Současný stav 12

2.1 Kyberprostor 12

2.2 Kybernetická bezpečnost 13

2.2.1 Základní principy kybernetické bezpečnosti 14

2.3 Riziko, aktivum, zranitelnost 15

2.3.1 Riziko 15

2.3.2 Aktivum 16

2.3.3 Zranitelnost 17

2.4 Kybernetické hrozby 19

2.4.1 Zdroje hrozby 19

2.4.2 Zdroje působení 20

2.4.3 Cíle hrozby 20

2.4.4 Motivace 21

2.4.5 Typy hrozeb 23

2.4.6 Kybernetická kriminalita 30

2.5 Kritická infrastruktura 31

2.5.1 Kritická informační infrastruktura 34

2.5.2 Významný informační systém 39

2.5.3 Významná síť 40

2.5.4 Základní služba 41

2.6 Subjekty podílející se na zajištění kybernetické bezpečnosti České republiky 42

2.6.1 Národní úřad pro kybernetickou a informační bezpečnost 42
2.6.2 CZ.NIC, zájmové sdružení právnických osob 44
2.6.3 Národní agentura pro komunikační a informační technologie, s. p. 46
2.6.4 Státní pokladna Centrum sdílených služeb, s. p. (SPCSS) 47
2.6.5 Národní centrála proti organizovanému zločinu SKPV 48
2.6.6 Útvar zvláštních činností služby kriminální policie a vyšetřování 48
2.6.7 Velitelství kybernetických sil a informačních operací 49
2.6.8 Vojenské zpravodajství 49
2.6.9 Poskytovatelé internetu 50
3 Cíl práce 52
4 Metodika 53
5 Výsledky 54
5.1 Kybernetické hrozby - analýza 54
5.1.1 Umělá inteligence a sítě 5G 54
5.1.2 Úniky dat 55
5.1.3 Dodavatelský řetězec 56
5.1.4 Kybernetická špionáž 57
5.1.5 Kryptomining 58
5.2 Distributed Denial of Service (DDoS) 59
5.2.1 Co je to DDoS útok ? 59
5.2.2 Rozdělení útoků 61
5.2.3 Techniky použití DDoS útoků 67

5.3 Návrh řešení ochrany proti DDoS útokům 69
5.3.1 Organizační opatření 69
5.3.2 Technická opatření 70
5.4 Ochrana kritické informační infrastruktury 76
6 Diskuze 79
7 Závěr 83
8 Seznam použitých zkratek 84
9 Seznam použité literatury 86
10 Seznam použitých obrázků 91

1 ÚVOD

Informační technologie v současné době představují vývoj a pokrok v naší společnosti. Snad každý z nás již zná a používá mobilní telefon a počítač, brouzdá po internetu, posílá emaily, chatuje, objednává zboží a platí za něj, poslouchá hudbu a sleduje televizi apod. V podstatě dělá stejnou činnost jako dříve, s tím rozdílem, že se pohybuje ve virtuálním světě, a to v kyberprostoru.

Tento svět jiný, nemá přesná pravidla ani hranice a stále se rychle vyvíjí. O to důležitější v tomto světě hraje bezpečnost, a to kybernetická bezpečnost. V tomto světě je velmi důležité, kdo jste, jak se chováte, jaké informace sdílíte apod. Tento svět Vás nutí být obezřetnější a přemýšlet o svém chování, poněvadž některé kroky jsou již nevratné a vytváří o Vás digitální stopu, která může být dále zneužita.

I v tomto světě existuje kritická infrastruktura, kde její narušení má závažný dopad na chod naší společnosti. Tu představují informační a komunikační systémy, které jsou spolu navzájem propojeny a zpracovávají velice důležitá a citlivá data. Jedná se o tzv. kritickou infomační infrastrukturu.

Předmětem mé práce je tedy provést rozbor kybernetických hrozeb vůči kritické informační infrastruktuře v České republice, zhodnotit riziko a jejich dopad. Následně navrhnout způsob ochrany proti těmto hrozbám.

2 SOUČASNÝ STAV

2.1 Kyberprostor

Na úvod se potřebujeme seznámit s pojmem kyberprostor, abychom dále pochopili význam a smysl slova kybernetická bezpečnost.

Kyberprostor dnes představuje virtuální prostředí, které není přesně vymezeno či ohraničeno. Toto virtuální prostředí tvoří informační a komunikační technologie, které jsou spolu propojené a navzájem komunikují pomocí komunikačních protokolů (převážně na bázi TCP/IP) a vytváří tak jednu globální počítačovou síť. Dále pak jednotlivými informačními systémy, které jsou do této sítě připojeny. Nedílnou součástí kyberprostoru jsou i uživatelé těchto systémů či správci a jejich interakce.

Mezi základní charakteristiky kyberprostoru patří **decentralizace**, tj. neexistuje žádný centrální místo, které by toto prostředí řídilo či spravovalo. Dále pak **globálnost**, tj. existuje na celém světě a není možno stanovit přesné hranice. **Otevřenost**, tj. může do ní přistupovat kdokoliv. **Bohatost na informace**, tj. najdeme zde nekonečné množství informací z kteréhokoliv oboru. **Interaktivnost**, tj. ovlivňovat samotné prostředí a informace zde obsažené [1].

V případě, že hledáme právní definici kyberprostoru, můžeme využít znění zákona č. 181/2014 Sb. § 2 písm. a) (zákon o kybernetické bezpečnosti), kde je uvedeno, že *„kybernetickým prostorem je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“* [2]

2.2 Kybernetická bezpečnost

V předešlé kapitole jsme se seznámili s definicí pojmu kyberprostor. To je pro nás velice důležité pro definici a popis pojmu kybernetická bezpečnost. Pojďme tedy vyjít z již ustálených definic.

Dle Jiráska a kol. představuje kybernetická bezpečnost *„souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.“* [3]

Pokud se podíváme do „Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020“. V této strategii je uvedeno, že: *„Kybernetická bezpečnost představuje souhrn organizačních, politických, právních, technických a vzdělávacích opatření a nástrojů směřujících k zajištění zabezpečeného, chráněného odolného kyberprostoru v České republice, a to jak pro subjekty veřejného a soukromého sektoru,tak pro širokou českou veřejnost.“* [4]

Za zmínku též stojí se podívat na právní normy věnující se kybernetické bezpečnosti. Zde můžeme vycházet ze zákona o kybernetické bezpečnosti (Zákon č. 181/2014 Sb.). Zákon jako takový sice samotný pojem neurčuje, ale snaží se popsat základy a principy kybernetické bezpečnosti.

V zákoně se můžeme seznámit s povinnostmi zavést bezpečnostní opatření týkajících se tzv. povinných subjektů a jejich právy. Je zde též vymezen okruh vztahů, zájmů a subjektů, vůči kterým dochází k uplatňování kybernetické bezpečnosti. Současně je v nich vymezován i kyberprostor, jakožto prostředí, ve kterém je kybernetická bezpečnost aplikována. [1]

2.2.1 Základní principy kybernetické bezpečnosti

Mezi nejznámější principy kybernetické bezpečnosti řadíme:

- Triáda CIA
- Prvky kybernetické bezpečnosti
- Životní cyklus kybernetické bezpečnosti

Triáda CIA

Triáda CIA vychází ze 3 základních principů **důvěrnost** (C - Confidentiality); **integrita** (I – Integrity); **dostupnost** (A – Availability) a vztahuje se především k informacím či datům jako takovým v návaznosti na ochranu informací.

Prvky kybernetické bezpečnosti

Prvky kybernetické bezpečnosti tvoří:

- Lidé
- Procesy
- Technologie

a představují prvky, které spolu vzájemně interagují za účelem dosažení co nejvyšší kybernetické bezpečnosti.

Životní cyklus kybernetické bezpečnosti

Životní cyklus kybernetické bezpečnosti představuje nekonečný cyklus opakujících činností za účelem z dokonalení kybernetické bezpečnosti. Ve zjednodušené formě můžeme uvést třeba „Prevence-Detekce-Reakce.“[5]

2.3 Riziko, aktivum, zranitelnost

2.3.1 Riziko

Jedním ze základních pojmů v oblasti kybernetické bezpečnosti je pojem riziko, které si zde popíšeme.

Výkladový slovník kybernetické bezpečnosti definuje riziko jako: *„(1) Nebezpečí, možnost škody, ztráty, nezdaru. (2) Účinek nejistoty na dosažení cílů. (3) Možnost, že určitá hrozba využije zranitelnosti aktiva nebo skupiny aktiv a způsobí organizaci škodu.*“ [3]

Dle čl. 4 odst. 9 NIS se rizikem rozumí „*jakákoli přiměřeně rozpoznatelná okolnost nebo událost, která by mohla mít negativní dopad na bezpečnost sítí a informačních systémů.*“[6] Rizikům jsou dnes prakticky vystaveny všechny prvky kybernetické bezpečnosti, ať už mluvíme komunikačních systémech a aplikací, nebo samotných uživatelích, kteří je používají.

V rámci analýzy rizik potřebujeme stanovit významnost definovaných rizik, a to pomocí dopadu rizika, které může způsobit, tak pomocí pravděpodobnosti vzniku rizika.

Významnost rizika = **Dopady** rizika * **Pravděpodobnost** vzniku rizika

Dopady rizika neboli následky hodnotíme v pětibodové stupnici např. takto: „Krizové, Významné, Střední, Nevýznamné, Zanedbatelné“

Pravděpodobnost vzniku rizika hodnotíme v pětibodové stupnici např. takto: „Jisté, Pravděpodobné, Možné, Nepravděpodobné, Vyloučené“

Při hodnocení rizika musíme brát v potaz i další okolnosti, jako jsou:

- vlastní povaha rizika či hrozby,
- zranitelnost aktiva,
- pravděpodobnosti, že se riziko promění v bezpečnostní událost či incident. [7]

Na základě analýzy rizik pak můžeme stanovit opatření za účelem minimalizace nebo úplného odstranění rizik.

2.3.2 Aktivum

Aktivem představuje cokoliv, co má určitou hodnotu pro osobu, organizaci či stát. Aktivum může mít povahu hmotnou (budova, komunikační sítě, zboží aj.) či nehmotnou (informace, znalosti, data, aplikace aj.) z pohledu občanského práva.

Dále mohou být aktivem uživatelé a administrátoři a jejich znalosti a zkušenosti nebo vlastnosti jako jsou funkčnost či vysoká dostupnost systému.

Vyhláška o kybernetické bezpečnosti (VoKB) dle § 2 písm. f) a g) aktiva dělí na podpůrná a primární.

„podpůrným aktivem technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního a komunikačního systému,

primárním aktivem informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém,“ [8]

2.3.3 Zranitelnost

Zranitelnost představuje slabé místo aktiva, softwaru, zabezpečení, které je využito jednou nebo více hrozbami. Zranitelnost, stejně jako hrozba, může být způsobena celou řadou faktorů spočívajících jak v jednání člověka, technické závadě, tak případně zásahu vyšší moci.

V oblasti kybernetické bezpečnosti se zranitelnosti dělí na:

- zranitelnosti známé
    - opravené – typickým případem jsou zranitelnosti softwaru, na který již výrobce vydal aktualizaci
    - neopravené – dotčený subjekt (výrobce, správce aj.) o zranitelnosti ví, ale nezajistil její opravu
- zranitelnosti neznámé
    - skryté
    - neobjevené

Bezpečnostní zranitelnosti představují potenciální bezpečnostními hrozby. Bezpečnostní zranitelnosti lze do určité míry eliminovat důsledným aktualizováním a záplatováním veškerého softwaru.[3]

Vyhláška o kybernetické bezpečnosti v příloze č. 3 uvádí některé ze zranitelností:

1. *nedostatečná údržba informačního a komunikačního systému,*
2. *zastaralost informačního a komunikačního systému,*
3. *nedostatečná ochrana vnějšího perimetru,*
4. *nedostatečné bezpečnostní povědomí uživatelů a administrátorů,*
5. *nedostatečná údržba informačního a komunikačního systému,*
6. *nevhodné nastavení přístupových oprávnění,*

7. *nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,*
8. *nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,*
9. *nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,*
10. *nedostatečná ochrana aktiv,*
11. *nevhodná bezpečnostní architektura,*
12. *nedostatečná míra nezávislé kontroly,*
13. *neschopnost včasného odhalení pochybení ze strany zaměstnanců.*[8]

2.4 Kybernetické hrozby

Kybernetickou hrozbu si můžeme představit jako negativní působení, které může mít za následek narušení, změnu, krádež či zničení informací nebo systému. Tyto hrozby primárně vznikají a přicházejí z kyberprostoru. V případě realizace kybernetické hrozby již ale mluvíme o kybernetickém útoku.[34]

Kybernetické hrozby můžeme rozdělit či kategorizovat dle

- Zdroje hrozby (lidské, technické chyby, vyšší moc)
- Zdroje působení (vnitřní, vnější)
- Cíle hrozby (prvky kybernetické bezpečnosti, triáda CIA, procesy)
- Motivace (zisk, konkurence, dokazování svých schopností apod.)
- Typu hrozby (ransomware, sociální inženýrství, DDoS, atd.) [9]

2.4.1 Zdroje hrozby

- **Hrozby způsobené člověkem**. Z tohoto pohledu je možné rozlišovat hrozby způsobené:
    - **úmyslně**,

      Mezi úmyslně způsobené kybernetické hrozby je možné zařadit například:
        - úmyslné smazání dat, konfigurace systému,
        - fyzické poškození počítačového systému či jiného prvku ICT,
        - zcizení dat a informací,
        - kybernetické útoky (malware, DDoS, phishing, neoprávněný odposlech).
    - **z nedbalosti.**

      Mezi kybernetické hrozby způsobené z nedbalosti je možné zařadit například:

        - omylem smazaná data,
        - fyzické poškození počítačového systému či jiného prvku ICT (např. pádem, překopnutím kabeláže),
        - poškození dat, systémů či jiných prvků na základě neseznámení se s interními akty,
        - jiná chyba uživatele.
- **Technické chyby** (chyba softwaru či hardwaru).
- **Vyšší moc**

  Mezi kybernetické hrozby způsobené vyšší mocí patří například:
    - výpadek napájení,
    - přírodní události (zásah blesku, vichřice) či katastrofy (povodně, zemětřesení),
    - požár.[1]

2.4.2 Zdroje působení

- hrozby vnitřní (zdroj hrozby se nachází uvnitř organizace)
- hrozby vnější (zdroj hrozby se nachází mimo organizaci) [10]

2.4.3 Cíle hrozby

- **Útok na triádu CIA**.
    - Confidentiality (důvěrnost) – např. krádeže dat, přístupových údajů a klíčů, hardware.
    - Integrity (celistvost) – chyby v databázích, v nastavení oprávnění.
    - Availability (dostupnost) – např. DoS a DDoS útoky; výpadky proudu.

- **Útok na některý z prvků kybernetické bezpečnosti.**

- **Lidé** – útoky sociálním inženýrstvím (ve světě reálném, ale i kyberprostoru), phishing, malware, krádeže.
- **Technologie** – jakékoliv hrozby mohu působit na:
  - hardware (počítače, servery, řídící prvky sítě, IoT),
  - databáze,
  - síť a síťovou infrastrukturu,
  - software (operační systém či jiné aplikace),
  - informace a data uložená v počítačových systémech.

- **Procesy** – neoprávněné testování zabezpečení či funkčnosti procesů nastavených.[1]

2.4.4 Motivace

Důležitým aspektem je též motivace v případě úmyslného jednáním člověka. Na základě analýzy motivace takovéhoto jednání je v rámci procesu reakce na hrozbu možné vytvořit nápravná opatření, aby nedocházelo ke stimulu této motivace i v budoucnu.

Dle motivace lze sledovat:

- hrozby za účelem získání finančního prospěchu,
- hrozby za účelem získání konkurenční převahy,
- hrozby za účelem dokázání svých schopností,
- hrozby za účelem odplaty,
- hrozby z důvodu neplnění povinností. [11]

Dle Aktérů:

- **státní aktéři a státem sponzorované skupiny** - nejvyšší hrozba, dostatek lidských a finančních prostředků, sofistikované a perzistentní techniky
- **kyberzločinci** - finanční prospěch, techniky ransomware a sociální inženýrství
- **teroristé** – šíření propagandy, rekrutování nových bojovníků
- **hacktivisté** – političtí aktivisté, narušování dostupnosti, důvěrnosti a integritu informací
- **black hats** – hackeři, vlastní prospěch
- **script kiddies** – amatéři, používají nástroje jiných [12]

2.4.5 Typy hrozeb

Příloha č. 3 Vyhlášky č. 82/2018 Sb. o kybernetické bezpečnosti uvádí některé z hrozeb. Dle této vyhlášky je hrozbou:

1) *„porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,*
2) *poškození nebo selhání technického anebo programového vybavení,*
3) *zneužití identity,*
4) *užívání programového vybavení v rozporu s licenčními podmínkami,*
5) *škodlivý kód (například viry, spyware, trojské koně),*
6) *narušení fyzické bezpečnosti,*
7) *přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,*
8) *zneužití nebo neoprávněná modifikace údajů,*
9) *ztráta, odcizení nebo poškození aktiva,*
10) *nedodržení smluvního závazku ze strany dodavatele,*
11) *pochybení ze strany zaměstnanců,*
12) *zneužití vnitřních prostředků, sabotáž,*
13) *dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,*
14) *nedostatek zaměstnanců s potřebnou odbornou úrovní,*
15) *cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,*
16) *zneužití vyměnitelných technických nosičů dat,*
17) *napadení elektronické komunikace (odposlech, modifikace).“* [8]

Přehled jednotlivých konkrétních metod či technik, které jsou zneužity při kybernetické hrozbách:

Sociální inženýrství

Cílem sociálního inženýrství je získání informací formou manipulace, ovlivňování a přesvědčování lidí, které by normálně neposkytli. Útočník cílí na nejslabší článek zabezpečení jakéhokoliv systému, tedy na člověka. Člověk není stroj, který lze bezpečně naprogramovat, ale živým jedincem, který jedná na základě svých zkušeností, znalostí a emocí. Útočník tak může pomocí specifické přípravy a psychologické manipulace ovlivnit některá rozhodnutí člověka tak, že provede určitou konkrétní činnost, které by se za jiných okolností nedopustil.

Asi nejznámější průkopníkem sociálního inženýrství je Kevin Mitnick, který ve své knize popisuje svůj příběh a jednotlivé sociotechnické metody manipulace s lidmi.[39]

Snahou útočníka je nejdříve získat co nejvíce volně dostupných informací o cíli útoku. Dále pak fyzický útok, kdy se snaží útočník vydávat za cizí osobu, která má určitou důvěru k cíli a je schopna jednodušeji získat interní informace. A konečně pak využít psychologický útok.

Některé metody sociálního inženýrství:

- Telefonický hovor
- Podvodný email
- Využití sociálních sítí
- Falešná technická podpora
- Vyzkoušení online služeb zdarma
- Reklamní materiál na datových nosičích

Pokud jde o cíl útoků sociálního inženýrství v rámci organizace, pak se možnými cíli mohou stát například:

- IT oddělení,
- pracovníci help desku,
- bezpečnostní pracovníci,
- recepční,
- správa budov,
- úklid

Botnet

Botnet přestavuje síť softwarově propojených botů, které provádí činnost na základě příkazu správce této sítě. Takto postavená síť může být použita k legální činnosti nebo k trestné činnosti. Tyto boty nalezneme na nezabezpečených počítačích nebo síťových zařízeních bez vědomosti vlastníků těchto zařízení. V rozvojem IoT se tato hrozba zvětšuje z důvodu velkého množství těchto zařízení s nízkou úrovní zabezpečení.

Malware

Malware je škodlivý software, který se využívá k narušení standardní činnosti počítačového systému, zisku informací nebo k získání přístupu k počítačovému systému. Existuje mnoho druhů malwaru v závislosti na činnosti, kterou provádí. Může se například sám dále šířit prostřednictvím e-mailů v rámci příloh nebo jako data v P2P sítích nebo může získávat například e-mailové adresy z napadeného počítačového systému.

Ransomware

Patří do rodiny malware a jedná se o tzv. vyděračský malware a označujeme ho ransomware. Ransomware je malware, který brání či omezuje uživatele v řádném užívání počítačového systému do doby, než dostane útočník zaplaceno „výkupné“. Ransomware se nejčastěji dostane do počítače pomocí trojského koně či červa, který je umístěn na webových stránkách, nebo je přílohou e-mailu. Jakmile je tento malware v počítačovém systému, dojde ke stažení vlastního ransomware a většinou dochází k zašifrování dat.

Spam

Jedná se o hromadné šíření nevyžádaného sdělení nejčastěji reklamního charakteru pomocí Internetu. Obecně se jedná o všechny doručené nevyžádané zprávy, které mohou obsahovat zprávy obsahující viry, trojské koně apod.

Phishing

Podstatou phishingu je využívání sociálního inženýrství. Představuje jednání, které po uživateli vyžaduje navštívení podvodné stránky (např. webovou stránku internetového bankovnictví a následné vyplnění přihlašovacích informací), případně jsou tyto informace vyžadovány přímo (např. při vyplnění formuláře).

Za phishing můžeme označit jakékoli podvodné jednání, které má v uživateli vzbudit důvěru, snížit jeho ostražitost či jej jinak donutit akceptovat scénář předem připravený útočníkem.

Pharming

Pharming představuje nebezpečnější formu phishingu. Jedná se o útok na DNS server, na kterém dochází k překladu doménového jména na IP adresu. K útoku dochází v momentě, kdy uživatel zadá na internetovém prohlížeči adresu webového serveru, na kterou chce přistoupit. Nedojde však k propojení na příslušnou IP adresu originálního webového serveru, ale na IP adresu jinou, podvrženou.

Webové stránky na falešné adrese zpravidla velmi věrně imitují originální stránky, de facto jsou od nich k nerozeznání. Uživatel následně zadá přihlašovací údaje, které získá útočník. Tento útok je zpravidla realizován při přístupu uživatele na stránky internetového bankovnictví.

Spear phishing

Spear phishing je specifický tím, že se jedná o přesně cílený phishing útok. Cílem útoku je konkrétní skupina, organizace nebo jednotlivec, konkrétní informace a data.

Útoky nultého dne

Útok nultého dne se snaží využít zranitelnosti používaného softwaru, která ještě není obecně známá a neexistuje pro ni obrana v podobě aktualizace softwaru. Do doby, než je vyjde aktualizace a její instalace, zůstává systém a jeho uživatel ohrožen. To může trvat několik dní, ale i třeba roků. Tyto zranitelnosti jsou způsobeny především programátorským chybám a jsou velice časté, neboť je čím dál větší tlak na uvedení softwaru na trh.

Útoky hrubou silou

Útok hrubou silou se většinou využívá pro získání dvojice uživatel a heslo. Je možné používat náhodná přihlašovací jména a hesla při pokusech o autentizaci, případně možné varianty omezit. Protože si uživatelé často volí málo silné heslo, je tento a automatizovaný útok poměrně úspěšný a široce rozšířený.

SQL injection

Jedná se o útok na internetové stránky prováděný přes neošetřený formulář, manipulací s URL nebo třeba i podstrčením upravené cookie. SQL injection je technika napadení databázové vrstvy programu vsunutím kódu přes neošetřený vstup a vykonání vlastního pozměňujícího poškozujícího SQL příkazu. Toto nezamýšlené neošetřené chování vzniká při propojení aplikační vrstvy s databázovou vrstvou.

Hacking

Jedná se o neoprávněné proniknutí do aplikací nebo počítačových systémů prolomením bezpečnostní ochrany. Může se jednat o zneužití chyb aplikací či systémů.

Sniffing

Sniffing je technika, která umožňuje odposlouchávání komunikace, která se používá např. při diagnostice sítě. Při odposlechu může útočník získat nejenom obsah komunikace, ale třeba i přihlašovací údaje, pokud již nejsou šifrovány.

APT (Advanced Persistent Threat)

Přetrvávající pokročilé hrozby (APT) jsou přesně cílené útoky proti konkrétní osobě nebo organizaci. Útočník kombinuje velkou škálu pokročilých technik od využití útoku nultého dne, kde si napíše funkční exploit a začlení ho do malwaru, až po využití sociálního inženýrství. Cílem útočníka je zajistit si trvalý přístup do systému dané organizace, neboť primárním cílem APT útoků je zpravidla získat citlivé informace, které se v dané organizaci nachází.

NÚKIB ve své výroční zprávě uvádí jako největší hrozby pro rok 2019 a dále tyto:

- *„Kybernetická špionáž*
- *Úniky dat*
- *Dodavatelé*
- *Volby*
- *Kryptomining*
- *Umělá inteligence a sítě 5G*
- *DDoS"*[12]

2.4.6 Kybernetická kriminalita

Využívání informačních technologií a jejich integrace do téměř všech odvětví lidské činnosti je jevem, který je pro dnešní dobu charakteristický. V podstatě nejde nalézt oblast lidské činnosti, kde by se přímo nebo zprostředkovaně nevyužívala výpočetní technika. Bohužel, tak jak rostou možnosti užívání těchto prostředků, rostou i možnosti a zároveň i četnost jejich zneužívání k páchání trestné činnosti.

V roce 2000 vydala Rada Evropy definici počítačové kriminality pocházející ze Statutu Komise expertů pro zločin v kyberprostoru: *„Trestný čin namířený proti integritě, dostupnosti nebo utajení počítačových systémů nebo trestný čin v tradičním smyslu, při kterém je užito moderních informačních a komunikačních technologií.“* [31]

V mezinárodních úmluvách se pro trestnou činnost páchanou prostředky informačních technologií užívá nejčastěji pojem „kybernetická kriminalita“ a používání tohoto pojmu se z oblasti normativní přeneslo též do slovníku odborné veřejnosti. Pojem kyberkriminalita má obdobný charakter jako pojmy *„násilná kriminalita“, „kriminalita mladistvých“, „ekonomická kriminalita“ apod. Takovýmito názvy jsou označovány skupiny trestných činů mající určitý společný faktor, jako např. způsob provedení, osobu pachatele (alespoň druhově) apod. Ve své podstatě přitom může jít o velmi různorodou směsici trestných činů, spojených oním společným faktorem (počítačem, programem, daty).“*[32]

2.5 Kritická infrastruktura

Kritická infrastruktura (KI) představuje infrastrukturu, která je klíčová pro fungování státu, ekonomiky a společnosti. V případě ohrožení nebo zkolabování této infrastruktury, může dojít k významného omezení fungování společnosti v daném státě.

V rámci České republiky je kritická infrastruktura definována v zákoně č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) jako: „*prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu*“ [13].

Dále je pak prvek kritické infrastruktury též vymezen a určen v krizovém zákoně jako: „*zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií; je-li prvek kritické infrastruktury součástí evropské kritické infrastruktury, považuje se za prvek evropské kritické infrastruktury*“ [13].

Definici průřezových a odvětvových kritérií vymezuje nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

Průřezovým kritériem pro určení prvku kritické infrastruktury je hledisko

- *Oběti s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin,*
- *ekonomický dopad s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo*

- *dopad na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125000 osob* [14].

Odvětvová kritéria pro určení prvku kritické infrastruktury jsou uvedena v příloze nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury a tvoří ji 9 skupin odvětví.

I. *energetika,*
II. *vodní hospodářství,*
III. *potravinářství a zemědělství,*
IV. *zdravotnictví,*
V. *doprava,*
VI. *komunikační a informační systémy,*
VII. *finanční trh a měna,*
VIII. *nouzové služby,*
IX. *veřejná správa.*[14]

Proces určování prvků KI

- *Prvky KI, jejichž provozovatelem je organizační složka státu (dále jen „OSS"):*
  - *ministerstva a ústřední správní úřady a ČNB zasílají Ministerstvu vnitra návrhy prvků KI a EKI, jejichž provozovatelem je OSS (§ 9 odst. 3 písm. d) a §13 odst. 4 písm. c) krizového zákona),*
  - *Ministerstvo vnitra zpracuje seznam, který je podkladem pro určení prvků KI a EKI, jejichž provozovatelem je OSS (§ 10 odst. 1 písm. f) krizového zákona),*
  - *vláda usnesením určí prvky KI a EKI, jejichž provozovatelem je OSS (§ 4 odst. 1 písm. e) krizového zákona).*

- *Prvky KI, které nejsou určovány podle § 4 odst. 1 písm. e) krizového zákona (jejichž provozovatelem není OSS):*
    - *ministerstva a ústřední správní úřady a ČNB určí opatřením obecné povahy prvky KI a EKI,*
    - *o tomto určení informují bez zbytečného odkladu Ministerstvo vnitra.*

Prvky kritické infrastruktury, jejichž provozovatelem je organizační složka státu byly určeny usnesením vlády č. 934 ze dne 14. prosince 2011, které bylo naposledy aktualizováno usnesením vlády č. 10 ze dne 7. ledna 2019. [15]

Subjektem KI se rozumí *provozovatel prvku kritické infrastruktury; jde-li o provozovatele prvku evropské kritické infrastruktury, považuje se tento za subjekt evropské kritické infrastruktury.*[13] Subjekt KI má povinnost určit styčného bezpečnostního zaměstnance, který poskytuje za subjekt KI součinnost při plnění úkolů podle krizového zákona.

Subjekt KI odpovídá za ochranu prvku KI a za tímto účelem zpracovává plán krizové připravenosti subjektu KI. V tomto plánu jsou identifikována možná ohrožení funkce prvku KI a stanovena opatření na jeho ochranu. Skládá se ze základní části, operativní části a pomocné části. Náležitosti a způsob zpracování plánu krizové připravenosti uvádí § 17 a § 18 nařízení vlády č. 462/2000 Sb., k provedení § 27 odst. 8 a § 28 odst. 5 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). [15]

2.5.1 Kritická informační infrastruktura

Kritická informační infrastruktura (KII) je podmnožinou kritické infrastruktury a z výše uvedených devíti odvětví se jedná o odvětví komunikační a informační systémy. Její přesná definice je uvedena v zákoně č. 181/2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Odvětvová kritéria pro komunikační a informační systémy:

„A. Technologické prvky pevné sítě elektronických komunikací:

a) centrum řízení a podpory sítě,
b) řídící ústředna,
c) mezinárodní ústředna,
d) transitní ústředna,
e) datové centrum,
f) telekomunikační vedení.

B. Technologické prvky mobilní sítě elektronických komunikací:

a) centrum řízení a podpory sítě,
b) ústředna mobilní sítě,
c) základnová řídící jednotka sítě pokrývající strategickou lokalitu,
d) základnová stanice sítě pokrývající strategickou lokalitu,
e) datové centrum.

C. Technologické prvky sítí pro rozhlasové a televizní vysílání:

a) vysílací zařízení pro šíření televizního nebo rozhlasového signálu určených pro informaci obyvatelstva za krizových situací s vysílacím výkonem nejméně 1 kW k

zajištění provozu rozhlasového a televizního vysílání veřejnoprávního provozovatele,

b) *řídící pracoviště provozu,*
c) *datové centrum,*
d) *síť pro rozhlasové a televizní vysílání k zajištění provozu rozhlasového a televizního vysílání veřejnoprávního provozovatele.*

D. Technologické prvky pro satelitní komunikaci:

a) *hlavní pozemní satelitní přijímací a vysílací stanice,*
b) *Evropský globální navigační družicový systém,*
c) *pozemní řídící a komunikační středisko,*
d) *pozemní propojovací síť.*

E. Technologické prvky pro poštovní služby:

a) *centrální a regionální výpočetní středisko, středisko centrálního snímání a úložiště dat,*
b) *sběrný přepravní uzel,*
c) *řídící a mezinárodní pošta,*
d) *poštovní dopravní infrastruktura.*

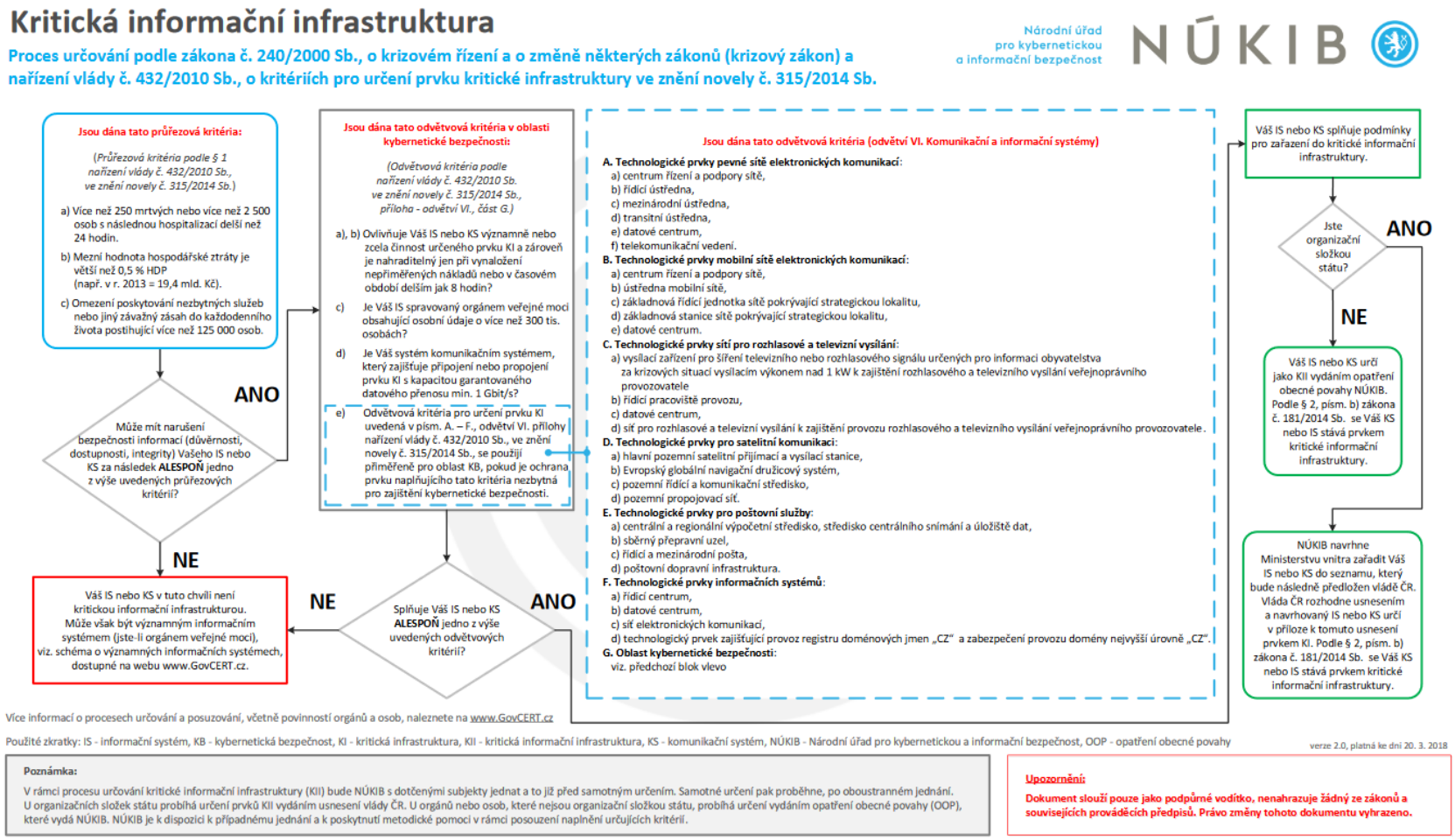
F. Technologické prvky informačních systémů:

a) *řídicí centrum,*
b) *datové centrum,*
c) *síť elektronických komunikací,*
d) *technologický prvek zajišťující provoz registru doménových jmen „CZ“ a zabezpečení provozu domény nejvyšší úrovně „CZ“.*

G. Oblast kybernetické bezpečnosti:

a) *informační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin,*
b) *komunikační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin,*
c) *informační systém spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300000 osobách,*
d) *komunikační systém, zajišťující připojení nebo propojení prvku kritické infrastruktury, s kapacitou garantovaného datového přenosu nejméně 1 Gbit/s,*
e) *odvětvová kritéria pro určení prvku kritické infrastruktury uvedená v písmenech A. až F. se použijí přiměřeně pro oblast kybernetické bezpečnosti, pokud je ochrana prvku naplňujícího tato kritéria nezbytná pro zajištění kybernetické bezpečnosti"* [14].

Postup určení prvku kritické informační infrastruktury vychází z podmínky splnění minimálně jednoho průřezového a odvětvového kritéria. Dále musíme rozlišit, zdali Informační systém (IS) nebo komunikační systém (KS) je ve správě organizační složky státu (OSS). V kladném případě Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) předloží návrh vládě ČR, která návrh projedná a vydá usnesení, které označí informační a komunikační systém za prvek kritické informační infrastruktury. V opačném případě NÚKIB vydá opatření obecné povahy a poté se informační a komunikační systém stane prvkem kritické informační infrastruktury. Níže uvedený obrázek detailně popisuje postup určení prvku kritické informační infrastruktury.



Obrázek 1 - Proces určování kritické informační infrastruktury [16]

Zákon ukládá povinnosti v oblasti kybernetické bezpečnosti jak osobám soukromého, tak veřejného práva. Stanovuje tři skupiny regulovaných subjektů a definuje jejich povinnosti. Za správce komunikačního nebo informačního systému kritické informační infrastruktury je považován ten, kdo určuje účel zpracování informací a podmínky provozování komunikačního nebo informačního systému, typicky tedy jeho vlastník. Správci jsou tak například jednotlivá ministerstva nebo jiné ústřední správní úřady, ale budou jimi i provozovatelé prvků kritické infrastruktury dle Krizového zákona a příslušného Nařízení o kritériích pro určení prvku KI. Správce v režimu Zákona je tedy subjekt odpovědný za plnění povinností stanovených Zákonem.

Systém zajištění kybernetické bezpečnosti je tvořen pomocí bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů, jejich následné evidence a provádění opatření k ochraně informačních systémů a služeb a sítí elektronických komunikací. Dodržování povinností uložených povinným subjektům Zákonem o kybernetické bezpečnosti je vynucováno ukládáním sankcí.[33]

Přehled prvků kritické informační infrastruktury je neveřejný. Nicméně některá ministerstva o těchto prvcích informují na svých stránkách.

K datu 26.9. 2019 NÚKIB uvádí počet systémů KII – 118, a správců KII – 48 subjektů. Jedná se o OSS i soukromou sféru. A to především v odvětvoví energetika, telekomunikace, ministerstva a statní úřady.

2.5.2 Významný informační systém

Významným informačním systémem (VIS) je informační systém spravovaný orgánem veřejné moci a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

Významným informačním systémem není systém, který je kritickou informační infrastrukturou či informačním systémem základní služby.

Dle § 2 písm. b) zákona č. 365/2000 Sb., o informačních systémech veřejné správy se *informačním systémem veřejné správy rozumí funkční celek nebo jeho část zabezpečující cílevědomou a systematickou informační činnost pro účely výkonu veřejné správy. Každý informační systém veřejné správy zahrnuje data, která jsou uspořádána tak, aby bylo možné jejich zpracování a zpřístupnění, provozní údaje a dále nástroje umožňující výkon informačních činností.*[17]

Vlastní stanovení významných informačních systémů je uvedeno ve vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích. Pro to, aby mohl být informační systém označen za významný, musí splnit určující kritéria, kterými jsou:

a) dopadová určující kritéria a

b) oblastní určující kritéria.

Zároveň vyhláška č. 317/2014 Sb. negativně vymezuje informační systémy, které nejsou významným informačním systémem. Konkrétně se jedná o informační systém, jehož správcem je obec a při výkonu působnosti obce hlavní město Praha.

Kritéria pro určení VIS jsou mnohem měkčí než v případě KII, nicméně se stále jedná o velmi důležité systémy pro chod státu nebo krajů. VIS stejně jako KII spadají do kompetence NÚKIB.

Seznam VIS systémů je uveden v příloze vyhlášky č. 317/2014 Sb. Jistě je nasnadě, že i tento přehled VIS systémů by neměl být veřejný.

K datu 26.9. 2019 NÚKIB uvádí počet systémů KII – 171, a správců KII – 68 subjektů. Jedná se pouze o orgány státní moci.

2.5.3 Významná síť

Dle § 2 ZoKB se rozumí „*Významnou sítí síť elektronických komunikací zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře*.“ [2]

Významná síť (VS) nepředstavuje samotnou kritickou informační infrastrukturu, ale zajišťuje propojení kritické informační infrastruktury s kybernetickým prostorem nebo vytváří přímé zahraniční propojení v ČR, které dnes zajišťují velcí domácí či zahraniční poskytovatelé internetu (ISP) a tvoří tzv. páteřní sítě.

Infrastruktura těchto subjektů vytváří vstupní a výstupní brány českého kyberprostoru. Koordinace a spolupráce s těmito subjekty je klíčová pro zajištění kybernetické bezpečnosti. VS spadají do kompetence národního CSIRTu, tedy CZ.NICu.

2.5.4 Základní služba

Základní služba je služba, která je závislá na informačních systémech nebo sítích elektronických komunikací v odvětvích:

1) energetika,
2) doprava,
3) bankovnictví,
4) infrastruktura finančních trhů,
5) zdravotnictví,
6) vodní hospodářství,
7) digitální infrastruktura nebo
8) chemický průmysl.

Dle § 2 ZoKB se rozumí „*základní službou služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví.*“ [2].

Samotné vymezení jednotlivých základních služeb je uvedeno ve vyhlášce č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby (PZS) a dále stanovení kritérií pro určení provozovatele základní služby a informačního systému. Při určení toho, zda je daná služba základní službou, se užijí odvětvová a dopadová kritéria. Tato kritéria jsou mnohem měkčí než v případě kritické informační infrastruktury.

K datu 26.9. 2019 NÚKIB uvádí počet systémů PZS – 56, a správců PZS – 38 subjektů. Jedná se pouze o soukromou sféru.

2.6 Subjekty podílející se na zajištění kybernetické bezpečnosti České republiky

V České republice existuje několik organizací, které legislativně vymezují kybernetický prostor, mají zásadní vliv na jeho správu a provoz, a samozřejmě zajišťují jeho ochranu. Pojďme se podívat na ty nejdůležitější.

2.6.1 Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB) je ústředním správním orgánem pro kybernetickou bezpečnost včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti problematiku neveřejné služby v rámci družicového systému Galileo. Vznikl 1. srpna 2017 na základě zákona číslo 205/2017 Sb., kterým se změnil zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) [18].

Ředitel Úřadu se též pravidelně účastní jednání Bezpečnostní rady státu (BRS) a je členem Výboru pro kybernetickou bezpečnost, který je stálým pracovním orgánem BRS pro koordinaci plánování opatření k zajišťování kybernetické bezpečnosti České republiky.

Národní centrum kybernetické bezpečnosti

Národní centrum kybernetické bezpečnosti (NCKB) je výkonnou sekcí NÚKIB. Sekce NKCB zajišťuje:

- činnost Vládního CERT České republiky (GovCERT.CZ)
- prevenci před kybernetickými hrozbami proti prvkům kritické informační infrastruktury, informačním systémům základní služby, proti významným

informačním systémům a vybraným informačním systémům veřejné správy

- řešení a koordinaci řešení kybernetických bezpečnostních incidentů u subjektů kritické infrastruktury, provozovatelů základní služby a orgánů veřejné správy
- osvětovou a vzdělávací činnost v oblasti kybernetické bezpečnosti
- spolupráci s národními i mezinárodními organizacemi podílejícími se na zajišťování bezpečnosti kybernetického prostoru
- pořádání a účast na kybernetických cvičeních na národní a mezinárodní úrovni
- výzkum a vývoj v oblasti kybernetické bezpečnosti
- vyhodnocování rizik v oblasti kybernetické bezpečnosti a přijímaní příslušných nápravných a preventivních opatření

Vládní CERT

Vládní CERT (GovCERT.CZ) a týmy typu CSIRT hrají klíčovou roli při ochraně kritické informační infrastruktury a významných informačních systémů podle zákona o kybernetické bezpečnosti (č. 181/2014 Sb.) a jeho prováděcích předpisů. Každá země, která má své kritické systémy připojeny do internetu, musí být schopna efektivně a účinně čelit bezpečnostním výzvám, reagovat na incidenty, koordinovat činnosti při jejich řešení a účelně působit při předcházení incidentům. [19]

Orgány a osoby, na které se vztahuje zákon o kybernetické bezpečnosti, musí plnit určité povinnosti vůči vládnímu CERT týmu a orgány a osoby podle § 3 písm. a) a b) plní povinnosti zejména vůči národnímu CERT týmu. Národní CERT tým zaštiťuje organizace CZ.NIC.

2.6.2 CZ.NIC, zájmové sdružení právnických osob

Zájmové sdružení právnických osob CZ.NIC bylo založeno předními poskytovateli internetových služeb v roce 1998 a nyní má již okolo 120 členů. Hlavními činnostmi sdružení jsou provozování registru jmen domén registrovaných pod doménou CZ, zabezpečování provozu domény nejvyšší úrovně .CZ a osvěta v oblasti jmen domén. V současné době se sdružení intenzivně věnuje rozšiřování technologie DNSSEC a služby mojeID, rozvoji systému správy domén a podpoře nových technologií a projektů prospěšných pro internetovou infrastrukturu v České republice. Sdružení provozuje také interní bezpečnostní tým CZ.NIC-CSIRT a od roku 2011 Národní CSIRT tým České republiky – CSIRT.CZ. V roce 2013 stál CZ.NIC u vzniku bezpečnostního projektu FENIX. CZ.NIC je členem sdružení EURid spravujícího evropskou doménu EU a dalších obdobně zaměřených mezinárodních společností (CENTR, ccNSO a další) [20].

CSIRT.CZ

CSIRT.CZ je Národní CSIRT České republiky. Národní CSIRT ČR je vykonávaný dle veřejnoprávní smlouvy uzavřené s Národním bezpečnostním úřadem. Ten se stal gestorem problematiky kybernetické bezpečnosti v říjnu 2011. Tým CSIRT.CZ plní úlohu národního CERT České republiky podle Zákona o kybernetické bezpečnosti. Národní CSIRT ČR je od 1. ledna 2011 provozován sdružením CZ.NIC. [21]

Tým CSIRT.CZ je členem mezinárodních uskupení CSIRT/CERT týmů. U Trusted Introducer je akreditovaný od roku 2011. V roce 2015 se tým CSIRT.CZ stal taky členem organizace FIRST.

Podle veřejnoprávní smlouvy s Národním bezpečnostním úřadem a Zákona o kybernetické bezpečnosti plní tým CSIRT.CZ úlohu Národního CERT týmu. Podle tohoto Zákona má tým následující povinnosti:

a) přijímá oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. a) a b) a tyto údaje eviduje a uchovává,
b) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. b) a tyto údaje eviduje, uchovává a chrání,
c) vyhodnocuje kybernetické bezpečnostní incidenty u orgánů a osob uvedených v § 3 písm. b),
d) poskytuje orgánům a osobám uvedeným v § 3 písm. a) a b) metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu,
e) působí jako kontaktní místo pro orgány a osoby uvedené v § 3 písm. a) a b),
f) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti.

Přehled činností CSIRT.CZ

- Řešení incidentů
- Informování o nákaze v doméně .CZ
- Skener webu
- Vzdělávaní
- Přednášky
- Pracovní skupiny
- Zátěžové testy
- Intrusion Detection systém
- Provozování honeypotů

2.6.3 Národní agentura pro komunikační a informační technologie, s. p.

Národní agentura pro komunikační a informační technologie, s. p. byla založena 1. února 2016 jako servisní organizace ministerstva vnitra České republiky. Poskytuje služby v oblasti informačních a komunikačních technologií s využitím více než 40 regionálních pracovišť. [22]

Statut agentury vymezuje široký rozsah činností a předurčuje NAKIT k vybudování nových kompetencí umožňujících např. informační a komunikační technologie nejen provozovat a udržovat, ale zároveň je dlouhodobě rozvíjet v souladu s potřebami jejich uživatelů.

Zajišťuje koncepční rozvoj kritické komunikační infrastruktury a bezpečné řešení sdílených služeb státu. Koncentruje klíčové ICT znalosti a tvoří moderní ICT organizaci. Níže jsou uvedeny ty nejdůležitější.

eGovernment

Komunikační a informační prostředí pro výkon veřejné správy.

- CMS – centrální místo služeb pro veřejnou správu
- DCeGov – dohledové centrum eGovernmentu
- KIVS – komunikační infrastruktura veřejné správy
- MORIS – modulární registr pro informační systémy
- Portál občana – centrální elektronické místo vstupu pro komunikaci občanů s úřady ČR

Integrovaný záchranný systém

Komunikační a informační prostředí pro zajištění činností IZS a bezpečnostních složek.

- ITS/ITS NGN – fixní hlasové a datové služby veřejné správy
- KSP – vybudování a modernizace operačních středisek HZS ČR
- NIS – integrace operačních středisek IZS
- PEGAS – mobilní radiokomunikační služby pro složky IZS

Resortní systémy

Interní ICT systémy v rámci ministerstva vnitra.

- EKIS – ekonomický informační systém MV
- ISoSS – informační systém o státní službě

2.6.4 Státní pokladna Centrum sdílených služeb, s. p. (SPCSS)

SPCSS je státní podnik, který vznikl za účelem plnit ICT strategii svého zřizovatele Ministerstva financí České republiky. Náplní SPCSS je funkce poskytovatele komplexních služeb bezpečného datového centra s geografickou redundancí odpovídající technické úrovně (Tier III dle Uptime Institutu) pro subjekty státní správy, a to v kvalitě srovnatelné nebo, zejména v oblasti fyzické a kybernetické bezpečnosti, převyšující nabídku komerčních datových center. Základem služeb SPCSS je služba Housingu pro ICT infrastrukturu zákazníků, která je dle požadavků zákazníků rozšířena o nadstavbové služby poskytnutí infrastruktury (IaaS), platformy (PaaS) nebo IT bezpečnosti (SECaaS). Nabízí komplexní řešení uzpůsobená potřebám našich zákazníků s důrazem na vysokou úroveň bezpečnosti a dostupnosti služeb. Služby SPCSS plně respektují požadavky na bezpečnost informačních systémů a soukromí jejich uživatelů a jsou v souladu se zákonem č. 181/2014 Sb., zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). [23]

V současnosti je většina služeb SPCSS poskytována subjektům v rámci resortu Ministerstva financí (tj. samotné Ministerstvo financí (MF), Generální finanční

ředitelství (GFŘ), Úřad pro zastupování státu ve věcech majetkových (ÚZSVM) a Generální ředitelství cel (GŘC)). Cílovou vizí je rozšíření využití nabízených služeb všemi orgány státní správy v rámci strategie Cloud computingu.

2.6.5 Národní centrála proti organizovanému zločinu SKPV

NCOZ SKPV je výkonným pracovištěm služby kriminální policie a vyšetřování s působností na celém území České republiky. V rámci své působnosti se specializuje na odhalování organizovaného zločinu, závažné hospodářské trestné činnosti a korupce, **kybernetické kriminality**, terorismu a extremismu. Ve vymezeném rozsahu je koordinačním, metodickým a kontrolním pracovištěm. Odhalováním a vyšetřováním organizovaného zločinu se podílí na bezpečnosti státu. V souladu se stanovenou podřízeností se podílí na řešení úkolů svěřených do působnosti Policejního prezidia ČR a Ministerstva vnitra ČR. [24].

V rámci NCOZ existuje sekce kybernetické kriminality, která se zaměřuje na trestnou činnost v oblasti kybernetické kriminality, která proniká do všech kriminálních oblastí, jelikož řada činností je uskutečňována ve virtuálním prostředí. Více informací v oblasti kyberkriminality naleznete ve Zprávě o činnosti NCOZ za rok 2018. [25]

2.6.6 Útvar zvláštních činností služby kriminální policie a vyšetřování

Útvar zvláštních činností služby kriminální policie a vyšetřování (dále jen „ÚZČ SKPV“) je útvarem Policie České republiky, který v souladu s příslušnými ustanoveními trestního řádu, zákona o Policii České republiky a dalších právních předpisů provádí ve prospěch oprávněných bezpečnostních subjektů odposlech a záznam telekomunikačního provozu, sledování osob a věcí a další specializované úkony. [26].

Kromě výkonných pravomocí má útvar i metodickou působnost v problematice sledování osob a věcí a v souladu s interními akty řízení policejního prezidenta řídí a technicky zajišťuje činnost systému centralizované ochrany. Vzhledem k výlučné působnosti v oblasti odposlechu a záznamu telekomunikačního provozu má nezastupitelnou roli při soustřeďování podkladových údajů pro zpracování pravidelné statisticko-analytické zprávy.

2.6.7 Velitelství kybernetických sil a informačních operací

Kybernetické síly a informační operace (KySIO) přispívají k bezpečnosti a obraně České republiky v kybernetickém prostoru a informačním prostředí. Působí nezávisle, společně nebo v součinnosti s pozemními, vzdušnými a speciálním silami. [27]

Na taktické úrovni monitorují, plánují a řídí operace v kybernetickém prostoru a v informačním prostředí, včetně podpory strategické komunikace AČR. KySIO zahrnují schopnosti ochrany vlastních částí kybernetického prostoru, informačních operací, informačních operací v kybernetickém prostoru, psychologických operací a civilně vojenské spolupráce.

Při ochraně kybernetického prostoru a vedení vojenských kybernetických operací úzce spolupracují s vojenským zpravodajstvím, kde se schopnosti vzájemně doplňují.

2.6.8 Vojenské zpravodajství

Vojenské zpravodajství (VZ) je jednotnou ozbrojenou zpravodajskou službou České republiky. Jako jediná česká zpravodajská služba integruje jak rozvědnou, tak kontrarozvědnou činnost. [28]

Od roku 2015 je Vojenské zpravodajství na základě rozhodnutí vlády garantem kybernetické obrany České republiky. Za tímto účelem buduje Vojenské zpravodajství Národní centrum kybernetických operací (NCKO), jehož úkolem je vytvoření účinného systému obrany v kybernetickém prostoru tak, aby Česká republika byla v případě kybernetického útoku schopna zabezpečit ochranu civilního obyvatelstva a infrastruktury.

VZ vypracovalo strategii kybernetické obrany pro období 2018–2022 pro řádné zajišťování obrany státu v kyberprostoru. [29]

V současné době je v legislativním procesu návrh změny zákona č. 289/2005 Sb., o Vojenském zpravodajství, ve znění pozdějších předpisů, jenž jde cestou definování pojmu kybernetické obrany, svěření jejího zajišťování Vojenskému zpravodajství jako součásti Ministerstva obrany a úpravy prostředků, které budou sloužit k zajišťování kybernetické obrany. [30]

2.6.9 Poskytovatelé internetu

Poskytovatelé internetového připojení (ISP) jsou subjekty zprostředkující přístup k internetu a jeho obsahu.

První skupinu ISP jsou poskytovatelé připojení, mezi které patří mobilní operátoři a operátoři pevných linek, kteří zajišťují připojení koncových účastníků do internetu. Česká republika má více jak tisíc poskytovatelů a na základě Zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) jsou registrováni u Českého telekomunikačního úřadu. Např. O2, T-Mobile, České Radiokomunikace, Dial Telecom apod.

Do této skupiny řadíme ještě skupinu tzv. tranzitních operátorů (Tier 1 a 2), kteří zajišťují propojení mezi ISP v dané zemi či celosvětově. Např. Telia, Core Backbone, Level 3, Verizon, GTT apod.

Druhou skupinou ISP jsou poskytovatelé obsahu, kteří zajištují připojení žádaného obsahu v internetu, a to především obsahující audio, video nebo data. Např. Seznam, YouTube, Google, Facebook, Uloz.to apod.

Skrze jednotlivá ISP prochází internetový provoz, a tudíž se podílejí na jeho samotném přenosu a zabezpečení. ISP jsou tedy klíčovými hráči na poli kybernetické bezpečnosti.

Dalšími subjekty v internetu jsou též tzv. „Neutral Internet Exchange" body v dané zemi, které sdružují ISP a vytváří tzv. přímé propojovací uzly mezi ISP. V ČR se jedná o NIX.CZ nebo Peering.cz. Důvodem vzniku těchto uzlů je využití přímého propojení ISP oproti placení poplatků na bázi 95th percentilu za propojení skrze tranzitní operátory a to především, když jde o lokální komunikaci v dané zemi.

3 CÍL PRÁCE

Hlavním cílem bakalářské práce je popis a analýza stavu kybernetických hrozeb v České republice se zaměřením na kritickou informační infrastrukturu.

V teoretické části budou vymezeny základní pojmy kybernetické bezpečnosti a kritické informační infrastruktury. Dále pak budou uvedeny subjekty podílející se na zajištění kybernetické bezpečnosti České republiky.

Jednotlivé kybernetické hrozby budou popsány a analyzovány dle jejich dopadu, použité metody, typu útočníka a cíle hrozby.

Detailní rozbor pak bude proveden ke kybernetické hrozbě Distributed denial-of-service (DDoS) a jeho dopadu na kritickou informační infrastrukturu. Následně bude navržen způsob ochrany proti této hrozbě.

4 METODIKA

Metodiku, kterou jsem použil, byla analýza jednotlivých typů kybernetických hrozeb. Každá kybernetická hrozba obsahuje vlastní popis, jaký má dopad, použité metody útočníka, typ útočníka a cíle hrozby.

V případě hrozby DDoS obsahuje analýza navíc dostupné nástroje útočníka a způsob detekce a ochrany proti konkrétní použité metodě.

Na závěr jsem uvedl přehled doporučení, která snižují nebo eliminují riziko DDoS útoků.

5 VÝSLEDKY

5.1 Kybernetické hrozby – analýza

Kybernetické hrozby jsme si popsali v kapitole 2.4. V následujících kapitolách provedeme jejich analýzu dle metodiky v kapitole 4. (Dopady, Metody, Útočník, Cíl). Analýzu hrozby DDoS rozebereme do většího detailu v samostatné kapitole 5.2.

5.1.1 Umělá inteligence a sítě 5G

Díky rozvoji umělé inteligence dochází k automatizaci mnoha činností, zpracování a vyhodnocení velkého množství dat v reálném čase. Sítě 5. generace ve spojitosti s IoT představují nekonečné množství systémových zařízení, která budou spolu komunikovat. Toto přinese velké možnosti jak útočníkům, tak i obráncům.

Dopady

odcizení osobních údajů, krádež identit, narušení důvěrnosti, dostupnosti nebo integrity informací, ztráta dat, kompromitace citlivých a utajovaných informací, nelegitimní využívání výpočetního výkonu obětí, narušení dostupnosti služeb, finanční ztráty, poškození konkurence, ztráta dat, kompromitace strategických informací, ohrožení konkurenceschopnosti, sabotáž

Metody

phishing, spear-phishing, DDoS, útoky hrubou silou

Útočník

státní aktéři, státem sponzorované skupiny, kyberzločinci, script kiddies

Cíl

uživatelé, veřejný sektor, kritická infrastruktura, finanční sektor, energetický sektor, zdravotnictví, školství

5.1.2 Úniky dat

Nebezpečí úniku dat je především v jeho případném dalším zneužití. Nejvíce žádané jsou osobní údaje uživatelů a přihlašovací údaje do aplikací. Odcizené informace jsou zneužívány k dalším útokům.

Dopady

odcizení osobních údajů, jejich možné zneužití k následným spear phishingovým útokům, krádežím identit

Metody

útoky hrubou silou, SQL injection a další

Útočník

státní aktéři, státem sponzorované skupiny, kyberzločinci, script kiddies, teroristé

Cíl

Uživatelé, veřejný sektor, finanční sektor, energetický sektor, zdravotnictví, školství

5.1.3 Dodavatelský řetězec

Útoky na dodavatelský řetězec je v současné době na vzestupu. Útok na tuto skupinu může být potencionálně zneužit k získání přístupu k veřejným i privátním institucím. Jedná se o zneužití nejslabšího článku v dodavatelském řetězci. V dnešní době bylo zaznamenáno několik útoků na používání tzv. managed služeb, a to především Cloud computingu. Dále pak legislativně nešťastně uchopen zákon o veřejných zakázkách, kde v mnoha případech je upřednostněna cena před bezpečností.

Dopady

ztráta dat, kompromitace strategických informací, ohrožení konkurenceschopnosti, sabotáž

Metody

phishing a spear-phishing na zaměstnance dodavatelských společností

Útočník

státní aktéři, státem sponzorované skupiny

Cíl

dodavatelské subjekty pro veřejný sektor, kritická infrastruktura, finanční sektor, energetický sektor, zdravotnictví

5.1.4 Kybernetická špionáž

Kybernetická špionáž představuje škodlivé aktivity s cílem získat citlivé informace bez souhlasu jeho držitele. Odcizené informace mohou být zneužity k dalším útokům. Např. zneužití emailové schránky k rozesílání infikovaného obsahu nebo zneužití přístupových údajů pro přístup do dalších systémů organizace. Snahou útočníků je zůstat v systému oběti dlouhodoběji nezpozorován.

Dopady

ztráta dat, kompromitace citlivých a utajovaných informací, ztráta obchodních tajemství vedoucí ke ztrátě konkurenceschopnosti

Metody

zranitelnosti nultého dne, pokročilé spear-phishingové kampaně

Útočník

státní aktéři, státem sponzorované skupiny

Cíl

veřejný sektor, kritická infrastruktura, finanční sektor, energetický sektor, zdravotnictví, školství

5.1.5 Kryptomining

Kryptomining je hrozba, která zneužívá výpočetní prostředky počítačových systémů k těžbě kryptoměn. Jedná se malware, který je před uživateli skryt. Hlavní motivací útočníka je zisk.

Dopady

nelegitimní využívání výpočetního výkonu obětí, bez zřetelných dopadů na důvěrnost a integritu, hypotetická možnost omezení dostupnosti informačních systémů

Metody

útok na výpočetní výkon napadených zařízení nebo napadení webové stránky využívající počítač návštěvníka

Útočník

kyberzločinci

Cíl

výpočetní prostředky uživatelů

5.2 Distributed Denial of Service (DDoS)

5.2.1 Co je to DDoS útok?

Jako Denial of Service (DoS) útoky jsou dnes označovány útoky, jejichž základním cílem je znepřístupnit nebo narušit plynulý chod on-line služeb legitimním uživatelům. V případě velkého množství útočících zařízení mluvíme o distribuovaném útoku, který označujeme jako DDoS.

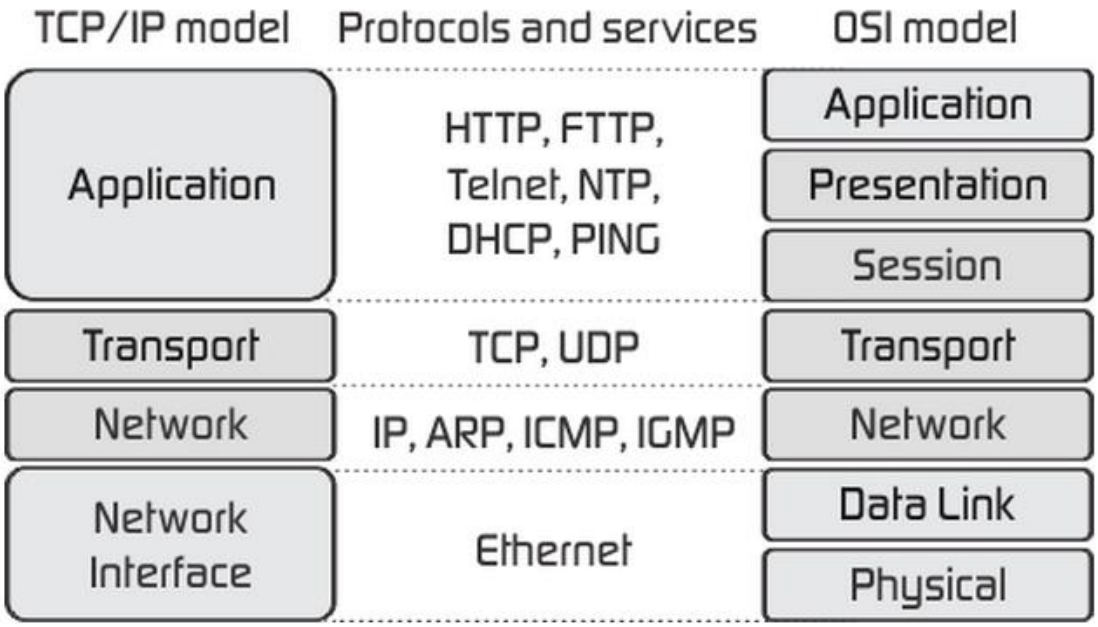
Nejčastější formou DDoS útoků jsou tzv. volumetrické útoky. Při těchto útocích dochází k přetížení serverů a zahlcení přístupových linek či síťových zařízení falešným datovým provozem.

Druhou, neméně nebezpečnou formou útoku jsou tzv. aplikační útoky. V případě aplikačního útoku se na rozdíl od volumetrického útoku nejedná o významné zvýšení objemu přenášených dat, ale o mnohonásobný nárůst požadavků směřující na infrastrukturu oběti. Útočník využívá některou ze známých zranitelností cílového systému, jejíž zneužití vede k přetížení nebo pádu aplikačního serveru nebo služby.[35]

Cílem útoků typu DoS/DDoS obvykle není infikovat počítačový systém nebo překonat bezpečnostní ochranu např. heslem, které jej chrání, ale pomocí série opakovaných požadavků jej buď zahltit, či dočasně vyřadit z provozu. Typicky tak dojde k omezení či zablokování přístupu ke službám.

Pro tyto účely existuje několik open source nástrojů nebo je možné si objednat DDoS útok jako službu (DDoS-as-a-Service) za pár dolarů.[45]

Pro pochopení různých druhů DDoS útoků potřebujeme znát základní koncept End-to-end komunikace, která vychází ze základního OSI modelu nebo TCP/IP modelu. Na obrázku níže je uveden vzájemný vztah a jednotlivé komunikační protokoly na daných vrstvách modelů.



Obrázek 2- Schéma OSI a TCP/IP modelu [36]

Dopady

narušení dostupnosti služeb, poškození konkurence, finanční ztráty, odlákání pozornosti od jiného útoku

Metody

botnety, DNS amplification, UDP/TCP Flood, HTTP flood aj. viz. níže

Útočník

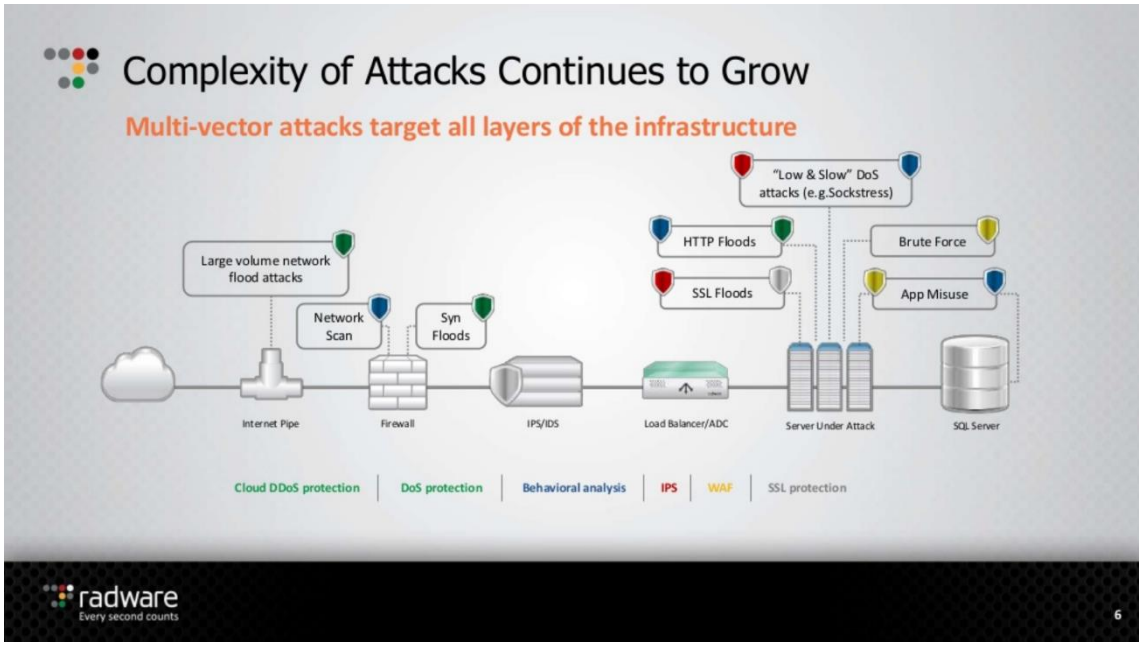
státní aktéři, státem sponzorované skupiny, hacktivisté, script kiddies, teroristé, kyberzločinci

Cíl

veřejný sektor, kritická infrastruktura, finanční sektor, energetický sektor, zdravotnictví, školství, ISP, dodavatelský řetězec, cloud, gaming

5.2.2 Rozdělení útoků

Na následujícím obrázku je znázorněna infrastruktura zákazníka a potencionální DDoS hrozby.



Obrázek 3 - Infrastruktura a DDoS hrozby[42]

Fyzická a linková vrstva

Na těchto vrstvách nemůžeme mluvit o DDoS útoku jako takovém. Zde připadá v úvahu pouze fyzické rozpojení infrastruktury nebo přerušení dodávky elektrické energie. To může být způsobeno pouze interně, a to buď chybou zaměstnance nebo jeho úmyslem.

V případě linkové vrstvy se bavíme pouze o lokálním segmentu infrastruktury. Potenciální hrozbu mohou tvořit interní komunikační systémy, které byly kompromitovány útočníkem, kde útočník získal přístup.

Síťová vrstva

Typickým příkladem útoku na této vrstvě je zahlcení s využitím ICMP protokolu. Jedná se o základní komunikační protokol. Útočník zasílá na cílový server vysoké množství ICMP paketů různého typu. Pro účely zjištění dostupnosti a doby odezvy se používá služba Ping. Bohužel se tato služba dá zneužít, mluvíme o útoku označovaném jako „**Ping Flood nebo ICMP Flood Attack**“. Cílové zařízení obdrží velké množství tzv. ICMP Echo Request paketů, na které zpětně odpovídá pomocí tzv. ICMP Echo Replay paketů. Při tomto útoku dochází k zahlcení linky a výpočetního výkonu cílového zařízení.[43]

„Smurf attack“ využívá též ICMP protokol. Útočník zasílá ICMP Echo na adresu broadcastu sítě s podvrženou zdrojovou adresou na adresu oběti. Tím dojde k odpovědi na dotaz od všech zařízení v lokální síti.

Pro generování těchto útoků je běžně utilitu Ping popř. nástroj hping. Omezení je možné provést pomocí filtrace určitých ICMP zpráv a nastavením filtru na limit ICMP zpráv za určitý čas.

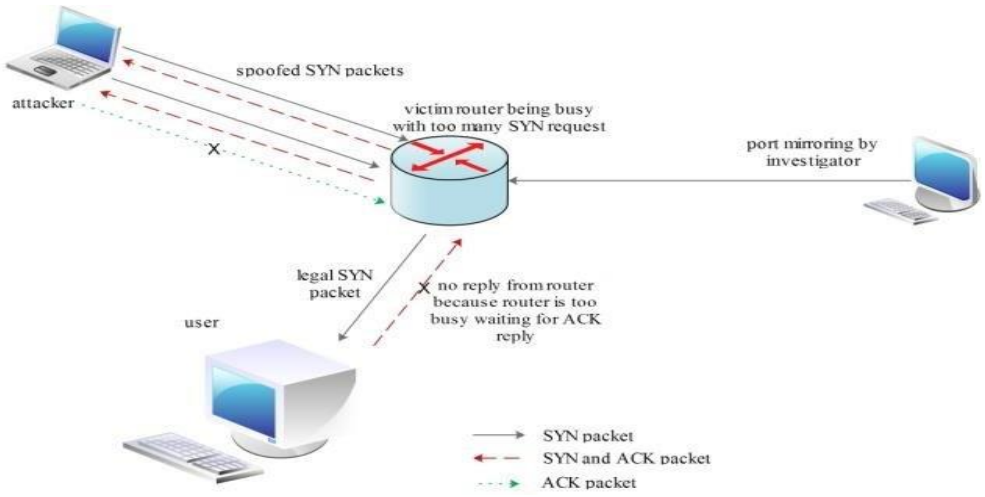
Transportní vrstva

Útoky na transportní vrstvě zneužívají transportní protokoly TCP (Transmission Control Protocol) a UDP (User Datagram Protocol). V případě stavového protokolu TCP je útok veden přes sestavování spojení (**TCP SYN Flood**) nebo je útok směrován na ukončení samotného spojení (**TCP RST Attack**), dále (**TCP ACK Flood**) podvržení neexistujících spojení nebo (**TCP Window Size**

Attack) k oznámení nemožnosti zaslání dat. V případě nestavového protokolu UDP dochází ke klasickému zahlcení cílového systému bez ověřování spojení (**UDP Flood Attack**).

TCP SYN Flood

TCP SYN Flood je útok, kdy se útočník snaží cílový systém zahltit velkým množstvím žádostí o navázání spojení. Útočník pošle posloupnost paketů s příkazem SYN cílovému systému, přičemž cílový systém na každý SYN paket odpoví zasláním SYN-ACK paketu, a útočník zpět již neodpoví. Cílový systém čeká na finální potvrzení, tzv. ACK paket od útočníka a drží pro toto spojení alokované zdroje, kterých má ale omezené množství. Tím může dojít k vyčerpání systémových zdrojů cíle útoku. Na obrázku níže je uvedeno schéma útoku.



Obrázek 4- TCP SYN flood attack [37]

TCP ACK Flood

TCP ACK Flood útok posílá na server oběti velké množství falešných ACK paketů, které nemají souvislost s žádnou aktuálně otevřenou relací. V důsledku toho dojde k vyčerpání systémových zdrojů sloužících k vyhodnocování příchozích paketů a následně ke snížení výkonu nebo jeho úplnému zhroucení.

V případě Fragmented ACK flood útoku se využívá paketů o velikosti 1500 bajtů k tomu, aby zahltil relativně velkou šířku přenosového pásma. [35]

TCP RST Flood

TCP RST útok je útok na sestavená spojení mezi klientem a serverem, kde útočník odhaduje sekvenční čísla TCP spojení a v případě, že se shoduje, spojení se ukončí. Předpokladem tohoto útoku je znalost IP adresy zdrojového systému.

TCP Window Size

TCP Window Size útok využívá zranitelnosti v TCP protokole. Velikost TCP okna je domluvena mezi zdrojem a cílem komunikace, což představuje množství dat, které je mezi nimi zasláno, aniž by muselo být potvrzeno. Tímto je řízen přenos dat v síti v závislosti na kvalitě spojení/ztrátovosti.

V případě, že je útočníkem nastavena velikost TCP okna na 0, je cílovému systému sděleno, aby neposílal žádná data. Cílový systém periodicky posílá kontrolní dotazy k ověření dostupnosti zdroje. V tomto případě však zdroj nebude nikdy dostupný a cílový systém musí stále držet spojení v paměti. Tímto způsobem může dojít k vyčerpání místa v tabulce spojení a dojde tak odepření přístupu dalším uživatelům.

UDP Flood Attack

Tento protokol má na starosti komunikaci v síti, podobně jako TCP. Oproti protokolu TCP ale nevyužívá ověřování navázání, průběhu a vypršení času komunikace. Je díky tomu podstatně rychlejší, ale na druhou stranu také snadno zneužitelný k útoku typu UDP Flood Attack.

V případě UDP Flood útoku útočník pošle velké množství UDP paketů na náhodné porty cílového systému, který musí na tyto UDP pakety zareagovat. Zkontroluje, zda jsou tyto porty otevřeny nějakou z jeho aplikací. Pokud tomu tak není, zasílá zpět informaci, že cílová destinace není dostupná. K tomu se využívá ICMP protokol, který slouží pro odesílání chybových zpráv.

Oblíbeným nástrojem pro generování flood útoků je např. Low Orbit Ion Cannon (LOIC), High Orbit Ion Cannon (HOIC) a hping. Jako obranu proti těmto útokům je vhodné použít DDoS sondy v kombinaci Scrubbing centra. Dále pak využití např. BGP FlowSpec.[44]

Aplikační vrstva

V případě aplikační vrstvy dochází k útokům na samotné aplikace cílového systému. Útoky jsou zaměřeny především na vyčerpání systémových zdrojů a zamezení přístupu běžným uživatelům. Především jsou zneužity bezpečnostní chyby a špatná konfigurace aplikací.

Útoky na aplikační vrstvě jsou většinou prováděny s určitým záměrem, jako je např. přerušení transakcí nebo přístupu do databáze. Na rozdíl od volumetrického útoku není tento typ útoku tak náročný na realizaci. Útočníkovi k němu zpravidla postačí mnohem méně zdrojů, přičemž potřebuje pouze dostatečný počet útočících strojů. Během útoku se útočník snaží, aby si napadený server myslel, že se jedná o běžný provoz, ale přitom se zaměřuje na specifické zranitelnosti cílové aplikace. Mezi nejrozšířenější útoky tohoto typu patří tzv. HTTP Flood Attack a Slowloris Attack. [38]

HTTP Flood

HTTP Flood útok cílí především na služby webových serverů. Útočník při tomto typu útoku vysílá velké množství legitimních HTTP GET nebo POST paketů, čímž se snaží maximálně vytížit zdroje cílového systému. Výsledkem je pokles výkonu, navýšení odezvy a mnohdy dokonce nedostupnost serveru.

Slowloris

Útok typu Slowloris otevře mnoho síťových spojení a snaží se je udržet otevřená co nejdéle. Http požadavky posílá velice pomalu, po částech a těsně před vypršením časového limitu. Server drží tato spojení otevřená, ale vzhledem k faktu, že může zároveň držet otevřený jen omezený počet spojení, musí další požadavky na spojení odmítat a zbytku světa je tak nedostupný. Tento typ útoku je velmi těžké odhalit, protože k žádné zjevné abnormalitě vlastně nedošlo – na serveru je vše v pořádku, tedy až na to, že nezvládá obsluhovat příchozí požadavky.

SSL Attack

Útoky na SSL jsou dnes velmi oblíbené, neboť konzumují velmi velké množství systémových zdrojů cílového systému. Jedná se o webové servery s podporou HTTPS. Útočník se snaží navázat mnoho SSL spojení, která konzumují velké množství výpočetního výkonu a paměti. Další alternativou je opakovaná negociace SSL spojení.

DNS Amplification

Dalším velice oblíbeným útokem je DNS Amplification útok. Tento útok využívá k zesílení svého účinku tzv. otevřené resolvery, což jsou DNS servery

poskytující své služby nejen uživatelům své vlastní sítě, ale i uživatelům nacházejícím se mimo ni. Útočník z podvržené IP adresy, která je identická s IP adresou oběti, zasílá na tyto DNS servery velké množství poměrně malých dotazů, což má za následek to, že oběť je následně zahlcena množstvím několikanásobně větších odpovědí, které si ve skutečnosti nevyžádala. Vzhledem k rozdílům ve velikosti mezi zasílanými a přijímanými dotazy může útočník bez problémů zahltit rychlejší linku oběti, i když sám má pomalejší linku.

Nástroje pro generování útoků je např. Low Orbit Ion Cannon (LOIC), High Orbit Ion Cannon (HOIC), Slowloris a R U Dead Yet? (R.U.D.Y.), ddos-toolbox

Jako obranu proti těmto útokům je vhodné použít DDoS sondy, WAF, monitorování aplikací, CAPTCHA.

5.2.3 Techniky použití DDoS útoků

V minulé kapitole jsme se seznámili s jednotlivými typy DDoS útoků v závislosti na referenčních modelech OSI a TCP/IP. V současné době se používá kombinace těchto útoků a mění jejich parametry. Pro vyšší efektivitu DDoS útoku se využívají následující techniky.

IP Spoofing

IP Spoofing spočívá v podvrhování zdrojové adresy odesílaných paketů, kdy útočník iniciující spojení jako zdrojovou adresu do odesílaných paketů vloží falešnou IP adresu a odešle je cílovému systému. Cílový systém pak odpovídá na tuto podvrženou zdrojovou adresu. To samozřejmě komplikuje efektivní obranu proti tomuto útoku.

Amplifikační útoky

S amplifikačními útoky jsme se seznámili u DNS Amplification útoku. Tyto útoky umožňují zesílení velikosti paketů nebo počtu paketů. Velice oblíbeným je právě DNS nebo NTP protokol, kde dochází k zesílení v řadu stovek datového provozu. V nedávné době byl velmi oblíbený útok s využitím Memcached serverů, kde může docházet až k zesílení 51000.

Botnet

Botnet představu síť kompromitovaných koncových zařízení malwarem. Útočník získal kontrolu na těmito zařízeními – boty a je schopen pomocí nich provést DDoS útok. Botnet může obsahovat i milion koncových zařízení. S rozvojem IoT (Internet of Things) je počet botů v budoucnu neomezený. Jedná se většinou o jednoúčelová zařízení, která se stala nedílnou součástí života moderních domácností jako např. webkamery, dětské chůvičky, set-top boxy, chytré televize, nebo řídící jednotky chytrých domácností. Nedostatečné zabezpečení přibližně jedné miliardy takových zařízení připojených k internetu, vytváří prostředí, které může být zneužito k DDoS útokům.

5.3 Návrh řešení ochrany proti DDoS útokům

Správná ochrana proti DDoS útokům musí být postavena na kombinaci organizačních a technických opatření.

5.3.1 Organizační opatření

Přehled doporučených opatření:

- Vlastní CSIRT tým – skupina administrátorů, která řeší bezpečnostní incidenty, komunikace směrem k
    - Vládní CERT (GovCERT.CZ) - cert.incident@nukib.cz;
    - Národní CSIRT (CSIRT.CZ) - abuse@csirt.cz.
- Fungující a zavedený systém řízení bezpečnosti informací v organizaci dle ISO/IEC 27001
- Soustavné vzdělávaní a školení administrátorů v kyberbezpečnosti
- Účast na kybernetických cvičeních (CZ.NIC, NÚKIB)

Měli bychom znát odpovědi na následující otázky:

Jak rychle jste schopni zaznamenat/diagnostikovat incident za pomoci analýzy síťových dat, logů ze serverů, IPS, firewallu? Sbíráte a uchováváte tyto logy?

Jak rychle jste schopni zajistit spolupráci Vašeho poskytovatele internetu? Víte, co pro Vás v případě útoku může udělat, koho máte kontaktovat a jak bude probíhat eskalace dále?

Máte připravené procedury, včetně všech potřebných kontaktních údajů a jednotlivých rolí pro případ, že útok nastane?

Provozujete odděleně infrastrukturu služeb běžících na internetu od služeb běžících pouze interně? Nebude dotčena interní část v případě útoku na veřejné služby?

Zvážili jste možnosti rychlého navýšení kapacity serverové farmy a internetové konektivity? Popřípadě možnost využití privátního nebo veřejného cloudu?

Víte o limitech své sítě, úzkých místech a neredundantních prvcích? Neobsahuje Vaše páteřní síťová infrastruktura SPOF (Single Point Of Failure)?

Umí Vaše zařízení zpracovávat SYN-cookies (jedná se o obranu proti DDoS útoku typu SYN flood)?[40]

5.3.2 Technická opatření

Konektivita, připojení do internetu

Jak již bylo dříve popsáno, významná síť představuje síť zajišťující přímé připojení ke kritické informační infrastruktuře. Významnou síť dnes představují ISP, kteří zajišťují konektivitu do dalších sítí a připojení k internetu.

Z hlediska vyšší dostupnosti je vhodné používat minimálně 2 ISP pro připojení k internetu. Dalším doporučením je, aby správce nebo provozovatel KII byl tzv. LIR providerem, tj. byl vlastníkem IP adresního rozsahu a měl vlastní Autonomní systém (AS), tak aby nebyl závislý na ISP a mohl na hraničních směrovačích svého AS řídit směrovací politiku z a do internetu.

Správce nebo provozovatel KII by měl používat technologie, které zajišťují ochranu proti DDoS v rámci své infrastruktury na perimetru sítě. Bohužel proti volumetrický útokům je třeba se chránit blíže k internetu, tzn. tuto službu musí poskytovat ISP v rámci své infrastruktury nebo využít specializovaných „Scrubbing center“, které jsou schopny tento typ útoků omezit či zablokovat.

FENIX

Projekt FENIX vznikl na půdě českého peeringového uzlu, sdružení NIX.CZ, v roce 2013 jako reakce na intenzivní DoS útoky, kterým v březnu tohoto roku čelila významná česká média, banky nebo operátoři. Smyslem projektu je umožnit v případě DoS útoku dostupnost internetových služeb v rámci subjektů zapojených do této aktivity.

Účast v projektu FENIX je spojená s řadou podmínek, které jsou zakotveny v pravidlech. Společnosti zapojené do tohoto projektu svým vstupem jasně ukazují, že mají zájem na zvýšení síťové bezpečnosti, a tedy i na větším bezpečí svých zákazníků. Projekt je určen společnostem, které poskytují připojení významným službám a potřebují zabezpečit jejich provoz i v těch nejkritičtějších situacích.[41]

Při volbě poskytovatele internetu je vhodné preferovat tyto subjekty, neboť více kladou důraz na kybernetickou bezpečnost a zároveň jsou schopny rychle kooperovat při útocích v českém kyberprostoru. Aktuální počet členů je 27.

Ostrovní režim a GeoIP

Jelikož většina KII poskytuje služby pro stát či občany v ČR, je vhodné v případě útoku selektivně omezovat přístup pouze z daného regionu a z vybraných IP adres, a tudíž přejít do (polo)ostrovního režim. IP adresní plán je přidělovaný v rámci daného regionu. (v Evropě je to organizace RIPE). Na základě ISP subjektů v ČR, jejich AS a IP adresních rozsahů jsme schopni určit konečnou množinu IP adres, které mohou představovat legitimního uživatele nebo útočníka. Pomocí služby GeoIP můžeme tento rozsah identifikovat a využít formou white-listů ve filtrovacích pravidlech směrovačů a firewallů.

Síťové sondy a monitoring

Nasazení síťových sond v prostředí zákazníka je základním stavebním kamenem. Síťové sondy sbírají provozní informace z jednotlivých datových spojení. Tyto provozní informace se předávají do kolektoru nástroji, který provádí jejich analýzu a detekci útoků. Pro tyto účely se využívá především protokol NetFlow/IPFIX. Na základě detekce útoku, je možné následně aplikovat filtr na síťová zařízení.

Využití protokolu NetFlow je sice efektivní, ale reakce je velice pomalá v řádu minut. Pro rychlejší detekci (v řádu sekund) je třeba analyzovat „živý provoz“, nicméně to může vyžadovat vysoké nároky na výpočetní prostředky a datové uložiště. Ty je možné snížit například sběrem dat s vyšší hodnotou vzorkování (např. 1:100, analyzuje se každý stý paket).

Monitoring sítě a datových toků je základní předpoklad obrany proti DDoS útoků. Znalost vlastního prostředí a datové komunikace je nutností. Pro tyto účely většinou zákazník využívá management síťové infrastruktury dodané výrobcem technologie nebo open source nástrojů upravených pro vlastní potřebu.

DDoS sondy

DDoS sondy jsou zařízení, kterými prochází datový provoz. Tyto sondy obsahují detekční modul a signatury známých DDoS útoků a jsou schopny velice rychle reagovat. Dále si vytvářejí tzv. baseline provozu, což představuje standardní datový provoz v době míru a jsou schopny reagovat na změny oproti této baseline. Pokud baseline neexistují nebo jsou špatně nastavena může sonda reagovat velkým množství false-positive nebo naopak nereagovat na daný útok.

Tyto DDoS sondy umějí pracovat jak s volumetrickými útoky, tak i aplikačními útoky.

Srubbing centrum

V případě volumetrických útoků jsou DDoS sondy ve vlastní síti neefektivní, neboť dojde k ucpání přístupové linky. Pro tyto účely je hodné využít „Scrubbing center“, které poskytují ISP nebo specializované firmy na DDoS ochranu. Provoz z internetu je přesměrován do těchto Scrubbing center, kde je vyčištěn od těchto útoků a následně přeposlán zákazníkovi. Tato Scrubbing centra disponují speciálními DDoS zařízeními a mají vysokou kapacitu tranzitních linek do internetu v řadu stovek nebo tisíců Gbit/s.

BGP

BGP je směrovací protokol, který se používá v internetu k zajištění výměny směrovacích informací mezi autonomními systémy (AS). AS představuje síť nebo skupinu sítí s jednotnou technickou a administrativní správou a jednotnou směrovací politikou. Autonomní systémy mezi sebou navazují dvoubodové BGP relace. Protokol BGP tedy používají ISP nebo zákazník na hraničních směrovačích do internetu.

RTBH

Remote Triggered Black Hole (RTBH) technika je hojně používaná v sítích ISP, ale lze ji poměrně jednoduše aplikovat i v běžných LAN sítích, které obsahují více směrovačů. RTBH filtrování je postaveno na tom, že jeden RTBH směrovač šíří prostřednictvím protokolu BGP informace o IP adresách, které mají být blokovány ostatním směrovačům, které daný provoz na tuto adresu zahodí.

Nevýhodou RTBH je zablokovaný veškerý provoz na danou IP adresu/rozsah. Proto je třeba tuto techniku používat obezřetně. Podrobněji je RTBH popsáno v RFC 5635. Alternativou k RTBH je možnost využít komplexnější variantu FlowSpec.

FlowSpec

FlowSpec je rozšířením protokolu BGP a definují ho RFC 5575 a 7674. Umožňuje distribuovat filtrovací pravidla a je více škálovatelný než RTBH. Podporuje parametry jako je zdrojová a cílová adresa, IP protokol, zdrojový a cílový port, typ a kód ICMP, TCP flagy, délka paketů a další. V případě detekce útoku vznikne jeho signatura, na jejím základě se pak přidá pomocí BGP FlowSpec do směrovače filtrovací pravidlo a útok je zablokován.

Výhodou FlowSpecu je vytvoření konkrétního specifického filtru dle signatury útoku, tzn. omezujeme pouze specifický provoz na danou IP adresu. Nevýhodou je naopak malá podpora ze strany ISP, kdy se snažíte pomocí FlowSpecu propagovat filtr na hraniční směrovač ISP.

Aplikační ochrana

V případě útoků na aplikační vrstvu se primárně bavíme o webovém provozu (HTTP/HTTPS). Velmi oblíbený prostředkem v enterprise segmentu jsou WAF a ADC řešení, která se však musí přizpůsobit dané aplikaci a pravidelně aktualizovat. V případě aplikačních útoků je důležitější sledovat spíše počet spojení než šířku pásmu, kterou útok zabírá. Útoky na aplikační většinou nezabírají takovou šířku pásma a jsou tak lehce přehlédnutelné, naopak velký počet dotazů a spojení může danou službu velice rychle udělat nefunkční.

Primárně se musíme zaměřit na HTTP GET/POST požadavky. Důležitými parametry z hlediska aplikace je počet současně připojených uživatelů, počet nově vytvořených spojení za sekundu, průměrný počet paketů na dotaz a časové limity dotazů. V případě POST požadavku též velikost a počet souborů.

5.4 Ochrana kritické informační infrastruktury

Úspěšná ochrana kritické informační infrastruktury rozhodující měrou závisí na připravenosti. Proti některým útokům se lze bránit velmi obtížně, pokud vůbec. Jedná se o útoky využívající dosud neznámých zranitelností, případně zranitelností, vůči nimž dosud neexistuje ochrana. Základem ochrany je jejich co nejrychlejší odhalení, například prostřednictvím vyhledávání anomálií provozu autonomními sondami.

Organizační opatření vycházejí ze stejného principu jako u hrozby DDoS, která je jednou z klíčových hrozeb pro KII. Technická opatření jsou závislá na typu kybernetické hrozby, které jsou popsány v předešlých kapitolách.

KII je z velké části spojená s již určenými prvky kritické infrastruktury identifikovanými zejména v oblastech energetiky, veřejné správy, elektronických komunikací a finančního trhu a měny. Nastane-li krizová situace (KS) v oblasti kybernetické bezpečnosti, může mít dopad na funkčnost subjektu KI a mít tak dopad na jeho fungování a služby.

KS způsobené narušením bezpečnosti informací v KII jsou z hlediska procesu řešení podobné. Řeší je zpravidla zasažený subjekt, NÚKIB a další instituce na centrální úrovni státu. Povaha KS je přímo závislá i na způsobu narušení bezpečnosti informací KII, kdy různé způsoby narušení mohou způsobit různé efekty, a tudíž je nutné k nim přistupovat individuálně.

Proces řešení KS způsobené narušením informací v KII je z podstaty věci nutné vést ve dvou rovinách. Následky ve fyzickém světě (tedy zapojení složek IZS a další procesy dle zákona č. 240/2000 Sb., krizového zákona) bude zpravidla řešeno do jisté míry odděleně od následků v kyberneticko-bezpečnostní rovině (tedy řešení incidentů dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti).

Zvládání KS způsobené narušením bezpečnosti informací v KII je nutné řešit z hlediska zvládání důsledků, které narušení KII způsobuje (tj. např. výpadek elektřiny, výpadek telekomunikačních služeb, nedostupnost dalších kritických služeb). To je řešeno postupy dle souvisejících typových plánů.

Dále je třeba se zaměřit na řešení příčiny a nápravu fungování systému KII. Především musíme uvažovat časový rozsah narušení bezpečnosti informací v informačních systémech, důsledek narušení bezpečnosti informací pro činnost KII, postupy a činnosti, které jsou pro zvládnutí situace potřebné.

Zásady pro řešení krizové situace vycházejí z principu individuální odpovědnosti za bezpečnost vlastníkem/správcem KII. Další zásadou je důvěra a spolupráce subjektů podílejících se na zajišťování kybernetické bezpečnosti ČR. Velice důležitá je prevence (systém řízení bezpečnosti informací), komunikace (interně, NÚKIB, národní CERT, PČR, složky IZS, ISP apod.) a koordinace (interně, externě).

Příčiny KS způsobené narušením bezpečnosti informací v informačním nebo komunikačním systému KII jsou řešeny zejména skrze instituty obsažených v ZoKB. Dopady způsobené KS vně problematiky kybernetické bezpečnosti jsou řešeny zejména v souladu se zákonem č. 240/2000 Sb., o krizovém řízení, a zásadami řešení KS v relevantních oblastech, kde dopad nastal.

Správci KII mají dle ZoKB povinnost hlásit kontaktní údaje směrem k NÚKIB s cílem vytvořit kontaktní osoby, které je možné v případě potřeby kontaktovat a řešit s nimi kybernetické bezpečnostní události a incidenty.

Další povinností je, hlásit kybernetické bezpečnostní incident. To umožňuje včasné informování Vládního CERTu tak, aby mohl incident sám analyzovat a informovat další subjekty, pro které může být hrozba relevantní. Zároveň hlášení

umožňuje Vládnímu CERT poskytnout zasaženým subjektům podporu či asistenci.

V případě přetrvávání KS na základě kybernetického bezpečnostního incidentu je podstatné, aby byl aktuální stav nadále komunikován zejména mezi zasaženým subjektem a NÚKIB, popřípadě dalšími institucemi, jejichž asistence je vhodná. V případě nemožnosti zvládat KS vlastními kapacitami, může subjekt KII požádat o podporu ze strany NÚKIB. V případě neefektivnosti pouhé metodické podpory je možné vyslat experty NÚKIB přímo na místo KS.

Z hlediska prevence NÚKIB vydává varování, dozví-li se o hrozbě v oblasti kybernetické bezpečnost. Varování jsou zveřejňovány na webu NÚKIB.CZ a mohou být oznamovány kontaktním osobám z řad správců KII.

NÚKIB však muže vydat i reaktivní opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem a subjekt KII je povinen je provést. Dále pak může vydat ochranné opatření, které reaguje na proběhlý kybernetický bezpečnostní incident a jeho cílem je podobnému incidentu předejít anebo snížit jeho dopad.

V případě, kdy je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky, může ředitel NÚKIB vyhlásit tzv. stav kybernetického nebezpečí. Za stavu kybernetického nebezpečí může NÚKIB nařizovat provedení reaktivních opatření i poskytovatelům služeb elektronických komunikací a subjektům zajišťujících sítě elektronických komunikací. O KS je zároveň informována vláda a prostřednictvím veřejnoprávních médií také široká veřejnost.

6 DISKUZE

Hlavním cílem své bakalářské práce bylo popsat a analyzovat kybernetické hrozby v České republice se zaměřením na kritickou informační infrastrukturu a následně jednu z hrozeb (Distributed denial-of-service) rozebrat podrobněji a navrhnout nebo doporučit způsob ochrany.

V teoretické části práce jsem se věnoval vymezením základních pojmů z oblasti kybernetické bezpečnosti. Popsal jsem kritickou informační infrastrukturu (KII) a způsob jejího určení. Za velice důležité jsem považoval zmínit i další skupiny dle ZoKB, a to vyznamné informační systémy, základní službu, vyznamné sítě a jejich vztah.

Dále jsem věnoval popisu jednotlivých typů kybernetických hrozeb, jejich rozdělení dle zdrojů hrozeb, zdrojů působení, cílů hrozeb, motivace útočníků a dalších.

V další části jsem uvedl seznam klíčových aktérů v kyberprostoru ČR a jejich roli v kybernetické bezpečnosti ČR. Zde bude zajímavé, jak letos proběhne schvalování novely o vojenském zpravodajství (VZ), neboť by VZ mohlo získat velké pravomoce z hlediska kybernetické bezpečnosti ČR.

V praktické části jsem se věnoval analýze jednotlivých kybernetických hrozeb dle stanovené metodiky na základě jejich dopadu, použité metody, typu útočníka a cíle hrozby.

V další části jsem se zaměřil detailněji na kybernetickou hrozbu Distributed denial-of-service (DDoS) a jejího dopadu na kritickou informační infrastrukturu. Cílem útoků typu DoS/DDoS obvykle není infikovat počítačový systém nebo překonat bezpečnostní ochranu např. heslem, které jej chrání, ale pomocí série

opakovaných požadavků jej buď zahltit, či dočasně vyřadit z provozu. Typicky tak dojde k omezení či zablokování přístupu ke službám.

Rozbor hrozby DDoS jsem provedl obdobně jako u ostatních hrozeb, navíc jsem zaměřil na způsob obrany na konkrétní typ DDoS útoku a nástroje, které útočníci používají.

Útoky typu DDoS jsem rozdělil na dvě skupiny:

- Volumetrické útoky – zde dochází k přetížení serverů a zahlcení přístupových linek či síťových zařízení falešným datovým provozem.
- Aplikační útoky – zde dochází k mnohonásobnému nárůstu požadavků směřující na infrastrukturu oběti, kde se využívá některá ze známých zranitelností cílového systému, jejíž zneužití vede k přetížení nebo pádu aplikačního serveru nebo služby.

Jelikož je komunikace v internetu postavena na protokolu IP, provedl jsem rozbor DDoS útoků i z pohledu TCP/IP a OSI modelu. V případě volumetrických útoků mluvíme o útoku na 3. a 4. vrstvu, u aplikačních útoků se bavíme o 6. a 7. vrstvě OSI modelu.

Také jsem se zmínil o použitých způsobech DDoS útoků, které podvrhují zdroj útoků (IP Spoofing), což nám komplikuje efektivní obranu nebo jsou schopny násobit sílu útoků (Amplication Attack), kde využívají standardní síťové protokoly, popřípadně některé zranitelnosti a v neposlední řadě využití velké sítě kompromitovaných zařízení (Botnet) k masivnímu distribuovanému útoku.

V další části jsem se zaměřil na ochranu proti DDoS útoků. Zde jsem provedl rozdělení ochrany na organizační a technická opatření. Z hlediska organizačních jsem se zaměřil primárně na preventivní opatření a připravenost na tyto hrozby.

Velice důležitá jsou též technická opatření, kde jako základní jsem uvedl konektivitu do internetu, což dnes představuje službu, kterou poskytuje ISP. Sítě velkých ISP označujeme dle ZoKB jako „Významné sítě“ a představují vstupní bod do kyberprostoru – internetu. V případě volumetrických útoků je nezbytností spolupráce s těmito poskytovali, neboť na hranici svého perimetru sítě se již nejsme schopni tomuto útoku bránit.

Efektivní obranu proti DDoS útokům můžeme též stavět na kolektivní obraně dalších aktérů v kyberprostoru ČR. Proto jsem zmínil projekt FENIX, který vznikl na základě masivních DDoS útoků v roce 2013. Projekt je určen společnostem, které poskytují připojení významným službám a potřebují zabezpečit jejich provoz i v těch nejkritičtějších situacích a jsou schopny přejít do tzv. ostrovního režimu (omezit datovou komunikaci pouze na důvěrné sítě, a to i geograficky).

Dále jsem se již věnoval především monitoring vlastního datové provozu, jeho sběru a ukládání pro hlubší analýzu, a to jak v době míru, tak i v případě, že jsem pod útokem. Znalost vlastního provozu, jeho charakteristik, časové závislosti je základním předpokladem k úspěšné obraně proti DDoS útokům. Organizace pro tyto účely vytvářejí dohledová centra sítě a bezpečnosti (NOC/SOC).

V současné době již existuje několik komerčních řešení na ochranu proti DDoS (Arbor, Radware, Cloudflare). Zmínil jsem se o specializovaných DDoS sondách a jejich vlastnostech s možností napojení na „Scrubbing centra“, která jsou jediná schopna se bránit masivním útokům.

V dalším bloku jsem se zaměřil na ochranu kritické informační infrastruktury (KII), která rozhodující měrou závisí na připravenosti. KII je z velké části spojená s již určenými prvky kritické Nastane-li krizová situace (KS) v oblasti

kybernetické bezpečnosti, může mít dopad na funkčnost subjektu KI a mít tak dopad na jeho fungování a služby.

Proces řešení KS způsobené narušením informací v KII je z podstaty věci veden ve dvou rovinách. Následky ve fyzickém světě (dle krizového zákona) bude zpravidla řešeno do jisté míry odděleně od následků v kybernetickobezpečnostní rovině (dle zákona o kybernetické bezpečnosti). Pro obě roviny existují postupy, tzv. typové plány.

Shrnul jsme zásady pro řešení krizové situace vycházející z principu individuální odpovědnosti za bezpečnost, prevenci, komunikaci, koordinaci, důvěrou a spoluprací subjektů podílejících se na zajišťování kybernetické bezpečnosti ČR. Příčiny KS způsobené narušením bezpečnosti informací v informačním nebo komunikačním systému KII jsou řešeny zejména skrze instituty obsažených v ZoKB.

Dále jsem uvedl povinnosti jednotlivých aktérů. Ze strany spávce KII se jedná o hlášení kontaktních osob, kybernetických bezpečnostních incident, žádosti o podporu ze strany NÚKIB s možnosti plné účasti. Ze strany NÚKIBu se jedná především vydávání varování, reaktivních opatření a v krajní nouzi o vyhlášení stavu kybernetického nebezpečí.

7 ZÁVĚR

V teoretické části jsem se věnoval základním pojmům kybernetické bezpečnosti a kritické informační infrastruktury. Dále jsem uvedl přehled subjektů podílejících se na zajištění kybernetické bezpečnosti České republiky.

V praktické části jsem se zabýval popisem a analýzou aktuálních kybernetických hrozeb. Detailněji jsem se zabýval kybernetickou hrozbou Distributed denial-of-service (DDoS) a jeho dopadu na kritickou informační infrastrukturu. Následně jsem navrhnul a doporučil způsob ochrany proti této hrozbě.

Trendem dalších let ze strany útočníků bude vylepšování technik pro DDoS útoky s využitím automatizace a umělé inteligence. Nejvyšší nárůst útoků se očekává směrem k aplikační vrstvě (HTTPS flood, burst attack, DNS attack, malware & bots). Rozvoj 5G sítí a využití IoT bude akcelerovat tyto útoky.

Do budoucna je vhodné se zabývat tématy, jako je kolektivní obrana v kyberprostoru ČR ze strany subjektů, které spadají pod zákon o kybernetické bezpečnosti. V závislosti na schválení novely o Vojenském zpravodajství se můžeme dotknout pojmu aktivní obrana a jeho dopadů v případě kybernetického útoku v kyberprostoru ČR.

8 SEZNAM POUŽITÝCH ZKRATEK

APT	Advanced Persistent Threat
BGP	Border Gateway Protocol
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
DDoS	Distributed Denial of Service
ENISA	European Network and Information Security Agency
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
ICT	Informační a komunikační technologie TPC/IP Transmission Control Protocol/Internet Protocol
IoT	Internet of Things
IP	Internet Protocol
IS	Informační systém
ISP	Internet Service Provider
KI	Kritická infrastruktura

KII	Kritická informační infrastruktura
KS	Komunikační systém
NAKIT	Národní agentura pro komunikační a informační technologie
NCKB	Národní centrum kybernetické bezpečnosti
NIX	Neutral Internet eXchange
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OSS	Organizační složky státu
RTBH	Remotely Triggered Black Hole
SQL	Structured Query Language
SSL	Secure Sockets Layer
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
VIS	Významný informační systém
VoKB	Vyhláška o kybernetické bezpečnosti
ZoKB	Zákon o kybernetické bezpečnosti

9 SEZNAM POUŽITÉ LITERATURY

1. KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.
2. Zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Zákony pro lidi [online]. 2014 [cit. 2020-04-16]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181
3. JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.
4. Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020. NBÚ [online] 2015. [cit. 2020-04-16]. Dostupné z: https://www.govcert.cz/download/gov-cert/container-nodeid-998/nskb-150216-final.pdf
5. SVOBODA, Ivan. Řešení kybernetické bezpečnosti. Přednáška v rámci CRIF Academy. (23. 9. 2014)
6. SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. (NIS) [online]. 2016 [cit. 2020-04-16]. Dostupné z: https://eur-lex.europa.eu/legal-content/cs/TXT/HTML/?uri=CELEX:32016L1148
7. Analýza rizik. [online]. [cit. 2020-04-16]. Dostupné z: https://www.vlastnicesta.cz/metody/analyza-rizik-risk/
8. Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat

(vyhláška o kybernetické bezpečnosti) Zákony pro lidi [online]. 2018 [cit. 2020-04-16]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

9. KOLOUCH, Jan, CyberCrime, Praha: CZ.NIC, z.s.p.o, 2016, ISBN 978-80-8816-815-7.
10. POŽÁR, Josef. Vybrané hrozby informační bezpečnosti organizace. [online]. [cit. 2020-04-16]. Dostupné z: https://www.cybersecurity.cz/data/pozar2.pdf
11. Před čím chránit? – Bezpečnostní hrozby, události, incidenty. [online]. [cit. 6. 7. 2018]. Dostupné z: https://www.kybez.cz/bezpecnost/pred-cim-chranit
12. NÚKIB. Zpráva o činnosti NÚKIB - 2018. [online]. [cit. 2020-04-16]. Dostupné z: https://www.nukib.cz/download/publikace/zprava-o-cinnosti-NUKIB-2018.pdf
13. Zákon č. 240/2000 Sb. Zákon o krizovém řízení a o změně některých zákonů (krizový zákon). Zákony pro lidi [online]. 2000 [cit. 2020-04-16]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240
14. Nařízení vlády č. 432/2010 Sb. Nařízení vlády o kritériích pro určení prvku kritické infrastruktury. Zákony pro lidi [online]. 2010 [cit. 2020-04-16]. Dostupné z: https://www.zakonyprolidi.cz/cs/2010-432
15. Kritická infrastruktura. HZS [online]. 2020 [cit. 2020-04-16]. Dostupné z: https://www.hzscr.cz/clanek/web-krizove-rizeni-a-cnp-kriticka-infrastruktura-kriticka-infrastruktura.aspx
16. Kritická informační infrastruktura. GOVCERT.CZ [online]. Brno, 2018 [cit. 2020-04-16]. Dostupné z: https://www.govcert.cz/download/kii-vis/Schema_KII.pdf
17. Zákon č. 365/2000 Sb. Zákon o informačních systémech veřejné správy a o změně některých dalších zákonů. Zákony pro lidi [online]. 2020 [cit. 2020-04-16]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-365

18. Národní úřad pro kybernetickou a informační bezpečnost. Úřední deska [online]. NÚKIB [cit. 2020-04-16]. Dostupné z: https://www.nukib.cz/
19. Národní úřad pro kybernetickou a informační bezpečnost. GOVCERT.CZ [online]. NÚKIB [cit. 2020-04-16]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/govcert-cz/
20. CZ.NIC. O nás [online]. [cit. 2020-04-16]. Dostupné z: https://www.nic.cz/page/351/
21. CSIRT.CZ. Služby [online]. [cit. 2020-04-16]. Dostupné z: https://www.csirt.cz/page/2764/sluzby/
22. NAKIT. O nás [online]. [cit. 2020-04-16]. Dostupné z: https://nakit.cz/o-agenture-nakit/
23. Státní pokladna Centrum sdílených služeb. Předmět činnosti [online]. [cit. 2020-04-16]. Dostupné z: https://www.spcss.cz/onas/predmet-cinnosti/
24. Národní centrála proti organizovanému zločinu SKPV (NCOZ). [online]. [cit. 2020-04-16]. Dostupné z: https://www.policie.cz/clanek/narodni-centrala-proti-organizovanemu-zlocinu-skpv.aspx
25. NCOZ. Zpráva o činnosti NCOZ za rok 2018. [online]. [cit. 2020-04-16]. Dostupné https://www.policie.cz/soubor/vyrocni-zprava-ncoz-skpv-2018-pdf.aspx
26. Útvar zvláštních činností služby kriminální policie a vyšetřování. [online]. [cit. 2020-04-16]. Dostupné z: https://www.policie.cz/clanek/utvar-zvlastnich-cinnosti-sluzby-kriminalni-policie-a-vysetrovani-716842.aspx
27. Velitelství kybernetických sil a informačních operací [online]. [cit. 2020-04-16]. Dostupné z: http://www.acr.army.cz/struktura/generalni/kyb/velitelstvi-kybernetickych-sil-a-informacnich-operaci-214169/
28. Vojenské zpravodajství [online]. [cit. 2020-04-16]. Dostupné z: https://www.vzcr.cz/kdo-jsme-35

29. Strategie kybernetické obrany ČR 2018 – 2022 [online]. [cit. 2020-04-16]. Dostupné z: https://www.vzcr.cz/uploads/46-Strategie-kyberneticke-obrany-CR.pdf
30. Novela zákona o Vojenském zpravodajství [online]. [cit. 2020-04-16]. Dostupné z: https://vzcr.cz/novela-zakona-o-vojenskem-zpravodajstvi-151
31. Matějka, Michal. Počítačová kriminalita. Praha: Computer Press, 2002. ISBN 80-7226-419-2.
32. SMEJKAL, Vladimír, Kybernetická kriminalita, Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2015, ISBN 978-80-7380-501-2.
33. HROMADA, Martin, HRŮZA, Petr, KADERKA, Josef, LUŇÁČEK, Oldřich, NEČAS, Miroslav, PTÁČEK, Bohumil, SKORUŠA, Leopold, SLOŽIL, Richard, Kybernetická bezpečnost: teorie a praxe, ed. 1., Praha: Powerprint, 2015, ISBN 978-80-87994-72-6.
34. POŽÁR, Josef, Základy teorie informační bezpečnosti, Praha: Vydavatelství PA ČR, 2007, ISBN 978-80-7251-250-8.
35. Typy DDoS útoků. [online]. [cit. 6. 7. 2018]. Dostupné z: https://flowguard.io/about-flowguard/types-of-ddos/
36. TCP/IP model vs OSI model. [online]. Fiberbit, 2013 [cit. 2020-05-09]. Dostupné z: http://fiberbit.com.tw/tcpip-model-vs-osi-model/
37. TCP SYN flood attack. [online]. ResearchGate, 2020 [cit. 2020-05-09]. Dostupné z: https://www.researchgate.net/figure/TCP-SYN-flood-attack_fig2_319416481
38. Ochrana pred útokmi DDoS. Příručka administrátora. [online]. CSIRT.SK, 2020 [cit. 2020-05-09]. Dostupné z: https://www.csirt.gov.sk/doc/DDoS_CSIRT.pdf
39. MITNICK, Kevin D. a William L. SIMON. Umění klamu. Gliwice: Helion, 2003. ISBN 83-7361-210-6.
40. Doporučení pro případ napadení DDoS útokem - jak se zachovat a jak postupovat. [online]. CZ.NIC, 2020 [cit. 2020-05-09].

https://www.govcert.cz/cs/informacni-servis/doporuceni/2150-doporuceni-pro-pripad-napadeni-ddos-utokem-jak-se-zachovat-a-jak-postupovat/

41. FENIX. O Fenixu. [online]. NIX.CZ, 2020 [cit. 2020-05-09]. Dostupné z: https://fe.nix.cz/#about
42. Complexity of Attack Continues to Grow. [online]. Radware, 2020 [cit. 2020-05-09]. Dostupné z: https://www.slideshare.net/deividtoledo/ddos-mitigation-defensepro-radware-53190134
43. Lawrence C. Miller, DDoS For Dummies®, Corero Network Security Edition, John Wiley & Sons, Inc., Hoboken, New Jersey, 2012. ISBN 978-1-118-18253-6
44. Eric Chou, Rich Groves. Distributed Denial of Service (DDoS). O'Reilly Media, Inc. 2018. ISBN: 978-1-492-02617-4.
45. The cost of launching a DDoS attack. [online]. Securelist, 2017 [cit. 2020-05-09]. Dostupné z: https://securelist.com/the-cost-of-launching-a-ddos-attack/77784/

10 SEZNAM POUŽITÝCH OBRÁZKŮ

Obrázek 1 - Proces určování kritické informační infrastruktury [16]..... 37

Obrázek 2- Schéma OSI a TCP/IP modelu [36]..... 60

Obrázek 3 - Infrastruktura a DDoS hrozby[42].....61

Obrázek 4- TCP SYN flood attack [37] 63