Zhodnocení možných rizik kybernetických útoků a jejich hrozba v krizovém řízení

(Assessing the potential risks of cyber-attacks and their threat in crisis management)

Michael Kozubek

Bakalářská práce
2018

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení

Univerzita Tomáše Bati ve Zlíně
Fakulta logistiky a krizového řízení
Ústav krizového řízení
akademický rok: 2017/2018

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Michael Kozubek**
Osobní číslo:	**L15178**
Studijní program:	**B3909 Procesní inženýrství**
Studijní obor:	**Ovládání rizik**
Forma studia:	**kombinovaná**

Téma práce: **Zhodnocení možných rizik kybernetických útoků a jejich hrozba v krizovém řízení**

Zásady pro vypracování:

1. **Analyzujte informační zdroje světa.**
2. **Analyzujte současný stav řešení zadané problematiky.**
3. **Vypracujte systémové vyjádření modelu.**
4. **Zpracujte výsledky modelování a návrhy pro praxi.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

[1] JIROVSKÝ, Václav. Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada Publishing, 2007. ISBN 978-80-247-1561-2.

[2] KOLOUCH, Jan. CyberCrime. Praha: CZ.NIC, 2016. ISBN 978-80-88168-18-8.

[3] MIDDLETON, Bruce. A History of Cyber Security Attacks: 1980 to Present. Boca Raton: CRC PRESS, 2017. ISBN 978-1498785860.

Další odborná literatura dle doporučení vedoucího bakalářské práce.

Vedoucí bakalářské práce:	**prof. Ing. Jiří Dvořák, DrSc.** Ústav krizového řízení
Datum zadání bakalářské práce:	**3. listopadu 2017**
Termín odevzdání bakalářské práce:	**15. května 2018**

V Uherském Hradišti dne 15. listopadu 2017

doc. RNDr. Jiří Dostál, CSc.
děkan

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta logistiky a krizového řízení

Ing. et Ing. Jiří Konečný, Ph.D.
ředitel ústavu

PROHLÁŠENÍ AUTORA BAKALÁŘSKÉ PRÁCE

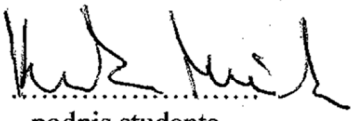
Beru na vědomí, že:

- odevzdáním bakalářské/diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby[1)];
- bakalářská/diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému a dostupná k nahlédnutí;
- na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3[2)];
- podle § 60[3)] odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- podle § 60[3)] odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tj. k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se bakalářská práce skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

V Uherském Hradišti 2.5.2018



podpis studenta

---

1) zákon č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, § 47b Zveřejňování závěrečných prací:

(1) Vysoká škola nevýdělečně zveřejňuje bakalářské, diplomové, disertační a rigorózní práce, u kterých proběhla obhajoba, včetně posudků oponentů a výsledku obhajoby prostřednictvím databáze kvalifikačních prací, kterou spravuje. Způsob zveřejnění stanoví vnitřní předpis vysoké školy. Vysoká škola disertační práce nezveřejňuje, byla-li již zveřejněna jiným způsobem.

(2) Bakalářské, diplomové, disertační a rigorózní práce odevzdané uchazečem k obhajobě musí být též nejméně pět pracovních dnů před konáním obhajoby zveřejněny k nahlížení veřejnosti v místě určeném vnitřním předpisem vysoké školy nebo není-li tak určeno, v místě pracoviště vysoké školy, kde se má konat obhajoba práce. Každý si může ze zveřejněné práce pořizovat na své náklady výpisy, opisy nebo rozmnoženiny.

(3) Platí, že odevzdáním práce autor souhlasí se zveřejněním své práce podle tohoto zákona, bez ohledu na výsledek obhajoby.

(4) Vysoká škola může odložit zveřejnění bakalářské, diplomové, disertační a rigorózní práce nebo jejich části, a to po dobu trvání překážky pro zveřejnění, nejdéle však na dobu 3 let. Informace o odložení zveřejnění musí být spolu s odůvodněním zveřejněna na stejném místě, kde jsou zveřejňovány bakalářské, diplomové, disertační a rigorózní práce, jíž se týká odklad zveřejnění podle věty první, jeden výtisk práce k uchování ministerstvu.

2) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 35 odst. 3:

(3) Do práva autorského také nezasahuje škola nebo školské či vzdělávací zařízení, užije-li nikoli za účelem přímého nebo nepřímého hospodářského nebo obchodního prospěchu k výuce nebo k vlastní vnitřní potřebě dílo vytvořené žákem nebo studentem ke splnění školních nebo studijních povinností vyplývajících z jeho právního vztahu ke škole nebo školskému či vzdělávacího zařízení (školní dílo).

3) zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, § 60 Školní dílo:

(1) Škola nebo školské či vzdělávací zařízení mají za obvyklých podmínek právo na uzavření licenční smlouvy o užití školního díla (§ 35 odst. 3). Odpírá-li autor takového díla udělit svolení bez vážného důvodu, mohou se tyto osoby domáhat nahrazení chybějícího projevu jeho vůle u soudu. Ustanovení § 35 odst. 3 zůstává nedotčeno.

(2) Není-li sjednáno jinak, může autor školního díla své dílo užít či poskytnout jinému licenci, není-li to v rozporu s oprávněnými zájmy školy nebo školského či vzdělávacího zařízení.

(3) Škola nebo školské či vzdělávací zařízení jsou oprávněny požadovat, aby jim autor školního díla z výdělku jím dosaženého v souvislosti s užitím díla či poskytnutím licence podle odstavce 2 přiměřeně přispěl na úhradu nákladů, které na vytvoření díla vynaložily, a to podle okolností až do jejich skutečné výše; přitom se přihlédne k výši výdělku dosaženého školou nebo školským či vzdělávacím zařízením z užití školního díla podle odstavce 1.

ABSTRAKT

Tato bakalářská práce se zaměřuje na zhodnocení kybernetických rizik a jejich hrozbu pro krizové řízení. Práce je rozdělena na teoretickou a praktickou část. Teoretická část definuje pojmy a analyzuje informační zdroje světa. Praktická část se rozděluje na rešerši současného stavu kybernetické bezpečnosti v ČR a její SWOT analýzu. Zpracovává systémové vyjádření modelu a věnuje se hodnocení vybraných kybernetických útoku na prvky kritické informační infrastruktury. Závěrem práce popisuje tyto rizika a navrhuje opatření, pro jejich snížení, do praxe.

Klíčová slova: kybernetická bezpečnost, kyberprostor, kybernetická ochrana, kritická informační infrastruktura

ABSTRACT

This bachelor thesis focuses on the assessment of cyber risks and their threat to crisis management. The thesis is divided into the theoretical and practical part. The theoretical part defines concepts and analyzes information sources of the world. The practical part is divided into the research of the current state of cyber security in the Czech Republic and its SWOT analysis. It processes the system's expression of its model and evaluates selected cyber-attacks on critical information infrastructure elements. In conclusion, it describes these risks and proposes measures to reduce them to practice.

Keywords: Cyber security, cyberspace, cyber protection, critical information infrastructure

Poděkování

Rád bych poděkoval mojí ženě, za podporu a trpělivost při mém studiu. Moji rodině za povzbuzování a pomoc. Mým spolužákům, za skvělý kolektiv, pozitivní a tvůrčí atmosféru. A v neposlední řadě panu prof. Ing. Jiřímu Dvořákovi, DrSc., vedoucímu této bakalářské za cenné rady při konzultacích a vedení.

Prohlašuji, že odevzdaná verze bakalářské/diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Žijeme ve velmi dynamické době, označované jako digitální věk. S rozvojem informačních technologií dnes dochází k digitalizaci společnosti. S tímto fenoménem přichází neustále nové a nové hrozby a bezpečnostní rizika, se kterými jde ruku v ruce i ochrana těchto informačních technologii. Dnes se již neobejde instituce nebo organizace bez bytí v digitálním kyberprostoru. Kromě fyzické existence dané instituce, organizace, nebo i prostého člověka, je i jejich virtuální ekvivalent. Internetové stránky, webové portály, sociální sítě a i informační infrastruktura, která zajištuje, že informační systémy, sloužící k výrobě a rozvodu energii, vody, tepla a dalších fungují, a jsou dnes samozřejmostí. Tím však vyvstávají i hrozby na tyto prvky. Kybernetická kriminalita, kybernetická špionáž nebo kyberterorismus, mohou být dnes i více závažné, než jejich fyzická předloha, mnohdy i likvidační. Proto si dnes moderní stát nemůže dovolit tento aspekt současného světa opomenout. Tato ochrana dnes jistě patří mezi prvořadé úkoly každé země.

Pracuji již několik let jako systémový administrátor v Armádě České Republiky a téma kybernetických rizik je tedy pro mě velice atraktivní. Moji bakalářskou práci jsem proto zaměřil na analyzování současných kybernetických hrozeb v krizovém řízení, zejména v kritické informační infrastruktuře. Na seznámení s legislativním rámcem problematiky a aktuálním stavem rozvoje kybernetické bezpečnosti v ČR

Cílem praktické části práce je hodnocení rizik pro krizové řízení, a vypracování systémově vyjádřeného modelu. To za pomoci rešerše rozvoje současného stavu kybernetické bezpečnosti v ČR. Účelem rešerše bude získání co nejpřesnější struktury. A z výše zmíněného závěrem této práce navrhnout výstupy pro praxi.

I. TEORETICKÁ ČÁST

1 TEORETICKÉ VÝCHODISKO PRÁCE

V teoretické části této práce jsou definovány nejpodstatnější pojmy, které osvětlují obsáhlou tématiku, jakou technická kybernetika je. Pro metody vypracování v praktické části je toto předpokladem pro úspěšnou orientaci v problematice. V této kapitole se tedy práce zabývá kybernetikou. Ta má širokou škálu vědních oborů, kterých se dotýká. Dále rozvádí pojmy kybernetický prostor, zkráceně kyberprostor, kybernetický systém, kybernetické rizika a kybernetická kriminalita.

1.1 Kybernetika

Poprvé definoval pojem kybernetika Norbert Wiener ve své knize *Kybernetika neboli řízení a sdělování v živých organismech a strojích*, ze kterého dnes již běžně definujeme kybernetiku jako vědu. Ta studuje jak lidé, zvířata a stroje spolu spolupracují a komunikují.[1]

Slovo kybernetika má svůj původ z řeckého *kybernétés.* Což znamená v překladu kormidelník. Předpoklad pro vznik je dán třemi faktory [10]:

- sociálně-ekonomické – dělba práce, ekonomicky přívětivé podmínky
- technické – rozvoj technologií, informační a komunikační technologie, materiály postupy
- přírodovědné – rozvoj vzdělání a objevů v matematice, chemii, fyzice, biologii, a dalších [9]

Dříve se tento obor připisoval pouze technickým odvětvím. S rozvojem informatizace a informačních technologii se začíná kybernetika objevovat i ve společenských a vědních oborech. Zejména kybernetická bezpečnost je dnes na vzestupu a počítáme s ní denně při běžném životě jednotlivce i chodů velkých organizací. Stává se dnes jedním z prvořadých úkolů.

1.2 Kybernetický prostor

Pojem kyberprostor má dnes ve společnosti spojitost hlavně s výpočetní technikou a internetem. Internet je nepochybně jedním z nejznámějších a nejkomplexnějších kybernetických prostorů. Není však jediný. Práce, rozděluje chápání kyberprostoru z hlediska historie, a z hlediska chápání kyberprostoru.

1.2.1 Historie Kyberprostoru

Historie kyberprostoru v moderním pojetí se váže nepochybně se vznikem první meziuniverzitní sítě ARPANET[1] v roce 1969. Sloužila jako testování decentralizované sítě, kde každý prvek je navzájem dostupný, bez centrálního řízení a zničení jedné buňky nemá za následek zničení systému, jako takového. Také jako testování vzdáleného přístupu k tehdejším nejvýkonnějším počítačům.[3] Tato první síť měla 4 uzly. Postupem času se začali připojovat další a další uzly, počítače a univerzity. Následně se zapojovaly počítače z celých USA. V 70. letech už překonala sít Atlantický oceán a připojily se některé státy Evropy jako třeba Norsko a Velká Británie.[4] V roce 1976 například poprvé poslala email, skrze síť ARPANET i královna Velké Británie Elizabeth II. [5] Tak se síť dále rozvíjela a počátkem 90. let již můžeme hovořit o Internetu, jak jej známe dnes.

1.2.2 Dnešní chápání kyberprostoru

Dnes můžeme chápat kyberprostor hned z několika úhlů pohledu. Obecně si jej můžeme představit jako počítače zapojený v datových centrech, ve firmách, v obchodech, v domácnostech. Chytré telefony s přístupem do internetu. Chytré spotřebiče, které dnes označujeme souhrnně zařízení IoT[2], například ledničky a televize. Řídicí systémy, průmyslové počítače, řízení dopravy a logistiky. Prostě vše co je řízené nějakým programem. Jako příklad takového kyberprostoru si můžeme představit, že se nacházíme v kyberprostoru klimatizační jednotky, pokud nastavujeme ovladačem teplotu v místnosti.

Například Zákon č. 181/2014 Sb., o kybernetické bezpečnosti definuje ve vysvětlení pojmů kyberneticky prostor jako: „*Jedná se o virtuální oblast, kde pracují, případně spolu prostřednictvím elektronických komunikací komunikují informační systémy, jednotlivé počítače i počítačové sítě. V kybernetickém prostoru jsou zpracovávány a vyměňovány informace a ukládána, sdílena či přenášena data v elektronické podobě“*.[6]

Oxford Dictionary slovník definuje kybernetický prostor jako: „ *teoretické prostředí, ve kterém dochází ke komunikaci přes počítačové sítě“* [7]

Výkladový slovník kybernetické bezpečnosti jej definuje jako: *„Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.“* [8]

---

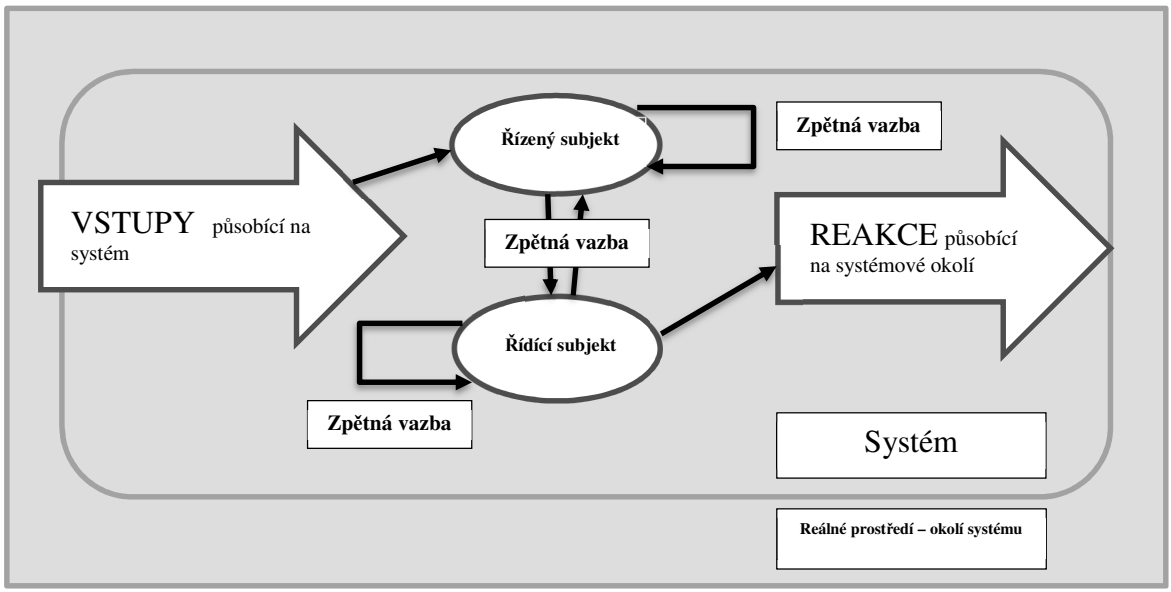
[1] ARPANET: „*Advanced Research Projects Agency NETwork*“
[2] IoT: *„Internet of Things“* neboli *„Internet věcí“* Jedná se o zařízení propojená do internetu.

1.3 Kybernetický systém

Kybernetický systém je složen z kybernetických prostorů. Chápat jej můžeme jako ucelený systém skládající se z jednotlivých prvků, na které působí vstupy. Které pak působí na systém a výstupy, kterým reaguje na okolí. Mezi jednotlivými prvky probíhá i zpětná vazba. Toto je zobrazeno na obrázku 1. Prvky mohou tvořit informační a komunikační technologie, lidé, procesy a další. Kybernetický systém se opírá o teorii systémů. Systém je charakterizován[10]:

- Strukturou: Prvky systému a jejich vzájemné vztahy. (vnitřní pohled)
- Chováním: Vztahem systému k okolí, souhrnem reakcí na všech výstupech. (vnější pohled)
- Stavem systému: Podmínky a údaje, které charakterizují systém
- Prostředím: Zejména vnějším okolím. A vstupy z něj do systému.
- Cílem systému: Cíl, kterému je vlastnost systému zaměřena
- Podsystémem: Uzavřený celek v systému, jenž plní určitý účel
- A dalšími

Teorie systému popsal Ludwig von Bertalanfy jako: *„množina element, které jsou vázány nějakým vztahem mezi sebou.“* A to již na počátku třicátých let. Definoval tak skutečnost, že vlastnosti dílčích prvků ovlivňují celek a celek vykazuje vlastnost, podobnou jako jsou elementy v něm obsažené.[10]



Obrázek 1 Kybernetický systém [11]

1.4 Kybernetické rizika

Kybernetické riziko můžeme chápat jako potenciál zneužití informačních a komunikačních technologií. Toto zneužití má za následek poškození nebo škodu. Ty můžou být třeba únik informaci, nefunkčnost služby, neoprávněný vstup do systému a podobně.

Obecně se uvádí, že kybernetické riziko je pravděpodobnost, že bezpečnostní hrozba, skutečně nastane, a to na zranitelném místě. Hrozba muže být pozitivní i negativní. Například u pozitivní hrozby je předpoklad, že její přítomnost evokuje k inovaci zlepšení systému. A tímto bude dosaženo významného úspěchu. Pozitivní i negativní kybernetické hrozby mají za následek realizaci kybernetické obrany a ochrany, k předcházení a aktivnímu boji proti kybernetickým útokům. Jsou tak tažnou silou kybernetické bezpečnosti. Při malé nebo žádné kybernetické bezpečnosti totiž mohou hrozit rozsáhlé poškození a škody, nebo může dojít k určitému uskutečnění škodlivého záměru útočníka. Což je i definicí kybernetického útoku. Jako příklad si uveďme kritickou infrastrukturu. Provedený kybernetický útok muže mít zásadní vliv na funkci systému, chod státu, chod veřejné zprávy a uspokojení základních potřeb obyvatelstva. Proto nastupuje kybernetická ochrana, aby zmírnila, či eliminovala tyto rizika.[15]

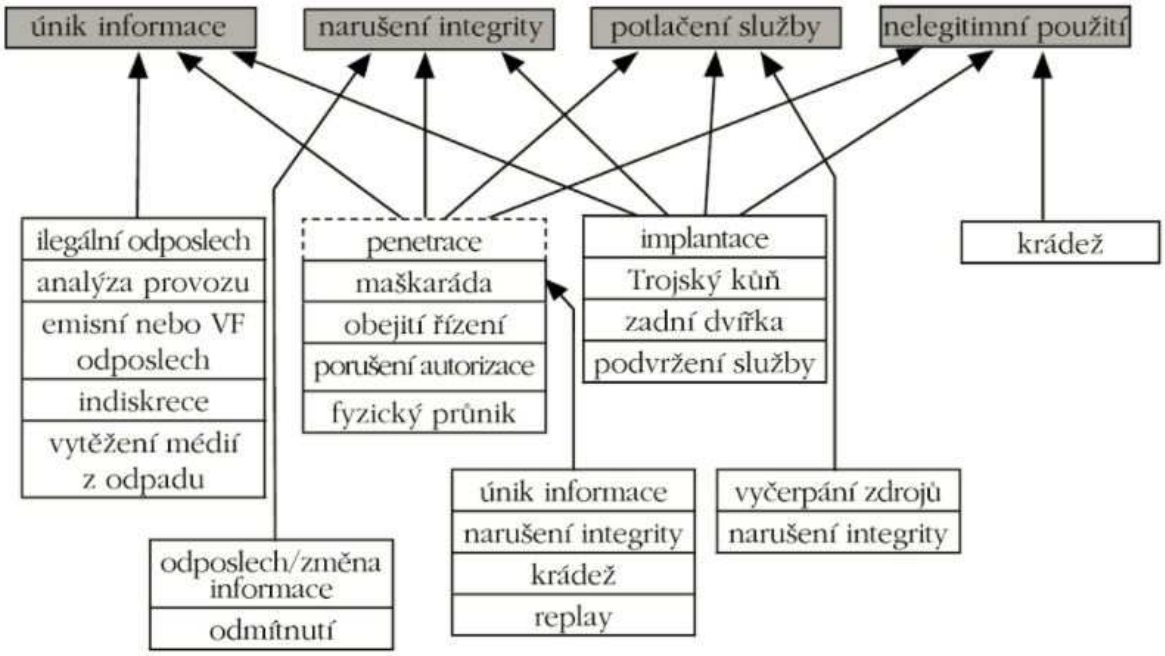
Václav Jirovský ve své knize Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství, identifikuje tyto základní kybernetické hrozby:[2]

- Únik informace: Informace citlivého charakteru, je prozrazena neautorizovanému[3] subjektu (například heslo). Muže vést přímo ke kybernetickým útokům.
- Narušení integrity: Tím může dojít k poruše dat, což vede k změnám dat, či jejich smazáni.
- Potlačení služby: Pokud je legitimnímu subjektu bráněno ve využití služeb, nebo přístupu k informacím tím, že je subjekt, který službu, či informaci poskytuje, záměrně přetěžován nekorektními a zbytečnými požadavky.
- Nelegitimní použití: Použití služeb nebo zdroje neautorizovanou osobou.

Tyto hrozby určují základní skupiny, do níž můžeme rozřadit jednotlivé typy kybernetických útoku. Na následujícím obrázku je velmi přehledně znázorněna provázanost

[3] Autorizace: Po provedení určité akce, operace, je subjektu udělen souhlas s přístupem k informacím, funkcím apod.

kybernetických útoku a prvků kybernetické kriminality. Vybraným kybernetickým útokům, se blíže budeme věnovat v následující sekci 1.5 Kybernetická kriminalita.



Obrázek 2 Dělení hrozeb [2]

1.5 Kybernetická kriminalita

Kybernetická kriminalita se začala objevovat již od prvního vzniku kybernetického systému, systému ARPANET. První vir „Creeper virus“, který do sítě vypustil v roce 1971 Bob Thomas, neměl zatím za úkol nic špatného provést, měl jen za úkol demonstrovat mobilní program se samotnou distribucí. Skutečná kriminalita na sebe však nenechala dlouho čekat [12]. Dnes popisujeme kriminalitu jako takovou činnost, kterou se porušují zákony dané společnosti, dobré mravy nebo zásady společenského chování. Při páchání této kriminality je napaden, ovlivněn jednotlivec, skupina či celá organizace. Kybernetická kriminalita může být na samostatném informačním prostředku či proti celé síti. Kybernetická kriminalita nezná hranic a proto je nebezpečná. Potencionální oběť může být v jiném státu, klidně tisíce kilometrů daleko. Tím se stěžuje odhalení této kriminality, jež je možné zase jen na základě použití informačních technologii.[2]

Motivací k páchání kybernetických zločinů můžeme rozdělit na několik směrů, uveďme si některé nejvýznamnější:[13]

- Pomsta: Obecně se jedná o snahu poškození nějakého subjektu narušitelem, který má anebo měl, bližší vztah k napadenému subjektu. Mezi osoby, které se

zařazují do této kategorie, můžeme zařadit třeba bývalé zaměstnance, kteří se cítí být dotčeni třeba tím, že byli neprávem propuštěni. Popřípadě se mohou touto formou kriminality řešit vnitřní konflikty zaměstnanců na pracovišti. Nebo muže jít i o zaměstnance, který se cítí být nedostatečně doceněn. Ten pak může tvořit například škodlivé kódy, viry, kterými si kompenzuje nedostatek uznání ve svém zaměstnání.

- Finanční zisk: Účelem kriminality je zisk. Ať už jde o malou krádež, jako třeba neoprávněné používání placené služby nebo rozsáhlá finanční kriminalita. Může se jednat i o prodej informací a know-how daného subjektu třetí straně za účelem zisku. Také častým projevem jsou útoky na objednávku, například DoS[4]/DDoS[5] útok.
- Publicita: Mezi tuto kybernetickou kriminalitu patří kyberterorismus, hackaktivizmus[6], snaha o zviditelnění začínajícího hackera ale i práce, zpravodajských služeb a v neposlední řadě publikování citlivých materiálu, tzv. whistle-blower.[7][14]
- Výstřednosti: Jako důvod útoku si můžeme představit klasického hackera. Motivací hackera je personální svoboda, popřípadě pomoc druhým. Pro něj je celý svět plný problému a výzev k vyřešení. Motivací mladých hackerů je zviditelnění v hackerské komunitě a tím dosažení uznání.
- Kyberterorismus: Motivací je většinou provedení teroristického kybernetického útoku, či útok různých extremistických organizaci a uskupení, hledajíce jednoduchost a dostupnost těchto útoku v dnešním světě a zároveň jistou formu vlastní bezpečnosti při takovémto útoku.

- Kybernetická špionáž: Za kybernetickou špionáží stojí většinou cizí státy, potažmo jejich bezpečnostní nebo zpravodajské struktury. Cílem je zisk zpravodajských informací, ovlivnění cílového institutu, společností či celého státního uskupení cílové země. Běžně dochází k prolínání těchto kategorii.

[4] DoS: (Denial of Service) V překladu potlačení služby, vysvětleno v další kapitole 1.5.1 Hacking a cracking

[6] Hacktivista: Složenina slov Hacking a Aktivista. Jedná se o Aktivistu, který k šíření myšlenek používá metody hackerů.

[7] Whistle-blower: Osoba, která informuje o osobě nebo organizaci, která se domnívá, že se zabývá nezákonnou nebo nemorální činností.

1.5.1 Hacking a craking

V této části si vysvětlíme pojem hacking a jak se liší oproti crackingu. Uvedeme si blíže, co je motivací hackeru. Na co je rozdělujeme a jaké prostředky používají k tomu, aby dosáhli svých cílů.

Jak jsme si zmínili v popisu motivace, ke konání kybernetické kriminality motivuje hackera několik faktorů. Motivace mladých hackerů se prosadit, touha překonávat výzvy a problémy, odhalování slabin kybernetického systému, za účelem podpoření a ošetření kybernetických rizik. Sami hackeři se považují za běžné uživatelé, kteří jsou ale obdaření velkou technickou znalostí informačních a komunikačních technologii. Ty však používají jen jako koníček. Tvrdí, že pronikají například do chráněného systému za účelem vlastního zhodnocení kvality. Ne za účelem získání dat, informací, služeb, nebo jejich měnění či zničení. Pokud však je jednáním a motivací opak tohoto, označují sami hackeři takového jedince za crackera. [2] Tím si ale musíme uvést, na jaké rovině legálnosti se hacker pohybuje a co je již klasifikováno jako překročení hranice mezi legálním a nelegálním. Obecně můžeme definovat Kybernetický útok hackerem jako: *„jakékoliv protiprávní jednání útočníka v kyberprostoru, které směřuje proti zájmům jiné osoby“* [16]. Může se jednat jen o narušení běžného života, daného i morálními a společenskými zásadami. Toto jednáni nemusí mít právní klasifikaci trestného činu, či přestupku. Jak dále podotýká Jan Kolouch ve své knize Cybercrime: *„Kybernetický trestný čin musí být zároveň kybernetickým útokem, ale ne každý kybernetický útok musí být trestným činem.“*[16]

Tím se také dostáváme k tomu, jak se dá podle legálnosti dělit hackery:[2]

- White hats: (Bíle klobouky) Uznávají hackerskou etiku.[8] Často jsou najímáni nebo jsou přímo zaměstnáni k tomu, aby svými znalostmi zlepšovali kybernetickou bezpečnost společnosti, systému.
- Black hats: (Černé klobouky) Již zmínění crackeři. Kteří svým hackingem nabourávají a prolamují systémy pro vlastní obohacení nebo pro svého zaměstnavatele či objednavatele hackerské služby.
- Grey hats: (Šedé klobouky) Hackeři, kteří se pohybují na hranici předchozích dvou skupin. Také se dá takto definovat hacker, který začínal

[8] Etika hackera: Pokud jsou informace správné a dobré, je etickou povinností se o ně dělit v maximální možné míře. A pokud jejich nabouráním, nedojde k poškození nebo škodě.

v jedné skupině, ale postupem času vlivem vlastního „dozrání“, přestoupil do druhé kategorie.

Vlastní kategorii jsou potom začínající hackeři, kteří ještě nedosáhli uznání komunity, ta je nazývá Script-kiddies, lammers, loosers. Jejich technické znalosti nedosahují takové úrovně jako hackeru profesionálů. Používají jen postupy, znalosti, které jsou v hackerské komunitě dostupné. Svojí neznalostí však mohou neúmyslně způsobit velké škody.[2]

Nástroje, které hackeři používají, víceméně kopírují vývoj software v průběhu let. Hackeři byli vždy o krok vpřed před správcem systému. Kdykoliv se vydá záplata systému nebo se odstraní slabina systému, tak se objeví nové možnosti jak systém napadnout. Jedná se o nekončící koloběh v kyberprostoru. [2]

Mezi úplně první používané nástroje se řadí „prolamovače“ hesel. Které zkouší kombinace znaku k prolomení hesla. Využívají hlavně slovníku a známých frází. Kdo používá hesla typu: „1234“ nebo „admin“ či „Password“, tak se dostává mezi velmi ohroženou skupinu lidí. Takové heslo totiž prolamovač hesla „rozlouskne“ za krátkou dobu. Obecně platí, že není neprolomitelné heslo. Ale je brán fakt, že prolomení hesla zabere tak dlouhou dobu, že informace, jež chceme získat, již nebudou aktuální. Nebo prostředky které vynaloží hacker na prolomení hesla, jsou mnohem větší než hodnota informace, kterou chce získat. [2]

Mezi další nástroje mohou patřit:[2]

- Backdoor: (v překladu: zadní vrátka) Tento nástroj využije hacker v případě, že najde „díru“ v systému a díky ní si zřídí přístup do systému.
- Sniffery: (v překladu: „čmuchače“) Ty, jak název napovídá, zachytávají tok v počítačových sítích a ukládají obsah pro pozdější analýzu provozu. Hacker tam má možnost „vidět“ všechny komunikace v síti.
- DoS: Zkratka znamená: „Denial of Service“, v překladu potlačení funkce služby. Taková služba v podstatě „zahltí“ daný server. Útok je totiž často prováděn z mnoha počítačů, botu, skrze botnet útok.[9] To zvyšuje zátěž serveru a ten je potom zahlcen nelegitimními požadavky na služby a není schopen vyřizovat ty legitimní. Jedná se dnes o velmi častý nástroj.

[9] Více o botnet útocích a definice „botů“ v kapitole 1.5.3 Botnet.

- Trojské koně: Stejně jako Řekové použili velkého dřevěného koně, aby infiltrovaly starověkou Troju, tak i tento škodlivý nástroj je často schován do legitimního programu a připraven na infiltraci u hostitele. Příkladem mohou být programy zdarma ke stažení z neprověřeného zdroje. Při jejich nainstalování se nainstaluje i trojský kůň, který umožní do systému umístit zadní vrátka pro hackera. Nebo tímto trojským koněm, ten může z napadeného subjektu vytvořit svojí buňku pro útok DoS. Často se s trojským koněm nainstaluje keylogger[10], kterým mohou hackeři zjistit naše heslo do systémů, internetových bankovnictví a dalších.

1.5.2 Sociální inženýrství

Sociální inženýrství je jedno z prvních velmi častých a dodnes používaných a úspěšných prvků kybernetické kriminality. Pokud bychom hledali jednoduchou definici, tak určitě nesmíme opomenout tu, kterou definoval sociální inženýrství ve své knize The art of Deception, v překladu: „Umění klamu“, Kevin D. Mitnick: *„Sociální inženýrství využívá vliv a přesvědčování, k oklamání lidí tím, že je přesvědčí, že sociální inženýr je někdo, kdo ale není, nebo manipulací. Ve výsledku je sociální inženýr schopen využívat lidi k získání informací, bez použití technologii“*.[17] Celý úspěch sociálního inženýra tak můžeme chápat jako schopnost využívat lidské mysli, apelovat na rizikové prvky lidské komunikace, jako důvěra, strach, vzájemnost, ale i touha. Obecně se však dá tvrdit, že sociální inženýr, sociotechnik[11], pracuje s lidskou hloupostí a nepozorností. Oběť má pocit falešné bezpečnosti. Mitnick také definoval rozdíl mezi sociotechnikem a podvodníkem. Podvodník je hnán ziskem, kdežto sociotechnik touhou o překonávání překážek a získání informací [17]. To však nepomohlo ani při jeho soudních řízeních, neboť tato formulace je sporná. V podstatě se sociální inženýrství používá jako nástroj v kybernetických útocích.

Jak jsme si již řekli, sociolog pracuje s pocitem bezpečí. Lidé cítí podvědomě větší bezpečí v kybernetickém nehmotném světě než ve skutečném a mnohdy dělají a říkají věci, které by normálně nedělali a neřekli. Mezi základní metody sociotechnika patří například:[16]

- Telefonický hovor – Jedná z nejstarších a nejúčinnějších metod. Sází na několik způsobů, jak cílový objekt působit. Mezi ně platí zjištění informací

[10] Keylogger: Program, kterým můžeme zaznamenat například všechny stisknuté klávesy a z nich najit heslo.
[11] Sociotechnik: Výraz pro Sociálního technika podle Kevina D. Mitnika

předem a tím v hovoru působit důvěryhodně. Slíbení zlepšení postavení ve firmě. Postupné budování důvěry, které nakonec graduje důvěrou mezi sociotechnikem a obětí, a mnoho dalších.

- Podvodný email – V současné době nejlevnější a tudíž nejrozšířenější metoda. Oběť se nachytá na podvodný text, nabídku, hoax[12][18] či jiné.
- Získávání informací z odpadků – Anglicky „Dumpster diving". Kdy se k přístupům k citlivým informacím dostává sociotechnik „prohrabáváním" košů a odpadkových kontejnerů. Tato metoda je využívána i mnohými bezpečnostními složkami. Informace se zajišťují ze starých diářů, faktur, tištěných zpráv a dalších.
- Falešný pracovník údržby – Touto metodou se sociotechnik vydává za osobu, která má za úkol opravit či nějak zasahovat do citlivých částí podniku.
- Infiltrace cíle pomocí zdarma poskytnutých paměťových medií – Jako jedna z nejjednodušších metod jak infiltrovat cíl je jejím zaměstnancům poskytnou zdarma paměťová media, jako například reklamní dárky. Zaměstnanec jej pak donese na své pracoviště a připojí do firemní sítě.
- Služba zdarma – Tato metoda využívá služeb, které se zdají býti zdarma. Ať už se jedná o Cloudové uložiště, různé služby zdarma či další. Používáním těchto „podezřelých" cílů útoku, sám „pozve" útočníka.

1.5.3 Botnet

Pojem botnet se začal objevovat se spojitostí s projekty zvanými „distribuované výpočty". Myšlenkou distribuovaných výpočtů je, že spousta počítačů není využita v domácnostech, ve školách a firmách výkonu na sto procent. Tím Vzniká velká spotřeba energetického výdeje na relativně malý výpočetní výkon. Projekty, kterých je desítky, pracují s tímto výkonem, který jim uživatel „poskytne". Uživatel, bot[13] se připojí tak, že si nainstaluje klienta, který spustí proces v počítači. Tento proces má menší prioritu, než jakýkoliv jiny proces, takže nedochází k omezení výkonu počítače, na kterém uživatel pracuje. Centrum projektu odesílá klientům dílčí výpočty, ty je zpracují a po dokončení je

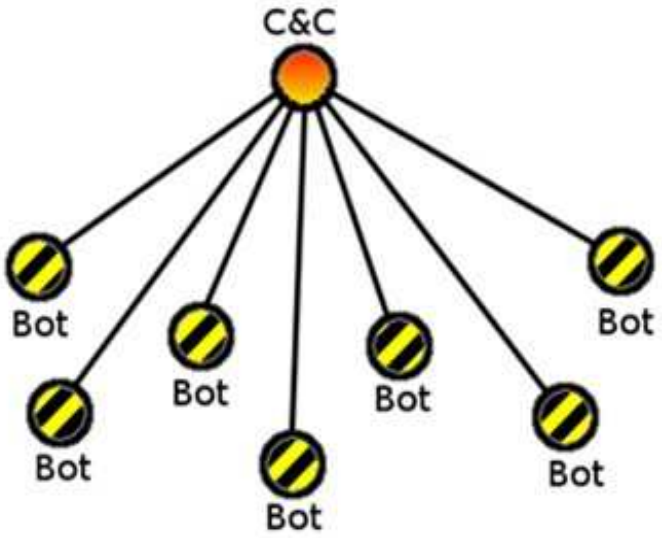
[12] Hoax: Jedním z velmi častých nešvarů, který se na Internetu vyskytuje, je šíření poplašných, nebezpečných a zbytečných řetězových zpráv, tzv. hoaxů.
[13] Bot: Zkrácenina slova robot. Jedná se o počítač napadený škodlivým programem. Vykonává procesy od řídící stanice. Někdy se uvádí pojem zombie.

odešlou zpět. Centrum je spojí ve finální projekt. Tím je možno dosáhnout stejného i většího výkonu jako nejvýkonnější sálové vědecké počítače.

Tuto myšlenku distribuovaných výpočtu začali hackeři používat i pro jiné než legální účely. Pokud bude samostatný počítač, například v roli mailového serveru odesílat miliony nevyžádaných emailů denně, mailové servery příjemců jej brzo vyhodnotí jako nadměrné využívání nelegitimních zpráv a daný server, zařadí mezi nedůvěryhodné. Pokud však má útočník svou „armádu“ botů a rozdělí tento provoz mezi stovky, či tisíce počítačů, muže klidně rozesílat co chce.

Botnetová síť se vyskytuje ve dvou architekturách.[19]

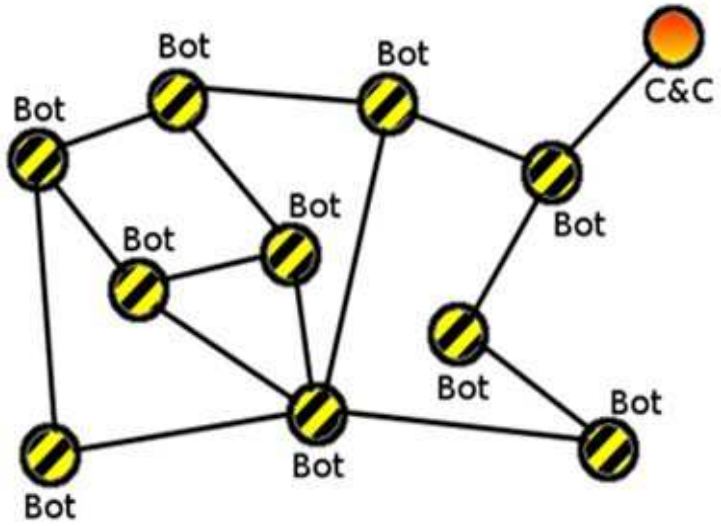
- Síť s jedním řídícím (Command & Control) počítačem, který ovládá podřízené boty – zombie.



Obrázek 3 Botnet s centrálním řízením [19]

- Síť s decentralizovanou soustavou. Hlavně se využívá v sítích P2P[14]. taková síť je odolnější proti případnému narušení této sítě.

[14] P2P: (Peer-to-peer) Spojení klient - klient, neboli komunikace přímo mezi klienty těchto služeb.



Obrázek 4 Botnet s decentralizovaným řízením [19]

1.5.4 Phishing a Pharming

Tyto fonicky psané anglické slova fishing a farming, v češtině rybaření a farmaření, představují podvodné jednání, které má za cíl oběd oklamat. Získat z oběti informace typu jméno, heslo, PIN, číslo účtu, číslo kreditní karty a další jiné informace. Jedná se o formu sociálního inženýrství avšak je prováděno ve větším formátu. Společným pojmem je spam[15], který znamená nevyžádanou poštu, službu, jejíž příjem je obtěžující.[16]

- Phishing: (rybaření) Oběť je postavena před předem promyšlený scénář, který má za úkol oslabit pozornost uživatele, uvěřit a jako ryba na háčku se nechat „chytit“ do podvodu. Při těchto útocích je často využíváno služeb botnetů. Ty se postarají o doručení návnad do cílové oblasti k uživateli. Nejčastěji je to formou emailu, spamu. Ten uživatele například informuje o změně služby, třeba aktualizaci internetového bankovnictví, a tím spojenou potřebu kliknout na odkaz uvedený v emailu. Ten uživatele přenese na webovou stránku, ta je však kopií originální, což na první pohled uživatel nemusí zjistit a tak zadáním údajů nebo PIN kódem se útočník dozvěděl dané informace. Dále jsou to zprávy informující uživatele o zahájení exekuce, zablokování počítače, kterým lze zabránit, posláním „pokuty“ na uvedený, zejména bitcoinový[16] účet. [16]. Mezi další formy fishingu je Spear Phising – cíli na konkrétní

[15] SPAM: Označení konzervy, lunchmeatu, za 2. světové války. Za její popularizací stojí komický skupina Monty Pyton. Ta tuto nepříliš oblíbenou náhražku masa využila jako něco nechtěného a obtěžujícího.
[16] Bitcoin: Virtuální měna, která není kontrolována žádnou vládou ani organizací, je decentralizována, platby jsou anonymní a hodnota 1 bitcoinu je řízena jen nabídkou a poptávkou na trhu.

skupinu, okruh uživatelů, kteří postupně slouží k infiltraci a phishingové zprávy se šíří mezi nimi. Tím je útok uvěřitelnější.

- Pharming: (farmaření) Jde o sofistikovanější formu útoku. Útočník imituje určitý DNS[17] server a uživatel při snaze se dostat na službu na originálním serveru se dostane na „duplicitní" server útočníka. Bývá k nerozeznání a uživatel většinou poskytne svou nepozornosti informace útočníkovi.
- Smishing: (složenina slov phishing a sms) Forma phishingového útoku formou sms zprav. Cíl útoku je nucen volat na placenou linku nebo přejít na podvodný web.[16]
- Vishing: (složenina VoIP[18] a fishing) Další typ phishingu. Útok je prováděn sociotechnikem přes například firemní telefonickou síť. Princip je stejný jako u všech phishingových útoků. [16]

1.5.5 Malware

Název je složeninou anglického malicious software neboli škodlivý software. Jan Kolouch definuje malware jako: *„Jakýkoliv software využitý k narušení standardní činnosti počítačového systému, zisku informací (dat), či využitý k získání přístupu k počítačovému systému."* [16] Malware se rozděluje na spoustu druhů, ty se nazývají podle toho, jaký úkol mají. Uvedeme si ty nejdůležitější.[16]

- Adware: (Z anglického: „advertising supported software", neboli reklamu podporující software) Po jeho průniku do systému je jeho hlavní úlohou zejména propagace určité formy reklamy. Zejména je to realizování pop-up reklamou, napadením internetového prohlížeče a dalšími.
- Spyware: (Z anglického: spy a software, neboli špión a software.) Tento software slouží hlavě k zjišťování informací a jejich následnému odeslání k útočníkovi. Podstatné je, že se toto děje bez vědomí uživatele. Mohou být i součástí oficiálních programu. Například pro kontrolu smluvních podmínek.
- Viry: Viry byly jednou z nejzávažnějších hrozeb při rozvoji počítačů. Jako reakcí na ně se začaly vyvíjet antivirové programy. Tento název se dochoval do dnešních dnů, i když tyto programy chrání počítače nejenom proti virům. Dodnes je potenciál virů využíván pro kybernetické útoky. Šíří se samy, i bez činnosti cílového uživatele a

[17] DNS: (Domain Name System) – Jedna ze základních rolí serverů. Slouží k překladu IP adres serveru a hierarchické uspořádání serverů.
[18] VoIP: (Voice over Internet Protocol) – Jedná se o technické řešení přenosu telefonního hovoru přes počítačové sítě.

jejich využití je takřka neomezené. Mohou útočit na celou řadu prvku systému. Je možné jej připojit k jakémukoliv i legálnímu programu. Virus může napadat soubory, mailové zprávy či zcela zničit počítač.

- WORM: (V překladu červ) Jejich rozdíl oproti virům je ten, že není potřeba hostitele k šíření, červ si hledá bezpečnostní slabiny v systému sám a sám se také šíří.
- Trojské koně: Blíže popsáno v kapitole: 1.5.1 Hacking a craking.

1.5.6 Ransomware

Dnešním rozšiřujícím se fenoménem je ransomware, název vychází z anglického ransom, neboli výkupné. Ransomwere napadá počítač zejména pomocí malware a provede útok. Ten se projeví „zašifrováním“, či znepřístupněním dat uživatele, někdy i celého systému. Ransomware potom informuje uživatele formou vyskakovacího okna o znepřístupnění dat, a začne jej vydírat pro opětovné zprovoznění. Uživatel je nucen odeslat částku, většinou v kryptoměně (Bitcoin). Po zaplacení muže i nemusí dojít k odblokování dat. Přesvědčivější ransomware dokonce uživateli ukáže pár souborů, které odšifruje. Uživatel je tím ujištěn, že platbou nepřijde o data.

Další formou je policejní ransomware, který po zašifrování se tváří jako oficiální program policie, nebo úřadu pro kybernetickou bezpečnost. Místo výkupného uživateli nabídne zaplatit pokutu a vyhnout se trestnímu stíhání, za například nelegální software. Princip je ale stejný.

Obrázek 5 Příklad českého ransomware [20]

2 KRIZOVÉ ŘÍZENÍ

Druhá kapitola teoretické části bakalářská práce se zabývá pojem krizové řízení a řízení rizik, což je nezbytné pro vymezení oblasti zpracované v praktické části a k definici východiska pro metodologii užívanou při vypracování cílů práce. V této části se práce zaměří na orgány a prvky krizového řízení v ČR, krizového řízení, řízení rizik, kde uvádí co je to riziko, jak jej identifikovat, analyzovat, hodnotit a jak jej ošetřit.

2.1 Základní definice krizového řízení

Krizové řízení vychází ze slov „krino“, řecky posouzení nebo rozhodování mezi dvěma variantami a řízení, což je pojem pro vedení či řízení procesu. „*Krize, krizový stav, krizová situace není dána velikostí ztrát nebo rychlostí ničivých dopadů, ale složitostí problémů spojených s hypoteticky možnou bezradností lidí situaci řešit, když na ně přímo či nepřímo působí.*“[22]

Z historického hlediska se na vývoj managementu můžeme dívat, jako na vývoj ve vojenských strategiích. Ta se opírala o čtyři základní manažerské funkce. Strategie a plánování, organizování, vedení a personální otázka. Tyto funkce dnes můžeme definovat jako:[21]

- Funkce plánování: Schopnost uvést myšlenku do plánu, systémově musí plán obsahovat: strukturu, informační formu, časovou realizaci. V krizovém řízení je plánování jedna z nejdůležitějších činností. Předchází dalším postupům a procesům. Plán v krizovém řízení je vždy krizový plán: „*souborem hierarchicky uspořádaných plánů tvořících jako celek dokumentaci nazvanou krizový plán*“ [22]
- Funkce organizování: Navazuje na plánování v průpravném období, zejména uváděním preventivních opatření. Posléze reakci na vzniklé mimořádné události. Při vzniku mimořádných událostí, která přerostla do krize, se aktivují přípravné střediska IZS[19], operační střediska, pohotovostní složky orgány veřejné správy a další. Organizování nekončí začátkem krize ale je potřeba i v průběhu krize, vlivem působení krizové situace. Zejména pokud selhávají jednotlivé složky řízení, zejména na vrcholové funkce.

[19] IZS – Integrovaný záchranný systém. Koordinovaný postup složek IZS provádění záchranných prací při mimořádné události.

- Funkce vedení: Vychází z funkce vedoucí pozice. Neboli schopni vést. Neboť půl úspěchu je vzděláním a školou, druhá půlka je přirozenou osobnosti, charizmatem, inteligencí, rychlého a racionálního uvažování.
- Funkce kontrolování: Porovnání plánů se skutečným stavem, podle kritérii. Cílem je stanovení k určení normálního stavu. Korekce se řídí řízením rizik.

Moderní management je založený na vědeckých pojetích a ekonomickém myšlení. Ekonomické a politické podmínky potom zobrazují, jak je reálný manažerský cíl. Jako je růst společnosti či uspokojování životních potřeb obyvatel. Strategie, manažerské řízení, ekonomická situace a ochrana systému se prolínají.

Systém, jakým můžeme definovat krizové řízení je několik. Například Hájek ve knize Krizový management (2008) definuje krizové řízení jako: *„Čím méně je předem neznámých ohnisek mimořádného stavu, a čím více je podnik vybaven zdroji k jejich zvládání, tím jistěji lze zvládat krizový stav a přechod do nového běžného stavu.“* [21]

Krizový zákon č.240/2000 Sb., § 2 o krizovém řízení definuje krizovou situaci jako: *„souhrn řídících činností věcně příslušných orgánu zaměřených na analýzu a vyhodnocení bezpečnostních rizik, plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s řešením krizové situace, nebo ochranou kritické infrastruktury.“* [24]

Valášek v knize Krizové řízení při nevojenských krizových situacích (2008) definuje obecnou definici krizové řízení: *„krizové řízení je ucelený soubor řídících činností a postupů, přístupů, názorů, zkušeností, metod a opatření, zaměřených na analýzu a vyhodnocení bezpečnostních rizik, plánování, organizování, realizaci a kontrolu činností, které se užívají orgány krizového řízení ke zvládnutí specifických stavů.“*[22]Krizové řízení je nedílnou součástí řízení státu, organizace či jiné instituce, které mají zájem na svém rozvoji.

2.2 Orgány a prvky krizového řízení v ČR

Podle jí zmíněného zákona č. 240/2000 Sb., o krizovém řízení, se krizovým řízením v ČR rozumí souhrn řídících činností orgánů krizového řízení. Orgány krizového řízení jsou:

- vláda,
- ministerstva a jiné ústřední správní úřady,
- Česká národní banka,
- orgány kraje a další orgány s působností na území kraje,

- orgány obce s rozšířenou působnosti (dále jen „ORP“),
- orgány obce.

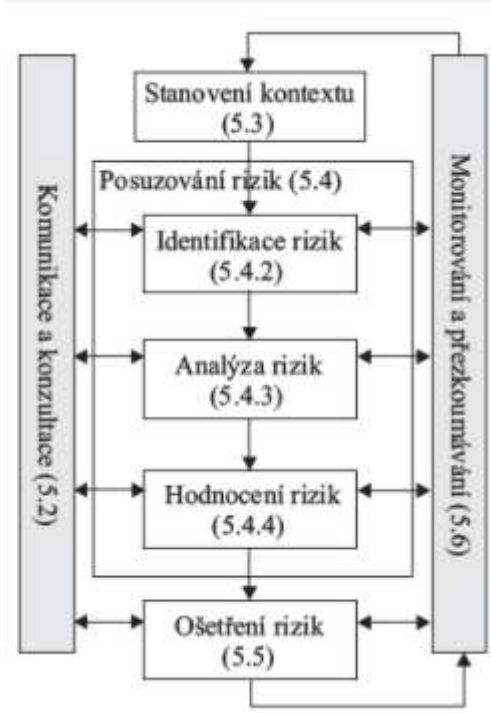
Tyto orgány se zabývají zaměřením na analýzu a vyhodnocení bezpečnostních rizik. Dále na plánování, organizování, realizaci a kontrolu činností prováděných v souvislosti s přípravou na krizové situace a jejich řešením nebo jako ochrana kritické infrastruktury. Podle zákona výše zmíněného zákona o krizovém řízení je koordinačním orgánem v přípravě na krizové stavy ministerstvo vnitra.

Podle čl. 9 ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky se zřizuje Bezpečnostní rada státu (Dále jen „BRS“). BRS je stálým pracovním orgánem vlády pro koordinaci problematiky bezpečnosti České republiky, připravuje a navrhuje opatření k zajišťování bezpečnosti ČR. Tvoří ji předseda vlády a členové vlády podle rozhodnutí vlády. V BRS působní čtyři stálé pracovní výbory. V hierarchii krizových štábu se skládá z Ústředního krizového štábu (ÚKŠ), krizového štábu kraje a krizového štábu obce s rozšířenou působností. Ty zřizují bezpečnostní rady kraje a bezpečnostní rady obce s rozšířenou působností.

Dále zmíněný krizový zákon definuje Kritickou infrastrukturou (KI), tím se rozumí prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, jehož narušení by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

2.3 Řízení rizik

Pojmem řízení rizik rozumíme koordinované úsilí o minimalizaci nebezpečí a úspěšné zvládnutí mimořádné události, nebo krizové situace. Na obrázku 6 je znázorněno obecné schéma řízení rizik, popisující jak postupujeme při řízení rizik.



Obrázek 6 Řízení rizik [27]

2.3.1 Riziko

Prvně si definujme riziko. Riziko je všudypřítomný průvodní jev, který působí na výsledky subjektu. Existují pozitivní a negativní rizika. (například zavádění nového výrobku, může způsobit zisky, ale i úpadek). Rizikem vyjadřujeme pravděpodobnost, s jakou nastane nechtěná událost, která muže mít za následek škodu nebo poškozeni. Tuto míru pravděpodobnosti vyjadřujeme procesem analýzy rizik.[26]

Výkladový slovník kybernetické bezpečnosti definuje riziko jako: *„Nebezpečí, možnost škody, ztráty, nezdaru. Účinek nejistoty na dosažení cílů. Možnost, že určitá hrozba využije zranitelnosti aktiva*[20] *nebo skupiny aktiv a způsobí organizaci škodu „* [8]

[20] Aktivum – Cokoliv, co má hodnotu pro jednotlivce, organizaci nebo veřejnou správu.

Rizika můžeme rozdělovat podle míry pravděpodobnosti kdy nastane, podle úrovně, podle dopadu neboli důsledků, podle míry ovlivnitelnosti, podle pořadí působnosti, podle velikosti, podle akceptovatelnosti, podle pravděpodobnosti, a dalších. [25]

Významnost rizika je vyjádřena pravděpodobností výskytu incidentu a mírou dopadu na aktivum

2.3.2 Identifikace rizika

Identifikaci rizik můžeme vnímat jako expozici vůči fyzikálním, chemickým, biologickým a sociálním podmínkám, jež mají škodlivý potenciál. Často se při stanovení rizik ptáme na tři otázky:[22]

- Co nežádoucího se může stát? Co může selhat?
- Jaká je možnost / pravděpodobnost, že se to stane?
- Jak závažné (intenzita, velikost apod.) mohou být účinky (dopady, následky)?

Podle závažnosti je dělení:[25]

- Bezvýznamná: Pravděpodobnost, že se vyskytne nebo případný dopad by byl mírný, až zanedbatelný, bez rizika pro fungování organizace. Maximálně vnitřní.
- Akceptovatelná: Vzniká interně i externě, případným projevením této hrozby vznikají mírná ohrožení, poškození je mírné, nevzniká žádné vážné ohrožení existence
- Nežádoucí: Interní i externí vliv. Dlouhodobě může ovlivnit poškození, ale ne poškození existence.
- Významná: Interní i externí vliv. Dlouhodobě může ovlivnit poškození a hrozí poškození existence.

Prvky rizika jsou: [25]

- Četnost: Vyjadřuje se nejčastěji jako počet událostí za časovou jednotku. Četnost se určuje ze známých dat.
- Důsledky: Jsou dány rozsahem, velikostí a účinkem rizika.
- Hrozba: Možnost výskytu určitého útoku proti určitému cíli.
- Zranitelnost: Možnost selhání bezpečnostních opatření.

2.3.3 Analýza rizik

Je dalším krokem k cíli, a to snižování rizik. Metody stanovení rizik se rozdělují na kvalitativní a kvantitativní a semikvantitativní. Kvalitativní jsou spíše pro obecný ráz identifikace, jsou snazší a jednodušší. Příkladem je subjektivní personalizace nebo kritérium uspořádání. Kdežto kvantitativní poskytují detailnější pohled na daná rizika, jako bodový odhad z historických dat, nebo podle důsledku a četnosti výskytu. Poslední možností je semikvantitativní, které doplňují, které tvoří přechod mezi předcházejícími [25]

2.3.4 Hodnocení rizik

Hodnocení rizika můžeme měřit jeho významnost, která je vyjádřena pravděpodobností výskytu incidentu, hrozby, na aktivum, které bude mít za následek dopad. Hrozba je příčina chtěného i nechtěného incidentu, s možným poškozením systému. Incident je něco nežádoucího, co muže negativně ovlivnit aktivum. Aktivum je vše, co má pro někoho hodnotu, ať už hmotnou nebo nehmotnou. Dopad je hodnota, škody pro aktivum.[8]

2.3.5 Ošetření rizika

Ošetření se skládá a navazuje na předchozí krok, identifikaci rizika. Po níž dochází k realizaci nápravy, či zmírnění důsledku krize. Ošetření krize volí takovou metodu, která bude vést ke zmírnění, či eliminaci krize. Dosáhne-li situace takového bodu, že riziko je nepřijatelné, subjekt od daného rizika ustoupí, neboli nebude realizovat daný projekt. [25]

3 ANALÝZA INFORMAČNÍCH ZDROJŮ SVĚTA

Pro doplnění informací do teoretické části pro praktické metody se neobejdeme bez analýzy informačních zdrojů světa. Také tato analýza informačních zdrojů světa je jedním z úkolů pro vypracování bakalářské práce. Pojem kybernetická bezpečnost není nový pojem, ale posledním desetiletím nabírá na významu. Což je také motivací k vydávání nových publikací, knih, zákonů, norem a v neposlední řadě i vědeckých a akademických pracích. I tato bakalářská práce, jak jsem již uvedl v úvodu práce, byla motivována stále se rozvíjejícímu fenoménu kybernetické bezpečnosti v ČR a světě. V této kapitole analyzuji informační zdroje světa. Zaměřím se na mnou vybrané tištěné knihy a akademické práce, které mě oslovily. Dále na mezinárodní normy ISO[21] platné pro oblast kybernetické bezpečnosti. Se zákony z oblasti kybernetické bezpečnosti v ČR a v EU se seznámíme blíže v kapitole 5.1 Legislativní rámec současné situace.

3.1 Světové zdroje

Ze světových zdrojů mne oslovily přední knihy na poli kybernetické kriminality a bezpečnosti. A to konkrétně kniha The Art of Deception [17], v češtině Umění klamu, od Kevina D. Mitnicka. Autor, který je určitým fenoménem ve světě kybernetické kriminality, se zabývá odvětvím sociálního inženýrství a manipulace s obětí. Popisuje začátky své kariéry a metody jaké se používaly. I když kniha není přesným popisem útoku na skutečné subjekty, popisuje synonymum cílů k reálnému prostředí ze zkušeností jejího autora. Některé poznatky z knihy jsou přínosem pro pochopení fungování sociálního inženýrství, jaké je popsáno v kapitole 1.5.2 Sociální inženýrství. A totiž hlavní fakt, že nejslabším článkem jakéhokoliv, ať už sebelépe zabezpečeného systému, je člověk. A při použití technik sociálního inženýrství, nemusí být útočníkovi znám celý složitý systém dané bezpečnosti, ale stačí správnými technikami a „příběhem“ si o přístup, data, nebo službu prostě požádat příslušnou osobu, většinou administrátora.

Jako další knihu ze světové literatury zabývající se touto problematikou bych vyzdvihl knihu A History of Cyber Security Attacks, 1980 to PRESENT [29], od Bruce Middletona vydanou v loňském roce, v roce 2017. Tato kniha shrnuje hlavní jednotlivé „módní“ vlny kybernetické kriminality od roku 1980 do data vydání knihy, do roku 2016. Tato kniha poskytuje cenné informace, neboť popisuje některé reálné incidenty a útoky.

[21] ISO - International Organization for Standardization – Mezinárodní organizace pro standardizaci

3.2 Akademické práce

Pro analýzu informačních zdrojů akademických prací jsem si vybral zástupce kvalifikačních prací, které svým obsahem řeší problematiku kybernetické bezpečnosti. Tímto zdrojem je diplomová práce: *Vybraná kybernetická rizika a jejich předcházení [30]*. Od autora Bc. Radka Zajíce. Práce popisuje řízení rizik a kybernetických rizik. Analyzuje vybraná kybernetická rizika. Ty popisuje, určuje jejich příčinu a navrhuje možné ošetření rizik. Z těchto rizik zmiňme třeba Kybernetická rizika, incidenty a hrozby, spojené s nejnovějšími technologiemi jako je IoT[22] - internet věcí, IPv6 internet protokol nové generace, využívání technologií cloud computing a moderní směr „Bring your own device“[23], neboli donesení a práce na vlastním zařízení do společnosti.

Druhým je bakalářská práce: *Analýza kybernetických hrozeb eGovernmentu a jejich rizik pro ČR* [31]. Od Bc. Jana Kleinera. Autor se zabývá kybernetickými hrozbami elektronizace státní správy. Identifikuje a na příkladech se snaží objasnit hrozby spojené s eGovernmentem, určuje dopady. Poté zpracovává kvantitativní analýzu rizik pro hrozby českého eGovernmentu.

3.3 Mezinárodní normy

Mezinárodní organizace pro standardizaci ISO rezervovala pro oblast bezpečnosti informací v roce 2009, kdy vyšla první verze, celou sérii norem ISO 27000. Tyto standardy dnes poskytují požadavky na Information Security Management Systems (ISMS), což je systém, který systematicky pracuje s firemními informacemi, aby zůstaly bezpečné. To zahrnuje osoby, procesy a IT systémy a aplikaci řízení rizik. Dodnes bylo vydáno několik desítek jednotlivých norem z rodiny ISO 27k norem. Pro oblast krizového řízení v ČR jsem vybral normu ISO/IES 27032. Norma navrhuje nejlepší praktiky pro řešení otázek, jako jsou například bezpečnost internetu, sítí a ICT[24]. Doporučuje návody pro efektivní sdílení informací a koordinaci řízení incidentů mezi organizacemi, uživateli, vládami a poskytovateli služeb. Zaměřujeme na sociální inženýrství, malware, odcizení identity, řízení rizik v kyberprostoru v rámci organizací a poskytování bezpečných a zabezpečených služeb poskytovateli služeb, tedy na klíčové hrozby týkající se kyberprostoru.

[22] IoT – Internet of Things – „Internet věcí“
[23] Bring your own device – „Přines si svoje zařízení“, jeden z fenoménu práce na soukromém zařízení
[24] ICT – Information communication technology – „Informační a komunikační technologie“

DÍLČÍ ZÁVĚR TEORETICKÉ ČÁSTI

První teoretická část bakalářské práce je věnována objasnění teorie, nutné k orientaci v problematice. Za důležitou informaci je zejména potřeba definice kyberprostoru a jak jej lze chápat z moderního pojetí. Teoretické práce nám poslouží jako jednouchý sborník pojmů kybernetické kriminality, který bude nápomocný při vypracovávání metod v praktické části. Za nejpřínosnější považuji informace ve třetí části, v analýze informačních zdrojů světa. Jsou nám přínosem praktické reálné informace, ze světových informačních zdrojů, o reálných útocích, které se již staly. Dále pak mezinárodní normy, podle nich je dnes tvořena legislativa, a také různorodé pohledy na problematiku v akademických pracích. Tyto informace byly zhodnoceny v praktické části, při vypracovávání modelu a návrhu opatření.

II. PRAKTICKÁ ČÁST

4 METODA ZPRACOVÁNÍ

Za účelem získání co nejpřesnějšího povědomí o stavu kybernetické bezpečnosti v ČR pro vypracování modelu v dalších částech, bude provedena rešerše legislativy, institucí, významnými dokumenty a závazky. Na závěr rešerše bude provedena SWOT analýza současného stavu, která nám kybernetickou bezpečnost v ČR analyzuje ze strategického hlediska. Použité informace budou základním kamenem pro vypracování systémového vyjádření modelu kybernetické bezpečnosti. Na základě oficiálních statistik zveřejňovaných výročními zprávami, i měsíčními publikacemi bude provedena semikvantitativní metoda analýzy rizik. A z výše zmíněného závěrem této práce navrhnout výstupy pro praxi.

4.1 SWOT analýza

SWOT analýza je univerzální a dnes velmi používanou technikou na analýzu vnitřních a vnějších faktorů. Skládá se ze 4 části:

- Strengths - silné stránky
- Weaknesses - slabé stránky
- Opportunities - příležitosti
- Threats – hrozby

Primárně jí používáme pro hodnocení na strategické úrovni celé organizace. Ale lze ji použít na menší a běžnější aspekty jako analýzu hodnocení zaměstnance, analýzu výrobku na trhu. Vnitřní složkou analýzy jsou silné a slabé stránky. Neboli v čem je daná organizace, či produkt na trhu dobrý a v čem tak trochu „pokulhává“. Vnější prostředí je reprezentováno příležitostmi a hrozbami, neboli kladnou a zápornou stránkou. Což jí pomůže zaměřit se na příležitosti v daných oblastech a vyhnutí se hrozbám. Důležité pravidla sestavování jsou zaměřit se na klíčové a důležité věci, fakta a objektivní informace. Je dobré provést analýzu ve více lidech a tím docílit lepší objektivnosti. Při vypracování se ptát na otázky správně, jak pomocí silných stránek využít svou situaci, jak využít tuto situaci k eliminaci slabých stránek, jak silné stránky využít k rozvoji příležitostí a jak s nimi eliminovat hrozby. [23]

4.2 Semikvantitativní analýza rizik

Semikvantitativní analýza rizik je metoda, která popisuje jev částečně kvantitativně a to pouze v dohodnuté stupnici. Neužívají se přesné fyzikální ani jiné jednotky. K hodnocení používá kvalitativně popsané stupnice, těm jsou přiděleny číselné hodnoty, jejichž

kombinací se určí míra rizika. Slouží jako například východisko k bezpečnostním opatřením v provozu. Semikvantitativní analýza používá číselný odhad rizika, kategorie četnosti výskytu a závažnosti důsledků jsou definovány slovně i kvantitativně. Míra rizika je jako u kvalitativní analýzy rizik vyjádřena maticí rizik. [25]

4.3 Systémově vyjádřené Modelování

Modelování můžeme rozumět, jako postup k teoretickému znázornění praktické skutečnosti. Pomáhá nám rozlišit co je a co není podstatné. Model může sloužit jako sjednocení myšlenek, znázornění procesy spojené s plánováním, nebo jen pouhá pomůcka pro pochopení reality. Za cíl má tedy popsaní a zachycení určité reality a uschování. Příkladem takovéhoto modelu může být mapa. Systém, jak je uvedeno v teoretické části, je abstraktní množina prvků určitých vlastností a vzájemných vztahů, zejména vůči okolí. Vůči okolí zaujímá konečný počet vztahů. Rozhodovací postup při modelování má šest kroků [28].

1. Identifikace – podstata problémů modelování.
2. Formulace modelu – charakter cíle modelování.
3. Vlastní realizace – Sběr dat, učení typu model a sestavení modelu.
4. Verifikace výsledků – ověření vůči skutečnosti.
5. Analýza výsledků – na základě verifikace.
6. Shrnutí výsledků

5 ANALÝZA SOUČASNÉHO STAVU KYBERNETICKÉ BEZPEČNOSTI V ČR

V následující kapitole bude provedena rešerše zabývající se analýzou současného stavu kybernetické bezpečnosti v České Republice a ochraně kritické infrastruktury. Výstupy z této rešerše budou základním kamenem pro další kapitoly. Nejdříve se zaměřuje na legislativní rámec současné situace a to z hlediska ČR a poté v rámci EU. Druhá části této kapitoly se zabývá jednotlivými subjekty vládní kybernetické ochrany, jež jsou zmíněnou legislativou ustanoveny. A třetí část se zabývá současným stavem kybernetické bezpečnosti podle naplňování Národní strategie kybernetické bezpečnosti České Republiky na období 2015-2020.

5.1 Legislativní rámec současné situace

Problematice kybernetické bezpečnosti je dnes věnována poměrně velká pozornost. S rostoucí aktivitou, činností a rozvojem informačních a komunikačních technologií v posledních desetiletích se zvyšuje aktivita v kyberprostoru. Proto činnosti státu jako garanta bezpečnosti České republiky, podle čl. 2 ústavního zákona č. 110/1998 SB., o bezpečnosti České Republiky, musí vést k ochraně kritické informační infrastruktury, jejího prvku a systému, která je součástí kritické infrastruktury. Neboť narušení funkce by mělo závažný dopad na bezpečnost státu a zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. Proto 29. 8. 2014 vešel v platnost zákon č. 181/2014 Sb. Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). Jeho účinnost nabyla od 1. 1. 2015, ale naplnění litery zákona dotčenými subjekty vešlo v platnost od 1. 1. 2016. Zákon se rozděluje do 3 oblastí, a to Organizační, technické opatření a bezpečnostní dokumentace. Pro tuto práci nás bude zajímat první oblast, a to řízení rizik. Definici podle kybernetického zákona jsme si uvedli v kapitole 0 Řízení rizik. V roce 2017 byl novelován a to prostřednictvím zákona č. 104/2017 Sb. s účinností od 1. července a zákona č. 205/2017 Sb. s účinností od 1. srpna 2017 Je nutno ještě dodat, že zákon neřeší bezpečnost systému podléhajících utajení. To řeší Zákon č. 412/2005 Sb. Zákon o ochraně utajovaných informací a o bezpečnostní způsobilosti.

Hlavním cílem zákona je [32]:

- stanovit základní úroveň bezpečnostních opatření
- zlepšit detekci kybernetických bezpečnostních incidentů
- zavést hlášení kybernetických bezpečnostních incidentů
- zavést systém opatření k reakci na kybernetické bezpečnostní incidenty,
- upravit činnost dohledových pracovišť.

Jedním z hlavního důvodu jeho novelizace, byla nutnost zakomponovat do české legislativy Směrnici 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, zkráceně Směrnici NIS [35]. Tato směrnice vyplývá ze strategie kybernetické bezpečnosti EU z roku 2013. Jakožto směrnice, nemá direktivní účinek na členské země EU, ale členský stát si jí sám zakomponuje do své legislativy. V ČR toto již plnil výše zmíněný kybernetický zákon. Který po novelizaci naplnil mimo jiné vytvořit 3-složkovou strukturu: 1. složka určuje výkon KB pro vládu, 2. složka určuje zřídit CSIRT[25] teamy, v ČR vládní a nevládní a 3. složka struktury je zřízení jednotného kontaktního místa, v případě ČR to nadále bude vykonávat Národní bezpečnostní úřad. Dále směrnice ukládá povinnost členskému státu se účastnit na mezinárodní spolupráci na strategické a operační úrovni. [35]. Bližší technická a organizační opatření jsou řešena ve Vyhláškách o kybernetické bezpečnosti.

5.2 Odpovědné instituce a orgány kybernetické ochrany v ČR

V teoretické části v kapitole 2.2 jsme si uvedli Orgány a prvky krizového řízení. Že jedním z hlavních cílů je ochrana kritické infrastruktury. Tou je i kybernetická bezpečnost. Mezi hlavní chráněné prvky v kybernetické bezpečnosti patří kritická informační infrastruktura (KII) a významné informační systémy (VIS). Narušení nebo nefunkčnost by měla závažný dopad na bezpečnost ČR. Pro ochranu kyberprostoru je potřeba zřizovat odpovědné instituce a orgány, které po právní úpravě vykonávají určené činnosti, na poli kybernetické bezpečnosti. Dále se musí zřizovat pro plnění závazků vůči NATO a EU.

[25] CSIRT – Computer Security Incident Responce Team – Team počítačové bezpečnosti reagující na incidenty

5.2.1 Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB)

Hlavním subjektem na poli Kybernetické ochrany je Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB).[32] Tento úřad spadá pod Národní bezpečnostní úřad (NBÚ), který je gestorem dohledových pracovišť a národní autoritou pro oblast kybernetické bezpečnosti. NÚKIB 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), z předchozího Národního centra kybernetické ochrany (NCKB). Je ústředním správním orgánem pro kybernetickou bezpečnost, ochrany utajovaných informací a kryptografické ochrany. Dále má za úkol problematiku neveřejných služeb evropského družicového systému Galileo.

Obrázek 7 Operační místnost GovCERT.CZ v NÚKIB [36]

5.2.2 Dohledová bezpečnostní pracoviště

Dle zákona o KB potažmo naplňování směrnic NIS, zřídila Česká Republika dvě dohledová bezpečnostní pracoviště. A to již zmíněný vládní CERT a národní CERT. Oba tyto týmy mají za úkol koordinace, řešení a nakládání s bezpečnostními incidenty, pomoc subjektu pod nimi spadající, osvětu a školící funkci. NÚKIB má za úkol provozovat Vládní CERT[26] České Republiky, nazvaný GovCERT.CZ. Národní CERT vykonává CSIRT.CZ, je vykonávaný dle veřejnoprávní smlouvy uzavřené s Národním bezpečnostním úřadem. A od roku 2011 je provozován sdružením CZ.NIC. Mezi základní úkoly patří řešení a koordinace řešení bezpečnostních incidentů, osvětová a školící činnost a proaktivní služby v oblasti bezpečnosti.

- ***Vládní CERT - GovCERT.CZ***

Má za úkol oblast pojmenovanou jako základní služba. NBÚ jenž rozhoduje, který subjekt spadá pod provozovatele základní služby. Základními službami rozumíme provozování základních, společenských a ekonomických činností (jako energetika, doprava, bankovnictví, infrastruktura trhů, zdravotnictví, vodní hospodářství, digitální infrastruktura, chemický průmysl), pracující s informačními a komunikačními systémy. Jejich narušení by mohlo mít významný dopad na výše zmíněné činnosti. [32]

Obrázek 8 Logo GovCERT.CZ [37]

- ***Národní CERT - CSIRT.CZ***

Má za úkol druhou oblast, tzv. digitální služby. Těmi se rozumí podle §2 písmena l) online tržiště (dochází mezi subjekty k uzavření kupní smlouvy), internetové vyhledávače, poskytovatele „cloud computing[27]“ a další. Rozhodnutí o naplnění subjektu parametrů digitálních služeb, je v kompetenci přímo těchto subjektů za splnění podmínek daných zákonem. Musí splnit definici digitálních služeb, musí být jedním z výše jmenovaných

[26] CERT – Computer Emergency Responce Team – Počítačový team nouzové reakce
[27] Cloud computing – umožnuje přístup k rozšiřitelnému a přizpůsobitelnému uložišti nebo k sdíleným výpočetním zdrojům

subjektů, nesmí být mikro a malé podniky. (mikro = do 10ti zaměstnanců, s ročním obratem 2 mil. eur, malé = do 50 zaměstnanců, a ročním obratem do 10 mil. eur). [35]

Obrázek 9 Logo CSIRT.CZ [38]

5.2.3 Další instituce a orgány

Ministerstvo vnitra - Z hlediska kybernetické bezpečnosti má klíčovou roli jako hlavní gestor elektronizace výkonu veřejné správy (eGovernmentu[28]). Provozuje řadu důležitých informačních a komunikačních systémů, pro fungování státní správy (základní registry, datové schránky, systém Czech Point[29], CMS[30], atd.) a IZS (linka 112).

Policie ČR – Z hlediska hrozeb v kyberprostoru se jedná o orgán činný v trestním řízení, s úkoly vyhledávat, odhalovat a vyšetřovat kybernetickou trestnou činnost. Veškeré trestné činy, páchané v kyberprostoru, jsou upraveny zákonem č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů. Jsou to činy proti důvěrnosti, integritě a dostupnosti počítačových dat a systémů (trestné činy proti majetku). Policie ČR má pro boj s kybernetickou kriminalitou útvar zvaný Národní centrál proti organizovanému zločinu služby kriminální policie a vyšetřování (NCOZ SKPV).

Ministerstvo obrany – Úloha MO je zajištění kybernetické bezpečnosti vojenských komunikačních a informačních systémů a vojenských sítí. V rámci vojenských systému se jedná zejména o Centrum CIRC[31], které patří pod Agenturu komunikačních a informačních systému. Většina vojenských sítí je oddělena od internetu, má nezávislé sítě. Ale několik systému je připojeno, jako třeba Internet Ministerstva obrany (IMO).

[28] eGovernment – Je zkratka elektronizace veřejné správy, za využití moderních digitálních nástrojů.
[29] CzechPoint – Český státní projekt, který umožňuje občanovi, na určitých místech přistupovat do systému katastru nemovitostí, rejstříku trestů a dalších.
[30] CMS - Systém pro správu obsahu, dokumentů, nejčastěji webového obsahu.
[31] CIRC – Computer Incident Responce Capability

Zpravodajské služby ČR – Mezi zpravodajské služby ČR patří Bezpečnostní informační služba, Úřad pro zahraniční styky a informace a Vojenské zpravodajství. Jejich úlohou je získávání a vyhodnocování informací, které mohou ohrozit zájmy a bezpečnost státu a obyvatelstva ČR. V mezích zákona provádí sběr a analýzu informací o hrozbách a rizicích v kyberprostoru.

5.3 Současný stav naplňování významných dokumentů

V současné době jsou v účinnosti dva hlavní dokumenty na poli kybernetické bezpečnosti v české republice. A to je Národní strategie pro kybernetickou bezpečnost České Republiky na období let 2015-2020 [34] a Audit národní bezpečnosti z roku 2016 [33]. Blíže si tyto dva dokumenty představíme.

5.3.1 Národní strategie pro kybernetickou bezpečnost České Republiky na období let 2015-2020

Národní bezpečnostní úřad, coby gestor a národní autorita pro oblast kybernetické bezpečnosti již vydal v pořadí druhou strategii [34]. Bezpečnostní strategie kybernetické ochrany pro rok 2012-2015 se zabývala několika hlavními úkoly, zejména to bylo přijetí kybernetického zákona citovaného v kapitole 5.1, a vytvořením Národního centra kybernetické bezpečnosti. Tím se dal impulz k dalšímu rozvoji a naplňování cílů strategie. S končící platností strategie pro rok 2012-2015 a s plněním hlavních cílů, začal NBÚ pracovat na Národní strategii pro kybernetickou bezpečnost České Republiky na období let 2015-2020. Tato Strategie je nyní ve své polovině. Do legislativ byla zakomponována Směrnice Evropské unie NIS. Došlo k vytvoření vládního a národního pracoviště kybernetické ochrany, opět popsaných v předcházející kapitole.

Spolu s Národní strategií se vydává i Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020, jenž je stejně jako u předchozí strategie nutný k dodržení stanoveného časového rámce, si dává za úkol realizovat a úspěšně naplňovat úkoly uvedené v Akčním plánu. Pro období 2015 – 2020 je definováno celkem 19 výzev, které jmenují možné události, jevy, které mohou v tomto časovém období nastat. Mezi tyto výzvy patří:

1. Česká republika jako možný testovací objekt
2. Nedostatečná důvěra veřejnosti ve stát

3. Vzrůstající počet uživatelů internetu, informačních a komunikačních technologií a narůstající kritičnost jejich selhání
4. Se vzrůstajícím počtem uživatelů mobilních platforem stoupá i množství mobilního malware
5. Možnosti zneužití zadních vrátek hardware pro exfiltraci informací
6. Koncept „internetu věcí“
7. Bezpečnostní rizika spjatá s přechodem z protokolu IPv4 na IPv6
8. Bezpečnostní rizika spjatá s elektronizací veřejné správy (eGovernment)
9. Nedostatečné zabezpečení malých a středních podniků
10. Big data, skladování dat v nových prostředích
11. Ochrana průmyslových řídicích systémů a informačních systémů ve zdravotnictví
12. Inteligentní energetické sítě
13. Vzrůstající závislost obranných složek státu na informačních a komunikačních technologiích
14. Malware je stále sofistikovanější
15. Botnety a DDoS/DoS útoky
16. Nárůst informační kriminality
17. Hrozby a rizika spjaté s užíváním sociálních sítí na internetu
18. Nízká digitální gramotnost koncových uživatelů
19. Nedostatek odborníků na kybernetickou bezpečnost a nutnost revize stávajících studijních programů ve školství

5.3.2 Audit národní bezpečnosti

Audit národní bezpečnosti za rok 2016 byl posledním vydaným auditem. [33] V úvodní části dokumentu je pojednáváno o situaci v Evropě a jejímu vlivu na bezpečnost České Republiky. Po zasedání expertů z oblasti všech bezpečnostních komunit byl vydán audit, který shrnuje deset nejvýraznějších hrozeb pro ČR. Tyto témata podle auditu nejsou kompletním soupisem všech hrozeb, ale pouze výtažkem těch nejzávažnějších. Kterým musí aktivně čelit a být na ně připravena reagovat. Dále úvodní ustanovení auditu se věnuje tématu koordinace při vyhodnocování hrozeb. Zde poznamenává, že je potřeba více propojit veřejný a soukromý sektor na poli odborných diskuzí a spolupráce. Poslední část úvodního ustanovení se zabývá potřebou vědeckého a vzdělávacího rozvoje, pro schopnost dále rozvíjet metody a výchovu odborníku na bezpečnost. Deset nejvýraznějších hrozeb je [33]:

1. Terorismus
2. Extrémismus
3. Organizovaný zločin
4. Působení cizí moci
5. Bezpečnostní aspekty migrace
6. Přírodní hrozby
7. Antropogenní hrozby
8. Hrozby v kyberprostoru
9. Energetická, surovinová a průmyslová bezpečnost
10. Hybridní hrozby a jejich vliv na bezpečnost občanů ČR

Pro naši práci si blíže představíme Hrozby v kyberprostoru. Zde zadání auditu určilo pět nejvýraznějších hrozeb pro celkovou bezpečnost kybernetického prostředí ČR. Tyto hrozby jsou:

1. Kybernetická špionáž
2. Narušení nebo snížení odolnosti IT infrastruktury
3. Nepřátelské kampaně
4. Narušení nebo snížení bezpečnosti eGovernmentu
5. Kyberterorismus

5.4 SWOT analýza kybernetické bezpečnosti v ČR

SWOT analýza je, jak jsme si uvedli v určení metodiky práce, ideální pro strategickou analýzu jakou kybernetická bezpečnost ČR je. Na základě rešerše současného stavu kybernetické bezpečnosti v ČR, uvedené v předchozích kapitolách, byla sestavena SWOT analýza pro definování silných a slabých stránek současného stavu naplňování kybernetické bezpečnosti. Při vypracování příležitostí a hrozeb jsem spolupracoval s týmem mých kolegů, s mnohaletou praxí v oboru IT a systémové správy serveru, ve statním sektoru.

Obrázek 10 SWOT analýza [11]

Silné stránky:

- Legislativní rámec, přijaté zákony a vyhlášky, implementované směrnice EU
- Fungující pracoviště dohledů, vládní GovCERT.CZ a národní CSIRT.CZ
- Dobrá spolupráce mezi zahraničními autoritami CERT a CSIRT teamu
- Rozvíjející se spolupráce s veřejným sektorem a veřejnými teamy CERT A CSIRT
- Dodržování Akčního plánu Národní strategie a výroční zprávy o naplňování
- Vypracovaná metodická podpora, konzultace a probíhající určování systému jako KII a VIS

Slabé Stránky:

- Nedostatečná podpora z vedení pro budování bezpečnostních politik, zejména zdlouhavé schvalování u subjektů státní správy.
- Nedostatečná identifikace aktiv a jejich určování
- Nedostatečná identifikace uživatelů, zejména s jejich životním cyklem
- Nedostatečná fyzická bezpečnost, režim vstupu a přístupu k technologii a vymezených prostor
- Celo-instituční problém personální obsazenosti odborníky a specialisty na ICT a kybernetickou bezpečnost
- Konkurence na trhu práce není nastavena adekvátně, nebo-li neschopnost kvalitně tyto pracovníky finančně ohodnotit

- Celkově omezené finanční prostředky na akvizici technologií a budování prvků kybernetické bezpečnosti
- Slabá informovanost obyvatel o eGovementu

Příležitosti:

- Personálně a technologicky posilovat prvky kybernetické bezpečnosti v rámci NÚKIB
- Dále pravidelně revidovat legislativní rámec problematiky
- Spolupracovat více s partnerskými CERT a CSIRT teamy v okolních státech a prohlubovat vzájemnou pomoc a sdílení informací
- Více se angažovat v akademické sféře při výchově nových odborníků na kybernetickou bezpečnost
- Zavádět školící centra pro informační a kyberneticko-bezpečnostní osvětu u zaměstnanců státní správy, KII a VIS, a dalších.
- Prohlubovat spolupráci s civilními centry kybernetické bezpečnosti

Hrozby:

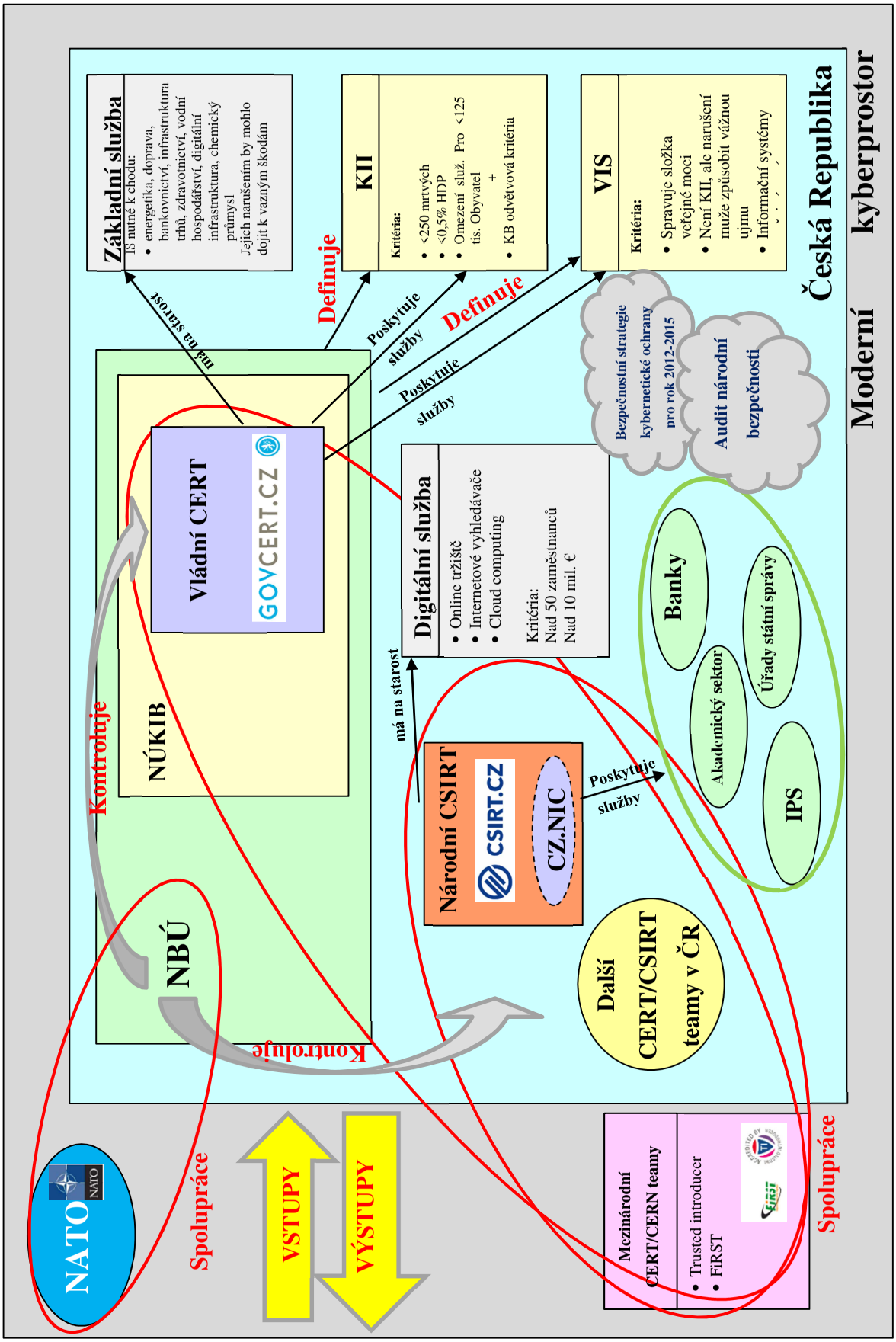
- Působení vlivu cizí moci, kybernetická špionáž a metody hybridního válčení
- Nepřátelské kampaně pod státní záštitou cizích státu
- Hrozby narušení KII, VIS jakožto i funkčnost eGovernmentu
- Outsourcing technologie ICT a s tím spojená rizika s rozšiřujícím se okruhem potenciálních hrozeb
- Dostupnost nástrojů a metod k provádění kybernetické kriminality a kyberterorismu
- Rozšíření zařízení typu smartphone, tablety, atd. a s nimi spojené riziko zneužití při kybernetickém útoku
- Špatné uplatňování bezpečnostních politik u institucí a organizací, zejména neukázněností uživatelů jako instalace nepovoleného sw, navštěvování internetových stránek se závadným obsahem, připojování neprověřených paměťových a jiných externích zařízení

6 SYSTÉMOVÉ VYJÁDŘENÍ MODELU KYBERNETICKÉ BEZPEČNOSTI ČR A HODNOCENÍ JEJICH RIZIK

V této kapitole bude provedeno sestavení systémově vyjádřeného grafického modelu kybernetické bezpečnosti v ČR, na základě rešerše v předchozí kapitole. To bude provedené s ohledem na okolní kyberprostor ČR a světový kyberprostor. To proto, že strategie České Republiky dodržuje princip sdílené bezpečnosti, nebo-li nelze kybernetickou bezpečnost České republiky oddělovat od kybernetické bezpečnosti globální, potažmo evropské a severoatlantické oblasti. Toto modelování musí nahlížet tento úzce propojený fakt. Martina Janková ve své grantové publikaci“ Možnosti systémového prostředí ICT v kyberprostoru podniku uvádí [40], že kyberprostor, jenž se objevuje procesu modelování moderní oblasti řízení projektu, umožnuje pohled na systém jako celek a jeho podsystémy a procesy, čímž zajistí optimální chování reálných kybernetických systémů, sledování odezev na podněty, vyjadřování stability modelovaných systémů a jejich efektivního řízení. To vede k provozování bezpečných ICT vzhledem k novým aktivitám informačních útoků na tyto systémy. Tímto docílíme dalšího bodu cílů práce a tím je vypracování systémového vyjádření modelu zadané problematiky, zajištění kybernetické bezpečnosti v ČR.

6.1 Model kybernetické ochrany v ČR

Model kybernetické ochrany v ČR na obrázku [10] slouží pro pochopení složitosti mezi entitami modelu. Nejprve je potřeba si definovat jednotlivé objekty, entity a vazby mezi nimi. Výčet objektů je dán zdrojem dat a tím byl zvolen rozbor písemných materiálů. Mezi tyto materiály patřily legislativní prvky, jež jsou definovány v kapitole 5.1, dále metodiky a postupy jsou pomocnými publikacemi národních a vládních dohledových prvků [37][38] a také platných norem analyzovaných v kapitole 3.3.



Obrázek 11 - Model kybernetické bezpečnosti ČR [11]

Popis:

Hlavní vrstvou je kybernetická vrstva moderního pojetí kybernetického prostoru světa, do kterého patří Česká republika. Zde je hlavní autoritou pro kybernetickou bezpečnost Národní bezpečnostní úřad, který zřizuje a spravuje podsystém, vládní CERT (GovCERT.CZ). Ten má na starosti prvky základní služby. Zároveň poskytuje služby entitám KII a VIS. Ty jsou definovány a určovány NBÚ. A vůči vládnímu CERTu plní povinnost ohlašování incidentu a informovanost o kontaktech. Na základně veřejnoprávní smlouvy je správcem národního CSIRT sdružení CZ.NIC. To plní stejné funkce a služby jako vládní CERT. Má na starosti entitu digitálních služeb a poskytují služby entitám, které splňují parametry pro specifikace digitálních služeb. Oba týmy kontroluje NBÚ a oba týmy stejně jako NBÚ, participují na mezinárodní spolupráci se zahraničními týmy CERT a CSIRT. Zároveň prochází pro tyto účely certifikaci u společnosti jako je Trusted introducer[32] a FiRST[33]. Na celý kyberprostor České republiky se vztahují dokumenty Národních strategií pro kybernetickou bezpečnost České Republiky na období let 2015-2020 a Audit národní bezpečnosti.

6.2 Hodnocení rizik

Po vytvoření modelu je dalším z cílů práce je provést hodnocení možných rizik kybernetických útoků na prvky krizového řízení. Na základě čehož bych rád odpověděl na otázku: Které rizika jsou podle současného vývoje řešených incidentu nejvýznamnější? A tím se zaměřil na návrh do praxe k jejich zmírnění. Analýza rizik informačních systémů v praxi se skládá z procesu mapování IS, zmapování aktiv jednotlivých subjektů. Tím si zjistíme, jaká aktiva jsou pro bezpečnost ČR důležitá. Dále pak na takzvaná podpůrná aktiva.

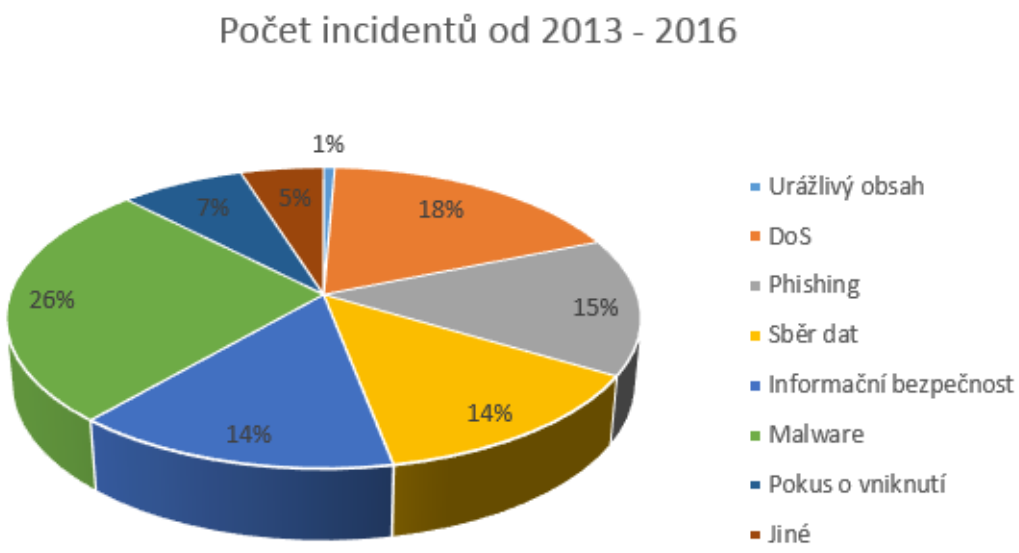
- Primární aktiva – Bývají to zpravidla informace, které se zpracovávají a uschovávají na daných prvcích KII
- Sekundární (podpůrná aktiva) – Většinou je chápeme jako prostředí, IS, v němž zpracováváme primární aktiva. Tím je dáno, že jsou nezbytně nutné pro chod primárních aktiv

[32] Trusted introducer - Spravuje seznam známých bezpečnostních týmů a akredituje a certifikuje je.
[33] FiRST – Organizace spojující spolupráci světových CSIRT a CERT

Pro chápání obsáhlosti celého procesu určování aktiv si uveďme, jaké oblasti se toto týká. V rámci infrastruktury a jejich organizací může jít zejména o počítačové sítě, které propojují celé kybernetické systémy. Součástí sítí, je použití prvků jako router, switch, nebo vedení v sítích metalickým, nebo dnes již používanějším optickým kabelem. Dále jde o vlastní koncové prvky sítě, které se skládají ze serveru, terminálů, sloužících k připojení k serveru, na jednotlivých počítačích běžící operační systém, a softwarové vybavení. Zjednodušeně, ve strategické úrovni dnes není schopna jedna entita určit aktiva celého kybernetického systému. Toto určování vzhledem je k časové a finanční náročnosti komplexní analýzy rizik, preferováno zpracováním analýzy rizik v každém jednotlivém subjektu nad jejich aktivy. Dle Národní strategie kybernetické bezpečnosti ČR na roky 2015-2020, tento proces pokračuje určováním KII a VIS. Rizika informační, tak souvisí s možnostmi napadení a zneužití kritických informací a systémů informačních technologií, které zpracovávají, uchovávají a přenášejí tyto informace. Ze všech výše uvedených důvodu jsem za relevantní zdroj dat zvolil výroční zprávy o stavu kybernetické bezpečnosti České republiky. V době psaní této práce, byla Zpráva o stavu kybernetické bezpečnosti České republiky 2017 stále ve schvalovacím procesu Bezpečnostní radou státu a vládou. Identifikaci rizik jsem tedy provedl na základě statistických údajů NÚKIB, z výročních zpráv z let 2013 – 2016, publikovaných na stránkách NÚKIB. [39] Což ale pro naši studii bude stačit.

Klasifikace	2013	2014	2015	2016	CELKEM	
Urážlivý obsah	4	0	0	0	4	0,7%
DoS	19	9	3	80	111	18,2%
Phishing	18	22	20	30	90	14,7%
Sběr dat	3	1	3	75	82	13,4%
Informační bezpečnost	3	3	76	6	88	14,4%
Malware	47	30	36	48	161	26,4%
Pokus o vniknutí	5	8	5	27	45	7,4%
Jiné	1	8	3	18	30	4,9%
CELKEM	100	81	146	284	611	

Tabulka 1 Počet incidentu hlášených na NÚKIB [11]



Obrázek 12 Graf incidentů za dané období [11]

Z výše zmíněného lze vyčíst, že za období 2013 – 2016 řešil NÚKIB, potažmo jimi spravující GovCERT.CZ celkem 611 incidentu. Toto číslo se zdá býti malé. Pokud totiž srovnáme, že za uvedené období národní CSIRT (tou dobou, 2013-2015, samozřejmě nebyl ještě v roli národní CSIRT.CZ) zaznamenalo celkem 3717 útoků. Je potřeba bráti v úvahu několik skutečností. Pole působnosti národního CSIRTU jsou jiné, jmenované v kapitole 5.2.2., a to digitální služby. Na které se utočí častěji i z principu věcí. Dalším podstatným faktem je to, že řada prvků KII se teprve v uvedené období, „určovala". A stále probíhá její proces určování. Posledním faktem uveďme i to, že některé subjekty neplní povinnost informovat o incidentu, jak jim to ukládá zákon. Což uvádí NÚKIB ve svých výročních zprávách.

Pro hodnocení rizik je dle uvedené metodiky zpracování. Tedy jsme si vybrali rizika, která by mohla způsobit škodu na některém z aktiv. Pro hodnocení rizik nám tedy chybí vytvoření matice rizik a na základě ní, určení významnosti námi vybraných rizik.

Pravděpodobnost rizika

Dopad rizika

dopad / pravděpodobnost	Vzácný - 1	Možný -2	Pravděpodobný-3	Téměř jistý - 4
Nízký - 1				
Střední - 2				
Vysoký - 3				
Kritický -4				

Tabulka 2 Matice rizik [11]

V matici rizik máme dvě osy. Osa dopadu rizika a osa pravděpodobnosti. Osu dopadu rizika si určíme na základě dopadové tabulky vydané NÚKIB [32] (Dopadová tabulka NÚKIB přiložená jako Příloha č.1). Druhou osu si určíme na základě uvážení jaká je pravděpodobnost, že toto riziko nastane. Jak uvádí R. Zajíc ve své práci „*Vybraná kybernetická rizika a jejich předcházení*" [30], pravděpodobnost je vždy individuální a hodnotitel analýzy rizik jí musí věnovat náležitou péči. Po prostudování statistik a publikací

vydaných NÚKIB a národního CSIRT jsem určil pravděpodobnost od Vzácné, až po téměř jistou. Uvedeným úrovním jsem určil hodnotu od 1 do 4.

Pro stanovení rizika si vypočteme rizika podle vzorce R = P x Z neboli míra rizika R, se rovná součinu pravděpodobnosti a důsledků rizika.

Mezní hodnoty jsou tedy následující:

- 1 – 2 : Nízké, přijatelné riziko
- 3 – 7 : Zvýšené riziko
- 8 - 16 : Vysoké riziko

6.2.1 Urážlivý obsah

Na základě statistických dat NÚKIB a určení míry pravděpodobnosti podle analýzy incidentů národního a vládního pracoviště dohledu CERT/CSIRT:

- Pravděpodobnost rizika: 1
- Dopad rizika: 1

Celkem: 1

Urážlivý dopad se příliš nevyskytoval, v počtu incidentu pouze 1% a riziko je také nízké. Výsledná hodnota je tedy 1.

6.2.2 DoS – Denial of service (odepření služby)

Na základě statistických dat NÚKIB a určení míry pravděpodobnosti podle analýzy incidentů národního a vládního pracoviště dohledu CERT/CSIRT:

- Pravděpodobnost rizika: 3
- Dopad rizika: 4

Celkem: 12

DoD Denial of service (odepření služby) se podílelo na incidentech za uvedené období celkem 18,2 %. Z daného určení vyplývá, že se jedná o poměrně významné riziko, zejména při zvážení faktu, že vyřazením může dojít k závažným škodám.

6.2.3 Phishing

Na základě statistických dat NÚKIB a určení míry pravděpodobnosti podle analýzy incidentů národního a vládního pracoviště dohledu CERT/CSIRT:

- Pravděpodobnost rizika: 4
- Dopad rizika: 4

Celkem: 16

Jedná se o bezesporu jeden z nejrizikovějších útoků. Vede ve statistikách národního CSIRT a i ve statistice vládního CERT je třetí. Z důvodu dnešní nízké odolnosti a pozornosti na tento typ útoku, zejména uživatele se jedná o nejnebezpečnější útok naší analýzy.

6.2.4 Sběr dat

Na základě statistických dat NÚKIB a určení míry pravděpodobnosti podle analýzy incidentů národního a vládního pracoviště dohledu CERT/CSIRT.

- Pravděpodobnost rizika: 2
- Dopad rizika: 2

Celkem: 4

Následující riziko národní CSIRT ještě rozděluje na Probe[34], nebo-le sondu a Portscan[35]. Jedná se ale obecně o zjišťování informaci o dané entitě, subjektu. Za cíl může být rozkrytí dané struktury za účelem budoucího útoku. Proto se výslednou hodnotu 4.

6.2.5 Informační bezpečnost

Na základě statistických dat NÚKIB a určení míry pravděpodobnosti podle analýzy incidentů národního a vládního pracoviště dohledu CERT/CSIRT.

- Pravděpodobnost rizika: 3
- Dopad rizika: 2

Celkem: 6

Mezi informační bezpečnost řadíme útoky na databáze institucí, nebo-li obecně tu část IS, která se zabývá informacemi. Ať už ve formě ukládání, zpracování a ukládání dat.

[34] Probe – Skenování celého rozsahu IP adres organizace- hledání konkrétního portu k útoku
[35] Portscan – Skenování celkových portů

6.2.6 Malware

Na základě statistických dat NÚKIB a určení míry pravděpodobnosti podle analýzy incidentů národního a vládního pracoviště dohledu CERT/CSIRT.

- Pravděpodobnost rizika: 4
- Dopad rizika: 4

Celkem: 16

Malware je dnes úzce spojen s útokem typu phishing a podobně. Jedná se tedy o opět jeden z nejnebezpečnějších typů útoků.

6.2.7 Pokus o vniknutí

Na základě statistických dat NÚKIB a určení míry pravděpodobnosti podle analýzy incidentů národního a vládního pracoviště dohledu CERT/CSIRT.

- Pravděpodobnost rizika: 2
- Dopad rizika: 2

Celkem: 4

Pokus o vniknutí je opět úzce spojem s bezpečností informací. Útočník může být zastaven, ale muže proniknout a opět sloužit, jako budoucí útok kritičtějšími metodami.

6.2.8 Jiné

Na základě statistických dat NÚKIB a určení míry pravděpodobnosti podle analýzy incidentů národního a vládního pracoviště dohledu CERT/CSIRT.

- Pravděpodobnost rizika: 1
- Dopad rizika: 2

Celkem: 2

Tyto jiné útoky NÚKIB hodnotí, jako hrozby které se odehrály jen jednou, ale jejich význam nelze podceňovat. Dle národního CSIRT je tento typ řazen jako tzv. IDS. Jedná se o osamocené, ale podezřelé pokusy o útok.

7 VÝSLEDKY MODELOVÁNÍ A NÁVRHY PRO PRAXI

Po zpracování SWOT analýzy stavu kybernetické bezpečnosti ČR a zpracování hodnocení rizik útoku na KII, je třeba okomentovat tyto rizika a navrhnout možnosti pro minimalizaci hrozeb a zvyšování kybernetické bezpečnosti. Tato poslední kapitola spojuje výše uvedené poznatky.

Dnešní úroveň komunikačních a informačních technologii ve státním sektoru se výrazně liší, co se zajištění kybernetické bezpečnosti týče. Vlivem přijetí zákona o kybernetické bezpečnosti se ujednotil pohled na problematiku přístupu k určování prvků KII, definovaly se orgány a instituce odpovědné za kybernetickou bezpečnost. A jsou jasně definované povinnosti správců KII dané zákonem.

Zákon o kybernetické bezpečnosti jasně definoval tři hlavní oblasti kybernetické bezpečnosti.

1. Organizační opatření
2. Technická opatření
3. Bezpečnostní dokumentace

Ty nám mohou být vodítkem při navrhování ošetření rizik. Výsledky hodnocení rizik nám ukázali jako hlavní hrozbu Fhishingu a malware, následovaném hrozbou DoS/DDoS. Při posouzení možných ošetření rizik můžeme postupovat tvrdou a měkkou cestou. Mezi měkkou patří osvěta osob v institucích pracujících a stanovení pevných pravidel práce těchto pracovníků v kyberprostoru KII. Dále provádění kontrol a auditů. Měkká cesta je však nebezpečná a selhání lidského faktoru. Proto je potřeba i uplatnit princip tvrdého opatření. Tím je systémové nastavení k oprávnění a přístupu k IS. Dále nasazení technických prostředků, softwarů a dalších prvků.

Mezi základní technické opatření se řadí autentizace osob. Prováděná za účelem identifikace identity osoby. Je realizovaná například pomocí hesel, snímačů biometrických vlastností osob (otisky prstů, snímání sítnice, a další), nebo použitím magnetických, čipových karet, autentizačních kalkulátoru, či vlastnictví digitálního podpis. **Pro autentizaci pracovníku navrhuji používat tyto technické prostředky a vést osvětu s jejich správným nakládáním.**

Ve vztahu k pracovníkům je potřeba rozvíjet povědomí o kyberprostoru a jeho úskalí. Dnes již se nikdo nepozastaví nad tím, že zamykáme své auto, že před odchodem z domu

zavřeme dveře, okna a povětšinou i aktivujeme elektronické zabezpečovací zařízení. Ale stále ještě mnoho běžných lidí si není schopno nastavit bezpečné heslo. To je také využívané útočníkem, kterému stačí „zkusit“ heslo kterým se uživatel přihlašuje do své osobní elektronické pošty, do podnikového přihlášení. Pokud patříte mezi uživatele, kteří používají jedno z těchto 30-ti nejpoužívanějších hesel [41]. Pro příklad uveďme prvních 5:

1. 123456
2. Password
3. 12345678
4. Qwerty
5. 12345

Tak byste měli vážně uvažovat o jeho změně. Základem by mělo být použití alespoň 8-10 znaků, alespoň jeden velký znak a jeden speciální znak.

Po zajištění autentizace je potřeba tyto identifikované osoby také autorizovat, neboli určit co mohou v systému dělat. A to určit jednotlivé úrovně, privilegii uživatelů. Například účetní by měla míti přístup do finančního software, ale určitě ne například do databáze objektů v GIS[36] dané organizace.

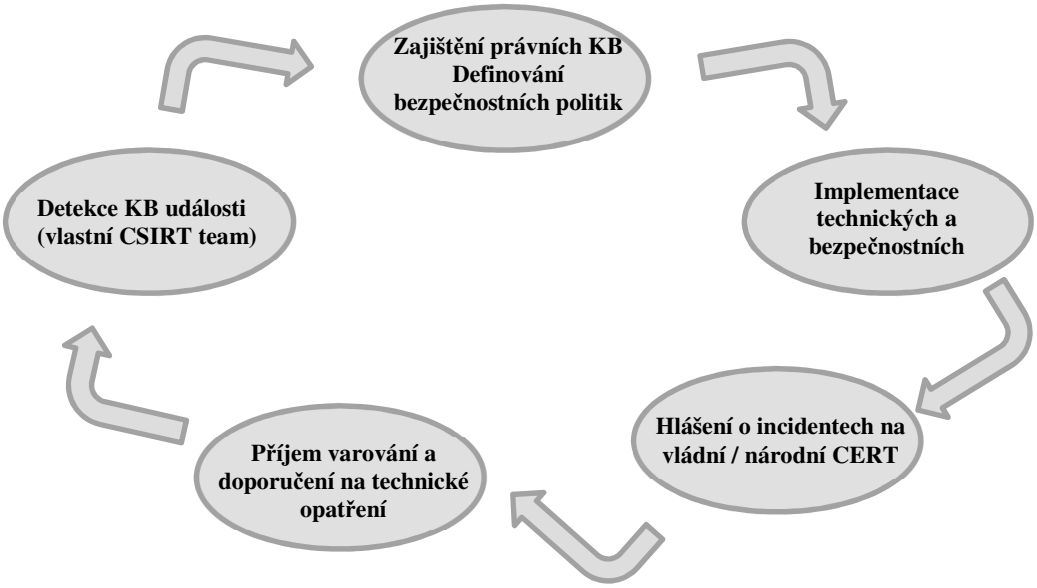
Pro zajištění důvěryhodnosti, autenticity a integrity dat, ať už to do organizace vstupujících, zpracovávajících, či vystupujících doporučuji použití prvků kryptografie. Ta je naukou o metodách převodu informaci jen za použití speciálních okolnosti. Mezi základní metody proto musíme zařadit provozování webových portálu organizace s podporou komunikace https[37], jenž jsou dnes při vytváření téměř standardem. Ale některé portály vyvíjené a posledních 10 let stále běží na nezabezpečeném protokolu http. **A jednu z dnes nejdůležitějších metod a to je certifikace počítačových systému, programového vybavení, digitálních podpisů a distribuce těchto certifikátů. Tyto subjekty zvané Certifikační autority (CA), vydávají digitální certifikáty, čímž potvrzují pravdivosti údajů v PKI[38] distribucích. Za pomocí těchto metod poté můžeme důvěřovat přenosu informací a subjektům. V České Republice je několik komerčních certifikačních autorit, ale zmiňme Ministerstvo vnitra České Republiky, které dnes poskytuje národní certifikační autoritu - Česká národní certifikační autorita – CSCA.**

[36] GIS – Geografický informační systém
[37] https - (Hypertext Transfer Protocol Secure) - Protokol umožňující zabezpečenou komunikaci v počítačové síti.
[38] PKI - Public Key Infrastructure – správa a distribuce veřejných klíčů.

Jakýkoli systém instituce v KII by měl používat nástroje pro zvýšení bezpečnosti systému. A to Antivirový software, který detekuje, identifikuje a eliminuje počítačové viry a škodlivý software - malware. Firewall, který řídí a zabezpečuje síťový provoz mezi sítěmi. Správce IS KII dále nesmí ani zapomínat na zálohování dat, k prevenci jejich ztráty nebo poškození. Zálohování zdroje energie, pro funkci kritických prvku IS KII v případě výpadku elektrické energie.

Jako nedílnou součást jakéhokoliv opatření je potřeba zpracovávat v organizacích dokumentaci. Ta je důležitou součásti bezpečnostní politiky a měla by obsahovat minimálně tyto informace. Specifikace systému, zde by měla být popsána architektura systému a jeho definice v KII. Manuály systému, popisující HW a SW a jak s ním pracovat a nakládat. A zejména provozní manuály procesu, kde jsou definovány konkrétní systémy, konfigurace, odpovědné osoby a chod systému a procesy a chování personálu na typové situace.

Instituce a organizace čeká dlouhá cesta k nastavení stabilní situace, která bude muset pružně reagovat na aktuální otázky bezpečnosti. Na obrázku: Obrázek 13 Návrh postupu při uplatňování ZKB , je uveden návrh opatření, která by měli vykonávat ve vztahu k plnění litery kybernetického zákona.



Obrázek 13 Návrh postupu při uplatňování ZKB [11]

Organizace musí zajistit plnění právních norem a zákonů. Musí dostatečně implementovat požadované technické a bezpečnostní opatření. Vést reportování a přijímaní reportů. Celý tento koloběh incidentů, aktiv, organizační struktury, rizika, protiopatření, je

nekončící koloběh. Po skončení analýzy rizik a jejich ošetření je potřeba dále s riziky pracovat a pravidelně cyklus opakovat.

Na závěr si shrneme základní opatření pro minimalizaci hrozeb:

- **Roztřízení IT vybavení (HW, SW), určení aktiv instituce/organizace**
- **Zavedení politiky kybernetické bezpečnosti, zpracování dokumentace a vyžadování jejího dodržování**
- **Správně provedená personální bezpečnost, určování přístupu uživatelů, jejich autentizace a autorizace.**
- **Zabezpečení přístupu do internetové sítě aplikací softwarových/hardwarových firewallů**
- **Užití antivirových softwarových produktů a jejich pravidelná aktualizace virových databází.**
- **Aktualizace všech prvků počítačových sítí. (operační systémy, SW produkty)**
- **Provádění auditů na všech úrovních organizace a zpracování informaci z nich získaných**

Tento výčet není etalon všech opatření, patři ale mezi ty základní, kterými dnes musí disponovat každá organizace působící jako prvek KII.

ZÁVĚR

Tato bakalářská práce se zabývala pojmem zhodnocení rizik a jejich hrozeb pro krizový management. Pro zhodnocení jsem si vybral prvky kritické informační infrastruktury, jenž jsou součásti kritické infrastruktury každého moderního státu. Cílem práce bylo hodnocení rizik pro KII a vypracování systémově vyjádřeného modelu KB. A na základě získaných informací navrhnout vhodná opatření, pro snížení rizik, do praxe.

Práce byla rozdělena na teoretickou a praktickou část. V teoretické části byly definovány pojmy potřebné k porozumění problematiky. Zejména se jednalo o kybernetiku, kyberprostor, kybernetický systém, rizika a bezpečnost. A definováno bylo krizové řízení v ČR. Tato část sloužila jako sborník pro rozbor dalších částí práce. Závěrem teoretické části byla analýza informačních zdrojů světa, jakožto nedílná součást doplnění teoretických informací o celosvětovém fenoménu, jakým kybernetické hrozby nepochybně jsou. Fakta z těchto zdrojů nám pomohla určit některé procesy při návrhu pro praxi. Zejména mezinárodní normy ISO 27k v oblasti KB. Praktická část, byla rozdělená také na tři části. A v úvodu této praktické části byla určená metodika zpracování. První kapitola zpracovává rešerši o současném stavu kybernetické bezpečnosti v ČR. Detailně rozebírá legislativu, zejména zákon č. 181/2014 Sb. tzv. kybernetický zákon. A platné vyhlášky, které upřesňují jednotlivé oblasti. Garantem KB v ČR je NBÚ a jeho Národní úřad pro kybernetickou a informační bezpečnost, dnes plní účel vládního pracoviště CERT. A na základě veřejnoprávní smlouvy mezi NBÚ a sdružením CZ.NIC, spravuje toto sdružení národní CSIRT pracoviště. Byl zde taky uveden současný stav naplňování dvou nejvýznamnějších dokumentu KB a to: Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 a Audit národní bezpečnosti. Ve druhé kapitole, praktické části bylo provedeno vypracování systémově vyjádřeného modelu KB v ČR na základě informací z rešerše. Hrozby, vybrané na základě SWOT analýzy v rešerši a na základě analýzy statistik incidentu vládního CERTu, získané z výročních zpráv, nám definovali jednotlivé rizika. Ze kterých jsme určili semikvantitativní analýzou nejvýraznější rizika. Těmi jsou hlavně útoky phishing, malware a Dos/DDoS. Na základě všech metod byl v závěrečné kapitole proveden návrh opatření k zmírnění rizik, a tím splnění všech cílů práce. Kybernetická bezpečnost je nekončícím koloběhem hodnocení bezpečnosti, návrhem, realizací, kontrolou, monitorováním a řízením kybernetických rizik. Tato práce mně rozšířila povědomí o rozsáhlosti KB v ČR a poskytne mě cenný úvod do problematiky pro další studium.

SEZNAM POUŽITÉ LITERATURY

[1] WIENER, Norbert. *Kybernetika neboli řízení a sdělování v živých organismech a strojích*. Praha: SNTL, 1960. Řada teoretické literatury.

[2] JIROVSKÝ, Václav. *Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praha: Grada Publishing, 2007. ISBN 978-80-247-1561-2.

[3] SCHNEIDER, Gary P., Jessica EVANS a Katherine T. PINARD. *The internet: illustrated*. 6th ed. Boston, MA: Course Technology Cengage Learning, 2010. Jak na to snadno a rychle. ISBN 978-0-538-75098-1.

[4] KIRSTEIN, Peter T. Early experiences with the ARPANET and Internet in the UK. *DEPARTMENT OF COMPUTER SCIENCE: Systems and Networks Research Group*[online]. Londýn, 13. květen 2016 [cit. 2018-01-20]. Dostupné z: http://nrg.cs.ucl.ac.uk/internet-history.html

[5] METZ, Cade. HOW THE QUEEN OF ENGLAND BEAT EVERYONE TO THE INTERNET. In: *WIRED* [online]. 25.12.2012 [cit. 2018-01-20]. Dostupné z: https://www.wired.com/2012/12/queen-and-the-internet/

[6] ČESKO. § 2 odst. 1 písm. a) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Zákony pro lidi.cz [online]. [cit. 20. 1. 2018]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181#p2-1-a

[7] Cyberspace. *Oxford Dictionaries* [online]. Oxford University Press, 2018, 2018 [cit. 2018-01-20]. Dostupné z: https://en.oxforddictionaries.com/definition/us/cyberspace

[8] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013 [cit. 2018-04-25]. ISBN 978–80–7251–397–0.

[9] PRUKNER, Vítězslav a Jaromír NOVÁK. *Základy managementu* [online]. Olomouc: Univerzita Palackého v Olomouci, 2014 [cit. 2018-01-20]. ISBN 978-80-244-4182-5. Dostupné z: https://publi.cz/books/189/Cover.html

[10] ERNEST, Petr. *Teorie systémů* [online]. 2004 [cit. 2018-01-20]. Dostupné z: http://labe.felk.cvut.cz/~obitko/xkui/materialy/systemy.pdf

[11] Vlastní tvorba

[12] Creeper Virus: Definition - What does Creeper Virus mean?. *Techopedia: The IT Education Site* [online]. 2018, 2018 [cit. 2018-01-20]. Dostupné z: https://www.techopedia.com/definition/24180/creeper-virus

[13] JANOUŠEK, Michal. *KYBERTERORISMUS: TERORISMUS INFORMAČNÍ SPOLEČNOSTI* [online]. In: . 2006, s. 65-66 [cit. 2018-01-21]. DOI: 10.3849/1802-7199. Dostupné z: http://www.obranaastrategie.cz/cs/archiv/rocnik-2006/2-2006/kyberterorismus-terorismus-informacni-spolecnosti.html#.WmRnmK7iZ9M

[14] Whistle-blower. *Oxford Dictionaries* [online]. Oxford University Press, 2018, 2018 [cit. 2018-01-20]. Dostupné z: https://en.oxforddictionaries.com/definition/us/whistle-blower

[15] STODOLA, Petr. *KYBERNETICKÁ A INFORMAČNÍ VÁLKA: Ochrana a obrana proti kybernetickým útokům* [online]. In: . Brno: Univerzita obrany [cit. 2018-01-21]. Dostupné z: https://moodle.unob.cz/pluginfile.php/20733/mod_resource/content/2/KIV%20T-9.pdf

[16] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, z.s.p.o., 2016. CZ.NIC. ISBN 978-80-88168-15-7.

[17] MITNICK, Kevin D. a William L. SIMON. *The art of deception: controlling the human element of security*. Indianapolis, Ind.: Wiley, c2002. ISBN 978-076-4542-800.

[18] HOAX. *HOAX* [online]. 2018, 2018 [cit. 2018-01-23]. Dostupné z: http://www.hoax.cz/cze/

[19] ORTLOFF, Stefan. FAQ: Disabling the new Hlux/Kelihos Botnet. *AO Kaspersky Lab.: SECURELIST* [online]. Moscow: KASPERSKY LAB HQ, 2018, 28. 3. 2012 [cit. 2018-01-25]. Dostupné z: https://securelist.com/faq-disabling-the-new-hluxkelihos-botnet-13/32634/

[20] Služba Kriminální Policie: Removal guide. *Malware Removal Guides* [online]. 2016, 29. 7. 2013 [cit. 2018-01-26]. Dostupné z: http://www.malwareremovalguides.info/sluzba-kriminalni-policie-a-vysetrovani-ransomware-removal-guide/

[21] HÁLEK, Vítězslav. *KRIZOVÝ MANAGEMENT: teorie a praxe*. Bratislava: DonauMedia, 2008. ISBN 978-80-89364-33-6.

[22] *Krizové řízení při nevojenských krizových situacích: účelová publikace pro krizové řízení* [online]. Praha: Ministerstvo vnitra - generální ředitelství Hasičského záchranného sboru ČR, 2008 [cit. 2018-01-27]. ISBN 978-80-86640-93-8.

[23] SWOT analýza. *ManagementMania*[online]. Plzeň: MANAGEMENTMANIA.COM, 2018 [cit. 2018-04-28]. Dostupné z: https://managementmania.com/cs/swot-analyza

[24] ČESKO. § 2 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). In: Zákony pro lidi.cz [online]. © AION CS 2010-2018 [cit. 26. 4. 2018]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240#p2

[25] PROCHÁZKOVÁ, Dana. *Analýza a řízení rizik.* V Praze: České vysoké učení technické, 2011. ISBN 978-80-01-04841-2.

[26] PROCHÁZKOVÁ, Dana a Jan PROCHÁZKA. *Krizové řízení*. Praha: Vysoká škola regionálního rozvoje Praha, 2014. ISBN 978-80-87174-30-2.

[27] MATUROVÁ, Jana a Miroslav VALTA. Prevence rizik: provádění kontrol technického stavu technických zařízení. *BOZPinfo* [online]. Praha: Výzkumný ústav bezpečnosti práce, 2018, 21. 10. 2013 [cit. 2018-01-29]. Dostupné z: http://www.bozpinfo.cz/prevence-rizik-provadeni-kontrol-technickeho-stavu-technickych-zarizeni

[28] PELÁNEK, Radek. *Modelování a simulace komplexních systémů: jak lépe porozumět světu* [online]. Brno: Masarykova univerzita, 2011 [cit. 2018-04-29]. ISBN 978-80-210-5318-2.

[29] MIDDLETON, Bruce. *A history of cyber security attacks: 1980 to present*. Boca Raton, FL: CRC Press, 2017. ISBN 978-1-4987-8586-0.

[30] ZAJÍC, Radek. *Vybraná kybernetická rizika a jejich předcházení*. Praha, 2016. Diplomová práce. České vysoké učení technické v Praze, Masarykův ústav vyšších studií a Vysoká škola ekonomická v Praze, Podnikání a komerční inženýrství v průmyslu. Vedoucí práce Ing. Igor Kukliš.

[31] KLEINER, Jan. *Analýza kybernetických hrozeb eGovernmentu a jejich rizik pro ČR*. Brno, 2017. Bakalářská práce. Masarykova univerzita, Fakulta sociálních studií. Vedoucí práce Petra Vejvodová.

[32] *Národní úřad pro kybernetickou a informační bezpečnost* [online]. Praha: NBÚ, 2018 [cit. 2018-04-17]. Dostupné z: www.govcert.cz

[33] *AUDIT NÁRODNÍ BEZPEČNOSTI*. Praha: Ministerstvo vnitra ČR, odbor bezpečnostní politiky a prevence kriminality, 2016.

[34] *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020*. Praha: Národní bezpečnostní úřad, 2012.

[35] VALENTOVÁ, Hana. *Směrnice NIS: panelová diskuse se zástupci ČEZ, NBÚ a CZ.NIC* [online]. In: . Youtube, 02.06.2016 [cit. 2018-04-17]. Dostupné z: https://www.youtube.com/watch?v=diSZiVEuBEY

[36] JELEN, Tomáš. "Operační místnost": kde IT odborníci sledují a vyhodnocují bezpečnostní hrozby #nukib. In: *Twitter* [online]. 2017, 1.8.2017 [cit. 2018-04-19]. Dostupné z: https://twitter.com/search?q=%23nukib

[37] GovCERT.CZ: Vládní CERT [online], 2017. NÚKIB [cit. 2018-04-19]. Dostupné z: https://www.govcert.cz/

[38] *CSIRT.CZ: Národní CSIRT* [online]. CZ.NIC, 2017 [cit. 2018-04-19]. Dostupné z: https://www.csirt.cz/

[39] *Zpráva o stavu kybernetické bezpečnosti České republiky 2016* [online]. Brno: Národní úřad pro kybernetickou a informační bezpečnost, 2017 [cit. 2018-04-27]. Dostupné z: https://www.nukib.cz/download/Zpravy-KB-vCR/Zpr%C3%A1va-stavu-KB-2016.pdf

[40] JANKOVÁ, Martina. *Možnosti systémového prostředí ICT v kyberprostoru podniku*. GRANT journal, 2014. ISSN 1805-0638.

[41] KUBEŠ, Jan. 30 NEJHORŠÍCH HESEL UPLYNULÉHO ROKU. *Dvojklik.cz* [online]. ESET software spol. s r.o., 2017, 29.12.2017 [cit. 2018-04-29]. Dostupné z: https://www.dvojklik.cz/30-nejhorsich-hesel-uplynuleho-roku

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

ARPANET	Advanced Research Projects Agency NETwork.
BRS	Význam druhé zkratky.
CERT	Význam třetí zkratky.
CMS	Centrální místo Služeb-Komunikační infrastruktura Informačních systémů veřejné správy
CSIRT	Computer Security Incident Responce Team
ČR	Česká Republika
DDoS	Distributed Denial of Service
EU	Evropská Unie
ICT	Information Communication Technology
IMO	Internet Ministerstva obrany
IoT	Internet of things
ISMS	Information Security Management Systems
IT	Information Technology
IZS	Integrovaný záchranný systém
KB	Kybernetická bezpečnost
KI	Kritická infrastruktura
KII	Kritická informační infrastruktura
NATO	North Atlantic Threaty Organization
NBÚ	Národní bezpečnostní úřad
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
ÚKŠ	Ústředního krizového štábu
VIS	Významné informační systémy
ZKB	Zákon o Kybernetické bezpečnosti

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

REJSTŘÍK

SEZNAM PŘÍLOH

Příloha 1

Národní úřad pro kybernetickou a informační bezpečnost NÚKIB

Regulace odpovídající úrovni dopadu						Úroveň dopadu	Vodítka (kategorie) pro určení závažnosti dopadů narušení bezpečnosti informací (dostupnost, důvěrnost, integrita) - NUKIB v1.0 / 23.02.2018								
							A. Bezpečnost a zdraví osob	B. Ochrana osobních údajů	C. Zákonné a smluvní povinnosti	D. Trestně-právní řízení	E. Veřejný pořádek	F. Mezinárodní vztahy	G. Řízení a provoz organizace	H. Ztráta důvěryhodnosti	I. Finanční ztráty	J. Zajišťování nezbytných služeb
Ostatní	ZVS	GDPR	ZKB - VIS, SZS	ZKB - KII, PZS	ZLA	1 nízká	*Žádné vodítko*	Může způsobit porušení etických, nikoli však právních předpisů vedoucí k negativním osobním dopadům na jednotlivce nebo skupinu osob.	Může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností.	*Žádné vodítko*	*Žádné vodítko*	*Žádné vodítko*	Může narušit řádné řízení nebo fungování části nebo celé organizace.	Může negativně ovlivnit vztahy s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání.	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	*Žádné vodítko*
						2 střední	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) jedné nebo několika osob.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2 % celkového ročního obratu - viz čl. 83/4 GDPR).	Může způsobit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody.	Může vytvořit podmínky pro páchání trestné činnosti nebo může ztížit její vyšetřování.	Může zapříčinit rozsáhlem, formou nebo místem omezené protesty (lokální nepokoje).	Může vyvěřet negativní obraz ČR v jednom teritoriu, popř. v jednom státě.	Může omezit provádění důležitých činností organizace.	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobé.	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05 % a 2 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit závažné omezení či narušení nezbytných služeb pro malé množství osob.
						3 vysoká *	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob, nebo ohrožení na životě jednotlivců.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na velkou skupinu osob (pokuta až 20 mil. EUR nebo 4 % celkového ročního obratu - viz čl. 83/5 GDPR).	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	Může vést k narušení vyšetřování trestné činnosti nebo soudní řízení (méně závažná kriminalita, krátkodobě, v jednotlivých případech).	Může zapříčinit rozsáhlem, formou nebo místem omezené protesty na úrovni významné části správního území obce s rozšířenou působností, jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje.	Může vyvěřet negativní obraz ČR ve světě.	Může způsobit dočasné zastavení nebo podstatné narušení důležitých činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.	Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.	Může přímo nebo nepřímo vést ke ztrátám vyšším než 2 % a nižším či rovným 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace). Pozn. v případě PZS je hranice ztráty stanovena na 0,25 % HDP.	Může způsobit závažné omezení, narušení či nedostupnost nezbytných služeb pro více než 25 000 osob (v rámci kategorie provozovatelů základních služeb se může lišit dle právní úpravy pro jednotlivé odvětví viz vyhláška č. 437/2017 Sb.).
						4 kritická **	Může vést k přímému ohrožení či ztrátě života skupiny osob.	*Žádné vodítko*	*Žádné vodítko*	Může vést k závažnému, dlouhodobému narušení schopnosti vyšetřovat trestnou činnost, popřípadě zpochybnění soudních řízení a rozhodnutí (závažná kriminalita, celkové zpochybnění systému).	Může zapříčinit hromadné nepokoje, např. generální stávku, nebo jiná závažně narušit veřejný pořádek s celostátními dopady.	Může negativně ovlivnit nebo poškodit diplomatické vztahy a tím způsobit nevýhodu pro zájmy ČR.	Závažným způsobem může zasáhnout do fungování celé organizace a může vést až k ukončení činnosti.	Může závažně a dlouhodobě ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti.	Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace). Pozn. v případě KII je hranice ztráty stanovena na 0,5% HDP.	Může způsobit rozsáhlé omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.
					ZLA	Narušení bezpečnosti informací v oblasti "důvěrnosti" může způsobit újmu zájmům České republiky anebo nevýhodnost pro zájmy České republiky a zároveň je informace typově uvedena v seznamu utajovaných informací (§ 2 písm. a) zákona č. 412/2005 Sb.). Na základě tohoto dopadu by se za splnění dalších legislativně stanovených podmínek mělo jednat o utajované informace. Pro určení odpovídajícího stupně utajení je třeba postupovat v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. A to za splnění dalších stanovených podmínek, např. uvedených v nařízení vlády č. 522/2005 Sb.								

** V případě, že je v některém z parametrů bezpečnosti (dostupnost, důvěrnost, integrita) dosažena max. úroveň dopadu "Vysoká", měl by správce zvážit zařazení informačního systému mezi významné informační systémy (VIS), případně mezi informační systémy základní služby (SZS).*
- Podmínkou pro zařazení systému mezi VIS je současné naplnění definice v § 2 písm. d) zákona č. 181/2014 Sb., a alespoň jednoho obligatorního kritéria podle přílohy č. 2 k vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a zároveň alespoň jednoho dopadového kritéria uvedeného v § 4 vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.
- Podmínkou zařazení systému mezi SZS je naplnění definice v § 2 písm. i) a j) zákona č. 181/2014 Sb., a současné naplnění odvětvových kritérií a alespoň jednoho dopadového kritéria uvedeného v příloze vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb.

*** V případě, že je v některém z parametrů bezpečnosti dosažena úroveň dopadu "Kritická", měl by správce zvážit zařazení informačního nebo komunikačního systému mezi prvky kritické informační infrastruktury (KII), případně mezi informační systémy základní služby (SZS).*
- Podmínkou zařazení systému mezi KII je současné naplnění definice v § 2 písm. b) zákona č. 181/2014 Sb., a alespoň jednoho odvětvového kritéria v odvětví VI., oblasti G. Kybernetická bezpečnost podle přílohy k nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury a zároveň alespoň jednoho průřezového kritéria uvedeného v § 1 nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.
- Podmínkou zařazení systému mezi OZS je naplnění definice v § 2 písm. i) a j) zákona č. 181/2014 Sb., a současné naplnění odvětvových kritérií a alespoň jednoho dopadového kritéria uvedeného v příloze vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb.

Poznámka ke sloupci „Ochrana osobních údajů":
Požadavky na zpracování osobních údajů v cloudových službách musí dle nařízení GDPR vycházet z hodnocení rizik daného scénáře zpracování pro práva a svobody fyzických osob. V případě zjištění vysokého rizika budou správci povinni provést tzv. „posouzení vlivu zpracování dat na ochranu osobních údajů" (DPIA, viz čl. 35), a zajistit adekvátní bezpečnostní opatření a mechanismy ochrany. Přitom předpokládáme využití některého ze schválených „kodexů chování" (viz čl. 40 GDPR) daným zpracovatelem a jeho cloudovou službou. Regulátor (ÚOOÚ) očekává, že do doby účinnosti nařízení GDPR bude schváleno několik kodexů chování, které vytvoří vhodný rámec standardizace pro vyšší úroveň dopadů zpracování osobních údajů.

Seznam použitých zkratek:
GDPR - nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
ZVS - zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
SZS - Informační systém základní služby podle § 2 písm. j) zákona č. 181/2014 Sb.
KII - kritická informační infrastruktura podle § 2 písm. b) zákona č. 181/2014 Sb.
PZS - provozovatel základní služby podle § 2 písm. k) zákona č. 181/2014 Sb.
ÚOOÚ - Úřad pro ochranu osobních údajů
VIS - významný informační systém podle § 2 písm. d) zákona č. 181/2014 Sb.
ZKB - zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
ZUI - zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti