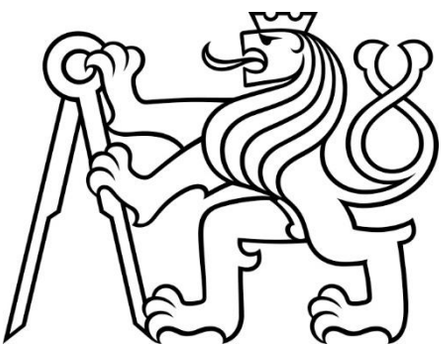
ČESKÉ VYSOKÉ
UČENÍ TECHNICKÉ
V PRAZE

FAKULTA
BIOMEDICÍNSKÉHO
INŽENÝRSTVÍ



BAKALÁŘSKÁ PRÁCE

2019

ŠIMON
BÍŽA

ČESKÉ VYSOKÉ UČENÍ TECHNICKÉ V PRAZE

Fakulta biomedicínského inženýrství

Katedra zdravotnických oborů a ochrany obyvatelstva

Analýza a využití průřezových kritérií pro kritickou informační infrastrukturu

Analysis and Use of Cross-Cutting Criteria fod Cricital Infrastructure

Bakalářská práce

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

Vedoucí práce: Ing. Josef Bernátek

Šimon Bíža

Kladno, květen 2019

Prohlášení

Prohlašuji, že jsem bakalářskou práci s názvem Analýza a využití průřezových kritérií pro kritickou informační infrastrukturu vypracoval samostatně pouze s použitím pramenů, které uvádím v seznamu bibliografických odkazů.

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

V Kladně dne 16.05.2019

…….
podpis

Poděkování

Rád bych touto cestou poděkoval panu Ing. Josefu Bernátkovi za trpělivost, pomoc a vstřícný přístup při zpracování bakalářské práce.

Abstrakt

Cílem této bakalářské práce je shrnutí stavu kybernetické bezpečnosti a hodnocení průřezových kritérií používaných k určení kritické informační infrastruktury. Teoretická část se zaměřuje na popis kybernetické bezpečnosti v České republice a na kritickou informační infrastrukturu. Praktická část rozebírá průřezová kritéria a zabývá se návrhem na jejich úpravu. Hodnocení dopadu úpravy na kybernetickou bezpečnost je provedeno SWOT analýzou.

Klíčová slova

Kybernetická bezpečnost; kritická informační infrastruktura; průřezová kritéria.

Abstract

The aim of this bachelor's thesis is to summarize the state of cyber security and evaluation of cross-cutting criteria used in critical information infrastructures determination.

The theoretical section focuses on description of cyber security in the Czech Republic and its critical information infrastructure. The practical section considers the cross-cutting criteria and proposes their amendments. The effect of said amendments on cyber security is assessed through SWOT analysis.

Keywords

Cyber security, critical information infrastructure, cross-cutting criteria.

Obsah

1 ÚVOD

V současné společnosti stále více vstupuje do popředí potřeba ochrany zdraví, života majetku a životního prostředí. Zajištění ochrany je složitý proces, který není nikdy stoprocentní. Je jednou z hlavních funkcí státu zajistit bezpečnost svých občanů.

Důležitou oblastí, která je potřeba chránit je infrastruktura státu. Z tohoto důvodu se určuje kritická infrastruktura, protože její narušení má dopad na chod společnosti. K určení kritické infrastruktury slouží průřezová a odvětvová kritéria.

V posledních několika desetiletích se velmi rozvíjí digitální infrastruktura. Její rozvoj s sebou přináší nové hrozby, proti kterým je potřeba se chránit. Některé prvky jsou natolik důležité, že jsou nazývány kritickou informační infrastrukturou. Ochranou informačních a komunikačních technologií se zabývá obor kybernetické bezpečnosti.

Předmětem mé práce je popsat stav kybernetické bezpečnosti v České republice, zhodnotit a navrhnout úpravu průřezových kritérií, s přihlédnutím na použití při určování kritické informační infrastruktury.

2 SOUČASNÝ STAV

2.1 Kybernetický prostor

Pokud se chceme zabývat problematikou kybernetické bezpečnosti, je důležité si hned na začátku vysvětlit, co je to kybernetický prostor.

Kybernetický prostor nemá jasně danou definici, která by se dala považovat za stoprocentně správnou. Její pojetí a chápaní se mění postupem času.

Americko-kanadský spisovatel William Gibson napsal v roce 1982 povídku s názvem „Jak vypálit Chrome“, ve které byl poprvé uveden pojem kyberprostor. Později použil stejný termín i v románu „Neuromancer“, kde Gibson kyberprostor označil jako datový prostor nebo datovou halucinaci vytvořenou počítačově zpracovanými daty ve formě imaginárního místa, kam může vstoupit pouze uživatelovo vědomí. Jeho myšlenka a pojem kyberprostor inspiroval nejen další knižní autory, ale především ovlivnil tvůrce počítačových systémů [1].

V souvislosti s počítačovými sítěmi byl americký básník a aktivista John Perry Barlow ten, který jako první použil termín kyberprostor. Popsal ho jako symbolický prostor pro mediovanou komunikaci, jejíž význam spočívá v komunikace prostřednictvím jakéhokoliv technického systému. Dále uvedl, že čím více bude vyspělá technologie, tím více bude komplexní kyberprostor [1].

V roce 2001 Computer Science and Communications Dictionary definuje kybernetický prostor jako nehmotné propojení informačních a komunikačních systémů, kde je možné vytvářet, ukládat, využívat a přeposílat informace. Jako příklad uvádějí celosvětovou síť Internet, který je nejvíce komplexním představitelem. [2].

V současné době je kybernetický prostor chápán jako virtuální realita, bez přesně určeného rozměru, která je závislá na technologiích z reálného světa. Především je vytvořen z informační a komunikační technologie (dále jen „ICT“), která je prezentována počítačovou síť pokrývající celý svět na základě TCP/IP protokolu umožňující komunikaci a výměnu dat. Vzájemné působení těchto systémů musí být ovlivněno jejich uživateli [3].

Kyberprostor má několik vlastností. Jednou z nejdůležitějších vlastností je pokrytí značné části světa neboli globálnost. Mezi další vlastnosti můžeme zařadit decentralizovanost, což znamená nepřítomnost žádného specifického vlastníka, který by kyberprostor spravoval, řídil nebo rozhodoval o jeho fungování. Další vlastností je otevřenost. Do kyberprostoru může každý uživatel nahrávat jakékoliv informace. Tyto informace nejsou nikým kontrolovány, tudíž není ověřena jejich pravost. Kvůli otevřenosti je kyberprostor zahlcen informacemi. Není tedy těžké najít informace, ale nesnáze může působit výběr informací pravdivých. V neposlední řadě je důležitým znakem kyberprostoru i relativně neprůhledné prostředí, které dává uživateli pocit anonymity. Tato vlastnost vede k páchání nelegální činnosti nazývající se kybernetická kriminalita. Uživateli páchající nelegální činnost poskytuje anonymita a vzdálenost od místa činu pocit bezpečí, což snáze vede k trestné činnosti. Všechny tyto vlastnosti a činnosti uživatelů směřují k tomu, že virtuální svět se propojuje s reálným, který je tímto značně ovlivňován [4].

Kybernetický prostor v České republice je definován podle zákona č. 181/2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) jako: „*digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací*“ [5]

2.2 Kybernetická bezpečnost

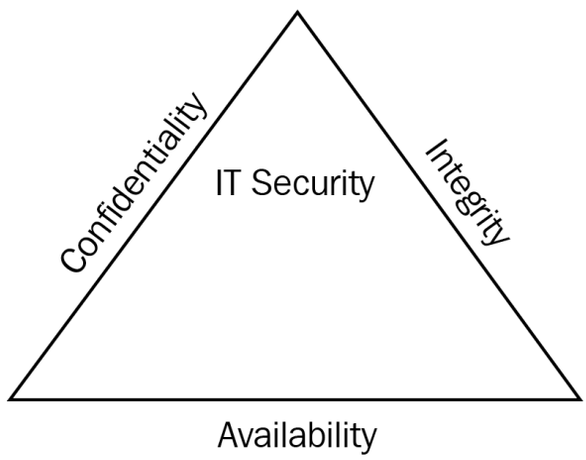
V této kapitole si popíšeme, co je to kybernetická bezpečnost a uvedeme základní pojmy s ní související.

Když si tento pojem rozdělíme na slova kyber a bezpečnost. Slovo kyber (z anglického cyber) je charakteristické pro vztah ICT s virtuálním prostorem zvaným kyberprostor, který jsme si popsali v předchozí kapitole. Význam slova bezpečnost je možné popsat jako snížení nebo eliminace hrozby negativně působící na aktivum, které má být chráněno. Spojením slov vzniká kybernetická bezpečnost. Již z předchozího rozboru vyplývá, že se jedná o zajištění bezpečnosti v informačních a komunikačních systémech. Přesněji se kybernetická bezpečnost zabývá ochranou informací před ničením a krádeží, ovšem také zajišťuje dostupnost a důvěrnost kybernetického prostoru. Můžeme tedy můžeme říci, že kybernetická bezpečnost spadá pod informační bezpečnost, ale zabývá se pouze informacemi v kyberprostoru [6, 7].

S rostoucím využíváním komunikačních a informačních systémů dochází ke zvýšení rizika, že dojde k úniku důležitých státních informací. Kvůli takové hrozbě je nutné zajistit bezpečnost. České republice kybernetickou bezpečnost upravuje zákon č. 181/2014 o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a jeho prováděcí předpisy. Hlavní cíl kybernetické bezpečnosti České republiky je zajistit funkčnost prvku kritické informační infrastruktury a významného informačního systému. Zákon stanovuje pracoviště zajišťující kybernetickou bezpečnost, minimální úroveň zabezpečení a systém opatření, která se vykonávají při zjištění kybernetické hrozby. Zákon, ale neuvádí žádnou definici kybernetické bezpečnosti [3]. Nejvíce výstižná definice je uvedena ve Výkladovém slovníku kybernetické bezpečnosti a je popsána jako: *„souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru“* [8, str.69]

2.2.1 Triáda CIA

Triáda CIA je model, který představuje zásady pro zabezpečení informací v rámci určité organizace. Jedná se o velmi používaný model pracující, jak z názvu vyplývá, na třech principech. Tyto principy představují důvěrnost, integritu a dostupnost. Aplikace triády CIA by měla vést k zajištění bezpečného systému organizace [9].



Obrázek 1 - Triáda CIA [10]

Důvěrnost (Confidentality)

Informace, data a ICT může používat jenom ten, kdo je k tomu oprávněn. Nežádoucím únik informací je chápán jako narušení jejich důvěrnosti. Kvůli velkému množství informací je důležité zavést jejich klasifikaci. Je nutné určit kategorie, do kterých se informace zařadí. Existuje několik klasifikačních schémat. Jednotlivec nebo organizace si zvolí schéma, které jim nejvíce vyhovuje. Vhodně zvolené schéma a správně klasifikované informace by měly snížit negativní účinky možného kybernetického útoku. Například uvedeme schémata klasifikace pro státní a komerční sféru [9].

1. Klasifikační schéma státní sféry
    - Přísně tajné – Informace, které jsou důležité pro bezpečnost státu. Jejich neoprávněné užívání může mít závažný dopad na národní bezpečnost.

- Tajné – Neoprávněné užívání informací, které může mít značný vliv na národní bezpečnost.
- Důvěrné – Neoprávněné užívání informací, které může mít podstatný vliv na národní bezpečnost.
- Vyhrazené – Neoprávněné užívání informací, které může mít nepříznivý vliv na národní bezpečnost [10].

2. Klasifikační schéma komerční sféry
    - Chráněné – Zneužití informací má zničující dopad na organizaci.
    - Interní – Zneužití informací má zá následky poškození organizace.
    - Citlivé – Zneužití informací má na organizaci negativní vliv.
    - Veřejné – Zneužití informace by nemělo mít žádný negativní vliv na organizaci [10,11].

Integrita (integrity)

Integrita zajišťuje správnost informací a dat. Zabraňuje, aby došlo k jejich úpravě nebo obměně. Pokud dojde k úpravě informací a dat, nemusí to být na první pohled viditelné. Je otázkou času, než se na to přijde. Bohužel čím déle je změna nepovšimnuta, tím více vzrůstá nebezpečí většího dopadu na organizaci. Je důležité mít zavedeny opatření a kontroly integrity dat a informací [11].

Ve vyhlášce o kybernetické bezpečnosti je uvedena stupnice, která hodnotí stupeň důležitosti informací a dat. Jsou zde uvedeny i požadavky na ochranu jednotlivých stupňů.

Tabulka 1 - Stupnice pro hodnocení integrity [12]

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány standardní nástroje (například omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).

Dostupnost (Availability)

Dostupnost znamená využití informací, dat a ICT v době, kdy jsou potřebné [13].

Ve vyhlášce o kybernetické bezpečnosti je uvedena stupnice pro hodnocení dostupnosti.

Tabulka 2 - Stupnice pro hodnocení dostupnosti [12]

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
Vysoká	Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné, a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

2.2.2 Prvky kybernetické bezpečnosti

Je mylná představa, že kybernetická bezpečnost se opírá jen o technologii. Technologie je velkou součástí kybernetické bezpečnosti, ale sama nestačí zajistit ochranu před kybernetickými hrozbami. Pokud nejsou zavedeny vhodné procesy a zaměstnanci nejsou řádně proškoleni, můžou být vytvořena slabá místa. Proto je kvalitní kybernetická bezpečnost postavena na lidech, procesech a technologiích [14].

Lidé

Lidé jsou považováni za důležitý prvek bezpečnosti, ale zároveň jsou bráni jako nejslabší článek, protože se nejčastěji dopouští chyb. Lidé také bývají nejsnadnější cílem pro útočníky. K minimalizaci lidských chyb je potřebné zavést odborná školení. Vyškolení lidé dokáží přijímat správná rozhodnutí a tím zvyšují bezpečnost [14].

Procesy

Procesy jsou klíčem k zavedení efektivní strategii kybernetické bezpečnosti. Jsou důležité při zavádění činností, úloh a dokumentace, kterou organizace bude využívat ke zmírnění rizik. Procesy je nutné neustále přezkoumávat, protože kybernetické hrozby se neustále mění, a tudíž je nezbytné, aby k nim byly procesy přizpůsobeny [14].

Technologie

Technologie je nejdůležitějším prvkem kybernetické bezpečnosti. Řadíme sem hardware a software, který je potřebný udržovat v práci schopnosti. Díky definovaným rizikům působícím na organizace je snadné najít, dané technologie a kontroly, které je potřeba zavést k ochraně. Technologie je využívána k prevenci, ale také ke snížení nebo eliminaci kybernetických hrozeb [14].

2.2.3 Životní cyklus kybernetické bezpečnosti

Zajišťování bezpečnosti je neustálý proces. Nejde ji jenom zavést, ale je nutné, aby se permanentně vyvíjela. Organizace musí být schopná reagovat na změny a přizpůsobovat se jim [15].

V první řadě je důležité identifikovat aktiva, která mohou být ohrožena. Dále se musí určit rizika, která hrozí aktivům. Pokud budou známa rizika, je potřebné zavést opatření. Všechna tato činnost se musí správně řídit. Nakonec se vše přezkoumá a zhodnotí se funkčnost veškerých opatření. Aby byla zajištěna kvalitní kybernetická bezpečnost, musí se cyklus neustále opakovat, protože se technologie, procesy a hrozby mění.

Životní cyklus je názorně popsán a zobrazen na následujícím obrázku.

Obrázek 2 - Životní cyklus kybernetické bezpečnosti [16]

2.2.4 Bezpečnostní role

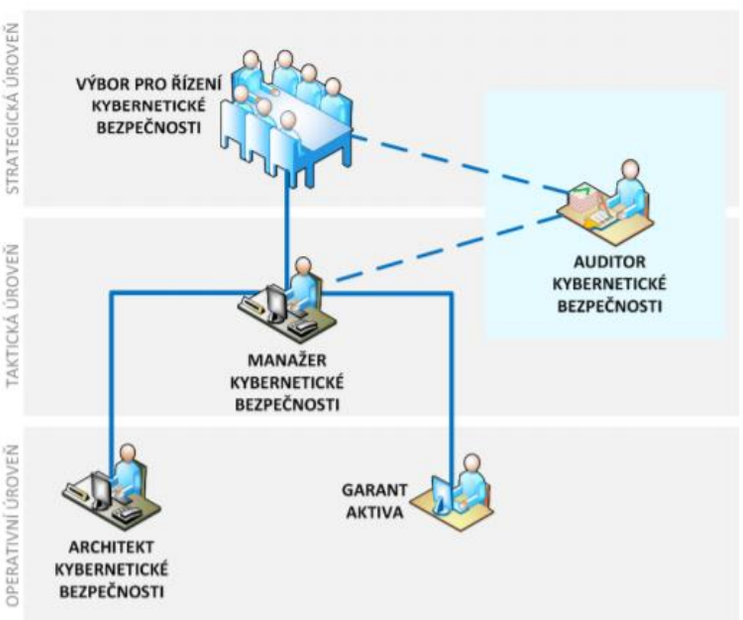
V každé organizaci potřebující zajištění kybernetické bezpečnosti by měl být vytvořen Výbor pro řízení kybernetické bezpečnosti. Jeho úkolem je zajistit řízení na strategické úrovni a koordinovat činnosti na nižších úrovních. Složení výboru záleží na dané organizaci, ale je doporučené dosazovat lidi se znalostmi v oblasti bezpečnosti a ICT.

Manažer kybernetické bezpečnosti je vyškolená osoba, která je zodpovědná za zajištění bezpečnosti informací. Zajišťuje řízení na taktické úrovni, má spojení se strategickou úrovní [17].

Architekt navrhuje opatření k zajištění kybernetické bezpečnosti. Zkouší funkčnost jeho navržených opatření. Jestliže jsou jeho opatření vyhovující, následně je zavede do provozu. V této pozici může pracovat osoba se zkušenostmi s bezpečnostní architekturou. Nachází se na operativní úrovni [17].

Auditor provádí kontrolu kybernetické bezpečnosti. Zjišťuje nedostatky a poté dává zpětnou vazbu výboru nebo manažerovi. Jeho postavení je mimo všechny úrovně. Je nutné, aby osoba na této pozici byla nestranná [17].

Garant aktiva, jinak nazývaný vlastník aktiva, zajišťuje bezpečnost chráněného zájmu. Hlavním smyslem je zajistit bezpečnost triády CIA. Pozice se nachází na operativní úrovni [17].



Obrázek 3 - Struktura bezpečnostních rolí v organizaci [17]

2.3 Kybernetické hrozby

Kybernetické hrozby přicházejí z kyberprostoru a jsou to protiprávní jednání, která mají za účel poškodit jinou osobu nebo organizaci. Můžeme si to představit jako cizí zásah, který má za následek změnu informace nebo negativní ovlivnění systému. Pokud dojde k realizování hrozby stává se z ní útok. Ve výkladovém slovníku kybernetické bezpečnosti je kybernetický útok definován jako: *"Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé, či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků" [9, str. 71].* Kybernetický útok nemusí být trestní čin, ale dokáží narušit běžný chod fyzických i právnických osob [18 ,4].

Hrozby mohou být způsobeny úmyslně, za účelem poškodit, ukrást, zničit nebo zneužít data či informace. Úmyslné hrozby dále dělíme na aktivní a pasivní. Aktivní hrozba zasahuje do systémů, ve kterých něco mění. Pasivní hrozba sleduje daný systém, předává získané informace, ale jinak do systému nezasahuje. Hrozby mohou být zapříčiněny útočníkem úmyslně, nebo neúmyslně, kdy dojde k chybě uživatele nebo systému [4].

Kybernetické hrozby nejčastěji směřují na prvky kybernetické bezpečnosti, kterými jsou výše zmínění lidé, procesy a technologie. Dalším častým cílem je triáda CIA. Z těchto poznatků vychází dělení hrozeb na 4 skupiny:

- Únik informace – Dojde k úniku chráněné informace k subjektu, který nemá oprávnění.
- Potlačení služby – Autorizovanému subjektu je bráněno k přístupu do systému nebo informacím.
- Narušení integrity – Informace jsou upraveny, smazány nebo jsou vytvořené nové.
- Nelegitimní použití – Použití informací subjektem, který nemá oprávnění [18,4].

2.3.1 Druhy kybernetických hrozeb

Existuje velké množství kybernetických hrozeb. V této podkapitole si uvedeme a popíšeme nejčastější případy.

Sociální inženýrství

Sociální inženýrství spočívá v přesvědčování a manipulaci s nejslabším prvkem kybernetické bezpečnosti, o kterém víme, že jím jsou lidé. Útočník se snaží manipulovat s člověkem, tak aby se dopustil věcí, které by jinak neudělal. Nejčastěji se vydává za někoho jiného, ze snahy být autoritativní nebo více důvěryhodný. Když útočník získá důvěru, pokusí se vylákat z osoby informace. Tento útok se nejčastěji provádí přes e-mail, textové zprávy nebo telefonicky. Osoba, která se stala obětí sociálního inženýrství, o tom nemusí zpočátku vědět. Dozví se to až později, když dojde ke škodám [19].

Příklad sociálního inženýrství je:

- Phising – E-mailová zpráva od známé organizace upozorňující na nějaký problém. Požaduje od uživatele osobní informace nebo přístupové údaje [19].

Malware

Malware je souhrnné označení pro škodlivý software. Jedná se o škodlivý kód, jehož účelem je poškodit systém nebo ukrást informace. Do systému se dostává různými způsoby. Nejčastější jsou přenosy přes datové médium, návštěvu internetové stránky nebo jako příloha e-mailu. Malware můžeme rozdělit podle vniknutí do systému nebo podle typu činnosti [20 ,11].

1. Druhy malwaru podle vniknutí do systému.

- Trojský kůň – Vydává se za jiný program nebo si ho uživatel stáhne spolu s jiným programem. Trojský kůň pracuje skrytě a provádí negativní činnost.
- Virus – Program, který se šíří ze systému na systém bez vědomí uživatele. Nejčastější přenos bývá přes datová média. Projevují se obrazovými nebo zvukovými efekty a dokáží vymazat data. Mohou působit i pasivněji. Bez žádné známky jejich existence pracují v systému a stahují další škodlivé programy.
- Červ – Program, který ke svému šíření používá počítačoví sítě. Nejčastějším médiem pro šíření jsou sdílené disky nebo komunikační kanály, jako je e-mail [21].

2. Druhy malwaru podle činnosti.

- Ransomware – Program, který zablokuje data uložena na disku. Za odblokování útočník požaduje peníze. Nikdy není jistě, že po zaplacení budou data zpřístupněna.
- Spyware – Sledovací program, který zaznamenává navštívené stránky. Pozoruje chování uživatele. Dokáže také získat osobní údaje, hesla a jiné údaje.
- Adware – Program ukazující nevyžádanou reklamu.
- Backdoor – Jsou to programy, které umožnují vstup do systému nepovolaným osobám a způsobit tam škodu. Jejich přístup je těžko detekovatelný [21].

Botnet

Pomocí malwaru je infikován značný počet počítačů a chytrých zařízení. Jakmile je zařízení infikováno, stává se botem a začíná samo pracovat. Uživatel o tom většinou neví. Bot se dokáže spojit s centrálním serverem. Tento server předává instrukce botům, pokud žádné nejsou, boti vyčkávají a snaží se nevzbuzovat

pozornosti. Počet takto infikovaným zařízení může být až desítky milionů zařízení [22].

DDos (Distributed Denial of Service)

DDos útoky jsou v současné době často používané. Jejich cílem jsou webové stránky nebo online služby. Princip útoku spočívá v posílání zpráv, dotazů nebo připojení uživatelů ve velkém množství. Servery nebo sítě nedokáží takové množství zpracovat a dojde tedy k jejich zahlcení. Poté se stane webová stránka nebo online služba nefunkční [23].

2.3.2 Kybernetická bezpečnostní událost

Zákon o kybernetické bezpečnosti definuje kybernetickou bezpečnostní událost v § 7, ods. (1) jako: *„událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací“* [24].

2.3.3 Kybernetický bezpečnostní incident

Zákon o kybernetické bezpečnosti definuje kybernetickou bezpečnostní událost v § 7, ods. (2) jako: *„narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události“* [24].

2.4 Národní úřad pro kybernetickou a informační bezpečnost

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) je ústředním správním orgánem. Jeho hlavní činností je zajišťovat kybernetickou bezpečnost a ochranu utajovaných informací či provádět kryptografickou ochranu. NÚKIB vznikl 1. srpna 2017 na základě zákona č. 205/2017 Sb., kterým se upravil

zákon č. 181/2014 Sb., o kybernetické bezpečnosti a přebral všechnu problematiku spojenou s kybernetickou bezpečností od Národního bezpečnostního úřadu [25].

Organizační struktura NÚKIB se člení na sekce a ty se dále dělí na odbory.

2.4.1 Národního centrum kybernetické bezpečnosti

Sekce Národního centra pro kybernetickou bezpečnost (dále jen „NCKB“) je výkonnou složkou NÚKIB. NCKB se skládá ze tří odborů:

1. Odbor kybernetických bezpečnostních politik (dále jen „OKBP“)
   Odbor zabývající se analýzami útoků na mezinárodní úrovni a zjišťováním trendů v kybernetické bezpečnosti. Z této analýzy poté vydávají informační materiály pro organizace ve státní sféře. Další činnost odboru je zpracování strategie k zajištění kybernetické bezpečnosti. Cílem strategie je vybudovat společnou a koordinovanou politiku, která zajistí kybernetickou bezpečnost v České republice. V neposlední řade OKBP organizuje cvičení, vzdělávání a osvětu v oblasti kybernetické bezpečnosti [26].

2. Odbor vládní CERT
   Název CERT je zkratka z anglického názvu Computer Emergency Response Team. Vládní CERT, nebo jinak označovaný jako GovCERT, hraje důležitou roli při zajištění ochrany u kritické informační infrastruktury a významných informačních systémů. Do působnosti vládního CERT týmu spadá kritická informační infrastruktura a veřejné instituce. Jeho hlavní činností je reagovat na bezpečnostní incidenty a poskytnout pomoc s jejich vyřešením. Vládní CERT pomáhá organizacím s preventivní činností. Jenou z preventivních činností je například penetrační testování. To spočívá ve vedení útoku proti testovanému systému, aby byla zjištěna slabá místa. Vládní CERT také provozuje forenzní laboratoř, ve které zkoumá potencionálně nakažená

zařízení. Jestliže bezpečnostní incident nespadá do působnosti vládního CERTU, předává ho jinému týmu nebo poradí, kam se obrátit [25, 26]

3. Odbor regulace

   Odbor, který spolupracuje na tvorbě legislativy. Podílí se na vyhledávání prvku kritické informační infrastruktury a významných informačních systémů [26, 27].

Národní CERT

Národní CERT tým se označuje jako CSIRT.CZ (Computer Security Incident Response Team). Sdružení CZ.NIC podepsalo v roce 2015 veřejnoprávní smlouvu a stalo se provozovatelem národního CERT týmu.

Tým CSIRT.CZ má stejné úkoly jako vládní CERT, avšak má jiné pole působnosti. Do tohoto pole se řadí všichni uživatelé a sítě na území České republiky.

Úkolem týmu je pomoc s řešením bezpečnostních incidentů. Jelikož nemá žádné výkonné pravomoci, funguje jako koordinátor a může poskytnout metodické pokyny pro zvládnutí incidentu. Další významná činnost tým CSIRT.CZ je organizování přednášek a školení [28].

2.5 Výbor pro kybernetickou bezpečnost

Výbor pro kybernetickou je jedním z výborů Bezpečnostní rady státu. Schází se jednou za tři měsíce. Schůzí výboru se účastní ředitel NÚKIB, předseda Bezpečnostní rady státu, náměstci vybraných ministrů, ředitelé bezpečnostních sborů a další. Jeho hlavní činností je zajištění kybernetické bezpečnosti v České republice, rozvíjení mezinárodní spolupráce a koordinace meziresortní spolupráce [29].

2.6 Kritická informační infrastruktura

Pojem infrastruktura představuje množinu prvků, které jsou vzájemně spojeny a zajišťují funkci systému. Jako systém si můžeme představit jakoukoliv organizaci, firmu, domácnost či stát. Infrastruktura státu se označuje jako veřejná infrastruktura a dělí se na sociální a technickou infrastrukturu. Funkční veřejná infrastruktura vede k zajištění dobrého národního hospodářství a kvalitního života obyvatelstva [30, 31].

V každém státě existuje infrastruktura, jejíž nefunkčnost by měla dopad na fungování společnosti. Označuje se jako životně důležitá neboli kritická infrastruktura [32] V České republice je kritická infrastruktura definovaná v zákoně č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) jako: *„prvek kritické infrastruktury nebo systém prvků kritické infrastruktury, narušení jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu“* [33].

Prvek kritické infrastruktury se určuje pomocí průřezových a odvětvových kritérií, která jsou uvedena v nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

Průřezová kritéria jsou hlediska s mezními hodnotami, která posuzují, jaký dopad bude mít nefunkčnost prvku. Jejich znění je:

- *Oběti s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin,*
- *ekonomický dopad s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo*
- *dopad na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125000 osob* [34].

Odvětvová kritéria jsou technické a provozní hodnoty, která upřesňují jednotlivá odvětví a rozdělují je do několika skupin:

- energetika,
- vodní hospodářství,
- potravinářství a zemědělství,
- zdravotnictví,
- doprava,
- komunikační a informační systémy,
- finanční trh a měna,
- nouzové služby,
- veřejná správa [35].

Z těchto devíti odvětví nás budou nejvíce zajímat komunikační a informační systémy. Pokud dojde k narušení bezpečnosti informací a bude naplněno některé z průřezových kritérií, je možné, že se jedná o kritickou infrastrukturu. Důležité je také zjistit, zda jsou naplněna i odvětvová kritéria v oblasti kybernetické bezpečnosti. K určení je možné použít i ostatní odvětvová kritéria, avšak je důležité, aby byla tato kritéria nezbytná k zajištění kybernetické bezpečnosti. Pokud prvek splňuje alespoň jedno průřezové i odvětvové kritérium stává se kritickou informační infrastrukturou. Jestliže prvek není ve správě státu NÚKIB vydá opatření obecné povahy a poté se informační a komunikační systém stane prvkem kritické informační infrastruktury. Pokud je informační a komunikační systém spravován státem, NÚKIB přeloží návrh vládě České republiky. Ta návrh projedná a vydá usnesení, které označí informační a komunikační systém za prvek kritické informační infrastruktury [3, 35]. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) definuje kritickou informační infrastrukturu jako: *„prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti“* [24].

Konkrétní odvětvová kritéria pro komunikační a informační systémy:

„A. Technologické prvky pevné sítě elektronických komunikací:

a) centrum řízení a podpory sítě,

b) řídící ústředna,

c) mezinárodní ústředna,

d) transitní ústředna,

e) datové centrum,

f) telekomunikační vedení.

B. Technologické prvky mobilní sítě elektronických komunikací:

a) centrum řízení a podpory sítě,

b) ústředna mobilní sítě,

c) základnová řídící jednotka sítě pokrývající strategickou lokalitu,

d) základnová stanice sítě pokrývající strategickou lokalitu,

e) datové centrum.

C. Technologické prvky sítí pro rozhlasové a televizní vysílání:

a) vysílací zařízení pro šíření televizního nebo rozhlasového signálu určených pro informaci obyvatelstva za krizových situací s vysílacím výkonem nejméně 1 kW k zajištění provozu rozhlasového a televizního vysílání veřejnoprávního provozovatele,

b) řídící pracoviště provozu,

c) datové centrum,

d) síť pro rozhlasové a televizní vysílání k zajištění provozu rozhlasového a televizního vysílání veřejnoprávního provozovatele.

D. Technologické prvky pro satelitní komunikaci:

a) hlavní pozemní satelitní přijímací a vysílací stanice,

b) Evropský globální navigační družicový systém,

c) pozemní řídící a komunikační středisko,

d) pozemní propojovací síť.

E. Technologické prvky pro poštovní služby:

a) centrální a regionální výpočetní středisko, středisko centrálního snímání a úložiště dat,

b) sběrný přepravní uzel,

c) řídící a mezinárodní pošta,

d) poštovní dopravní infrastruktura.

F. Technologické prvky informačních systémů:

a) řídicí centrum,

b) datové centrum,

c) síť elektronických komunikací,

d) technologický prvek zajišťující provoz registru doménových jmen „CZ“ a zabezpečení provozu domény nejvyšší úrovně „CZ“.

G. Oblast kybernetické bezpečnosti:

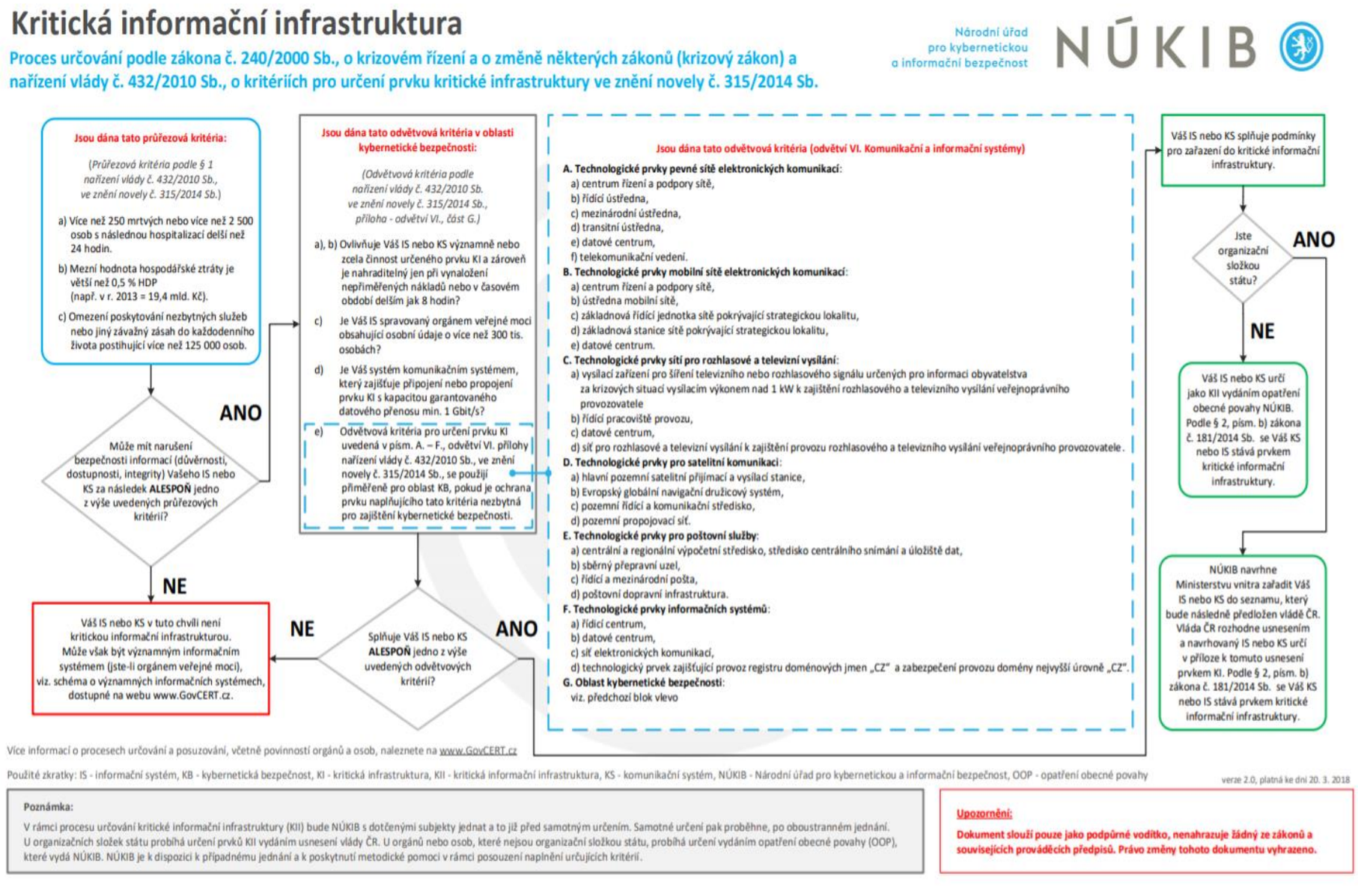
a) informační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin,

b) komunikační systém, který významně nebo zcela ovlivňuje činnost určeného prvku kritické infrastruktury, a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období přesahujícím 8 hodin,

c) informační systém spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300000 osobách,

d) komunikační systém, zajišťující připojení nebo propojení prvku kritické infrastruktury, s kapacitou garantovaného datového přenosu nejméně 1 Gbit/s,

e) odvětvová kritéria pro určení prvku kritické infrastruktury uvedená v písmenech A. až F. se použijí přiměřeně pro oblast kybernetické bezpečnosti, pokud je ochrana prvku naplňujícího tato kritéria nezbytná pro zajištění kybernetické bezpečnosti" [36].



Obrázek 4 – Postup určování kritické informační infrastruktury [37]

2.7 Významný informační systém

Významný informační systém je takový systém, který je provozovaný orgánem veřejné moci. Tento informační systém nespadá do kritické informační infrastruktury, ale jeho narušení by mělo negativní dopad na výkon veřejné moci [38].

Významný informační systém se určuje podle dopadových a oblastních kritérií uvedené ve vyhlášce č. 317/2014 sb., o významných informačních systémech Naplnění těchto kritérií určuje sám správce systému [38].

3 CÍL PRÁCE

Hlavním cílem bakalářské práce je posouzení a analýza průřezových kritérií, která se používají ke stanovení prvku kritické informační infrastruktury. Případně pokud budou kritéria shledána nedostatečná, navrhne se jejich úprava. Dopad upravených kritérií na kybernetickou bezpečnost bude zhodnocen pomocí SWOT analýzy.

V teoretické části budou popsány pojmy související s kybernetickou bezpečnost v České republice a bude vymezena kritická informační infrastruktura.

4 METODIKA

Jednou z metod použitou v této práci je komparativní metoda. Jedná se o metodu porovnávání. Tuto metodu jsem využil k porovnání hodnot průřezových kritérií se statistickými hodnotami. Zpracoval jsem takto statistické hodnoty počtu obyvatel v obcích a okresech České republiky, objemu HDP pro rok 2018 a tržeb vybraných firem.

Další použitou metodou byla analýza. Pro jednotlivá kritéria jsem analyzoval oblasti, ve kterých by se mohla nacházet kritická informační infrastruktura. Jednotlivé oblasti jsem následně popsal a snažil se zjistit, jak velkou roli v nich hrají informační a komunikační systémy.

Po použití předchozích metod jsem navrhl úpravu průřezových kritérií. Dopad úprav na kybernetickou bezpečnost jsem zhodnotil pomocí SWOT analýzy.

5 VÝSLEDKY

5.1 Průřezová kritéria

V této kapitole se budu věnovat analýze průřezových kritérií a navržením jejich případné úpravy.

5.1.1 Průřezové kritérium s hlediskem obětí s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin

Česká republika k 1.1.2019 má 10 649 800 obyvatel, kteří žijí v 6 253 obcích. Pokud si vypočítáme, kolik má mít průměrně obyvatel jedna obec, zjistíme, že v každé obci by žilo 1703 lidí. Z tohoto průměru je viděl nemožnost dosáhnutí kritéria 2500 osob s následnou hospitalizací pro průměrnou obec. V České republice se ale nenachází průměrné obce. Jsou tu obce s vysokým počtem obyvatel a na druhou stranu s nízkým počtem obyvatel [39].

Tabulka 3 - Rozdělení obcí podle počtu obyvatel [39]

Počet obyvatel (v tisících)	Příklady měst	250 úmrtí na počet obyvatel (v %)	2 500 hospitalizovaných na počet obyvatel (v %)
20–50	Náchod, Znojmo, Chrudim	1,25 – 0,5	12,5 – 5
50–100	Jihlava, Pardubice, Opava	0,5 – 0,25	5 – 2,5
Nad 100	Praha, Brno, Liberec, Plzeň, Olomouc a Ostrava	0,25 a méně	2,5 a méně

Z této tabulky vyplývá, že kritérium 250 mrtvých a 2500 hospitalizovaných má uplatnění v obcích pod 100 000 obyvatel se, ale zdá být problematické, protože 2 500 hospitalizovaných představuje vysoké procento obyvatel. Podle mého předpokladu

se i v menších obcích nacházejí prvky kritické informační infrastruktury, jejíž narušení by způsobilo relativně velký počet zraněných a mrtvých. Kvůli velikosti obce by ale nebylo naplněno toto průřezové kritérium. Tento prvek tedy není zařazen mezi kritickou informační infrastrukturu, a tudíž nemusí splňovat přísnější podmínky zabezpečení.

V následujícím textu bych se chtěl zamyslet nad případy, při kterých by mohlo dojít k usmrcení nebo zranění většího počtu osob v souvislosti se selháním komunikačních a informačních systémů.

Doprava

V dnešní době téměř veškerá doprava nějakým způsobem závisí na komunikačních a informačních systémech. Jedná se o systémy řízení provozu dopravních zařízení (řízení letového provozu, řízení železniční dopravy) a řídící systémy dopravních prostředků samotných (řídící systém letadel). Vzhledem k rychlému rozvoji technologií v oblasti dopravy je stále důležitější ochrana komunikačních a informačních systémů.

- Letecká doprava

  Vyznačuje se vysokým počtem přepravovaných osob na dopravní prostředek a při nehodě vysokou pravděpodobností úmrtí. Nehoda v obydlené oblasti počet úmrtí ještě zvyšuje. Z toho vyplývá, že systémy v letecké dopravě by měly spadat do kritické informační infrastruktury.
- Železniční doprava

  V České republice je hustá železniční síť na přepravu materiálu a osob (průměrně 500 000 lidí přepraveno denně). V jedné drážní soupravě (např. Pendolino, CityElephant) je odhadem možné přepravovat až 500 osob. Při narušení komunikačního systému a následné srážce dvou vlaků je zde teoretická možnost úmrtí více než 250 osob. Největší vlaková tragédie

v České republice se stala u Stéblové v roce 1960. Nehoda měla za následek 118 mrtvých a 100 zraněných [40, 41].

- Pražské metro

  Denně přepraví více než jeden milion osob. Při narušení nebo selhání informačních a komunikačních systému v metru může dojít ke srážce souprav v tunelu s nebezpečím vzniku požáru. To představuje potenciální ohrožení s počtem většího úmrtí osob [42].

Podle mého názoru ostatní typy dopravy (silniční, vodní) z hlediska selhání nebo zneužití informačních a komunikačních systémů nemají schopnost ohrozit takový počet lidí, aby byla naplněna kritéria.

Jaderná elektrárna

V České republice jsou dvě jaderné elektrárny, Temelín a Dukovany. V jejich okolí se nachází značný počet obcí. Při narušení chodu jaderné elektrárny s následným únikem radiace nebo výbuchem bude postižena značná část území spolu s obyvatelstvem. Naplnění kritérií pro jadernou elektrárnu je jisté.

Chemický a petrochemický průmysl

Na území České republiky je několik chemických a petrochemických závodů. Při ovládnutí či selhání systémů je zde potenciál úniku jedovatých látek, případně výbuchu. V závislosti na lokalitě, kde se objekt nachází, může být ohrožen takový počet lidí, aby bylo splněno kritérium.

Zdravotnická zařízení

Ve zdravotnických zařízeních je poskytována pomoc lidem. Pokud dojde k narušení provozu zdravotnického zařízení jsou ohroženi na životech hospitalizovaní pacienti i potenciální pacienti, kterým nebude moci být poskytnuta pomoc. Aby byla naplněna kritéria je nutné znát kolik je v zařízení lůžek a jaké jsou kapacity.

Největší nemocnicí v České republice je Fakultní nemocnice v Motole s kapacitou 2 199 lůžek a stovkami ambulantně ošetřených pacientů každý den. Potenciálně tedy vzniká možnost naplnění kritéria ve větších nemocnicích [43].

Panika

Při narušení služeb nebo při rozšíření nepravdivé poplašné zprávy může dojít k nárustu paniky mezi lidmi. Způsobená panika zapříčiní smrt a zranění. Jako přiklad bych uvedl možnost masové hysterie na místech s vysokou koncentrací osob (fotbalový zápas, koncert, náboženská setkání atd.)

Návrh úpravy kritéria

Podle mého názoru je potřeba tato kritéria vhodně upravit. Česká republika je malá země s nízkým počtem obyvatel. Takováto kritéria jsou využitelná pouze ve větších obcích, ale nelze je vhodně aplikovat na menší obce. Proto mi připadá, že kritéria jsou nastavena vysoko. Existuje spousta prvků, které při nefunkčnosti mohou ohrozit zdraví a životy velkého počtu lidí, avšak nesplňují kritéria usmrcených a hospitalizovaných osob. Moje navrhovaná úprava je snížit kritéria.

Navrhoval bych kritérium pro usmrcené snížit na hodnot 50 osob a zraněných na hodnotu 500 osob. Vycházel jsem z procentuálního vyjádření stávajících hodnot kritérií ve 100 000 městech. Záměrem se bylo dostat na stejné procentuální vyjádření u města s 20 000 obyvateli.

SWOT analýza

Předmětem této analýzy je hodnocení dopadu navržené změny kritéria na kybernetickou bezpečnost.

Tabulka 4- SWOT analýza upravovaného prvního kritéria

Silné stránky	Slabé stránky
• Větší počet prvků kritické informační infrastruktury	• Zvýšení nákladů na provoz
Příležitosti	**Hrozby**
• Budování silnější infrastruktury • Lepší bezpečnost obyvatel	• Nedostatečný rozpočet • Nedostatek kvalifikovaných zaměstnanců

Zavedením změny kritéria dojde ke zvýšení počtu prvků spadajících do kritické informační infrastruktury. Následkem toho bude robustnější a odolnější oblast kybernetické bezpečnosti v České republice. Problémem by mohlo být zvýšení nákladů na provoz. Tento záměr by mohl ohrozit nedostatečný rozpočet a nedostatek kvalifikovaných zaměstnanců na trhu práce.

5.1.2 Průřezové kritérium s hlediskem ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu

Hrubí domácí produkt (dále jen „HDP“) v roce 2018 tvořil 5 310,3 mld. Kč, z toho 0,5 % je 26,56 mld. Kč. Když bylo toto kritérium v roce 2010 uvedeno do praxe, HDP tvořilo 3 667,6 mld. Kč z kterých 0,5 % je 18,34 mld. Kč. Z uvedeného je vidět, že Česká republika bohatne, zvyšuje se HDP, tím se zvyšuje i hodnota pro splnění kritéria [44].

Pro ilustraci si uvedeme nejvýdělečnější firmy za rok 2018. Na nich bych chtěl ukázat, jak dlouho by trvalo, aby firma zaznamenala ztrátu ve výši rovnající se 0,5 % HDP. V následující tabulce je vypsáno deset firem, které se v roce 2018 nejvíce podíleli na tvorbě HDP.

Tabulka 5 - Nejvýdělečnější firmy v České republice [45]

Firmy	Tržby (v mld. Kč)	Tržby za den (v mld. Kč)	Počet dní ke ztrátě 26,56 mld. Kč
ŠKODA AUTO, a.s.	407	1,12	24
ČEZ, a.s.	202	0,55	48
AGROFERT, a.s.	155	0,42	63
Energetický a průmyslový holding, a.s.	153	0,42	63
UNIPETROL, a.s.	119	0,33	80
FOXCONN CZ s.r.o.	104	0,29	92
MORAVIA STEEL, a.s.	57	0,16	166
BOSCH Group ČR	52	0,14	190
ČEPRO, a.s.	48	0,13	204
MOL Česká republika, s.r.o.	46	0,13	204

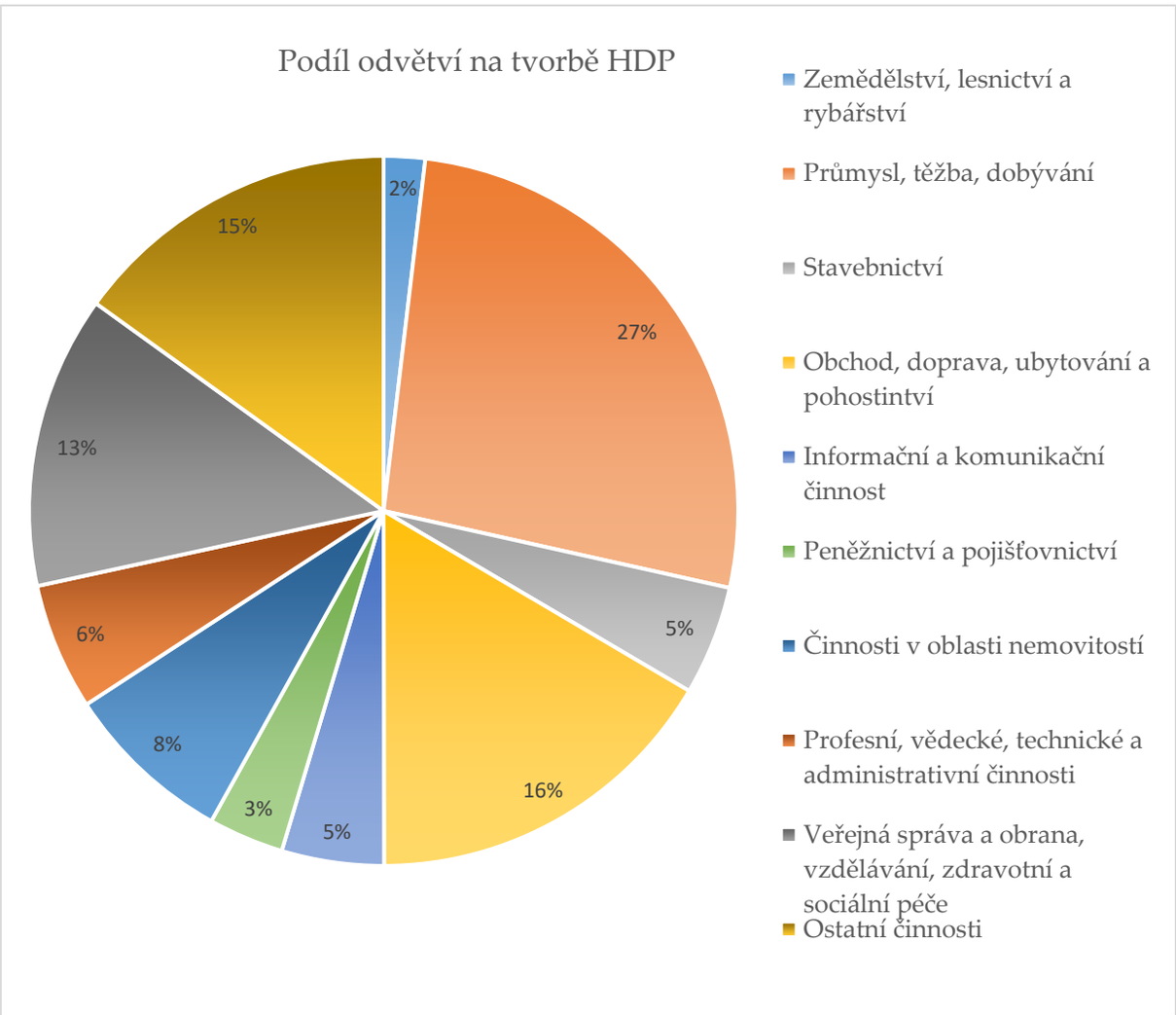
V tabulce jsou uvedeny tržby firem za celý rok. Roční tržba je přepočítána na denní tržbu a zaokrouhlena na dvě desetinná místa. V posledním sloupci je uveden počet dní, ve kterých firma nebude moci provádět svoji činnost a tím vznikne škoda 0,5 % HDP, tedy 26,56 mld. Kč. Jak můžeme vidět u nejvýkonnější české firmy Škoda auto, a.s. by muselo dojít ke kompletnímu přerušení výroby na 24 dní.

Tabulka 6 - Součet nejvýdělečnějších firem [45]

Firma	Součet tržeb (v mld. Kč)	Tržby za den (v mld. Kč)	Počet dní ke ztrátě 26,56 mld. Kč
10 nejvýdělečnějších	1343	3,68	7

V předchozí tabulce jsem použil součet tržeb firem. Následně byla celková tržba přepočítána na denní tržbu a čas, který by byl potřebný ke ztrátě 0,5 % HDP. Aby bylo splněno kritérium je třeba vyřadit z provozu 10 nejvýdělečnějších firem na 7 dní.

Podle následujícího grafu, který nám zobrazuje procentuální podíl jednotlivých odvětví na HDP, rozeberu vliv informačních a komunikačních systémů na tato odvětví.



Obrázek 5 – Graf podílu odvětví na tvorbě HDP [45]

Zemědělství, lesnictví a rybářství

Tato odvětví tvoří 2 % z celkového HDP. Informační a komunikační systémy nehrají v těchto odvětvích velkou roli. Naplnění kritéria je nepravděpodobné.

Průmysl, těžba a dobývání

Odvětví tvoří 27 % z celkového HDP. Role informačních a komunikačních systému je v tomto odvětví velká, ať už se jedná o prvky komunikační, prvky automatizace a řídících systémů či informační systémy. Jelikož se jedná o odvětví s největším příspěvkem do HDP, je největší pravděpodobnost, že by kritérium mohlo být naplněno. Narušení těchto odvětí má dopad i v ostatních oblastech. Energetický průmysl ovlivňuje téměř všechny ostatní oblasti, nefunkčnost by měla synergický efekt.

Stavebnictví

Stavebnictví tvoří 5 % HDP. Z pohledu narušení komunikačních a informačních systémy mi přijde oblast stavebnictví zanedbatelná.

Obchod, doprava, ubytování a pohostinství

Odvětví s druhým největším podílem na tvorbě HDP a to 16 %. V těchto odvětvích májí informační a komunikační systémy největší vliv v dopravě a obchodě. Problémy v dopravě mohou zapříčinit další problémy v jiných oblastech a tím se můžou finanční ztráty násobit.

Informační a komunikační činnost

Oblast tvořící 5 % HDP. Nedostupnost služeb v této oblasti, zvláště potom telefonních služeb a internetu, by znamenalo problémy pro ostatní odvětví. Z hlediska HDP nepatří mezi nejvýznamnější.

Peněžnictví a pojišťovnictví

Podíl na HDP tvoří 3 %. Informační a komunikační infrastruktura zde hraje klíčovou roli, ale z hodnoty HDP není významný. Výpadek by nezpůsobil závažné

škody v tomto sektoru. Vliv nedostupnosti služby by měl větší finanční dopad na ostatní odvětví.

Činnost v oblasti nemovitostí

Podíl HDP je 8 %. Informační systémy jsou v oblasti využívány, ale jejich výpadek by neměl způsobit citelné ztráty.

Profesní, vědecké, technické a administrativní činnosti

Oblast tvořící 6 % HDP. Za zmínku stojí vědecká činnost, u které by se mělo dbát na ochraně informací. Při úniku či krádeži výzkumné práce by mohlo dojít k potenciálně vysokým ztrátám.

Veřejná správa, obrana, vzdělávání, zdravotní a sociální péče

Oblasti tvořící 13 % HDP. Nefunkčnost veřejné správy by mohla způsobit kolaps veřejného života. Nebyly by vypláceny důchody a sociální dávky. Mohla by být znesnadněna činnost bezpečnostních a záchranných sborů. Omezením chodu nemocnic vznikají potíže s ošetřením pacientů. Všechny tyto oblasti mají dopad na tvorbu HDP.

Návrh úpravy kritéria

Po provedeném rozboru kritéria je mým názorem, že je téměř nemožné jeho podmínku naplnit. Proto bych se zamyslel nad možností vyřazení kritéria.

SWOT analýza

Předmětem této analýzy je hodnocení dopadu navržené změny kritéria na kybernetickou bezpečnost.

Tabulka 7 - SWOT analýza zrušeného kritéria

Silné stránky	Slabé stránky
• Žádné	• Neexistence kritéria
Příležitosti	**Hrozby**
• Zlevnění procesu určování prvku • Zjednodušení procesu určování prvku	• Nezjištění prvku kritické informační infrastruktury

Navrhovanou úpravou kritéria dojde ke zlevnění a zjednodušení určování prvku kritické informační infrastruktury. Tím, že kritérium nebude používáno pro určování kritické informační infrastruktury může dojít k opomenutí některého prvku.

5.1.3 Průřezové kritérium s hlediskem dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob

Česká republika má 10 649 800 obyvatel. Z celkového počtu obyvatel tvoří 125 000 osob 1,3 %. Na území České republiky se nachází pouze 6 měst, které přesahují 100 000 obyvatel, z toho 4 přesahují 125 000 obyvatel. To znamená, že se musí jednat o služby, které působí na rozsáhlejším území. Průměrná hustota obyvatel je 136 na kilometr čtvereční. Rozloha České republiky je 78 865 kilometrů čtverečních. Z toho vyplývá, že pokud má být postiženo 125 000 lidí, rozloha událost musí mít v průměru 919 kilometrů čtverečních. Samozřejmě je to jenom průměr, v místech většího zalidnění a větší koncentrace osob rozloha klesá. Podíváme-li se na tabulku okresů v Jihočeském kraji, ve které vidíme počet obyvatel a rozlohu. Tabulka nám

ilustruje nemožnost naplnění kritéria pro poměrně velká území České republiky. [40].

Tabulka 8 - Počet obyvatel a rozloha v okresech [44]

Okres	Počet obyvatel	Rozloha (v km²)
České Budějovice	194 585	1 639
Český Krumlov	61 381	1 616
Jindřichův Hradec	90 653	1 944
Písek	71 308	1 127
Prachatice	50 971	1 375
Strakonice	70 738	1 032
Tábor	102 497	1 326

Mezi služby jejíchž výpadek by postihl více než 125 000 osob můžeme zařadit:

Distribuce elektrické energie

Narušení informačních systémů rozvodů a výroby energie může způsobit výpadek elektrárny, případně rozvodné sítě. Následkem je neschopnost dodávat elektrickou energii podnikům a obyvatelstvu. Průměrná spotřeba elektrické energie na osobu v domácnosti je 1,4 megawatthodiny za rok. Což činí 3,8 kilowatthodiny za den. Pro 125 000 osob to představuje 475 megawatthodin za den potřebného výkonu. Pro orientaci je níže uvedena tabulka s vybranými českými elektrárnami, jejich instalovaným výkonem a energií dodanou za den provozu [47].

Tabulka 9 - Výkon elektráren [46]

Elektrárna	Instalovaný výkon (v MW)	Výkon za 24 hodin (v MWh)
Hodonín (uhelná)	105	2 520
Dukovany (jaderná)	2 040	48 960
Počerady (paroplynová)	838	20 112

Podíváme-li se do tabulky č. 7 na elektrárnu Hodonín, která patří k nejmenším uhelným elektrárnám, vidíme, že je schopna dodávat potřebnou energii pro více než 600 000 lidí. I výpadek té nejmenší elektrárny naplní hodnotu kritéria.

Distribuce elektrické energie je důležitá i pro ostatní odvětví.

Distribuce vody

Útokem na systémy v úpravnách vod může dojít k úplnému přerušení dodávky vody nebo k jejím znehodnocení nevhodným dávkováním chemických přípravků. Zamezení dodávky vody se docílí také napadením systému distribuce, kde dojde k vyřazení části vodovodního řadu (zavření ventilů, vypnutí čerpadla).

Distribuce pohonných hmot

V případě vyřazení dodávek ropy je po nějaký čas možné čerpat ropu ze státních rezerv, tudíž nedojde k okamžitému omezení. Po čase se omezení může projevit v nedostupnosti pohonných hmot. K tomu by také mohlo dojít, kdyby jedna ze tří českých rafinerií byla vyřazena z provozu. Nedostatek pohonných hmot by se projevil omezením dopravy osob, ale především veškerého zboží. Časem by se to mohlo projevit na snížení výkonu záchranných a bezpečnostních složek.

Distribuce plynu

Ovládnutím systému rozvodu plynu má v lepším případě za následek přerušení dodávky plynu. V horším případě je systém napaden a ovlivněn tak, že dojde až k výbuchu plynovodu. Tím se omezí dostupnost plynu. Tento nedostatek se projeví v nemožnosti vytápět domácnosti a veřejné budovy, které mají plynové kotelny, či nefunkčností paroplynových elektráren.

Doprava

Narušením dopravních systémů Českých drah a Pražského metra ztíží přepravu osob např. do zaměstnání. Následné využití automobilové přepravy může způsobit zahlcení silnic.

Bankovní služby

Vyřazením bankovních služeb (internetové bankovnictví, nemožnost použití platebních karet) je znemožněno obyvatelstvu platit své závazky, nakupovat potraviny a ostatní zboží, pokud nemají zásobu ve finanční hotovosti.

Návrh úpravy kritéria

Hodnota 125 000 zasažených osob je dle mého názoru vysoká. Kritérium je uplatnitelné pro území s vyšší hustotou obyvatel. Navrhuji úpravu kritéria snížením počtu zasaženým osob na 50 000. U kritéria mi také schází časový limit nedostupnosti služby, proto bych navrhoval jeho zavedení. Každá služba má jiný časový limit, po který jsme schopni se bez ní obejít. Při stanovení hodnoty jsem vycházel z nejnižší akceptovatelné doby nedostupnosti služby. Nejvíce potřebná služba je dodávka energií v zimním období, kdy již jeden den omezení služby je nekomfortní. Proto bych zvolil 24 hodin jako minimální limit pro uplatnění kritéria.

SWOT analýza

Předmětem této analýzy je hodnocení dopadu navržené změny kritéria na kybernetickou bezpečnost.

Tabulka 10 - SWOT analýza upravovaného třetího kritéria

Silné stránky	Slabé stránky
• Vetší počet prvků kritické informační infrastruktury • Ochrana většího území	• Zvýšení nákladů na provoz • Zvýšení náročnosti určení prvku
Příležitosti	**Hrozby**
• Kvalitnější kritická informační infrastruktura • Zajištění bezpečnosti více obyvatel	• Nedostatečný rozpočet • Častější výpadky služeb • Nedostatek kvalifikovaného personálu

Úpravou kritéria dojde ke zvýšení počtu prvků spadajících do kritické informační infrastruktury a zvětšení chráněného území. Bude zajištěna bezpečnost většího počtu obyvatel. Kybernetická bezpečnost bude na vyšší úrovni. Zvýšení nákladů na provoz je zmírněno navrženým časovým omezením nedostupnosti. Nedostatečný rozpočet na provoz systému a problémy s personálním obsazením by mohly ohrozit realizaci projektu.

6 DISKUZE

V roce 2004 se Evropská komise a rada začaly zabývat zabezpečením kritické infrastruktury. V roce 2008 byla vydána a schválena Směrnice rady 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. Ve směrnici jsou uvedena průřezová kritéria pro určení prvku kritické infrastruktury. V návaznosti na tento dokument Česká republika jakožto člen Evropské unie měl povinnost zavést některé předpisy do své legislativy. Česká republika tuto povinnost splnila v roce 2010, kdy vydala zákon č. 430/2010, kterým se mění zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon). V této úpravě zákona byly definovány pojmy v oblasti kritické infrastruktury a popsána, co to jsou průřezová kritéria. K zákonu bylo vydáno i nařízení vlády č. 432/2010 sb., které obsahuje konkrétní hodnoty průřezových kritérií.

S rostoucí závislostí osob, organizací i států na informačních a komunikačních systémech rostla jejich důležitost. I každá kritická infrastruktura má své informační a komunikační systémy, které je nutné chránit. Proto se v zákoně č. 181/2014 o kybernetické bezpečnosti a o změně souvisejících zákonů definují tyto systémy jako kritická informační infrastruktura. Jejíž zabezpečením se zabývá oblast kybernetické bezpečnosti.

Jak už bylo zmíněno výše, hlavním cílem kybernetická bezpečnost v České republice je zajistit ochranu kritické informační infrastruktury před napadením, které přichází nejčastěji z kybernetického prostoru. Účelem takového napadení může být zničení systému, krádež informací, špionáž, vydírání a další.

Zajištění kybernetické bezpečnosti má na starosti ústřední správní orgán nazývaný Národní úřad pro kybernetickou a informační bezpečnost, který tuto oblast převzal v roce 2017 od Národního bezpečnostního úřadu. Výkonnou složkou

NÚKIB je Národní centrum kybernetické bezpečnosti. Tato sekce má na starosti zajištění preventivní činnosti a bezpečnosti prvků kritické informační infrastruktury před kybernetickými útoky. Pro tento úkol je zřízen tým s názvem Vládní CERT, který reaguje a řeší kybernetické bezpečnostní incidenty.

Vrátíme se zpět ke kritické informační infrastruktuře a podíváme se na princip, kterým se určuje. Jak jsem již uváděl na začátku diskuze, vše vyplývá z právních dokumentů, ve kterých jsou uvedena kritéria, jimiž se tyto prvku určují. Kritéria jsou rozdělena na průřezová a odvětvová. Pokud má prvek být kritickou informační infrastrukturou musí splňovat alespoň jedno průřezové kritérium. Průřezové kritérium je hledisko:

a) obětí s mezní hodnotou více než 250 mrtvých nebo více než 2500 osob s následnou hospitalizací po dobu delší než 24 hodin, nebo
b) ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo
c) dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125000 osob [34].

Jestliže je tedy naplněno některé z průřezových kritérií, musí se dále zkoumat odvětvová kritéria. To jsou přesně dané technické hodnoty. Po naplnění minimálně jednoho odvětvového kritéria se stane zkoumaný objekt prvkem kritické informační infrastruktury.

V praktické části jsem zkoumal využitelnost hodnocení průřezových kritérií sloužících k určování kritické informační infrastruktury. Při hodnocení jsem vycházel z geografických, demografických a ekonomických údajů České republiky. Podle daných kritérií jsem se zaměřil na oblasti, ve kterých jsem předpokládal, že by

nefunkčnost jejich informačních a komunikačních systémů splnila požadované hodnoty ke stanovení kritické informační infrastruktury.

Jako první bylo posouzeno kritérium, kde jsou stanoveny mezní hodnoty 250 mrtvých a 2 500 hospitalizovaných. Na kritérium jsem se pokusil podívat z hlediska celkového počtu obyvatel v České republice, jejich rozložení v okresech a obcích. Obce jsem rozdělil do tří kategorií podle počtu obyvatel a vypočítal jsem, kolik procent by tvořilo 250 mrtvých a 2500 hospitalizovaných. V kategorii nad 100 000 obyvatel to činí 0,25 % a méně pro úmrtí a 2,5 % a méně pro hospitalizované. V obcích o velikosti 50 000 až 100 000 obyvatel jsou tyto poměry 0,5 % až 0,25 % a 5 % až 2,5 %. V poslední kategorii, ve které je počet obyvatel v obci 20 000 až 50 000, by počet mrtvých v těchto obcích tvořil 1,25 % až 0,5 % a hospitalizovaných 12,5 % až 5 %.

Následně jsem se pokusil rozebrat tuto problematiku z hlediska oblastí, kde by mohlo při nefunkčnosti nebo zneužití informačního či komunikačního systému dojít k velkému počtu obětí na životech nebo zraněných. Začal jsem oblastí dopravy, ve které jsem identifikoval největší rizika v letecké a železniční dopravě. Další velké riziko představují jaderné elektrárny, chemické a petrochemické závody. Dle mého názoru by neměla být podceněna také kybernetická bezpečnost nemocnic.

Z předchozího rozboru jsem dospěl k závěru, že by mělo dojít k úpravě kritéria. Podle mého názoru by mělo dojít k jeho snížení na hodnoty 50 mrtvých a 500 hospitalizovaných. K uvedenému výsledku jsem dospěl úvahou, jelikož i v menších obcích se mohou nacházet prvky, které by měly být chráněny jako kritická infrastruktura. Mým záměrem bylo docílit stejného procenta, jako u hodnot současného kritéria aplikovaného na obec se 100 000 obyvateli pro obec s 20 000 obyvateli.

Problematikou průřezových kritérií se zabývá ve své diplomové práci Bc. Věra Tomková. Při úpravě kritéria s počtem mrtvých a hospitalizovaných použila jinou metodiku. Její hodnoty jsou 146 mrtvých a 1458 hospitalizovaných. Ve své práci také zmiňuje kritéria používána v Maďarsku. Maďarské hodnoty jsou minimálně 20 mrtvých nebo 75 zraněných za 24 hodin a minimálně 40 mrtvých nebo 150 zraněných za 72 hodin. Moje úprava je tedy radikálnější než u Bc. Tomkové, ale oba dva se shodujeme na snížení hodnot kritéria. Naopak v Maďarku jsou hodnoty mnohem nižší oproti mému návrhu.

Druhým posuzovaným kritériem byla ztráta vyšší než 0,5 % HDP. Pro lepší představu jsem si přepočítal, kolik je 0,5 % HDP financí. Z toho vyšlo, že v roce 2018 to bylo 26,56 mld. Kč. Poté jsem uvedl deset nejvýdělečnějších firem v České republice a jejich tržby. Zajímalo mě, na jak dlouho by musela být přerušena jejich činnost, aby se ztráta tržby rovnala 26,56 mld. Kč (uvažoval jsem nepřetržitý provoz). U firmy s nejvyššími tržbami je to 24 dní. Pokud bychom stejně postupovali u součtu tržeb všech deseti firem, dostaneme se na 7 dní zastavení výroby.

Ze statistických údajů o zdrojích HDP byl vytvořen graf s procentuálním zastoupením jednotlivých oblastí ekonomiky státu. V každém z těchto odvětví jsem posoudil, jaký vliv v něm mají informační a komunikační systémy, a jaký dopad by měla jejich nefunkčnost na HDP.

Z předešlé analýzy bych označil toto kritérium jako nadbytečné při určování prvku kritické informační infrastruktury a navrhl bych ho nepoužívat. K tomuto závěru mě dovedla vypočítaná délka výpadku deseti nejvýdělečnějších firem. Myslím si, že je obtížné zapříčinit nefunkčnost informačních a komunikačních systému na 7 dní. Pokud by k takové události došlo, s největší pravděpodobností by bylo naplněno alespoň jedno z dalších kritérií (nejspíše kritérium o omezení poskytování služeb).

Znovu budu navrhovanou úpravu kritéria porovnávat s diplomovou prací Bc. Věry Tomkové. I u tohoto kritéria použila jinou metodu úpravy. Navrhuje snížit hodnotu ztráty HDP z 0,5 % na 0,25 %. Z mého pohledu snížení na 0,25 % nehraje zásadní roli.

Poslední hodnocené kritérium je o omezení poskytovaných služeb pro 125 000 osob. K analyzování tohoto kritéria jsem přistoupil podobně jako u prvního kritéria. V potaz jsem vzal počet obyvatel v České republice, hustota zalidnění, rozložení obyvatelstva v krajích a okresech. Pro ilustraci jsem uvedl tabulku s okresy v Jihočeském kraji, jejich počet obyvatel a rozlohu. Z porovnání okresů je vidět rozdílnost počtu obyvatel na srovnatelném území.

Následně jsem se zamyslel nad službami, které svojí důležitostí zasahují do každodenního života velkého množství lidí. Mezi hlavní služby patří dodávky energií a vody.

Z vyhodnocení sesbíraných informací jsem navrhl dvě úpravy kritéria. První spočívá ve snížení počtu zasažených osob ze 125 000 na 50 000. K tomu mě vedlo již zmíněné porovnání velikosti okresů v Jihočeském kraji a počtu jejich obyvatel. Stanovil jsem si okres jako správní jednotku. Nejnižší počet obyvatel v okresech Jihočeského kraje je 50 971 (Prachatice). Proto jsem stanovil hodnotu kritéria na 50 000. Druhá úprava kritéria spočívá v zavedení časového limitu, po který nemusí být služba poskytována. Mnou stanovená hodnota se rovná 24 hodinám. K tomu jsem dospěl úvahou, jak dlouho je člověk schopen snášet snížení komfortu v podobě především nedostatku tepla, světla a vody.

Má úprava kritéria v porovnání s úpravou v diplomové práci Bc. Věry Tomkové se z části shoduje. Oba navrhujeme snížení hodnoty zasažených obyvatel. V její práci na 72 917 a v mé na již zmíněných 50 000.

Zhodnocením úpravy kritérií pomocí SWOT analýzy jsem došel k závěru, že by tyto úpravy měli dva hlavní dopady na kybernetickou bezpečnost. Prvním je vznik nových prvků kritické informační infrastruktury. Z toho vyplývá druhý dopad, kterým by bylo zvýšení nákladů na provoz.

7 ZÁVĚR

V teoretické části bakalářské práce jsem se zabýval popisem základních pojmů v oblasti kybernetické bezpečnosti a subjektů, které se jí v České republice zabývají. Dále jsem uvedl, co je to kritická informační infrastruktura.

V praktické části jsem se zabýval stanoveným cílem, kterým bylo posouzení a hodnocení průřezových kritérií používaných pro určení kritické informační infrastruktury v České republice. Poté byla navržena úprava kritérií, která jsem zhodnotil SWOT analýzou.

Studiem a rozborem problematiky jsem došel k závěru, že by bylo vhodné upravit všechna stávající průřezová kritéria. Má úprava u dvou kritérií spočívala ve snížení zákonem stanovených hodnot a třetí kritérium jsem navrhl pro určovaní kritické informační infrastruktury nepoužívat. Snížení hodnot kritérií by mělo vést ke zvýšení počtu prvků kritické informační infrastruktury a tím i ke zvýšení úrovně kybernetické bezpečnosti. Problémem by mohlo být zvýšení finanční náročnosti na provoz prvků, popřípadě nedostatek kvalifikovaného personálu. Zrušení kritéria s hlediskem ekonomického dopadu zjednoduší proces určování prvků infrastruktury.

Do budoucna by bylo vhodné analyzovat i odvětvová kritéria, která se taktéž používají k určení kritické informační infrastruktury, a posoudit jejich uplatnění podobnou metodikou jako jsem provedl u průřezových kritérií ve své práci.

Závěrem bych rád uvedl, že Česká republika je v oblasti kybernetické bezpečnosti na světové úrovni. Avšak je důležité se stále zlepšovat, jelikož digitální technologie prochází neustálým rychlým vývojem. Je tedy nutné sledovat vývoj trendů a vhodně na ně reagovat.

8 SEZNAM POUŽITÝCH ZKRATEK

ICT	Informační a komunikační technologie
TPC/IP	Transmission Control Protocol/Internet Protocol
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
NCKB	Národní centrum kybernetické bezpečnosti
OKBP	Odbor kybernetických bezpečnostních politik
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
HDP	Hrubý domácí produkt

9 SEZNAM POUŽITÉ LITERATURY

[1] POLČÁK, Radim, Martin ŠKOP a Jakub MACEK. Normativní systémy v kyberprostoru: (úvod do studia). Brno: Masarykova univerzita, 2005. ISBN 80-210-3779-2.

[2] HRŮZA, Petr. Kybernetická bezpečnost II. Brno: Univerzita obrany, 2013. ISBN 978-80-7231-931-2.

[3] KOLOUCH, Jan a Pavel BAŠTA. CyberSecurity. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-31-7.

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

[5] MAISNER, Martin. Zákon o kybernetické bezpečnosti: komentář. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8.

[6] Cyber. Techtarget [online]. [cit. 2019-05-13]. Dostupné z: https://searchmicroservices.techtarget.com/definition/cyber

[7] Kybernetická bezpečnost (Cyber Security). Cybersecurity [online]. Petr Jirásek, 2017 [cit. 2019-05-13]. Dostupné z: https://www.cybersecurity.cz/basic.html

[8] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. Výkladový slovník kybernetické bezpečnosti: Cyber security glossary. Třetí aktualizované vydání. Praha: Policejní akademie ČR v Praze, 2015. ISBN 978-80-7251-436-6.

[9] NEIL, Ian. CompTIA Security+ Certification Guide: Master IT security essentials and exam topics for CompTIA Security+ SY0-501 certification. Packt Publishing, 2018. ISBN 978-1-78934-801-9.

[10] ČERMÁK, Miroslav. CIA: Důvěrnost. Cleverandsmart [online]. 2013 [cit. 2019-05-13]. Dostupné z: https://www.cleverandsmart.cz/duvernost/

[11] ŠULC, Vladimír. Kybernetická bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2018. ISBN 978-80-7380-737-5.

[12] Vyhláška č. 82/2018 Sb. *Zakonyprolidi* [online]. 2018 [cit. 2019-05-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2018-82

[13] ČERMÁK, Miroslav. CIA: Dostupnost. Cleverandsmart [online]. 2010 [cit. 2019-05-13]. Dostupné z: https://www.cleverandsmart.cz/dostupnost/

[14] DUTTON, Julia. Three pillars of cyber security. *Itgovernance* [online]. Ely, 2017 [cit. 2019-05-13]. Dostupné z: https://www.itgovernance.co.uk/blog/three-pillars-of-cyber-security

[15] The Sage Cybersecurity Lifecycle: Cybersecurity isn't a destination. *Sagedatasecurity* [online]. [cit. 2019-05-13]. Dostupné z: https://www.sagedatasecurity.com/lifecycle

[16] Základní pojmy. *Kybez* [online]. [cit. 2019-05-13]. Dostupné z: https://www.kybez.cz/bezpecnost/pojmoslovi

[17] BEZPEČNOSTNÍ ROLE a jejich začlenění v organizaci. *Govcert* [online]. Brno, 2019 [cit. 2019-05-13]. Dostupné z: https://www.govcert.cz/download/kii-vis/VKB/bezpe%C4%8Dnostn%C3%AD-role_v1.1.pdf

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

[19] Sociální inženýrství. *Národní centrum kybernetické bezpečnosti* [online]. Brno [cit. 2019-05-13]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/doporuceni/2486-socialni-inzenyrstvi/

[20] Malware. *Eset* [online]. [cit. 2019-05-13]. Dostupné z: https://www.eset.com/cz/malware/

[21] KRÁL, Mojmír. *Bezpečný internet: chraňte sebe i svůj počítač*. Praha: Grada Publishing, 2015. Průvodce (Grada). ISBN 978-80-247-5453-6.

[22] BOTNET. *Internetembezpecne* [online]. Karlovy Vary [cit. 2019-05-13]. Dostupné z: https://www.internetembezpecne.cz/internetem-bezpecne/malware/botnet/

[23] What is a distributed denial of service attack (DDoS) and what can you do about them? *Emerging Threats* [online]. [cit. 2019-05-13]. Dostupné z: https://us.norton.com/internetsecurity-emerging-threats-what-is-a-ddos-attack-30sectech-by-norton.html

[24] Zákon č. 181/2014 Sb. *Zakonyprolidi* [online]. 2019 [cit. 2019-05-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-181

[25] Národní úřad pro kybernetickou a informační bezpečnost. *Úřední deska* [online]. NÚKIB [cit. 2019-05-13]. Dostupné z: https://www.nukib.cz/

[26] Národní úřad pro kybernetickou a informační bezpečnost. *Organizační struktura* [online]. [cit. 2019-05-13]. Dostupné z: https://www.nukib.cz/cs/o-nukib/organizacni-struktura-uradu/

[27] Hlášení incidentů. *Národní úřad pro kybernetickou a informační bezpečnost* [online]. [cit. 2019-05-13]. Dostupné z: https://www.govcert.cz/cs/vladni-cert/hlaseni-incidentu/

[28] CSIRT.CZ. *Služby* [online]. [cit. 2019-05-13]. Dostupné z: https://www.csirt.cz/page/2764/sluzby/

[29] Vláda České republiky: Výbor pro kybernetickou bezpečnost. *Vlada* [online]. [cit. 2019-05-13]. Dostupné z: https://www.csirt.cz/paghttps://www.vlada.cz/cz/ppov/brs/pracovni-vybory/kyberneticka_bezpecnost/vybor-pro-kybernetickou-bezpecnost-159932/e/2764/sluzby/

[30] Infrastruktura (Infrastructure). *Managementmania* [online]. [cit. 2019-05-13]. Dostupné z: https://managementmania.com/cs/infrastruktura-infrastructure

[31] KRATOCHVÍLOVÁ, Danuše a FOLWARCZNY, Libor, Ochrana obyvatelstva, ed. 2., Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2013, ISBN 978-80-7385-134-7

[32] ŠENOVSKÝ, Michail, ADAMEC, Vilém, ŠENOVSKÝ, Pavel, Ochrana kritické infrastruktury, ed. 1., Ostrava: Sdružení požárního a bezpečnostního inženýrství, 2007, ISBN 978-80-7385-025-8

[33] Zákon č. 240/2000 Sb. *Zakonyprolidi* [online]. 2017 [cit. 2019-05-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2000-240

[34] Nařízení vlády č. 432/2010 Sb. *Zakonyprolidi* [online]. 2015 [cit. 2019-05-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2010-432

[35] JORDÁN, Vilém a Viktor ONDRÁK. *Infrastruktura komunikačních systémů II: kritické aplikace*. Brno: CERM, Akademické nakladatelství, 2015. ISBN 9788021452404.

[36] Nařízení vlády č. 315/2014 Sb. *Zakonyprolidi* [online]. 2015 [cit. 2019-05-13]. Dostupné z: https://www.zakonyprolidi.cz/cs/2014-315

[37] Kritická informační infrastruktura. *Govcert* [online]. Brno, 2018 [cit. 2019-05-13]. Dostupné z: https://www.govcert.cz/download/kii-vis/Schema_KII.pdf

[38] Národní centrum kybernetické bezpečnosti: POVINNÉ OSOBY. *Govcert* [online]. [cit. 2019-05-13]. Dostupné z: https://www.govcert.cz/cs/regulace-a-kontrola/povinne-osoby/

[39] Počet obyvatel. *Český statistický úřad* [online]. 2019 [cit. 2019-05-13]. Dostupné z: https://www.czso.cz/csu/czso/pocet-obyvatel-v-obcich-za0wri436p

[40] Služby v regionálních vlacích ČD. *České dráhy* [online]. [cit. 2019-05-13]. Dostupné z: https://www.cd.cz/nase-vlaky/regionalni-vlak-cd/cityelefant/-25418/#kotva

[41] PŘEHLED: Vlaková neštěstí na území Česka. Při největší tragédii zemřelo 118 lidí. *Lidovky* [online]. Praha: MAFRA, 2015 [cit. 2019-05-13]. Dostupné z: https://www.lidovky.cz/domov/vlakova-nestesti-v-cesku-pri-nejvetsi-tragedii-zemrelo-118-lidi.A150722_101134_ln_domov_sk

[42] Pražské metro. *Metro Praha* [online]. Praha [cit. 2019-05-13]. Dostupné z: http://www.metro-praha.info/

[43] Fakultní nemocnice v Motole v číslech. *Fakultní nemocnice v Motole* [online]. Praha [cit. 2019-05-13]. Dostupné z: http://www.fnmotol.cz/o-nas/historie-a-soucasnost/fakultni-nemocnice-v-motole-v-cislech/

[44] Český statistický úřad. *HDP, národní účty* [online]. Praha, 2019 [cit. 2019-05-13]. Dostupné z: https://www.czso.cz/csu/czso/hdp_narodni_ucty

[45] 100 nejvýznamnějších. *Czechtop100* [online]. 2018 [cit. 2019-05-13]. Dostupné z: https://www.czechtop100.cz/cs/projekty/zebricky/100-nejvyznamnejsich

[46] Výroba elektřiny. *Skupina ČEZ* [online]. 2019 [cit. 2019-05-13]. Dostupné z: https://www.cez.cz/cs/vyroba-elektriny.html

10 SEZNAM POUŽITÝCH OBRÁZKŮ

11 SEZNAMU POUŽITÝCH TABULEK