

Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky



Vybrané aspekty zákona o kybernetické bezpečnosti

BAKALÁŘSKÁ PRÁCE

Studijní program: Aplikovaná informatika

Studijní obor: Aplikovaná informatika

Autor: Eliška Kühnerová

Vedoucí bakalářské práce: prof. Ing. Petr Doucek, CSc.

Praha, leden 2019

Prohlášení

Prohlašuji, že jsem bakalářskou práci Vybrané aspekty zákona o kybernetické bezpečnosti vypracovala samostatně za použití v práci uvedených pramenů a literatury.

V Praze dne 11. prosince 2018

.....

Eliška Kühnerová

Poděkování

Mé poděkování patří především vedoucímu práce panu prof. Ing. Petru Douckovi, CSc. za ochotu, trpělivost, odborné vedení, rady poskytnuté při zpracování této práce a veškerý čas mi věnovaný. Také děkuji osobám z praxe za poskytnuté informace, konzultace a praktické poznatky.

Abstrakt

Bakalářská práce se zaměřuje na zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB) včetně navazujících a souvisejících předpisů, vyhlášek a nařízení. Cílem práce je rozbor, analýza ZKB a seznámit čtenáře s výsledky této analýzy. Dále se práce zaměřuje na kritickou infrastrukturu a proces určení kritické informační infrastruktury. V závěru práce autorka provedla analýzu implementace vybraných požadavků ZKB v telekomunikační společnosti.

Přínosem práce je získání přehledu o aktuálním znění ZKB a souvisejících předpisů, vývoji kybernetické bezpečnosti na území České republiky a představení postupu určování kritické informační infrastruktury, získání přehledu o vykonané práci zaměstnanců telekomunikační společnosti v bezpečnostních rolích, zmapování praktického splnění povinností a představení implementačních postupů pro vybrané povinnosti vyplývající ze zákona.

Klíčová slova

kybernetická bezpečnost, zákon o kybernetické bezpečnosti, vyhláška o kybernetické bezpečnosti, kritická infrastruktura, bezpečnostní opatření.

Abstract

The bachelor thesis focuses on Law No. 181/2014 Coll. on Cyber Security (hereinafter the “CSA”) entered into force together with implementing regulations. The aim of the thesis is to analyze the CSA and to inform the reader about the results of this analysis. Furthermore, the thesis focuses on critical infrastructure and the process of identifying critical information infrastructure. At the end of the thesis the author made an analysis of the implementation of selected CSA requirements in the telecommunication company.

The acquisition of the thesis is to get an overview of the current version of the CSA and related regulations, to present a procedure for determining the critical information infrastructure, to get an overview of the work performed by the employees of the telecommunication company in security roles, to map the practical fulfillment of the obligations and to introduce the implementation procedures for selected cybersecurity obligations.

Keywords

Cybersecurity, Law No. 181/2014 Coll. on Cyber Security, Cyber Security Regulation, Critical infrastructure, Security measures.

Obsah

Úvod	7
1.1 Úvodní slovo	7
1.2 Vymezení cíle a postupu	7
1.3 Používané zkratky	8
1.4 Důležité pojmy	10
2 Rešerše	12
2.1 Rešerše uskutečněných vysokoškolských prací	12
2.2 Rešerše publikací věnující se ZKB	14
3 Kybernetická bezpečnost	15
3.1 Definice kybernetické bezpečnosti	15
3.2 Vývoj kybernetické bezpečnosti na území ČR	17
4 Rozbor ZKB a jeho dopadů	20
4.1 Důvod vzniku ZKB	20
4.2 Vývoj ZKB	21
4.3 Účel zákona	23
4.4 Povinné subjekty dle ZKB	24
4.5 Povinnosti správců systémů KII vyplývající ze ZKB	26
4.6 Dohledová pracoviště	28
4.7 Přestupky a pokuty s nimi spojené	29
4.8 Prováděcí předpisy	31
5 Kritická infrastruktura	33
5.1 Krizový zákon	34
6 ZKB v praxi	36
6.1 Uvedení do kontextu společnosti	36
6.2 Proces určování KII	37
6.3 Postup hodnocení dopadů	40
6.4 Implementace vybraných požadavků ZKB	41
6.4.1 Organizační opatření	42
6.4.2 Technická opatření	44
Závěr	45
Seznam literatury	46
Seznam obrázků	50
Seznam tabulek	51

Úvod

1.1 Úvodní slovo

Bezpečnost. Slovo, pod kterým si jistě každý něco představí, ať už ve spojitosti s vlastní bezpečností či bezpečností svého majetku. Ale co kybernetická bezpečnost? Pravidelně se setkávám s tím, že lidé netuší, jak kybernetický svět může být nebezpečný a co skrývá za hrozby. Role Internetu a počítačů je pro dnešní společnost velmi zásadní, Internet není pouze zdrojem zábavy, ale obrovským zdrojem informací, prostředkem komunikace i obchodu. Sdílení útržků z osobního života na sociálních sítích se stalo fenoménem, ale málo kdo si uvědomuje, jak i jen pouhá fotka může být v rukách útočníka nebezpečná či jak cenná naše osobní data vůbec jsou. Na trh se dostává čím dál více „chytrých“ zařízení, které slibují úsporu času a ulehčení práce. Samozřejmě je rozhodně pohodlnější například ráno naskládat špinavé oblečení do pračky, cestou z práce přes aplikaci praní zapnout, dorazit domů a mít prádlo čisté, nicméně kolik uživatelů zajímá, zda tento přístup není nějakým způsobem zranitelný? Nežijeme již pouze v reálném světě, ale i v tom kybernetickém, a vyhnout se jeho nástrahám a rizikům je zcela nemožné. Co ale možné je, je naučit se rizikům předcházet a naučit se s nimi pracovat.

Kybernetická bezpečnost je obor budoucnosti, neustále se vyvíjí a je potřeba se pořád učit něčemu novému, objevovat nové informace a vzdělávat se. V dnešním světě je potřeba náležitá osvěta a edukovat nejen mladé generace, uvést je do problému a učit, jak hrozbám předcházet a jak se bránit. Zákon o kybernetické bezpečnosti je pomyslným stavebním kamenem a každý, kdo se pohybuje v této oblasti, by ho měl znát, po odborníky až po laiky. Pravdou však je, že ne všichni ví, co je obsahem zákona či co přijetí zákona znamenalo v praxi pro organizace. Vzhledem k obsáhlosti tématu byly v práci vybrány pouze některé aspekty ZKB.

1.2 Vymezení cíle a postupu

Cílem práce je rozbor a analýza ZKB se zaměřením na kritickou infrastrukturu a seznámit čtenáře s výsledky této analýzy. Dalším cílem je analyzovat průběh implementace požadavků ZKB v telekomunikační společnosti a méně technickou formou sestavit přehled problematiky zavádění ZKB v praxi, popsat aplikaci identifikovaných povinností vycházející z legislativy, zejména provádění organizačních a technických bezpečnostních opatření. Přínosem práce je získání přehledu o vykonané práci zaměstnanců telekomunikační společnosti v bezpečnostních rolích, zmapování praktického splnění povinností a představení implementačních postupů pro vybrané povinnosti vyplývající ze zákona. Základní použitou metodou je rešerše literatury, již zveřejněných průzkumů, důvodových zpráv a jiných relevantních zdrojů a následná syntéza. Bude zkoumán důvod vzniku a vývoj zákona, následně analyzovány vybrané části zákona, na jejichž základě dojde ve spolupráci s telekomunikační společností k popsání implementace vybraných požadavků ZKB v praxi.

1.3 Používané zkratky

V následujících řádcích jsou vysvětleny zkratky, které byly v práci použity:

Tabulka 1: Přehled použitých zkratek

Zkratka	Popis
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
ČR	Česká republika
ENISA	Agentura Evropské unie pro bezpečnost sítí a informací
EU	Evropská unie
ICT	Informační a komunikační technologie
IS	Informační systém
ISO	International Organization for Standardization – mezinárodní organizace pro standardizaci
KB	Kybernetická bezpečnost
KI	Kritická infrastruktura (dle krizového zákona)
KII	Kritická informační infrastruktura (dle zákona o kybernetické bezpečnosti)
MKRPKB	Meziresortní koordinační rada pro oblast kybernetické bezpečnosti
MV	Ministerstvo vnitra
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
NSIB	Národní strategie informační bezpečnosti České republiky
NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
OECD	Organizace pro ekonomickou spolupráci a rozvoj
RKB	Rada pro kybernetickou bezpečnost
Sb.	Sbírka zákonů České republiky
VIS	Významný informační systém

V tabulce níže jsou uvedeny zkratky jednotlivých legislativních dokumentů:

Tabulka 2: Přehled legislativních dokumentů

Legislativní dokument	Zkratka
Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury	-
Prováděcí nařízení komise (EU) 2018/151	-
Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii	Směrnice NIS
Ústavní zákon č. 1/1993 Sb., Ústava České republiky	-
Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)	VKB
Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích	VVIS
Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby	-
Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících zákonů (zákon o kybernetické bezpečnosti)	ZKB
Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)	krizový zákon

V této práci byly veškeré legislativní dokumenty citovány v aktuálním znění a to k 26.4. 2018.

1.4 Důležité pojmy

V této podkapitole jsou stručně vymezeny důležité pojmy zmíněné v ZKB [1]. Vymezení pojmů lze nalézt v § 2 zákona, pokud není uvedeno jinak.

Kybernetický prostor- „digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací“, [2]

Kritická informační infrastruktura (KII)- „prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy¹ v oblasti kybernetické bezpečnosti“, [2] (detailnější vysvětlení viz. Kapitola Kritická infrastruktura)

Významný informační systém (VIS)- „informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci“,

Správce informačního systému- „orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního systému“,

Bezpečnostní opatření – dle § 4 ZKB „souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru“ [2]

Základní služba (ZS)- služba, jejíž poskytování závisí na sítích či informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení činností v jednom z následujících odvětví:

- a) energetika,
- b) doprava,
- c) bankovníctví,
- d) infrastruktura finančních trhů,
- e) zdravotnictví,
- f) vodní hospodářství,
- g) digitální infrastruktura,
- h) chemický průmysl²

Informační systém ZS- „systém, na jehož fungování závisí poskytování základní služby a provozovatelem služby je orgán či osoba odpovědná za poskytování základní služby a určená NBÚ“

Provozovatele ZS- „orgán nebo osoba, která poskytuje základní službu a která je určena Národním úřadem pro kybernetickou a informační bezpečnost (NÚKIB)“

² Chemický průmysl nebyl ve směrnici NIS definovaný, tato oblast byla přidána pro specifické potřeby ČR.

Kybernetická bezpečnostní událost – dle § 7 ZKB „událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací“,

Kybernetický bezpečnostní incident – dle § 7 ZKB „narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události“,

Stav kybernetického nebezpečí – dle § 21 ZKB „stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací“.

2 Rešerše

Před započítím práce jako takové autorka provedla rešerši již zveřejněných a uskutečněných vysokoškolských prací ke zjištění, jakým způsobem bylo v minulosti zpracováno téma kybernetické bezpečnosti, zákona jako takového a kritické infrastruktury. Pro vyhledání relevantních zdrojů byl využit portál theses.cz, který slouží jako národní registr závěrečných prací. Systém je vyvíjen a provozován Masarykovou univerzitou v Brně. Dále také databáze kvalifikačních prací Vysoké školy ekonomické v Praze vskp.vse.cz.

Dle průzkumu dostupných zdrojů není Zákon o kybernetické bezpečnosti tématem ojedinělým, nicméně vzhledem k jeho aktuálnosti se nevyskytuje tak často, jak by se dalo předpokládat. Zákon a jeho implementace je námětem především diplomových prací, bakalářských prací bylo nalezeno minimum. Bakalářská práce, která by se věnovala procesu implementace požadavků ZKB, nebyla nalezena žádná.

Autoři se často věnovali dopadům ZKB ve veřejné správě, zavádění ISMS³ v konkrétním podniku či implementací požadavků ZKB vázané normami ISO/IEC 27000. Níže uvádím některé vybrané práce a jejich zaměření.

2.1 Rešerše uskutečněných vysokoškolských prací

Michal Gerža ve své práci, které nese název *Návrh implementace bezpečnostní politiky [3] v informačním systému veřejné správy*⁴ zmapoval využití a provázanost informačních technologií v oblasti veřejné správy. Značná část práce se věnuje projektům e-governmentu. V praktické části se zaměřuje na implementaci bezpečnostní politiky na městském úřadě, informační strategii, informační koncepcí, bezpečnostní politikou. Zákonu o kybernetické bezpečnosti se věnuje spíše okrajově.

V diplomové práci *Zákon o kybernetické bezpečnosti a jeho dopady na povinné subjekty [4]* se autor věnoval nejprve obecně ZKB, provedl jeho rozbor a uvedl čtenáře do problematiky KB. Následně se věnoval dopadům ZKB na krajských úřadech ČR, kde provedl dotazníkové šetření. V průzkumu se dotazoval na názory pracovníků na tuto legislativu, ochotu využití finančních prostředků z fondů IROP či outsourcingu KB. Z průzkumu pak lze usoudit, že pro krajské úřady ZKB znamená vysokou administrativní, finanční i personální zátěž.

Podobnému tématu se věnoval i Roman Smetana [5], který ve své práci popisoval postupy spojené s řízením bezpečnosti a popisoval dopady implementace ZKB ve veřejné správě. Dále autor hodnotil aktuální stav a vývoj informační bezpečnosti na úrovni ČR.

3 Z anglického Integrated Security Management System (integrovaný systém řízení bezpečnosti)

Jan Píša [6] ve své práci představil principy KB vycházející z norem řady ISO 27000 a následně podrobně analyzoval a provedl rozbor ZKB. V druhé části práce analyzoval bezpečnost v konkrétním úřadu (kvůli zachování anonymity nebylo uvedeno o jaký úřad se jedná). Zaměřil se především na bezpečnost síťové infrastruktury a fyzickou bezpečnost objektu jako takového.

Stejně tak se normám z rodiny ISO 27000 věnoval i Tomáš Stránský [7]. Ten se ve své diplomové práci zabýval analýzou rizik informační bezpečnosti, popisem norem ISO 27000 a v druhé části své poznatky aplikoval v konkrétním podniku v souladu s ISO/IEC 27000 a navrhoval doporučení, která by mohla pomoci zmírnit bezpečnostní rizika.

Práce *Kybernetická bezpečnost a legislativa ČR* [8] se zaměřuje především obecně na kybernetickou kriminalitu, následně autor provedl analýzu legislativy ČR týkající se KB a věnoval se věcnému návrhu ZKB.

V diplomové práci nesoucí název *Kybernetická bezpečnost z pohledu podnikové informatiky* [9] se autor zaměřil na problematiku KB podnikatelských subjektů. V práci byly identifikovány hrozby, pro které následně stanovil kategorie podnikatelských subjektů, které by mohly být danou hrozbou dotčeny. Na základě toho byla vytvořena metodická pomůcka k testování KB. Tato práce zákon jako takový neřeší, ale zabývá se spíše útoky na subjekty, ale praktická část se věnuje doporučení bezpečnostních opatření a aplikaci ZKB. Práce je z roku 2016, tedy opět již některé části nejsou aktuální.

Z rešerše uskutečněných vysokoškolských prací vyšlo, že podobnou formou žádná práce nebyla zpracována a ZKB se autoři věnují spíše okrajově a žádný ze zkoumaných subjektů nebyl z privátního sektoru.

2.2 Rešerše publikací věnující se ZKB

Většina dostupných publikací se věnuje ZKB spíše okrajově, častým námětem knih bývá kybernetická kriminalita, bezpečnost v kyberprostoru či je tématem kybernetická bezpečnost obecně. Velké množství knih je vydáno před rokem 2015, nelze je tedy považovat jako aktuální vzhledem k rychlosti vývoje KB.

Výhradně ZKB a prováděcím předpisům se věnuje kniha *Zákon o kybernetické bezpečnosti: komentář* [10]. Na úvod čtenáře seznamuje s důvodem vzniku zákona, zbytek knihy se věnuje jednotlivým hlavám zákona, kde autoři jednotlivé paragrafy následně rozebírají, popisují a vysvětlují. Kniha byla vydána 15.5. 2015 a popisuje zákon k 30. 4. 2015, tedy obsah již není zcela aktuální.

V knize *Kybernetická bezpečnost: teorie a praxe* [11] autoři shrnují výsledky projektu „Aktuální kybernetické hrozby v České republice a jejich eliminace“. Autoři analyzují český právní řád před přijetím ZKB, následně jaké dopady vyplývají z přijetí. Dále porovnávají první předpisy ČR s vybranými členskými státy Evropské unie. Velká část publikace je stejně jako v předchozím případě věnována kybernetické kriminalitě a KII. Posledním tématem je popularizace KB, jak je důležité vzdělávat od dětí až po seniory a samotnou otázkou „jak“ takové vzdělání realizovat. Ačkoliv některá témata jsou rozebrána dopodrobna, je publikace vhodná i pro neodbornou veřejnost, po každé kapitole následuje shrnutí a dílčí závěr, kde je vysvětlen smysl kapitoly, což poskytuje větší přehlednost a porozumění.

V publikaci *Vybrané aspekty kybernetické bezpečnosti* [12] z roku 2015 se autoři zpočátku zabývají rozdílem a porovnáním kybernetické a informační bezpečnosti, hodnotí, jaký je stav bezpečnosti v České republice a jaké potenciální hrozby mohou nastat. Další část publikace je věnována kritické infrastruktuře a snaží se popsat možné útoky na ni a vysvětlují pohled útočníka a jeho postupy.

Kniha *CyberCrime* [13] se okrajově dotýká ZKB. Knihu napsal pedagog, právník a odborník na kybernetickou bezpečnost v jedné osobě a toto spojení odráží i kniha. Autor se v publikaci zaměřuje především na kyberkriminalitu, zmiňuje i ZKB, nicméně již v úvodu autor vysvětluje, jak je důležité oddělit kybernetickou kriminalitu a bezpečnost oddělit. Kniha je rozdělena do 7 kapitol: *Pojem kybernetické trestné činnosti a pojmy související, Působnost práva v kyberprostoru, Anonymita uživatele, Projevy kyberkriminality, Trestněprávní ochrana před kyberkriminalitou, Trestněprocesní a kriminalistické aspekty odhalování, prověřování a vyšetřování kyberkriminality a Náměty de lege ferenda*. Kniha obsahuje i několik reálných příkladů z praxe a vše je vysvětlováno jednoduchou formou.

Z rešerše je patrné, že k aktuální legislativě není žádná literatura, žádná publikace, která by poskytla rady při zavádění ZKB, popisovala aktuální povinnosti, poskytla podporu při implementaci a ucelený přehled o zákoně.

3 Kybernetická bezpečnost

Jak již bylo naznačeno v úvodu, v současném světě stále roste používání informačních technologií, což vede k urychlení komunikace, zlepšování služeb a tím i k celkovému rozvoji společnosti. Závislost společnosti na informačních technologiích se stále rapidně zvyšuje a málokdo si dokáže bez nich představit pouhý den. Dle studie nákladů na kyberkriminalitu nesoucí název „*Cost of Cyber Crime Study*“ [14] vydána společností Accenture, která zkoumala, kolik stály firmy reakce na kyber útoky, se zvýšily tyto náklady minulý rok o 23 procent.⁵ Obecně můžeme říci, že stejně jako se vyvíjí informační a komunikační technologie a pronikají do společnosti, úměrně k tomu dochází i k rozvoji potenciálních hrozeb, zvyšuje se riziko zneužití těchto technologií, počet i intenzita útoků. Hrozby jsou stále sofistikovanější a není možné se před nimi schovat.

3.1 Definice kybernetické bezpečnosti

Jak již píše autoři *Výkladového slovníku kybernetické bezpečnosti* [15], přesně definovat pojmy v oblasti IT je poměrně nesnadný úkol, jelikož se tento obor stále rozvíjí a vzniká tak duplicitní pojmenování tentýž jevů, a to nejen v jazyce českém, ale i v kmenovém jazyce oboru – angličtině. Ačkoliv je český jazyk poměrně rozmanitý, v případě pojmu „bezpečnost“ je poněkud „nedostačující“ oproti jiným jazykům. Například ve zmíněné angličtině můžeme bezpečnost přeložit jako „security“, ve smyslu zabezpečení pomocí nějaké činnosti člověka nebo systému, nebo jako „safety“, což vyjadřuje především vlastnost nějaké věci.

Před definováním samotné bezpečnosti je důležité si definovat pojmy hrozba a riziko a jak spolu tyto pojmy souvisí.

Hrozba „je libovolný subjekt, jenž svým působením (činností) může poškodit nebo zničit konkrétní chráněnou hodnotu nebo zájem jiného subjektu (tzv. hrozba intencionální) jev či událost jako bezprostřední příčina poškození nebo zničení konkrétní chráněné hodnoty nebo zájmu (tj. tzv. hrozba neintencionální).“ [16]

Riziko „představuje možnost vzniku události s výsledkem odchylným od předpokládaného cíle, a to s určitou objektivní matematickou nadějí či statistickou pravděpodobností. Je to tedy kvantifikovaná nejistota. Hovoří o míře (váze) hrozby.“ [16]

Zjednodušeně lze říci, že rizikem je to, „co stát podstupuje“, aby nebyla překročena únosná míra při snaze redukovat hrozby. Pro stanovení míry rizika je tedy důležité si prvně analyzovat a kvantifikovat hrozbu z hlediska možných dopadů na chráněný zájem.

⁵ Výzkum proběhl na základě dat z 254 společností v 7 zemích: Spojených státech, Spojených státech, Velké Británii, Německu, Francii, Itálii, Austrálii a Japonsku.

Kybernetická bezpečnost je pak podmnožinou samotné bezpečnosti. Ani v tomto případě neexistuje jednotná obecně známá definice a ani odborníci z praxe s nemohou na přesné definici shodnout. Dle Ing. Petra Hrůzy, Phd. [17] je KB „*souhrn právních, organizačních, technických a fyzických opatření, která umožňují odolávat úmyslně i neúmyslně vyvolaným kybernetickým útokům a zmírňovat či napravovat jejich následky*“. Z pohledu České republiky dle Lucie Kadlecové, M.A [18] je KB chápána jako aktivita státu chránící KII a další informační a komunikační systémy pomocí bezpečnostních opatření zahrnující především preventivní opatření a opatření reaktivního charakteru vůči napadeným subjektům v případě kybernetických incidentů.

Dle průzkumu od PwC CyberSecurity Teamu⁶ lidé vnímají kyberbezpečnost pouze jako technický aspekt spojený s prevencí, a tedy pouze jako záležitost ICT oddělení. Pouze malá část vnímala KB i z jiného než technického pohledu, například v souvislosti s ochranou osobních údajů. Z průzkumu také vyšlo, že pouze 58 % dotázaných firem proškoluje veškeré své zaměstnance, 72 % neškoli žádný management a 3 % dokonce v rámci KB neškoli vůbec. V jiném průzkumu⁷, tentokrát od společnosti Kaspersky ve spolupráci s B2B International, vyplynulo, že za 46 % kybernetických incidentů může chyba zaměstnance a v 28 % se jednalo o únik dat zákazníků či zaměstnanců. Všechna tato čísla jsou poněkud alarmující. Zaměstnancům, jakožto nejjednodušším a nejzranitelnějším terčům, by měla být přisuzována větší váha a společnosti by měly investovat do vzdělání v oblasti KB napříč firmou. Povědomí o KB je, nicméně poměrně malé procento lidí ji vidí jako prioritu. Nejde však pouze o firmy a její zaměstnance, je potřeba toto povědomí šířit na širokou veřejnost, především pak na děti, které se stávají uživateli Internetu čím dál v mladším věku a rodiče často nemají o jejich aktivitách přehled, ačkoliv právě oni by měli jít svým dětem příkladem a informovat je o možných hrozbách. Často se ale sává, že nevědomost pramení již u rodičů a děti jsou v této oblasti „zběhlejší“. Vedle rodičů by tak měla hrát roli škola, kde by se učili správným návykům a základům kyberbezpečnosti, bohužel prozatím ani toto spojení není natolik funkční, jak by bylo potřeba. V ČR existuje několik projektů a organizací, které se snaží šířit osvětu nejen mezi dospělými, ale převážně dětmi. Dá se tedy očekávat, že v příštích letech bude povědomí o KB mnohem vyšší a že již větší procento lidí bude schopno KB správně definovat.

⁶ Průzkum „*Kyberbezpečnost a my*“, PricewaterhouseCoopers Audit, s.r.o., TATE International, s.r.o. z roku 2017

⁷ Průzkum „*The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within*“, Kaspersky Lab and B2B International, 2017

3.2 Vývoj kybernetické bezpečnosti na území ČR

V minulém desetiletí byla v České republice národní kybernetická bezpečnost řešena především na základě vládních koncepčních dokumentů a iniciativ soukromého a akademického sektoru. V roce 2000 byla vydána ministerstvem vnitra *Koncepce boje proti organizovanému zločinu*⁸. Koncepce formulovala úkoly a opatření určená k boji proti organizovanému zločinu a jejím cílem bylo předcházet, potlačovat a odhalovat organizované zločiny především na území ČR. [19]

Následující rok byla ministrem vnitra přijata *Koncepce boje proti trestné činnosti v oblasti informačních technologií*, která byla v souladu s výše zmíněnou koncepcí. Koncepce boje proti trestné činnosti v oblasti informačních technologií může být považována jako první podstatnější dokument, který má za snahu zajištění kybernetické bezpečnosti. V jejím Harmonogramu opatření popisuje úkoly rozdělené do 5 oblastí – legislativní; organizační; oblast vzdělávání, výzkumu a mediálního působení; oblast mezinárodní spolupráce a oblast koordinační a kontrolní. [20]

24. března 2004 byla přijata *Státní informační a komunikační politika e-Česko 2006* [21]. Cílem tohoto dokumentu bylo formulovat cíle a novou strategii státu v oblasti telekomunikací a definovat principy a zásady, které se budou uplatňovat při dalším rozvoji informační společnosti. Cíle musely být nastaveny tak, aby splňovaly evropské priority, jelikož vznik *Státní informační a komunikační politiky* úzce souvisel se vstupem ČR do Evropské Unie (dále EU), ale zároveň zohledňovaly specifické potřeby ČR. Dle těchto potřeb pak byly stanoveny prioritní oblasti ČR seřazené podle důležitosti: dostupné a bezpečné komunikační služby, informační vzdělanost, moderní veřejné služby on-line a dynamické prostředí pro elektronické podnikání.

Dalším důležitým dokumentem byla *Národní strategie informační bezpečnosti České republiky* (NSIB) z roku 2005. Ta dělí své strategické cíle do 6 oblastí [22]:

- a) řízení informační bezpečnosti a řízení rizik,
- b) znalosti o informační bezpečnosti,
- c) národní a mezinárodní spolupráce v oblasti informační bezpečnosti,
- d) používání nejlepších praxe v oblasti informační bezpečnosti,
- e) ochrana lidských práv a svobod,
- f) konkurenceschopnost české ekonomiky.

⁸ Usnesení vlády České republiky ze dne 23. října 2000 č. 1044 k Aktualizované Koncepci boje proti organizovanému zločinu

Každá z oblastí obsahuje jeden strategický cíl a současně opatření, která pomohou jednotlivý cíl dosáhnout. Prvním z cílů bylo zlepšení řízení informační bezpečnosti a řízení rizik, a to pomocí zavedení nejlepší praxe (tzv. best practice) do systémů řízení informační bezpečnosti, soustavného monitorování hrozeb, ochrany kritické informační infrastruktury (KII) státu. Dalším z cílů byl „rozvoj znalostí o informační bezpečnosti“, tedy plošné zvyšování povědomí bezpečnosti a bezpečnostních rizicích, ale i o možnostech obrany, a to pomocí školicích a vzdělávacích programů.

Aby bylo možné uchránit se před potenciálními hrozbami a zabezpečit své systémy a počítačové sítě, je potřeba, aby Česká republika spolupracovala nejen na národní úrovni, ale také v mezinárodním měřítku. Je tedy zřejmé, že podpora národní a mezinárodní spolupráce v oblasti informační bezpečnosti je dalším důležitým cílem. ČR je součástí několika programů v rámci EU a Organizace pro ekonomickou spolupráci a rozvoj (OECD). Zájmem bylo tuto spolupráci i nadále prohlubovat. Následuje podpora používání nejlepší praxe v oblasti informační bezpečnosti, a to pomocí výměny zkušeností, podpory spolupráce veřejné správy s národní normalizační organizací při vydávání norem a zvyšování uživatelské přívětivosti systémů. Informace o zákaznících, know how, obchodní tajemství, soukromé informace a mnohé další je potřeba chránit. Podpora ochrany lidských práv a svobod je předposledním cílem NSIB. Opatření vztahující se k tomuto cíli je zajistit legislativní ochranu základních lidských práv a svobod a vytvořit provozní prostředí, které by zajišťovalo informační bezpečnost a ochranu soukromí. Posledním cílem NSIB byla „podpora konkurenceschopnosti české ekonomiky“ na základě podpory dostupnosti a použitelnosti informací, monitorování a vyhodnocování legislativy a nejlepší praxe a odstraňování bariér. Na NSIB poté navazuje *Akční plán realizace opatření Národní strategie informační bezpečnosti České republiky* definující konkrétní úkoly, které měly směřovat k zajištění informační bezpečnosti v České republice [23].

Dalším důležitým milníkem v historii kyberbezpečnosti byl rok 2010, přesněji 15. března, kdy vláda České republiky přijala *usnesení č. 205 o řešení problematiky kybernetické bezpečnosti České republiky* [24]. Ve zmíněném usnesení je stanoveno Ministerstvo vnitra jakožto gestor problematiky KB a zároveň národní autoritou pro tuto oblast. Úkolem Ministerstva vnitra bylo dle usnesení „koordinovat činnost ostatních státních institucí v oblasti zajišťování kybernetické bezpečnosti a zahájit zajišťování provozu vládního pracoviště CSIRT (Computer Security Incident Response Team)“. V tomtéž roce vznikla Meziresortní koordinační rada pro oblast kybernetické bezpečnosti (MKRPKB) jakožto podpora výkonu gesční a koordinační role Ministerstva vnitra. MKRPKB byly uděleny úkoly jako koordinace činnosti státních institucí v oblasti KB, řešení aktuálních otázek týkajících se KB, shromažďování, analyzování a vyhodnocování údaje o stavu zajištění KB poskytované členy koordinační rady, ... MKRPKB zaniká ke konci roku 2011 po přechodu gesce nad oblastí KB na Národní bezpečnostní úřad (NBÚ).

NBÚ, který se stal autoritou pro oblast KB, bylo vládou usnesením č. 781 z 19. října 2011 uloženo zajistit vznik Národního centra kybernetické bezpečnosti a vládní koordinační místo pro okamžitou reakci na počítačové incidenty (neboli tzv. vládní CERT) a také do 31. března 2012 vládě předložit návrh zákona o kybernetické bezpečnosti ve spolupráci s ministry vnitra a obrany a ředitelem Bezpečnostní informační služby. Nově pak namísto MKRPKB vznikla Rada pro kybernetickou bezpečnost.

Členy rady byli zástupci příslušných státních institucí, kterými jsou Ministerstvo vnitra, Ministerstvo obrany, Ministerstvo zahraničních věcí, Ministerstvo financí, Ministerstvo průmyslu a obchodu, Ministerstvo dopravy, Policie České republiky, Úřad pro zahraniční styky a informace, Bezpečnostní informační služba, Vojenské zpravodajství, Úřad pro ochranu osobních údajů a Český telekomunikační úřad [25].

Dalším důležitým momentem, ačkoliv ne již tak vzdáleným od současnosti, byl vznik Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), který je aktuálně ústředním správním orgánem pro KB včetně ochrany utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. (nukib.cz). Hlavními úkoly úřadu jsou provoz Vládního CERT České republiky (GovCERT.CZ), spolupráce s ostatními národními a také mezinárodními CERT® a CSIRT týmy, příprava bezpečnostních standardů pro informační systémy KII a VIS, osvěta a podpora vzdělávání v oblasti kybernetické bezpečnosti, výzkum a vývoj v oblasti KB, ochrana utajovaných informací v oblasti informačních komunikačních systémů a kryptografická ochrana. Úřad sídlí v Brně a vznikl 1. srpna 2017 [26].

4 Rozbor ZKB a jeho dopadů

Tato kapitola uvádí čtenáře do kontextu ZKB. Cílem je analyzovat důvod vzniku, jak se vyvíjel v čase a provést rozbor zákona jako takového.

4.1 Důvod vzniku ZKB

Jak již bylo zmíněno v kapitole č. 3, závislost společnosti na informačních technologiích stále roste. Na informačních technologiích závisí informační systémy, které napomáhají až už například řízení dopravy či například výkonu veřejné moci. Závislost státu, obyvatel i celé ekonomiky na IT stále roste a stále se zvyšuje propojení služeb a systémů. Na druhé straně se však zvyšuje i riziko zneužití těchto systémů. Kybernetická kriminalita se stále rozvíjí, počty útoků rostou a tyto útoky mohou způsobit jak značné ekonomické problémy, tak i v případě útoku na prvky kritické infrastruktury mohou ohrozit chod samotného státu.

Jak vyplývá z průzkumu firmy S&T [27], před existencí ZKB byl stav ve většině českých společností poněkud tristní. Dle průzkumu minimálně tři čtvrtiny českých firem neměly žádný krizový plán, který by udržel společnost v případě nouze, dokumentovaný a testem prověřený nouzový scénář mělo méně než 5 % firem a více než 85 % uživatelů používá totožné heslo do rozdílných aplikací. Většina manažerů žila v iluzi, že zrovna jejich firmu nemůže nějaký kybernetický útok či únik dat postihnout. Až poté, co je firma dotčena nějakým incidentem, začne se bezpečnostní politikou zabývat.

V důvodové zprávě [28] je poukázáno na DDoS útoky z března 2014 na finanční organizace, zpravodajské servery a jiné subjekty, kdy tyto subjekty společně nesdílely žádné informace a nebylo možné přijmout nějaké ochranné opatření. Jednotná regulace, institucionální dohled a koordinace informací byla tedy žádoucí a jak se píše v Ústavě ČR, soukromým osobám je možné uložit povinnosti pouze prostřednictvím zákona, což dalo za vznik ZKB. Tato právní úprava měla za cíl stanovit základní úroveň bezpečnostních opatření, vylepšit detekci a zavést hlášení kybernetických bezpečnostních incidentů a upravit činnost dohledových pracovišť.

4.2 Vývoj ZKB

Tato podkapitola volně navazuje na podkapitolu 3.2. Bude věnována vývoji ZKB jako takového.

3. února 2012 byl návrh věcného záměru ZKB byl poslán do meziresortního připomínkového řízení, veřejnost mohla po celý měsíc vyjádřit své případné připomínky. 30. května byl předložený věcný záměr zákona vládou schválen [29]. 28. června 2013 byl návrh zákona zaslán vládě České republiky k projednání a 2. ledna 2014 se stal schváleným a předložen k dalšímu legislativnímu projednávání [30]. Dne 13. srpna 2014 byl ZKB prezidentem Milošem Zemanem podepsán a účinnosti nabyl k 1. lednu 2015. Před nabytím účinnosti musely být vypracovány tzv. prováděcí předpisy, vznikly tak 3 předpisy [31]:

- Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti);
- Vyhláška, stanovující významné informační systémy a jejich určující kritéria;
- Novela nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

Dne 9. 5. 2017 byla Poslaneckou sněmovnou po svém schválení ve 3. čtení postoupena do Senátu novela ZKB, která probíhala současně ve dvou „částích“. První probíhala v souvislosti s transpozicí Směrnice evropského parlamentu a Rady EU 2016/1148 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (směrnice NIS) [32] ze dne 6. července 2016. Jakožto členský stát EU jsme měli povinnost transponovat tuto směrnici do českého právního řádu. ČR musela přijmout úpravu do 21 měsíců od vstupu směrnice NIS v platnost, tedy nejpozději do května 2018. Na jaře 2016 byla svolána pracovní skupina složená z odborníků na úrovni resortů, následně z řad odborné veřejnosti. 23. listopadu 2017 byla směrnice schválena vládou. Novela nepřinesla zásadní změnu ZKB či jeho principů, nýbrž zvýšila rozsah zajištění KB. Nejdůležitějšími změnami zmíněnými v jednom z podpůrných materiálů NBÚ [33] bylo zavedení nových institutů – základní a digitální služby, s tím souvisí i zavedení nových povinných orgánů a osob⁹- poskytovatel digitální služby, provozovatel základní služby a správce a provozovatel informačního systému základní služby. Dále nová zákonná úprava v rámci uzavírání smluv mezi orgány veřejné moci a poskytovateli cloud computingu, smlouvy nově musí nově například stanovit úroveň poskytovaných služeb, určit vlastníka uchovávaných dat, zavést pravidla zákaznického auditu či nastavit podmínky o ukončení smluvního vztahu (z pohledu bezpečnosti).

⁹ Povinné orgány budou popsány v kapitole 4.4

Novela obsahuje i novou informační povinnost mezi povinnými orgány a osobami, kdy například správce KII musí informovat provozovatele KII, že se stává provozovatelem KII, a že se na něj ZKB vztahuje. Rozšířily se povinnosti při kybernetických bezpečnostních událostech a incidentech, úprava poskytování informací v rámci oblasti KB veřejnosti, rozšíření povinnosti provádět opatření dle ZKB i na nově zaveden subjekty, rozšíření pravomocí národního i vládního CERT, zřízení Národního úřadu pro kybernetickou a informační bezpečnost (NÚKIB), určení práv a povinností tohoto úřadu a nová úprava přestupků a sankcí. Díky novelizaci se stal ZKB přehlednější

4.3 Účel zákona

Účelem zákona je upravit práva a povinnosti osob a orgánů veřejné moci v oblasti KB, sjednotit pravidla a postupy při kyberbezpečnostních incidentech, přispět ke zlepšení jejich detekce a zvýšení ochrany před jejich uskutečněním, což by vedlo k celkovému zvýšení efektivity řešení těchto incidentů, dále stanovit pravidla spolupráce privátního sektoru s veřejnou správou. Primárním účelem zákona tedy není řešit jednotlivé kyberbezpečnostní incidenty, ale vytvořit prostředí, kde budou kritická informační a komunikační infrastruktura preventivně chráněna a žádná kyberbezpečnostní událost nepředstaví žádné bezpečnostní riziko.

Účelem novely zákona bylo „zdokonalit“ původní znění ZKB a naplnit požadavky směrnice NIS, tedy především posílit bezpečnost informačních systémů, rozšíření okruhu povinných subjektů

Mezi cíle, které si kladla právní úprava ZKB, patří:

- a) stanovení základní úroveň bezpečnostních opatření,
- b) zlepšení detekce kybernetických bezpečnostních incidentů,
- c) zavedení hlášení a systému opatření k reakci na kybernetické bezpečnostní incidenty,
- d) upravení činnosti dohledových pracovišť

Zákon je „postaven“ na dvou zásadách a třech pilířích. První ze zásad je minimalizace zásahu do práv soukromoprávních subjektů, druhou zásadou je individuální odpovědnost za bezpečnost vlastních informačních systémů. Pilíře tvoří [1].:

- a) bezpečnostní opatření (standardizace),
- b) hlášení kybernetických bezpečnostních incidentů,
- c) protipatření, tzn. reakce na incidenty.

ZKB se skládá z šesti částí. Část první sestává ze šesti hlav:

Hlava I – Základní ustanovení,

Hlava II – Systém zajištění kybernetické bezpečnosti,

Hlava III – Stav kybernetického nebezpečí,

Hlava IV – Výkon státní správy,

Hlava V – Kontrola, nápravná opatření a přestupky,

Hlava VI – Závěrečná ustanovení.

4.4 Povinné subjekty dle ZKB

Obecně lze říci, že subjekty, jimž jsou zákonem ukládány povinnosti, spravují specifické a informační a komunikační systémy. Zákon definuje 8 typů subjektů uvedené v § 3 písm. a) až h) ZKB [1]:

- a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací¹⁰, pokud není orgánem nebo osobou podle písmene b),
- b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),
- c) správce a provozovatel informačního systému kritické informační infrastruktury,
- d) správce a provozovatel komunikačního systému kritické informační infrastruktury,
- e) správce a provozovatel významného informačního systému,
- f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d),
- g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a
- h) poskytovatel digitální služby.

Směrnice zavedla dva nové druhy povinných subjektů. Prvním z nich jsou provozovatelé základních služeb (definice ZS viz. předchozí kapitola). Lze říci, že ZS je alternativou KII, ačkoliv se částečně rozcházejí, provozovatelé ZS jsou širší. Jsou určovány na základě předem daných kritérií, které rámcově stanovuje směrnice. Druhým novým druhem jsou poskytovatelé digitálních služeb, kteří jsou regulováni zcela nově. Jedná se o internetové jedná se například o online vyhledávače či služby cloud computingu. Povinnosti u těchto poskytovatelů jsou mírnější než u KII i u provozovatelů ZS. Mimo jiné zde působí princip maximální harmonizace, což znamená, že nelze vybočit z úrovně bezpečnosti, kterou ukládá směrnice NIS [32].

V následujících tabulkách je pro přehlednost zobrazen stav před a po novele a k jakému CERT náleží.

Subjekt	CERT
Poskytovatel el. služeb komunikací	Národní CERT
Orgán/ osoba zajišťující významnou síť	
Správce IIS/KII	Vládní CERT
Správce KS/KII	
Správce VIS	

Tabulka 3: Subjekty před novelou ZKB

Subjekt	CERT
Poskytovatel el. služeb komunikací	Národní CERT
Orgán/ osoba zajišťující významnou síť	
Poskytovatel digitálních služeb	
Správce a provozovatel IIS/KII	Vládní CERT
Správce a provozovatel KS/KII	
Správce a provozovatel VIS	
Správce a provozovatel IS základní služby	
Provozovatel základní služby	

Tabulka 4: Subjekty po novele ZKB

4.5 Povinnosti správců systémů KII vyplývající ze ZKB

Pro subjekty vyjmenované v předchozí kapitole ZKB ukládá řadu povinností, které musí začít plnit nejpozději do 1 roku od jejich určení, výjimkou je povinnost nahlásit kontaktní údaje, to musí být provedeno do 30 dnů od jejich posouzení či určení. Další povinností je detekování a hlášení kybernetických bezpečnostních incidentů a provádění vydaných reaktivních a ochranných opatření. V neposlední řadě pak zavést bezpečnostní opatření.

Bezpečnostní opatření jsou základním kamenem zákona a z operačního hlediska je to jedna z nejdůležitějších částí. Bezpečnostní opatření jsou činnosti, které vedou k ochraně před kybernetickými bezpečnostními incidenty a hrozbami. Zákon je v § 4 vymezuje jako „*souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru*“ [1]. Dle Výkladového slovníku [15] pak bezpečnostní opatření znamenají „*ochranná opatření pro zajištění bezpečnostních požadavků kladených na systém. Mohou mít různý charakter (fyzická ochrana zařízení a informace, personální bezpečnost – kontrola pracovníků, organizační opatření – provozní předpisy apod.)*.“ Jak je nastíněno v této definici, bezpečnostní opatření lze rozdělit na dva typy – organizační opatření a technická opatření. Jejich hlavním smyslem je vytvořit preventivní mechanismy umožňující povinným subjektům se autonomně vyrovnat s kybernetickými událostmi.

Mezi organizační opatření patří:

- systém řízení bezpečnosti informací,
- řízení rizik,
- bezpečnostní politika,
- organizační bezpečnost,
- stanovení bezpečnostních požadavků pro dodavatele,
- řízení aktiv,
- bezpečnost lidských zdrojů,
- řízení provozu a komunikací KII nebo VIS,
- řízení přístupu osob ke KII nebo k VIS, akvizici, vývoj a údržba KII a VIS,
- zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
- řízení kontinuity činností,
- kontrolu a audit KII a VIS.

Technická opatření, která musí zavést firmy a organizace spadající pod zákon č. 181/2014 Sb.:

- fyzická bezpečnost,
- nástroj pro ochranu integrity komunikačních sítí,
- nástroj pro ověřování identity uživatelů,
- nástroj pro řízení přístupových oprávnění,
- nástroj pro ochranu před škodlivým kódem,
- nástroj pro zaznamenávání činnosti KII a VIS, jejich uživatelů a administrátorů,
- nástroj pro detekci kybernetických bezpečnostních událostí,
- nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
- aplikační bezpečnost,
- kryptografické prostředky,
- nástroj pro zajišťování úrovně dostupnosti informací,
- bezpečnost průmyslových a řídicích systémů.

4.6 Dohledová pracoviště

Dohled, zda povinné subjekty plní povinnosti stanovené ZKB, provádí 2 dohledová pracoviště– národní a vládní CERT. CERT neboli „Computer Emergency Response Team“ je tým odborníků. Jedná se o registrovanou ochrannou známku Carnegie Mellon University v USA, což znamená, že nelze název CERT používat bez jejího svolení. Dle novely ZKB musejí nově povinné subjekty hlásit bezpečnostní incidenty národnímu či vládnímu CERT.

Národní CERT přijímá oznámení kontaktních údajů, hlášení o kybernetických bezpečnostních incidentech, jež eviduje, uchovává chrání a vyhodnocuje. Poskytovateli digitální služby slouží jako kontaktní místo a poskytuje metodickou podporu. V České republice zaštiťuje národní CERT organizace CZ.NIC.

Další z úkonů je předávání údajů o kybernetických informačních incidentech nahlášených osobami či orgány zajišťující VIS nebo poskytovateli digitálních služeb Národnímu úřadu pro kybernetickou a informační bezpečnost. Tyto údaje předává bez uvedení ohlašovatele (§ 17, odstavec 2, písmeno g), ale za stavu kybernetického nebezpečí či v případě potřeby kontroly na vyžádání úřadu NÚKIB předává i kontaktní údaje.

Dále plní roli CSIRT (z anglického Computer security incident response team, dle Výkladového slovníku [15] skupina pro reakce na počítačové bezpečnostní incidenty složená z odborníků na informační bezpečnost a jejichž úkolem je bezpečnostní incidenty řešit) a spolupracuje s CSIRT dalších členských států, které informuje o případných incidentech, které by mohly mít dopad na kontinuitu poskytování základní či digitální služby v daném státě. Souběžně informuje o svém postupu NÚKIB. Národní CERT tým zaštiťuje organizace CZ.NIC.

Provozovatelem vládního CERT je v České republice GovCERT.CZ. Vládní CERT přijímá oznámení kontaktních údajů a hlášení o kybernetických bezpečnostních incidentech od subjektů zmíněných v kapitole 4.5, kterým poskytuje metodickou podporu a pro něž působí jako kontaktní místo. Dále provádí hodnocení zranitelností v oblasti KB, od národního CERT přijímá údaje, které dále vyhodnocuje¹¹.

Pod vládní CERT se řadí systémy důležité pro chod státu nebo zprostředkující základní služby pro občany a významné informační systémy (systémy státní správy), které by v případě narušení ovlivnili chod daného úřadu. [35]

¹¹ Veškeré činnosti jsou popsány v § 20 a) až n)

4.7 Přestupky a pokuty s nimi spojené

NÚKIB dle ZKB vykonává kontrolu v oblasti KB. Zjišťuje, jak povinné subjekty, které byly popsány v kapitole 4.5, plní své povinnosti a dodržují prováděcí právní předpisy. V případě, že došlo ze strany subjektu k nějakému pochybení, uloží NÚKIB kontrolovanému orgánu či osobě, aby je ve stanovené lhůtě odstranila, případně i určí jakým způsobem (nápravná opatření). V případě, že povinnost dle podle § 13 za stavu kybernetického nebezpečí není splněna či není splněna některá povinnost z nápravného opatření, subjekt může být sankciován.

S nově vzniklými povinnostmi pro provozovatele přišel ZKB i s novými přestupky a pokutami za jejich vykonání. V případě, že NÚKIB rozhodne, že nějaká z povinností nebyla splněna, může provozovateli uložit pokutu až ve výši 1 000 000 Kč, stejně je tomu v případě nepředání či nezničení kopií dat, provozních údajů a informací.

Oproti původnímu znění byla zvýšena pokuta ze 100 000 Kč na 1 000 000 Kč, a to za nezavedení či neprovedení bezpečnostních opatření, nevedení bezpečnostní dokumentace, neohlášení bezpečnostního incidentu, nesplnění povinnosti, kterou uložil NÚKIB dle § 13 či § 14, nebo neohlášení některé z povinností uloženou nápravným opatřením dle § 24.

Pokutu až do výše 200 000 Kč může NÚKIB uložit v případě, že provozovatel neumožní správci dohled nad zničením dat, provozních údajů a informací dle § 6a odst. 3, dále v případě, že provozovatel nepředá data, provozní údaje či informace na vyžádání správce dle § 6a odst. 2.

Nejnižší a jedinou nepozměněnou sankcí oproti znění ZKB před novelou je pokuta za neoznámení kontaktních údajů podle § 16 odst. 2, písm. b), která činí 10 000 Kč.

Pro lepší přehlednost přestupků a pokut k nim náležitým byla vytvořena následující tabulka:

Tabulka 5: Přehled přestupků a náležitých pokut [Zdroj: [1]]

§ 25	Přestupek	Pokuta	Povinný subjekt
odst.1	Neplnění povinností uložených rozhodnutím nebo opatřením obecné povahy při SKB nebo uložených nápravných opatření podle § 24	1 000 000 Kč	Poskytovatel služby a subjekt zajišťující síť el. komunikací, subjekt zajišťující významnou síť
odst. 2 písm. a)	Nezavedení nebo neprovádění bezpečnostních opatření, nevedení bezpečnostní dokumentace	1 000 000 Kč	Správce a provozovatel informačního a komunikačního systému KII, nebo VIS
odst. 2 písm. b)	Neohlášení kybernetického bezpečnostního incidentu	1 000 000 Kč	
odst. 2 písm. c) a d)	Nesplnění povinností uložené rozhodnutím nebo opatřením obecné povahy podle § 13, § 14 nebo rozhodnutím podle § 15a	1 000 000 Kč	
odst. 2 písm. e)	Nepředání dat, provozních údajů a informací podle § 6a odst. 2	200 000 Kč	
odst. 2 písm. f)	Nepředání dat, provozních údajů a informací podle § 6a odst. 3	1 000 000 Kč	
odst. 2 písm. g)	Nezničení kopií dat, provozních údajů a informací podle § 6a odst. 3	200 000 Kč	
odst. 2 písm. h)	Neumožnění dohledu nad průběhem zničení dat, provozních údajů a informací podle § 6a odst. 3	200 000 Kč	
odst. 2 písm. i)	Neoznámení kontaktních údajů nebo jejich změny NÚKIB podle § 16 odst. 2 písm. b)	10 000 Kč	
odst. 2 písm. j)	Nesplnění některé z povinností uložené nápravným opatřením podle § 24.	1 000 000 Kč	

4.8 Prováděcí předpisy

Právní úprava KB v ČR není ani zdaleka tvořena jen ZKB. Povinnosti při ochraně informační a komunikační infrastruktury totiž kromě něj zakládá i řada dalších součástí českého právního řádu.

Zákon doprovázejí prováděcí právní předpisy, konkrétně vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti a vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích [30], která byla novelizována vyhláškou č. 205/2016 Sb. Zákon 181/2014 Sb. byl s účinností od 1. července 2017 novelizován zákonem č. 104/2017 Sb. (novela zákona o informačních systémech veřejné správy), a s účinností od 1. srpna 2017 zákonem č. 205/2017 Sb.

Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti) (dále „VKB“) [36], která byla přijata 15. prosince 2014 a účinnosti nabyla 1.1. 2015, je zásadní pro zavádění bezpečnostních opatření. Tato vyhláška určuje povinným subjektům (správcům KII a VIS), jaká musí zavést bezpečnostní opatření, jejich obsah a rozsah, stanovuje obsah a strukturu bezpečnostní dokumentace pro informační nebo komunikační systém KII či VIS. Dále se věnuje kybernetickým bezpečnostním incidentům, popisuje jejich typy a kategorie, náležitosti a způsob jejich hlášení a v neposlední řadě také náležitosti oznámení o provedení reaktivního opatření a jeho výsledku, vzor oznámení kontaktních údajů a jeho formu. Bezpečnostní opatření jsou rozdělena na organizační a technická opatření.

Nyní probíhá novelizace, která má za cíl sjednotit vyhlášku se směrnicí NIS a s novelou ZKB, opravit chyby, aktualizovat opatření, a především dosáhnout vyššího stupně KB u již určených povinných subjektů a rozšířit povinnosti i na nové subjekty, které prozatím regulovány nebyly [37]. Návrh vyhlášky zpracoval NÚKIB za podpory tzv. „expertního týmu“ neboli týmem expertů na informační a kybernetickou bezpečnost, kteří byli přímo osloveni NCKB. Nová verze VKB by měla být oproti stávajícímu znění přehlednější, měly by být odstraněny duplicity, které se ve vyhlášce nacházely a přidány nové přílohy [38].

Aktuálně¹² se vyhláška nachází v Meziresortním připomínkovém řízení. Předpokládaná účinnost nového znění je odhadována na květen 2018 [38].

K 1.1. 2015 nabyla účinnosti další důležitá vyhláška a to vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích [39], která stanovuje významné informační systémy a kritéria pro jejich určování. Ve vyhlášce bylo konkrétně zmíněno 92 systémů a 35 subjektů, které VIS spravují. Dále pak byly popsány určující kritéria dělící se na dopadová a oblastní určující kritéria.

¹² K 10.4. 2018

Důvodem vzniku vyhlášky byla nemožnost přesně stanovit VIS a splnění náležitostí, které vyplývají ze ZKB a jak je zmíněno v důvodové zprávě, nejasnost při určování VIS by vedla k zvýšení rizika kybernetických bezpečnostních incidentů. Primárním cílem vyhlášky je tedy zajištění vyšší bezpečnosti VIS. Tato vyhláška byla novelizována a dne 29.6.2016 zveřejněna ve Sbírce zákonů pod č. 205/2016 Sb. a nabyla účinnosti 1.7. 2016. Novela přinesla aktualizovaný seznam VIS.

Dále je potřeba zmínit nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku KI [40]. Nařízení vlády ze dne 22.12. 2010 určuje kritéria, podle kterých jsou KI určovány, rozdělené na průřezová a odvětvová kritéria (kritéria blíže autorka popisuje v podkapitole 5.2.4 Proces určování KII).

V neposlední řadě pak vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby [41]. Vyhláška 1.února. 2018 nabyla účinnosti vyhláška zapracovávající požadavky, které vychází ze Směrnice NIS. Obsahem jsou odvětvová a dopadová kritéria potřebná pro určení provozovatele ZS. Odvětvová kritéria se rozlišují podle 8 odvětví, ve kterém poskytuje orgán či osoba službu, následně dle druhu služby, druhu subjektu a speciálních kritérií. Pojem ZS a odvětví byla popsána v kapitole 1.4. Vyhlášku zpracoval NÚKIB.

5 Kritická infrastruktura

Zmínky o kritické infrastruktuře můžeme pozorovat již od roku 1984, kdy v reportu [42] od americké vládní agentury *Congressional Budget Office* byly definovány „důležité infrastruktury rozhodující v činnosti národního hospodářství“. Přesné spojení „kritická infrastruktura“ nebylo vyřčeno, nicméně dle popisu se jednalo v podstatě o totéž jako současně. V národní strategii z roku 2003 byla KI popsána výrokem „*Když stiskneme spínač, očekáváme světlo. Když zvedneme telefon, očekáváme, že zazní tón. Když zvedneme kohoutek, očekáváme pitnou vodu.*“¹³ Nejde však pouze o elektřinu, telekomunikace či pitnou vodu. KI je Výkladovým slovníkem [15] definována jako systémy a služby, jejichž úplná či částečná nefunkčnost by měla závažný dopad na bezpečnost státu, jeho ekonomiku, veřejnou správu a v důsledku na zabezpečení základních potřeb obyvatelstva. Do 31.12. 2010 nebyla problematika KI v českém právním řádu ukotvena,

KI vychází již ze zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) [2], o kterém se autorka zmiňuje více v podkapitole 5.1.

Kritickou informační infrastrukturou (KII) se pak rozumí komplex informačních a komunikačních systémů, jejichž nefunkčnost by mohla mít vážný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob či ekonomiku státu. Aby výše zmíněné bylo zabezpečeno, ať už za běžných či kritických podmínek, musí být funkční 4 pilíře KII [36]:

- prevence,
- detekce,
- reakce,
- krizový management.

Cílem je minimalizace dopadů výpadku KI, aby toto narušení bylo co nejméně četné, krátkodobé a zvladatelné. Ochrana KII se stále vyvíjí. Aktuálně nejvyšší hrozbou může být teroristický útok či živelné pohromy. Vilém Adamec [43] ve své knize popisuje ještě další možné hrozby jako jsou například stávky, sociální nepokoje či vojenské napadení.

KII musí plnit 100 % povinností, které jsou určené vyhláškou č. 316/2014 Sb. Aktuálně je jako KII určeno dle Adama Kučíského [36] cca 280 systémů.

¹³ Přeloženo z anglického „When we flip a switch, we expect light. When we pick up a phone, we expect a dial tone. When we turn a tap, we expect drinkable water.“

5.1 Krizový zákon

Vedle ZKB a prováděcích předpisů zmíněných v kapitole 4.9 je nutné ve spojitosti s KI uvést i zákon č. 240/2000 Sb.- o krizovém řízení a o změně některých zákonů (krizový zákon) [2]. Do 31.12. 2010 nebyla problematika KI v českém právním řádu ukotvena, 1. ledna 2011 nabyla účinnosti novela tohoto zákona, která nově uvádí, že za KI se považuje prvek KI nebo systém prvků KI, jehož narušení funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

Tento zákon upravuje problematiku krizových stavů, upravuje působnost a pravomoc státních orgánů a orgánů územních samosprávných celků a stanovuje práva a povinnosti právnických a fyzických osob při přípravě na krizové situace nesouvisející se zajišťováním obrany České republiky před vnějším napadením¹⁴, a při jejich řešení a při ochraně kritické infrastruktury a odpovědnost za porušení těchto povinností [2]. Před existencí zákona nebyla krizová problematika nijak právně upravena.

Zákon definuje tzv. krizové situace a dělí je na

- stav nebezpečí,
- nouzový stav,
- stav ohrožení státu.

Krizové stavy se dělí dle důležitosti, posuzuje se doba trvání situace a intenzitě dopadů, velikost oblasti a množství zasažených lidí událostí. Zákon dělí dopady do 6 kategorií:

- 0: zanedbatelné z hlediska života občana,
- 1: nedůležité z hlediska občana,
- 2: důležité z hlediska občana,
- 3: závažné z hlediska společnosti,
- 4: velmi závažné z hlediska společnosti,
- 5: ohrožující existenci či podstatu společnosti

¹⁴ Zákon č. 222/1999 Sb., o zajišťování obrany České republiky

Dále Krizový zákon definuje krizové řízení, čímž se dle § 2 rozumí souhrn činností orgánů krizového řízení zaměřených na analýzu a vyhodnocení bezpečnostních rizik a plánování, organizaci, realizaci a kontrolu činností prováděných v souvislosti s:

1. přípravou na krizové situace a jejich řešením, nebo
2. ochranou kritické infrastruktury,

Krizové řízení lze tedy pojmout jako soubor opatření, které by subjekty plnily v případě krizového stavu pro zajištění bezpečnosti a ochrany obyvatelstva. Cílem je udržení zdraví obyvatel, zajištění funkčnosti veřejné správy, zajistit dostupnost důležitých služeb atd.

Orgány krizového řízení jsou:

- vláda,
- ministerstva a jiné ústřední správní úřady,
- orgány kraje a ostatní orgány s územní působností,
- hasičský záchranný sbor kraje,
- Policie ČR,
- orgány obce.

Úkoly orgánům uděluje vláda, hlavními jsou analyzování rizik či tvoření plánů pro řešení krizových situací, a řídí a kontroluje činnost ostatních orgánů. Ministerstva zřizují pracoviště krizového řízení.

Subjekty KI jsou dle krizového zákona povinni vypracovat plán krizové připravenosti, ve kterém musí být zmíněny veškerá možná ohrožení funkce prvku KI a stanovena ochranná opatření, dále pak musí umožnit příslušnému ministerstvu nebo jinému ústřednímu správnímu úřadu vykonat kontrolu plánu a oznámit příslušnému ministerstvu či jinému ústřednímu správnímu úřadu informace o organizační, výrobní nebo jiné změně, například v případě, že by společnost zastavila provozu či ukončila činnost.

6 ZKB v praxi

Každá společnost je jedinečná a stejně tak i její cesta k bezpečnosti. Každá má specifické postupy, techniky či prostředí, tedy i postup aplikace požadavků je svým způsobem unikátní. V této kapitole autorka poznatky z teoretické části práce a zabývá se postupem implementace požadavků KB v telekomunikační společnosti. Veškeré informace byly poskytnuty touto společností, ať už formou polostandardizovaného rozhovoru s pracovníky, oficiálních webových stránek společnosti či volně dostupných materiálů, které v rámci zachování anonymity firmy nemohou být přesně uvedeny.

6.1 Uvedení do kontextu společnosti

Společnost je telekomunikačním operátorem, který působí na telekomunikačním trhu na území České republiky. Poskytuje služby veřejných elektronických komunikací i služby orientované na přesné požadavky zákazníka. Podle rozsahu společnosti je zařazena na telekomunikačním trhu mezi společnosti s významnou tržní silou.

Společnost je provozovatelem a vlastníkem telekomunikačních systémů, které tvoří technickou základnu pro široké spektrum datových a hlasových služeb. Obchodní činnost je rozvíjena v oblasti operátorských propojení, pronájmu okruhů, poskytování různého druhu konektivit a komunikační podpory energetických sítí.

Společnost dále působí jako alternativní komunikační operátor, poskytuje základní veřejné služby pro volání v rámci České republiky, ale i do zahraničí. Společnost disponuje rozsáhlou infrastrukturou, hustou sítí přípojných bodů, výkonnou přenosovou sítí a vysokorychlostním připojením do zahraničí.

Veškeré informace sepsané v následující části práce jsou aktuální k 26.4. 2018. Společnost si nepřála uvést své jméno, stejně tak některé názvy nástrojů používaných v rámci technických opatření.

6.2 Proces určování KII

8. prosincem 2014 započala jednání týkající se určování KII a následné určování probíhalo v několika vlnách. V první fázi bylo vytipováno 46 systémů, jednalo se o informační a komunikační systémy, jejichž správcem byly ústřední orgány státní správy. V druhé fázi došlo k určování subjektů z řad ostatních organizačních složek státu. Ve třetí fázi byly určovány KII mezi soukromými subjekty.

Pro určování KII jsou důležité [45].:

- ZKB – definuje KII,
- Krizový zákon – stanoví proces určení KII,
- Nařízení vlády č. 432/2010 Sb.- stanoví kritéria pro KII.

Prvky KI se určují dle průřezových a odvětvových kritérií. V případě, že platí alespoň jedno z průřezových kritérií a alespoň jedno z odvětvových, jedná se kritický IS. Pokud se jedná o IS organizační složky státu, je zařazen do seznamu KI, který je schvalován vládou.

Průřezová kritéria vyplívají z § 1 nařízení vlády č. 432/2010 Sb., ve znění novely č. 315/2014 Sb.. Tato kritéria jsou stejná pro všechna odvětví a dělí se na 3 hlediska: počet obětí, ekonomický dopad a dopad na veřejnost. V případě, že není splněno ani jedno z kritérií, nepovažuje se jako prvek KI. Přesné znění průřezových kritérií dle nařízení vlády:

- a) Více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací delší než 24 hodin.
- b) Mezní hodnota hospodářské ztráty je větší než 0,5 % HDP (např. v r. 2013 = 19,4 mld. Kč).
- c) Omezení poskytování nezbytných služeb nebo jiný závažný zásah do každodenního života postihující více než 125 000 osob

Druhou skupinou jsou odvětvová kritéria dána stejným nařízením vlády jako v předchozím případě. Tato kritéria se týkají veškerých odvětví se o následující kritéria:

- a) IS, který významně nebo zcela ovlivňuje činnost určeného prvku KI a zároveň je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období delším jak 8 hodin.
- b) KS, který významně nebo zcela ovlivňuje činnost určeného prvku KI a zároveň je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období delším jak 8 hodin.
- c) IS spravovaný orgánem veřejné moci obsahující osobní údaje o více než 300 000 osobách.
- d) KS, který zajišťuje připojení nebo propojení prvku KI s kapacitou garantovaného datového přenosu min. 1 Gbit/s.
- e) Odvětvová kritéria pro určení prvku KI uvedená v písm. A. – F., odvětví VI. Přílohy nařízení vlády č. 432/2010 Sb., ve znění novely č. 315/2014 Sb., se použijí přiměřeně pro oblast KB, pokud je ochrana prvku naplňujícího tato kritéria nezbytná pro zajištění KB.

Poslední kritérium umožňuje určení KII subjektům, které nespadají do a) až d), ale naplňují průřezová kritéria a kritérium z odvětví VI. *Komunikační a informační systémy*:

A. Technologické prvky pevné sítě elektronických komunikací:

- a) centrum řízení a podpory sítě,
- b) řídicí ústředna,
- c) mezinárodní ústředna,
- d) transitzní 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 řídicí jednotka sítě pokrývající strategickou lokalitu,
- d) základnová stanice sítě pokrývající strategickou lokalitu,
- e) datové centrum.

C. Technologické prvky sítě pro rozhlasové a televizní vysílání:

- a) vysílací zařízení pro šíření televizního nebo rozhlasového signálu určených pro informaci obyvatelstva
- b) za krizových situací vysílacím výkonem nad 1 kW k zajištění rozhlasového a televizního vysílání veřejnoprávního
- c) provozovatele
- d) řídicí pracoviště provozu,
- e) datové centrum,
- f) 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 řídicí a komunikační středisko,
- d) pozemní propojovací síť.

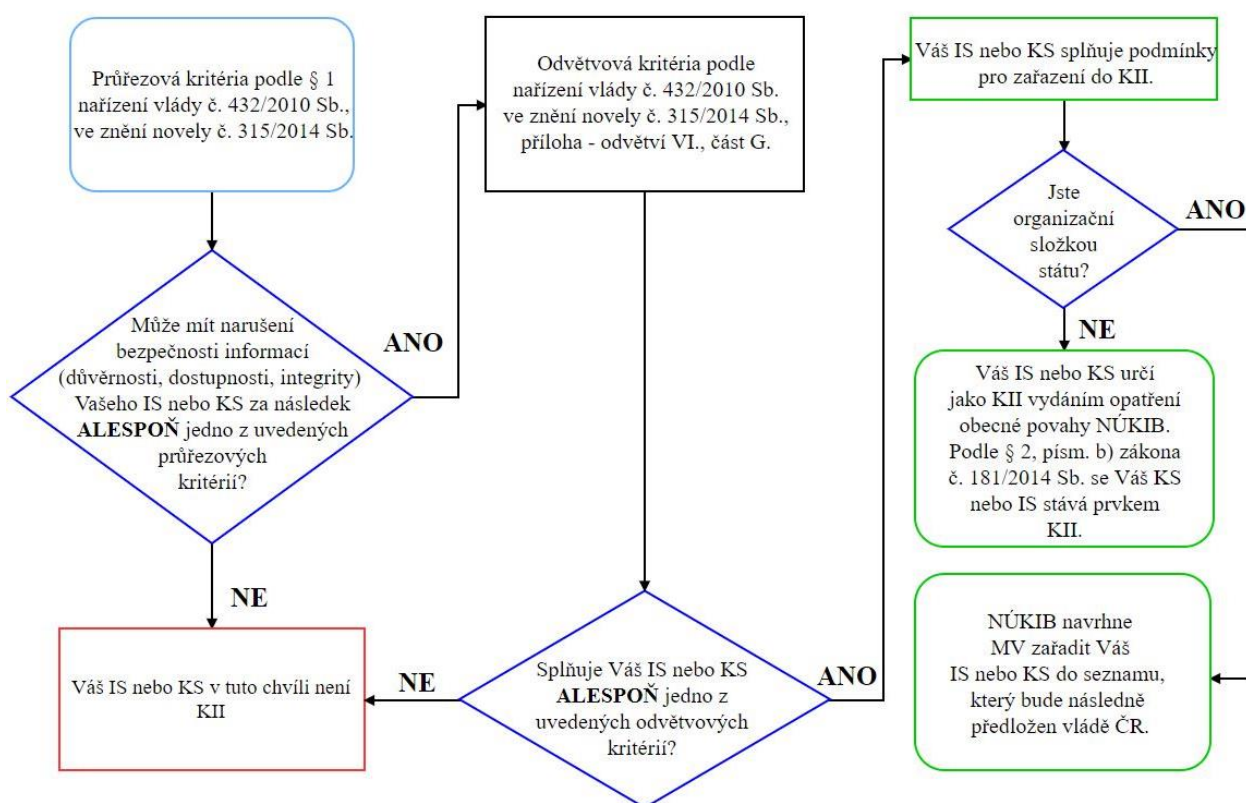
E. Technologické prvky pro poštovní služby:

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

F. Technologické prvky informačních systémů:

- řídící centrum,
- datové centrum,
- síť elektronických komunikací,
- technologický prvek zajišťující provoz registru doménových jmen CZ a zabezpečení provozu domény nejvyšší úrovně CZ.

Prvotním impulsem pro určovací proces bylo kontaktování subjektu ze strany NBÚ. Společnost zhodnotila své IS a KS, zda naplňuje kritéria pro určení za KII. Při tomto zhodnocení probíhala úzká spolupráce s NBÚ. Až poté, co se ukončí určovací proces, může se stát společností KII. V případě zkoumané společnosti, v průběhu roku 2015 bylo společnosti ze strany NBÚ potvrzeno, že bude určena jako subjekt provozující KII a byly určeny 3 prvky KII. Pro lepší přehlednost je proces určení znázorněn v následujícím obrázku:



Obrázek 1: Proces určování podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve znění novely č. 315/2014 Sb. [Zdroj: autorka dle [45]]

6.3 Postup hodnocení dopadů

Účelem této kapitoly je poskytnout čtenáři přehled o postupu hodnocení dopadů narušení bezpečnosti informací u aktiv, informačních a komunikačních systémů, ICT služeb a k následnému řízení rizik dle Metodiky k vodítkům pro hodnocení dopadů [46]. Pro posouzení závažnosti dopadů způsobených narušením bezpečnosti informací (důvěrnosti, dostupnosti, integrity) jsou navrženy následující oblasti dopadů:

- 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.

V každé oblasti se závažnost dopadů dělí na 4 úrovně – nízkou, střední, vysokou a kritickou. Při hodnocení se nezkoumají hrozby, které zapříčinily narušení bezpečnosti a neurčuje se pravděpodobnost scénářů. Posuzují se nejhorší možné scénáře, které by mohly nastat. Ty se probírají se správcem (garantem) daného IS a garantem procesu či služby, kterou IS poskytuje. Hodnotí se veškeré aspekty narušení bezpečnosti informacím, což znamená narušení důvěrnosti, dostupnosti a integrity dat.

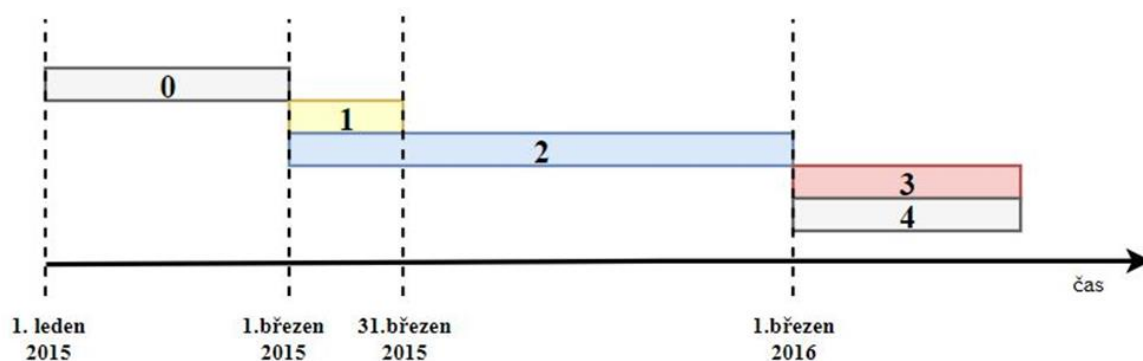
Nejprve je získán obecný popis daného IS, především účel a rozsah zpracovaných informací. Dále se porovnávají kritické scénáře popsané garantem a porovnávají se s obecnými vodítky pro hodnocení dopadů zveřejněnými NBÚ. Dále se pak hodnotí jednotlivé následky, tedy dochází k hodnocení následků:

- nedostupnosti,
- ztráty dat,
- narušení důvěrnosti dat,
- a narušení integrity dat.

6.4 Implementace vybraných požadavků ZKB

Před započítím samotné implementace bylo třeba zhodnotit stávající stav prostředí firmy. Prvním krokem tedy bylo provedení rozdílové analýzy, taktéž známé jako „Gap“ analýza, což je analytická metoda, při které se zkoumal aktuální stav ve společnosti vůči požadavkům ZKB. Vznikl teoretický koncept implementace a postupně byly přijímány doprovodné preventivní nástroje a opatření vedoucí k plné adaptaci implementace a společně se subjekty státní exekutivy byl zjišťován rozsah prvků KI. V roce 2015 byla navázána užší spolupráce se subjekty krizového řízení a integrovaného záchranného systému.

Pro přehlednost shrnutí implementace za použití časové osy:



Obrázek 2: Časová osa implementace požadavků ZKB ve společnosti. [Zdroj: autorka dle [45]]

0. Proces určování prvků KII (oboustranné jednání s NBÚ),
1. Probíhala lhůta pro nahlášení kontaktních údajů,
2. Přejídná lhůta (implementace bezpečnostních opatření podle vyhlášky č. 316/2014 Sb.),
3. Plnění povinností podle ZKB (hlášení kybernetických bezpečnostních incidentů, provádění bezpečnostních opatření),
4. Možnost státního dozoru (audit) ze strany NBÚ – kontrola souladu se zákonem o kybernetické bezpečnosti.

Ze ZKB vychází, že společnost je povinná mít bezpečnostní dokumentaci a splňovat organizační a technická opatření. ZKB stanovuje, jaké povinnosti a daná opatření jsou. VKB pak co tyto povinnosti a opatření znamenají. Popisuje, co je v daných případech potřeba udělat, nicméně nedefinuje jak. V následující části práce je uvedeno, jak či jakým způsobem byly naplněny povinnosti ve vybrané společnosti.

6.4.1 Organizační opatření

Organizační opatření vychází především z ISO norem rodiny 27000, které organizacím pomáhají zavést a provozovat ISMS. V normě ČSN ISO/IEC 27002 jsou specifikovány požadavky na výběr a zavedení bezpečnostních opatření. Proto došlo u některých požadavků spíše k „revizi“ než k zavádění kompletně nových opatření.

Do organizačních opatření spadá řízení aktiv, to lze rozdělit do 3 fází: identifikace aktiv, hodnocení a klasifikace aktiv. Obecně můžeme říci, že aktivem může být cokoliv, čeho si nějakým způsobem ceníme a o co nechceme (či nesmíme) přijít. Aktivum může mít hmotnou povahu, ať už to jsou počítače, zboží či přenosové cesty. V tomto případě se nám snaží protistrana tato aktiva ukrást či poškodit. Všechna aktiva ale nemusí být hmotná, může jít o informace či know how, kdy útočník se snaží tato aktiva získat. Dále se může jednat o jednotlivé schopnosti společnosti, například schopnost poskytovat služby, útočník se snaží tyto schopnosti omezit. V neposlední řadě může jít i například o reputaci dané společnosti, kterou se snaží protistrana pokazit. Klasifikování informací bylo důležité proto, aby se rozhodlo, jak se s danou informací má nakládat a jaké jsou parametry pro jejich uchovávání. Informace byly rozděleny na interní, veřejné a důvěrné. Ve zkoumané společnosti byla aktiva rozlišena na primární a podpůrná. Mezi ta primární jsou zařazena data, informace a poskytované služby. Ve společnosti byla vyhodnocena jako nejdůležitějším primárním aktivem právě informace. Byla zhodnocena úroveň důležitosti primárních aktiv, hodnotila se jejich důvěrnost, dostupnost a integrita. Dále byly identifikovány vazby mezi podpůrnými a primárními aktivy. Dalším bodem bylo určení pravidel definujících manipulaci s nimi dle úrovně, především zaměřenými na sdílení a přenášení aktiv, aby nedošlo k úniku či poškození dat. V neposlední řadě byla určena pravidla ochrany aktiv.

Byla zavedena metodika pro řádné identifikování a kvantifikování rizika, kterým je či může být společnost vystavena, pomýšlející nejen na technologické faktory, ale i možné riziko ekologického charakteru (například přírodní katastrofy), sociálního či ekonomického charakteru. Po identifikaci probíhala analýza rizik, rizika byla posuzována podle míry možnosti vzniku a hodnocena a byly stanoveny potenciální hrozby (ale i příležitosti), které by v případě rizika mohly nastat. Společnost využila postupy, které jsou založené na systémovém přístupu k řízení rizik. Využila zkušeností jiných evropských společností, především v řízení provozního rizika. Pravidelně dochází ke kontrole a aktualizaci aktiv, dochází k aktualizaci seznamu hrozeb, zranitelnosti a rizik a pravidelně se obnovuje bezpečností i provozní dokumentace. Systém řízení informační a kybernetické bezpečnosti je nastaven tak, aby byl v souladu s veškerými požadavky vycházejícími z legislativy a také z bezpečnostních požadavků zákazníků a smluvních partnerů.

V průběhu roku 2016 společnost naplňovala požadavky vyplývající ze ZKB v souladu s již vytyčeným rámcem systematické identifikace bezpečnostních rizik a zlepšováním schopností překonat důsledky mimořádných událostí. Praktickou aplikací strukturovaných opatření společnost mířila k dosažení certifikace ISO 27001:2013 s cílem ochrany informačního kapitálu a jednoduššímu řízení, měření a zlepšování.

V návaznosti na § 6 VKB byl zaveden výbor pro řízení KB. Vyhláška definuje bezpečnostní role, které má společnost povinnost zavést, byl tak začleněna role manažera KB, který má například odpovědnost za systém řízení bezpečnosti informací a je hlavní řídicí osobou v této oblasti, dále zodpovídá za interní předpisy a soulad s legislativou, má na starosti seznam aktiv a jejich garantů, stejně tak seznam pracovníků a jejich bezpečnostních rolí. Další rolí je architekt KB, který zajišťuje návrh a implementaci technických bezpečnostních opatření a určuje nástroje, které povedou k zajištění těchto opatření, analyzuje úroveň architektury KB a rizika a pracuje na postupech, které by vedly k zmírnění těchto rizik. Auditor KB vyhodnocuje účinnost nastavených bezpečnostních opatření, vede dokumentaci o auditu, vyhodnocuje výsledky auditu a navrhuje nápravná opatření. Mimo tyto 3 role byl veškerým aktivům přidělen jejich garant, který za ně zodpovídá. Tento výbor má odpovědnost za implementaci bezpečnostní politiky, vyhodnocuje stav bezpečnosti informací ve společnosti, napomáhá v prosazování KB napříč společnostmi či například vypracovává podklady pro zhodnocení účinnosti a stavu KB.

Důležitým bodem bylo stanovení bezpečnostních požadavků na dodavatele. Společnost provedla analýzu rizik, byl nastaven věcný reporting, kterým byli řízeni dodavatelé, který je řízen systémově. Část reportingu byla přenechána dodavatelům. Byly upraveny smlouvy s dodavateli, přidaly se povinnosti, které vyplývaly z VKB. Bezpečnostní požadavky jsou tak smluvně ošetřeny. Dodavatelé jsou důkladně proškolení a rizika spojená s dodavateli pravidelně hodnocena.

Další nezbytnou součástí implementace bylo zpracování plánu v rámci bezpečnosti lidských zdrojů. Ne nadarmo se říká, že každý řetěz je tak silný, jak silný je jeho nejslabší článek. Mohou být nastaveny sebelepší opatření, procesy a technické nástroje, avšak pokud selže lidský faktor, je velká pravděpodobnost, že dojde k problému. Společnost si je výše zmíněného přísloví vědoma, a proto vkládá velké finanční obnosy do školení svých zaměstnanců. Jsou kladeny vysoké nároky na odbornost zaměstnanců a kvalifikaci. Zaměstnanci jsou vzděláváni na zákonných školeních, pravidelně dochází k přezkoušení znalostí a pracuje se nejen na jejich odborné stránce a zvyšování kvalifikace, ale i na tzv. „soft skills“ a také na jazykových schopnostech. V roce 2017 mimo odborná školení byl spuštěn „program“ pro klíčové zaměstnance, kde si mohou zaměstnanci sami volit školení dle jejich preferencí a rozvíjet se individuálně.

V létě 2017 proběhl předcertifikační audit KB ISO/IEC 27001:2013 Ke konci roku 2017 proběhl audit KB ve smyslu platné právní úpravy na úseku KB.

6.4.2 Technická opatření

Jak již bylo zmíněno, aktiva jsou pro společnost velmi cenná a jejich ohrožení by mohlo mít fatální následky. V průběhu roku 2016 se společnost zaměřila na posilování bezpečnosti KII a byla zahájena implementace bezpečnostních politik, jejichž cílem bylo především zvýšení zabezpečení aktiv, dále pak postupné zvyšování úrovně fyzické a systémové bezpečnosti, aby nebylo možné znevážit aktiva a aby bylo zamezeno možnému neoprávněnému přístupu a poškození aktiv. Chráněny jsou celé objekty i jednotlivé prostory s technickými aktivy. Jsou zavedeny kamerové systémy a systémy kontrolující vstupy. Ověřuje se identita veškerých uživatelů, byly zpřísněny požadavky na hesla, na jejich délku, složitost a zda již podobné heslo nebylo použito. Politiky byly nastaveny tak, aby jejich působením nebyl nějakým způsobem utlumen provoz. Společnost i nadále pokračuje v rozvoji a implementování bezpečnostních politik, aby zajistila soulad s platným právem a bylo zahájeno ověřování dynamiky a účinnosti bezpečnostních procesů.

V 1.polovině roku 2015 společnost v souladu se ZKB implementovala „Data Retention“ neboli sběr provozních a lokalizačních údajů (komponenta Internet, provoz ISP).

Ve společnosti je zaveden systém (log management) pro centralizovanou správu protokolů událostí. Systém dlouhodobě ukládá zaznamenané bezpečnostní a provozní události jednotlivých technologií KI a komunikačních systémů společnosti. Systém plní úlohu „forenzního skladu“, data jsou zde ukládána pro případ, že by bylo zpětně nutno prošetřit některé události či v případě kybernetických incidentů dohledat nějaké důkazy. Centralizace logů zajišťuje rychlý a jednoduchý přístup k logům, které se pak snáz analyzují. Splňuje tak § 21, § 22 a § 24 VKB – zaznamenává činnosti KII, jejich uživatelů a administrátorů, detekuje kybernetické bezpečnostní události, které sbírá a vyhodnocuje. V případě, že jsou využívány ne příliš odolné algoritmy, klíče či protokoly, dojde k upozornění. V rámci aplikační bezpečnosti se aplikace přístupné zvenčí vždy testují a je zajištěna kontrola, která má za cíl ochránit aplikace před neoprávněnou změnou.

Systém nesplňuje pouze technická opatření, ale i již zmíněná opatření organizační. Například umožňuje z analyzovaných dat generovat audity dle auditora. požadavky normy ČSN ISO/IEC 27001:2014 na pořizování auditních záznamů.

Závěr

Jak vyplynulo z práce, kybernetická bezpečnost je aktuálním fenoménem na území celého světa. Ovlivňuje nejen organizace či povinné subjekty, ale všechny, kteří mají přístup k informačním technologiím. Není sporu, že informační a komunikační technologie se budou nadále vyvíjet

Je potřeba si uvědomit, že kybernetická bezpečnost není cílová destinace, nýbrž cesta. Jedná se o nepřetržitý proces, který rozhodně nekončí jednorázovou implementací bezpečnostních nástrojů. Vše se neustále rozvíjí, proto je potřeba i již zavedená opatření pravidelně posuzovat a kontrolovat a v případě potřeby zavádět nová. Dále pak ve spolupráci s vládním či národním CERT je potřeba reagovat na nové hrozby, které se také neustále vyvíjí, proto zůstat o krok pozadu může mít fatální následky. Stejně tak je potřeba si uvědomit, že KB není záležitostí pouze státních úřadů či firem, ale i všech domácích uživatelů. Spousta lidí nemá představu, jak moc cenná jejich data jsou, že je potřeba se v kybernetickém prostředí chovat obezřetně a náležitě zabezpečit veškerý svůj hardware i domácí síť.

Cíle, které byly stanoveny v úvodu práce, mohou být považovány jako splněné. Z rešerše zdrojů vyšlo, že tato oblast téměř není pokryta literaturou, která by odrážela aktuální stav a povinnosti vyplývající pro organizace. V rámci práce došlo k rozboru vybraných povinností ZKB, byl analyzován důvod vzniku a jeho vývoj, vybrané povinnosti a popsána kritická infrastruktura. Následně teoretické poznatky byly použity k popisu postupu v praxi a byl popsán proces, kterým si společnost musela projít a jak se vypořádala s vybranými požadavky, které vychází ze ZKB. Ze syntézy vyšlo, že spousta opatření byla již ve společnosti zavedena ještě před tím, než a ni začal ZKB působit.

Z pohledu společnosti, hlavními cíli bylo naplnit požadavky ZKB a zvýšit úroveň bezpečnosti, což lze považovat za splněné. Aktuálně se společnost zaměřuje na neustálé zlepšování bezpečnosti, klade důraz na to, aby bezpečnost zajišťovali všichni zaměstnanci, efektivně se vypořádává s rizikem, aby veškerá data byla klasifikována a řádně chráněna, aktivně podporuje business cíle, bezpečnost řídí s ohledem na náklady a v neposlední řadě vše zajišťuje v souladu s legislativou. Nadále bude pokračovat školicí program pro klíčové zaměstnance, zvyšovat s odbornost technických pracovníků, ale stejně tak bude proškolována celá společnost a zvyšováno povědomí o kybernetické bezpečnosti.

Seznam literatury

- [1] Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti). In: Sbírka zákonů. ISSN 1211-1244
- [2] Zákon č. 240/2000 Sb. - Zákon o krizovém řízení a o změně některých zákonů (krizový zákon) In: Sbírka zákonů. ISSN 1211-1244
- [3] GERŽA, Michal. *Návrh implementace bezpečnostní politiky v informačním systému veřejné správy* [online]. Zlín, 2015. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Dostupné z: <https://theses.cz/id/ww3zk8>
- [4] DRAGANOV, Vojtěch. *Zákon o kybernetické bezpečnosti a jeho dopady na povinné subjekty* [online]. Praha 2015. Diplomová práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky. Dostupné z: <https://vskp.vse.cz/eid/49564>
- [5] SMETANA, Roman. *Kybernetická bezpečnost ve veřejné správě* [online]. Praha, 2017. Bakalářská práce. Vysoká škola finanční a správní, a. s., Fakulta právních a správních studií. Dostupné z: <https://is.vsfs.cz/th/r3qal/>
- [6] PIŠA, Jan. *Implementace kybernetické bezpečnosti a normy ISO 27000 ve státní správě* [online]. Hradec Králové, 2015. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu. Dostupné z: <https://theses.cz/id/fi5li5/STAG64822.pdf>
- [7] STRÁNSKÝ, Tomáš. *Bezpečnost podnikové IT infrastruktury a implementace ISO 27000* [online]. Česka Třebová, 2015. Diplomová práce. Univerzita Hradec Králové, Fakulta informatiky a managementu. Dostupné z: <https://theses.cz/id/q88diy/STAG64823.pdf>
- [8] KRATOCHVIL, David. *Kybernetická bezpečnost a legislativa ČR* [online]. Praha, 2013. Diplomová práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky. Dostupné z: <http://www.vse.cz/vskp/eid/38486>
- [9] KAMENÍČEK, Lukáš. *Kybernetická bezpečnost z pohledu podnikové informatiky* [online]. Praha, 2016. Diplomová práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky. Dostupné z: <http://www.vse.cz/vskp/eid/52801>
- [10] MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti: komentář*. Praha: Wolters Kluwer, 2015. ISBN 978-80-7478-817-8. 7478-817-8.
- [11] HROMADA, Martin, Petr HRŮZA, Josef KADERKA, Oldřich LUŇÁČEK, Miroslav NEČAS, Bohumil PTÁČEK, Leopold SKORUŠA a Richard SLOŽIL. *Kybernetická bezpečnost: teorie a praxe*. Praha: Powerprint, 2015. ISBN 978-80-87994-72-6.
- [12] ČAPEK, Jan, Miloslav HUB, Radim ROUDNÝ, Hana KOPÁČKOVÁ, Jan FUKA a Martin IBL. *Vybrané aspekty kybernetické bezpečnosti*. Pardubice: Univerzita Pardubice, 2015. ISBN 978-80-7395-953-1.
- [13] KOLOUCH, Jan. *CyberCrime*. Praha: CZ.NIC, 2016. ISBN 978-80-88168-15-7.
- [14] ACCENTURE. *Cost of Cyber Crime Study: Insights on the security investments that make a difference* [online]. Michigan, 2017 [cit. 2018-04-1]. Dostupné z: https://www.accenture.com/t20170926T072837Z_w_us-en_acnmedia/PDF-61/Accenture-2017-CostCyberCrimeStudy.pdf. Ponemon Institute LLC.

- [15] JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽAR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary*. 3. aktualizované vydání. Praha: Policejní akademie ČR v Praze, Česká pobočka AFCEA, 2015. ISBN 978-80-7251-436-6.
- [16] ANTUŠÁK, Emil a Zdeněk KOPECKÝ. *Úvod do teorie krizového managementu I*. 2. vyd. Praha: Oeconomica, 2003. ISBN 80-245-0548-7.
- [17] HRŮZA, Petr. *Kybernetická bezpečnost*. Brno: Univerzita obrany, 2012. ISBN 978-80-7231-914-5
- [18] KADLECOVÁ, Lucie. *Konceptuální a teoretické aspekty kybernetické bezpečnosti* [online]. 2015 [cit. 2018-04-26]. Dostupné z: https://is.muni.cz/el/1423/podzim2015/BSS469/um/Prezentace_FSS_Konceptua_lni_a_teoreticke_aspekty_KB.pdf. NCKB / Institut mezinárodních studií, Fakulta sociálních věd, Univerzita Karlova.
- [19] MINISTERSTVO VNITRA. *Koncepce boje proti organizovanému zločinu (2000)* [online]. 2000 [cit. 2018-04-1]. Dostupné z: <https://www.databaze-strategie.cz/cz/mv/strategie/koncepce-boje-proti-organizovanemu-zlocinu>
- [20] MINISTERSTVO VNITRA. *Koncepce boje proti trestné činnosti v oblasti informačních technologií včetně Harmonogramu opatření* [online]. 2001 [cit. 2018-04-1]. Dostupné z: <http://www.mvcr.cz/soubor/koncepce-pdf.aspx>
- [21] MINISTERSTVO INFORMATIKY ČESKÉ REPUBLIKY. *Státní informační a komunikační politika e-Česko 2006* [online]. Praha, 2006 [cit. 2018-04-1]. Dostupné z: <http://www.culturenet.cz/res/data/002/000269.pdf>
- [22] SMEJKAL, Vladimír a RAIS, Karel. *Řízení rizik ve firmách a jiných organizacích*. 4. vydání, Praha, Grada Publishing, 2013. ISBN 978-80-247-4644-9
- [23] MINISTERSTVO INFORMATIKY ČESKÉ REPUBLIKY. *Národní strategie informační bezpečnosti ČR NSIB ČR Verze: 0.8* [online]. Praha, 2005 [cit. 2018-04-1]. Dostupné z: <https://moodle.unob.cz/mod/resource/view.php?id=12529>
- [24] VLÁDA ČESKÉ REPUBLIKY. *Usnesení vlády České republiky ze dne 15. března 2010 č. 205 o řešení problematiky kybernetické bezpečnosti České republiky* [online]. 2010 [cit. 2018-04-2]. Dostupné z: <https://apps.odok.cz/attachment/-/down/KORN97BQ9ASZ>
- [25] NBÚ. *Informace k usnesení vlády České republiky č. 781 ze dne 19. října 2011* [online]. 27. říjen 2011 [cit. 2018-04-10]. Dostupné z: <https://www.nbu.cz/cs/aktualne/867-994-informace-k-usneseni-vlady-ceske-republiky-ze-dne-19-rijna-2011-c-781/>
- [26] NÚKIB. *Co je NÚKIB* [online]. [cit. 2018-04-10]. Dostupné z: <https://nukib.cz/cs/>
- [27] S&T CZ S.R.O. *Tři čtvrtiny tuzemských firem neví, jak postupovat v nouzi* [online]. 27.4. 2010 [cit. 2018-04-10]. Dostupné z: <http://www.itpoint.cz/sntcz/clanky/?i=tri-ctvrtiny-tuzemskych-firem-nevi-jak-postupovat-v-nouzi-5382>
- [28] NBÚ. *Důvodová zpráva* [online]. 15. 04. 2013 [cit. 2018-04-10]. Dostupné z: <https://www.govcert.cz/download/legislativa/container-nodeid-708/nbu-zkb-navrh-130415-duvodzprava.pdf>
- [29] NÚKIB. *Vláda schválila návrh věcného záměru zákona o kybernetické bezpečnosti* [online]. 30. 05. 2012 [cit. 2018-04-24]. Dostupné z: <https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2191-vlada-schvalila-navrh-vecneho-zameru-zakona-o-kyberneticke-bezpecnosti/>

- [30] NBÚ. *Informace o změnách zákona 181/2014 Sb. o kybernetické bezpečnosti účinných od 1.července 2017* [online]. 22.6. 2017 [cit. 2018-04-16]. Dostupné z: https://nukib.cz/download/legislativa/2017/Zm%C4%9Bna_z%C3%A1kona_o_kybernetick%C3%A9_bezpe%C4%8Dnosti_1_7_2017-final.pdf
- [31] LUPA.CZ. *Kdo (a co) bude spadat pod nový zákon o kybernetické bezpečnosti?* [online]. 22.9. 2014 [cit. 2018-04-17]. Dostupné z: <https://www.lupa.cz/clanky/kdo-a-co-bude-spadat-pod-novy-zakon-o-kyberneticke-bezpecnosti/>
- [32] Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS)
- [33] NBÚ. *Podpůrný materiál popisující změny v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti účinných od 1. srpna 2017* [online]. 22.6. 2017 [cit. 2018-04-16]. Dostupný z: https://nukib.cz/download/legislativa/2017/Zm%C4%9Bna_z%C3%A1kona_o_kybernetick%C3%A9_bezpe%C4%8Dnosti_velk%C3%A1_novela_v4.pdf
- [34] NBÚ. Návrh zákona o kybernetické bezpečnosti byl odeslán k meziresortnímu připomínkovému řízení [online]. 15. 04. 2013 [cit. 2018-04-11]. Dostupné z: <https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2157-navrh-zakona-o-kyberneticke-bezpecnosti-byl-odeslan-k-meziresortnimu-pripominkovemu-rizeni/>
- [35] KUČÍNSKÝ, Adam. *Novela zákona o kybernetické bezpečnosti* [online]. 4.4. 2017 [cit. 2018-04-11]. Dostupné z: https://www.govcert.cz/download/kii-vis/CyberCon2017/Kucinsky-Novela_ZKB_2017.pdf
- [36] Vyhláška č. 316/2014 Sb. o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Národní bezpečnostní úřad, 2014 [cit. 2018-04-24]. Dostupné také z: https://www.govcert.cz/download/kii-vis/vkb_uz.pdf
- [37] NÚKIB. *Nová vyhláška o kybernetické bezpečnosti: Odůvodnění vyhlášky* [online]. 19.4. 2018 [cit. 2018-04-25]. Dostupné z: https://www.govcert.cz/download/kii-vis/NovaVKB/VKB_oduvodneni_po_MPR.docx
- [38] KUČÍNSKÝ, Adam. *Novela zákona o kybernetické bezpečnosti* [online]. 4.4. 2017 [cit. 2018-04-16]. Dostupné z: https://www.govcert.cz/download/kii-vis/CyberCon2017/Kucinsky-Novela_ZKB_2017.pdf
- [39] Vyhláška č. 317/2014 Sb. Vyhláška o významných informačních systémech a jejich určujících kritériích. In: Sbírka zákonů. ISSN 1211-1244
- [40] Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku KI. In: Sbírka zákonů. ISSN 1211-1244
- [41] Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby. In: Sbírka zákonů. ISSN 1211-1244
- [42] Vaughan, R. and Pollard, R. *Rebuilding America, Vol. I, Planning and Managing Public Works in the 1980s*. Council of State Planning Agencies. Washington, DC. 1984
- [43] ADAMEC, Vilém. *Kritická infrastruktura na úrovni územních systémů*. [online]. 22.9. 2014 [cit. 2018-04-17]. Dostupné z: http://www.population-protection.eu/attachments/041_vol4n2_rostek_adamec.pdf

- [44] Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.
- [45] NÚKIB. *Kritická informační infrastruktura: Proces určování podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve znění novely č. 315/2014 Sb.* [online]. 20.3. 2018 [cit. 2018-04-24]. Dostupné z: https://nukib.cz/download/kii-vis/Schema_KII.pdf
- [46] NÚKIB. *Metodika k vodítkům pro hodnocení dopadů* [online]. 20.3. 2018 [cit. 2018-04-24]. Dostupné z: https://nukib.cz/download/kii-vis/Metodika_k_voditkum_pro_hodnoceni_dopadu_NUKIB_v.1.2_s_prilohou.pdf

Seznam obrázků

Obrázek 1: Proces určování podle zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) a nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury ve znění novely č. 315/2014 Sb. [Zdroj: autorka dle [27]] ... 39

Obrázek 2: Časová osa implementace požadavků ZKB ve společnosti. [Zdroj: autorka dle [45]]

Seznam tabulek

Tabulka 1: Přehled použitých zkratk.....	Chyba! Záložka není definována.
Tabulka 2: Přehled legislativních dokumentů.....	Chyba! Záložka není definována.
Tabulka 3: Subjekty před novelou ZKB.....	25
Tabulka 4: Subjekty po novele ZKB	25
Tabulka 5: Přehled přestupků a náležitých pokut [Zdroj: [28]]	Chyba! Záložka není definována.