Vysoká škola ekonomická v Praze

Fakulta informatiky a statistiky

Katedra informačních technologií

Studijní program: Aplikovaná informatika

Obor: Informační systémy a technologie

Zákon o kybernetické bezpečnosti a jeho dopady na povinné subjekty

DIPLOMOVÁ PRÁCE

Student : Bc. Vojtěch Draganov

Vedoucí : RNDr. Igor Čermák, CSc.

Oponent : Mgr. David Hájíček

2016

Prohlášení:

Prohlašuji, že jsem diplomovou práci zpracoval samostatně a že jsem uvedl všechny použité prameny a literaturu, ze které jsem čerpal.

V Praze dne 26. května 2016 .....

Vojtěch Draganov

Poděkování

Děkuji všem, kteří mi pomohli dovést tuto práci i celé studium do cíle. Zejména děkuji vedoucímu práce RNDr. Igoru Čermákovi, CSc. za možnost psát práci na toto zajímavé téma a cenné podněty a připomínky. Také velmi děkuji všem respondentům provedeného průzkumu a jiným, kteří byli ochotni obětovat svůj čas pro to, aby mi poskytli poznatky z praxe, bez kterých by tato práce byla jen shrnutím psaných zdrojů. Děkuji také rodině za podporu a toleranci během celého mého studia.

Abstrakt

Práce zkoumá zákon č. 181/2014 Sb., o kybernetické bezpečnosti (dále „ZKB“) a jeho dopady na povinné subjekty se zaměřením na krajské úřady České republiky. Obsahuje nejprve uvedení do problematiky ZKB a kybernetické bezpečnosti z hlediska státu, z této úrovně se pak přenáší na úroveň organizace. Stěžejním pilířem a přínosem práce je rozbor ZKB s cílem zjištění dopadů tohoto zákona na povinné subjekty a následně na základě tohoto rozboru navrhnout a provést dotazníkový průzkum dopadů ZKB na krajských úřadech ČR. Průzkum se týká organizace a řízení bezpečnosti, zátěže organizace vzniklé v souvislosti se ZKB, ochoty využití finančních prostředků z fondů IROP na opatření ze ZKB, outsourcingu kybernetické bezpečnosti a také názoru pracovníků na tuto legislativu.

Z průzkumu kromě jiného vyplývá, že dotazované krajské úřady, navzdory standardizačnímu tlaku pramenícímu z legislativy, se z hlediska organizace bezpečnosti velmi liší; respondenti se naopak shodli na tom, že zákon o kybernetické bezpečnosti sice znamená pro organizaci významnou administrativní a finanční zátěž, ale také že je dobrým krokem k zajištění lepší bezpečnosti informačních a komunikačních systémů. Z průzkumu také vyplývá, že oblast kybernetické bezpečnosti se na některých úřadech teprve začíná řešit. Tato oblast je nyní ve zkoumaných organizacích velmi dynamická a analýzu dopadů bude vhodné opakovat znovu poté, kdy proběhne první vlna implementace zákona.

Klíčová slova

zákon o kybernetické bezpečnosti, kybernetická bezpečnost, informační bezpečnost, kritická informační infrastruktura, významný informační systém, krajský úřad

Abstract

The thesis looks into the act No. 181/2014 Coll. Cyber Security Act (hereinafter referred to as "CSA") and its impact on obliged entities with focus on the regional authorities of the Czech Republic. The thesis starts with introduction into the issue of the CSA and cybersecurity from the point of view of the state, subsequently it refocuses on the level of regulated organizations.

The main pillar and contribution of the thesis is the CSA analysis with the aim to identify impact of the CSA on the obliged entities. Based on this analysis author designed the questionnaire survey of the CSA impact on the regional authorities. The survey relates to information security management system, kinds of burden stemmed from the CSA implementation, willingness to use funding from the European Regional Development Fund (ERDF) to implement the CSA, a possibility to outsource the cybersecurity and also opinions of the county council staff about the CSA.

The survey shows that in spite of a pressure on standardization stemming from legal framework, county councils differs significantly in regard to information security management systems. On the other hand, respondents agreed on positive impact of the CSA on improvement of information and the cyber security although the CSA brings significant financial and organizational load to the organization. The survey also shows that some regional authorities only start to implement cybersecurity currently. The cybersecurity evolves in the researched organization quite dynamically and it would be beneficial to repeat the impact analyses again, after first wave of the CSA implementation will be finished.

Keywords

Cyber Security Act, cyber security, information security, critical information infrastructure, important information system, regional authority

Obsah

1 Úvod 1

1.1 Úvodní slovo 1

1.2 Vymezení cíle a postupu 2

1.3 Používané zkratky 3

2 Komentovaná rešerše 6

3 Kontext zákona o kybernetické bezpečnosti – základní pojmy kybernetické bezpečnosti 9

3.1 Bezpečnost na úrovni státu (ČR) 9

3.1.1 Krizové stavy 11

3.1.2 Kritická infrastruktura 12

3.2 Kybernetická bezpečnost, bezpečnost informací, kyberprostor 14

3.2.1 Kybernetická bezpečnost nebo bezpečnost informací? 14

3.2.2 CERT/CSIRT pracoviště 19

3.2.3 Vývoj kybernetické bezpečnosti v ČR 21

3.2.4 ZKB v kontextu EU 28

4 Rozbor ZKB a jeho prováděcích předpisů z hlediska dopadů na povinné subjekty 31

4.1 ZKB v kostce – smysl a účel zákona 31

4.1.1 Principy, na kterých je zákon postaven 32

4.1.2 Zákon a prováděcí předpisy 33

4.1.3 Plánovaná novelizace ZKB a vyhlášky č. 317/2014 Sb. 34

4.1.4 Institucionální zajištění, subjekty důležité ve vztahu k ZKB 35

4.2 Proč zákon o kybernetické bezpečnosti 36

4.3 Struktura zákona a vyhlášky č. 316/2014 Sb. 37

4.4 Základní pojmy ZKB 39

4.5 Dotčené subjekty a proces jejich určování 40

4.5.1 Systémy kritické informační infrastruktury a proces jejich určování 42

4.5.2 Významné informační systémy a proces jejich určování 44

4.6 Povinnosti správců systémů KII a VIS vyplývající ze ZKB 48

4.6.1 Bezpečnostní opatření 48

4.6.2 Povinnosti nad rámec bezpečnostních opatření 51

4.6.3 Organizování bezpečnosti a bezpečnostní role podle ZKB 52

4.6.4 Lhůty k plnění povinností 54

4.7 Vybrané aspekty ZKB vzhledem k jeho uplatňování a k průzkumu 55

4.7.1 Finanční podpora – Výzva č. 10 Integrovaného regionálního operačního programu ... 55
4.7.2 ZKB, ISO/IEC 27001 a úroveň bezpečnosti povinných subjektů před ZKB ... 56
4.7.3 Dopad ZKB na obce ... 57
4.7.4 Pomocné materiály od NBÚ ... 58
4.7.5 Stav kybernetického nebezpečí ... 59
4.8 Kritika ZKB ... 60
4.9 Shrnutí dopadů ZKB na povinné subjekty ... 61
4.9.1 Zátěž (administrativní, finanční, personální) ... 61
4.9.2 Úroveň kybernetické bezpečnosti ... 62
4.9.3 Shrnutí otázek vhodných pro průzkum, které vyplynuly z rozboru ZKB ... 63

5 Průzkum kybernetické bezpečnosti na krajských úřadech ... 65
5.1 Cíl a metoda průzkumu ... 65
5.1.1 Shrnutí předmětu a metody průzkumu ... 68
5.2 Sběr dat – dotazník ... 69
5.2.1 Struktura dotazníku – zkoumané oblasti ... 69
5.2.2 Výsledek sběru dat ... 70
5.2.3 Kraje zapojené do průzkumu ... 70
5.3 Průzkum a jeho vyhodnocení ... 71
5.3.1 Řízení kybernetické bezpečnosti a její organizace – dělení ... 71
5.3.2 Blok I – zjištění VIS a systémů KII ... 72
5.3.3 Blok II – kybernetická bezpečnost před ZKB ... 73
5.3.4 Blok III – organizování kybernetické bezpečnosti ... 75
5.3.5 Blok IV – outsourcing ... 78
5.3.6 Zátěž vyplývající ze ZKB na organizaci ... 79
5.3.7 Financování z IROP ... 83
5.3.8 Názory pracovníků na ZKB ... 84
5.4 Celkové shrnutí a zhodnocení průzkumu ... 86
5.4.1 Návrhy pro další výzkum ... 87

6 Závěr ... 89

Seznam literatury ... 91

Seznam tabulek ... 97
Seznam tabulek ... 97

Seznam příloh ... 98

Příloha A: Popis elektronické přílohy ... 99

Příloha B: Dotazník 100

Příloha C: Struktura dotazníku 105

Příloha D: Data získaná z dotazníku 107

D.1 Odpovědi na uzavřené otázky 108

D.2 Odpovědi na otevřené otázky 110

D.3 Komentáře k otázkám 112

Příloha E: Významné informační systémy krajů 117

1 Úvod

1.1 Úvodní slovo

Smrt více než 250 osob, zranění 2500 osob s následnou hospitalizací delší než 24 hodin nebo finanční ztráty v řádu desítek miliard korun. I takové dopady může mít narušení bezpečnosti důležitého informačního či komunikačního systému. Tato čísla jsou dokonce jen spodními hranicemi dopadu[1] potenciálního bezpečnostního incidentu pro to, aby mohl být (za splnění dalších podmínek) dle českých norem informační či komunikační systém zařazen do tzv. kritické informační infrastruktury. V oblasti obchodu pak ztráta či zcizení know-how, citlivých dat, přímé finanční ztráty, ztráta důvěryhodnosti, finančních údajů, nemožnost poskytovat služby a z toho vyplývající důsledky.

Je nesporné, že fungování naší informační společnosti se stává stále více závislé na používání informačních technologií ať už pro ekonomickou činnost nebo osobní život. Bez ohledu na hodnocení správnosti tohoto směřování je nabíledni, že bezpečnost těchto technologií stále více ovlivňuje bezpečnost celé společnosti a to nejen ve fungování ekonomiky, ale také při zaručování základních potřeb, práv a svobod člověka z hlediska státu. Přitom množství i kvalita kybernetických útoků roste, kybernetická zločinnost se profesionalizuje a stala se samostatným odvětvím získávání nelegálních peněz. Stejné prostředky se pak stávají také účinným bojovým nástrojem v rukách světových mocností.

Na jedné straně tedy stále větší závislost na informačních a komunikačních technologiích a na druhé straně rostoucí množství i kvalita kybernetických útoků. Reakce České republiky na tento stav vykrystalizovaly během několika let z původně nekoordinovaných snah různých resortů veřejné správy i soukromého sektoru do podoby poměrně komplexního systému prevence a ochrany vybraných klíčových systémů, který je kodifikován v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti[2] a jeho prováděcích předpisech.

[1] Fakta budou upřesněna dále v práci, zde jen pro ilustraci.

[2] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících předpisů.

1.2 Vymezení cíle a postupu

V předložené práci se věnuji – kromě uvedení základních informací zasazujících problematiku zákona o kybernetické bezpečnosti do kontextu – dopadům této legislativní úpravy na organizace, které mají povinnost mu vyhovět. Protože takových organizací je velké množství a jejich povinnosti se dělí podle toho, pod které písmeno § 3 ZKB[3] spadají, bylo vhodné vzhledem k rozsahu diplomové práce a možnostem autora zaměřit zkoumání na určitou a pokud možno homogenní skupinu organizací. Jako taková skupina byly vybrány krajské úřady (dále také jako „KrÚ“), neboť jsou součástí veřejné správy, vykonávají podobnou agendu (stejná kompetence a působnost [1]) a dalo se předpokládat, že spravují téměř výlučně významné informační systémy[4] dle zákona o kybernetické bezpečnosti.

Cílem práce bylo nejprve provést rozbor ZKB za účelem zjištění dopadů tohoto zákona na povinné subjekty a následně na základě tohoto rozboru pak navrhnout a provést dotazníkový průzkum, který ověří zjištěné dopady na krajských úřadech ČR a zjistí základní fakta o stavu kybernetické bezpečnosti na těchto úřadech.

Vedlejším cílem je dále také uvedení základních informací o české legislativě kybernetické bezpečnosti, vzniku zákona o kybernetické bezpečnosti a jeho kontextu.

Smyslem tohoto průzkumu je odpovědět na otázky vzniklé na základě rozboru ZKB z hlediska dopadů na povinné subjekty a tím zjištění základních faktů o stavu kybernetické bezpečnosti na krajských úřadech z hlediska řízení bezpečnosti, jejího organizačního začlenění, zátěže vyplývající ze ZKB na organizaci, ochotu využití možnosti financování z integrovaného regionálního operačního programu, možnost outsourcingu kybernetické bezpečnosti a také zjištění subjektivních názorů dotazovaných pracovníků na ZKB jako takový.

Vzhledem k charakteru řešené problematiky je využito zejména metod kvalitativního výzkumu. Při vyhodnocení dotazníku totiž nemělo smysl využívat pokročilé matematické či statistické metody, neboť tyto nad takto malou cílovou skupinou (14 krajů) nemají smysl. V dotaznících byl také ponechán značný prostor k libovolnému vyjádření dotazovaných formou volitelných komentářů ke každé z uzavřených[5] otázek.

Pro zjištění aktuálního stavu „v terénu“ jsem využil také metodu polostrukturovaného rozhovoru. Polostrukturovaný byl zvolen z toho důvodu, aby se mohl rozhovor přirozeně vyvíjet a dostat se tak i k otázkám, jež nebyly dopředu formulované. Každý z dotazovaných pracovníků navíc řeší problematiku z jiné pracovní pozice, s jiným

[3] K tomu viz kap. 4.5 Dotčené subjekty.

[4] K tomu také tamtéž.

[5] Tj. pouze výběr z několika daných variant.

profesionálním backgroundem a tím je také dán odlišný přístup k věci a poukazuje to na vhodnost hovoru méně svázaného striktně danou posloupností dotazů.

Značná část práce je tvořena také pomocí rešeršní činnosti, kde jako zdroje dat slouží kromě dostupné literatury a právních předpisů zejména online prameny jako oficiální stránky NBÚ, národního CERT, dále pak materiály z konferencí, dostupné prezentace a v neposlední řadě i články z běžných zpravodajských či profesně zaměřených magazínů. K vyhledání informací v českém tisku a médiích posloužil kromě vyhledávače Google také systém Anopress IT, který je pro studenty VŠE k dispozici. K právním normám jsem přistupoval skrze Portál veřejné správy, kde jsou dostupná aktuální znění zákonů z informačního systému ASPI, a také právní systém Fulsoft, taktéž dostupný v rámci služeb knihovny VŠE.

Za účelem zjištění aktuálních informací ve zkoumané oblasti jsem také navštívil blok Kybernetická bezpečnost na konferenci ISSS 2016 (Internet ve Státní Správě a Samosprávě) konané 4–5. dubna 2016 v Hradci Králové.

1.3 Používané zkratky

Na následujících řádcích jsou vysvětleny zkratky používané v této práci:

Zkratka	**Popis**
CERT	Computer Emergency Response Team
CSIRT	Computer Security Incident Response Team
č.	číslo (při odkazu na právní předpisy)
ČR	Česká republika
ENISA	Agentura Evropské unie pro bezpečnost sítí a informací
EU	Evropská unie
HW	hardware
IS	informační systém
ISMS	integrovaný systém řízení bezpečnosti
ISO	International Organization for Standardization – mezinárodní organizace pro standardizaci
ISVS	Informační systémy veřejné správy
KI	kritická infrastruktura (dle krizového zákona)

KII	kritická informační infrastruktura (dle zákona o kybernetické bezpečnosti)
KrÚ	krajský úřad
MV	Ministerstvo vnitra
NATO	Severoatlantická aliance
NBÚ	Národní bezpečnostní úřad
NCKB	Národní centrum kybernetické bezpečnosti
OVM	orgán veřejné moci
RKB	Rada pro kybernetickou bezpečnost
Sb.	Sbírka zákonů České republiky
SW	software
TERENA	Trans-European Research and Education Networking Association
ÚOOÚ	Úřad pro ochranu osobních údajů
VIS	významný informační systém

Níže je uvedena tabulka s používanými zkratkami legislativních dokumentů:

Tabulka č. 1: *Zkratky legislativních dokumentů*

Zkratka	**Alt. zkr.**	**Popis**
Ústava	–	ústavní zákon č. 1/1993 Sb., Ústava České republiky
krizový zákon	–	zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)
zákon č. 365/2000 Sb.	zákon o ISVS	zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
nařízení vlády č. 432/2010	–	nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
směrnice NIS	NIS	návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti síťových a informačních systémů COM/2013/048 final
nařízení vlády č. 315/2014 Sb.	–	nařízen vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
vyhláška č. 316/2014	VKB	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)
vyhláška č. 317/2014	VVIS	vyhláška č. 317/2014 Sb., o o významných informačních systémech a jejich určujících kritériích
zákon č. 181/2014 Sb.	ZKB, zákon	zákon č. 181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Všechny citované právní předpisy jsou citované *ve znění pozdějších předpisů* a to do dne 1.4.2016, pokud není uvedeno jinak.

2 Komentovaná rešerše

V této kapitole shrnuji současný stav zpracování problematiky zákona o kybernetické bezpečnosti v literatuře a odborných pracích, zejména pak v pracích vysokoškolských kvalifikačních. Pro vyhledání relevantních kvalifikačních prací pro rešerši jsem využil především systém theses.cz provozovaný fakultou informatiky Masarykovy university v Brně. Pro vyhledání dalších odborných prací, i jiných než kvalifikačních, jsem použil vyhledávací službu Google Scholar a dále také běžné vyhledávání Googlu.

Kvalifikační práce

Na základě průzkumu dostupných zdrojů se tématu Zákona o kybernetické bezpečnosti přímo zatím mnoho kvalifikačních prací nevěnovalo, případně se autoři věnovali některým konkrétním oblastem jako např. CERT/CSIRT týmy, implementací ISMS[6] do konkrétní organizace státní správy či podniku, dopady ZKB na Integrovaný záchranný systém apod. Většina nalezených prací z oblasti kybernetické bezpečnosti se zabývá implementací požadavků ZKB z hlediska řízení bezpečnosti informací navázaných na ISO/IEC 27000. Některé (většina) se věnují více technickým otázkám jako síťové prvky a SW nástroje k podpoře ZKB a některé více organizačním. Nalezl jsem také kvalitní práce rozebírající kybernetickou kriminalitu z hlediska právní teorie z Masarykovy univerzity a nebo práci zaměřenou na vzdělávání v kybernetické bezpečnosti. Níže uvádím některé z prací a jejich zaměření:

PŠEJA, Jan. *Implementace požadavků kybernetické bezpečnosti do specifického prostředí lokální sítě veřejné správy.*[7]

> Tato práce se zabývá implementací bezpečnosti do lokální sítě městského úřadu Kroměříž, zkoumá nejprve povrchně bezpečnost v obcích Zlínského kraje a detailně se pak zabývá řešením zabezpečení zmíněného městského úřadu na organizační a zejména technické úrovni. Vzhledem k tomu, že obce jsou z působnosti ZKB vyjmuté, neřeší zde autor specifické požadavky (nad rámec standardní informační bezpečnosti) vyplývající ze zákona pro povinné osoby jako je komunikace s CERT a povinnosti provádět opatření při stavu kybernetického nebezpečí.

---

[6] Integrated Security Management System (integrovaný systém řízení bezpečnosti)

[7] PŠEJA, Jan. *Implementace požadavků kybernetické bezpečnosti do specifického prostředí lokální sítě veřejné správy.* [online]. Zlín, 2015. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Dostupné z: http://hdl.handle.net/10563/34132

PÍŠA, Jan. *Implementace kybernetické bezpečnosti a normy ISO 27000 ve státní správě.*[8]

V práci autor analyzuje bezpečnost v prostředí konkrétního úřadu státní správy s více než 1400 pracovníky, z bezpečnostních důvodů však neuvádí, který to je. Zaměřuje se zejména na fyzickou bezpečnost objektu a síťovou infrastrukturu s použitím konkrétního nástroje. Samotný ZKB rozebírá podrobněji, než předchozí výše zmíněná práce. Opět zde není prostor věnovaný požadavkům ZKB nad rámec ochrany perimetru.

STRÁNSKÝ, Tomáš. *Bezpečnost podnikové IT infrastruktury a implementace ISO 27000.*[9]

Předmětem práce je především analýza rizik a návrh vhodných opatření v konkrétním podniku v souladu s ISO/IEC 27000. Nezabývá se zvláštními požadavky ZKB nad rámec bezpečnostních opatření.

GERŽA, Michal. *Návrh implementace bezpečnostní politiky v informačním systému veřejné správy.*[10]

Tato práce především navrhuje postup implementace bezpečnostní politiky pro městský úřad. Problematika je probírána ze široka, mapuje využití a provázanost informačních technologií v oblasti veřejné správy ČR, pojednává o projektech e-governmentu, obecně o řízení bezpečnosti informací, v praktické části se pak zabývá informační strategií, informační koncepcí, bezpečnostní politikou. Vazbami bezpečnosti na ZKB se věnuje spíše okrajově, nevěnuje se specifickým požadavkům nad rámec bezpečnostních opatření, neboť obce tyto povinnosti nemají.

KRATOCHVÍL, David. *Kybernetická bezpečnost a legislativa ČR.*[11]

---

[8] PÍŠA, 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

[9] STRÁNSKÝ, Tomáš. *Bezpečnost podnikové IT infrastruktury a implementace ISO 27000* [online]. Česká Třebová, 2015. Diplomová práce. Univertiza Hradec Králové, Fakulta informatiky a managementu. Dostupné z: https://theses.cz/id/q88diy/STAG64823.pdf

[10] GERŽA, Michal. *Návrh implementace bezpečnostní politiky v informačním systému veřejné správy* [online]. Zlín, 2015 [vid. 17. březen 2016]. Diplomová práce. Univerzita Tomáše Bati ve Zlíně, Fakulta aplikované informatiky. Dostupné z: https://stag.utb.cz/StagPortletsJSR168/KvalifPraceDownloadServlet?typ=1&adipidno=39644

[11] KRATOCHVÍL, David. Kybernetická bezpečnost a legislativa ČR [online]. Praha, 2013 [vid. 16. březen 2016]. Diplomová práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky. Dostupné z: http://isis.vse.cz/lide/clovek.pl?zalozka=13;id=567;studium=121730;download_prace=1

> Tato práce se zaměřuje obecně na kybernetickou kriminalitu a následně analyzuje legislativu v ČR týkající se kybernetické bezpečnosti a také věcný návrh Zákona o kybernetické bezpečnosti. Protože práce byla obhájena roku 2013, nebylo ještě možné analyzovat platné paragrafové znění zákona a ani to, jakým způsobem zákon na povinné subjekty bude dopadat ve skutečnosti.

Problematika CERT/CSIRT týmů, týkající se ZKB je rozebrána v bakalářské práci Dominiky Rezníčkové:

REZNÍČKOVÁ, Dominika. CERT / CSIRT tímy a kybernetická bezpečnosť.[12]

> Tato práce se věnuje kybernetické bezpečnosti v ČR a zejména jejímu důležitému aspektu – CERT/CSIRT týmům. Autorka nabízí náhled do fungování CSIRT.CZ tj. CSIRT týmu, který provozuje sdružení CZ.NIC na základě informací poskytnutých tamními pracovníky.

Odborné práce MU Brno

Problematice kybernetické bezpečnosti se především po právní stránce na špičkové úrovni věnuje Ústav práva a technologií při právnické fakultě Masarykovy Univerzity v Brně pod vedením Doc. JUDr. Radim Polčáka, PhD. Tento ústav vydává svůj odborný časopis, kde se vyskytují příspěvky na toto téma např.:

HARAŠTA, Jakub. *Právní aspekty kybernetické bezpečnosti ČR.*[13]

POLČÁK, Radim. *Kybernetická bezpečnost jako aktuální fenomén českého práva*.[14]

R. Polčák také vydal knihu Internet a proměny práva[15], kde se mimo jiné zabývá i kybernetickou bezpečností a to především z hlediska právní teorie a filozofie.

---

[12] REZNÍČKOVÁ, Dominika. *CERT / CSIRT tímy a kybernetická bezpečnosť* [online]. Praha, 2015. Diplomová práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky. Dostupné z: https://www.vse.cz/vskp/id/1267824

[13] HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti ČR. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy* [online]. roč. 4, č. 8/2013. ISSN 1805-2797. Dostupné z: https://journals.muni.cz/revue/article/download/2980/R_2015_11_TEMA_Polčák_v2.

[14] POLČÁK, Radim. Kybernetická bezpečnost jako aktuální fenomén českého práva. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy* [online]. roč. 6, č. 11/2015. ISSN 1805-2797. Dostupné z: https://journals.muni.cz/revue/article/download/2980/R_2015_11_TEMA_Polčák_v2.

[15] POLČÁK, Radim. Internet a proměny práva. Téma. Praha: Auditorium, 2012. ISBN 978-80-87284-22-3.

3 Kontext zákona o kybernetické bezpečnosti – základní pojmy kybernetické bezpečnosti

Účelem této kapitoly je uvedení kontextu, ve kterém zákon o kybernetické bezpečnosti vznikl a ve kterém se nachází. Jsou tu uvedeny základní pojmy z oblasti týkající se bezpečnosti České republiky, na které zákon o kybernetické bezpečnosti navazuje, dále se tato kapitola zabývá institucionálním zajištěním kybernetické bezpečnosti ČR a také základními pojmy z oblasti bezpečnosti informací, otázkou kybernetické bezpečnosti a jejímu vývoji v ČR.

3.1 Bezpečnost na úrovni státu (ČR)

V této kapitole jsou vysvětleny základní pojmy z široké oblasti bezpečnosti státu vybrané s ohledem na téma práce tj. legislativně-právní prostředí krizového managementu v ČR, kritická infrastruktura a krizové stavy.

Zákon o kybernetické bezpečnosti zapadá do kontextu českého systému bezpečnosti a krizového řízení. To nelze opomenout, neboť na normy tohoto systému v několika ohledech navazuje a upravuje tak kromě dalších dílčích předpisů jeho specifickou část zaměřenou na kybernetickou bezpečnost. Proto je nejprve pojednáno obecně o bezpečnosti státu a jejím systému z hlediska institucionálního a legislativního zajištění.

Bezpečnost (státu) jako takovou lze charakterizovat různými více či méně vágními způsoby. Pojem není jednotně vymezen v legislativě ani odborné literatuře. Z teoretického hlediska se dá bezpečnost charakterizovat jako „*systémový fenomén, základem kterého je absence vojenské hrozby, zajištění svrchovanosti, územní celistvosti a demokratických základů státu, úsilí o zajištění politického a společenského sebeurčení, ekonomické prosperity a blahobytu státu.*“ [2 s. 226] Publikace [2] dále nabízí několik dalších pohledů na věc. Méně teoreticky lze bezpečnost charakterizovat pojmy jako „*stabilita, určitost, pořádek, spolehlivost, rovnováha, existence (život) jedince či společnosti bez hrozeb, stav a pocit jistoty*“. [2] Stanovení objektivní míry bezpečnosti a (ne)možnost její kvantifikace je složitou otázkou[16]. Bezpečnost státu se liší podle zaměření na *vnější* a *vnitřní* [17]. V dnešní době jsou hranice těchto kategorií rozmlžené a často splývají. Tak je tomu i u

[16] Pro detailněji zpracovanou problematiku bezpečnosti, krizového managementu a přehled legislativy v této oblasti odkazuji na publikaci [2] (ANTUŠÁK, Emil. *Krizový management: hrozby – krize – příležitosti.* Vyd. 1. Praha: Wolters Kluwer Česká republika, 2009. ISBN 978-80-7357-488-8.)

[17] K tomu více v [3 s. 13] a [4].

otázky kybernetické bezpečnosti (viz dále), kde hrozby přicházejí jak zvenčí, tak zevnitř. Pokud je bezpečnost ohrožena nebo narušena, nastává mimořádná či krizová situace (3.1.1 Krizové stavy).

Česká republika k zajišťování své bezpečnosti vytváří a rozvíjí komplexní systém, který propojuje různé roviny fungování státu (politické, vojenské, hospodářské, právní a sociální aj.) Základ tohoto systému tvoří legislativní vyjádření vzájemných vazeb a působností jednotlivých složek státu (zákonodárná, výkonná a soudní moc, územní samosprávy, právnické a fyzické osoby), jejich povinnosti a také vazby směřující mimo tento systém. Funkční bezpečnostní systém kromě úspěšného zvládání již nastalých krizových situací funguje zejména preventivně přípravou na takové situace, jejich včasnou identifikaci a varováním. [5]

Zajistit bezpečnost svých občanů a zachování státní suverenity jsou základní povinnosti státu a jako takové jsou garantované na nejvyšší úrovni Ústavou (ústavní zákon č. 1/1993 Sb., Ústava ČR) a ústavními zákony:

- ústavní zákon č. 110/1998 Sb., o bezpečnosti ČR,
- ústavní zákon č. 300/2000 Sb., změna Ústavy a ústavního zákona č. 110/1998 Sb.,

na které pak navazuje na nižší úrovni právní síly krizová legislativa tvořená zákony a jejich prováděcími předpisy či jinými podzákonnými předpisy např.:

- zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon),
- zákon č. 222/1999 Sb., o zajišťování obrany ČR,
- zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy,
- zákon č. 239/2000 Sb., o integrovaném záchranném systému

a množství dalších[18]. Do tohoto výčtu je dle mého soudu nyní možné zařadit právě i zákon č. 181/2014 Sb., o kybernetické bezpečnosti, jež je předmětem této práce.

Pro fungování bezpečnostního systému jsou zásadní tyto ústřední orgány státu:

- prezident republiky,
- Parlament ČR,
- Vláda,
  - v rámci vlády Bezpečnostní rada státu a její pracovní orgány,
- ministerstva a další ústřední orgány státní správy.

[18] výčet např. v [2]

Vláda jakožto ústřední výkonný orgán státní moci je výkonným orgánem bezpečnostního systému ČR a je odpovědná za jeho funkčnost. Důležitá je její klíčová role ve vydávání nařízení a usnesení k příslušným zákonům a projednává a navrhuje právní předpisy, strategie a koncepce. Zřejmě nejdůležitějším strategickým dokumentem vydávaným vládou ve spolupráci s Kanceláří prezidenta republiky a Parlamentem ČR je bezpečnostní strategie, jež je základním dokumentem bezpečnostní politiky ČR na který pak navazují další strategie a koncepce [5] včetně dokumentů týkajících se kybernetické bezpečnosti.

Orgány uvedené výše v poslední odrážce – tedy ministerstva a jiné ústřední orgány státní správy – mohou na základě zákonného zmocnění vydávat předpisy k upřesnění postupů a realizaci opatření. [3] Toto je velmi podstatné i pro systém zajištění kybernetické bezpečnosti. NBÚ je totiž ústředním orgánem státní správy podle zákona č. 2/1969 Sb., který v rámci kybernetické bezpečnosti má takové kompetence.

Pro další pokračování v pojednání o bezpečnosti je podstatné vymezit zásadní pojmy řízení bezpečnosti (obecné i informační – o té dále v práci) a těmi jsou **hrozba** a **riziko**. Definic je možné najít mnoho, vybral jsem následující:

Hrozba (treat) *„je libovolný subjekt, jenž svým působením (činností) může poškodit nebo zničit konkrétní chráněnou hodnotu nebo zájem jiného subjektu (tzv. hrozba intencionální) nebo jev či událost jako bezprostřední příčina poškození nebo zničení konkrétní chráněné hodnoty nebo zájmu (tj. tzv. hrozba neintencionální).*“ [2 s. 48]

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.*“ [2 s. 48]

Asymetrické hrozby jsou charakteristické použitím takových prostředků a způsobů jednání ze strany protivníka, kterým nelze stejným způsobem čelit. Definice se různí, podstatné je *použití nekonvenčních prostředků* a *dosažení neúměrně velkého efektu*. Zmiňováno je také postavení obou stran – asymetrický útok použije zpravidla slabší protistrana, protože nemá prostředky pro přímou konfrontaci se silnějším protivníkem. [2] Asymetrickou hrozbou mohou být i útoky na kritickou infrastrukturu skrze kyberprostor.

3.1.1 Krizové stavy

Pokud se situace vyvíjí tak, že již není možno ji řešit standardními prostředky, eskalací hrozeb dochází ke krizové situaci, nastupují mimořádná řešení v podobě krizových stavů. Krizový stav je zvláštní právní kategorií umožňující státu použít v mimořádné situaci mimořádné prostředky – tzn. omezit za účelem odvrácení nebezpečí práva a svobody a nařizovat povinnosti nad standardní míru (§ 5–7 krizového zákona). Krizový

stav nenastane sám od sebe eskalací hrozeb, ale musí být vyhlášen. [2] V České republice máme tyto krizové stavy:

- stav nebezpečí (vyhlašuje hejtman kraje, nevojenský stav),
- nouzový stav (vyhlašuje vláda ČR, nevojenský stav),
- stav ohrožení státu (vyhlašuje parlament ČR, vojenský stav),
- válečný stav (vyhlašuje parlament ČR, vojenský stav).

Stav nebezpečí je (jediným) krizovým stavem na úrovni kraje, další tři jsou celostátní. Nouzový stav a stav ohrožení ale může být vyhlášen i na omezeném území. [6] Kromě těchto „základních" stavů lze v české legislativě najít ještě dále stavy nouze pro oblast průmyslové bezpečnosti (stav nouze v elektroenergetice, v plynárenství, v teplárenství) a také stav nouze v devizovém hospodářství (zákon č. 219/1995 Sb. [7]).

K výše zmíněným krizovým stavům se způsobem vyhlašování nyní může zařadit i *stav kybernetického nebezpečí* podle ZKB. Protože se však přímo nedotýká práv a povinností občanů, nejedná se o zvláštní stav s obecnou a věcnou působností, tedy vztahuje se jen na okruh subjektů a vztahů, na které běžně dopadá ZKB, není vhodné jej upravovat v krizovém zákoně. [8] Svým charakterem je tedy spíše podobný stavům nouze v oblasti průmyslové bezpečnosti a stavu nouze v devizovém hospodářství. Více ke stavu kybernetického nebezpečí viz kap. 4.7.5 Stav kybernetického nebezpečí.

3.1.2 Kritická infrastruktura

Čím je civilizace technicky vyspělejší a závislejší na svých technologiích, tím se stává skrze tyto technologie také zranitelnější. Infrastruktura dnešního moderního státu je tvořena především vzájemně provázanými technologiemi a jejich zranitelnost tak znamená zranitelnost infrastruktury. Některé části infrastruktury jsou pro řádné fungování státu a společnosti natolik klíčové, že by jejich narušení znamenalo velmi vážnou újmu státu a jeho občanům. Tyto klíčové součásti infrastruktury se státy přirozeně snaží chránit a nazývají se kritickou infrastrukturou (dále „KI"). „*Ohrožení funkčnosti kritické infrastruktury*" je i jednou z jedenácti bezpečnostních hrozeb, které přímo vyjmenovává aktualizovaná Bezpečnostní strategie ČR z roku 2015, přičemž je zde zmiňována i souvislost s kybernetickými útoky. [5]

Podle krizového zákona se kritickou infrastrukturou rozumí „*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*". [9]

Tlak na ochranu prvků kritické infrastruktury, na ČR vyplývá i z členství v EU, ta se snaží koordinovat společnou politiku ochrany kritické infrastruktury. Zaměřuje se

kromě ochrany KI členských států i na ochranu kritické infrastruktury, která je svým významem klíčová pro celé evropské společenství. Diskuse na půdě evropských institucí se projevily mj. ve *Směrnici Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu*. Krizový zákon implementuje tuto směrnici do legislativy ČR, proto je v něm vymezena mj. i evropská kritická infrastruktura, jejíž narušení by mělo závažný dopad na jiný členský stát EU. Na krizový zákon navazuje *nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury*, kde jsou popsána tzv. odvětvová a průřezová kritéria, která musí prvek splňovat, aby se mohl stát součástí kritické infrastruktury. Takovým prvkem může být stavba, zařízení, prostředek nebo veřejná infrastruktura tj. součásti dopravní infrastruktury, energetická zařízení aj.

Aby mohl být prvek či systém určen jako součást kritické infrastruktury, musí nejprve naplnit definici kritické infrastruktury a prvku kritické infrastruktury (dané krizovým zákonem). Potom musí splnit další kritéria, která se dělí, jak bylo zmíněno výše, na průřezová a odvětvová. Průřezová kritéria jsou obecná kritéria platící pro všechna odvětví a posuzují závažnost vlivu způsobeného narušením funkce prvku kritické infrastruktury tzn. ztráty na životech, dopad na zdraví osob, vážný ekonomický dopad aj[19]. Odvětvová kritéria určují technické či provozní hodnoty specifické pro konkrétní odvětví. Např. v oblasti energetiky a výroby elektřiny minimální megawattový výkon elektrárny nebo v jiném odvětví počet lidí, které zásobuje nenahraditelný vodní zdroj apod. Pro určení prvku jako součásti kritické infrastruktury je nutné, aby systém naplnil alespoň jedno z průřezových kritérií a alespoň jedno z odvětvových kritérií. Pokud splní všechny výše zmíněné podmínky, stále ještě není automaticky součástí kritické infrastruktury. Musí být ještě oficiálně určen příslušným úřadem, pak je teprve zařazen do kritické infrastruktury. Výše zmíněné platí stejně pro kritickou informační infrastrukturu, se kterou pracuje ZKB. Tj. pro proces určování orgánů a osob spadajících dle ZKB pod § 3 písm. c) a d).

V postupu pro určování prvků existuje odlišnost na základě toho, zda jejich provozovatelem je či není organizační složka státu. Prvky, které provozuje organizační složka státu, musí určit vláda. Ty prvky, které neprovozuje organizační složka státu, určuje příslušný ústřední správní úřad (ministerstva a další úřady vyjmenované v kompetenčním zákoně tj. zákon č. 2/1969 Sb., případně jiné). Vztaženo k ZKB: v případě, že orgán nebo osoba dle § 3 písm. c) a d) je organizační složkou státu (např. ministerstva[20] a další úřady), je prvek informační infrastruktury určen usnesením vlády. V ostatních případech, kdy se jedná o soukromoprávní subjekt, je tento prvek určen opatřením obecné povahy.

---

[19] Přesně vymezeno v § 2 odst. l) krizového zákona [9]

[20] Velké množství těchto prvků provozuje Ministerstvo vnitra.

Na základě *nařízení vlády č. 315/2014 Sb.,* které bylo publikováno souběžně se ZKB a aktualizuje výše zmíněné nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, se v odvětvových kritériích pod odvětvím *VI. komunikační a informační systémy* objevuje nově kategorie *G. Oblast kybernetické bezpečnosti*, na kterou se odkazuje definice kritické informační infrastruktury v ZKB.

3.2 Kybernetická bezpečnost, bezpečnost informací, kyberprostor

Tato kapitola uvádí základní pojmy z oblasti bezpečnosti informací, kybernetické bezpečnosti a diskutuje rozdíl mezi bezpečností informací a kybernetickou bezpečností. Pojednává také o vývoji kybernetické bezpečnosti v ČR a mezinárodní spolupráci ČR na poli kybernetické bezpečnosti.

3.2.1 Kybernetická bezpečnost nebo bezpečnost informací?

V této části diskutuji pojetí kybernetické bezpečnosti („kyberbezpečnosti“) a vztahu tohoto pojmu k bezpečnosti informací a zákonu o kybernetické bezpečnosti.

Dobře definované pojmy jsou základem dobrého dorozumění. V oblasti ICT je to ale úkol dosti nesnadný, neboť – jak poznamenávají autoři Výkladového slovníku kybernetické bezpečnosti – se velmi dynamicky rozvíjí, neustále se objevují nové termíny a také vznikají mnohé duplicity a to i v kmenovém jazyce oboru – angličtině. [10] Jsem přesvědčen, že pokus o přesnou definici výše zmíněných pojmů nebo spíše zpracování možných variant by vydalo na samostatnou diplomovou práci. Pro základní orientaci v termínech je vhodný Výkladový slovník kybernetické bezpečnosti, [10] ve kterém se autoři snažili shrnout a definovat nejpoužívanější pojmy z oblasti kybernetické bezpečnosti. Aktuální je třetí vydání z roku 2015. Vzhledem k tomu, že předmětem práce je zákon o kybernetické bezpečnosti, je rozumné především pracovat z termíny vycházejícími z tohoto zákona.

Nejprve k samotnému pojmu bezpečnosti. Bezpečnost lze definovat různými způsoby. Lze ji chápat jako cílový stav a také jako souhrnný pojem pro označení souboru opatření, metod a nástrojů k zajištění stavu, který je bezpečný. Protože stoprocentní bezpečnost je možná pouze teoreticky, bylo by lépe říci k zajištění stavu, kde jsou rizika snížena na akceptovatelné minimum za vynaložení akceptovatelných prostředků. Ve slovníku [10] je bezpečnost definována jako „*Vlastnost prvku (např. informační systém), který je na určité úrovni chráněn proti ztrátám, nebo také stav ochrany (na určité úrovni) proti ztrátám.*“ Dále pokračuje: „*Bezpečnost IT zahrnuje ochranu důvěrnosti, integrity a dosažitelnosti při zpracování, úschově, distribuci a prezentaci informací.*“

Ve výše uvedené definici bezpečnosti IT se objevují tři zásadní pilíře (nebo také aspekty) informační bezpečnosti známé jako princip C.I.A. – tedy důvěrnost (confidentiality), integrita (integrity), dostupnost (availability). Jednoduše řečeno, důvěrnost je aspekt zaručující, že k informaci se dostanou pouze osoby, které jsou k tomu oprávněné. Pokud je naplněn aspekt *důvěrnosti*, informace nebude vyzrazena. Technicky vzato se týká operací čtení (read). *Integrita* je zaručením ochrany proti nežádoucím změnám informace. Pokud je aspekt integrity naplněn, informace nemůže být neoprávněně změněna. Z technického pohledu se jedná o ochranu proti neoprávněnému zápisu (write). *Dostupnost* znamená, že informace je k dispozici tehdy, kdy je oprávněnou osobou potřeba. Dosažení úplného naplnění těchto třech aspektů je možné pouze v teorii. Při uplatnění tohoto principu v praxi jde o vybalancování požadované důvěrnosti, integrity a dostupnosti. Ne pokaždé je totiž potřeba dávat stejný důraz na všechny tři aspekty. Zvyšování úrovně bezpečnosti v kterémkoli z nich totiž přirozeně zvyšuje náklady ať už finanční nebo v podobě administrativní zátěže.

Bezpečnost informací je ve výše zmíněném slovníku definována nejprve velmi prostě a široce jako „*zachování (ochrana) důvěrnosti, integrity a dostupnosti informací*“, [10] tedy pomocí výše zmíněných aspektů informační bezpečnosti. Tato slovníková definice se nezabývá kontextem ani prostředky k dosažení této bezpečnosti a kopíruje definici v ZKB (§ 2 písm. c). Hned dalším heslem ve slovníku je „*Bezpečnost informací / informačních systémů*“, doplněno zkratkou „INFOSEC“, která je o mnoho konkrétnější a tím pádem také delší: „*Uplatnění obecných bezpečnostních opatření a postupů sloužících: (1) k ochraně informací před jejich ztrátou nebo kompromitací (ztráta důvěrnosti, integrity, a dalších vlastností jako např. autentičnost, odpovědnost, nepopíratelnost a spolehlivost), případně k jejich zjištění a přijetí nápravných opatření. (2) k zachování dostupnosti informací a schopnosti s nimi pracovat v rozsahu přidělených oprávnění. Opatření INFOSEC zahrnují bezpečnost počítačů, přenosu, emisí a šifrovací bezpečnost a odhalování ohrožení skutečností a systémů a jeho předcházení.*“

Pojmy bezpečnost a informační bezpečnost jsou již nastíněné. Než přejdu ke kybernetické bezpečnosti, je vhodné ještě rozebrat pojem kybernetický prostor neboli kyberprostor. Vymezení tohoto pojmu je základem pro vymezení pojmů jako kybernetická bezpečnost, kybernetická kriminalita, kyberterorismus atd. Vymezit tento pojem může být komplikovanější, než u předchozích uvedených. Výkladový slovník kybernetické bezpečnosti, který zde používám jako referenční zdroj uvádí, že kybernetický prostor je „*Digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací.*“ [10] Uvádí tedy také definici dle zákona o kybernetické bezpečnosti, stejně jako u bezpečnosti informací. Zřejmě proto, aby nevnášel do českého prostředí větší pojmovou nekonzistenci. Tato definice je poměrně pragmatická, lze ale klást otázky např. zda je nutné omezovat ochranu pouze na digitální prostředí. Např. analogový telefonní hovor nebo analogová data by tak byly vyčleněny. Jak vidno např. podle [11 s. 453], o šířce

definice v zákoně se diskutovalo a v čase se vyvíjela. Původně definice zahrnovala podmínku připojení k veřejné síti, což bylo zbytečně omezující, protože velké množství důležitých informací a aktiv se pohybuje na neveřejných sítích (privátní sítě oddělené od internetu jako např. některé sítě Ministerstva vnitra ČR nebo různé řídicí sítě v energetice apod.) V [11 s. 453] se navrhuje o něco širší vymezení: „*Kybernetickým prostorem se rozumí prostředí tvořené informačními systémy a službami a sítěmi elektronických komunikací.*“ Zde tedy oproti předchozí chybí podmínka digitálního prostředí a zpracování a výměna informací.

Kybernetická bezpečnost: „*Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru.*“ [10] Tato definice je poněkud obecná, je z ní možno vyčíst, že se jedná o ochranu za pomocí nejrůznějších prostředků, je zde patrný důraz i na lidské aspekty (organizace a vzdělávání). Nespecifikuje proti čemu má být kybernetický prostor chráněn. Aby bylo možné lépe posoudit, co je kybernetická bezpečnost, je nutné také vědět, co jsou kybernetické hrozby, tedy proti čemu má kybernetická bezpečnost chránit. Na obecnější úrovni lze říci, že se může jednat kromě úmyslných útoků také o lidskou chybu[21], přírodní událost a nebo technické selhání. [12]

Je rozdíl, pokud jde o úmyslné útoky, zda je útok prováděn konvenčními prostředky (míním prostředky způsobující mechanické poškození jako jsou trhaviny nebo přímé mechanické poškození) na fyzické systémy (hardware) s cílem poškodit kyberprostor (např. přerušení vedení nebo mechanické poškození serveru za účelem odstavení určité elektronické služby apod.) a nebo je útok prováděný přímo z kyberprostoru se stejným cílem. Ještě jiná situace nastane při útoku prostřednictvím kyberprostoru s cílem poškodit fyzické zařízení (útok na SCADA[22] systémy nebo jiné průmyslové systémy). Příkladem by byl dnes již velmi známý případ speciálního malware Stuxnet, který cílil na PLC[23] kontroléry od Siemensu a pravděpodobně tak zničil některá zařízení Írán-

[21] Jako příklad lze uvést poškození transkontinentálních podmořských kabelů v roce 2008, které ovlivnilo na 60% z 50 milionů uživatelů Internetu v Indii a další v jiných zemích. Pravděpodobnou příčinou byl tanker, který za sebou táhl kotvu mořským dnem. [19] Narušení takových kabelů by ale mohl být i úmyslný útok.

[22] Supervisory Control And Data Acquisition (systémy supervizního řízení a sběru dat) – „*Systém shromažďující v reálném čase data z čidel v provozu a posílající je na centrální počítač pro další zpracování a řízení.*“ Používají se ve většině rozsáhlejších průmyslových procesech. [13]

[23] Programmable Logic Controller (programovatelný logický automat) – používá se v průmyslové automatizaci.

ského jaderného programu. [14] Přesto, že do výše zmíněné definice kybernetické bezpečnosti se vejdou všechny tři varianty, fyzický útok např. na důležitý komunikační uzel by pravděpodobně jen málokdo nazval kybernetickým útokem.

Za zajímavý může být považován fakt, že pojem kybernetické bezpečnosti není zákonem o kybernetické bezpečnosti vymezen. Nepřímo lze však vymezení zjistit na základě vymezení kybernetické bezpečností události a kybernetického bezpečnostního incidentu. Kybernetickou bezpečnostní událost chápe ZKB jako „*událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací*[24].“ Z toho se dá usoudit, že kybernetická bezpečnost se týká bezpečnosti informací, služeb a sítí. To poměrně dobře odpovídá definici kybernetického prostoru uvedené v ZKB i v [10] (tedy vymezení kybernetického prostoru pomocí informačních systémů, služeb a sítí.)

Nutno podotknout, že definice kyberprostoru se nenachází ani v oficiálních dokumentech EU jako Strategie kybernetické bezpečnosti Evropské Unie z roku 2013 [16] a navazujícího návrhu směrnice, která má vést k zajištění vysoké společné úrovně bezpečnosti sítí a informací v EU [12] – tzv. směrnice NIS. Pro další možnosti definice kyberprostoru odkazuji na [17], kde autor zpracoval přes 10 definic kyberprostoru z různých oficiálních dokumentů včetně tabulky zobrazující na základě klíčových slov, které aspekty se v definici vyskytují.

Co se týče vztahu kybernetické bezpečnosti a bezpečnosti informací: Přesné vymezení vztahu těchto dvou pojmů je, vzhledem k množství možností jejich vymezení, problematické. Jediná pravda zde není, a tak záleží na úhlu pohledu na základě kterého potom je jeden z pojmů buď podmnožinou druhého, nebo je mezi nimi průnik. Variantu, že spolu vůbec nesouvisí pochopitelně vylučuji. Dle výše zmíněných definicí z [10] i ze ZKB lze vyvodit, že bezpečnost informací je součástí kybernetické bezpečnosti. Kybernetickou bezpečnostní událostí totiž může být narušena podle ZKB nejen bezpečnost informací, ale také bezpečnost služeb a integrita[25] sítí elektronických komunikací. Kybernetická bezpečnost tak, jak je chápána zákonodárcem, je daleko širší problematika než bezpečnost informací (organizace). Zahrnuje komplexní systém ochrany kybernetického prostoru od stanovení bezpečnosti informací v organizaci k systému včasného varování a spolupráci se zahraničím na úrovni státu.

Bezpečnost informací se zabývá „pouze“ ochranou informace, byť v jakékoli podobě, zatímco u kybernetické bezpečnosti jde nejen o ochranu informací, ale i o ochranu kyberprostoru. Bezpečnost kyberprostoru totiž není jen bezpečnost informací v něm se

[24] Dle zákona č. 127/2005, o elektronických komunikacích [15]

[25] Integritou sítě je chápána dle zákona č. 127/2010 Sb. o elektronických komunikacích chápána „*funkčnost a provozuschopnost propojených sítí elektronických komunikací, ochrana těchto sítí vůči poruchám způsobeným elektromagnetickým rušením nebo provozním zatížením.*“

vyskytujících, ale je také prevencí před zločiny, které se v kyberprostoru páchají, jako je např. šíření závadných materiálů (např. dětská pornografie nebo materiály porušující autorská práva) apod.

Bezpečnost informací a kybernetická bezpečnost může do velké míry splývat, pokud je nazíráno z hlediska ochrany informací jedné organizace. Samotná organizace se nepotřebuje zabývat bezpečností kyberprostoru na území státu[26]. Rozdíl mezi bezpečností informací a kyberbezpečností zde může být nahlížen tak, že kybernetická bezpečnost se více zabývá hrozbami z Internetu, specializuje se na ochranou (pomocí různých nástrojů ať HW, SW, organizačních opatření nebo jinými) proti útokům hrozícím z kyberprostoru a jako taková se buď překrývá nebo stává součástí informační bezpečnosti, která dohlíží na bezpečnost informací i z hlediska fyzických přístupů atd.

Lze najít také úplně opačné názory, které považují kybernetickou bezpečnost za součást bezpečnosti informací. K tomuto závěru lze dojít, pokud je na věc nahlíženo např. z hlediska ochrany informace. Totiž za předpokladu, že se kybernetická bezpečnost zabývá ochranou informací pouze v digitální podobě a chrání informace před útoky vedené skrze kyberprostor, zatímco informační bezpečnost chrání informace v jakékoli podobě a před čímkoli, musí být nutně kybernetická bezpečnost součástí bezpečnosti informací.

Výbornou ukázkou toho, jak jsou pojmy chápány různě napříč různými státy a organizacemi je report organizace New America [18] a také pomůcka NATO CCDCOE[27] [19], která z něj čerpá, kde se nachází množství pojmů z oblasti kybernetické bezpečnosti a k nim jsou uváděny definice z různých oficiálních zdrojů států a mezinárodních organizací.

Považuji za dobré uvést také poznámku o vztahu dalších dvou pojmů a to *kybernetika* a *kybernetická bezpečnost*. Kybernetická bezpečnost není bezpečnost kybernetiky, jedná se o bezpečnost kyberprostoru (viz výše), bezpečnost informačních a komunikačních technologií. Proto také je vhodné používat sousloví kybernetický zákon ve smyslu zákona o kybernetické bezpečnosti obezřetně s vědomím, že může osobám neznalým věci asociovat spíše zákony kybernetiky místo toho, co ve skutečnosti představuje.

[26] Jsem si vědom neobratnosti tohoto výroku, kybernetický prostor je typický právě tím, že rozmlžuje hranice (států).

[27] NATO Cooperative Cyber Defence Centre of Excellence

Odlišná terminologie je také užívána zákonem 412/2005 Sb., o ochraně utajovaných informací[28] (a prováděcích předpisech). Tyto předpisy z určitých hledisek upravují totéž a to může podporovat další terminologické nejasnosti.

Za výchozí pojetí výše uvedených pojmů v této práci bude považováno pojetí vycházející z české legislativy kybernetické bezpečnosti a ze slovníku [10], pokud nebude uvedeno jinak.

3.2.2 CERT/CSIRT pracoviště

CERT a CSIRT jsou zkratky pro označení bezpečnostních týmů, které si mohou tvořit organizace pro svou potřebu dohledu nad určitou oblastí (např. síť, doména). V této jasně definované oblasti (pole působnosti) pak jsou zodpovědné za řešení bezpečnostních incidentů. Z pohledu uživatelů se jedná o místo, na které se mohou obrátit při podezření na bezpečnostní incident, jeho zjištění nebo řešení. [20]

- CERT – Computer Emergency Response Team (skupina pro reakci na počítačové hrozby [10]), zkratka vznikla a patří Carnegie-Mellon University
- CSIRT – Computer Security Incident Response Team (skupina pro reakce na počítačové bezpečnostní incidenty [10])

Každá ze zkratek vznikla historicky rozdílně, v principu se ale jedná o totéž. Pro jednoduchost v práci CERT a CSIRT považuji za synonyma, pokud není uvedeno jinak. CERT pracoviště se sdružují v mezinárodních organizacích. Takovými jsou např. organizace FIRST a TI (v rámci TERENA[29]). Kromě toho, že zabezpečují větší důvěryhodnost týmu, fungují také jako jakési „katalogy“ obsahující základní informace o týmech (kontakty, pole působnosti atd.) [20]

Některé CERT/CSIRT týmy mohou mít výkonnou moc tj. zasáhnout ve své síti za účelem řešení bezpečnostního incidentu a některé jsou pouze koordinační tj. zajišťují hladkou komunikaci mezi ostatními týmy, vytvářejí metodické pokyny aj. Koordinační role je typická pro vládní či národní CERT týmy.

CERT týmy mohou být ustanoveny jako pracoviště zastřešující dohled nad sítí určité organizace (státní nebo soukromé), ale tyto týmy jsou také organizovány na státní nebo

---

[28] Celým názvem zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti

[29] „*Trans-European Research and Education Networking Association, evropská mezinárodní organizace podporující aktivity v oblasti internetu, infrastruktur a služeb v rámci akademické komunity*“ [10]

dokonce mezinárodní úrovni. Druhé zmíněné mají trochu odlišnou roli – mají být poslední instancí, od které lze očekávat pomoc a mají zejména koordinační a vzdělávací roli. Např. CSIRT.CZ v tomto ohledu zajišťuje roli PoC (Point of Contact) – jednoduchý a důvěryhodný kontakt pro ČR a udržuje a rozvíjí zahraniční vztahy se světovou komunitou CERT/CSIRT týmů a s organizacemi podporujícími tuto komunitu jako ENISA, TERENA, FIRST.

V ČR byl zaveden zákonem o kybernetické bezpečnosti na státní úrovni koncept dvou týmů – „vládního" a „národního" týmu. Vládní provozuje NBÚ a národní nyní na základě veřejnoprávní smlouvy s NBÚ provozuje sdružení CZ.NIC. Zdůvodnění tohoto konceptu je obsaženo v důvodové zprávě k ZKB (kap. Národní a vládní CERT). Ve shrnutí jde o to, že vládní i národní CERT mají každý díky svému rozdílnému institucionálnímu postavení své výhody. Vládní CERT, jež je součástí NBÚ a tedy orgánu veřejné moci, „*může disponovat nařizovacími a sankčními pravomocemi, a tím zajišťovat přímé uplatňování státní moci na úseku kybernetické bezpečnosti.*" [8 s. 50] Pravomoci NBÚ jsou však omezeny vzhledem k principům, na kterých je zákon postaven a tak se vládní tým soustředí pouze na vybrané informační a komunikační systémy, jež jsou pro zájmy České republiky klíčové. Národní CERT naproti tomu nedisponuje nařizovacími ani jinými výkonnými pravomocemi, ale soukromoprávní povaha pak má své jiné výhody: Zejména v nepředvídatelných situacích má výhodu toho, že jako soukromoprávní subjekt může „*využít toho, že jeho provozovatel může činit vše, co mu není zákonem zakázáno (na rozdíl od situace, kdy by národní CERT provozoval orgán veřejné moci, jemuž je umožněno činit pouze to, co mu zákon výslovně ukládá nebo umožňuje)*". [8 s. 50] Toto umožní použití kreativních řešení omezených jen jejich zákonností. Výhodou je také využití kontaktů na národní a mezinárodní úrovni jak v soukromé sféře (národní CERT), tak ve sféře veřejné (vládní CERT).

Pro ilustraci: Národní tým CSIRT.CZ zveřejňuje na svém webu statistiky řešených incidentů: https://www.csirt.cz/page/2635/statistiky-resenych-incidentu/. V roce 2015 řešil 3771 bezpečnostních incidentů (nejvíce v kategoriích phishing, spam, malware, jiné, virus, trojan, DoS, probe).

Konkrétně se může se jednat např. o tyto incidenty (podle [21]):

- zveřejněná phishingová stránka,
- zavirovaný stroj či síť, který/á je zdrojem spamu,
- stroj se zjevně narušenou bezpečností,
- stroj, který je zdrojem DoS útoku, scanů apod.

Pro zajímavost uvádím informaci ze zprávy o činnosti CSIRT.CZ za rok 2012: Z celkových 7260 zpráv, které v roce 2012 přišly na adresu abuse@csirt.cz určenou pro hlášení těchto incidentů, bylo 6398 bylo vyřazeno jako spam.

Více k problematice CERT/CSIRT týmů (zejména k fungování národního CSIRT.CZ) viz v bakalářská práce Dominiky Rezníčkové[30] a dále také [20], [22] případně webové stránky pracovišť.

3.2.3 Vývoj kybernetické bezpečnosti v ČR

V této kapitole je pojednáno o vývoji kybernetické bezpečnosti v České republice zejména z hlediska veřejného sektoru a státu. Na úvod uvádím dva výroky:

„*Česká republika je jedním z posledních civilizovaných států, kde doposud nedošlo k implementaci národního řešení kybernetické bezpečnosti,(…)*“ [23 s. 355] (rok 2012)

„*Česká republika je jedním z prvních civilizovaných států, který zavedl komplexní právní úpravu národní kybernetické bezpečnosti.“* [24 s. 95] (rok 2015)

První prohlášení, ze kterého lze cítit určitý apel nebo stížnost, napsal v knize Internet a proměny práva docent Radim Polčák z Masarykovy univerzity v Brně. Druhý výrok patří stejnému autorovi, jen o tři roky později. Objevil se v odborném článku Kybernetická bezpečnost jako aktuální fenomén českého práva. Rozpor těchto výroků není neopodstatněný. Během let 2012 a 2015 totiž došlo v ČR k výraznému posunu na poli koordinace kybernetické bezpečnosti na celostátní úrovni, zvláště ve smyslu přípravy legislativy a jejímu uvedení do praxe. V roce 2012 došlo ke zveřejnění a schválení věcného návrhu zákona o kybernetické bezpečnosti, k prvnímu lednu roku 2015 již byl zákon účinný. K tomu všemu vedla poměrně dlouhá cesta od nekoordinovaných snah a iniciativ, kterou je možné sledovat mj. na základě vydaných různých pozičních a koncepčních dokumentů (koncepce, strategie, akční plány, politiky aj.) Těmi jsou[31]:

- Aktualizovaná koncepce boje proti organizovanému zločinu (2000),
- Koncepce boje proti trestné činnosti v oblasti informačních technologií,
- Státní informační a komunikační politika e-Česko 2006 (2004),
- Národní strategie informační bezpečnosti České republiky (2005)
- Akční plán realizace opatření Národní strategie informační bezpečnosti České republiky. (2007)

[30] REZNÍČKOVÁ, Dominika. *CERT / CSIRT tímy a kybernetická bezpečnosť* [online]. Praha, 2015. Diplomová práce. Vysoká škola ekonomická v Praze, Fakulta informatiky a statistiky. Dostupné z: https://www.vse.cz/vskp/id/1267824

[31] dle [8]

- Zřízení Meziresortní koordinační rady pro oblast kybernetické bezpečnosti (2010) (usnesením vlády ze dne 24. května 2010 č. 380 o zřízení Meziresortní koordinační rady pro oblast kybernetické bezpečnosti)
- Memorandum o Computer Security Incident Response Team (CSIRT) České republiky
- Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015 (2011)
- Přechod gesce nad kybernetickou bezpečností na NBÚ a zřízení Rady pro kybernetickou bezpečnost (2011) usnesením vlády ze dne 19. října 2011 č. 781 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast.
- Schválení Věcného záměru zákona o kybernetické bezpečnosti (2012).

V době před publikováním ZKB nebyla problematika kybernetické bezpečnosti v českém právním řádu specificky řešena. Dílčí aspekty byly upraveny napříč legislativou v různých předpisech. Výčet všech souvisejících předpisů je uveden v důvodové zprávě k ZKB (viz [25 s. 6–9]).

Na přelomu milénia se v ČR objevují první koncepční dokumenty zaměřené na kybernetickou bezpečnost, v té době řešené v rámci boji proti trestné činnosti. Následuje Státní informační a komunikační politika e-Česko 2006 (2004), na základě které vznikají další strategické dokumenty včetně Národní strategie informační bezpečnosti České republiky z roku 2005[32] a akčního plánu, který na ni navazuje. V této strategii byla již mj. řešena ochrana kritické informační infrastruktury státu, realizace systému včasného varování a reakce včetně úkolu ustavit národní centrum pro řízení, monitoring a analýzu bezpečnostního prostředí informačních a komunikačních systémů ČR, kromě realizace efektivní spolupráce na národní úrovni také aktivní mezinárodní spolupráce atd. V roce 2005 také byl formulován úkol vytvoření komplexního dokumentu, který by mapoval problematiku kybernetických hrozeb z hlediska bezpečnostních zájmů ČR a to v Národním akčním plánu boje proti terorismu (aktualizované znění pro léta 2005 až 2007).

Zpočátku některé snahy státu týkající se včasného varování a reakce formulované v koncepčních dokumentech zůstávaly víceméně na papíře. Nejen proto se začaly tvořit CERT/CSIRT pracoviště nezávisle na státu a to jak na akademických pracovištích, tak i v rámci samosprávy. [26] Příkladem takového fungujícího pracoviště může být CESNET-CERTS tým, jež byl vytvořen na přelomu let 2003 a 2004 [27] a měl za úkol především příjem hlášení bezpečnostních incidentů v síti CESNET2 a jejich řešení, dále

[32] Za povšimnutí stojí, že v této době ještě nebyl používán termín kybernetická bezpečnost.

strategický a technologický rozvoj jako vývoj IDS (Intrusion Detection System), vytváření a realizace bezpečnostní strategie v síti CESNET 2 a spolupráci se zahraničím. Dalšími týmy tohoto typu v ČR jsou mj. CSIRT-MU provozovaný Masarykovou univerzitou v Brně, CZ.NIC-CSIRT provozovaný sdružením CZ.NIC pro dohled nad sítí sdružení CZ.NIC a českou národní doménou „.cz“ a Active24-CSIRT provozovaný společností Active24. Ten byl prvním oficiálním CSIRT týmem v komerčním sektoru ČR. Kromě oficiálních týmů (i těch zde neuvedených) je v ČR ve skutečnosti takových dohledových a bezpečnostních pracovišť mnohem více a byť nejsou vždy nazývány CERT/CSIRT, je jejich činnost obdobná, [21] disponují renomovanými odborníky, mají zkušenosti s útoky, sdílí navzájem informace a některé jsou zapojeny i do mezinárodních struktur. [8]

V důvodové zprávě se uvádí hned za výše zmíněným akčním plánem již zřízení Meziresortní koordinační rady pro oblast kybernetické bezpečnosti. Tomu ale předcházela ještě kromě jiného aktivita Ministerstva vnitra, které v roce 2006 vypsalo v rámci svého výzkumného programu čtyřletý projekt „Problematika kybernetických hrozeb z hlediska bezpečnostních zájmů ČR“ (zkráceně „Kybernetické hrozby“). Výběrové řízení vyhrálo v lednu 2007 konsorcium univerzitních pracovišť pod vedením Matematicko-fyzikální fakulty Univerzity Karlovy, jehož členy byly kromě této fakulty z UK také Právnická fakulta, Fakulta sociálních věd a dále také České vysoké učení technické, CESNET a společnost Ness Technologies. Jak lze vidět už i z odborné různorodosti zapojených pracovišť, projekt byl široce zaměřený. Předmětem byla „*celá řada činností souvisejících s metodami odhalování kybernetické kriminality a terorismu a kvantifikací nebezpečnosti technologických trestných činů*“ [28] a to např. analýza technické realizace rozsáhlých IP a IPv6 sítí provozovaných veřejnoprávními, státními a akademickými subjekty a identifikace jejich slabých míst, vybudování distribuované hierarchie pro systematické řešení bezpečností problematiky v sítích prostřednictvím CSIRT týmů, programové vybavení pro forenzní analýzu digitálních dat a také zkoumání sociálně-psychologických faktorů této oblasti. K výše zmíněnému patří také analýza právní problematiky kyberprostoru. [28] Výsledkem mělo být „*ucelené vyhodnocení ohrožení České republiky kybernetickými hrozbami a nabídka metod a nástrojů na boj s tímto fenoménem.*“ [28]

V této době (první kvartál roku 2007) ještě existovala také snaha vybudovat státní CERT tým a to na tehdejším Ministerstvu informatiky, což se také stalo – na základě memoranda uzavřeného mezi Ministerstvem informatiky a společností Relsie, s.r.o. Paradoxně se tak stalo v době, kdy se na Ministerstvu vnitra vyhodnocovalo výběrové řízení na budování celé hierarchie CSIRT týmů. Toto pracoviště, vzniklé na základě zmíněného memoranda, však působilo spíše formálně. [26] Věcný záměr i důvodová zpráva o těchto faktech mlčí. Buď je autoři nepovažovali za důležité uvést a nebo to má jiný důvod, což lze na základě prostudovaných materiálů těžko posoudit.

V roce 2010 bylo Ministerstvo vnitra stanoveno gestorem problematiky kybernetické bezpečnosti pro ČR a jako takové mělo zřídit Meziresortní koordinační radu pro oblast kybernetické bezpečnosti, která měla pro tuto oblast být hlavním koordinačním orgánem. V následujícím roce byl ale (usnesením vlády ze dne 19. října 2011 č. 781) **ustaven gestorem a národní autoritou pro oblast kybernetické bezpečnosti Národní bezpečnostní úřad**. Autor považuje tento krok za velmi rozumný vzhledem ke značné kumulaci agendy (a tím i moci), kterou MV v oblasti státní informatiky řídí. Tímto usnesením byla také zrušena výše zmíněná Meziresortní koordinační rada pro oblast kybernetické bezpečnosti [29] a důležitou roli ve spolupráci mezi resorty od té doby zaujímá Rada pro kybernetickou bezpečnost [30] jako poradní orgán předsedy vlády pro oblast kybernetické bezpečnosti a podpora výkonu gesční a koordinační role NBÚ. [31] V tomto usnesení se také schvaluje vznik Národního centra kybernetické bezpečnosti (dále „NCKB“) jako součásti NBÚ a také jsou NBÚ navyšovány personální i finanční kapacity z nichž některé jsou převedeny z Ministerstva vnitra jako předchozího gesčního orgánu.

K 1.1.2011 začal fungovat jako národní CSIRT CZ.NIC. Memorandum za účelem zřízení národního CERT bylo uzavřeno mezi Ministerstvem vnitra a CZ.NIC z. s. p. o., v prosinci 2010. Po přechodu gesce v oblasti z Ministerstva vnitra na NBÚ (viz výše) bylo podepsáno dočasné memorandum s CZ.NIC již s tímto úřadem [32] a to bylo nahrazeno dalším novým podepsaným v prosinci 2012 s platností do 31.12.2015.

Pro vývoj kybernetické bezpečnosti na úrovni veřejné správy a legislativy je klíčový dokument Strategie pro oblast kybernetické bezpečnosti 2011 – 2015 (o rok později aktualizovaný na základě výše zmíněného usnesení vlády č. 781 z roku 2011 již pod gescí NBÚ jako **Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 – 2015**), který je v souladu s obecnou bezpečnostní strategii ČR z roku 2011. Mezi strategickými cíli a opatřeními se zde [30] nachází (výběr):

- **Vytvoření legislativního rámce,**
  - tento bod je z hlediska ZKB klíčový, jde o zaúkolování NBÚ vytvořením specializovaného zákona o kybernetické bezpečnosti, který má vymezit činnosti a odpovědnosti Národního centra kybernetické bezpečnosti a definovat povinnosti pro subjekty, které vytvářejí či využívají služeb ICT v kyberprostoru a také má vymezit způsoby a rozsahy spolupráce se soukromým sektorem, veřejností a mezinárodními institucemi.
- **Vybudování Národního centra kybernetické bezpečnosti (NKCB) a vládního pracoviště CERT**,
- **Ochrana kritických informačních infrastruktur** jako jedna z hlavních priorit kybernetické bezpečnosti,

- **Posilování kybernetické bezpečnosti informačních a komunikačních systémů veřejné správy**,
  - mj. publikace informací o kybernetické bezpečnosti na portálu GovCERT.cz, zavádění bezpečnostních norem a standardů, zpracovávání metodických materiálů pro dosažení pořadované minimální úrovně kybernetické bezpečnosti. Zmiňuje se zavádění systému řízení informační bezpečnosti (ISMS, Information Security Management System)
- **Koordinace aktivit k zajištění kybernetické bezpečnosti v Evropě**,
  - opatření založená na Akčním plánu pro ochranu kritických informačních infrastuktur (EU), spolupráce s ENISA[33] v oblasti cvičení, školení a sdílení informací a možnosti budoucí spolupráce např. v NATO Policy on Cyber Defence nebo agenturou eu-LISA[34].
- **Zvyšování povědomí o kybernetické bezpečnosti.**

V roce 2012 byl schválen Věcný záměr zákona o kybernetické bezpečnosti, který vypracoval NBÚ na základě výše zmíněného usnesení vlády č. 781. Předložený věcný záměr byl schválen vládou usnesením č. 381 ze dne 31. května 2012 a tím byl také uložen řediteli NBÚ úkol zpracovat do konce července 2013 paragrafové znění zákona. [8] V této době tedy probíhaly práce na znění ZKB. Za důležité z hlediska přístupu odpovědných subjektů k tvorbě předpisů i celého systému kybernetické bezpečnosti považuji, že kromě konzultací s akademickou sférou, soukromými subjekty a státními institucemi v ČR, během kterých došlo k některým posunům oproti věcnému záměru[35], byl NBÚ iniciativní také v zahraničí, kde byly navazovány důležité kontakty a konzultovány koncepty a sdíleny informace zkušenosti o budoucí kyberbezpečnostní legislativy a to jak ohledně fungování budoucího vládního CERT – kontakty s CERT Coordination Center pod záštitou Carnegie-Mellon University, FIRST (Forum of Incident Response and Security Teams), tak ohledně celého konceptu. [8] V důvodové zprávě je uvedeno, že „*reakce na celkovou koncepci a připravovanou legislativu je možno shrnout jako velmi pozitivní, zejména co se týče progresivního přístupu obsaženého v návrhu zákona*“ [25 s. 45] Pro více informací ohledně konzultací odkazuji tamtéž.

---

[33] European Network and Information Security Agency – Evropská agentura pro bezpečnost sítí a informací.

[34] Evropská Agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva.

[35] Rozšíření pojmu kyberprostor i na systémy, které nejsou „on-line“ (k tomu také viz kap. 3.2.1), vyjmutí systémů zpracovávající utajované informace z působnost zákona a také zavedení výjimky z regulace pro informační a komunikační systémy zpravodajských služeb [8].

Rok 2014 byl zásadní na poli legislativy kybernetické bezpečnosti i celého jejího budování. V tomto roce byl zákon o kybernetické bezpečnosti a o změně souvisejících zákonů přijat. Návrh byl vypracovaný NBÚ ve spolupráci s akademickou sférou, soukromým sektorem i státními institucemi. Během 2. ledna 2014 až koncem června 2014 prošel zákon všemi čteními Poslanecké sněmovny Parlamentu, kde sice došlo k několika úpravám na základě připomínek poslanců, ale koncept byl zachován, 23. července byl schválen Senátem a 13. srpna 2014 podepsán prezidentem ČR. [33] Účinnost byla stanovena na 1. ledna 2015. ZKB by byl nekompletní bez svých prováděcích předpisů, které byly vypracovány a schváleny také v roce 2014. Jsou to:

- 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),
- vyhláška 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích – vypracovali společně NBÚ a MV – a
- novela nařízení vlády ze dne 22. prosince 2010 č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury – v gesci MV.

Přijetí první zmíněné vyhlášky předcházelo dvoukolové připomínkové řízení s cílem dosáhnout co možná nejširší diskuse o připravované legislativě a optimalizace dopadů na povinné subjekty. Progresivním krokem bylo zveřejnění návrhu vyhlášky v únoru 2014 na webových stránkách NBÚ s výzvou k připomínkování odbornou veřejností. Tyto pak byly vypořádány na veřejném jednání. [33]

Následovalo vytvoření nových koncepčních dokumentů kybernetické bezpečnosti ČR na strategické úrovni a to: Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 a k ní vypracovaný Akční plán k Národní strategii kybernetické bezpečnosti[36] České republiky na období let 2015 až 2020. Protože klíčové cíle předchozí strategie a akčního plánu byly považovány za splněné, nezaměřují se tyto

[36] Na základě tohoto akčního plánu začala vznikat také aktuálně velmi sledovaná a v některých ohledech kontroverzní Národní strategie cloud computingu. Na konferenci ISSS 2016 jí byla věnována hodinová panelová diskuze u „kulatého stolu". Poměrně kontroverzní z hlediska bezpečnosti může být snaha o začlenění některých systémů bezpečnostních složek ČR včetně zpravodajských služeb a armády do tohoto cloudu [34] a to zvláště pokud by se velmi citlivá státní data dostala do části eGovernment cloudu spravovaného komerčním sektorem, kde sice mohou být dodrženy všechny standardy, ale je složitou otázkou, zda z principu do rukou soukromého sektoru taková data patří. Jsou navrhována různá řešení (např. umístění citlivých dat nejen kritické infrastruktury do části cloudu, která bude spravována výhradně státem). V této práci ale není více místa pro rozvedení tohoto tématu.

dokumenty na budování základních kapacit pro zajištění základní míry kybernetické bezpečnosti, ale již směřují k jejímu dalšímu hlubšímu a pokročilejšímu zajišťování. [33] [35] Jedná se o úplně novou strategii představující předěl ve vnímání kybernetické bezpečnosti státem. [36]

Kromě legislativy a vytváření koncepčních dokumentů se v roce 2014 také podařilo otevřít nové specializované pracoviště Národního centra kybernetické bezpečnosti v renovovaném objektu v Brně. Probíhala také intenzívní spolupráce NBÚ s různými subjekty na národní i mezinárodní úrovni (EU, ENISA, NATO, OBSE, CECP[37], bilaterální spolupráce s USA, Rumunskem, Izraelem, účast na mezinárodních cvičeních kybernetické bezpečnosti). GovCERT.CZ v srpnu 2014 mj. vstoupil mezi akreditované týmy sdružení Trusted Introducer působícího v rámci evropské organizace TERENA za účelem sdružování evropských bezpečnostních týmů a to jak vládních, tak národních i komerčních. Na národní úrovni pak spolupráce s akademickou sférou, Policií ČR a bezpečnostními složkami, Ministerstvem obrany i soukromými subjekty (Microsoft, banky). Konalo se také národní cvičení CYBER CZECH 2014 do kterého byly zapojeni zástupci z ministerstev, dalších ústředních správních úřadů a jiných orgánů včetně bezpečnostních sborů, akademických pracovišť a soukromých subjektů. Důraz byl kladen také na osvětovou činnost – přednášky na konferencích, analýza a zapojení se do výuky škol různých stupňů.

K 1. lednu 2015 je účinný zákon o kybernetické bezpečnosti a v tomto roce probíhá také ještě v několika vlnách určování systémů spadajících do kritické informační infrastruktury. Toto určování ještě stále probíhá k datu odevzdání práce (26. dubna 2016). Více k určovacímu procesu viz kap. 4.5.1 Systémy kritické informační infrastruktury a proces jejich určování. V prosinci 2015 byla uzavřena veřejnoprávní smlouva mezi NBÚ a CZ.NIC, na jejímž základě CZ.NIC provozuje Národní CERT CSIRT.CZ.

Česká republika se účastní mezinárodní spolupráce v oblasti kybernetické bezpečnosti. Mimo výše zmíněné existuje také memorandum o spolupráci v kybernetické obraně s NATO, ČR má stálého zástupce CCDCOE v Tallinnu, kromě EU spolupracuje s Izraelem, USA, Jižní Koreou a účastní se velkých mezinárodních cvičení – Lock Shields, Cyber Czech, CyberCoalition (NATO), CMX 2015 (NATO), CyberEurope 2015 (ENISA). [37]

Aktuální informací (z 22. dubna 2016) je úspěch českého kybernetického týmu na cvičení Lock Shields 2016, kde obsadil páté místo (z 20 týmů) a v oblasti zabezpečení SCADA systémů získal dokonce nejvíce bodů ze všech států.

---

[37] Central European Cyber Security Platform (Středoevropská platforma pro kybernetickou bezpečnost), založena v květnu 2013 na základě iniciativy Rakouska a ČR

3.2.4 ZKB v kontextu EU

I na úrovni EU se řeší kybernetická bezpečnost v rámci strategického a koncepčního plánování. Do současnosti bylo EU vydáno několik koncepčních dokumentů např. již v roce 2001 dokument *Bezpečnost sítí a informací – návrh evropského politického přístupu*[38], *Strategie pro bezpečnou informační společnost* (rok 2006) a další (podrobněji zpracováno např. v návrhu směrnice NIS v kapitole 1.2 Obecné souvislosti návrhu). Podstatné je také vydání sdělení o ochraně kritické informační infrastruktury (CIIP) v březnu 2009. V různých dokumentech publikovaných EU se v různé míře zdůrazňuje potřeba spolupráce a jednotného postupu v zajišťování připravenosti, odolnosti a bezpečnosti infrastruktury ICT, vytvoření účinných a koordinovaných bezpečnostních mechanizmů a vybudování kapacit EU ke splnění těchto cílů.

Ucelenou vizi kybernetické bezpečnosti EU podává v klíčovém dokumentu *Strategie kybernetické bezpečnosti Evropské Unie* z roku 2013 [16] a navazujícího *Návrhu směrnice Evropského parlamentu a rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii* [12] (dále jako *směrnice NIS*[39]). Návrh směrnice NIS byl zveřejněn v únoru roku 2013 a měl dvě části. V první části je vymezena strategie kybernetické bezpečnosti EU. Druhá část je tvořena samotným návrhem směrnice. V lednu letošního roku (2016) byl tento návrh schválen výborem IMCO[40] a v nejbližší době (jaro 2016) [39] by mělo být schváleno již platné znění a to nejprve v Radou EU a pak Evropským parlamentem. [40], [41]. Ke dni 21. dubna 2016 byl tento dokument předmětem jednání v Radě[41].

Cílem směrnice NIS je zavést určitou minimální úroveň zabezpečení digitálních technologií, sítí a služeb. Obsahuje i uložení povinnosti oznamovat závažné kybernetické incidenty určitému vymezenému okruhu podniků a to širším, než vymezuje ZKB. Podle návrhu směrnice se regulované podniky dělí do dvou skupin na základě vymezených kritérií a odlišují se stupněm regulace: poskytovatelé tzv. digitálních služeb neboli poskytovatelé služeb informační společnosti (menší stupeň regulace) a poskytovatele tzv. základních služeb neboli provozovatelé kritické infrastruktury (větší stupeň regulace)

---

[38] KOM (2001) 298

[39] zkratka Network Information Security directive

[40] Committee on the Internal Market and Consumer Protection (IMCO) – Výbor Evropského parlamentu pro vnitřní trh a ochranu spotřebitele. *„Výbor IMCO je příslušný pro legislativní dohled nad pravidly EU pro volný pohyb zboží a služeb, volný pohyb pracovníků, celní politiku, vytváření norem a hospodářské zájmy spotřebitelů a pro kontrolu jejich dodržování.“ [38]*

[41] Viz: http://eur-lex.europa.eu/procedure/CS/2013_27

oblasti energetiky, dopravy, zdravotnictví a další. [41], [12] K první jmenované je v příloze II směrnice uveden demonstrativní výčet. Jedná se o platformy pro elektronické obchodování, internetové platební brány, sociální sítě, vyhledávače služby cloud computingu a obchody s aplikacemi – v tomto ohledu tedy širší, než orgány a osoby vymezené v § 3 ZKB. Z důvodu proporcionality byly z působnosti směrnice (co se týče poskytovatelů digitálních služeb) vyčleněny malé podniky a mikropodniky[42], pro které by implementace všech povinností mohla znamenat nepřiměřenou finanční a administrativní zátěž[43] [42].

Každá členská země také bude mít povinnost určit národní orgán zodpovědný za řešení kybernetické bezpečnosti, vytvořit příslušnou strategii kybernetické bezpečnosti a také zřídit skupinu pro reakci na počítačové hrozby (CERT). V tomto ohledu je ČR již připravená.

Na základě schvální této směrnice bude ČR muset aktualizovat svou aktuální legislativu kybernetické bezpečnosti. Oficiální detaily o aktualizaci české legislativy se autorovi nepodařilo zjistit, nicméně byl informován pracovníkem kraje Vysočina, že na toto téma již probíhaly diskuze minimálně mezi tímto krajem a NBÚ (tj. ještě před schválením směrnice). Co se týče změn české legislativy, je pravděpodobné, že dojde k rozšíření okruhu povinných osob a také k přitvrzení sankcí, neboť sankce v ZKB nemusí být dle měřítek EU brány jako dostatečně odrazující[44]. Novelizace ZKB je diskutována také v kap. 4.1.3 Plánovaná novelizace ZKB a vyhlášky č. 317/2014 Sb.

Institucionální zajištění kybernetické bezpečnosti v EU

Na úrovni Evropské unie se kybernetickou bezpečností zabývají kromě základních evropských institucí (Evropská komise, Rada Evropské unie, Evropský parlament) tyto instituce:

- ENISA – Agentura Evropské unie pro bezpečnost sítí a informací,
- Evropské centrum pro boj proti kyberkriminalitě – funguje jako součást Evropského policejního úřadu EUROPOL.

V rámci Evropské komise pak působí Výbor pro bezpečnost sítí a informací.

Agentura ENISA slouží jako centrum, kde se soustřeďují poznatky kybernetické bezpečnosti EU, a pomáhá mj. členským státům EU, aby byly lépe vybaveny a

---

[42] dle Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků (Úř. věst. L 124, 20.5.2003, s. 36).

[43] To lze vyčíst z návrhu směrnice NIS ke dni 10. února 2016 zaslaného na COREPER (Výbor stálých zástupců, Rada).

[44] „*Stanovené sankce musí být účinné, přiměřené a odrazující.*“ [42 s. 65]

připraveny ve smyslu prevence, odhalování a řešení problémů v oblasti bezpečnosti informací. Poskytuje jim praktické poradenství (nácviky řešení krizových situací, vývoj národních strategií kybernetické bezpečnosti, podpora skupin typu CERT) a zveřejňováním různých zpráv a studií. Řeší různé výzkumné úkoly a spolupracuje s jinými evropskými agenturami a institucemi.

Poznámka: Názor veřejnosti (občanů) EU na kybernetickou bezpečnost zkoumá projekt Eurobarometr fungující v rámci Evropské komise. Dostupné na adrese http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/General/index, pod kategorií Special EB jako „Cyber security“. Z tohoto průzkumu uskutečněného podruhé v roce 2014 vyplynulo např. to, že polovina uživatelů internetu v EU objevila na svém počítači škodlivý software a více než polovina uživatelů internetu se obává, že se stanou obětí kybernetického zločinu různého druhu (krádež identity, škodlivý kód, online bankovní podvod). [43]

4 Rozbor ZKB a jeho prováděcích předpisů z hlediska dopadů na povinné subjekty

V této kapitole jsou shrnuty nejdůležitější oblasti zákona o kybernetické bezpečnosti a jeho prováděcích předpisů z hlediska dopadů na povinné subjekty. Vzhledem k tomu, že autorův průzkum je zaměřen na krajské úřady, je důraz v této kapitole kladen především na subjekty, které jsou správci významných informačních systémů. Bylo předpokládáno, že krajské úřady budou vesměs správci těchto systémů[45]. [1]

Vzniku zákona (včetně prováděcích předpisů) a vývoji kybernetické bezpečnosti se věnovala kapitola 3.2.3 Vývoj kybernetické bezpečnosti v ČR.

4.1 ZKB v kostce – smysl a účel zákona

Pro zvážení dopadů ZKB na povinné subjekty je nejprve nezbytné specifikovat účel zákona a jeho dopady obecně. Na ZKB lze pohlížet z několika hledisek. Pro tuto práci nejpodstatnější je rozlišení, zda zkoumáme ZKB z pohledu státu nebo z pohledu organizace, na kterou povinnosti dané zákonem dopadají. Z hlediska státu se jedná o *„nastavení systému koordinace a kooperace mezi nejdůležitějšími subjekty kybernetické bezpečnosti a na zavedení bezpečnostních opatření k ochraně informačních a komunikačních systémů důležitých pro stát.“ [33]*. Tato oblast je pokryta ustanovením národní autority pro oblast kybernetické bezpečnosti, která celou oblast metodicky a legislativně koordinuje a může také v případě nutnosti zasáhnout formou koordinovaných opatření[46].

Z hlediska subjektů, na které povinnosti ZKB dopadají, ZKB spolu s vyhláškou 316/2014 Sb. znamená implementaci a provádění víceméně standardních bezpečnostních opatření do vybraných subjektů (podniků, úřadů, …) z veřejného i soukromého sektoru, k tomu provozování dohledových pracovišť typu CERT, povinnost zmíněných subjektů s nimi komunikovat a nad to pak zavedení národní autority pro oblast kybernetické bezpečnosti, která celou oblast metodicky a legislativně koordinuje a může také v případě nutnosti zasáhnout formou koordinovaných opatření.

[45] Tento předpoklad byl průzkumem potvrzen (viz kap. 5.3.2 Blok I – zjištění VIS a systémů KII, výsledky)

[46] Tj. varování, reaktivní a ochranná opatření dle § 11–15 ZKB.

Smysl a účel ZKB shrnují tři pilíře, na kterých tato legislativa stojí:

- *zavedení preventivních bezpečnostních opatření u KII a VIS,*
- *vytvoření* systému *hlášení kybernetických bezpečnostních incidentů a předávání informací mezi hlavními subjekty kybernetické bezpečnosti v České republice a*
- *zakotvení pravomocí NBÚ v oblasti kybernetické bezpečnosti, včetně možnosti vydávat opatření v reakci na určité kybernetické bezpečnostní incidenty. Zákon zároveň zakotvuje činnost Vládního CERT a Národního CERT.* [33]

Z hlediska dopadů zákona na povinné subjekty je nezbytné mít na zřeteli, že smyslem a účelem zákona je především *prevence*, nikoli potírání trestné činnosti v kyberprostoru ani zakládání trestní odpovědnosti. Na to jsou v ČR jiné zákony (trestní zákoník, zákon o trestní odpovědnosti právnických osob), které umožňují trestné činy páchané v kyberprostoru stíhat. V důvodové zprávě i v [24] je uvedeno přirovnání ZKB k systému protipožární ochrany. Ta funguje také preventivně a případných žhářů se již netýká, ty řeší orgány činné v trestném řízení. Problematikou kybernetické kriminality (kybernality) se velmi detailně věnuje publikace Vladimíra Smejkala [44].

Za podstatné považuji zdůraznit, že nejedná se pouze o prevenci z hlediska hrozeb plynoucích z kyberprostoru a tedy zajištění perimetru sítí ICT. Jde o zavedení standardního komplexního řízení bezpečnosti informací do organizací, které spravují informační a komunikační systémy významné nebo kritické pro stát a to včetně řízení lidských zdrojů, fyzické bezpečnosti, systematické analýzy rizik atd.

4.1.1 Principy, na kterých je zákon postaven

Tato kapitola stručně uvádí o právní principy, zásady, na kterých je ZKB postaven a jak se tyto principy v Zákoně projevují.

Z hlediska právní teorie je zákon postaven na těchto principech (z důvodové zprávy k zákonu):

- Princip ochrany informačního sebeurčení člověka,
- Princip ochrany nedistributivních práv,
- Princip minimalizace státního donucení,
- Princip autonomie vůle regulovaných subjektů,
- Princip bdělosti ve vztahu k ostatním státům a mezinárodnímu společenství. [8]

Pro detailnější rozbor těchto principů v této práci není místo, odkazuji na důvodovou zprávu [25] a zejména pak na teoretické práce z Masarykovy univerzity jako [23] nebo [24]. Tyto principy jsou zde však zmíněny, neboť determinují i rozsah dopadů

zamýšlených zákonodárcem na povinné subjekty a také roli státu při koordinaci kybernetické bezpečnosti[47].

Mimo výše zmíněné právní principy uvedené v důvodové zprávě zákona uvádějí představitelé NBÚ také *princip standardizace*, který znamená, že kdekoli to jde, jsou aplikovány mezinárodní standardy a zdůrazňují také *anonymitu*, ve smyslu záznamů o incidentech tak, aby nemohly sloužit ke sledování nebo identifikaci konkrétního člověka. [45] Uvádí také princip *technologické neutrality*, jež představuje snahu definovat veškeré požadavky tak, aby mohly být splněny využitím různých služeb a produktů a nebyly tak vázány na určitou technologii či výrobce.

4.1.2 Zákon a prováděcí předpisy

Jak bylo zmíněno již v kapitole o vývoji kybernetické bezpečnosti v ČR, legislativa kybernetické bezpečnosti je u nás tvořena těmito předpisy:

- *zákon č. 181/2014 Sb., o kybernetické bezpečnosti a změně souvisejících zákonů (zákon o kybernetické bezpečnosti)*,
- *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)*,
- *vyhláška 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích*,
- *nařízení vlády č. 315/2014 Sb., kterým se mění nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury*.

Zákon č. 181/2014 Sb. je hlavním předpisem v oblasti kybernetické bezpečnosti, upravuje práva a povinnosti osob v této oblasti a také působnost a pravomoci orgánů veřejné moci (NBÚ, MV).

Vyhláška č. 317/2014 Sb. (dále také jako „VVIS“) a nařízení vlády č. 315/2014 Sb. jsou předpisy, které specifikují jaké osoby a organizace spadnou do působnosti ZKB.

Pro zavádění bezpečnostních opatření, a tedy i dopady na povinné subjekty, je klíčová vyhláška č. 316/2014 Sb. o kybernetické bezpečnosti. Tato vyhláška určuje povinným

[47] V této souvislosti autor považuje za podstatné zmínit, že při tvorbě ZKB bylo (dle důvodové zprávy [8]) zvažováno několik možných variant a to od nulové varianty, kdyby zůstala kybernetická bezpečnost bez specifické právní regulace, až po variantu obecné působnosti a přímé regulace, která by umožnila přímou kontrolu a možnost aplikování bezpečnostních opatření státem (NBÚ) a znamenala by enormní regulatorní zátěž (dopady) na povinné subjekty a také problémovou ústavní konformitu. [8 s. 22–23]

subjektům (správcům KII a VIS), jaká musí zavést bezpečnostní opatření a další povinnosti, aby vyhověly ZKB. Jedná se o v podstatě o soupis „best practise“ požadavků na zajištění požadované míry kybernetické bezpečnosti.

4.1.3 Plánovaná novelizace ZKB a vyhlášky č. 317/2014 Sb.

Z hlediska dopadů na povnné subjekty je podstatná také stabilita právního prostředí, které jim povinnosti ukládá. Z tohoto pohledu je třeba zmínit, že po přijetí evropské směrnice NIS bude ZKB s největší pravděpodobností novelizován zejména co se týče okruhu povinných osob a sankcí (viz kap. 3.2.4 ZKB v kontextu EU).

Novelizována bude také vyhláška 317/2016 Sb. a to z důvodu přesunutí některých VIS mezi KII a aktualizování seznamu VIS v příloze této vyhlášky. Některé uvedené významné informační systémy totiž naplňují kritéria KII a některé systémy uvedené jako VIS již nenaplňují kritéria VIS ani KII a tak budou ze seznamu vypuštěny. Celkový počet VIS se ale v návrhu nové vyhlášky zvyšuje a to z 92 na 105. Z původního seznamu 30ti systémů bylo 22 určeno jako kritická informační infrastruktura a 8 bylo vypuštěno s tím, že již nenaplňují kritéria významných informačních systémů. Vyhláška měla nabýt účinnosti 1. dubna 2016 [46], ale pravděpodobně pod vlivem množství připomínek se tak ještě nestalo. Ke dni 26. dubna 2016 ještě vyhláška nebyla publikovaná.

Z výše uvedeného vyplývá, že novelizace ZKB na základě evropské směrnice NIS s velkou pravděpodobností nebude mít na krajské úřady významný dopad. Jeden z pracovníků KrÚ[48] (kraj Vysočina) poskytl autorovi také informaci o tom, že na základě jím provedené předběžné analýzy nejspíše nebude mít směrnice NIS na KrÚ vliv. Zdůraznil však, že vzhledem k tomu, že směrnice ještě není oficiálně schválená a nejsou dostupné žádné oficiální informace, je možné v tomto ohledu nanejvýše vytvářet domněnky. Dle autora se může projevit směrnice NIS na KrÚ také za předpokladu, že budou na základě této směrnice zvýšeny sankce v ZKB – tedy v případě porušení povinností krajským úřadem. Situace bude nejspíše obdobná i u jiných orgánů veřejné správy.

[48] Tento krajský úřad vedl s NBÚ diskuze ohledně vlivu směrnice NIS na ZKB.

4.1.4 Institucionální zajištění, subjekty důležité ve vztahu k ZKB

Nejdůležitější vrcholové státní orgány působící v oblasti kybernetické bezpečnosti jsou:

- Národní bezpečnostní úřad (NBÚ),
- Národní centrum kybernetické bezpečnosti (NCKB) – organizační útvar NBÚ,
- Rada pro kybernetickou bezpečnost (RKB),
- Ministerstvo vnitra (MV).

Kromě institucí, které jsou podstatné z hlediska legislativy se kybernetickou bezpečností zabývají i další subjekty. V akademické sféře je z hlediska kybernetické bezpečnosti aktivní zejména Masarykova univerzita, která v rámci Ústavu výpočetní techniky pracuje na projektu s názvem Kybernetický polygon (KYPO), které se zabývá výzkumem, vývojem a sestavením unikátního prostředí pro analýzu hrozeb ohrožujících bezpečnost kritických informačních infrastruktur. Projekt byl finančně podpořený Ministerstvem vnitra. V tomto prostředí lze vytvářet komplexní scénáře simulující nejrůznější síťové konfigurace sloužící pro školení či experimenty a umožňují tak simulovat různé typy útoků a obrany. Umožňuje mj. vizualizovat děje a události probíhající v počítačové síti i na jednotlivých strojích, má vestavěnou měřicí infrastrukturu. Podpořeno je superpočítačovým centrem CERIT Scientific Cloud, který umožňuje řešení do vysoké míry škálovat. Na této univerzitě vznikl také samostatný studijní obor věnující se kybernetické bezpečnosti. Výzkum v oblasti kybernetické bezpečnosti (týkající útoků typu DDoS) probíhá také na Vysokém učení technickém v Brně. [47] [48]

V soukromé sféře je z hlediska ZKB podstatné sdružení právnických osob CZ.NIC, které v současné době provozuje na základě veřejnoprávní smlouvy s NBÚ národní CERT s názvem CSIRT.CZ (dle § 18 ZKB tzv. provozovatel národního CERT). Do ČR také bude umístěna první aréna CyberGym společnosti společnosti Corpus Solutions a.s. určená k tréninku proti kybernetickým útokům. Krátce před odevzdáním práce byla také zveřejněna aktuální informace (20. dubna) o tom, že společnost O2 IT Services otevřela v Praze „Security Expert Center“ (SEC), jež poskytuje služby v oblasti kybernetické bezpečnosti státním i soukromým subjektům. Umožňuje např. identifikovat klíčová aktiva společnosti (např. informační aktiva, lidské zdroje, procesy nebo systémy) a nastavit optimální model jejich ochrany. Umožňuje realizovat bezpečnostní dohled umožňující identifikovat zranitelnost jejich IT. Článek deklaruje, že se jedná o jednoho z mála poskytovatelů řešení, jehož nasazení odpovídá potřebám ZKB a nabízí jej i správcům kritické infrastruktury. [49]

4.2 Proč zákon o kybernetické bezpečnosti

Zákon o kybernetické bezpečnosti je v mezinárodním měřítku ojedinělou koncepcí a ČR je jednou z prvních zemí, která přijala samostatný zákon upravující kybernetickou bezpečnost. Otázkou je, zda je to možno hodnotit jako pozitivum – samotný fakt, že ČR je první zemí, která podobný zákon přijala, ještě neznamená, že je také světovou špičkou v oboru a řeší problém koncepčně nejlépe. Podle prostudovaných zdrojů Česká republika nicméně pozadu v oboru není a zvolená koncepce i v zahraničí budí pozitivní ohlasy. [25] [33] Důvody vedoucí ČR k zavedení této legislativy jsou zevrubně popsány v důvodové zprávě k zákonu.

Zavést a kontrolovat systém řízení bezpečnosti v organizaci je každopádně rozumné a to tím více, čím důležitější systémy organizace provozuje. Na tom, že ZKB je rozumným krokem k dosažení větší bezpečnosti se shoduje i naprostá většina autorem oslovených pracovníků v provedeném výzkumu v kap. 5. Tato opatření však nejsou zadarmo a organizace nějakým (i významným) způsobem zatíží. Toto je také předmětem průzkumu v kap. 5.

Co se týče systémů provozovaných orgány veřejné moci, ty měly povinnost (kromě těch ze zákona vyjmutých) zajišťovat bezpečnost informací v rámci svých provozovaných informačních systémů již dříve. Tuto povinnost měly a mají podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy. Objevuje se v § 3 odst. 8., dále v § 5a odst. 1. a to v rámci vytváření (udržování, uplatňování a vyhodnocování) informační koncepce. Zvláštní zmínka o bezpečnosti je také v § 5 písm. b):

„*Orgány veřejné správy uplatňují opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy.*“

ZKB také na rozdíl od zákona 365/2000 Sb. a jeho prováděcích předpisů klade větší důraz na faktické zavedení bezpečnostních opatření, než na dokumentaci IS. Shrnuto, kdyby se úrovni bezpečnosti informačních systémů ve veřejné správě věnovala dostatečná pozornost, nebylo by pravděpodobně třeba zákonné úpravy v této podobě. Situace je podobná i se systémy kritické infrastruktury. V takovém případě by nejspíše stačila zákonná úprava zajišťující pouze koordinaci na národní a mezinárodní úrovni pro snazší komunikaci jednotlivých subjektů a jejich CERT či podobných útvarů s národním či vládním CERT. Podobného argumentu by se dalo ale využít i u jakékoli jiné úpravy (mám na mysli výroky typu „kdyby nebyla kriminalita, nemusel by existovat trestní zákoník“, které sice dávají smysl, ale žádný reálný problém v podstatě neřeší). V situaci, jaká je, je tedy zákonná a podzákonná úprava, která detailněji vymezí a bude vynucovat kroky k zajištění základní úrovně bezpečnosti, potřebná.

Odhlédneme-li od objektivní potřeby zajištění základní míry bezpečnosti ve státem provozovaných organizacích klíčových pro chod ČR, na zajištění kybernetické bezpečnosti českou legislativou je vyvíjen také tlak z Evropské unie (podobně jako v případě „obecné“ ochrany kritické infrastruktury nezaměřené na kyberbezpečnost, k tomu viz kap. 3.1.2 Kritická infrastruktura). Za prvé jde o tzv. due diligence – princip bdělosti – který zjednodušeně řečeno znamená, že pokud Česká republika nebude aktivní v ochraně „svého[49]“ kybernetického prostoru a ten bude zdrojem kybernetických hrozeb pro ostatní země, mohou to tyto země ČR dávat za vinu.

Publikace zákona a zejména jeho vyhlášky 316/2014 může být také i výhodná pro subjekty, které pod působnost ZKB nespadají, ať už to jsou soukromé podniky nebo státní organizace. Mohou takto totiž zcela zdarma získat „best practice“ příručku pro zavedení řízení bezpečnosti v organizaci postavenou na oborových standardech a pracovat s ní dle svého vlastního uvážení. To může vypadat jako pozitivní vedlejší efekt, nicméně pokud se zasadí do kontextu strategií kybernetické bezpečnosti ČR, dalo by se považovat i za plnění cílů zaměřených na zvyšování bezpečnostního povědomí a vzdělávání v oblasti kyberbezpečnosti. Zmíněné cíle se nacházejí ve strategii na období 2012–2015 [30] i v té aktuální 2015–2020. [35]

Díky různým konzultacím, účasti zainteresovaných osob na konferencích, nutnosti zavádění konkrétních bezpečnostních opatření a také medializaci se o problematice bezpečnosti více „mluví“, vznikají nová pracovní místa v oboru bezpečnosti, jsou vytvářeny specializované studijní plány na vysokých školách, toto vše lze považovat za přispění k celkovému zvýšení bezpečnostního povědomí společnosti a již to je pozitivní dopad na kybernetickou bezpečnost České a zdejších organizací.

4.3 Struktura zákona a vyhlášky č. 316/2014 Sb.

Zákon má šest 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 správní delikty,
- Hlava VI – Závěrečná ustanovení.

[49] Vymezení části kybernetického prostoru, který spadá pod určitý stát, je složitou otázkou. Více k tomu v teoretické práci [23].

Zbylé části (druhá a další) se věnují změnám dalších předpisů (např. zákona o utajovaných informacích a dalších) a účinnosti.

V hlavě I se uvádí předmět úpravy a vymezují se pojmy.

Hlava II obsahuje většinu ustanovení, které jsou podstatné z hlediska dopadů na povinné subjekty:

- Bezpečnostní opatření (§ 4–6),
- Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident (§ 7),
- Hlášení kybernetického bezpečnostního incidentu (§ 8),
- Evidence (§ 9–10),
- Opatření (§ 11),
- Varování (§ 12),
- Reaktivní a ochranné opatření (§ 13–15),
- Kontaktní údaje (§ 16),
- Národní CERT (§ 17),
- Provozovatel národního CERT (§ 18),
- Veřejnoprávní smlouva (§ 19),
- Vládní CERT (§ 20).

Hlava III se týká stavu kybernetického nebezpečí, Hlava IV stanovuje, že státní správu v oblasti kybernetické bezpečnosti vykonává NBÚ a definuje jeho povinnosti, Hlava V se zabývá kontrolou, nápravnými opatřeními a správními delikty a Hlava VI jsou závěrečná ustanovení (zmocnění MV a NBÚ k vydání navazujících vyhlášek v § 28 a také jsou zde mj. obsaženy lhůty k plnění povinností).

Pro dopady na povinné osoby je z hlediska povinností, které musejí zavést, nejpodstatnější Hlava II Systém zajištění kybernetické bezpečnosti a v rámci ní zejména § 4–6 definující *bezpečnostní opatření*, které musí osoby dle § 3 písm. c) až e) (tedy správci systémů KII a VIS) zavést. Bezpečnostní opatření se zde dělí na organizační opatření a technická opatření. Zákon dále obsahuje taxativní výčet opatření náležející do skupiny organizačních i technických opatření, ale nikterak je nekonkretizuje. Tato opatření a návod, jak je zavést, jsou detailně uvedeny ve vyhlášce o kybernetické bezpečnosti č. 316/2014 Sb. (dále také jako „VKB“). Více k bezpečnostním opatřením viz kap. 4.6.1 Bezpečnostní opatření.

Členění vyhlášky je následující:

- Část první – Úvodní ustanovení
    - (vymezení předmětu úpravy a základních pojmů)
- Část druhá – Bezpečnostní opatření
    - Hlava I – Organizační opatření
    - Hlava II – Technická opatření
    - Hlava III – Bezpečnostní dokumentace
- Část třetí – Kybernetický bezpečnostní incident
    - (typy a kategorizace kybernetických bezpečnostních incidentů, a forma a náležitosti jejich hlášení)
- Část čtvrtá – Reaktivní opatření a kontaktní údaje
    - (povinnost oznanování provedení reaktivních opatření a oznamování kontaktních údajů – odkazy na formuláře v přílohách vyhlášky)
- Část pátá – Účinnost.

Vyhláška obsahuje důležité přílohy:

- Příloha 1 – Hodnocení úrovně a důležitosti aktiv,
- Příloha 2 – Hodnocení rizik,
- Příloha 3 – Minimální požadavky na kryptografické algoritmy,
- Příloha 4 – Struktura bezpečnostní dokumentace,
- Příloha 5 – Formulář hlášení kybernetického bezpečnostního incidentu,
- Příloha 6 – Formulář oznámení o provedení reaktivního opatření a jeho výsledku,
- Příloha 7 – Formulář pro hlášení kontaktních údajů.

4.4 Základní pojmy ZKB

V této kapitole jsou stručně vymezeny vybrané základní pojmy ze zákona o kybernetické bezpečnosti (z hlediska dalších kapitol). Vymezení všech pojmů v ZKB je uvedeno v § 2 tohoto zákona.

- **správce systému** – (buď informačního nebo komunikačního) – orgán nebo osoba, které určují účel zpracování informací a podmínky jeho provozování.
- **kritická informační infrastruktura** – *„prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti*“ (pro detailnější vysvětlení prvku kritické infrastruktury viz kap.

3.1.2 Kritická infrastruktura) oblast kybernetické bezpečnosti je oblastí v rámci odvětvových kritérií pro určení prvku kritické infrastruktury (v nařízení vlády č. 432/2010 Sb. ve znění nařízení vlády 315/2014 Sb.)

- **bezpečnostní opatření** – „*soubor opatření, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru*“
- **významný informační systém** – „*informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci*“ (dle ZKB)
- **kybernetická bezpečnostní událost** – „*událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací.*“
- **kybernetický bezpečnostní incident** – „*narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.*“

4.5 Dotčené subjekty a proces jejich určování

Při stanovování dopadů ZKB na povinné subjekty je klíčové uvést, jaké existují povinné subjekty z pohledu ZKB. Na následujících řádcích je pojednáno o dotčených subjektech, nejprve obecně a následně detailněji v podkapitolách. Zákon rozeznává celkem 5 typů subjektů, kterým jsou ukládány povinnosti a které se liší množstvím uložených povinností. Tyto subjekty jsou uvedeny v § 3 písm. a) až e) ZKB:

a) *poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací*[50](…),

b) *orgán nebo osoba zajišťující významnou síť*(…),

c) *správce informačního systému kritické informační infrastruktury*,

d) *správce komunikačního systému kritické informační infrastruktury* a

e) *správce významného informačního systému*.

Toto vymezení částečně používá pojmy ze zákona č. 127/2005 Sb., o elektronických komunikacích a to v případě obou typů subjektů podle písmena a).

[50] Dle zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů.

Vyjmenované subjekty lze rozdělit do dvou pomyslných skupin. **První skupinou** jsou subjekty podle písmen a) i b), které jsou tvořené převážně soukromoprávními subjekty a ZKB na ně klade v souladu s principem minimálních zásahů do práv soukromoprávních osob pouze omezené požadavky. [50] Rozsah povinností poskytovatelů služeb a subjektů zajišťujících síť elektronických komunikací se rozšiřuje při vyhlášení stavu kybernetického nebezpečí (kap. 4.7.5.).

Druhou skupinou, na kterou ZKB klade výrazně více povinností jsou orgány a osoby v písm. c), d) a e). Nejvíce povinností a nejpřísnější bezpečnostní opatření jsou ukládány správcům informačních a komunikačních systémů kritické informační infrastruktury – písm. c) a d). Pro přehlednost je v práci souhrnně označuji jako „systémy kritické informační infrastruktury" (dále zkráceně jako „systémy KII"). Pod písmeno e) spadají správci významných informačních systémů, kteří musí plnit obdobné povinnosti jako správci KII, ale v menším rozsahu. NBÚ uvádí, že mají zhruba 60% povinností oproti správcům systémů KII. [51]

Tyto dvě skupiny se liší také tím, pod který CERT spadají. První skupina tj. osoby písm. a) a b) spadají pod národní CERT a zbývající, tedy c), d) a e), spadají pod vládní CERT.

Velmi podstatný je fakt, že z působnosti zákona byly vyčleněny systémy pracující s utajovanými informacemi podle zákona č. 412/2005 Sb., o utajovaných informacích[51] (§ 1 odst. 2). Jejich ochrana je totiž komplexně zajištěna jiným právním předpisem na základě kterého podléhají vyšší formě regulace (certifikace NBÚ). [8]

Práce je dále zaměřena na skupinu správců systémů kritické informační infrastruktury a zejména na správce významných informačních systémů.

K tomu, aby mohl systém být zařazen mezi kritickou informační infrastrukturu nebo významný informační systém, musí splnit určitá kritéria a projít určovacím procesem. U orgánů a osob podle § 3 písm. a), b) ZKB určování neprobíhá, tyto subjekty musejí samy zhodnotit, zda se na ně zákon vztahuje či ne. O určovacím procesu v pravém slova smyslu lze hovořit až u systémů kritické informační infrastruktury a významných informačních systémů – tedy § 3 písm. c), d), e) ZKB. To, že nějaký systém je systémem kritické informační infrastruktury nebo významným informačním systémem je možno konstatovat teprve až po ukončení celého určovacího procesu[52]. Do té doby nespadají pod § 3 ZKB (leda že by naplňovaly kritéria prvních dvou písmen).

---

[51] Zákon č. 412/2005 Sb., o utajovaných informacích a bezpečnostní způsobilosti.

[52] S výjimkou těch VIS, které jsou taxativně vyjmenovány v příloze vyhlášky č. 317/2014 Sb. U těchto vyjmenovaných neprobíhá určovací proces.

Kritéria i proces určování pro systémy KII a VIS se liší. Přehledně graficky formou vývojového diagramu tento proces znázorňují metodické pomůcky vypracované NBÚ[53]. Důležité je, že proces určování je kontinuální proces, některé systémy budou v budoucnu přibývat, některé ubývat (tvorba/zánik systémů, změny z hlediska určujících kritérií). V následujících dvou podkapitolách je popsán určovací proces pro systémy KII a pro VIS.

4.5.1 Systémy kritické informační infrastruktury a proces jejich určování

V určovacím procesu systémů KII jsou podstatné tyto zákony:

- *zákon o kybernetické bezpečnosti* – definuje KII,
- *krizový zákon* – stanovuje proces určení prvků kritické infrastruktury a
- (novelizované) *nařízení vlády č. 432/2010 Sb*., které stanovuje kritéria pro KII

Systémy KII nejprve musí splnit určitá kritéria:

- *průřezová*[54] kritéria (posuzují závažnost narušení funkce systému – rozsah ztrát na životech, počet zraněných, ekonomické dopady, omezení poskytování nezbytných služeb při nefunkčnosti systému a jiné),
- *odvětvová* kritéria[55] (jde o konkrétní údaje souvisejícími s daným odvětvím[56], popsáno výše v kap. 3.1.2).

---

[53] Dostupné z: https://www.govcert.cz/cs/kii--vis/kriticka-informacni-infrastruktura/ a https://www.govcert.cz/cs/kii--vis/vyznamne-informacni-systemy/

[54] hlediska průřezových kritérií jsou stanoveny takto: 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), dopad na veřejnost (s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125000 osob) – z nařízení vlády č. 432/2010 Sb. ve znění nařízení vlády č. 315/2014 Sb. [52]

[55] G. Oblast kybernetické bezpečnosti v nařízení vlády č. 432/2010 Sb. ve znění nařízení vlády č. 315/2014 Sb.

[56] U odvětví kybernetické bezpečnosti např. (dle nařízení vlády č. 432/2010 Sb. ve znění novely č. 315/2014 Sb.) „*informační nebo komunikační systém, který ovlivňuje významně nebo zcela činnost určeného prvku KI a zároveň je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období delším než 8 hodin*“.

Kromě těchto kritérií musí také naplňovat § 2 písm. g) krizového zákona[57]. U systémů KII je zásadní, že spadají do kritické infrastruktury podle krizového zákona (viz kap. 3.1.2), protože tímto zákonem je dán průběh určovacího procesu. Tento proces je rozdílný podle toho, zda se jedná o soukromoprávní subjekt nebo organizační složku státu.

Pro to, aby systém mohl být posouzen jako prvek KII, musí být naplněno alespoň jedno průřezové a alespoň jedno odvětvové kritérium. Při posuzování naplnění kritérií se u KII nehodnotí pouze narušení dostupnosti, ale všechny tři základní pilíře informační bezpečnosti takže i narušení důvěrnosti a integrity. [51, 53]

Praxe určování vypadá v případě soukromoprávních subjektů tak, že mezi potenciálním správcem KII a NBÚ probíhají konzultace a ujasňování vzájemných názorů (trvá i několik měsíců)[58] a určovací proces je posléze zakončen vydáním opatření obecné povahy.

V případě systémů spravovaných orgánem veřejné moci NBÚ nejprve předkládá ministerstvu vnitra seznam navržených systémů KII, to jej projednává v pracovních komisích vlády a následně předává vládě, která systémy určí svým usnesením. [51, 53]

Určování systémů KII soukromoprávních subjektů bylo rozděleno do třech vln. První vlna již proběhla (květen 2015 schváleno 45 prvků ministerstev a ústředních správních úřadů), další dvě (další organizační složky státu, soukromý sektor včetně státních podniků) stále probíhají. [51, 53]

Krizový zákon může být předmětem kritiky z hlediska odvětvových kritérií, kde v některých odvětvích existují „bílá místa“, kterých se zákon nedotýká i když by z povahy věci měl. Např. se jedná o oblast zdravotnictví, kde je kritérium pro určení prvku KI 2500 akutních lůžek, takové zdravotnické zařízení ale v ČR není. V odvětvových kritériích pro KI také není zařazen chemický průmysl [1], přičemž negativní dopady (ve smyslu průřezových kritérií krizového zákona) v této oblasti mohou být jistě značné.

Pro ilustraci – ke dni 5.4. proběhlo 160 jednání mezi NBÚ a soukromými i státními subjekty, ve veřejném sektoru bylo určeno 48 prvků rozdělených mezi 17 správců a v soukromém sektoru bylo určeno 50 prvků u 19 správců a další jednání stále probíhají. Ke dni obhajoby práce budou tato čísla pravděpodobně větší. [51, 53]

---

[57] které říká, že „*narušení funkce by mělo závažný dopad na bezpečnost státu, základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.*“ [9]

[58] Informace byla poskytnuta v rámci rozhovoru pracovníkem Telco Pro Services, a.s. (skupina ČEZ), kde tato fáze konzultací a ujasňování vzájemných názorů trvala cca 6 měsíců (při schůzích zhruba jednou za měsíc).

Systémy KII ministerstva vnitra

Podle určujících kritérií je možné u některých systémů zjistit, zda spadají pod KII (zda byly určeny skutečně pak lze bez dalších informací pouze odhadnout), na internetu se však dají nalézt i dílčí informace o tom, že některé konkrétní systémy spadají do KII a to z některých článků internetových novin a zejména z různých zveřejněných prezentací – většinou z konferencí nebo jiných setkání na dané téma. Některé nalezené materiály obsahují zřejmě i informace, které by neměly být zveřejněny. Takovým materiálem je např. na internetu dostupná prezentace Ministerstva vnitra[59] [54, slide 17], kde jsou uvedeny pravděpodobně všechny systémy Policie ČR a MV spadající do KII dle přílohy Usnesení vlády ČR č. 390/2015 Sb. a to seřazené v harmonogramu provádění analýz rizik těchto systémů po měsících. Z tohoto dokumentu je možno vyčíst, že mezi informační systémy KII patří kromě informačních systémů základních registrů např. ještě:

- Informační systém PČR služby cizinecké a pohraniční policie,
- Vízový informační systém,
- Schengenský informační systém,
- Centrální registr zbraní,
- Integrovaná telekomunikační síť – IT S,
- Radiokomunikační síť – PEGAS,
- Informační systém pro evidenci udělení azylu,
- Informační systém elektronické spisové služby, aj.

Výše zmíněné jsou tedy příklady systémů KII v resortu vnitra. Pokud se harmonogram uvedený v prezentaci nezměnil, měla by být v době obhájení této práce již hotová analýza rizik téměř všech systémů uvedených v prezentaci.

4.5.2 Významné informační systémy a proces jejich určování

Významné systémy podle ZKB jsou výjimečné tím, že jsou to výhradně systémy, které spravuje stát (slovy zákona orgán veřejné moci tj. ministerstva, jiné správní úřady a územní samosprávné celky[60]). Proces určování VIS je o něco jednodušší než KII a to z těchto důvodů: správci VIS jsou výhradně orgány veřejné moci a tyto systémy nespadají pod krizový zákon. Významný informační systém je definován ZKB tak, že

[59] Dostupné z: http://www.egovernment.cz/setkani/4.pdf

[60] podle z. 365/2000 Sb., o informačních systémech veřejné správy

- musí být spravován orgánem veřejné moci,
- nesmí být zároveň kritickou informační infrastrukturou,
- může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.

K výše uvedenému musí – analogicky jako u systémů KII – naplnit určitá určující kritéria. Pro VIS jsou tato kritéria jsou uvedena ve vyhlášce č. 317/2014 Sb. o významných informačních systémech a jedná se o:

- *dopadová kritéria*[61],
- *oblastní kritéria*[62].

Opět platí, že musí být naplněno alespoň jedno z obou skupin (tj. jedno dopadové a jedno oblastní). Principiálně se tedy jedná o podobné rozlišení jako u kritické infrastruktury – dopadová kritéria určují, jaké dopady by měla nefunkčnost systému způsobená narušením bezpečnosti informací a oblastní kritéria určují konkrétní věcné oblasti, které jsou pro ochranu podstatné (u VIS však pouze oblasti v rámci působení veřejné správy např. vedení správního řízení, výkon spisové služby, elektronická pošta a další). Oproti kritické infrastruktuře jsou dopadová kritéria podstatně mírnější, u první skupiny – § 4 písm. a) VVIS – dopadových kritérií jde především o to, že jejich nefunkčnost může omezit nebo výrazně ohrozit působnost orgánu veřejné moci[63]. Druhá skupina – § 4 písm. b) VVIS – je podobně strukturovaná jako průřezová kritéria KI, ale s daleko mírnějšími dopady, které s výjimkou posledního bodu nesmí dosáhnout hodnot průřezových kritérií pro určení prvku KI:

- *ohrožení nebo narušení prvku kritické infrastruktury,*
- *oběti na životech s mezní hodnotou více než 10 mrtvých nebo 100 zraněných osob vyžadujících lékařské ošetření, s případnou hospitalizací s dobou delší než 24 hodin,*
- *finanční nebo materiální ztráty s mezní hodnotou více než 5% stanoveného rozpočtu orgánu veřejné moci,*
- *zásah do osobního života nebo do práv fyzických nebo právnických osob postihující nejméně 50000 osob, nebo*
- *výrazné ohrožení nebo narušení veřejného zájmu, přičemž následky podle bodů 1 až 4 nedosáhnou hodnot pro určení prvku kritické infrastruktury podle průřezových kritérií stanovených krizovým zákonem.* [55]

---

[61] Pro srovnání s výše uvedenými průřezovými kritérii KI:

[62] § 3 vyhlášky 317/2014 Sb.

[63] omezit *„po dobu delší než 3 pracovní dny“* a nebo *„výrazné ohrožení výkonu působnosti orgánu veřejné moci, které lze odvrátit za vynaložení nepřiměřených nákladů na provoz nebo obnovu informačního systému*“ [55]

Protože kraje (krajské úřady) nevykonávají všechny činnosti, které vykonávají ostatní orgány veřejné moci, jsou oblastní kritéria ještě takto rozdělena [53]:

- *kritéria u orgánu veřejné moci* (14 kritérií) a
- *kritéria u orgánu veřejné moci – kraje v rámci přenesené působnosti* (10 kritérií).

Protože se průzkum v práci zabývá krajskými úřady, uvádím zde kritéria z přílohy VVIS pro kraje:

- databáze obsahující osobní údaje,
- vedení správního řízení,
- hospodaření orgánu veřejné moci,
- elektronická pošta,
- vedení internetových stránek,
- příprava na krizové situace a jejich řešení,
- mezinárodní spolupráce,
- státní dozor,
- kontrolní a inspekční činnost,
- zadávání veřejných zakázek. [55]

Určování VIS se dělí podle toho, zda se jedná o systém uvedený v příloze 1 vyhlášky 317/2014 Sb. a nebo systém, který uvedený v příloze vyhlášky není[64]. U systémů, které nejsou uvedeny v příloze této vyhlášky, provede určení správce systému. Určovací proces VIS tedy končí okamžikem, kdy jej za takový správce systému označí. Toto může být oficiálně vydáním interního právního aktu, které ale není ze zákona povinné, jedná se pouze o fakultativní (byť NBÚ doporučovaný) krok. Podle slov A. Kučínského z NBÚ na přednášce během ISSS 2016 se NBÚ dozví o VIS prakticky tak, že mu přijde formulář pro hlášení kontaktních údajů pro daný systém. [50]

Na tomto místě pro připomenutí znovu zmiňuji novelizaci VVIS (o ní více v kap. 4.1.3 Plánovaná novelizace ZKB a vyhlášky č. 317/2014 Sb.), kterou budou některé systémy z VIS vyřazeny (některé z důvodu přesunutí do KII a některé vyřazeny pro nenaplnění kritérií VIS ani KII). Toto potvrzuje, že proces určování je kontinuální.

Za zajímavý autor považuje fakt, že podle NBÚ (prezentace ze září 2015 [1]) by kritéria pro VIS mohly naplnit i některé univerzity.

---

[64] Ve vyhlášce měly být po novelizaci uvedené i ty, které dosud uvedené nebyly – např. právě významné informační systémy krajských úřadů. Seznam VIS, které krajské úřady navrhovaly v připomínkovém řízení o novelizaci VVIS je uveden v příloze E.

U určování VIS také existují „bílá místa“ podobně jako u krizového zákona. Zde se jedná zejména o vyloučení velkých měst, která spravují důležité systémy (a jistě by naplnily kritéria VIS, pokud by nebyly vyčleněny). Také někteří správci důležitých informačních systémů nejsou orgány veřejné moci. [1]

Už samotný proces určování působí jako administrativní zátěž na dotčené organizace, které musí vědět, jaké systémy za jakým účelem spravují a zejména pak provést analýzu dopadů nefunkčnosti jejich systémů na základní funkčnost kraje na základě které rozhodnou, jaké systémy zařadí mezi VIS. Z veřejně dostupných materiálů Kraje Vysočina lze zjistit, že krajům (a pravděpodobně i ostatním OVM) je doporučováno posoudit naplnění kritérií pro VIS u jednotlivých informačních systémů interním aktem řízení a to v následující posloupnosti činností:

- *vytvoření seznamu jednotlivých informačních systémů*,
- *stanovení kompetencí (statutárním orgánem) za posouzení naplnění kritérií pro VIS ze seznamu*,
- *u jednotlivých systémů, které naplňují kritéria pro VIS, vydefinování, o která kritéria se jedná*,
- *vytvoření závěrečné zprávu o posouzení naplnění kritérií u jednotlivých systémů*,
- *schválení závěrečné zprávy statutárním orgánem*,
- *nahlášení kontaktních údajů na NBÚ*[65]. [56]

Podstatné je, že tato činnost se neprovádí jen jednou. Jedná se o kontinuální proces, kdy je nutno sledovat informační systémy organizace a pokud některý naplní určující kritéria VIS, je nutno jej nahlásit NBÚ. Je tedy zřejmé, že tato činnost musí být svěřena některému pracovníkovi nebo organizačnímu celku do náplně práce nebo činnosti.

Významné informační systémy na krajských úřadech

Příkladem subjektů, které spravují systémy neuvedené v příloze vyhlášky o VIS, jsou krajské úřady. Mezi systémy, které krajské úřady určily/určují jako významné, patří zejména jejich ekonomické systémy, systémy spisové služby, ale také i webové portály a emailové systémy nebo jiné systémy (výjimečně). Systémy, které krajské úřady určily jako VIS jsou uvedeny v příloze E této práce. Např. Kraj Vysočina vybral jako VIS tyto systémy (uvedeno ve zprávě o posouzení VIS tohoto kraje [57]):

- GINIS - Ekonomické moduly (komplexní ekonomické agendy),
- GINIS SSL (elektronický systém spisové služby),

[65] Pro doplnění – materiál, ze kterého je čerpáno, byl vytvořen pro jednání rady kraje v lednu 2016.

- Webový portál kraje Vysočina (interní a externí web kraje),
- Elektronický poštovní systém (elektronická pošta v rámci krajského úřadu).

Některé kraje (např. Plzeňský, Olomoucký) zařadily mezi VIS i integrační sběrnici zajišťující komunikaci mezi interními systémy KrÚ a systémem základních registrů.

4.6 Povinnosti správců systémů KII a VIS vyplývající ze ZKB

Povinnosti, které vyplývají orgánům a osobám ze ZKB se různí podle toho, o kterou osobu či orgán pole § 3 se jedná. Pro osoby § 3 písm. a) se jedná pouze o hlášení kontaktních údajů národnímu CERT, pro písm. b) jsou o něco větší – kromě hlášení kontaktních údajů přibývá detekování kybernetických bezpečnostních událostí a hlášení kybernetických bezpečnostních incidentů národnímu CERT.

Detailněji se kapitola zaměřuje na správce systémů KII a správce VIS a to především vzhledem k tomu, že následný průzkum se zaměřuje na krajské úřady, u kterých se předpokládá, že budou ve většině případů správci VIS jen výjimečně KII. V následujících podkapitolách je tedy pojednáno o povinnostech těchto subjektů. Grafické znázornění všech povinností vyplývajících ze ZKB zpracoval přehledně NBÚ v jenom ze svých pomocných materiálů[66] a NBÚ byl také zpracován velmi užitečný materiál typu „checklistu“ pro snadnější provádění auditu bezpečnostních opatření[67]. V následujících podkapitolách níže jsou rozebrány nejpodstatnější povinnosti z hlediska dopadů na dotčené organizace.

4.6.1 Bezpečnostní opatření

Dle slov zákona se bezpečnostním opatřením rozumí *„souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací v kybernetickém prostoru.*“

Povinné osoby (správci systémů KII a správci VIS) musejí implementovat a provádět množství opatření sloužící k zajištění bezpečnosti jejich informačních a komunikačních systémů. Jedná se o:

[66] Tento materiál ukazuje povinnosti z hlediska systému kybernetické bezpečnosti státu: Dostupný z: https://www.govcert.cz/download/nodeid-686/

[67] Tento materiál ukazuje přehledně povinnosti z hlediska vyhlášky č. 316/2014 Sb. Dostupný z: https://www.govcert.cz/download/nodeid-588/

- bezpečnostní opatření, která se dělí na
  - organizační opatření a
  - technická opatření.
- další opatření, která jsou nad rámec bezpečnostních opatření a jsou předmětem kap. 4.6.2.

Obsah bezpečnostních opatření, obsah a strukturu bezpečnostní dokumentace a rozsah bezpečnostních opatření pro dotčené subjekty stanoví prováděcí předpis – vyhláška 316/2014 Sb. Autor se domnívá, že nemá smysl (i vzhledem k rozsahu práce) do detailu zde rozebírat jednotlivá opatření. Podstatné je, že se jedná o komplexní zajištění systému řízení bezpečnosti informací v organizaci vycházející z ISO/IEC 27001 a to jak z organizačního, tak z technického hlediska. Dále je podstatné, že správci VIS mají povinnost plnit zhruba 60% povinností oproti KII [51]. Úlevy pro správce VIS většinou spočívají v tom, že nemusejí zavádět všechna opatření jednotlivých oblastí bezpečnosti do takové hloubky jako správci KII. Rozdíly jsou výborně vidět v „checklistu", který zpracoval NBÚ (zmíněný výše[68]). Tímto NBÚ velmi usnadnil orientaci ve vyhlášce organizacím, které si takový materiál nemusejí pracně samy připravovat. Jako příklad lze uvést oblast organizační bezpečnosti (bezpečnostní role – viz kap. 4.6.3) nebo systém řízení bezpečnosti informací (§ 3 VKB), kde např. správci KII musí provádět audit nejméně jedenkrát ročně, zatímco správci VIS nejméně jednou za tři roky nebo v souvislosti s prováděnými nebo plánovanými změnami. Jistě lze diskutovat, proč to či ono opatření už je mimo povinnost pro správce VIS a naopak. Důležité však je, že se jedná pouze o minimální povinná opatření a pokud organizace (její vedení) dá větší důraz na bezpečnost, může zavést i opatření nad rámec stanovených vyhláškou. Příkladem budiž jeden z krajských úřadů, který zavádí systém řízení bezpečnosti informací pro celý úřad dle ISO/IEC 27001, byť z vyhlášky pro správce VIS taková míra zabezpečení jako povinnost neplyne.

Ve vyhlášce je navržena také struktura bezpečnostní dokumentace (politika systému řízení bezpečnosti informací, politika organizační bezpečnosti, řízení dodavatelů, klasifikace aktiv atd.)[69] a další dokumentace (zprávy z auditu kybernetické bezpečnosti, přezkoumání systému řízení bezpečnosti informací, metodika pro identifikaci a hodnocení aktiv a rizik atd.)[70] Povinné subjekty tak mají vytvořen aspoň základ pro vytvoření své bezpečnostní dokumentace. Zde ovšem velmi záleží na vedení organizace a

[68] Viz předchozí poznámka pod čarou.

[69] Viz přílohu 4 VKB.

[70] tamtéž

osobách zodpovědných (pokud takové vůbec jsou[71]) za oblast bezpečnosti v organizaci – i při dodržení vytvoření všech povinných a doporučovaných materiálů stále hrozí riziko zavedení do velké míry formální bezpečnosti, která existuje převážně (jen) papíře, ale ve skutečnosti nemá na bezpečnost v organizaci reálný pozitivní dopad. Poměrně vágní definice bezpečnosti na základě zákona 365/2000 Sb. a jeho prováděcích předpisů[72], které kladou důraz zejména na dokumentaci bezpečnosti, než na faktické zavedení konkrétních opatření, mohou tomuto přístupu být nápomocny.

Protože ZKB je postaven na principu autonomie vůle regulovaných subjektů ve spojení s principem technologické neutrality, jsou v zákoně (a vyhlášce) sice stanoveny konkrétní cíle bezpečnostních opatření, ale forma jejich realizace je ponechána na vůli regulovaného subjektu. To znamená značnou volnost ve výběru architektury, technologií i dodavatelů. [24] Jak dále uvádí [24], určitou nevýhodou tohoto řešení je skutečnost, že *„povinné subjekty budou mít jen omezenou míru právní jistoty ohledně otázky, zda právě jejich konkrétní řešení odpovídá zákonným požadavkům“* I přes velkou míru určitosti vyhlášky je tato v některých ohledech stále ještě dosti abstraktní.

Z hlediska dopadů do organizace lze na základě výše uvedeného předpokládat, že – pokud nebyla bezpečnost řešena již dříve na úrovni povinností dle ZKB – bude mít zavedení bezpečnostních opatření pozitivní vliv na kvalitu bezpečnosti informací organizace. Do jaké míry bude bezpečnost prováděna formálně a do jaké míry bude skutečně účinná bude záležet zejména vedení a odpovědných pracovnících.

Pokud organizace bezpečnost neřešila na úrovni požadavků na ni kladených dle ZKB, nutně bude dopadem také velká administrativní a finanční zátěž, neboť ustanovení a zavedení systému řízení bezpečnosti informací včetně technických prostředků (pokud nebyly používány už před tím) si žádá značné prostředky.

Pro potvrzení či vyvrácení těchto tezí slouží část průzkumu kap. 5, která je věnována zjišťování náročnosti zajišťování souladu organizace se ZKB a také alespoň stručné

---

[71] V rámci průzkumu uvedeném v kap. 5 jeden z respondentů uvádí (a dává najevo svůj nesouhlas), že dosud bohužel není u nich v organizaci žádný pracovník zodpovědný za řízení kybernetické bezpečnosti (sic!). Některé krajské úřady mají naopak takových pracovníků několik s jasně rozdělenými kompetencemi. Na tomto příkladu lze vidět, do jaké míry je bezpečnost organizace i ve veřejné správě (kde by bylo na místě očekávat velkou míru standardizace) ovlivněna pochopením jejího vedení pro bezpečnost.

[72] Vyhláška č. 529/2006 Sb. o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy); vyhláška č. 530/2006 Sb. o postupech atestačních středisek při posuzování dlouhodobého řízení informačních systémů veřejné správy.

zjištění toho, zda organizace již měla snahu zavádět bezpečnost dle oborových standardů a zda tato bezpečnost převyšovala či nepřevyšovala požadavky kladené ze ZKB a vyhlášky.

4.6.2 Povinnosti nad rámec bezpečnostních opatření

Kromě výše zmíněných bezpečnostních opatření mají z hlediska ZKB povinné subjekty ještě další povinnosti, těmi jsou:

- hlášení kontaktních údajů vládnímu cert týmu,
- provádění reaktivních opatření,
- oznámení o provedení reaktivních opatření vládnímu CERT,
- detekce kybernetických bezpečnostních událostí,
- hlášení kybernetických bezpečnostních incidentů.

Tyto povinnosti, narozdíl od základních bezpečnostních opatření v organizaci, vedou k možnosti koordinovat kybernetickou bezpečnost na úrovni státu. *Hlášení kontaktních údajů* je jednoduchý úkon, který spočívá ve vyplnění formuláře v příloze 7 VKB a jeho zaslání na NBÚ. Formulář sice obsahuje část identifikace informačního systému KII nebo VIS, ale na základě té je teprve povinnost formulář vyplňovat (nelze ji tedy počítat do náročnosti vyplňování formuláře). Jediným náročnějším krokem (než vyplnění názvu organizace, adresy sídla a IČO a zaslání formuláře na NBÚ) tak může být jen určení fyzické osoby, která je za orgán nebo osobu oprávněna jednat ve věcech upravených zákonem. *Provádění reaktivních opatření* a *oznámení o provedení reaktivních opatření* by za normálních okolností (tj. neprobíhající kybernetický útok, který vyžaduje koordinaci z národní/státní úrovně) by nemělo znamenat prakticky žádnou zátěž, kromě zavedení těchto procesů do organizace pro případ jejich potřeby[73]. Nejnáročnější s výše uvedených povinností zřejmě je *detekce kybernetických bezpečnostních událostí.* U detekce kybernetických bezpečnostních událostí velmi záleží na nastavení tohoto procesu v organizaci (nejedná se jen o technické zařízení, ale také správné hlášení incidentů uživatelem, což s sebou nese určité překážky dané tím, že k tomuto musí být uživatel proškolen a musí být přesvědčen, aby tak činil a jde také o určení správné hranice mylné detekce bezpečnostního incidentu / nedetekce skutečného incidentu). Samotné *hlášení kybernetických bezpečnostních incidentů* pak spočívá ve vyplnění formuláře v příloze 5 VKB. Pro úplnost – formuláře správci KII a

[73] U správců systémů KII to znamená ještě také zohlednění těchto reaktivních opatření v hodnocení rizik (VKB § 4 písm. f).

VIS zasílají NBÚ datovou schránkou, e-mailovou zprávou nebo v listinné podobě na adresu tohoto úřadu[74]. Náročnější může být pouze v případě, že by takových incidentů bylo větší množství.

Lze se domnívat, že v souhrnu budou tyto povinnosti nad rámec bezpečnostních opatření podstatně méně náročné z hlediska administrativní i finanční zátěže na organizaci, než zavádění bezpečnostních opatření (viz předchozí kapitolu). Pro posouzení tohoto předpokladu na příkladu krajských úřadů jsou v průzkumu v kap. 5 otázky, které zjišťují nejen hodnocení zátěže bezpečnostních opatření, ale také hodnocení zátěže právě těchto povinností nad rámec bezpečnostních opatření.

4.6.3 Organizování bezpečnosti a bezpečnostní role podle ZKB

Zásadní složkou řízení bezpečnosti je její organizace – jak je začleněna v organizační struktuře organizace, kolik pracovníků ji řeší, jaké jsou určené role a jejich povinnosti. Ve VKB jsou pevně stanovené povinné bezpečnostní role, na správce KII jsou opět kladeny přísnější požadavky, u VIS je tato stránka do velké míry ponechána na volbě organizace.

Ve VKB jsou definovány tyto role (§ 6):

- *manažer kybernetické bezpečnosti* (odpovědný za systém řízení bezpečnosti informací),
- *architekt kybernetické bezpečnosti* (zajišťuje návrh a implementaci bezpečnostních opatření),
- *auditor kybernetické bezpečnosti* (provádí audit kybernetické bezpečnosti),
- *garant aktiva* (zajišťuje rozvoj, použití a bezpečnost aktiva).

U správců KII jsou všechny tyto role povinné, pro správce VIS platí, že je má implementovat přiměřeně (viz níže). K těmto rolím VKB definuje ještě *výbor pro řízení kybernetické bezpečnosti* povinný pro správce VIS i KII. Jedná se o organizovanou skupinu na strategické úrovni, která by měla být tvořena osobami, které jsou pověřeny celkovým řízením a rozvojem systémů KII nebo VIS. ZKB ani prováděcí předpisy jej nikterak blíže neregulují, způsob sestavení i složení výboru je tedy plně v rukou vedení organizace. [58] Otázku bezpečnostních rolí a jejich začlenění v organizaci řeší metodický podpůrný materiál NBÚ „Bezpečnostní role a jejich začlenění v organizaci.“[75]

---

[74] Osoby podle 3 § písm. b) hlásí tyto incidenty národnímu CERT přes webový formulář.

[75] Dostupný z: https://www.govcert.cz/download/nodeid-589/

KII – otázka personálního zajištění

Dosti diskutovanou otázkou byla možnost personálního obsazení těchto rolí, neboť na roli manažera, architekta i auditora kybernetické bezpečnosti je vyhláškou kromě proškolení stanoven požadavek nejméně 3 let doložitelné praxe v oboru[76]. To zejména ve veřejné správě může znamenat překážku především vzhledem k možnostem finančního ohodnocení takových pracovníků. Situaci usnadňuje to, že tyto role všechny nemusí být vykonávány různými osobami. Je tedy možné (byť v rozporu s nejlepšími praktikami), aby jedna osoba vykonávala současně např. roli manažera i architekta kybernetické bezpečnosti. [58]

VIS – otázka „přiměřeného" určení bezpečnostních rolí

Vyhláška na správce VIS neklade takové nároky jako na správce KII a říká, že výše zmíněné role mají určit přiměřeně. Materiál NBÚ [58] přesto doporučuje tyto role definovat. Podle materiálu NBÚ [58] pro VIS jsou u těchto rolí menší požadavky na požadovanou praxi apod. Za klíčové NBÚ považuje zejména určení role manažera kybernetické bezpečnosti a garantů aktiv. [51] Jak v tomto případě postupovaly krajské úřady je jedním z předmětů průzkumu v kap. 5.

Zavedení výboru pro kybernetickou bezpečnost je povinné i u VIS, v dotazníku byla přesto v rámci zjišťování zaváděných rolí na krajských úřadech ponechána možnost odpovědět, zda úřady tento výbor zavedou. Autor považuje za zajímavé, že jeden z úřadů uvedl, že o zřízení tohoto výboru zatím neuvažuje, protože z důvodu možného outsourcingu.

V zákoně ani ve vyhlášce nejsou vymezena přesná kritéria pro vzdělání rolí kybernetické bezpečnosti v organizaci. Je tak v tomto ohledu ponechána velká míra svobody managementu. To na druhou stranu znamená, že lze vzdělání „doložit" absolvováním prakticky jakéhokoli kurzu s daným zaměřením, což nemusí být pro požadovanou odbornost vždy ideální. Pokud by ale bylo stanoveno konkrétní penzum znalostí, stát by je pravděpodobně musel také nějak testovat a tím by opět rostla administrativa kladená shora na povinné subjekty. Snaha tvůrců ZKB byla (alespoň v tomto ohledu) ponechat co největší svobodu. Je však možné, že do budoucna bude nějaký certifikační program uveden.

[76] U manažera praxe s řízením informačních systémů, u architekta praxe s navrhováním bezpečnostní architektury, u auditora praxe v provádění auditů.

4.6.4 Lhůty k plnění povinností

Pro povinné subjekty se v ZKB nachází několik lhůt:

- lhůta pro nahlášení kontaktních údajů,
- přechodná lhůta pro implementaci bezpečnostních opatření dle VKB.

Kontaktní údaje musely nahlásit povinné subjekty podle § 3 a), b) do 30 dnů ode dne nabytí účinnosti zákona. Stejně tak musely učinit správci významných informačních systémů uvedených ve vyhlášce 317/2014 Sb. Správci systémů KII a správci VIS, které nejsou uvedeny ve vyhlášce, měli (a budoucí určené budou muset) kontaktní údaje nahlásit do 30 dnů ode dne, kdy skončil určovací proces daného systému (tzn. den, kdy bylo vydáno opatření obecné povahy nebo usnesení vlády o určení systému KII nebo den, kdy správce posoudil svůj systém jako VIS[77].) Hlášení kontaktních údajů spočívá ve vyplnění daného formuláře (v příloze VKB) a jeho zaslání na NBÚ. Nemělo by tedy činit větší problémy[78].

Více diskutabilní je lhůta určená pro implementaci všech bezpečnostních opatření, která činí 1 rok od skončení určovacího procesu[79] (prakticky od stejného okamžiku jako lhůta pro hlášení kontaktních údajů) bez rozdílu, zda se jedná o systémy KII nebo VIS. Zda je roční lhůta k zavedení všech požadovaných povinností dostatečně dlouhá doba je otázkou. Pravděpodobně by měla být tato lhůta schůdnější pro správce VIS, kteří musejí splnit cca 60% požadavků oproti správcům systémů KII. V organizacích veřejné správy je nutné počítat s poměrně dlouhými prodlevami při získávání peněžních prostředků (z rozpočtu a zejména pak při využití fondů EU) a pokud jsou či budou některá opatření zaváděna externě, tak také se lhůtami a administrativní náročností veřejných zadávacích řízení. Roli hraje ale také výchozí stav jejich systémů popř. systému řízení bezpečnosti. Systémy veřejné správy měly povinnost již před ZKB zajišťovat bezpečnost informačních systémů dle zákona č. 365/2000 Sb. Do jaké míry tak činily je také otázkou. Protože z dostupných zdrojů nelze posoudit, zda je roční lhůta pro zavedení bezpečnostních opatření dostatečně dlouhá, byla tato otázka také zařazena do průzkumu v kap. 5. a také byly zařazeny otázky, které měly za cíl zjistit alespoň základná informace o výchozím stavu na KrÚ (zda považují požadavky ZKB náročnější, než jimi dříve zaváděná opatření a také jestli používaly při řízení bezpečnosti nějaké

[77] Toto může být oficiálně vydáním interního právního aktu, které ale není ze zákona povinné. Podle slov A. Kučínského z NBÚ na přednášce během ISSS 2016 se NBÚ dozví o VIS prakticky tak, že mu přijde formulář pro hlášení kontaktních údajů pro daný systém. [53]

[78] Ve formuláři je však již potřeba vyplnit osobu zodpovědnou za kybernetickou bezpečnost v organizaci, se kterou bude vedena případná komunikace. Organizace tedy musí někoho před odesláním formuláře určit.

[79] viz kap. 4.5.1.

oborové standarty nebo normy). Tato problematika je také diskutována z pohledu výchozího stavu kybernetické bezpečnosti a standardů řízení bezpečnosti v kap. 4.7.2 ZKB, ISO/IEC 27001 a úroveň bezpečnosti povinných subjektů.

4.7 Vybrané aspekty ZKB vzhledem k jeho uplatňování a k průzkumu

4.7.1 Finanční podpora – Výzva č. 10 Integrovaného regionálního operačního programu

Jak vyplývá ze strategických a koncepčních dokumentů, kybernetická bezpečnost je pro Evropskou unii jednou z podstatných priorit. Důkazem toho může být skutečné uvolnění finančních prostředků ze strukturálních fondů EU, které se v ČR projevilo vyhlášením Výzvy č. 10 Kybernetická bezpečnost k žádostem o podávání podpory z Integrovaného operačního regionálního programu (IROP). Tato výzva byla vyhlášena Ministerstvem pro místní rozvoj v září 2015 a je alokována ve výši 1,4 mld.[80] Kč. Výzva se přímo týká podpory povinných subjektů ZKB a to konkrétně správců systémů kritické informační infrastruktury a významných informačních systémů. Prostředky jsou však určeny (pouze) na technická opatření vyplývající ze ZKB (není tedy možno tyto prostředky použít na administrativní nebo organizační opatření, byť také ze ZKB vyplývají). [59]

Ke dni 5.4.2016[81] ještě nebyl na Ministerstvo pro místní rozvoj žádný projekt podán, ale některé subjekty již na projektech pracují a konzultují je s ministerstvem. Vzhledem k tomu, že prostředků je zatím dostatek a subjekty mezi sebou nemusí soutěžit o to, kdo dřív projekt podá, není takový tlak na co nejdřívější podání[82]. Tomu, že žádný projekt nebyl podán také nahrává fakt, že vyplnit dobře žádost o podporu z IROP je poměrně náročné a následné audity mohou být pro organizace neméně náročné. [59]

Pokud se organizaci úspěšně podaří čerpat prostředky z těchto fondů a projdou i následnými audity, pak tato výzva může být velmi užitečná ve snížení finančních dopadů

[80] Jedná se o alokaci s kofinancováním. Celková alokace z Evropského fondu pro regionální rozvoj (EFRR) je 4,64 mld. EUR. Kofinancování je v poměru 85% EFRR a 15%národní spolufinancování případně 80,863% EFRR a 19,137% národní u celorepublikových projektů. Tato podpora spadá do prioritní osy 3 – instituce a strategického cíle 3.2 „Zvyšování efektivity a transparentnosti veřejné správy prostřednictvím rozvoje využití a kvality systémů IKT“

[81] Přednáška Aleše Pekárka z Ministerstva pro místní rozvoj na konferenci ISSS 2016, kde pouze ústně zmínil uvedené.

[82] Dle slov A. Pekárka z přednášky zmíněné v předchozí poznámce.

ZKB na organizace. Otázkou je, zda administrativní zátěž tyto výhody nepřevýší. Ochotu využití prostředků IROP ze strany krajských úřadů jsem proto zařadil do otázek průzkumu (viz kap. 5 Průzkum kybernetické bezpečnosti na krajských úřadech).

4.7.2 ZKB, ISO/IEC 27001 a úroveň bezpečnosti povinných subjektů před ZKB

Autoři ZKB[83] i jiné zdroje uvádějí, že při tvorbě vyhlášky obsahující souhrn bezpečnostních opatření bylo vycházeno především z normy ISO/IEC 27001:2013. Z toho lze vyvodit několik závěrů:

- vyhláška je postavena na mezinárodně uznávaných nejlepších praktikách,
- organizace, které již svou bezpečnost řídily (byť částečně nebo bez certifikace) na základě ISO/IEC 17799 nebo 27001, mají část požadavků dle VKB pokrytou a o to nižší jsou následně nutné investice na zajištění souladu s požadavky.

Nejpodstatnější souvislost mezi standardem ISO/IEC 27001 a ZKB s klíčovým dopadem do organizací, které musí být v souladu se ZKB je fakt, že zákonné požadavky na zavedení bezpečnostních opatření lze splnit prokázáním certifikace dle této normy (ISO/IEC 27001:2013 případně ČSN ISO/IEC 27001:2014). Pokud je informační nebo komunikační systém povinných osob (platí pro správce KII i VIS) zcela zahrnutý do systému řízení bezpečnosti informací, který je certifikovaný na základě těchto norem a k tomu vede patřičnou dokumentaci (vymezená v § 29 VKB), pak splňuje požadavky na zavedení bezpečnostních opatření podle ZKB a navazující VKB. Certifikační orgán musí být akreditovaný. Výše uvedené je předmětem § 29 vyhlášky o kybernetické bezpečnosti.

V důvodové zprávě k ZKB (kapitola *technická a ekonomická náročnost zavádění bezpečnostních opatření u povinných osob*) se uvádí, že *většina subjektů*[84], které budou zavádět povinně bezpečnostní opatření, již řeší kybernetickou bezpečnost vlastní organizace na úrovni standardů ISO/IEC 20000 nebo ISO/IEC 27001. Uvádí pak doslova: „*vzhledem k tomu, že navrhovaná právní úprava z těchto standardů vychází, neměla by být*

[83] Dle ředitele Národního centra kybernetické bezpečnosti Vladimíra Rohela byly využity mezinárodní normy všude, kde byly aplikovatelné. [45]

[84] Otázkou je, co konkrétně znamená „většina subjektů“. Většina znamená více než polovina, pokud se jedná např. o 60% subjektů, není již výhled zdaleka tak optimistický.

adaptace na zákonné povinnosti v takových případech otázkou prakticky žádných dodatečných investic[85]“. [8] Znamená to mj. že zákonodárce nepovažoval povinnosti nad rámec těchto bezpečnostních opatření[86] za technicky a ekonomicky náročné. Dále se uvádí: „*Tam, kde není u orgánů a osob s povinností zavádět bezpečnostní opatření dosud tato problematika řešena (což je vzhledem k důležitosti těchto systémů, služeb a sítí možno jednoznačně považovat za chybu na straně správce, resp. poskytovatele), počítá navrhovaná právní úprava s přechodným obdobím.*“ [8] Lze naprosto souhlasit, že se jedná o chybu, pokud bezpečnost nebyla na adekvátní úrovni řešena. Z citovaného textu však vyplývají dvě otázky:

- **První otázka:** Pokud by se ukázalo u orgánů veřejné moci, že bezpečnost na adekvátní úrovni neřešily, jedná se v případě těchto orgánů veřejné moci (krajských úřadů vzhledem k tématu průzkumu) čistě o jejich chybu a nebo se jedná o systémovou chybu poukazující na nedostatečné metodické vedení?
- Z citovaného tvrzení vyplývá, že zákonodárce navrhuje přechodnou dobu[87] zejména pro ty subjekty, kde nebyla problematika bezpečnosti adekvátně řešena. **Druhou otázkou** tedy je, zda je toto přechodné období dostatečně dlouhé i pro povinné osoby, které bezpečnost na adekvátní úrovni neřešily.

Z výše uvedeného tedy plyne vhodnost zkoumání toho, na jaké kvalitativní úrovni povinné subjekty bezpečnost skutečně řešily a zda a do jaké míry se v těchto organizacích uplatňovaly výše zmíněné standardy – z toho následně vyplývají dopady v podobě míry administrativní a finanční zátěže nutné ke splnění zákonných požadavků. Protože se na tuto otázku nedá odpovědět z rešerše veřejně dostupných zdrojů, situaci na krajských úřadech v tomto ohledu zkoumá průzkum v kap. 5. V průzkumu je zahrnuta otázka zjišťující, zda krajské úřady používaly nějaké (případně jaké) standardy k řízení bezpečnosti informací ještě před ZKB, zda považují zákonné požadavky za přísnější, než jimi dříve zaváděné a také je zahrnuta otázka zjišťující názor respondentů z povinných subjektů na délku přechodného období.

4.7.3 Dopad ZKB na obce

Informační systémy obcí, přestože by měly některé z nich splňovat určující kritéria pro významné informační systémy (především vzhledem k počtu obyvatel), jsou z působnosti ZKB vyjmuté (§ 3 vyhlášky 317/2014 Sb. odst. 2). Přestože NBÚ potvrzuje, že obce jsou z působnosti ZKB vyjmuté, doporučuje jim dobrovolně vyžít nově vzniklé

[85] zvýrazněno autorem této práce

[86] Viz kap. 4.6.2 Povinnosti nad rámec bezpečnostních opatření.

[87] Viz kap. 4.6.4 Lhůty k plnění povinností.

standardy při zabezpečování svých informačních systémů. Obce totiž také mají povinnost mají povinnost zajišťovat bezpečnost svých informačních systémů a to podle zákona č. 365/2000 Sb., o informačních systémech veřejné správy (o tom více v kap. 4.2 Proč zákon o kybernetické bezpečnosti).

ZKB ale i přes to na obce určitý dopad mít může. Obce totiž provozují a užívají systémy jiných správců, které již spadají pod působnost zákona (např. systém základních registrů a další). Tito správci mohou na obce některé povinnosti přenášet, takže ZKB na obce ale nepřímo, v omezeném rozsahu a na jiném právním základě. [60] Konkrétnější informace se autorovi nepodařilo zjistit. Je určitá pravděpodobnost, že obce by do budoucna mohly být regulované, oficiální zdroje ale takové záměry neuvádějí.

Vzhledem k povinnostem zabezpečit svůj informační systém, nepřímému dopadu zákona na obce a objektivní bezpečnostní situaci je obcím doporučeno řídit bezpečnosti informací obdobným způsobem, jaký zavádí ZKB a vyhláška. [60]

4.7.4 Pomocné materiály od NBÚ

Zákon a to, jak jej NBÚ propaguje, nechává v určitých ohledech povinným osobám poměrně velkou svobodu. Dle autorových zjištění na základě nalezených materiálů lze usuzovat, že NBÚ jde o výsledek spíše než o byrokracii a snaží se zavedení ZKB do praxe pokud možno usnadnit. To dokládá vydání řady dokumentů sloužící jako pomůcky, které přehledným způsobem vysvětlují různé pojmy, problémy a doporučení k jejich zavádění. Jsou tu např. pomocná schémata, podle kterých lze určit, zda daná osoba spadá pod působnost ZKB nebo do kritické informační infrastruktury či mezi významné informační systémy. Dále pak pomocné dokumenty ohledně bezpečnostních rolí a jejich začlenění do organizační struktury organizace, vysvětlení nepřiměřených nákladů, přehledné schéma s lhůtami a přechodnými obdobími. Tyto dokumenty jsou vesměs přehledné, stručné a jasné. Ve všech je výslovně uvedeno, že se jedná jen o „podpůrné vodítko“ a nenahrazují zákon ani související předpisy, což je pochopitelné.

NBÚ také uvádí, že při kontrolách neplánuje za každou cenu sankcionovat pokutami a blokováním systémů, spíše se bude snažit řešit nedostatky domluvou.

Pro usnadnění zavádění ZKB do praxe (ať již stavění ISMS podle vyhlášky nebo auditování) stojí za zmínku zejména dokument pro audit opatření podle VKB – tedy „checklist“, kde jsou v tabulce přehledně vypsané všechny požadavky vyhlášky 316/2014 s tím, že jsou řazené po paragrafech a odstavcích vyhlášky a zároveň je uvedeno, zda se povinnost týká KII, VIS nebo obou dvou. To velmi zjednodušuje orientaci v povinnostech povinných osob. Tyto dokumenty jsou k nalezení na stránkách NKCB zde: https://www.govcert.cz/cs/kii--vis/kii--vis/

4.7.5 Stav kybernetického nebezpečí

V ČR je z krizové legislativy známo několik mimořádných stavů (stav nebezpečí, nouzový stav, stav ohrožení státu, válečný stav, viz kap. 3.1.1 Krizové stavy). ZKB přidává k těmto stávajícím krizovým stavům nový – Stav kybernetického nebezpečí. V čem tento stav spočívá?

Takto mluví zákon: *„Stavem kybernetického nebezpečí se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací*[88]*."* [61] Podobně jako výše zmíněné mimořádné stavy umožňuje tento stav státu rozšíření pravomocí za hranici běžných možností fungování. Při vyhlášeném stavu kybernetického nebezpečí nedochází k žádnému navýšení kompetencí NBÚ, pouze pod jeho běžné zákonem vymezené kompetence, které se aplikují za normálních okolností na KII a VIS, spadají i subjekty podle § 3 písm. a) a b) ZKB (tj. poskytovatelé služeb a sítí elektronických komunikací a subjekty zajišťující významné sítě). Po vyhlášení tohoto stavu se tedy musí do míry vymezené zákonem řídit pokyny NBÚ i subjekty, které se jimi jinak řídit nemusí. Nejedná se tedy zdaleka o tak razantní zásahy do práv osob jako u krizových stavů podle krizového zákona. Přesto se ale považuje stav kybernetického nebezpečí za natolik závažný (slovy zákona naléhavý veřejný zájem), že provozovatelé rozhlasového a televizního vysílání mají v souvislosti s ním povinnost poskytnout státnímu orgánu (NBÚ) nezbytný vysílací čas pro informování veřejnosti[89]. O vyhlášení stavu kybernetického nebezpečí rozhoduje ředitel NBÚ, zveřejňuje se v rádiovém a televizním vysílání a tento stav je časově omezený.

Stav kybernetického nebezpečí se dotýká zejména orgánů a osob 3 § a), b), které během tohoto stavu musí provádět reaktivní opatření vydaná NBÚ a také posílat oznámení o provedení těchto reaktivních opatření vládnímu CERT týmu. Správci systémů KII a VIS mají tyto povinnosti i bez vyhlášení stavu kybernetického nebezpečí, takže dopady vyhlášení tohoto stavu jsou na správce systémů KII a VIS minimální.

---

[88] Tj. zákon č. 412/2005 Sb., ochraně utajovaných informací a o bezpečnostní způsobilosti

[89] Dle zákona č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a o změně dalších zákonů (který byl změněn zákonem o kybernetické bezpečnosti § 37). Takovou povinnost mají dále v souvislosti s vyhlášením nouzového stavu, stavu ohrožení státu, válečného stavu a opatřením na ochranu veřejného zdraví[89].

4.8 Kritika ZKB

Kritiku zákona o kybernetické bezpečnosti lze rozdělit do několika oblastí. Kritizovat se dají např. konkrétní formulace, legislativně-technické provedení předpisu, terminologie, vybrané povinné subjekty, rozsah povinností, způsob stanovení bezpečnostních opatření (prováděcí předpis) a další oblasti.

Jedním z bodů kritiky ZKB jsou otázky týkající se jeho prováděcích předpisů. Konkrétně zda není přesunuto do prováděcích předpisů příliš mnoho důležitých prvků a také zda by nebylo lepší řešit poměrně rozsáhlé pasáže odpovídající normám řady ISO/IEC 27000 odkázáním se právě na tyto normy. [62]

Další otázkou, která může být předmětem kritiky, je také rozdílná terminologie oproti zákonu č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. Na tuto skutečnost poukázal Smejkal v článku [62] a diskutuje kriticky také podmínky pro postup výběru národního CERT (článek vyšel ještě v době, kdy zákon byl ještě ve fázi návrhu).

Zásadní otázkou, která byla kladena odbornou veřejností při diskuzi ohledně ZKB také bylo, zda není nadbytečné vytvářet na pokrytí kybernetické bezpečnosti samostatný zákon místo toho, aby byly vhodně rozšířeny a využity stávající zákony týkající se informatiky veřejné správy, které aspekt bezpečnosti již obsahují. Proti tomuto bodu kritiky stojí pragmatický názor, že jednotná norma je pro „uživatele“ přehlednější a takto je také bude v praxi snadněji prosaditelná a implementovatelná. [63] Úprava se také takto stala pravděpodobně lépe viditelnou a medializovatelnou. Zároveň tím ale zákonodárce na sebe bere odpovědnost vysvětlit nutnost tohoto kroku veřejnosti. [64]

Existuje také názor (viz [65]), že takový zákon nepotřebujeme, neboť by oblast ohrožení státu měla být zahrnuta do zákona o krizovém řízení. Zdůvodňován je tím, že velké útoky na informační a komunikační infrastrukturu by se týkaly i dalších oblastí fungování státu a tak i dalších „nepočítačových“ složek krizového řízení. [65]

Právní regulace v této oblasti přirozeně může vyvolávat (a také v počátcích vyvolávala [63]), obavy o soukromí občanů i firem, strach z odposlouchávání či dokonce cenzury internetu. Vzhledem ke koncepci zákona – pokud se nezmění – je nyní zřejmé, že jsou tyto obavy zbytečné. V internetovém blogu [65] se objevuje trefné přirovnání se stanicemi STK – jde o implementaci určitých technologických i organizačních pravidel, nikoli o kontrolu obsahu – tedy dá se s určitým nadhledem přirovnat ke kontrole technického stavu vozidla a jeho způsobilosti k jízdě, nikoli prohledávání zavazadlového prostoru a kontroly převážených lidí.

Lze očekávat, že množství pracovníků organizací, na které ZKB dopadá, jej mohou vnímat jako další regulaci s diskutabilním efektem přinášející mnoho práce. Autor však

přepokládá, že pracovníci, kteří jsou si vědomi rizik a mají určité bezpečnostní povědomí, jej budou hodnotit spíše pozitivně. Jaký mají skutečně názor na ZKB pracovníci krajských úřadů zjišťuje průzkum provedený v kap. 5.

Předmětem diskuze může být také (ne)pokrytí určitých oblastí zákonem – např. vyčlenění obcí ze správců významných informačních systémů přes to, že některé mají vzhledem k počtu obyvatel systémy, jejichž narušení by mělo významné dopady. Některé důležité informační systémy, které by splnily kritéria VIS naopak nejsou spravovány orgánem veřejné moci a tak mezi VIS nespadají. Co se týče kritérií kritické informační infrastruktury, není zahrnuto např. odvětví chemického průmyslu a kritérium pro zdravotnická zařízení je takové, že jej nenaplňuje žádné zdravotnické zařízení ČR. [1] Tato kritéria pro určení kritické infrastruktury jsou spíše záležitostí krizového zákona a navazující vyhlášky než ZKB, ale kybernetická legislativa s nimi tvoří logický celek.

4.9 Shrnutí dopadů ZKB na povinné subjekty

V kapitolách 4.2 až 4.8 byl proveden rozbor ZKB z hlediska dopadů na povinné subjekty se zaměřením na správce systémů KII a VIS. Předmětem této kapitoly je shrnutí nejpodstatnějších dopadů, které lze u těchto povinných subjektů předpokládat, a výběr dopadů a oblastí, které budou dále předmětem průzkumu v kap. 5.

4.9.1 Zátěž (administrativní, finanční, personální)

ZKB klade na povinné subjekty značné požadavky, které nutně musí znamenat podstatnou administrativní, finanční a personální zátěž. Tyto dopady lze řadit mezi negativní dopady ZKB z pohledu organizace.

Administrativní zátěž

Administrativní zátěž vyplývá na povinné subjekty především nutnosti zavést a provádět komplexní systém bezpečnostních opatření dle vyhlášky 316/2014 Sb. Jedná se o značný zásah (pokud organizace neřešila bezpečnost na požadované úrovni) do procesů organizace. Kromě jiného musí být prováděna analýza rizik (na určené úrovni), vedena rozsáhlá bezpečnostní dokumentace, zaváděny nové technologie atd. Nad rámec těchto bezpečnostních opatření pak ze ZKB plynou další povinnosti – předávání kontaktních údajů NBÚ, provádění reaktivních opatření a jejich hlášení a detekce resp. hlášení kybernetických bezpečnostních událostí resp. incidentů.

Další administrativní zátěž vyplývá také ze samotného určovacího procesu (analýza vlastních systémů, analýza dopadů a srovnávání s určujícími kritérii, konzultace s NBÚ).

Toto vše nutně znamená kromě tvorby významného množství dokumentů také procesní změny, což způsobuje administrativní zátěž.

Finanční zátěž

Pravděpodobně největší finanční zátěž působí nutnost zavedení technologických opatření (fyzická bezpečnost, nástroje detekce kybernetických bezpečnostních událostí a jejich sběr a vyhodnocování aj.) a definování nových pracovních pozic, ale případně i zvyšování kvalifikací personálu (např. školení na bezpečnostní role, provádění školení za účelem zvýšení bezpečnostního povědomí v organizaci) a také outsourcing, pokud organizace uzná za vhodné.

Finanční zátěž na technologická opatření může být naopak snížena využitím prostředků z výzvy č. 10 integrovaného regionálního operačního programu (zvyšuje naopak administrativní zátěž a také skýtá určité riziko případného navrácení prostředků v případě procesního pochybení).

Personální zátěž

Ve vyhlášce 316/2014 Sb. jsou jasně definované bezpečnostní role, které musí povinné subjekty zavést. Pevně jsou stanovené pro správce KII, správci VIS pak určují role přiměřeně dle svého uvážení. Jedná se o role architekta, manažera, auditora kybernetické bezpečnosti, dále o garanta aktiva a výbor pro řízení kybernetické bezpečnosti. Tyto role mohou být svěřeny pouze pracovníkům kompetentním, vyškoleným a s doložitelnou praxí (3 roky v oboru). Některé role mohou splynout v jedné osobě.

I pokud nejsou tyto role stanoveny (může být případ správců VIS), je potřeba v organizaci pověřit někoho zodpovědností za zavádění a řízení kybernetické bezpečnosti.

Personální zátěž lze v určitém smyslu převádět na finanční (náklady na pracovníky případně outsourcing).

4.9.2 Úroveň kybernetické bezpečnosti

Po zavedení všech povinností ZKB a VKB lze očekávat zvýšení úrovně kybernetické bezpečnosti nejen v organizacích, ale také i všeobecně na území ČR (větší bezpečnostní povědomí povinných subjektů, systém varování a koordinace v případě kybernetických hrozeb či útoků). Také lze očekávat větší míru standardizace v řízení bezpečnosti povinných subjektů a to na základě nejlepších praktik, ze kterých vyhláška k ZKB vychází. Celkové zvýšení bezpečnostního povědomí organizací i občanů ČR z hlediska celku potvrzuje i Aleš Špidla, prezident českého institutu manažerů informační bezpečnosti. [66] Tyto dopady lze naopak považovat za pozitivní.

V kap. 4.7.2 byla nastolena otázka administrativních a finančních dopadů na povinné subjekty v závislosti na tom, na jaké kvalitativní úrovni bezpečnost informací zajišťovaly ještě před ZKB. Pokud bezpečnostní opatření zaváděly na úrovni zmíněných standardů (a dle důvodové zprávy k ZKB by to měla být většina organizací), neměly by – dle této důvodové zprávy – pro tyto subjekty plynout prakticky žádné dodatečné investice. Pokud by to tak skutečně bylo, lze očekávat, že by dopady do organizace byly minimální. Zda povinné subjekty (jejich část – krajské úřady) skutečně řešily bezpečnost informací na úrovni zmíněných standardů (tzn. zda požadavky ZKB skutečně nejsou přísnější, než jimi dříve zaváděná opatření) je předmětem průzkumu v kap. 5, konkrétně podkapitoly 5.3.3.

4.9.3 Shrnutí otázek vhodných pro průzkum, které vyplynuly z rozboru ZKB

Z rozboru dopadů ZKB, jež byl předmětem kapitol 4.2 až 4.8 vyplynuly otázky, na které je možné najít odpověď pouze průzkumem skutečného stavu v dotčených organizacích. Jsou to tyto otázky:

- Je předokládáno, že krajské úřady jsou vesměs správci VIS a že jen výjimečně budou správci KII. Je tento předpoklad pravdivý?
- Jaký je názor pracovníků dotčených subjektů na legislativu kybernetické bezpečnosti? Vnímají zákon pouze jako další regulaci ve smyslu „nutného zla“ a nebo vnímají pozitivní přínosy pro organizaci?
- Jsou povinnosti vyplývající ze ZKB přísnější, než dříve zaváděná opatření? (U orgánů veřejné moci – krajských úřadů – tedy povinnosti dle zákona 365/2000 Sb. o informačních systémech veřejné správy.)
- Znamená zajišťování souladu ZKB pro organizace významnou administrativní či finanční zátěž?
- Jsou významné z hlediska administrativní nebo finanční náročnosti i povinnosti nad rámec bezpečnostních opatření? (zasílání kontaktních údajů, detekce a hlášení kybernetických bezpečnostních událostí resp. incidentů)
- Je přechodné období pro zavedení všech povinností povinnými subjekty dostatečně dlouhé?
- Využívaly povinné subjekty nějaké oborové standardy k řízení bezpečnosti? Do jaké míry?
- Jakým způsobem je kybernetická bezpečnost začleněna do organizační struktury povinných subjektů?

- Spoluúčastnily se povinné subjekty na tvorbě legislativy kybernetické bezpečnosti?
- Jsou povinné subjekty ochotné čerpat prostředky z fondů IROP? Pokud nejsou, je to kvůli velké administrativní zátěži?
- Jak se staví povinné subjekty k možnosti outsourcingu kybernetické bezpečnosti? (Řeší zejména případné personální nedostatky.)
- Které dopady ZKB na jejich organizaci vnímají sami pracovníci povinných subjektů jako nejzásadnější?

5 Průzkum kybernetické bezpečnosti na krajských úřadech

5.1 Cíl a metoda průzkumu

Tato kapitola představuje autorem navržený a provedený průzkum, jehož cílem bylo zkoumat a ověřit dopady ZKB na povinné subjekty zjištěné na základě rozboru ZKB v předchozí kapitole a formulované v otázkách v kap. 4.9.3. Smyslem bylo zjistit, zda se zjištěné dopady skutečně v těchto organizacích projevují a tam, kde nelze zjistit objektivní data, alespoň zkoumat názor pracovníků povinných subjektů na věc.

Protože povinných subjektů je velké množství a jejich povinnosti se dělí podle toho, pod které písmeno § 3 ZKB spadají, bylo vhodné, vzhledem k rozsahu diplomové práce a možnostem autora, zaměřit zkoumání na určitou a pokud možno homogenní skupinu organizací. Jako taková skupina byly vybrány krajské úřady, neboť jsou součástí veřejné správy a vykonávají podobnou agendu (stejná kompetence a působnost [1]).

Průzkum se týká těchto oblastí z hlediska:

- řízení kybernetické bezpečnosti,
- organizace kybernetické bezpečnosi,
- zátěže (administrativní, finanční) vyplývající ze ZKB na organizaci,
- ochoty využití možnosti financování z integrovaného regionálního operačního programu (IROP) na podporu opatření ZKB,
- možnosti outsourcingu kybernetické bezpečnosti a také
- subjektivních názorů dotazovaných pracovníků na ZKB jako takový.

Postup průzkumu probíhal na základě následujících bodů:

- vytyčení cíle na základě studia dopadů ZKB do organizace,
- navržení obsahu a rozsahu dotazníku,
- vytvoření konkrétních otázek dotazníku,
- volba konkrétní formy a podoby dotazníku,
- kontakt a rozesílání dotazníků (analýza organizační struktury KrÚ, telefonické kontaktování krajských úřadů s cílem zajistit vhodné respondenty a rozesílání dotazníků emailem),

- zpracování dat (strukturovaný záznam, viz přílohu D),
- vyhodnocení dat a tvorba závěrů.

Průzkum byl veden spíše do šířky, než do hloubky a byl proveden formou dotazníkového šetření a následné doplňkové emailové nebo telefonické komunikace. Bylo plánováno na každý krajský úřad (včetně Magistrátu hlavního města Prahy tzn. 14 úřadů) zaslat jeden dotazník. Protože se krajské úřady od sebe liší organizační strukturou, bylo před zasláním dotazníku potřeba zjistit, kdo má problematiku kybernetické bezpečnosti v organizaci na starost. V některých případech se dají dílčí informace nalézt na webových stránkách úřadů, ve většině případů však bylo potřeba se s daným KrÚ telefonicky spojit a zjistit, kdo je za kybernetickou bezpečnost zodpovědný. Dotazník byl ve všech případech směřován konkrétním osobám, které se kybernetickou bezpečností v rámci úřadu zabývají, a s většinou z nich bylo vyplnění dotazníku předem telefonicky vyjednáno. Vzhledem k výrazným odlišnostem v organizaci bezpečnosti mezi jednotlivými KrÚ (ve kterém organizačním útvaru se nachází pracovník odpovědný za kybernetickou bezpečnost a zdali vůbec takový je, kolik pracovníků se problematikou zabývá atd.) nebylo možné zajistit ideální situaci, kdy dotazník na všech úřadech vyplní pracovníci jedné konkrétní pracovní pozice (např. vedoucí odboru informatiky). Dotazník tak v některých případech vyplňoval bezpečnostní ředitel (přímo podřízený řediteli úřadu), v jiných případech vedoucí oddělení či odboru informatiky a v některých případech také pracovník útvaru krizového řízení (detailněji níže ve vyhodnocení výsledků průzkumu). Jednalo se o pracovníky buď přímo odpovědné za kybernetickou bezpečnost nebo takové, kteří kybernetickou bezpečnost aspoň nějakým způsobem řeší (přičemž preferováni byli ti, kteří se jí zabývají na koncepční úrovni). To samo o sobě již napovídá, že k bezpečnosti v oblasti ICT není v těchto organizacích přistupováno jednotně, přestože mají stejné kompetence a vykonávají stejnou agendu.

Zásadní z hlediska průzkumu bylo zajistit pokud možno co největší návratnost dotazníků. Z tohoto důvodu musel být dotazník vytvořen tak, aby na jednu stranu nebyl příliš pracný na vyplnění a neodradil tak pracovníky od vyplnění[90], na druhou stranu aby i přesto zjistil podstatné informace. Některé informace ohledně bezpečnosti mohou být (a jsou) pracovníky oprávněně považovány za citlivé, z tohoto důvodu byl dotazník koncipován tak, aby se takovým otázkám vyhnul a pohybuje se spíše v obecné rovině. Pro zajištění větší důvěry a návratnosti dotazníku jsem také zdůraznil dotazovaným možnost anonymního zpracování. Některé krajské úřady tuto možnost využily a výslovně uvedly, že si přejí být zpracovány anonymně (byla požadována anonymizace

[90] Průzkum prováděný samostatně v rámci diplomové práce přirozeně nemá u dotazovaných takovou váhu, jako průzkum prováděný např. v rámci grantového programu nebo institucí veřejné správy jako NBÚ apod. S tím bylo nutno při vytváření dotazníku také počítat a vhodně volit především rozsah a pracnost.

jména pracovníka i kraje). Vzhledem k tomu, že požadavek anonymizace uvedlo velmi malé množství respondentů, budou anonymizovány odpovědi všech, aby nebylo možné odvodit z uvedených neanonymních, který krajský úřad odpovídal.

Z výše zmíněného plyne, že se nejednalo o dotazníkové šetření v tradičním slova smyslu tj. výběr reprezentativního vzorku, ze kterého by se výsledky zobecňovaly na celou zkoumanou populaci a následné užití matematických a statistických metod pro jeho vyhodnocení. Dotazníkem totiž bylo možné oslovit celou zkoumanou množinu. Vzhledem k počtu krajských úřadů v České republice se jednalo o sběr informací v malém okruhu respondentů. Dotazníky byly následně v některých případech doplněny emailovou a telefonickou komunikací.

Jako nástroj pro vytvoření dotazníku byl použit MS Word a dotazníky byly zasílány e-mailem jako jeden soubor MS Word (formátu *.docx) v příloze e-mailu[91]. Nevyužil jsem žádnou z dostupných (byť populárních a kvalitních) webových služeb na vytváření dotazníků – autor předpokládal, že pracovníci krajských úřadů budou mít větší důvěru v soubor MS Office a bude tak zajištěna větší návratnost.

Celý dotazník tak, jak byl rozesílán na krajské úřady, se nachází v příloze B Dotazník. Soubor, který byl zasílaný respondentům jako e-mailová příloha se nachází v netištěné elektronické příloze (viz Příloha A: Popis elektronické přílohy).

Krajské úřady byly jako předmět průzkumu zvoleny vzhledem k několika důvodům:

- jedná se o podobné organizace, které mají stejné kompetence a působnost, řeší tedy podobnou agendu, na základě toho také využívají podobné informační systémy a lze je tak mezi sebou porovnávat,
- lze předpokládat větší míru ochoty poskytnout informace, než u správců kritické informační infrastruktury (je pravděpodobné, že správci kritické informační infrastruktury by byli vzhledem k citlivosti této agendy méně kooperativní),
- jedná se o nejnižší hierarchickou úroveň veřejné správy, kde bylo možno předpokládat plošný dopad ZKB – autor předpokládal, že pracovníci veřejné správy na této úrovni budou kooperativnější, než pracovníci orgánů vyšší úrovně v hierarchii (např. ministerstev či jiných ústředních samosprávných úřadů).

[91] Dostupné viz Příloha A: Popis elektronické přílohy.

5.1.1 Shrnutí předmětu a metody průzkumu

V této části jsou shrnuty nejpodstatnější údaje o průzkumu:

cíl průzkumu:	zkoumání a ověření dopadů ZKB na povinné osoby (analyzované v kap. 4) na skupině krajských úřadů a zjištění základních faktů ohledně stavu kybernetické bezpečnosti v těchto organizacích
forma:	sběr informací pomocí dotazníků rozesílaných e-mailem a doplňkově emailová a telefonická komunikace
respondenti:	pracovníci krajských úřadů odpovědní za kybernetickou bezpečnost (u různých úřadů různá úroveň v organizační struktuře), za každý úřad jeden dotazník vyplňován jedním pracovníkem nebo kolektivem pracovníků, ponecháno na rozhodnutí dotazovaných
časové období:	dotazníky postupně rozesílány emailem 7. až 13. dubna po předchozích telefonických konzultacích
maximální počet zkoumaných subjektů	14
návratnost	10 ze 13 zaslaných dotazníků (z celkových 14 jeden odmítnul dotazník vyplnit již při telefonickém předjednávání[92])

[92] Nutno však podotknout, že se nejednalo o neochotu pracovníka. Dotazník týkající se dopadů ZKB na KrÚ byl odmítnut z důvodu ještě nedostatečného zhodnocení situace z hlediska KrÚ a bylo mi doporučeno úřad kontaktovat v průběhu léta, kdy již bude situace jasnější. Pracovník považoval za neseriózní vůči autorovi poskytovat informace v daném stádiu vývoje situace. U jiného KrÚ se autor setkal s tím, že dotazovaný pracovník byl v krátké době před průzkumem žádán o vyplnění dotazníku k několika jiným kvalifikačním pracím a ochota vyplňovat další tak již pochopitelně nebyla velká.

5.2 Sběr dat – dotazník

5.2.1 Struktura dotazníku – zkoumané oblasti

Dotazník obsahuje 21 otázek, které lze rozdělit do výše zmíněných oblastí průzkumu:

- řízení kybernetické bezpečnosti a její organizace (11 otázek), pro přehlednost rozděleno do bloků:
  - Blok I – zjištění VIS a KII (2 otázky),
  - Blok II – pohled do minulosti (2 otázky),
  - Blok III – organizování kybernetické bezpečnosti (5 otázek),
  - Blok IV – outsourcing (2 otázky),
- zátěž vyplývající ze ZKB na organizaci (5 otázek),
- financování z IROP (2 otázky),
- subjektivní názory pracovníků na ZKB (2 otázky).

Z uvedeného plyne, že důraz byl kladen především na řízení kybernetické bezpečnosti a také dopady ZKB na organizaci z hlediska zátěže (finanční, administrativní). V samotném dotazníku nejsou otázky striktně seskupené a řazené tímto způsobem. Některé otázky mohou také vyhovovat zároveň více uvedeným zkoumaným oblastem[93]. Pro získání co největšího množství informací a souvislostí bylo ke každé otázce (vyjma třech otevřených odpovědí) umožněno respondentům přidat komentář. Někteří dotazovaní této možnosti využívali a poskytli tak cenné informace. Někteří respondenti byli ještě následně kontaktováni pro upřesnění.

Dvě první otázky dotazníku zjišťují, zda je organizace správcem VIS a/nebo systému KII. Tyto dvě jsou pro přehlednost také uvedeny v kategorii řízení kybernetické bezpečnosti a její organizace.

Jsou použity 3 typy otázek:

- uzavřená *ano, ne*,
- uzavřená *určitě ano, spíše ano, spíše ne, určitě ne,*
- otevřená otázka s možností libovolné odpovědi.

[93] Např. otázka na změnu organizační struktury organizace na základě ZKB lze zařadit nejen do části řízení kybernetické bezpečnosti a její organizace, ale také do části zkoumající zátěž způsobenou ZKB na organizace. Např. otázky na financování z IROP by také mohly být podřazeny této části, neboť tato podpora se týká finanční i administrativní zátěže (více dostupných finančních prostředků, větší administrativní zátěž).

Možnosti odpovědí k jednotlivým otázkám ukazuje tabulka č. 1 v příloze C (str. 105).

Některé otázky jsou koncipované tak, že odráží do nějaké míry subjektivní názor respondentů. Jsou to otázky č.: 3, 4, 6, 8, 9, 20, 21. U těchto otázek (kromě té poslední, otevřené) bylo použito čtyř možností odpovědi a to: *určitě ano, spíše ano, spíše ne, určitě ne.*

Jak bylo zmíněno již výše, celý dotazník se nachází v příloze B Dotazník.

5.2.2 Výsledek sběru dat

Bylo osloveno 14[94] krajských úřadů a rozesláno 13 dotazníků (jeden odmítl již při telefonickém jednání), ze kterých se 10 vrátilo. Data, která byla dotazníkovým šetřením nasbírána, jsou v zájmu přehlednosti umístěna v tabulkách v příloze D.

K vyhodnocení jsou velmi podstatné komentáře, které pracovníci k odpovědím přidávali. V některých případech využili komentáře i místo odpovědi (např. tam, kde byla problematika teprve v jednání nebo kde nestačily autorem navržené uzavřené odpovědi). Komentáře jsou uvedeny níže za tabulkou a originální data jsou uložena v elektronické příloze (viz Příloha A: Popis elektronické přílohy).

5.2.3 Kraje zapojené do průzkumu

Níže uvádím seznam krajů a pracovníků, kteří byli ochotni se průzkumu zúčastnit. Výsledky průzkumu jsou v zájmu respondentů (někteří o to požádali) anonymizované, v práci ani přiložených materiálech tedy nedojde ke spárování výsledků s konkrétními kraji či jmény[95]. Průzkumu se zúčastnily tyto krajské úřady a tito jejich pracovníci:

- Jihočeský kraj: Ing. Jaroslava Císlerová,
- Karlovarský kraj: Ing. Petr Kulda,
- Kraj Vysočina: Ing. Dominik Marek,
- Královéhradecký kraj: Ing. Martin Kořínek, Ph.D.,
- Magistrát hl. m. Prahy: Bc. Miloslav Svoboda,
- Moravskoslezský kraj: Ing. Pavel Žák,
- Olomoucký kraj: Mgr. Jiří šafránek,

[94] Krajských úřadů je v ČR i s Magistrátem hlavního města Prahy čtrnáct.

[95] Uvedené pořadí (dle abecedy) je jiné, než používané dále jako K1, K2 až K10.

- Pardubický kraj: Ing. Martin Halámka,
- Ústecký kraj: Bc. Jan Jelínek,
- Zlínský kraj: Ing. Jiří Fux.

Výše uvedeným autor velmi děkuje za ochotu poskytnout informace do průzkumu. Bez nich by nemohl být realizován. Kontakty na tyto osoby jsou veřejně dostupné v telefonních seznamech na webových portálech krajských úřadů.

5.3 Průzkum a jeho vyhodnocení

V této kapitole jsou představeny otázky dotazníku, jejich význam, souvislosti s dopady zjištěnými rozborem ZKB v předchozí kapitole a především jsou uvedeny a zhodnoceny odpovědi respondentů včetně komentářů, které autor k dané otázce považoval za podstatné. Kapitola je v zájmu větší přehlednosti členěna do podkapitol podle výše popsaných částí průzkumu. „Surová“ data jsou uvedena v příloze E této práce. Jednotlivé kraje jsou označovány K1, K2 až K10.

Ke každé skupině otázek je uveden důvod, proč otázka byla do dotazníku zahrnuta a jaký měla účel.

5.3.1 Řízení kybernetické bezpečnosti a její organizace – dělení

Tato stěžejní část průzkumu se zaměřuje na řízení a organizaci kybernetické bezpečnosti na KrÚ. Nejprve jsou uvedeny dvě otázky, které ověřují předpoklad, že jsou KrÚ převážně správci významných informačních systémů a také zda spravují systémy kritické informační infrastruktury (Blok I). Následuje další dvojice otázek zkoumající úroveň bezpečnosti na KrÚ před ZKB – zda KrÚ řešily informační bezpečnost na základě nějakého oborového standardu či normy a zda považují požadavky ZKB na bezpečnost přísnější, než jimi již dříve zaváděné na základě povinnosti zajišťovat bezpečnost dle 365/2000 Sb., o informačních systémech veřejné správy (Blok II). Další blok otázek řeší organizování kybernetické bezpečnosti z hlediska existence samostatného organizačního útvaru zodpovědného za kybernetickou bezpečnost, jeho případné začlenění do organizační struktury, počtu pracovníků řešících kybernetickou bezpečnost a také vyčlenění pracovníka zodpovědného za kybernetickou bezpečnost od útvaru zajišťujícího provoz ICT, plánované změny na základě ZKB a plánované zavedení bezpečnostních rolí dle ZKB (Blok III). Pro přehlednost je tato část rozdělena do těchto bloků:

- Blok I – zjištění VIS a systémů KII (otázky 1, 2),
- Blok II – kybernetická bezpečnost před ZKB (otázky 10, 11),
- Blok III – organizování kybernetické bezpečnosti (13–16, 18),
- Blok IV – outsourcing (otázky 19, 20).

5.3.2 Blok I – zjištění VIS a systémů KII

Otázky tohoto bloku ověřují předpoklad formulovaný v kap. 4, že krajské úřady budou vesměs správci VIS a že jen výjimečně budou správci KII. Otázky v tomto bloku sloužily také z hlediska návratnosti dotazníku jako jednoduše zodpověditelné otázky, které respondenty neodradí od dalšího pokračování.

Výsledky

Otázka 1: „*Je nebo v nejbližší době bude Vaše organizace správcem významného informačního systému podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti?*“

- ano: 10x
- ne: 0x

Všechny dotazované KrÚ uvedly, že jsou nebo v nejbližší době budou správci významných informačních systémů dle § 3 písm. e) ZKB.

Otázka 2: „*Je nebo v nejbližší době bude Vaše organizace správcem systému kritické informační infrastruktury podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti?*“

- ano: 0x
- ne: 9x

Jeden z krajů, který má mezi kraji specifické postavení uvedl, že pravděpodobně ano, ale dosud to není jednoznačné. Jeden KrÚ uvedl, že nepředpokládá správu systému KII ani do budoucna. Zbylé KrÚ otázku nekomentovaly.

Zhodnocení

Z odpovědí jednoznačně vyplývá, že všechny dotazované KrÚ jsou správci alespoň jednoho významného informačního systému a žádný z nich až na jednu výjimku není správcem systému spadajícího do kritické informační infrastruktury. Tímto byl potvrzen předpoklad formulovaný v úvodu kap. 4 a v kap. 4.9.3 – Shrnutí otázek vhodných pro průzkum, které vyplynuly z rozboru ZKB.

5.3.3 Blok II – kybernetická bezpečnost před ZKB

Předmětem zkoumání tohoto bloku je zjištění stavu kybernetické bezpečnosti krajských úřadů před zavedením ZKB a to především z hlediska alespoň hrubého porovnání úrovně prováděných bezpečnostních opatření na základě zákona č. 365/2000 Sb., o informačních systémech veřejné správy a požadavků vyplývajících ze ZKB. Tento blok vyplývá především z kap. 4.7.2 a ověřuje tvrzení z důvodové zprávy k ZKB, která říká, že většina regulovaných subjektů již řeší kybernetickou bezpečnost na úrovni standardů ISO/IEC 20000 nebo ISO/IEC 27001 a nebudou tedy požadavky ZKB výrazně zatíženy.

V tomto bloku se nachází otázky č. 7 a 10 dotazníku.

Výsledky

Otázka 7: „*Podle zákona 365/2000 Sb., o ISVS je zajišťování bezpečnosti informačních systémů provozovaných veřejnou správou povinné již několik let. Jsou požadavky ZKB a navazující vyhlášky na bezpečnostní opatření VIS přísnější, než Vámi již dříve zaváděná opatření?*“

- ano: 9x
- ne: 0x

Jeden kraj neuvedl žádnou odpověď.

Otázka 10: „*Zaváděla Vaše organizace řízení bezpečnosti informací podle nějakého oborového standardu či normy ještě před ZKB? (Pokud ano, prosím specifikujte v komentáři.)*“

- ano: 6x
- ne: 4x

Komentáře k této otázce autor považuje za velmi sdělné a jsou uvedeny všechny. Nejprve komentáře krajů, které uvedly odpověď „ano“:

- „*jako podklad byla použita norma ISO 27001*“,
- „*resp. byly snahy, ZoKB v tomto směru zafungoval jako spouštěč připravených opatření*“,
- „*ISO/IEC 27001*“,
- „*podle ISO 27000, bez certifikace*“,
- „*Snažili jsme se držet doporučení aktuálně platných norem, (.., 27k.), ale pouze tam, kde to pro nás mělo smysl. Nikdy jsme neusilovali o atestaci.*“,
- „*27001*“.

Komentáře krajů, které uvedly odpověď „ne“:

- „*částečně analýza rizik dle ISO 27000*“.

Od dalšího z respondentů, který uvedl „ne“ bylo později při dodatečné komunikaci zjištěno, že v současnosti usilují o zavedení certifikace ISO/IEC 27001 pro celý úřad.

Zhodnocení

Lze vidět, že přes odlišnosti v uspořádání KrÚ a různou míru postupu v řešení informační bezpečnosti byly KrÚ ve vztahu k informační bezpečnosti proaktivní minimálně ve snaze řídit zajišťování bezpečnosti pomocí oborových standardů (7 z 10[96]) nebo se jimi aspoň inspirovat. Všechny KrÚ, které zaváděly nebo se snažily zavést nějaký standard, uvedly ISO/IEC 27000 případně konkretizovali na 27001, ale vesměs jen jako podklad (4 respondenti uvedli, že nebyla snaha o certifikaci, ostatní nebyli tak sdílní). Dle slov jednoho z respondentů u jejich KrÚ zafungoval ZKB jako spouštěč připravených bezpečnostních opatření, to lze hodnotit jako velmi pozitivní dopad.

Přesto, že 6 z 10 respondentů se při řízení bezpečnosti minimálně inspirovalo standardy z rodiny ISO/IEC 27000, ani jeden – dle odpovědí na otázku č. 7 – neimplementoval bezpečnostní opatření alespoň na úrovni požadavků z VKB pro správce VIS. To jednoznačně implikuje nutnost dodatečných investic do bezpečnosti a z toho i vyplývající administrativní zátěž. Krajské úřady tedy nepatří mezi tu většinu povinných subjektů zmíněnou v důvodové zprávě k ZKB, pro kterou není adaptace na zákonné povinnosti otázkou prakticky žádných investic.

Na základě těchto výsledků autor dospívá také k názoru, že by bylo vhodné do dotazníku zařadit otázku zjišťující, zda krajské úřady zvolí ke splnění povinností ZKB cestu přes certifikaci na ISO/IEC 27001 (a její prokázání na základě § 29 VKB) nebo zda budou „jen“ dodržovat vyhlášku 316/2014 Sb. Lze se domnívat, že pro kraje bude méně náročné splnit požadavky vyhlášky (neboť spravují pouze VIS a z toho plynou menší požadavky na bezpečnostní opatření).

Rovněž lze vyvodit, že krajské úřady nebyly donuceny na základě zákona č. 365/2000 Sb. a jeho prováděcích předpisů implementovat systematicky řízení informační bezpečnosti na úrovni adekvátní provozování významných informačních systémů dle ZKB. Na vině může být přílišná volnost zákona o informačních systémech veřejné správy a jeho důraz zejména na dokumentaci bezpečnosti namísto implementace konkrétních opatření. Vzhledem k tomuto stavu lze předpokládat, že krajským úřadům pravděpodobně nebylo poskytnuto účinné metodické vedení při implementaci bezpečnosti

[96] Do sedmi je započítán i úřad, který odpověděl „ne“, ale prováděl analýzu rizik dle ISO/IEC 27000.

podle zákona 365/2000 Sb. ve srovnání s aktivitami NBÚ[97] u zákona o kybernetické bezpečnosti.

5.3.4 Blok III – organizování kybernetické bezpečnosti

Tato část průzkumu zkoumá organizační aspekty kybernetické bezpečnosti na KrÚ, zejména jaké je začlenění kybernetické bezpečnosti do organizační struktury regulovaných subjektů (zda existuje zvláštní organizační útvar a kde je začleněn, kolik pracovníků se kybernetické bezpečnosti věnuje, zda ZKB způsobí změny organizační struktury).

V tomto bloku se nachází otázky 13, 14, 15, 16 a 18 dotazníku.

Výsledky

Otázka 13: „*Je ve Vaší organizaci zvláštní organizační útvar věnující se bezpečnosti informací nebo kybernetické bezpečnosti (např. odbor či oddělení apod.)?*“

- ano: 4x
- ne: 6x

Jeden kraj uvedl komentář k odpovědi „ano“:

„*ano, bezpečnostní ředitel / manažer KB – jedna osoba; vedoucí informatiky – jedna osoba; plánujeme zřízení třetí pozice – bezpečnostní správce*“

Jeden kraj uvedl komentáře k odpovědi „ne“:

„*ani útvar, ani oddělení, tuto činnost zatím zabezpečuje jeden člověk*“

Otázka 14: „*Pokud je odpověď na předchozí otázku ano, kde v organizační struktuře je takový útvar začleněn? Kolik lidí se této oblasti věnuje?*“

Jedná se o otevřenou otázku. Vzhledem ke koncepci této otázky uvádím všechny odpovědi:

K1: „*Spadá pod pana ředitele, viz. předchozí odpověď*“,

K2: „*manažer KB je zařazen do odboru krizového řízení, zbytek rolí jen na odboru informatiky*“,

[97] Lze počítat např. pomocné materiály vytvořené NBÚ pro podporu zavádění ZKB – checklist pro audit/zavádění jednotlivých opatření dle vyhlášky, materiál vysvětlující bezpečnostní role a jejich začlenění v organizaci nebo vysvětlení pojmu nepřiměřené náklady.

K7: „*odbor bezpečnosti + odbor informatiky, cca 5-7 osob*“,

K9: „*kancelář ředitele*“,

K10: „*Dané oblasti se věnuje 1 pracovník (+ 1 externí poradce), je zařazen do běžného odboru, mimo odbor informatiky*“

Kraje 3, 5, 6 a 8 neuvedly žádnou odpověď.

Otázka 15: „*Je útvar či pracovník řídící kybernetickou bezpečnost oddělen od útvaru, který zajišťuje provoz ICT? Pokud je oddělen, ve kterém útvaru (odboru, oddělení apod.) je začleněn? /Prosím do komentáře/*“

- ano: 4x
- ne: 6x

Komentáře:

K2: „viz výše“ (tj. bezpečnostní ředitel/manažer KB v jedné osobě, vedoucí informatiky, plánuje se třízení pozice bezpečnostního správce)

K3: „*odbor informatiky*“

K7: „*v odboru bezpečnosti*“

K10: „*odbor analýz a podpory řízení*“

Otázka 16: „*Změnila či bude se měnit struktura organizace nebo počet lidí věnujících se bezpečnosti na základě implementace ZKB? (Vyčlenění zvláštního útvaru či pracovníků atd. Případné detaily prosím do komentáře.)*“

- ano: 3x
- ne: 5x

Dva zbývající kraje uvedly, že zatím ještě nemohou odpovědět, věc je v jednání.

Komentáře k odpovědi „ano“:

K2: „*v budoucnu se předpokládá oddělení role bezpečnostního ředitele (ISMS) od manažera kybernetické bezpečnosti v okamžiku, kdy agenda bude vyžadovat celý úvazek*“

K7: „*v roce 2014 vzniklo bezpečnostní oddělení na odboru informatiky (v souladu s bodem 15), toto oddělení bylo ale paradoxně v r. 2015 zrušeno bez náhrady*“

Komentáře k odpovědi „ne“:

K4: „*pouze změna pracovní náplně stávajících zaměstnanců*“

K8: „*Vedení se domnívá, že se to týká informatiky a že to zvládne jeden pracovník při vykonávání svých stávajících povinností.*“

K10: „*Zvyšování počtu zaměstnanců obecně ve státní správě není úplně populární, proto nelze předpokládat, že by se zvýšil počet zaměstnanců zabývající se bezpečností.*“

Otázka 18: „*(Pouze pro správce VIS): Vyhláška 316/2014 Sb. vyžaduje po správcích významného informačního systému zavést tzv. bezpečnostní role – architekt, manažer, auditor kybernetické bezpečnosti a garant aktiva – pouze přiměřeně. Které z těchto rolí jste stanovili či plánujete zavést?*“

Odpovědi tříděné podle bezpečnostních rolí:

- architekt: 5x (z 8 KrÚ, které role vyplnily)
- manažer: 8x (z 8 KrÚ, které role vyplnily)
- auditor: 4x (z 8 KrÚ, které role vyplnily)
- garant aktiva: 8x (z 8 KrÚ, které role vyplnily)
- výbor pro ř. k. b.: 6x (z 8 KrÚ, které role vyplnily)

Role vyplnilo 8 krajů, další 2 uvedly odpověď do komentáře – u obou je věc zatím předmětem jednání.

Jeden z krajů plánuje zavést kromě všech uvedených rolí ještě roli správce aktiva (ten kraj, který zavádí pro celý úřad ISO/IEC 27001).

K4 ještě dále informoval: „*Prozatím u nás není stanoven zaměstnanec, který by byl za kyberbezpečnost zodpovědný :(Nejspíše by se mělo jednat o bezpečnostního ředitele, který je vedoucím oddělení krizového řízení, v náplni práce to má i další zaměstnanec tohoto oddělení. Čistě technickou stránku má na starosti IT oddělení. Co se týče výboru pro řízení kyberbezpečnosti tak o tom prozatím neuvažujeme, stále je ve hře outsourcing.*“[98]

K8 také dále informoval: „*Dohodli jsme se, že Výbor kybernetické bezpečnosti mít budeme. Jeho činnost se bude odvíjet od složení. Jsem si vědom, že by mělo být odděleno řízení a management kybernetické bezpečnosti od provozu ICT, ale vedení rozhodlo jinak. ZKB nám určitě pomůže v oblasti bezpečnosti, podaří se získat nějaké finance, realizovat nějaká opatření, ale na druhou stranu nám přibude hodně práce a odpovědnosti.*“[99]

Zhodnocení

Z odpovědí respondentů uvedených v tomto Bloku III zřetelně vyplývá zejména jedno podstatné zjištění: organizování kybernetické bezpečnosti (zejména její začlenění v organizační struktuře a počet pracovníků věnujících se kybernetické bezpečnosti) napříč

[98] e-mailová zpráva autorovi ze dne 12. dubna 2016

[99] e-mailová zpráva autorovi ze dne 14. dubna 2016

krajskými úřady je značně nejednotné. Je patrné, že ani pod vlivem ZKB nejspíše nedojde ke sjednocení kybernetické bezpečnosti na KrÚ z tohoto organizačního hlediska. Stále tedy velmi záleží (a někteří respondenti dosti zřetelně vyjádřili svou nelibost či podivení např. odpověď K8 na otázku 16 a jeho vyjádření k otázce 18) na bezpečnostním povědomí vrcholového vedení organizace, jakým způsobem bude bezpečnost v organizaci řízena. Otázkou je, zda by nebylo vhodné i tuto stránku kybernetické bezpečnosti na krajských úřadech (potažmo ostatních orgánech veřejné moci, kde lze předpokládat podobnou situaci) sjednotit. Zákon o kybernetické bezpečnosti nicméně dle vyjádření některých respondentů pomáhá prosazovat kybernetickou bezpečnost u vedení v jejich organizacích a každý krok ku předu v této oblasti je nutno hodnotit pozitivně.

5.3.5 Blok IV – outsourcing

Tento blok se zabývá otázkou outsourcingu kybernetické bezpečnosti na KrÚ. Z kap. 4 vyplývá předpoklad, že outsourcingem lze řešit především případnou nedostatečnou personální kapacitu.

Tento blok obsahuje otázky 19 a 20 dotazníku.

Výsledky

Otázka 19: „*Realizujete kybernetickou bezpečnost vlastními silami nebo (byť zčásti) externě?*“

- jen vlastními silami: 1x
- částečný/úplný outsourcing: 3x (bez rozlišení na částečný/úplný)
- *částečný* outsourcing: 6x

Některé kraje v dotazníku rozlišily u této otázky, že plánují částečný outsourcing a některé ne.

Komentáře:

Jeden z krajů uvedl „*činnosti související s provozem vlastními silami, audit externě (např. penetrační testy apod.)*“ k odpovědi částečný/úplný outsourcing, lze jej tedy řadit mezi ty, které provádějí částečný outsourcing (celkem tedy 7 krajů).

Tyto komentáře uvedly kraje plánující částečný outsourcing:

„*částečně nám pomáhá (formou poradenství) externí pracovník*“

„*v jednání, příprava veřejné zakázky*“

Otázka 20: „*Je realizace bezpečnosti pomocí outsourcingu schůdná (vzhledem k procesní nutnosti zajišťování prostředků a vyhlašování výběrových řízení, řízení odpovědností atd.)?*“

- určitě ano: 1x
- spíše ano: 7x
- spíše ne: 1x
- určitě ne: 0x

Jeden z krajů nevybral žádnou odpověď, ale komentoval slovy: „*ano, může to být jedna z variant (na základě ekonomické analýzy)*“. Vzhledem k tomu, že se jedná o jednu ze zvažovaných z variant, lze jej počítat do odpovědi „spíše ano“.

Zhodnocení

Na základě výše uvedených výsledků lze tvrdit, že krajské úřady jsou u řešení kybernetické bezpečnosti otevřené spolupráci s externími dodavateli. Žádný z KrÚ neuvedl, že outsourcing určitě není schůdný a pouze jediný kraj odpověděl „spíše ne“ na tutéž otázku. Dá se říci, že 8 z 10 respondentů jsou přesvědčeni o tom, že outsourcing je spíše schůdný a jeden uvádí „určitě ano“. To dokládají také odpovědi na otázku 19, u které 9 z 10 krajů uvedlo, že realizují kybernetickou bezpečnost částečně nebo úplně externě. Z toho 7 krajů těží z částečného outsourcingu a 2 toto nerozlišily, zda se jedná o částečný nebo úplný outsourcing. Vzhledem k charakteru organizací a k uvedeným komentářům se lze však s velkou pravděpodobností domnívat, že outsourcing se týká především poradenství nebo auditingu řešení kybernetické bezpečnosti krajských úřadů. Současně se dá usuzovat, že KrÚ zatím povětšinou nemají dostatečné kapacity k tomu, aby mohly kybernetickou bezpečnost řešit samostatně.

5.3.6 Zátěž vyplývající ze ZKB na organizaci

Tato část průzkumu se věnuje zkoumání negativních dopadů ZKB na povinné subjekty v podobě zátěže na organizaci. Nejprve zjišťuje, zda je přechodná doba pro zavedení bezpečnostních opatření dle názoru pracovníků povinných subjektů dostatečně dlouhá (otázka nastolená v kap. 4.6.4 a 4.7.2), dále ověřuje, zda pro povinné subjekty ZKB znamená významné dopady v podobě administrativní či finanční zátěže a také zkoumá, zda jsou jako významný dopad vnímány i povinnosti nad rámec bezpečnostních opatření (kap. 4.6.2). Tato část také obsahuje otázku č. 21, ve které měli respondenti možnost vyjádřit nejzásadnější dopady ZKB na jejich organizaci.

Do této části spadají otázky 6, 8, 9, (17), 21 dotazníku.

Výsledky

Otázka 6: *„V případě určení systému jako VIS nebo KII je povinnost do jednoho roku od této skutečnosti zajistit soulad se ZKB. Je či byla podle Vašeho názoru tato doba dostatečně dlouhá?“*

- určitě ano: 0x
- spíše ano: 4x
- spíše ne: 6x
- určitě ne: 0x

Komentáře k odpovědi „spíše ne“:

„Spíše ne z hlediska technických opatření, které vyplývají ze zákona.“

„především s ohledem na rozpočtové období (trvá déle než rok výdaj naplánovat, vysoutěžit řešení a to pak implementovat)“

„vzhledem ke zdlouhavým procesům, které souvisí s veřejnými zakázkami a dále potřebou zachovat posloupnost realizace jednotlivých kroků, je 1 rok spíše málo (a to nezmiňuji problematiku plánování finančních prostředků a personálních kapacit)“

Komentáře k odpovědi „spíše ano“:

„To vyplývá z toho, že již část požadavků splňujeme.“

„Spíše ano, protože subjekty mohou zavést bezpečnostní opatření pouze pro určené VIS (resp. KII). My máme času málo, protože jsme se rozhodli certifikovat dle 27001 celý úřad, ale v obecné rovině je na to v podstatě dost času.“

Jeden z krajů, který odmítl vyplnit dotazník, telefonicky uvedl, že tato lhůta jim připadá dostatečně dlouhá na zavedení požadovaných opatření.

Otázka 8: *„Jsou požadavky ZKB významné z hlediska administrativní či finanční zátěže?“*

- určitě ano: 8x
- spíše ano: 2x
- spíše ne: 0x
- určitě ne: 0x

Komentář kraje, který odpověděl „určitě ano“: *„Technická bezpečnost je jen součástí ZKB, důraz je kladen na „procesy, administrativu, papíry“*.

Jeden z krajů odkazuje na svůj komentář v předchozí otázce, kde zmiňuje zdlouhavé procesy s veřejnými zakázkami a celkovou procesní náročnost.

Otázka 9: „*Jsou požadavky ZKB nad rámec bezpečnostních opatření (tj. hlášení bezpečnostních událostí/incidentů, kontakt s vládním CERT, …) významné z hlediska administrativní či finanční zátěže?*“

- určitě ano: 3x
- spíše ano: 5x
- spíše ne: 1x
- určitě ne: 0x

Jeden z krajů neodpověděl s odůvodněním, že jako správce VIS je v přechodném období: „*Zde zatím nemohu odpovědět, jako správce VIS, jsem v přechodném období (12 měsíců)*“

Otázka 17 měla zjistit náročnost zavedení povinných bezpečnostních rolí pro správce systémů KII. Žádný z respondentů systém KII nespravuje, ***tato otázka se v případě krajských úřadů ukázala jako nerelevantní***.

Otázka 21: „*Jaké jsou podle Vás ve shrnutí nejzásadnější dopady zákona o kybernetické bezpečnosti na Vaši organizaci?“*

Tato otázka byla záměrně koncipována jako otevřená, aby respondenti nebyli ovlivňováni a omezováni výčtem možností a mohli tak napsat takové dopady, které sami uznají za nejzásadnější. Vzhledem ke koncepci a důležitosti této otázky z hlediska průzkumu uvádím všechny odpovědi:

K1: „*Z hlediska uživatelů zvýšení povědomí o rizicích a dopadech bezpečnosti informací v organizaci. Z hlediska správců a administrátorů ve spojení s normou ISO 27001 nastavení a dodržování jednotných postupů a pravidel.“*

K2: „*větší důraz na bezpečnost – ZoKB pomáhá prosazovat problematiku bezpečnosti; zvýšené výdaje; organizační změny*“

K3: „*organizační a finanční*“

K4: „*Nutné administrativní kroky, značné papírování, téměř žádná novinka ve stávající ICT HW bezpečnosti.*“

K5: „*Zvýšená administrativa, problém s personálním zajištěním, neschopnost financovat bezpečnostní role, vyšší bezpečnost.“*

K6: /

K7: „*zákonná možnost nastolení pořádku v oblasti kybernetické bezpečnosti*“

K8: „*Větší administrativa, více práce, větší náklady, sjednocení úrovně bezpečnosti s ostatními*“

K9: „*finanční*“

K10: „*řešení bezpečnosti informací systémovým způsobem*“

Shrnuto:

- organizační/administrativní: 5x
- finanční: 5x
- pozitivní vliv na bezpečnost: 6x

Zhodnocení

Co se týče délky přechodné lhůty k zavedení bezpečnostních opatření z vyhlášky 316/2014 Sb., odpovědi nejsou vyhraněné (ani jeden KrÚ však neuvedl „určitě ano“ nebo „určitě ne“). Více KrÚ (6 ku 4) se však domnívá, že tato lhůta spíše není dostatečně dlouhá. Mírně tedy převažují odpovědi „spíše ne“. Dá se předpokládat, že tuto otázku budou dotčené subjekty schopny jednoznačně zodpovědět po té, co tato lhůta uplyne. Někteří respondenti uvedli relevantní důvody, které mohou vést k průtahům v projektech implementace bezpečnostních opatření (zejména zdlouhavé procesy související s veřejnými zakázkami, nutnost zachování posloupnosti určitých kroků, rozpočtové plánování) a na základě kterých – zvláště tam, kde vedení organizace nedává kybernetické bezpečnosti dostatečný důraz – se bude času spíše nedostávat.

Naopak velmi jednoznačné odpovědi se objevují u osmé otázky, kde 8 z 10 respondentů je přesvědčeno, že ZKB znamená významnou administrativní nebo finanční zátěž pro organizaci a zbylí 2 uvádí, že spíše ano. To potvrzuje zjištěná fakta z otázek Blou II – kybernetická bezpečnost před ZKB – a také to potvrzuje, že stav informační bezpečnosti na KrÚ nebyl před ZKB na úrovni požadavků adekvátních pro správce VIS.

V rozporu s předpokladem vyplývajícím z kap. 4.6.2 – tedy, že opatření nad rámec bezpečnostních opatření nebudou příliš významná z hlediska zátěže na organizace, se respondenti poměrně jednoznačně shodli na tom, že tato opatření spíše nebo určitě významná z hlediska zátěže na organizaci jsou.

Volná vyjádření krajských úřadů k nejzásadnějším dopadům ZKB na jejich organizaci vyznívají jednak mírně pozitivně ve smyslu vlivu ZKB na zlepšení kybernetické bezpečnosti, jednak i negativně ve smyslu administrativní a finanční zátěže a také zmíněné pochybnosti, zda ZKB bude skutečně účinným nástrojem k reálnému (ne jen administrativnímu a „papírovému“) zlepšení kybernetické bezpečnosti.

5.3.7 Financování z IROP

Tato část průzkumu měla za cíl zjistit, zda jsou krajské úřady ochotné využít prostředky z výzvy 10 integrovaného regionálního operačního programu (viz kap. 4.7.1). Výzva umožňuje čerpat povinným subjektům desítky milionů na technická bezpečnostní opatření dle ZKB. Cílem bylo zjistit počty těch, kteří výzvu využijí nebo nevyužijí a také zjistit případné důvody pro to, že tyto prostředky nebudou čerpat. Autor předpokládal odpovědi typu přílišné administrativní složitosti nebo rizika následných auditů.

Do této části spadají otázky dotazníku 11 a 12.

Výsledky

Otázka 11: „*Od 21.10.2015 je vypsána Výzva č. 10 IROP – Kybernetická bezpečnost určená na technická bezpečnostní opatření VIS a KII podle ZKB. Organizaci umožňuje čerpat částky v desítkách milionů Kč. Plánujete čerpání peněz z tohoto programu?*“

- ano: 4x
- ne: 5x

Jeden respondent nevybral ani jednu z odpovědí a do komentáře odpověděl „spíše ne“.

Otázka 12: „*Pokud je odpověď na předchozí ne, proč? (Přílišná administrativní složitost? Riziko vyplývající z následných auditů? Jiný důvod?)*“

Otevřená otázka. Odpovědi:

K2: „*obecně malá ochota čerpat z dotačních titulů – rizika nekonzistentních auditů*“

K3: „*Některá technická opatření již byla realizována mimo jiné i v rámci projektu IOP.*“

K7: „*bez odpovědi*“

K8: „*Využili jsme již dříve jiné Výzvy.*“

K10: „*přílišná administrativní složitost (tvorba projektu), úzké zaměření výzvy pouze na VIS (KII)*“

Všechny odpovědi také v příloze D, Tabulka P2: Odpovědi na otázky č. 12 a 14.

Zhodnocení

Bylo zjištěno, že jen 4 z 10 dotazovaných KrÚ plánují využít prostředky výzvy č. 10 IROP k rozvoji technických bezpečnostních opatření.

Dále bylo zjištěno, že 5 KrÚ výzvu neplánuje využít a jeden spíše neplánuje. Čtyři respondenti uvedli své důvody: Jeden z krajů uvedl obecně malou ochotu čerpat z dotačních titulů kvůli rizikům nekonzistentních auditů, další uvádí přílišnou administrativní

složitost při tvorbě projektu a také úzké zaměření výzvy pouze na VIS[100] (a KII). Dva kraje uvedly, že neplánují výzvu 10 IROP využít, protože již prostředky čerpaly (z jiné výzvy IOP).

Celkově tedy 6 krajů bude čerpat či již čerpalo prostředky z operačního programu EU a 4 z nich to neplánují z výše uvedených důvodů. Důvody, které kraje uvedly pro nečerpání peněz z fondů se shodují s autorovým předpokladem (přílišná administrativní složitost, riziko plynoucí z následných auditů), nicméně ostatní kraje tyto skutečnosti od čerpání neodradily. U 6 z dotazovaných krajů lze hovořit o pozitivním dopadu IROP z hlediska finanční zátěže.

5.3.8 Názory pracovníků na ZKB

Tato část průzkumu má za cíl zjistit názory pracovníků KrÚ na ZKB jako takový. Smyslem bylo zjistit, zda považují pracovníci krajských úřadů, na které ZKB dopadá, tuto legislativu za rozumný krok k dosažení větší úrovně bezpečnosti důležitých informačních nebo komunikačních systémů a také zda hodnotí požadavky ZKB a navazující vyhlášky za jasné a srozumitelné. V této části je také zjišťováno, zda se KrÚ podílely na připomínkování ZKB.

Této části se týkají otázky 3, 4 a 5 dotazníku.

Výsledky

Otázka 3: „*Považujete ZKB za rozumný krok k dosažení větší úrovně bezpečnosti důležitých informačních nebo komunikačních systémů?*“

- určitě ano: 4x
- spíše ano: 6x
- spíše ne: 0x
- určitě ne: 0x

Jeden z respondentů uvedl k této otázce komentář: „*Kdo si je možných rizik vědom, připravoval se a připravuje i bez zákona. Kdo si vědom rizik není, nepomůže ani zákon.*“

Otázka 4: „*Jsou požadavky ZKB a navazující vyhlášky jasné a srozumitelné? Víte přesně, jaké konkrétní povinnosti máte?*“

- určitě ano: 3x
- spíše ano: 5x
- spíše ne: 1x

[100] Tento kraj plánuje certifikovat dle ISO/IEC 27001 celý úřad.

- určitě ne: 0x

Jeden kraj zmínil, že ještě nemůže odpovědět, protože se nachází teprve v přechodné lhůtě[101].

Otázka 5: *„Využila Vaše organizace možnost podílet se na připomínkách k ZKB? (Úspěšně? – případné detaily prosím do komentáře.)*"

- ano: 3x
- ne: 5x

Dva respondenti neví (jeden z nich uvádí, že připomínkování mohlo proběhnout legislativním odborem a jeden nastoupil na své místo až v době probíhající implementace bezpečnostních opatření).

Jeden z těch, kteří uvedli že ne, komentuje slovy *„zákon i vyhláška jsou srozumitelné, problematika byla široce diskutována*".

Další komentují: *„V průběhu tvorby zákona byly svolány dvě schůzky na NBÚ, později se již neuskutečnily. Jednání na úrovni Asociace krajů v době platnosti ZKB nebyly již plodné.*"

„Nyní, již takou možnost máme a využijeme ji při přípravě a úpravě ZoKB z hlediska NISu."

„Legislativu jsme sledovali, ale připomínky jsme nepodávali."

Zhodnocení

Dle uvedených odpovědí lze jednoznačně říci, že ZKB je pracovníky krajských úřadů vnímán pozitivně, alespoň ve vztahu k bezpečnosti informačních a komunikačních systémů. Všichni dotazovaní uvedli „určitě ano" nebo „spíše ano", ani jeden neuvedl negativní odpověď. Co se týče srozumitelnosti a jednoznačnosti požadavků, zde také většina respondentů až na jednoho ZKB hodnotí spíše pozitivně.

Co se týče využití možnosti se podílet na připomínkách k ZKB, zde již nejsou odpovědi tak jednoznačné. Lze ale pozorovat, že krajské úřady legislativu kybernetické bezpečnosti spíše sledovaly nebo sledují – 3 se přímo účastnily připomínek a 2 z těch, které nevyužily možnosti připomínkovat o této možnosti věděly a problematiku diskutovaly a jeden z KrÚ se bude účastnit připomínkování do budoucna v rámci úpravy ZKB na základě evropské směrnice NIS.

[101] Přechodná lhůta viz kap. 4.6.4 Lhůty k plnění povinností.

5.4 Celkové shrnutí a zhodnocení průzkumu

Vzhledem k počtu vrácených dotazníků lze zvolenou metodu průzkumu z hlediska návratnosti hodnotit kladně. Pracovníci krajských úřadů byli vesměs kooperativní a umožnili jej provést. Respondenti využili v hojné míře i možnost otázky komentovat a proaktivně tak poskytli svůj náhled na věc nebo detaily ohledně dané otázky, čímž byly získány pro tuto práci velmi cenné informace.

V průzkumu byly zodpovězeny všechny otázky formulované v kap. 4.9.3 na základě rozboru ZKB:

- Byl potvrzen předpoklad, že KrÚ jsou vesměs správci VIS a žádný z dotázaných zatím není správcem KII (u jednoho se o tom uvažuje) – viz 5.3.2,
- byl také zjištěn názor pracovníků dotčených subjektů na legislativu kybernetické bezpečnosti – většina respondentů jej považuje spíše za rozumný krok k dosažení lepší úrovně kybernetické bezpečnosti – viz 5.3.8,
- byla zodpovězena otázka, zda jsou povinnosti vyplývající ze ZKB přísnější, než opatření dříve zaváděná na základě zákona č. 365/2000 Sb. o ISVS – zcela jednoznačně jsou přísnější než dříve zaváděná opatření – viz 5.3.6,
- bylo zjištěno, zda zajišťování souladu se ZKB pro organizace znamená významnou administrativní či finanční zátěž – z odpovědí vyplývá, že jednoznačně ano – viz též 5.3.6,
- byla zodpovězena otázka, zda jsou z hlediska zátěže na organizaci významné i povinnosti nad rámec bezpečnostních opatření – až na jeden KrÚ byly odpovědi pouze „spíše ano“ a „určitě ano“, tedy zátěž významná je – viz 5.3.6,
- byly zjištěny názory pracovníků KrÚ, zda považují přechodné období na implementaci všech požadavků ZKB za dostatečně dlouhé – mírně převažuje názor, že spíše ne – viz též 5.3.6,
- byly zjištěny odpovědi na otázku, zda využívaly povinné subjekty nějaké oborové standardy k řízení bezpečnosti a do jaké míry – vesměs používaly normy z rodiny ISO/IEC 27000 i když většinou jen částečně, nikoli k certifikaci – viz 5.3.3,
- byla též zodpovězena otázka začlenění kybernetické bezpečnosti do organizační struktury KrÚ – lze říci, že v tomto ohledu se jednotlivé KrÚ velmi liší, proaktivně ale budou implementovat bezpečnostní role – viz 5.3.4,
- bylo zjištěno, zda se KrÚ spoluúčastnili na tvorbě legislativy kybernetické bezpečnosti – většina se neúčastnila, některé záměrně z důvodu, že neměli potřebu zasahovat – viz 5.3.8,
- byly nasbírány odpovědi na otázku, zda jsou povinné subjekty ochotné čerpat prostředky z fondů IROP a případné důvody, proč ne – mírně převažují negativní

odpovědi, ale nejen z důvodu administrativní zátěže nebo rizika nekonzistentních auditů, ale také některé kraje již tuto nebo jinou možnost využily – viz 5.3.7,

- také bylo zjištěno, jak se staví povinné subjekty k možnosti outsourcingu kybernetické bezpečnosti – navzdory administrativě spojené s veřejnými zakázkami alespoň částečný outsourcing plánuje využít 9 z 10 krajů, pravděpodobně především z hlediska auditingu a poradenství – viz 5.3.5,
- bylo také zjištěno, jaké dopady považují respondenti za nejzásadnější – zmíněny byly zejména negativní administrativní a finanční dopady a také pozitivní dopady vzhledem ke zvýšení úrovně bezpečnosti nebo jejího snadnějšího prosazení – viz 5.3.8.

Z provedeného průzkumu mj. vyplývá to, že krajské úřady problematiku kybernetické bezpečnosti sice řeší, ale množství se jich nachází teprve ve fázi jednání a rozhodování a v přechodné lhůtě pro implementaci bezpečnostních opatření. Jedná se tedy momentálně o velmi dynamickou oblast a průzkum dopadů bude vhodné opakovat v době, kdy bude dokončena první vlna implementace povinností vyplývajících ze ZKB a řada nyní nejasných otázek bude v procesu implementace zodpovězena.

5.4.1 Návrhy pro další výzkum

Vzhledem k tomu, že množství povinných subjektů teprve se zajišťováním souladu se ZKB začíná a tato oblast je nyní velmi dynamická, průzkum dopadů ZKB na povinné subjekty bude vhodné provést opakovaně v době, kdy se situace více ustálí (nikdy by se neměla úplně ustálit, to by odporovalo principu kontinuálního zlepšování, ale lze předpokládat, že po první vlně implementací bezpečnostních opatření by situace měla být klidnější). Toto může být předmětem dalšího zkoumání.

Další výzkum může být také prováděn se zaměřením na určitý aspekt kybernetické bezpečnosti např. čistě na organizační či technická opatření a jejich časové/finanční náročnosti apod. a jít tak v určité oblasti do větší hloubky. Zde je ovšem potřeba zajistit možnost získat data. Je to vhodná volba spíše pro ty, kteří ve zkoumané organizaci pracují nebo vystupují v roli dodavatele.

Hlavní cílovou skupinou v této práci jsou krajské úřady. Dopady ZKB by bylo vhodné analyzovat také i v dalších povinných subjektech (např. provést obdobný výzkum na ústředních správních úřadech), případně se zaměřit na konkrétní problém organizací určitého typu – např. řešení hlášení bezpečnostních incidentů na národní vs. vládní CERT v organizacích typu velkých energetických podniků, které spravují systémy spadající pod národní i vládní CERT. Tyto podniky totiž mohou být orgány a osobami podle § 3 písm. a), b), c) i d) dle ZKB. Ve složitěji organizovaných podnicích také může nastat

situace, kdy dceřiný podnik financuje matka, která rozhoduje o tom, zda a kolik prostředků poskytne na implementaci, přičemž dle ZKB je ale za implementaci zodpovědný dceřiný podnik.

Bylo by také možné (a velmi vhodné) zabývat se dále mírou potřeby sjednocení metodického vedení orgánů veřejné správy z hlediska organizování kybernetické bezpečnosti.

6 Závěr

Česká republika zavedla, mj. i díky tlaku vyvíjenému z EU, komplexní systém kybernetické bezpečnosti za účelem ochrany informačních systémů klíčových pro chod státu a zajišťování základních potřeb a bezpečnosti obyvatelstva. Mezi tyto klíčové systémy patří systémy kritické informační infrastruktury spravované soukromými osobami i státem a také významné informační systémy spravované orgány veřejné moci. Systém kybernetické bezpečnosti a cesta k legislativě kybernetické bezpečnosti byly popsány v kap. 3 a 4.

Hlavní pilíř a přínos práce tvoří kapitoly 4 a 5. V kapitole 4 je zákon o kybernetické bezpečnosti rozebrán z hlediska dopadů na povinné subjekty a na základě tohoto rozboru jsou formulovány otázky, které jsou shrnuty v podkapitole 4.9 – Shrnutí dopadů ZKB na povinné subjekty. S cílem ověření předpokládaných dopadů ZKB na povinné subjekty formou zodpovězení otázek formulovaných ve 4.9.3 byl následně navržen a proveden průzkum stavu kybernetické bezpečnosti na krajských úřadech s důrazem na dopady způsobené zákonem o kybernetické bezpečnosti do těchto organizací. Tento průzkum je předmětem kapitoly 5. Průzkum byl proveden formou dotazníkového šetření a týká se všech oblastí, které vyplynuly z rozboru v kap. 4., tj.: organizace a řízení bezpečnosti, zátěže na organizaci vzniklou v souvislosti se ZKB, ochoty využití finančních prostředků z fondů IROP, outsourcingu kybernetické bezpečnosti a také názoru pracovníků na tuto legislativu. Výsledky průzkumu jsou shrnuty v kap. 5.4 – Celkové shrnutí a zhodnocení průzkumu.

Cíle práce formulované v úvodu (kap. 1.2 Vymezení cíle a postupu) tímto byly naplněny.

Z průzkumu vyplývají tyto hlavní závěry:

Lze s jistotou konstatovat, že implementace ZKB znamená pro krajské úřady významnou zátěž a to jak administrativní, tak finanční a personální. Významná z hlediska zátěže na organizaci je nejen implementace bezpečnostních opatření, ale také – a to v rozporu s formulovaným předpokladem (kap. 4.6.2) i tvrzením z důvodové zprávy k ZKB – implementace povinností nad rámec těchto opatření (tj. zasílání kontaktních údajů, detekce a hlášení událostí resp. incidentů, pro více viz 4.6.2).

Podstatným zjištěním je značná nejednotnost v organizování kybernetické bezpečnosti mezi jednotlivými krajskými úřady, která je dána pravděpodobně rozdílným přístupem k problematice bezpečnosti u vedení těchto subjektů. ZKB tak navzdory značné standardizaci bezpečnosti mezi povinnými subjekty pravděpodobně nepřispěje k významnému sjednocení kybernetické bezpečnosti v ohledu jejího organizování mezi touto kategorií povinných subjektů. Respondenti se nicméně shodli na tom, že ZKB je dobrým krokem pro zajištění lepší úrovně bezpečnosti informačních a komunikačních systémů povinných subjektů a vyplývá z něj, že objektivní tlak na soulad s legislativou

umožňuje pracovníkům kompetentním za kybernetickou bezpečnost lépe prosazovat u managementu projekty týkající se kybernetické bezpečnosti a také prosazovat nastavení a dodržování jednotných postupů a pravidel. Jeden z respondentů uvedl, že nejzásadnějším dopadem ZKB je „*zákonná možnost nastolení pořádku v oblasti kybernetické bezpečnosti*“. ZKB tak v některých případech může sloužit jako „spouštěč“ dříve připravených či chtěných opatření, která se nedařilo prosadit.

Jednoznačně se také ukázalo, že požadavky ZKB z hlediska bezpečnostních opatření jsou u všech dotazovaných (kromě jediného, který neodpověděl) přísnější, než jimi dříve zaváděná opatření na základě zákona č. 365/2000 Sb. o informačních systémech veřejné správy a jeho prováděcích předpisů, který – na rozdíl od ZKB – klade větší důraz spíše na dokumentaci než na konkrétní implementaci bezpečnostních opatření. KrÚ nicméně i před ZKB užívaly při řízení bezpečnosti normy řady ISO/IEC 27000, byť většinou nikoli na úrovni certifikace.

Výše uvedené výsledky autor považuje za stěžejní přínosy práce. Mohou být užitečné všem, kteří se zajímají o dopady ZKB na povinné subjekty, které jsou správci významných informačních systémů a zejména pak pracovníkům krajských úřadů pro porovnání „svých“ úřadů s ostatními.

Na základě různých aktivit, pořádání mnoha konferencí na toto téma a medializaci ZKB se o problematice kybernetické bezpečnosti více mluví, což lze považovat za pozitivní dopad ZKB z hlediska bezpečnostního povědomí celé české společnosti. Díky úsilí těch, kteří se snaží pozvednout bezpečnostní povědomí v ČR, se autor začal o tuto problematiku také zajímat a na základě toho vznikla i tato práce.

Pokud výsledky práce budou někomu užitečné a pomohou např. pracovníkům krajských nebo jiných úřadů, bude naplněno autorovo přání.

Seznam literatury

1. KUČÍNSKÝ, Adam a Martin KONEČNÝ. Zkušenosti a výsledky určování KII a VIS. In: [online]. Praha. 2015. Dostupné z: http://www.cybersecurity.cz/data/NBU_2015-KII_VIS.pdf.

2. ANTUŠÁK, Emil. *Krizový management: hrozby – krize – příležitosti.* Vyd. 1. Praha: Wolters Kluwer Česká republika, 2009. ISBN 978-80-7357-488-8.

3. SOUČEK, Vladimír, Eva STAŇKOVÁ, Martin LINHART a KOLEKTIV. *Vnitřní bezpečnost a veřejný pořádek: Krizové řízení (Modul G)* [online]. Praha: Ministerstvo vnitra, Odbor bezpečnostní politiky, 2005 [vid. 19. březen 2016]Dostupné z: www.mvcr.cz/soubor/bezpecnost-pdf.aspx

4. *Terminologický slovník pojmů z oblasti krizového řízení a plánování obrany státu* [online]. Praha: Ministerstvo vnitra, Odbor bezpečnostní politiky, 2009 [vid. 19. březen 2016]Dostupné z: http://krizport.firebrno.cz/file/165_1_1/

5. KOLEKTIV AUTORŮ POD VEDENÍM MINISTERSTVA ZAHRANIČNÍCH VĚCÍ ČESKÉ REPUBLIKY. *Bezpečnostní strategie České republiky 2015* [online]. Praha: Ministerstvo zahraničních věcí České republiky, 2015 [vid. 19. březen 2016]. ISBN 978-80-7441-005-5. Dostupné z: http://www.vlada.cz/assets/ppov/brs/dokumenty/bezpecnostni-strategie-2015.pdf

6. Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky [online]. In: Fulsoft [právní systém]. [vid. 13. leden 2016]. Dostupné z: http://www.fulsoft.cz/a0x7o.

7. Zákon č. 219/1995 Sb., Devizový zákon [online]. In: Fulsoft [právní systém]. [vid. 19. březen 2016]. Dostupné z: http://www.fulsoft.cz/a0x7q.

8. NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. Důvodová zpráva (k zákonu o kybernetické bezpečnosti). In: MAISNER, Martin a Barbora VLACHOVÁ. Zákon o kybernetické bezpečnosti: komentář. Vydání první. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8.

9. Zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) [online]. [vid. 14. březen 2016]. Dostupné z: https://portal.gov.cz/app/zakony/download?idBiblio=49557&nr=240~2F2000~20Sb.&ft=pdf.

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

11. MATES, Pavel a Vladimír SMEJKAL. *E-government v České republice: právní a technologické aspekty*. 2., podstatně přeprac. a rozš. vyd., V nakl. Leges vyd. 1. Praha: Leges, 2012. Edice Teoretik. ISBN 978-80-87576-36-6.

12. EU. *Návrh SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii* [online]. Brusel. 2013. [vid. 26. březen 2016]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX:52013PC0048.

13. BALDA, Pavel. *Informační a řídící systémy I. SCADA a HMI systémy* [online]. Prezentace k přednášce ZČU v Plzni, FAV, KKY. Plzeň. [b.r.]. [vid. 27. březen 2016]. Dostupné z: http://vendulka.zcu.cz/Download/Free/IRS1/IRS1-08_SCADA_HMI.pdf.

14. WUEEST, Candid. *Targeted Attacks Against the Energy Sector* [online]. 13. leden 2014. S.l.: Symantec. [vid. 25. březen 2016]. Dostupné z: https://scadahacker.com/library/Documents/Cyber_Events/Symantec%20-%20Targeted%20Attacks%20Against%20the%20Energy%20Sector.pdf.

15. Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích) [online]. In: Portál veřejné správy. [vid. 19. únor 2016]. Dostupné z: https://portal.gov.cz/app/zakony/download?idBiblio=59921&nr=127~2F2005~20Sb.&ft=pdf.

16. EU. *Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace* [online]. Brussels. 2013. [vid. 17. březen 2016]. Dostupné z: http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=1667.

17. RAJNOVIC, Damir. Cyberspace – What is it? *Cisco Blogs* [online]. 26. červenec 2012 [vid. 25. březen 2016]. Dostupné z: http://blogs.cisco.com/security/cyberspace-what-is-it

18. MAUER, Tim a Robert MORGUS. *Compilation of Existing Cybersecurity and Information Security Related Definitions* [online]. S.l. New America, 2014. Dostupné z: https://static.newamerica.org/attachments/175-compilation-of-existing-cybersecurity-and-information-security-related-definitions/OTI_Compilation_of_Existing_Cybersecurity_and_Information_Security_Related_Definitions_Updated122015.pdf.

19. NATO. Cyber Definitions. *NATO CCDCOE Resources* [online]. [vid. 27. březen 2016]. Dostupné z: https://ccdcoe.org/cyber-definitions.html

20. KROPÁČOVÁ, Andrea. CERT/CSIRT týmy a jejich role - Root.cz. *root.cz* [online]. 5. červen 2013 [vid. 27. březen 2016]. Dostupné z: http://www.root.cz/clanky/cert-csirt-tymy-a-jejich-role/

21. CSIRT.CZ. *Zpráva o činnosti CSIRT.CZ (Národního CSIRT ČR) za rok 2012* [online]. S.l. 2013. [vid. 29. březen 2016]. Dostupné z: https://www.csirt.cz/files/csirt/Zprava_o_cinnosti_CSIRT.CZ.2012.pdf.

22. BRONK, Henk, Marco THORBRUEGGE a Mehis HAKKAJA. *CSIRT Setting Up Guide: A Step-by-step Approach On How To Set Up a CSIRT* [online]. S.l. ENISA, 2006. Dostupné z: https://www.enisa.europa.eu/activities/cert/support/guide/files/csirt-setting-up-guide/at_download/fullReport.

23. POLČÁK, Radim. *Internet a proměny práva*. Téma. Praha: Auditorium, 2012. ISBN 978-80-87284-22-3.

24. POLČÁK, Radim. Kybernetická bezpečnost jako aktuální fenomén českého práva. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy* [online]. roč. 6, č. 11/2015. ISSN 1805-2797. Dostupné z: https://journals.muni.cz/revue/article/download/2980/R_2015_11_TEMA_Polčák_v2.

25. NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. Důvodová zpráva (k zákonu o kybernetické bezpečnosti) [online]. [vid. 28. únor 2016]. Dostupné z: https://www.govcert.cz/download/nodeid-1855/.

26. PETERKA, Jiří. CSIRT, nebo CERT? *dsl.cz* [online]. 4. srpen 2008 [vid. 29. březen 2016]. Dostupné z: http://www.dsl.cz/clanky/1028-csirt-nebo-cert

27. Záměr 2006: CESNET CSIRT. *Cesnet* [online]. 2012 1996 [vid. 29. březen 2016]. Dostupné z: http://wayback.webarchiv.cz/wayback/20121025182306/http://www.cesnet.cz/doc/2006/zprava/csirt.html

28. Projekt Kybernetické hrozby. *CSIRT.cz* [online]. [vid. 29. březen 2016]. Dostupné z: https://www.csirt.cz/page/892/projekt-kyberneticke-hrozby/

29. ČR. *Usnesení vlády české republiky ze dne 19. října 2011 č. 781 o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast* [online]. Praha. 2011. [vid. 29. březen 2016]. Dostupné z: https://www.nbu.cz/cs/aktuality/994-informace-k-usneseni-vlady-ceske-republiky-ze-dne-19-rijna-2011-c-781/.

30. *Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 - 2015* [online]. Praha. Národní bezpečnostní úřad, 2011. [vid. 11. duben 2014]. Dostupné z: https://www.govcert.cz/download/nodeid-727/.

31. VLÁDA ČASKÉ REPUBLIKY. *Příloha k usnesení vlády ze dne 19. října 2011 č. 781: Statut Rady pro kybernetickou bezpečnost* [online]. Praha. 2011. [vid. 29. březen 2016]. Dostupné z: https://www.govcert.cz/download/nodeid-1525/.

32. CZ.NIC - CZ.NIC ohlídá kybernetickou bezpečnost České republiky. [online]. [vid. 29. březen 2016]. Dostupné z: https://www.nic.cz/page/830/cz.nic-ohlida-kybernetickou-bezpecnost-ceske-republiky/

33. NÁRODNÍ BEZPEČNOSTNÍ ÚŘAD. *Zpráva o stavu kybernetické bezpečnosti České republiky 2014* [online]. S.l. 2015. [vid. 20. březen 2016]. Dostupné z: https://www.govcert.cz/download/nodeid-612/.

34. HARTMANN, Ivo. Bitva tajných služeb s ministerstvem vnitra o citlivá data. *Česká Justice* [online]. 18. duben 2016 [vid. 19. duben 2016]. Dostupné z: http://www.ceska-justice.cz/blog/bitva-tajnych-sluzeb-s-ministerstvem-vnitra-o-citliva-data/

35. *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020* [online]. S.l.: NBÚ, [b.r.]Dostupné z: https://www.govcert.cz/download/nodeid-1004/

36. COOK, Šárka a Dušan NAVRÁTIL. Na aktuální téma s ředitelem NBÚ Dušanem Navrátilem. *kybez.cz: Portál Kybernetické Bezpečnosti [převzato z časopisu Review pro obranný a bezpečnostní průmysl]* [online]. 4. prosinec 2015 [vid. 30. březen 2016]. Dostupné z: https://www.kybez.cz/zpravy/-/blogs/revue-aobp-na-aktualni-tema-s-reditelem-nbu-dusanem-navratilem

37. NAVRÁTIL, Dušan. *Kybernetická bezpečnost ČR 2015: Aktivity NBÚ, Zkušenosti a výsledky určování KII a VIS* [online]. Praha. NBÚ, 2015. [vid. 23. únor 2016]. Dostupné z: http://www.cybersecurity.cz/data/NBU_Navratil2015.pdf.

38. EVROPSKÝ PARLAMENT. Vnitřní trh a ochrana spotřebitelů. *Evropský parlament: Výbory* [online]. [vid. 17. duben 2016]. Dostupné z: http://www.europarl.europa.eu/committees/cs/imco/home.html

39. COUNCIL OF THE EUROPEAN UNION. Improving cyber security across the EU. *Council of the European Union* [online]. 18. prosinec 2015 [vid. 17. duben 2016]. Dostupné z: http://www.consilium.europa.eu/en/policies/cyber-security/

40. EUROSKOP. Informační společnost v březnu 2015. *Euroskop.cz - Monitoring legislativy EU* [online]. 4. září 2015 [vid. 17. duben 2016]. Dostupné z: https://www.euroskop.cz/13/25598/clanek/informacni-spolecnost-v-breznu-2015/

41. EUROSKOP. Informační společnost v lednu 2016. *Euroskop.cz - Monitoring legislativy EU* [online]. [vid. 17. duben 2016]. Dostupné z: https://www.euroskop.cz/13/26917/clanek/informacni-spolecnost-v-lednu-2016/

42. EU. *Návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti síťových a informačních systémů v Unii - politická dohoda* [online]. Brusel. 2016. [vid. 17. duben 2016]. Dostupné z: http://eur-lex.europa.eu/legal-content/CS/TXT/PDF/?uri=CONSIL:ST_5894_2016_INIT&qid=1460898934549&from=CS.

43. EU. *Special Eurobarometer 423 Cyber Security Report* [online]. S.l.: s.n., 2015 [vid. 26. březen 2016]. ISBN 978-92-79-46185-9. Dostupné z: http://ec.europa.eu/COMMFrontOffice/PublicOpinion/index.cfm/ResultDoc/download/DocumentKy/64573

44. SMEJKAL, Vladimír. *Kybernetická kriminalita*. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, s.r.o, 2015. Ediční řada Pro praxi. ISBN 978-80-7380-501-2.

45. ROHEL, Vladimír. Dopady zákona o kybernetické bezpečnosti na povinné osoby. *DSM – data security management*. 2013, roč. XVII, č. 4. ISSN 1211-8737.

46. NBÚ. *Odůvodnění k návrhu vyhlášky, kterou se mění vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích* [online]. Praha. 2016. [vid. 21. duben 2016]. Dostupné z: https://apps.odok.cz/attachment/-/down/RACKA67D9HLM.

47. SEDLÁK, Jan. V Brně otevře Kybernetický polygon pro simulaci hackerských útoků. [online]. 28. duben 2015 [vid. 19. duben 2016]. Dostupné z: http://e-svet.e15.cz/it-byznys/v-brne-otevre-kyberneticky-polygon-pro-simulaci-hackerskych-utoku-1184644

48. MASARYKOVA UNIVERZITA. KYPO - Kybernetický polygon. [online]. [vid. 19. duben 2016]. Dostupné z: https://www.kypo.cz/?lang=cs

49. VELECKÝ, Petr. O2 IT Services otevřelo v Praze centrum kybernetické bezpečnosti – ITBIZ – Vaše jednička mezi nulami. *itbiz.cz* [online]. 20. duben 2016 [vid. 25. duben 2016]. Dostupné z: http://www.itbiz.cz/tiskove-zpravy/o2-it-services-otevrelo-v-praze-centrum-kyberneticke-bezpecnosti

50. MAISNER, Martin a Barbora VLACHOVÁ. *Zákon o kybernetické bezpečnosti: komentář*. Vydání první. Praha: Wolters Kluwer, 2015. Komentáře (Wolters Kluwer ČR). ISBN 978-80-7478-817-8.

51. KUČÍNSKÝ, Adam. Představení výzvy č. 10 IROP – Kybernetická bezpečnost (přednáška).

In: [online]. Hradec Králové. 4. květen 2016. [vid. 4. červenec 2016]. Dostupné z: https://www.isss.cz/archiv/2016/download/prezentace/nbu_kucinsky.pdf.

52. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury [online]. [vid. 22. březen 2016]. Dostupné z: http://www.fulsoft.cz.zdroje.vse.cz/33/432-2010-sb-narizeni-vlady-o-kriteriich-pro-urceni-prvku-kriticke-infrastruktury-ve-zneni-ucinnem-k-1-1-2015-uniqueidOhwOuzC33qe_hFd_-jrpTuGR1zhsUxSSiFyPLd6oM1cCD-vMUnwPlw/?query=432%2F2010&serp=1.

53. KUČÍNSKÝ, Adam. *Představení výzvy č. 10 IROP – Kybernetická bezpečnost* [online]. Zvukový záznam přednášky. Hradec Králové: 4. květen 2016. [vid. 22. duben 2016]. Dostupné z: https://www.isss.cz/archiv/2016/download/audio/kyber_1kucinsky.mp3.

54. TŮMA, Miroslav. *Kybernetická bezpečnost resortu MV* [online]. S.l.: Ministerstvo vnitra České republiky. [vid. 28. únor 2016]. Dostupné z: http://www.egovernment.cz/setkani/4.pdf.

55. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích [online]. In: Portál veřejné správy. [vid. 11. únor 2016]. Dostupné z: https://portal.gov.cz/app/zakony/download?idBiblio=83171&nr=317~2F2014~20Sb.&ft=pdf.

56. MAREK, Dominik, Marek CHLUP a D. BUŘIČOVÁ. *Určení významných informačních systémů dle zákona č. 181/2014 Sb. o kybernetické bezpečnosti pro: jednání rady kraje č. 3/2016 dne 19. 1. 2016* [online]. Jihlava. Kraj Vysočina, 2016. [vid. 2. duben 2016]. Dostupné z: http://extranet.kr-vysocina.cz/samosprava/soubory/rada/materialy/2016/03/RK-03-2016-35.doc, http://extranet.kr-vysocina.cz/samosprava/index.php?akce=rada_materialy_detail&id=27806.

57. MAREK, Dominik a Chlup MAREK. RK-03-2016-35, př. 3: *Zpráva o posouzení VIS* [online]. Jihlava. Kraj Vysočina, 2016. [vid. 4. únor 2016]. Dostupné z: http://extranet.kr-vysocina.cz/samosprava/soubory/rada/materialy/2016/03/RK-03-2016-35pr03.doc.

58. NBÚ. *Bezpečnostní role a jejich začlenění v organizaci* [online]. S.l. [b.r.]. [vid. 21. leden 2016]. Dostupné z: https://www.govcert.cz/download/nodeid-589/.

59. PEKÁREK, Aleš. Představení 10. výzvy IROP „Kybernetická bezpečnost". In: [online]. Hradec Králové. 4. květen 2016. [vid. 5. duben 2016]. Dostupné z: https://www.isss.cz/archiv/2016/download/prezentace/mmr_pekarek.pdf.

60. KOTZIAN, Robert. *Dopad zákona o kybernetické bezpečnosti na města a obce* [online]. Hradec Králové. ČIMIB, [b.r.]. [vid. 4. červen 2016]. Dostupné z: https://www.isss.cz/archiv/2015/download/prezentace/cimib_kotzian.pdf.

61. *Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)* [online]. S.l.: In: Portál veřejné správy. [vid. 21. leden 2016]. Dostupné z: https://portal.gov.cz/app/zakony/download?idBiblio=82522&nr=181~2F2014~20Sb.&ft=pdf.

62. SMEJKAL, Vladimír. Jak je to se zákonem o kybernetické bezpečnosti. *DSM – data security management*. 2013, roč. XVII, č. 4. ISSN 1211-8737.

63. KLESLA, Jan. Pro kybernetickou bezpečnost jsou klíčové prováděcí předpisy. *Právní rádce.* [online]. 2014, roč. 12, s. 16. [vid. 15. březen 2016]. ISSN 1210-4817. Dostupné z: http://pravniradce.ihned.cz/c1-63247640-pro-kybernetickou-bezpecnost-jsou-klicove-provadeci-predpisy.

64. HARAŠTA, Jakub. Právní aspekty kybernetické bezpečnosti ČR. *Revue pro právo a technologie: odborný recenzovaný časopis pro technologické obory práva a právní vědy* [online]. roč. 4, č. 8/2013. ISSN 1805-2797. Dostupné z: https://journals.muni.cz/revue/article/download/2980/R_2015_11_TEMA_Polčák_v2.

65. NÁPRAVNÍK, Jiří. Kyber-bezpečnost a připravovaný zákon |. [online]. 15. duben 2013 [vid. 27. březen 2016]. Dostupné z: http://napravnik.blog.ihned.cz/c1-59692700-kyber-bezpecnost-a-pripravovany-zakon

66. SYSTEM ONLINE. Lidé jako klíčový prvek kybernetické bezpečnosti státu. *System OnLine* [online]. 19. listopad 2015 [vid. 16. duben 2016]. Dostupné z: http://www.systemonline.cz/it-security/lide-jako-klicovy-prvek-kyberneticke-bezpecnosti-statu-z.htm

Seznam tabulek

Seznam tabulek

Tabulka č. 1: Zkratky legislativních dokumentů 5

Seznam tabulek přílohy D je uvededen v této příloze.

Seznam příloh

Příloha A: Popis elektronické přílohy 99

Příloha B: Dotazník 100

Příloha C: Struktura dotazníku 105

Příloha D: Data získaná z dotazníku 107

Příloha E: Významné informační systémy krajů 117

Příloha A: Popis elektronické přílohy

V této příloze se nachází popis netištěné elektronické přílohy (přiložena k tištěné a svázané práci na DVD a ve školním informačním systému ISIS).

Jedná se o soubor typu *.zip, který obsahuje dva adresáře:

- Zasilany_dotaznik – obsahuje kopii souboru, který byl rozesílán na krajské úřady,
- Vracene_dotazniky_anonymizovane – obsahuje data, která jsem získal od respondentů a to jako soubory typu Microsoft Word *.docx a pak tabulku Microsoft Excel *.xlsx, která obsahuje data ze získaných dotazníků zpracovaná formou tabulky. Data jsou anonymizována.

Příloha B: Dotazník

Tato příloha obsahuje znění dotazníku tak, jak byl navržen autorem a rozesílán na krajské úřady včetně úvodního slova respondentům. Kopie rozesílaného souboru je uložena v netištěné elektronické příloze (viz Příloha A: Popis elektronické přílohy.)

Dopady ZKB na krajské úřady – průzkum

Prostřednictvím tohoto dotazníku bych rád zjistil názor pracovníků krajských úřadů na současnou legislativní úpravu kybernetické bezpečnosti – zákon o kybernetické bezpečnosti (dále jako „ZKB“) a jeho prováděcích předpisů. Tento průzkum poslouží jako zdroj mé diplomové práce, která se věnuje dopadům ZKB na povinné osoby.

Jsem si vědom, že poskytovat citlivé informace ohledně bezpečnosti není možné. Z tohoto důvodu je dotazník koncipován tak, aby se takovým otázkám pokud možno vyhnul. Zajímá mě zejména názor pracovníků povinných subjektů na legislativní povinnosti, zda považují tuto regulaci spíše za přínosnou či za zbytečnou práci navíc nebo je přes své případné klady z nějakého důvodu problematická.

Pokud některou otázku budete považovat za příliš citlivou, neodpovídejte na ni. Dotazník obsahuje 21 otázek, většina je typu ano/ne, vyplnění by tedy nemělo zabrat více než 15 minut. Všechny otázky jsou volitelné. Budu velmi rád i za zčásti vyplněný dotazník nebo telefonický rozhovor místo dotazníku či za případné připomínky k otázkám. Vážím si Vašeho času. Každý názor je pro mě cenný.

Děkuji!

INSTRUKCE K VYPLNĚNÍ

Nehodící se odpovědi vymažte nebo škrtněte. (Případně vybrané odpovědi zvýrazněte např. takto: **ano** – ne)

Pokud otázku nebudete chtít odpovědět, přeskočte ji, případně zanechte komentář.

Ke každé odpovědi je možno napsat komentář, pokud uznáte za vhodné.

Vyplněný dotazník prosím zašlete na emailovou adresu vojta@draganov.cz. Uveďte prosím, zda si přejete být v práci zpracováni anonymně (bez jména pracovníka nebo i bez názvu kraje).

Pro případné dotazy mě můžete kontaktovat na výše zmíněné emailové adrese nebo volat na +420 xxx xxx xxx[104].

---

[104] Autor si nepřeje zveřejňovat své soukromé telefonní číslo v diplomové práci.

DOTAZNÍK

1. Je nebo v nejbližší době bude Vaše organizace správcem významného informačního systému podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti?

Odpověď: *ano* *ne*

Komentář:

2. Je nebo v nejbližší době bude Vaše organizace správcem systému kritické informační infrastruktury podle § 3 zákona č. 181/2014 Sb., o kybernetické bezpečnosti?

Odpověď: *ano* *ne*

Komentář:

3. Považujete ZKB za rozumný krok k dosažení větší úrovně bezpečnosti důležitých informačních nebo komunikačních systémů?

Odpověď: *určitě ano* *spíše ano* *spíše ne* *určitě ne*

Komentář:

4. Jsou požadavky ZKB a navazující vyhlášky jasné a srozumitelné? Víte přesně, jaké konkrétní povinnosti máte?

Odpověď: *určitě ano* *spíše ano* *spíše ne* *určitě ne*

Komentář:

5. Využila Vaše organizace možnost podílet se na připomínkách k ZKB? (Úspěšně? – případné detaily prosím do komentáře.)

Odpověď: *ano* *ne*

Komentář:

6. V případě určení systému jako VIS nebo KII je povinnost do jednoho roku od této skutečnosti zajistit soulad se ZKB. Je či byla podle Vašeho názoru tato doba dostatečně dlouhá?

Odpověď: *určitě ano* *spíše ano* *spíše ne* *určitě ne*

Komentář:

7. Podle zákona 365/2000 Sb., o ISVS je zajišťování bezpečnosti informačních systémů provozovaných veřejnou správou povinné již několik let. Jsou požadavky ZKB a navazující vyhlášky na bezpečnostní opatření VIS přísnější, než Vámi již dříve zaváděná opatření?

Odpověď: *ano* *ne*

Komentář:

8. Jsou požadavky ZKB významné z hlediska administrativní či finanční zátěže?

Odpověď: *určitě ano* *spíše ano* *spíše ne* *určitě ne*

Komentář:

9. Jsou požadavky ZKB nad rámec bezpečnostních opatření (tj. hlášení bezpečnostních událostí/incidentů, kontakt s vládním CERT, …) významné z hlediska administrativní či finanční zátěže?

Odpověď: *určitě ano* *spíše ano* *spíše ne* *určitě ne*

Komentář:

10. Zaváděla Vaše organizace řízení bezpečnosti informací podle nějakého oborového standardu či normy ještě před ZKB? (Pokud ano, prosím specifikujte v komentáři.)

Odpověď: *ano* *ne*

Komentář:

11. Od 21.10.2015 je vypsána Výzva č. 10 IROP – Kybernetická bezpečnost určená na technická bezpečnostní opatření VIS a KII podle ZKB. Organizaci umožňuje čerpat částky v desítkách milionů Kč. Plánujete čerpání peněz z tohoto programu?

Odpověď: *ano* *ne*

Komentář:

12. Pokud je odpověď na předchozí ne, proč? (Přílišná administrativní složitost? Riziko vyplývající z následných auditů? Jiný důvod?)

Otevřená odpověď:

13. Je ve Vaší organizaci zvláštní organizační útvar věnující se bezpečnosti informací nebo kybernetické bezpečnosti (např. odbor či oddělení apod.)?

Odpověď: *ano* *ne*

Komentář:

14. Pokud je odpověď na předchozí otázku ano, kde v organizační struktuře je takový útvar začleněn? Kolik lidí se této oblasti věnuje?

Otevřená odpověď:

15. Je útvar či pracovník řídící kybernetickou bezpečnost oddělen od útvaru, který zajišťuje provoz ICT? Pokud je oddělen, ve kterém útvaru (odboru, oddělení apod.) je začleněn? /Prosím do komentáře/

Odpověď: *ano* *ne*

Komentář:

16. Změnila či bude se měnit struktura organizace nebo počet lidí věnujících se bezpečnosti na základě implementace ZKB? (Vyčlenění zvláštního útvaru či pracovníků atd. Případné detaily prosím do komentáře.)

Odpověď: *ano* *ne*

Komentář:

17. (*Pouze pro správce KII*) Vyhláška 316/2014 Sb. vyžaduje po osobách v § 3 c), d) zavést tzv. bezpečnostní role – architekt, manažer, auditor kybernetické bezpečnosti a garant aktiva. ZKB vyžaduje na tyto pozice vyjma garanta praxi alespoň tři roky v oboru řízení bezpečnosti IT a také vyškolení (byť parametry školení nejsou zákonem upraveny). Je tato povinnost splnitelná bez větších obtíží?

Odpověď: *ano* *ne*

Komentář:

18. (*Pouze pro správce VIS*): Vyhláška 316/2014 Sb. vyžaduje po správcích významného informačního systému zavést tzv. bezpečnostní role – architekt, manager, auditor kybernetické bezpečnosti a garant aktiva – pouze přiměřeně. Které z těchto rolí jste stanovili či plánujete zavést?

Odpověď: *architekt* *manažer* *auditor* *garant aktiva* *(výbor pro kybernetickou bezpečnost)*

Komentář:

19. Realizujete kybernetickou bezpečnost vlastními silami nebo (byť zčásti) externě?

Odpověď: *jen vlastními silami* *částečný/úplný outsourcing*

Komentář:

20. Je realizace bezpečnosti pomocí outsourcingu schůdná (vzhledem k procesní nutnosti zajišťování prostředků a vyhlašování výběrových řízení, řízení odpovědností atd.)?

Odpověď: *určitě ano* *spíše ano* *spíše ne* *určitě ne*

Komentář:

21. Jaké jsou podle Vás ve shrnutí nejzásadnější dopady zákona o kybernetické bezpečnosti na Vaši organizaci?

Otevřená odpověď:

Připomínky či poznámky k celému dotazníku:

Děkuji za ochotu a za Váš čas!

Příloha C: Struktura dotazníku

Pro lepší orientaci v dotazníku je v této příloze vytvořená tabulka, která ukazuje možnosti odpovědí na jednotlivé otázky.

***Tabulka C1**: Tabulka otázek (Zdroj: autor)*

	Možnosti odpovědí
O1	*ano, ne*
O2	*ano, ne*
O3	*určitě ano, spíše ano, spíše ne, určitě ne*
O4	*určitě ano, spíše ano, spíše ne, určitě ne*
O5	*ano, ne*
O6	*určitě ano, spíše ano, spíše ne, určitě ne*
O7	*ano, ne*
O8	*určitě ano, spíše ano, spíše ne, určitě ne*
O9	*určitě ano, spíše ano, spíše ne, určitě ne*
O10	*ano, ne*
O11	*ano, ne*
O12	(otevřená otázka)
O13	*ano, ne*
O14	(otevřená otázka)
O15	*ano, ne*
O16	*ano, ne*
O17	*ano, ne* (pouze pro správce KII)
O18	*architekt, manažer, auditor, garant aktiva, (výbor pro kybernetickou bezpečnost)*
O19	*jen vlastními silami, částečný/úplný outsourcing*
O20	*určitě ano, spíše ano, spíše ne, určitě ne*
O21	(otevřená otázka)

O1 až O21 – označení pro jednotlivé otázky.

Otázky č. 12, 14 jsou podmíněné každá svou předcházející otázkou.

Otázky č. 17 a 18 jsou také podmíněné. Otázka č. 17 se týká pouze správců systémů KII a otázka č. 18 se týká pouze správců VIS.

Příloha D: Data získaná z dotazníku

V této příloze jsou ve strukturované podobě uvedena data získaná z dotazníku. Odpovědi jsou rozdělené podle rozlišení otázek na uzavřené a otevřené. Poté jsou uvedeny komentáře k jednotlivým otázkám.

Pro všechny v této příloze uvedené tabulky platí, že zdrojem je autorův průzkum. U tabulek již není zdroj uváděn.

Použité značení společné pro všechny tabulky**:**

K1 až K10 – označení pro jednotlivé krajské úřady.

O1 až O21 – označení pro jednotlivé otázky.

Seznam tabulek této přílohy

Tabulka P1: Odpovědi na uzavřené otázky 108
Tabulka P2: Odpovědi na otázky č. 12 a 14 110
Tabulka P3: Odpovědi na otázku č. 21 111
Tabulka P4: Komentáře k otázce 1 112
Tabulka P5: Komentáře k otázce 2 112
Tabulka P6: Komentáře k otázce 3 112
Tabulka P7: Komentáře k otázce 4 112
Tabulka P8: Komentáře k otázce 5 113
Tabulka P9: Komentáře k otázce 6 113
Tabulka P10: Komentáře k otázce 8 114
Tabulka P11: Komentáře k otázce 9 114
Tabulka P12: Komentáře k otázce 10 114
Tabulka P13: Komentáře k otázce 11 114
Tabulka P14: Komentáře k otázce 13 115
Tabulka P15: Komentáře k otázce 15 115
Tabulka P16: Komentáře k otázce 16 115
Tabulka P17: Komentáře k otázce 18 116
Tabulka P18: Komentáře k otázce 19 116
Tabulka P19: Komentáře k otázce 20 116

D.1 Odpovědi na uzavřené otázky

***Tabulka P1**: Odpovědi na uzavřené otázky*

	K1	K2	K3	K4	K5	K6	K7	K8	K9	K10
O1	ano	ano*	ano*	ano	ano	ano	ano	ano	ano	ano*
O2	ne	ne*	ne	ne	ne	ne	*P.K.*	ne	ne	ne
O3	spíše ano	určitě ano	spíše ano	spíše ano*	určitě ano	spíše ano	určitě ano	spíše ano	určitě ano	spíše ano
O4	určitě ano	určitě ano	spíše ano	spíše ne	určitě ano	spíše ne	spíše ano	spíše ano	určitě ano	určitě ano*
O5	ne*	ne*	ne	ano*	ne	ano	*P.K.*	ne*	ano	P.K.
O6	spíše ne*	spíše ne*	spíše ne	spíše ano	spíše ne	spíše ne	spíše ne*	spíše ano*	spíše ano	spíše ano*
O7	ano	ano	ano	ano	ano	ano	ano	ano	ano	/
O8	spíše ano	spíše ano	určitě ano	určitě ano*	určitě ano	určitě ano	určitě ano*	určitě ano	určitě ano	určitě ano*
O9	*P.K.*	spíše ano	určitě ano	spíše ano	spíše ano	určitě ano	spíše ano	určitě ano	spíše ano	spíše ne
O10	ano*	ano*	ano*	ne*	ne	ne	ano*	ano*	ano	ne
O11	ano	„spíše ne“*(P.K.)*	ne	ano	ano	ne	ne	ne	ano	ne
O13	ne*	ano*	ne	ne	ne	ne	ano	ne	ano	ano
O15	ne	ano*	ne*	ano	ne	ne	ano*	ne	ne	ano*
O16	*P.K.*	ano*	*P.K.*	ne*	ne	ano	ano*	ne*	ne	ne*
O17	/	/	/	/	/	/	/	/	/	/
O18	ar, ma, ga	ar, ma, au, ga, vý*	*P.K.*	*P.K.*	ma, ga, vý	ar, ma, au, ga, vý	ar, ma, ga, vý	ma, ga, vý	ma, au, ga	ar, ma, au, ga, vý*
O19	j.v.s.	č/ú*	č*	č/ú	č	č	č/ú	č	č	č*
O20	*ano, (…) (P.K.)*	spíše ano	spíše ano	spíše ano	spíše ano	spíše ano	spíše ano	spíše ano	spíše ne	určitě ano*

K1 až K10 – označení pro jednotlivé krajské úřady,

O1 až O21 – označení pro jednotlivé otázky,

* – označuje, že k otázce byl napsán komentář,

/ – označuje nevyplněnou odpověď,

P.K. – pouze komentář – respondent nevybral ani jednu z možností a odpovídal v komentáři.

Pro otázku č. 18 platí značení: *ar* – architekt kybernetické bezpečnosti, *ma* – manažer kybernetické bezpečnosti, *au* – auditor kybernetické bezpečnosti, *ga* – garant aktiva, *vý* – výbor pro kybernetickou bezpečnost.

Pro otázku 19 platí značení[105]: *j.v.s.* – jen vlastními silami, *č/ú* – částečný nebo úplný outsourcing, *č* – částečný outsourcing, *ú* – úplný outsourcing.

[105] Tuto otázku autor koncipoval jako uzavřenou s pouhými dvěma možnostmi a to „*jen vlastními silami*“ a „*částečný/úplný outsourcing*“. Někteří respondenti však využili možnost sdělit do průzkumu, zda outsourcing je (či bude) částečný nebo úplný tak, že zvýraznili jen jedno ze slov oddělených lomítkem. Tam, jde je uvedena odpověď „*č/ú*“ to rozlišeno není.

D.2 Odpovědi na otevřené otázky

Následuje výčet odpovědí na otevřené otázky, které se kvůli své délce nemohly vejít do výše uvedené tabulky.

***Tabulka P2**: Odpovědi na otázky č. 12 a 14*

	O12	**O14**
K1	/	*„Spadá pod pana ředitele, viz. předchozí odpověď"*
K2	*„obecně malá ochota čerpat z dotačních titulů – rizika nekonzistentních auditů"*	*„manažer KB je zařazen do odboru krizového řízení, zbytek rolí jen na odboru informatiky"*
K3	*„Některá technická opatření již byla realizována mimo jiné i v rámci projektu IOP."*	/
K4	*/ (využijí IROP)*	/
K5	*/ (využijí IROP)*	/
K6	/	*„odbor bezpečnosti + odbor informatiky, cca 5-7 osob"*
K7	*„bez odpovědi"*	/
K8	*„Využili jsme již dříve jiné Výzvy."*	/
K9	*/ (využijí IROP)*	*„kancelář ředitele"*
K10	*„přílišná administrativní složitost (tvorba projektu), úzké zaměření výzvy pouze na VIS (KII)"*	*„Dané oblasti se věnuje 1 pracovník (+ 1 externí poradce), je zařazen do běžného odboru, mimo odbor informatiky"*

K1 až K10 – označení pro jednotlivé krajské úřady.

O1 až O21 – označení pro jednotlivé otázky.

/ – značí ponechání prázdné odpovědi

/ (využijí IROP) – k otázce O12 – Tato otázka je podmíněná odpovědí „ano" v předchozí otázce č. 11. Pokud respondent uvedl v předchozí otázce ano, je v této tabulce uvedeno „*využijí IROP*". Pokud odpověděl v předchozí otázce „ne" a neuvedl v otázce č. 12 nic, je uvedeno lomítko „/" jako vynechaná odpověď. U všech ostatních odpovědí bylo v předchozí otázce uvedeno „ne".

***Tabulka P3**: Odpovědi na otázku č. 21*

	O21
K1	*„Z hlediska uživatelů zvýšení povědomí o rizicích a dopadech bezpečnosti informací v organizaci. Z hlediska správců a administrátorů ve spojení s normou ISO 27001 nastavení a dodržování jednotných postupů a pravidel.“*
K2	*„větší důraz na bezpečnost – ZoKB pomáhá prosazovat problematiku bezpečnosti; zvýšené výdaje; organizační změny“*
K3	*„organizační a finanční“*
K4	*„Nutné administrativní kroky, značné papírování, téměř žádná novinka ve stávající ICT HW bezpečnosti.“*
K5	*„Zvýšená administrativa, problém s personálním zajištěním, neschopnost financovat bezpečnostní role, vyšší bezpečnost.“*
K6	/
K7	*„zákonná možnost nastolení pořádku v oblasti kybernetické bezpečnosti“*
K8	*„Větší administrativa, více práce, větší náklady, sjednocení úrovně bezpečnosti s ostatními,“*
K9	*„finanční“*
K10	*„řešení bezpečnosti informací systémovým způsobem“*

/ – značí vynechanou odpověď

D.3 Komentáře k otázkám

Komentáře k otázkám tvoří také klíčový zdroj informací, neboť umožnily pracovníkům krajských úřadů vyjádřit se nad rámec daných možností otázky. V zájmu šetření místa a také papíru jsou v tabulkách řádky krajů, které nevyplnily komentář, vynechány.

***Tabulka P4**: Komentáře k otázce 1*

	Komentáře k otázce 1
K2	*„od února 2016, 4 systémy“*
K3	*„Webový portál, Spisová služba, Firemní e-mailová komunikace, Ekonomický systém.“*
K10	*„Kraj Vysočina začátkem roku určil 4 významné informační systémy (web kraje, spisová služba, ekonomické moduly, Exchange). Tyto informace budou (o všech krajích) zveřejněny v novele vyhlášky 317/2014 S.“*

***Tabulka P5**: Komentáře k otázce 2*

	Komentáře k otázce 2
K2	*„nepředpokládáme ani v budoucnu“*
K3	*„Webový portál, Spisová služba, Firemní e-mailová komunikace, Ekonomický systém.“*
K7	*„pravděpodobně ano/dosud nejednoznačné“*

***Tabulka P6**: Komentáře k otázce 3*

	Komentáře k otázce 3
K4	*„Kdo si je možných rizik vědom, připravoval se a připravuje i bez zákona. Kdo si vědom rizik není, nepomůže ani zákon.“*

***Tabulka P7**: Komentáře k otázce 4*

	Komentáře k otázce 4
K10	*„Implementace ISO/IEC 27001 nám dává poměrně přesnou metodiku zavádění bezpečnostních opatření, abychom byli v souladu se zákonem (a navazujících vyhlášek).“*

***Tabulka P8**: Komentáře k otázce 5*

	Komentáře k otázce 5
K1	*„Nyní, již takou možnost máme a využijeme ji při přípravě a úpravě ZoKB z hlediska NISu .“*
K2	*„zákon i vyhláška jsou srozumitelné, problematika byla široce diskutována“*
K4	*„V průběhu tvorby zákona byly svolány dvě schůzky na NBÚ, později se již neuskutečnily. Jedná na úrovni Asociace krajů v době platnosti ZKB nebyly již plodné.“*
K7	*„o této aktivitě nevím, mohlo to proběhnout např. legislativním odborem…“*
K8	*„Legislativu jsme sledovali, ale připomínky jsme nepodávali“*
K10	*„Bohužel nedokáži odpovědět, na tuto pozici jsem nastoupil v době, kdy implementace bezpečnostních opatření byla již v plném proudu.“*

***Tabulka P9**: Komentáře k otázce 6*

	Komentáře k otázce 6
K1	*„Spíše ne z hlediska technických opatření, který vyplývají ze zákona“*
K2	*„především s ohledem na rozpočtové období (trvá déle než rok výdaj naplánovat, vysoutěžit řešení a to pak implementovat)“*
K7	*„vzhledem ke zdlouhavým procesům, které souvisí s veřejnými zakázkami a dále potřebou zachovat posloupnost realizace jednotlivých kroků, je 1 rok spíše málo (a to nezmiňuji problematiku plánování finančních prostředků a personálních kapacit)“*
K8	*„To vyplývá z toho, že již část požadavků splňujeme“*
K10	*„Spíše ano, protože subjekty mohou zavést bezpečnostní opatření pouze pro určené VIS (resp. KII). My máme času málo, protože jsme se rozhodli certifikovat dle 27001 celý úřad, ale v obecné rovině je na to v podstatě dost času.“*

K otázce 7 žádný z respondentů neuvedl komentář.

***Tabulka P10**: Komentáře k otázce 8*

	Komentáře k otázce 8
K4	*„Technická bezpečnost je jen součástí ZKB, důraz je kladen na „procesy, administrativu, papíry“*
K7	*„viz komentář k bodu 6“*
K10	*„administrativní určitě ano, finanční spíše ano“*

***Tabulka P11**: Komentáře k otázce 9*

	Komentáře k otázce 9
K1	*„Zde zatím nemohu odpovědět, jako správce VIS, jsem v přechodném období (12 měsíců),“*

***Tabulka P12**: Komentáře k otázce 10*

	Komentáře k otázce 10
K1	*„jako podklad byla použita norma ISO 27001“*
K2	*„resp. byly snaha, ZoKB v tomto směru zafungoval jako spouštěč připravených opatření“*
K3	*„podle ISO 27000, bez certifikace“*
K4	*„částečně analýza rizik dle ISO 27000“*
K5	*„ISO/IEC 27001“*
K7	*„ISO/IEC 27001“*
K8	*„Snažili jsme se držet doporučení aktuálně platných norem, (.., 27k.), ale pouze tam, kde to pro nás mělo smysl. Nikdy jsme neusilovali o atestaci.“*
K9	*„27001“*

***Tabulka P13**: Komentáře k otázce 11*

	Komentáře k otázce 11
K2	*„spíše ne“*

Otázka 12 je otevřená, odpovědi jsou uvedené v D.2.

***Tabulka P14**: Komentáře k otázce 13*

	Komentáře k otázce 13
K1	*„ani útvar, ani oddělení, tuto činnost zatím zabezpečuje jeden člověk“*
K2	*„ano, bezpečnostní ředitel / manažer KB – jedna osoba; vedoucí informatiky – jedna osoba; plánujeme zřízení třetí pozice – bezpečnostní správce“*

Otázka 14 je otevřená, odpovědi jsou uvedené v D.2.

***Tabulka P15**: Komentáře k otázce 15*

	Komentáře k otázce 15
K2	*„viz výše“*
K3	*„odbor informatiky“*
K7	*„v odboru bezpečnosti“*
K10	*„Odbor analýz a podpory řízení“*

***Tabulka P16**: Komentáře k otázce 16*

	Komentáře k otázce 16
K1	*„Zatím nedokážeme odpovědět, z hlediska organizace a budoucích služeb, by to bylo vhodné, možná se otvírá varianta využití služby třetí stran (outsourcing)“*
K2	*„v budoucnu se předpokládá oddělení role bezpečnostního ředitele (ISMS) od manažera kybernetické bezpečnosti v okamžiku, kdy agenda bude vyžadovat celý úvazek“*
K3	*„v jednání“*
K4	*„pouze změna pracovní náplně stávajících zaměstnanců“*
K7	*„v roce 2014 vzniklo bezpečnostní oddělení na odboru informatiky (v souladu s bodem 15), toto oddělení bylo ale paradoxně v r. 2015 zrušeno bez náhrady“*
K8	*„Vedení se domnívá, že se to týká informatiky a že to zvládne jeden pracovník při vykonávání svých stávajících povinností.“*
K10	*„Zvyšování počtu zaměstnanců obecně ve státní správě není úplně populární, proto nelze předpokládat, že by se zvýšil počet zaměstnanců zabývající se bezpečností.“*

K otázce 17 žádný z respondentů neuvedl komentář.

***Tabulka P17**: Komentáře k otázce 18*

	Komentáře k otázce 18
K2	*„aktuálně probíhá implementace těchto rolí v souladu s tím, jak jsou novelizovány vnitřní předpisy úřadu“*
K3	*„v jednání“*
K4	*„možná bude řešeno formou služeb, outsourcingu“*
K10	*„plánujeme zavedení všech rolí (navíc tam máme technického správce aktiva)“*

***Tabulka P18**: Komentáře k otázce 19*

	Komentáře k otázce 19
K2	*„činnosti související s provozem vlastními silami, audit externě (např. penetrační testy apod.)“*
K3	*„v jednání, příprava veřejné zakázky“*
K10	*„částečně nám pomáhá (formou poradenství) externí pracovník“*

***Tabulka P19**: Komentáře k otázce 20*

	Komentáře k otázce 20
K1	*„ano, může to být je jedna z variant (na základě ekonomické analýzy)“*
K10	*„V našem případě určitě ano (jelikož se jedná o formu poradenství)“*

Otázka 21 je otevřená, odpovědi jsou uvedené v D.2.

Příloha E: Významné informační systémy krajů

V této příloze jsou uvedeny významné informační systémy, které krajské úřady navrhovaly formou připomínek k novelizaci vyhlášky 317/2014 Sb. v průběhu 25.1.2016 – 22.2.2016. Zdroj: Aplikace o/dok VeKLEP, Vláda ČR[106].

Tato data nebyla získána dotazníkovým šetřením, ale z veřejného zdroje, proto údaje nejsou anonymizovány.

Královéhradecký kraj

- Spisová služba EZOP,
- Ekonomický informační systém

Ústecký kraj

- Ekonomický systém Navision,
- Spisová a archivní služba EZOP,
- Internetový portál Ústeckého kraje VISMO,
- Poštovní server Microsoft Exchange.

Olomoucký kraj

- ERP – Ekonomický systém,
- Spisová služba (SSL),
- Integrační směrnice (ISb),
- Webový portál (WP),
- Elektronický poštovní systém (EPS).

Pardubický kraj

- Integrovaný informační systém GINIS

Kraj Vysočina

- Webový portál (VISMO),
- Elektronický poštovní systém,

[106] Dostupné z: https://apps.odok.cz/veklep-detail?p_p_id=material_WAR_odokkpl&p_p_lifecycle=0&p_p_state=normal&p_p_mode=view&p_p_col_id=column-1&p_p_col_count=3&_material_WAR_odokkpl_pid=RACKA66GM6F2&tab=remarks

- GINIS - Spisová služba,
- GINIS - Ekonomické moduly.

Jihočeský kraj

- ekonomický systém,
- spisová služba,
- firemní e-mailová komunikace (elektronický poštovní systém),
- webový portál (webové stránky kraje).

Plzeňský kraj

- Mailový server - Systém pro příjem a odesílání elektronické pošty v rámci komunikace krajského úřadu,
- Integrační sběrnice - Komunikační systém, zpracovává a zajišťuje komunikaci mezi interními systémy a externím systémem - základní registry,
- Spisová služba - evidence dokumentů a spisová služba,
- Webový portál kraje - Systém pro webový portál a komunikací s veřejností v rámci webového portálu,
- ERP - Ekonomický informační systém pro evidenci majetku, vedení účetnictví, tvorba rozpočtu.

Karlovarský kraj

- Ekonomický systém a spisová služba,
- Webové stránky kraje,
- Elektronický poštovní systém.