IV.

I. OBECNÁ ČÁST

SHRNUTÍ ZÁVĚREČNÉ ZPRÁVY RIA

1. Základní identifikační údaje

<table>
<tr><td colspan="2">Název návrhu zákona: Návrh zákona, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.</td></tr>
<tr><td>Zpracovatel / zástupce předkladatele:
Národní bezpečnostní úřad</td><td>Předpokládaný termín nabytí účinnosti,
1. dnem druhého kalendářního měsíce po vyhlášení ve Sbírce zákonů</td></tr>
<tr><td colspan="2">Implementace práva EU: ANO
- uveďte termín stanovený pro implementaci: květen 2018
- uveďte, zda jde návrh nad rámec požadavků stanovených předpisem EU: ANO</td></tr>
<tr><td colspan="2">2. Cíl návrhu zákona</td></tr>
<tr><td colspan="2">Hlavním cílem návrhu zákona je provedení věcných změn na základě transpozice směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. Zároveň jsou návrhem zákona odstraněny některé nedostatky stávající právní úpravy kybernetické bezpečnosti.</td></tr>
<tr><td colspan="2">3. Agregované dopady návrhu zákona</td></tr>
<tr><td colspan="2">3.1 Dopady na státní rozpočet a ostatní veřejné rozpočty:
ANO</td></tr>
<tr><td colspan="2">3.2 Dopady na podnikatelské subjekty:
ANO</td></tr>
<tr><td colspan="2">3.3 Dopady na územní samosprávné celky (obce, kraje)
ANO</td></tr>
<tr><td colspan="2">3.4 Sociální dopady: NE</td></tr>
<tr><td colspan="2">3.5 Dopady na životní prostředí: NE</td></tr>
</table>

Závěrečná zpráva o hodnocení dopadů regulace

1. Důvod předložení a cíle

Směrnice Evropského parlamentu a Rady 2016/xy/EU ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (dále jen „směrnice“) musí být v souladu s právem Evropské unie zapracována do českého právního řádu ve stanovené transpoziční lhůtě, která činí 21 měsíců od nabytí platnosti této směrnice. Zároveň předložený návrh zákona reflektuje připomínky z praktické aplikace již účinného zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

Cílem směrnice je dosáhnout vysoké společné úrovně bezpečnosti sítí a informačních systémů, což v praxi znamená zvýšení bezpečnosti sítí a informačních systémů, na nichž je do značné míry postaveno fungování naší společnosti a hospodářství. Za tímto účelem je od členských států požadováno, aby zlepšily svou připravenost a vzájemnou spolupráci, a od provozovatelů základních služeb v uvedených oblastech (např. energetika a doprava), klíčových poskytovatelů digitálních služeb (platforem pro elektronické obchodování, vyhledávačů apod.), jakož i od orgánů veřejné správy, aby podnikli odpovídající kroky v zájmu řízení bezpečnostních rizik a oznamování případů závažných narušení bezpečnosti vnitrostátním příslušným orgánům.

1.1 Název

Návrh zákona, kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

1.2 Definice problému

Výrazný nárůst používání informačních technologií v současném světě vede na jedné straně k vytvoření informační společnosti, urychlení komunikace a velkému rozvoji služeb a tím celé společnosti. Závislost společnosti a jejího fungování na informačních technologiích rapidně narůstá, a to ve všech oblastech (nejedná se tedy pouze o služby informační společnosti, jako je internetový obchod, ale i o fungování informačních systémů, na jejichž správné funkci je závislá celá řada základních služeb jako například řízení dopravy, přenos energií, výkon veřejné moci apod.). Nejenom ekonomické aktivity se však přesouvají do kybernetického prostoru. Vznikem sociálních, herních a zájmových sítí se z nejznámější části kybernetického prostoru, z internetu, stává významný celospolečenský jev, jehož prostřednictvím lze společnost výrazně pozitivně nebo i negativně ovlivňovat.[1]

[1] Podle Akčního plánu pro rozvoj digitálního trhu česká internetová populace dnes čítá více než 6,8 mil. osob. Dopad internetové ekonomiky, tedy činností přímo spojených s internetem, odpovídá zhruba 3 % HDP. Je však nutné uvést, že digitální technologie mají velmi průřezový charakter a ovlivňují tím celou řadu dalších odvětví. Pokud vezmeme v potaz toto komplexní pojetí, odhaduje se, že fenomén internetu se do HDP promítá téměř 10 %.

Je však nutno si uvědomit, že se vzrůstající závislostí společnosti na informačních technologiích vzrůstá i riziko zneužívání těchto technologií nebo útoků, které mají rozsáhlé dopady a významně tak ovlivní činnost subjektů, které s nimi pracují.

Bezpečnost sítí a informačních systémů je tak důležitým předpokladem pro ekonomiku i společnost, stejně jako pro vytvoření spolehlivého prostředí pro celosvětový obchod se službami. Informační systémy a jejich bezpečnost však mohou být narušeny mnoha různými vlivy, které nemusí být pouze technické povahy, ale mohou vzniknout i lidskou chybou nebo úmyslným útokem. Tyto incidenty představují v současné době čím dál tím větší a komplexnější riziko. Z internetové veřejné konzultace na téma „Zvyšování bezpečnosti sítí a informací v EU“ [2], kterou provedla Evropská komise v roce 2012, vyplynulo, že 57 % respondentů mělo v roce 2011 zkušenost s narušením bezpečnosti, které mělo vážný dopad na jejich činnost. Nedostatečná bezpečnost sítí a informačních systémů, potažmo informací, přitom může ohrozit zcela zásadní služby, jež jsou závislé na jejich integritě. V důsledku pak mohou podniky přestat fungovat, může dojít ke značným finančním ztrátám v ekonomice členských států, potažmo EU a k nepříznivým dopadům na fungování společnosti. Bezpečnost kybernetického prostoru každé země se tak stává mimo jiné hodnotícím kritériem i pro potencionální investory a významně ovlivňuje konkurenceschopnost dané země.

Obecným trendem v celém světě je tak kvalitní ochrana informačních technologií před zásahy, které mohou ohrozit jejich chod. Cílené útoky proti informačním technologiím jsou celosvětovým fenoménem a jejich dopad může způsobit vedle rozsáhlých ekonomických škod ve veřejném i v soukromém sektoru i negativní politické důsledky, a to jak v národním měřítku, tak v měřítku globálním. V případech, ve kterých je útok veden proti prvkům kritické infrastruktury (např. energetické systémy, produktovody, zdravotnické informační systémy a informační systém veřejné správy) nebo základním službám, může být v konečném důsledku ohrožena dokonce bezpečnost nebo základní hodnoty, na kterých je postaveno fungování právního státu. Takové útoky jsou navíc stále komplexnější a sofistikovanější a povaha těchto útoků je přitom silně diferencovaná. Může se jednat o útoky motivované kriminálními, politickými, ekonomickými nebo teroristickými zájmy. Mohou však být organizovány a sponzorovány jednotlivými státy (např. malware Stuxnet nebo útoky na Estonsko v roce 2007). Zároveň však mohou vzniknout následkem lidského selhání a chyb.

V době, v níž se stále větší část ekonomické aktivity přesouvá do prostředí internetu a roste procento hrubého domácího produktu, které je závislé na správném fungování technologií, lze konstatovat, že investice do kybernetické bezpečnosti je adekvátním a odůvodněným nákladem pro prevenci, resp. snížení rizika častých a rozsáhlých útoků a incidentů výrazně oslabujících či negujících ekonomické, politické, kulturní a další přínosy rozvoje elektronické sféry.

S ohledem na fakt, že kybernetický prostor nezná hranic a není tedy otázkou teritoriální, je navíc nutné útoky na informační technologie řešit i z pohledu mezinárodního společenství. Informační systémy jsou často propojené napříč státy a bez mezinárodní spolupráce není tudíž možno v kyberprostoru dosáhnout uspokojivých výsledků. Tato spolupráce doposud fungovala na dobrovolné úrovni na základě dlouhodobě budovaných partnerství mezi jednotlivými vnitrostátními orgány a organizacemi. V důsledku však mnohdy bývají z této spolupráce právě vyloučeni partneři,

[2] Internetová veřejná konzultace s názvem „Zvyšování bezpečnosti sítí a informací v EU“ proběhla od 23. července do 15. října 2012.

jejichž úroveň technologického a personálního vybavení zaostává. Takový postup však často znamená, že nedochází ke kýženému sdílení informací, což v konečném důsledku může snížit bezpečnost kyberprostoru jako takového, protože nezvládnutý incident v jeho jedné části může fatálně ovlivnit subjekty nacházející se i na druhé straně světa.

Vezmeme-li v úvahu užší perspektivu Evropské unie (dále také „EU"), hrají informační a komunikační technologie (dále také „ICT") zásadní roli při usnadňování přeshraničního pohybu zboží, služeb a osob, čímž se stávají klíčovým prvkem pro fungování vnitřního trhu EU. Výrazné narušení těchto systémů v jednom státě se může dotknout dalších států i EU jako celku. Odolnost a stabilita sítí a informačních systémů je proto základním předpokladem pro dokončení jednotného digitálního trhu a pro hladké fungování vnitřního trhu. Pravděpodobnost a četnost výskytu bezpečnostních incidentů a nemožnost zajistit účinnou ochranu rovněž podrývají důvěru veřejnosti v ICT. Například průzkum Eurobarometr o kybernetické bezpečnosti v roce 2012 zjistil, že 38 % uživatelů internetu v EU se obává, že online platby nejsou bezpečné, a kvůli obavám týkajícím se bezpečnosti změnili své chování. 18 % z nich dokonce uvedlo, že si kvůli tomu pravděpodobně nekoupí žádné zboží online a 15 % spíše nepoužije internetové bankovnictví[3].

Snaha o řešení této problematiky se pak projevila zejména vypracováním Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor. Současně s tímto dokumentem Evropská komise (dále také „Komise") předložila dne 7. února 2013 návrh směrnice, přičemž tato směrnice byla oficiálně schválena dne 6. července 2016, tj. téměř dva a půl roku od jejího představení.

Komise však nastínila rostoucí důležitost bezpečnosti sítí a informací už v roce 2001 ve svém sdělení Bezpečnost sítí a informací – návrh evropského politického přístupu[4]. Po něm následovalo v roce 2006 přijetí strategie pro bezpečnou informační společnost[5], jejímž cílem bylo vytvořit v Evropě kulturu bezpečnosti sítí a informací. Její hlavní body byly potvrzeny usnesením Rady[6].

Komise dále dne 30. března 2009 vydala sdělení o ochraně kritické informační infrastruktury (CIIP)[7], v němž se zaměřila na ochranu Evropy před narušením kybernetického prostoru a posílení bezpečnosti. V rámci tohoto sdělení byl vyhlášen akční plán na podporu snah členských států zajistit ochranu a odpovídající reakci, který byl poté zakotven v závěrech předsednictví z ministerské konference o ochraně kritické informační infrastruktury CIIP v Tallinnu v roce 2009. Dne 18. prosince 2009 pak Rada přijala usnesení o společném evropském přístupu k bezpečnosti sítí a informací[8].

Digitální agenda pro Evropu[9], přijatá v květnu 2010, a související závěry Rady[10] zdůraznily společné přesvědčení, že důvěra a bezpečnost jsou základními podmínkami pro široké rozšíření informačních

[3] Eurobarometr 390/2012.
[4] KOM(2001) 298.
[5] KOM(2006) 251 http://eur-lex.europa.eu/LexUriServ/site/cs/com/2006/com2006_0251cs01.pdf.
[6] 2007/068/01.
[7] KOM(2009) 149.
[8] 2009/C 321/01.
[9] KOM(2010) 245.
[10] KOM(2010) 2020 a závěry Evropské rady ze dne 25.–26. března 2010 (EUCO 7/10).

a komunikačních technologií, a tím i pro dosažení cílů strategie Evropa 2020 a jejího rozměru spočívajícího v „inteligentním růstu“[11]. V kapitole Digitální agendy pro Evropu nazvané „Důvěra a bezpečnost“ se zdůrazňuje, že je třeba, aby všechny zainteresované strany spojily své síly a uceleným způsobem se pomocí prevence, připravenosti a informovanosti snažily zajistit bezpečnost a odolnost infrastruktury ICT a rovněž aby vytvořily účinné a koordinovaně fungující bezpečnostní mechanismy. Zejména pak klíčové opatření č. 6 Digitální agendy pro Evropu vyzývá k opatřením zaměřeným na posílení a zajištění vysoké úrovně politiky bezpečnosti sítí a informací.

Ve svém sdělení o CIIP z března 2011 nazvaném „Dosažené výsledky a další kroky – směrem ke globální kybernetické bezpečnosti“[12] Komise bilancuje, čeho bylo od vyhlášení akčního plánu o CIIP v roce 2009 dosaženo, a dochází k závěru, že realizace plánu ukázala, že řešení otázky bezpečnosti a odolnosti na čistě vnitrostátní úrovni je nedostačující a že Evropa by měla ve svém úsilí vybudovat jednotný a společný celounijní přístup pokračovat. V rámci sdělení o CIIP z roku 2011 byla ohlášena řada opatření a Komise vyzvala členské státy, aby zřídily kapacity pro zajišťování bezpečnosti sítí a informací a přeshraniční spolupráci.

Rada Evropské unie ve svých závěrech o CIIP ze dne 27. května 2011 zdůraznila naléhavou potřebu zajistit bezpečnost ICT systémů a sítí a jejich odolnost proti jakýmkoliv možným narušením, ať už náhodným nebo úmyslným, vybudovat v celé EU kapacity zajišťující připravenost, bezpečnost a odolnost, zdokonalit technickou způsobilost, s níž by se Evropa zhostila úkolu ochrany sítí a informační infrastruktury, a upevnit spolupráci členských států pomocí mechanismů spolupráce členských států v případech narušení bezpečnosti.

Internetová veřejná konzultace s názvem „Zvyšování bezpečnosti sítí a informací v EU“ z roku 2012 ukázala, že zainteresované strany obecně souhlasí s potřebou zvýšit bezpečnost sítí a informací v EU. Například: 82,2 % respondentů bylo toho názoru, že vlády v EU by měly pro zajištění vysokého stupně bezpečnosti sítí a informací dělat více; 82,2 % se domnívalo, že uživatelé informačních systémů si nejsou vědomi existujících bezpečnostních hrozeb a narušení bezpečnosti sítí a informací; 66,3 % by v zásadě souhlasilo se zavedením zákonné povinnosti řízení rizik v oblasti bezpečnosti sítí a informací a 84,8 % uvedlo, že by takové povinnosti měly být stanoveny na úrovni EU. Velká část respondentů se domnívala, že povinnosti týkající se bezpečnosti sítí a informací by měly být zavedeny zejména v těchto odvětvích: bankovnictví a finance (91,1 %), energetika (89,4 %), doprava (81,7 %), zdravotnictví (89,4 %), internetové služby (89,1 %) a veřejná správa (87,5 %). Respondenti se rovněž domnívali, že pokud by byla zavedena povinnost oznamovat porušení bezpečnosti sítí a informací odpovědnému vnitrostátnímu orgánu, měla by být stanovena na úrovni EU (65,1 %), a potvrdili, že by se měla vztahovat i na orgány veřejné správy (93,5 %). Respondenti konečně také uvedli, že povinné zavedení řízení rizik v oblasti bezpečnosti sítí a informací podle nejmodernějších standardů by pro ně nepředstavovalo významné dodatečné náklady (63,4 %) a že významné dodatečné náklady by neznamenala ani povinnost oznamovat případy porušení bezpečnosti (72,3 %).

Další průzkum Eurobarometr o kybernetické bezpečnosti z roku 2015[13] ukázal, že internetoví uživatelé mají stále obavy z kybernetické trestné činnosti.

[11] Závěry Rady ze dne 31. května 2010 o Digitální agendě pro Evropu (10130/10).
[12] KOM(2011) 163.
[13] Eurobarometr 423/2015.

Nejnovějším strategickým dokumentem, který se kybernetickou bezpečností na úrovni EU rozsáhleji zaobíral, byla Strategie pro jednotný digitální trh v Evropě[14], která uvádí, že právě přijetí směrnice bude významným krokem vpřed. V rychle se vyvíjející oblasti technologií a řešení zaměřených na bezpečnost on-line sítí stále přetrvávají specifické nedostatky. K tomu, aby průmysl v EU zvýšil úsilí při zajišťování bezpečnějších řešení a aby tato řešení přejali občasné, orgány veřejné moci i podniky, je třeba přijmout ucelenější přístup. Podle této strategie pouze 22 % Evropanů má plnou důvěru ke společnostem, jako jsou vyhledávače, sociální sítě a e-mailové služby, a 72 % uživatelů internetu vyjadřuje znepokojení nad tím, že je od nich on-line požadováno příliš mnoho osobních údajů. Komise si tak v tomto dokumentu stanovila za cíl iniciovat v první polovině roku 2016 vytvoření partnerství veřejného a soukromého sektoru pro kybernetickou bezpečnost v oblasti technologií a řešení pro on-line bezpečnost sítí. Dalšími klíčovou oblastí je pak rozvoj průmyslových a technologických zdrojů pro kybernetickou bezpečnost.

Pracovní dokument k této strategii[15] navíc uvádí, že celkové finanční škody vniklé následkem kybernetických útoků jsou odhadovány v řádu stovek až tisíců miliard dolarů v celosvětovém měřítku, přičemž lze sledovat výraznou tendenci v nárůstu počtu těchto incidentů a rozšiřování jejich rozsahu, tím pádem i vzniklých škod.

Navíc je nutno zmínit, že společnosti se ne vždy mohou z následků kybernetických bezpečnostních incidentů vzpamatovat. Mnohdy totiž tyto incidenty napáchají takové škody na jejich službách a pověsti, že jsou pro ně v podstatě likvidační, zejména pokud se jedná o firmy, kde je bezpečnost a důvěrnost dat základním předpokladem pro jejich podnikání. Například průzkum mezi generálními řediteli[16] provedený společností PricewaterhouseCoopers v roce 2015 ukázal, že 61 % z nich považuje kybernetické hrozby za riziko pro rozvoj jejich společností.

V rámci celoevropské regulace tohoto fenoménu byl tak postupně vyvíjen tlak, aby problematika ochrany kybernetického prostoru byla řešena formou závazné právní regulace. Narůstající potřebu zajištění ochrany kybernetického prostoru reflektovala EU naplno v červenci 2012, kdy Komise zahájila veřejné konzultace k záměru legislativně upravit otázku kybernetické bezpečnosti v EU.

Vyústěním všech těchto inciativ bylo předložení návrhu výše uvedené směrnice, jejímž cílem je vytvořit harmonizované podmínky pro efektivní spolupráci a spolehlivé sdílení informací mezi členskými státy, na základě kterých by mohly být i dobrovolně koordinovány regulatorní zásahy. Na vyšší úrovni má samozřejmě směrnice za cíl zavést povinnost vytvořit potřebné strategické dokumenty, vytvořit na vnitrostátní úrovni příslušné organizační struktury a nastavit rámec pro ukládání povinností, které budou muset být plněny ze strany subjektů spadajících do působnosti směrnice.

Konkrétně musí každý členský stát podle této směrnice přijmout národní strategii pro bezpečnost sítí a informačních systémů, jmenovat vnitrostátní příslušný orgán, popřípadě orgány odpovědné za bezpečnost sítí a informačních systémů a zřídit bezpečnostní tým nebo týmy typu CSIRT (Computer

[14] COM(2015) 192 final.
[15] SWD(2015) 100 final.
[16] PwC, 18th Annual Global CEO Survey, 2015.

Security Incident Response Team), respektive CERT (Computer Emergency Response Team). Směrnice dále požaduje, aby vnitrostátní příslušné orgány spolupracovaly v rámci kooperačních struktur umožňujících bezpečnou a efektivní spolupráci včetně dobrovolné výměny informací a počítá s ukládáním povinností subjektům regulace, kterými jsou provozovatelé základních služeb a poskytovatelé digitálních služeb. Tyto subjekty budou povinny přijmout vhodná technická a organizační opatření k řízení bezpečnosti rizik jejich sítí a informačních systémů. Tato opatření by přitom měla vycházet z mezinárodních nebo evropských norem, respektive specifikací týkajících se bezpečnosti sítí a informačních systémů, přičemž doporučení a pokyny týkající se technických oblastí, které by měly být v těchto normách zohledněny, budou vypracovány Evropskou agenturou pro bezpečnost sítí a informací (dále také „ENISA“) ve spolupráci s členskými státy. Regulované subjekty budou zároveň povinny oznamovat příslušnému orgánu incidenty, které budou mít významný dopad na kontinuitu jimi poskytovaných služeb. Vnitrostátní příslušný orgán by pak měl disponovat prováděcími a donucovacími pravomocemi spočívajícími zejména v oprávnění vydávat závazné pokyny těmto subjektům a v oprávnění požadovat od těchto subjektů informace potřebné k posouzení bezpečnosti jejich sítí a informačních systémů.

Je nutno zdůraznit, že Česká republika (dále také „ČR“) v tomto ohledu nezaostává za ostatními členskými státy a v oblasti kybernetické bezpečnosti patří mezi pokrokové státy s vypracovaným systémem ochrany kritické informační infrastruktury a dalších významných informačních systémů veřejné správy. Již v roce 2011 bylo na základě usnesení vlády č. 781 ze dne 19. října 2011 zřízeno Národní centrum kybernetické bezpečnosti jako organizační součást Národního bezpečnostního úřadu (dále také „NBÚ“). Předmětné usnesení vlády uložilo řediteli NBÚ vybudovat do konce roku 2015 nejen plně funkční Národní centrum kybernetické bezpečnosti, ale i vládní koordinační místo pro okamžitou reakci na počítačové incidenty (dále také „vládní CERT“), který je součástí Národního centra kybernetické bezpečnosti, tj. součástí NBÚ. Navíc Česká republika plní již nyní velkou část závazků vyplývajících ze směrnice, protože dne 1. ledna 2015 nabyl účinnosti zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), který do značné míry vyhovuje požadavkům této regulace.

1.3 Popis existujícího právního stavu v oblasti kybernetické bezpečnosti

V současné době je problematika kybernetické bezpečnosti již v ČR specificky řešena zákonem o kybernetické bezpečnosti. Dílčí aspekty ochrany ČR před kybernetickými útoky jsou však předmětem i jiných právních předpisů, usnesení vlády a nadnárodních koncepčních dokumentů. Zároveň není možno tuto problematiku koncepčně vyjmout ze širších souvislostí, které zahrnují bezpečnost ČR jako takovou, digitální agendu i ochranu soukromí jednotlivců. Kybernetická bezpečnost se tedy vztahuje zejména k těmto právním předpisům a dokumentům:

1.3.1 Ústavní pořádek ČR

- Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů,

- Listina základních práv a svobod, ve znění ústavního zákona č. 162/1998 Sb.,

- Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.

1.3.2 Zákony

- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů,

- Zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů, ve znění pozdějších předpisů,

- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů,

- Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů,

- Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů,

- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,

- Zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů,

- Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů,

- Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů,

- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim,

- Zákon č. 106/1999 Sb. o svobodném přístupu k informacím, ve znění pozdějších předpisů,

- Zákon č. 231/2001 Sb. o provozování rozhlasového a televizního vysílání a o změně dalších zákonů, ve znění pozdějších předpisů.

1.3.3 Prováděcí předpisy

- 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 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb.,

- Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznamy utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb.,

- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění nařízení vlády č. 315/2014 Sb.,

- Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb.,

- 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. 242/2012 Sb., o stanovení rozsahu a formy předávané informace o narušení bezpečnosti a ztrátě integrity sítě,

- Vyhláška č. 241/2012 Sb., o stanovení náležitostí technicko-organizačních pravidel k zabezpečení bezpečnosti a integrity veřejné komunikační sítě a interoperability veřejně dostupných služeb elektronických komunikací za krizových stavů.

1.3.4 Usnesení vlády

- 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,

- Usnesení vlády České republiky ze dne 30. května 2012 č. 382 k návrhu věcného záměru zákona o kybernetické bezpečnosti,

- Usnesení vlády České republiky ze dne 16. února 2015 č. 105 k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020,

- Usnesení vlády České republiky ze dne 25. května 2015 č. 382 k Akčnímu plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020,

- Usnesení vlády ze dne 26. srpna 2015 č. 694 k Akčnímu plánu pro rozvoj digitálních služeb.

1.3.5 Primární právo EU

- Listina základních práv Evropské unie,
- Smlouva o fungování Evropské unie.

1.3.6 Právní předpisy EU

- Směrnice Evropského parlamentu a Rady 2014/61/ES ze dne 15. května 2014 o opatřeních ke snížení nákladů na budování vysokorychlostních sítí elektronických komunikací,

- Směrnice Evropského parlamentu a Rady 2002/19/ES ze dne 7. března 2002 o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení (přístupová směrnice), ve znění směrnice 2009/140/ES,

- Směrnice Evropského parlamentu a Rady 2002/20/ES ze dne 7. března 2002 o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice), ve znění směrnice 2009/140/ES,

- Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice), ve znění směrnice 2009/140/ES,

- Směrnice Evropského parlamentu a Rady 2002/22/ES ze dne 7. března 2002 o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací (směrnice o univerzální službě), ve znění směrnice 2009/136/ES,

- Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (směrnice o soukromí v elektronických komunikacích), ve znění směrnice 2009/136/ES,

- Směrnice Evropského parlamentu a Rady 2006/24/ES ze dne 15. března 2006 o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a o změně směrnice 2002/58/ES,

- Směrnice Evropského parlamentu a Rady 1999/5/ES ze dne 9. března 1999 o rádiových a koncových telekomunikačních zařízeních a vzájemném uznávání jejich shody,

- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, ve znění nařízení č. 1007/2008,

- Nařízení Evropského parlamentu a Rady (EU) č. 526/2013 ze dne 21. května 2013 o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004,

- Směrnice Evropského parlamentu a Rady 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES,

- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů),

- Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu,

- Směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV,

- Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV,

- Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při

poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti,

- Směrnice Evropského parlamentu a Rady 2000/31/ES ze dne 8. června 2000 o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu),

- Nařízení Evropského parlamentu a Rady (EU) č. 1077/2011 ze dne 25. října 2011, kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva,

- Rozhodnutí Rady 92/242/EHS ze dne 31. března 1992 o bezpečnosti informačních systémů,

- Rámcové rozhodnutí Rady 2002/465/JHA o společných vyšetřovacích týmech,

- Závěry Rady 2009/C 62/05 ze dne 27. listopadu 2008 o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti.

1.3.7 Další dokumenty EU a mezinárodní dokumenty

- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o vytvoření bezpečnější informační společnosti zdokonalením bezpečnosti informační infrastruktury a bojem proti počítačovým trestným činům (KOM/2000/890),

- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o bezpečnost sítí a informací – návrh evropského postoje (KOM/2001/298),

- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Strategie pro bezpečnou informační společnost – „Dialog, partnerství a posílení účasti“ (KOM/2006/251),

- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o ochraně kritické informační infrastruktury - „Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“ (KOM/2009/149),

- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Digitální agenda pro Evropu (KOM/2010/245),

- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Strategie vnitřní bezpečnosti Evropské unie: pět kroků směrem k bezpečnější Evropě (KOM/2010/673),

- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů o ochraně kritické informační infrastruktury – „Dosažené výsledky a další kroky: směrem ke globální kybernetické bezpečnosti“ (KOM/2011/163),

- Společné sdělení Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru

a Výboru regionů Strategie kybernetické bezpečnosti Evropské unie: otevřený, bezpečný a chráněný kyberprostor (JOIN/2013/1),

- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Strategie pro jednotný digitální trh v Evropě (KOM/2015/192),

- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů Posílení evropského systému kybernetické odolnosti a podpora konkurenceschopného a inovativního odvětví kybernetické bezpečnosti (KOM/2016/410),

- Usnesení Rady 2002/C 43/02 ze dne 28. ledna 2002 o společném postoji a specifických činnostech v oblasti bezpečnosti sítí a informací,

- Usnesení Rady 2003/C 48/01 ze dne 18. února 2003 o evropském postoji vůči kultuře bezpečnosti sítí a informací,

- Rámcové rozhodnutí Rady 2005/222/SVV ze dne 24. února 2005 o útocích proti informačním systémům,

- Usnesení Rady 2009/C321/01 ze dne 18. prosince 2009 o společném evropském přístupu k bezpečnosti sítí a informací,

- Akční plán Evropské unie pro boj s terorismem (INI/2004/2214),

- Evropský parlament, Bezpečnost informačních systémů a sítí: Směrem ke kultuře bezpečnosti,

- Úmluva Rady Evropy č. 185 o kybernetické kriminalitě,

- Úmluva Rady Evropy č. 196 o prevenci terorismu,

- Doporučení Parlamentního shromáždění č. 1565 (2007) jak předcházet kybernetické kriminalitě proti státním orgánům v členských a pozorovatelských státech

- Doporučení Rady ministrů CM/Rec(2011)8E ze dne 21. září 2011 o ochraně a podpoře univerzality, integrity a otevřenosti internetu,

- Doporučení Rady ministrů CM/Rec(2008)6E ze dne 26. března 2008 o prostředcích podpory respektu ke svobodě projevu a právu na informace ve vztahu k internetovým filtrům,

- Doporučení Rady ministrů Rec(2001)8E ze dne 5. září 2011 o samoregulaci vzhledem ke kybernetickému obsahu (samoregulace a ochrana uživatele před protiprávním a škodlivým obsahem v nových informačních a komunikačních službách),

- Deklarace Rady ministrů Decl-21.09.2011_2E ze dne 21. září 2011 o principech internet governance,

- Doporučení Rady ministrů Rec(95)13E ze dne 11. září 1995 k problémům trestního práva procesního v souvislosti s informačními technologiemi,

- Deklarace Rady ministrů Decl-28.05.2003E ze dne 28. května 2003 o svobodě komunikace na internetu,

- Doporučení Valného shromáždění 1670 (2004) Internet a právo,

- Deklarace Rady ministrů Decl-07.12.2011_2E ze dne 7. prosince 2011 o ochraně svobody projevu a svobody shromažďování vzhledem k soukromě provozovaným internetovým platformám a poskytovatelům online služeb, OBSE,

- Zpráva zvláštního zpravodaje k otázkám podpory a ochrany práva na svobodu projevu č. A/HRC/17/27, OSN,

- Rozhodnutí Rady ministrů OBSE č. 3/2004 O boji proti používání Internetu pro účely terorismu ze dne 7. prosince 2004,

- Rozhodnutí Rady ministrů OBSE č. 3/2004 O boji proti používání Internetu pro účely terorismu ze dne 7. prosince 2004,

- Doporučení Rady o řízení digitálních bezpečnostních rizik pro hospodářskou a sociální prosperitu, C(2015)115 (OECD),

- Doporučení Rady k ochraně kritické informační infrastruktury, C(2008)35 (OECD),

- Rozhodnutí Stále rady č. 1106 ze dne 3. prosince 2013 o úvodní sadě opatření OBSE pro budování důvěry ke zmírnění rizika konfliktu vycházejícího z využití informačních a komunikačních technologií,

- Rozhodnutí Stále rady č. 1202 ze dne 10. března 2016 o opatřeních OBSE pro budování důvěry ke zmírnění rizika konfliktu vycházejícího z využití informačních a komunikačních technologií,

- Akční plán zemí G8 pro potírání „high-tech" zločinu.

1.3.8 Poziční a koncepční dokumenty veřejné správy ČR

Vzhledem k provázanosti kybernetické bezpečnosti s dalšími otázkami moderní digitální společnosti je potřeba ochrany ČR před kybernetickými útoky řešena i prostřednictvím následujících vládních koncepčních dokumentů, iniciativ soukromého a akademického sektoru a kooperativních aktivit technického charakteru s různou mírou zapojení státu:

1) *Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015* (2011)[17] - navazovala na Bezpečnostní strategii České republiky a definovala záměry ČR v oblasti kybernetické

[17] Usnesení vlády České republiky ze dne 20. července 2011 č. 564 o Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011-2015.

bezpečnosti. Za cíl si tato strategie stanovila především ochranu před hrozbami, kterým jsou informační a komunikační systémy vystaveny, a snížení potenciálních škod způsobených v případě útoků na tyto informační a komunikační systémy. Tohoto cíle mělo být dosaženo prostřednictvím následujících opatření:

I. Vytvoření legislativního rámce,
II. Zajištění posilování kybernetické bezpečnosti kritické infrastruktury a v informačních systémech veřejné správy,
III. Vybudování vládního pracoviště CERT,
IV. Podpora mezinárodní spolupráce v oblasti kybernetické bezpečnosti,
V. Spolupráce státu, soukromé a akademické sféry,
VI. Zvyšování povědomí o kybernetické bezpečnosti.

Současně se strategií byl přijat také Akční plán, který byl rozčleněn do jednotlivých oblastí. Každá oblast obsahovala úkoly k naplňování jednotlivých strategických cílů Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015 do projektů a úkolů orgánů veřejné správy, které jsou věcně v jejich gesci.

2) Přechod gesce nad kybernetickou bezpečností na NBÚ a zřízení Rady pro kybernetickou bezpečnost (2011)[18] - od října 2011 se stal gestorem problematiky kybernetické bezpečnosti a národní autoritou pro tuto oblast NBÚ. Vláda současně NBÚ uložila, aby do roku 2015 zajistil vznik plně funkčního Národního centra kybernetické bezpečnosti a vládního CERT.

Současně s přechodem gesce zaniká Meziresortní rada pro oblast kybernetické bezpečnosti a nově vzniká Rada pro kybernetickou bezpečnost, která je poradním orgánem předsedy vlády pro oblast kybernetické bezpečnosti. Za cíl má také podporu gesční a koordinační role NBÚ v oblasti kybernetické bezpečnosti. Členy rady jsou zástupci příslušných státních institucí, kterými jsou kromě NBÚ Ministerstvo vnitra, Ministerstvo obrany, Ministerstvo zahraničních věcí, Ministerstvo financí, Ministerstvo průmyslu a obchodu, Ministerstvo dopravy, Policie České republiky, Úřad pro zahraniční styky a informace, Bezpečnostní informační služba, Vojenské zpravodajství, Úřad pro ochranu osobních údajů a Český telekomunikační úřad.

3) Schválení *Věcného záměru zákona o kybernetické bezpečnosti* (2012)[19] - NBÚ vypracoval v souladu s úkolem uloženým usnesením vlády ze dne 19. října 2011 č. 781 o ustanovení NBÚ gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast věcný záměr zákona o kybernetické bezpečnosti. Vláda schválila předložený věcný záměr zákona o kybernetické bezpečnosti dne 30. května 2012 a současně uložila řediteli NBÚ zpracovat zákon o kybernetické bezpečnosti a předložit jej vládě do konce července 2013.

4) *Strategie pro oblast kybernetické bezpečnosti České republiky na období 2012 – 2015* (2012)[20] –

[18] 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.
[19] Usnesení vlády České republiky ze dne 30. května 2012 č. 382 o věcném záměru zákona o kybernetické bezpečnosti.
[20] Usnesení vlády České republiky ze dne 23. května 2012 č. 364 o Strategii pro oblast kybernetické bezpečnosti České republiky na období let 2012 až 2015 a Akčním plánu opatření ke Strategii pro oblast kybernetické

tato strategie vznikla na základě úkolu uloženého vládou aktualizovat Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015. Jejím cílem bylo formulovat oblasti, priority a cíle kybernetické bezpečnosti, které je nutné zavést od praxe v období let 2012 – 2015 a vycházela z úsilí vládních i nevládních institucí ke zvyšování kybernetické bezpečnosti. Jí navrhované iniciativy měly zlepšit kybernetickou bezpečnost pro vládní instituce, kritickou infrastrukturu i pro komerční sféru, potažmo i pro občany.

Hlavními prioritními okruhy této strategie byly:

I. Vytvoření legislativního rámce
II. Podpora mezinárodní spolupráce
III. Národní spolupráce (v oblasti veřejné, soukromé a akademické)
IV. Koordinace a řízení rizik kybernetické bezpečnosti ČR
V. Zvyšování povědomí a znalostí o kybernetické bezpečnosti

Z této strategie vycházel *Akční plán opatření ke Strategii pro oblast kybernetické bezpečnosti České republiky na období 2012 – 2015*[21], rozčleněný do pěti oblastí. V každé oblasti byly rozpracovány úkoly k naplňování jednotlivých strategických cílů uvedené strategie do projektů a úkolů orgánů veřejné správy.

5) *Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020* (2015)[22] - tato strategie navazuje na předešlou strategii pro oblast kybernetické bezpečnosti na období 2012 až 2015. Strategie představuje pro ČR zásadní předěl ve vnímání a zajišťování kybernetické bezpečnosti. Konkrétně oproti předešlé strategii pro oblast kybernetické bezpečnosti na období 2012 až 2015 se kvalitativně posunula od budování základních kapacit nezbytných pro zajištění základní míry kybernetické bezpečnosti směrem k jejímu hlubšímu a pokročilému zajišťování.

Obsahově tato strategie představuje ucelený soubor opatření směřujících k dosažení co nejvyšší míry kybernetické bezpečnosti v ČR a za tímto účelem definuje vizi ČR v této oblasti. Zároveň jsou ve strategii stanoveny základní principy, které bude ČR následovat a dodržovat při zajišťování kybernetické bezpečnosti. Strategie také definuje konkrétní výzvy a problémy na poli kybernetické bezpečnosti jak pro ČR, tak i pro mezinárodní prostředí, v jehož rámci se ČR nachází a kterým musí čelit. Stěžejní část strategie pak představují hlavní cíle, kterých bude v následujících pěti letech dosaženo, a které jsou rozděleny do těchto 8 prioritních oblastí:

I. Zajištění efektivity a posilování všech struktur, procesů a spolupráce při zajišťování kybernetické bezpečnosti
II. Aktivní mezinárodní spolupráce
III. Ochrana národní kritické informační infrastruktury a významných informačních systémů

bezpečnosti České republiky na období let 2012 až 2015.

[21] Usnesení vlády České republiky ze dne 23. května 2012 č. 364 o Strategii pro oblast kybernetické bezpečnosti České republiky na období let 2012 až 2015 a Akčním plánu opatření ke Strategii pro oblast kybernetické bezpečnosti České republiky na období let 2012 až 2015.

[22] Usnesení vlády České republiky ze dne 16. února 2015 č. 105 k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020.

IV. Spolupráce se soukromým sektorem
V. Výzkum a vývoj, spotřebitelská důvěra
VI. Podpora vzdělávání, osvěta a rozvoj informační společnosti
VII. Podpora rozvoje schopností Policie České republiky vyšetřovat a postihovat informační kriminalitu
VIII. Právní úprava pro kybernetickou bezpečnost (vytváření právního rámce) a účast na tvorbě a implementaci evropských a mezinárodních pravidel

6) Na strategii navazuje *Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020* (2015)[23], který byl vládou schválen dne 25. května 2015 - tento akční plán definuje na příštích pět let konkrétní kroky k naplnění hlavních cílů národní strategie a stanoví u nich kompetentní orgán a termíny plnění. Akční plán připravil NBÚ ve spolupráci se všemi relevantními partnery. Obsahuje např. činnosti potřebné k zajištění účinnějšího potírání informační kriminality, identifikované ve spolupráci s Ministerstvem vnitra a s policií, úkoly v oblasti mezinárodní spolupráce určené s Ministerstvem zahraničních věcí a v neposlední řadě postup vytváření a následného zajišťování kybernetické obrany České republiky vymezený v součinnosti s Ministerstvem obrany.

7) *Veřejnoprávní smlouva s CZ.NIC* (2015) – na základě této smlouvy, uzavřené mezi NBÚ a sdružením CZ.NIC, provozuje toto sdružení prostřednictvím bezpečnostního týmu CSIRT.CZ národní CERT. Tato smlouva byla uzavřena podle zákona o kybernetické bezpečnosti.

8) Problematika digitální agendy jako takové je komplexně zachycena *Akčním plánem pro rozvoj digitálního trhu* schváleného vládou 26. srpna 2015 (2015)[24], jehož cílem je shrnout na jedno místo směřování vládní politiky a klíčová opatření, která jednotliví gestoři ve státní správě připravují. Tento plán nenahrazuje existující a schválené koncepční dokumenty, nýbrž je zastřešuje, přičemž klade důraz na to, aby státní intervence nebrzdila dynamický vývoj digitálních technologií. Právě naopak zdůrazňuje chytrou regulaci založenou na kvalitních datech a argumentech posuzujících nutnost regulatorních opatření. Součástí tohoto plánu je také závazek intenzivně komunikovat všechna plánovaná opatření se sociálními a hospodářskými partnery, se zákonodárci i s občanskou společností. Plán však zdůrazňuje, že pokud má vláda v tomto snažení uspět, bude pro jakoukoliv další práci stěžejní věnovat digitální agendě adekvátní personální kapacity a finanční zdroje.

Systematika plánu je rozdělena do šesti kapitol, které pokrývají zásadní témata s vazbou na sektor digitální ekonomiky. Patří mezi ně:

I. Infrastruktura v pojetí budování vysokorychlostních internetových sítí a zajištění kybernetické bezpečnosti
II. Digitální vzdělávání a zvyšování digitálních kompetencí u občanů
III. Přístup ke zboží a službám na internetu
IV. Rozvoj elektronické veřejné správy
V. Nové trendy zaměřující se na digitalizaci průmyslu, ekonomiku založenou na datech a přístup k datům veřejného sektoru

[23] Usnesení vlády České republiky ze dne 25. května 2015 č. 382 k Akčnímu plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020.
[24] Usnesení vlády ze dne 26. srpna 2015 č. 694 k Akčnímu plánu pro rozvoj digitálních služeb.

VI. Správa digitální agendy na úrovni vlády a komunikace s veřejností

1.3.9 Zhodnocení současného právního stavu v oblasti kybernetické bezpečnosti v ČR

V rámci ČR existuje již poměrně komplexní právní úprava týkající se kybernetické bezpečnosti, která z velké části odpovídá i požadavkům uvedeným ve směrnici. Touto právní úpravou je zákon o kybernetické bezpečnosti. Vedle něj však existují i dílčí úpravy zaměřující se na specifičtější oblasti. Tyto právní úpravy jsou ve vztahu k zákonu o kybernetické bezpečnosti lex specialis, popřípadě jdou úplně mimo režim zákona o kybernetické bezpečnosti.

Podle současného právního rámce mají povinnost přijmout opatření v oblasti řízení rizik a oznamovat kybernetické bezpečnostní incidenty orgány a osoby uvedené v § 3 písm. c) až e) zákona o kybernetické bezpečnosti; těmi jsou správci informačního nebo komunikačního systému kritické informační infrastruktury a správci významného informačního systému[25]. Zákon o kybernetické bezpečnosti pak do omezené míry ukládá povinnosti i poskytovatelům služby elektronických komunikací a subjektům zajišťujícím síť elektronických komunikací a orgánům nebo osobám zajišťujícím významnou síť.

Zvláštní právní úpravu pak obsahuje zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů, a to v § 98 a 99, které se vztahují na podnikatele zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací. Tyto subjekty mají povinnost zajišťovat bezpečnost a integritu své sítě a bezpečnost služeb, které poskytují. Dále existuje zvláštní právní úprava pro kvalifikované a nekvalifikované poskytovatele služeb vytvářejících důvěru, kteří jsou regulováni podle nařízení eIDAS[26]. Zabezpečení informačních a komunikačních systémů nakládajících s utajovanými informacemi pak upravuje zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

Předkládaný návrh zákona má doplnit především zákon o kybernetické bezpečnosti, a to v souladu s požadavky stanovenými ve směrnici. Novela by tak měla odstranit mezery mezi národní úpravou a požadavky plynoucími z direktivy EU a pod režim zákona o kybernetické bezpečnosti vztáhnout i doposud neregulované subjekty, jejichž ochrana je ve společenském a ekonomickém zájmu. V návaznosti na tento návrh zákona bude nutné i novelizovat prováděcí vyhlášku zákona o kybernetické bezpečnosti a vytvořit novou vyhlášku, která bude uvádět určující kritéria provozovatelů základních služeb, případně základních služeb a informačních systémů základních služeb.

1.4 Identifikace dotčených subjektů

[25] V současné době je v legislativním procesu návrh zákona, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony, který rozšiřuje působnost zákona o kybernetické bezpečnosti na novou kategorii povinných osob – provozovatele informačního nebo komunikačního systému kritické informační infrastruktury a provozovatele významného informačního systému.

[26] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Úř. Věst. L 257, 28. 8. 2014, s. 73).

Zákon o kybernetické bezpečnosti označuje dotčené subjekty jako orgány a osoby v oblasti kybernetické bezpečnosti, které spravují specifické informační a komunikační systémy.

Vzhledem k základním principům této právní úpravy jsou v současné době za standardní situace ukládány konkrétní povinnosti k zavedení bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů a provádění opatření pouze těm subjektům, jejichž systémy, sítě nebo služby mají zásadní až kritický význam pro fungování státu nebo informační společnosti. Pouze při vyhlášení stavu kybernetického nebezpečí se okruh subjektů majících na úseku kybernetické bezpečnosti povinnost provádět opatření rozšiřuje i na ostatní poskytovatele služeb a správce systémů a sítí.

Zákon o kybernetické bezpečnosti částečně přebírá definice z ostatních právních předpisů, a to zejména ze zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Nově jím byly vytvořeny kategorie správců informačních a komunikačních systémů zařazených do kritické informační infrastruktury, správců významných informačních systémů a kategorie subjektů zajišťujících významné sítě. Zákon dále užívá dvou odlišných pojmů, a to služby a sítě elektronických komunikací a komunikační systémy. Pojem služby a sítě elektronických komunikací vychází ze zákona o elektronických komunikacích, zatímco pojem komunikační systémy v sobě zahrnuje jak tyto služby a sítě elektronických komunikací, tak i další, například neveřejné komunikační systémy.

Shora uvedená klasifikace povinných subjektů má kaskádovitý charakter. Typicky tedy např. subjekt zajišťující významnou síť, která bude zařazena do kritické informační infrastruktury, bude mít ve vztahu k této síti na úseku kybernetické bezpečnosti povinnosti odpovídající správci komunikačního systému zařazeného do kritické informační infrastruktury.

Nad rámec této současné úpravy zavádí směrnice dvě kategorie subjektů, kterým budou ukládány povinnosti v oblasti kybernetické bezpečnosti (bezpečnosti sítí a informačních systémů) - provozovatele základní služby a poskytovatele digitální služby. Návrh zákona pak z důvodu praktické aplikace této úpravy a její konzistentnosti se stávajícím režimem zákona o kybernetické bezpečnosti zavádí navíc dvě další kategorie subjektů, na které budou fakticky nejvíce dopadat povinnosti stanovené návrhem zákona, a to správce informačního systému základní služby a provozovatele informačního systému základní služby, pokud jím není správce. Zejména v případě správce informačního systému základní služby je však očekáváno, že bude ve většině případů identický s provozovatelem základní služby. Podle zákonné definice správce informačního systému totiž správce určuje účel zpracování informací a podmínky provozování informačního systému. Provozovatelem základní služby je pak subjekt odpovědný za poskytování základní služby, přičemž v rámci výkonu této odpovědnosti může být rovněž správcem informačního systému základní služby.[27]

[27] Definice provozovatele informačního systému je obsažena v návrhu zákona, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony, přičemž provozovatelem informačního nebo komunikačního systému je orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém.

Pouze v případech, že tomu tak není, a jedná se o dva autonomní subjekty, uvádí zákon o kybernetické bezpečnosti povinnosti i pro provozovatele základních služeb, aby byl zachován smysl a účel směrnice.

Provozovatelem základní služby se podle směrnice rozumí veřejný nebo soukromý subjekt, který ve specifikovaném odvětví poskytuje službu, jež je základní z hlediska zachování činností kritických pro společenské nebo ekonomické činnosti, přičemž poskytování této služby je závislé na sítích a informačních systémech a incident by významně narušil poskytování této služby.

Tito provozovatelé budou určováni členským státem, ve kterém poskytují základní službu, přičemž se předpokládá, že v tom samém státě budou zpravidla i usazeni. V případě možného přeshraničního dopadu bude mít takový členský stát povinnost před určením konzultovat ostatní dotčené členské státy EU. Konkrétní odvětví, v rámci kterých budou provozovatelé základních služeb určováni, uvádí příloha II směrnice. Těmito odvětvími jsou: energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, dodávky a rozvody pitné vody a digitální infrastruktura. Směrnice však ukládá členským státům regulovat provozovatele základní služby podle zásady minimální harmonizace, je tudíž možné, aby členské státy tuto úpravu rozšířili i na další, směrnicí neuváděná odvětví.

Parametry dopadových kritérií pro určení provozovatelů základních služeb jsou stanoveny ve směrnici, přičemž konkretizovány budou v prováděcím právním předpise k zákonu o kybernetické bezpečnosti.

Podle směrnice se jedná o tyto parametry:

- počet uživatelů závislých na službě poskytované daným subjektem;
- závislost dalších odvětví na službě poskytované daným subjektem;
- možný dopad incidentů (intenzita a trvání) na ekonomické nebo společenské činnosti nebo na veřejnou bezpečnost;
- podíl daného subjektu na trhu;
- zeměpisný rozsah oblasti, která by mohla být incidentem dotčena;
- důležitost subjektu, pokud jde o udržování dostatečné úrovně dané služby; s přihlédnutím k dostupnosti alternativních způsobů jejího zajištění;
- případné zvláštní okolnosti podle jednotlivých odvětví.

Kategorie provozovatelů základních služeb se fakticky částečně kryje s již existujícími prvky kritické infrastruktury, resp. kritické informační infrastruktury, které jsou určovány podle zákona o kybernetické bezpečnosti a zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů (krizový zákon), směrnice však zavádí některé nové odvětvové a průřezové parametry pro určovací kritéria. Pro srovnání, průřezová kritéria pro určování prvků kritické infrastruktury podle nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury, ve znění nařízení vlády č. 315/2014 Sb. (dále také „nařízení vlády č. 432/2010 Sb.“), jsou:

a) více než 250 mrtvých nebo 2500 hospitalizovaných po dobu delší než 24 hodin,
b) ekonomický dopad s hospodářskou ztrátou státu vyšší než 0,5% HDP, nebo

c) dopad na veřejnost spočívající v rozsáhlém omezení poskytování nezbytných služeb nebo jiném závažném zásahu do každodenního života více než 125 000 osob.

Je tedy zřejmé, že část subjektů spadajících pod kritéria transponovaná podle směrnice zároveň naplní již existující průřezová kritéria pro určování kritické infrastruktury podle nařízení vlády.

Na druhou stranu nařízení vlády, které je prováděcím právním předpisem krizového zákona, rovněž obsahuje oblastní kritéria, která nejsou směrnicí pokryta (např. veřejná správa nebo potravinářství a zemědělství).

Kritickou infrastrukturou podle krizového zákona se navíc rozumí prvek nebo systém prvků kritické infrastruktury, přičemž narušení jeho funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu. Prvkem kritické infrastruktury je zejména stavba, zařízení, prostředek nebo veřejná infrastruktura, určené podle průřezových a odvětvových kritérií. Směrnice je oproti tomu zaměřena na služby, které jsou buď základní pro společenské nebo ekonomické činnosti, nebo digitální ve smyslu služeb informační společnosti.

Lze tedy vyvodit, že kategorie provozovatelů základních služeb by měla být samostatně regulována, přičemž subjekty naplňující kritéria a definice pro provozovatele základní služby i kritické infastruktury, kteří budou zároveň důležití pro fungování státu jako takového a budou naplňovat kritéria podle nařízení vlády č. 432/2010 Sb., budou regulováni jakožto kritická informační infrastruktura. Ostatní provozovatelé základních služeb, případně správci a provozovatelé informačních systémů základních služeb budou muset splňovat obdobné požadavky jako kritická informační infrastruktura, zároveň však nebudou spadat pod režim krizového zákona, čímž budou vyjmuti z plnění povinností tímto zákonem stanovených.

Jako druhou kategorii povinných osob směrnice zavádí poskytovatele digitálních služeb. Definice digitální služby odpovídá vymezeným službám informační společnosti. Tento termín je v českém právním řádu upravený zákonem č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů, ve znění pozdějších předpisů (zákon o některých službách informační společnosti).

Poskytovatelem digitální služby podle směrnice může být pouze právnická osoba (na rozdíl od poskytovatele služby podle zákona o některých službách informační společnosti, který zahrnuje i osoby fyzické). Dále tento poskytovatel není mikropodnikem či malým podnikem ve smyslu příslušných právních předpisů EU.[28] Navíc jsou poskytovatelé digitálních služeb pro účely směrnice vymezeni pouze ve vztahu ke třem druhům digitálních služeb: online tržištím, internetovým vyhledávačům a službám cloud computingu.

Tyto subjekty nepodléhají procesu určování členským státem. Do regulace tak automaticky spadají všechny subjekty, které naplní výše zmíněná kritéria. ČR bude mít osobní působnost vůči těm subjektům, které jsou usazeny na jejím území nebo je na jejím území usazen jejich (v případě subjektů usazených mimo EU) zástupce určený pro účely plnění povinností podle směrnice.

[28] 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).

Přijatá regulace podléhá tzv. maximální harmonizaci, což znamená, že na rozdíl od úpravy provozovatelů základních služeb Česká republika u poskytovatelů digitálních služeb nesmí přijímat přísnější pravidla, než jaká vyplývají ze směrnice. Komise má navíc ve směrnici stanovené zmocnění k přijímání prováděcích aktů týkajících se bezpečnostních požadavků na poskytovatele digitálních služeb, určení parametrů významnosti dopadů incidentů u poskytovatelů digitálních služeb a formátů a postupů týkajících se požadavků na hlášení incidentů poskytovateli digitálních služeb.

1.5 Popis cílového stavu

Podle důvodové zprávy si směrnice klade za cíl přijmout právní předpisy, které vytvoří rovné podmínky a odstraní současné mezery v legislativě.

Konkrétní cíle směrnice jsou tedy následující:

Zaprvé, směrnice vyžaduje, aby všechny členské státy zajistily alespoň minimální úroveň vnitrostátních kapacit ustavením příslušných orgánů odpovědných na vnitrostátní úrovni za bezpečnost sítí a informačních systémů, zřízením bezpečnostních týmů typu CSIRT (dále také „týmy CSIRT“) a přijetím národní strategie bezpečnosti sítí a informačních systémů. V tomto ohledu má ČR již ze značné části povinnosti stanovené touto směrnicí transponovány. Zákon o kybernetické bezpečnosti totiž v § 22 odst. 1 uvádí, že státní správu v oblasti kybernetické bezpečnosti vykonává NBÚ. Rovněž tento zákon zřizuje i dvě dohledová pracoviště CERT, která již v současné době z velké míry splňují parametry pro bezpečnostní týmy typu CSIRT podle přílohy I směrnice.

Zadruhé, členské státy, respektive jejich vnitrostátní příslušné orgány a týmy CSIRT, by měly spolupracovat v rámci kooperačních struktur zřízených na úrovni EU umožňujících bezpečnou a efektivní spolupráci včetně dobrovolné výměny informací. Těmito strukturami jsou skupina pro spolupráci zajišťující koordinaci členských států na strategické úrovni a síť CSIRT, která představuje platformu pro dobrovolnou výměnu informací mezi týmy CSIRT jednotlivých členských států a která může v případě kybernetického bezpečnostního incidentu sloužit i jako platforma pro koordinovanou reakci.

Zatřetí, po vzoru rámcové směrnice 2002/21/ES je účelem této směrnice zajistit rozvoj kultury řízení rizik a sdílení informací mezi soukromým a veřejným sektorem. Podniky z konkrétních klíčových odvětví a orgány veřejné správy budou mít povinnost posuzovat rizika, jimž čelí, a přijímat odpovídající a přiměřená opatření k zajištění bezpečnosti sítí a informačních systémů. Tyto subjekty budou vnitrostátním příslušným orgánům povinně podávat zprávy o všech incidentech vážně ohrožujících jejich sítě a informační systémy a majících významný dopad na kontinuitu základních služeb, které poskytují.

Jak již bylo vysvětleno výše, směrnice zavádí dvě kategorie subjektů, kterým budou ukládány povinnosti v oblasti kybernetické bezpečnosti, přičemž specifikuje odvětví, kterých se směrnice týká. Zároveň stanoví obecné parametry pro identifikaci takových subjektů, pro bezpečnostní opatření, která budou subjekty muset přijmout, a pro kategorie incidentů, které budou subjekty povinny hlásit. Dále směrnice ukládá členským státům povinnost přijmout strategii (vnitrostátní rámec) pro

bezpečnost sítí a informačních systémů a upravuje povinnosti členských států v oblasti spolupráce s orgány Unie i mezi sebou navzájem.

Obecně směrnice stanoví povinnosti členských států na nejnižší možné úrovni nezbytné k dosažení odpovídající připravenosti a k zajištění spolupráce založené na důvěře. Kromě toho tak členské státy mohou řádně zohlednit svá vnitrostátní specifika. Směrnice tedy nevylučuje možnost členských států nastavit si plnění jednotlivých povinností na ještě přísnější úrovni. Jejím cílem totiž není unifikace, nýbrž harmonizace jednotlivých právních řádů. Členské státy tak mají prostor pro rozšíření požadované regulace, popřípadě zvýšení požadovaných bezpečnostních standardů. Výjimka je však v tomto ohledu stanovena pro poskytovatele digitálních služeb, kteří jsou regulováni podle principu maximální harmonizace. Díky širokému rozsahu působnosti tak bude moci každý členský stát provádět směrnici s ohledem na skutečná rizika, jimž čelí, a jež uvedl ve své národní strategii pro bezpečnost sítí a informačních systémů. Nadto mají členské státy možnost přijmout i další, potažmo přísnější opatření, s cílem zabezpečit své základní státní funkce, zejména pokud jde o zajištění národní bezpečnosti. Tato opatření se vztahují i na opatření na ochranu informací, jejichž zpřístupnění členské státy považují za neslučitelné s podstatnými zájmy své bezpečnosti, a zachování veřejného pořádku, především pokud jde o umožnění vyšetřování, odhalování a stíhání trestné činnosti. Povinnost zavést systém řízení rizik se vztahuje pouze na klíčové subjekty a vyžaduje opatření úměrná daným rizikům. Zároveň budou regulované subjekty navíc povinny hlásit pouze incidenty, které mají významný dopad na poskytování jejich služeb, přičemž v případě poskytovatelů digitálních služeb musí být uvedené služby nabízeny na území Unie a poskytovatelé jsou povinni splnit ohlašovací povinnost pouze v případě, že mají přístup k informacím potřebným pro posouzení dopadu incidentu.

Cílovým stavem realizace navrhované právní úpravy je zajištění transpozice směrnice do českého právního řádu a zvýšení bezpečného fungování informační společnosti ČR, tj. zajištění bezpečné realizace základního práva na informační sebeurčení prostřednictvím informačních systémů, služeb a sítí elektronických komunikací. Cílem navrhované právní úpravy je též ochrana nedistributivních práv státu, tj. zajištění veřejného zájmu na bezpečnosti kritické informační infrastruktury, významných informačních systémů a informačních systémů, jejichž prostřednictvím je provozována základní služba.

Rovněž má návrh zákona za cíl odstranit některé nedostatky, které byly zjištěny aplikační praxí zákona o kybernetické bezpečnosti.

Cílovým stavem je ve shora uvedeném smyslu fungující systém kybernetické bezpečnosti zahrnující provozovatele základních služeb, kteří budou muset splňovat tyto povinnosti:

- informovat správce nebo provozovatele informačního systému základní služby o jejich určení jakožto provozovatele základní služby, pokud nejsou sami správcem nebo provozovatelem informačního systému základní služby;

- oznámit NBÚ významný dopad kybernetického bezpečnostního incidentu na kontinuitu poskytování základní služby, a to i tehdy, pokud takovýto významný dopad způsobí kybernetický bezpečnostní incident, který postihnul poskytovatele digitální služby;

- informovat veřejnost o probíhajícím kybernetickém bezpečnostním incidentu na základě povinnosti uložené NBÚ;

- poskytnout kontaktní údaje.

Na provozovatele základní služby se rovněž bude vztahovat stávající právní úprava týkající se výkonu státní správy a souvisejících činností NBÚ a vládního CERT.

Další povinnosti stanovené směrnicí a transponované do zákona o kybernetické bezpečnosti se pak budou vztahovat na správce a provozovatele informačního systému základní služby. Tyto subjekty tak budou především plnit povinnost:

- implementace bezpečnostních opatření v rámci jejich sítí a informačních systémů;

- detekce kybernetických bezpečnostních událostí;

- hlášení kybernetických bezpečnostních incidentů.

Dále se bude na tyto subjekty vztahovat i již existující právní úprava týkající se

- systému opatření k reakci na kybernetické bezpečnostní incidenty;

- činnosti NBÚ zahrnující činnosti vládního CERT.

Pro poskytovatele digitálních služeb budou zákonné povinnosti uplatněny v omezené míře, aby pro ně nepředstavovaly nepřiměřenou zátěž a neomezovaly tak jejich konkurenceschopnost. Na poskytovatele digitálních služeb se tak vztahuje:

- implementace bezpečnostních opatření v míře přiměřené k řízení bezpečnostních rizik, jimž jsou vystaveny jejich sítě a informační systémy;

- hlášení kybernetických bezpečnostních incidentů, které mají významný dopad na poskytování digitálních služeb;

- hlášení kontaktních údajů;

- činnost národního CERT a příslušného orgánu (NBÚ).

Navrhovaná právní úprava však nemá za cíl zasahovat do obsahového fungování informační společnosti, ale pouze zabezpečit proti úmyslným nebo nahodilým kybernetickým bezpečnostním incidentům informační kanály, jimiž člověk realizuje své právo na informační sebeurčení a jimiž stát vykonává svá nedistributivní informační práva.

Cílem navrhované právní úpravy je především doplnit minimální požadavky na standardní zabezpečení kritické informační infrastruktury a významných informačních systémů a rozšířit je i na

informační systémy provozovatelů základních služeb, respektive správců a provozovatelů informačních systémů základních služeb, a zajistit vládnímu dohledovému pracovišti v reálném čase přehled o kybernetické bezpečnostní situaci v rámci subjektů spadajících pod regulaci zákona o kybernetické bezpečnosti. Provozovatelům základních služeb, správcům informačních systémů základních služeb a provozovatelům informačních systémů základních služeb zajistí navrhovaná právní úprava nepřetržitý kontakt s vládním dohledovým pracovištěm umožňující kvalitnější identifikaci kybernetických bezpečnostních rizik s původem mimo příslušný systém, službu nebo síť, efektivnější analýzu kybernetických bezpečnostních událostí a účinnější reakci na kybernetické bezpečnostní incidenty. Tato opatření bezprostředně povedou k řešení shora identifikovaného problému zabezpečení vitálních národních informačních funkcionalit, tj. k zabezpečení nejdůležitějších informačních systémů a zabezpečení nejdůležitějších služeb a sítí před kybernetickými bezpečnostními incidenty.

Ve vztahu k poskytovatelům digitálních služeb, kteří nespadají mezi vitálně důležité části, zavádí navrhovaná právní úprava pouze povinnost přijmout přiměřená bezpečnostní opatření, hlásit kybernetické bezpečnostní incidenty s významným dopadem a oznamovat kontaktní údaje. Současně navrhovaná právní úprava počítá se spoluprací těchto subjektů se soukromoprávním národním dohledovým pracovištěm (dále také „národní CERT“). Tyto subjekty tak budou moci využívat výhod vzájemné výměny informací o řešení kybernetických bezpečnostních incidentů, jakož i získávat metodickou podporu a pomoc odpovídající odborné úrovně. Cílem navrhované právní úpravy je tedy v tomto směru zvýšení bezpečnosti těchto informačních a komunikačních systémů prostřednictvím zajištění informačního a expertního servisu podporujícího přirozené snahy správců informačních systémů, podnikatelů a dalších subjektů o zvyšování bezpečnosti jejich vlastních systémů, sítí a služeb.

1.6 Zhodnocení rizika

1.6.1 Riziko porušení povinností stanovených právním řádem EU (pozdní transpozice směrnice)

Členské státy EU mají povinnost plnit závazky vyplývající pro ně ze základních smluv EU. Podle článku 288 smlouvy o fungování Evropské unie je směrnice závazná pro každý stát, kterému je určena, pokud jde o výsledek, jehož má být dosaženo, přičemž volba formy a prostředků se ponechává vnitrostátním orgánům. Hlavním rizikem spojeným s neprovedením transpozice je tedy nedodržení závazků vyplývajících z primárního práva EU, které je ČR, jakožto členský stát EU, povinna plnit. Navíc má Komise v případě nedodržení těchto závazků k dispozici prostředky, kterými může členské státy k plnění povinností donutit, přičemž nejkrajnější variantou je podání žaloby Soudnímu dvoru Evropské unie. V tomto ohledu by tedy mohla být výrazně poškozena pověst ČR v rámci EU i na národní úrovni.

1.6.2 Riziko fragmentace vnitřního trhu EU a porušování základních hodnot EU

Neprovedení transpozice směrnice by mohlo ohrozit i fungování vnitřního trhu a znevýhodnění českých podnikatelů v digitálním sektoru. Sítě a informační systémy hrají totiž zásadní roli při usnadňování přeshraničního pohybu zboží, služeb a osob. Často jsou propojené, přičemž internet je

ze své podstaty globálním nástrojem. Vzhledem k tomuto přirozenému nadnárodnímu rozměru se může narušení těchto systémů v jednom členském státě dotknout dalších členských států nebo dokonce celé EU. Odolnost a stabilita sítí a informačních systémů je proto základním předpokladem pro hladké fungování vnitřního trhu. V současné době již vlivem nesrovnalostí vyplývajících z nestejných vnitrostátních kapacit pro zajištění bezpečnosti sítí a informačních systémů, politik a úrovně ochrany v jednotlivých členských státech vznikly na vnitřním trhu bariéry, což odůvodňuje i zásah ze strany EU.

Absence transpozice směrnice by vzhledem k přeshraniční povaze bezpečnosti sítí a informačních systémů znamenala, že ČR bude jednat samostatně právě bez ohledu na vzájemnou provázanost evropských sítí a informačních systémů. Odpovídající míra koordinace mezi ČR s dalšími členskými státy by přitom zajistila, aby rizika týkající se bezpečnosti sítí a informačních systémů mohla být efektivně řízena na přeshraniční úrovni, na níž vznikají. Rozdílné předpisy o bezpečnosti sítí a informačních systémů představují bariéru pro podniky, které chtějí působit v několika zemích, i pro dosažení globálních úspor z rozsahu. Z hlediska českých podnikatelů by navíc neprovedení transpozice mohlo ohrozit jejich mezinárodní pověst a zhoršit tak jejich postavení oproti podnikatelům z ostatních členských států.

Pro vytvoření rovných podmínek a odstranění mezer v legislativě je navíc zavedení povinností na úrovni EU nezbytné. Přístup založený čistě na dobrovolnosti by vedl k tomu, že by spolupracovala jen malá část členských států, které mají kybernetickou bezpečnost zajištěnou na vysoké úrovni. Aby se mohly zapojit všechny členské státy, musí být zajištěna požadovaná minimální úroveň zajištění bezpečnosti u každého z nich. Opatření přijatá v oblasti bezpečnosti sítí a informačních systémů jednotlivými vládami musí být jednotná a koordinovaná, aby zabraňovala vzniku incidentů týkajících se bezpečnosti sítí a informačních systémů a minimalizovala jejich dopady. Kromě toho společný postup ve věci politiky bezpečnosti sítí a informačních systémů může velmi pozitivně ovlivnit ochranu základních práv a především práva na ochranu osobních údajů a soukromí.

Směrnice má dále mimo jiné za cíl zvýšit i ochranu spotřebitelů, podniků i vlád v EU před narušováním bezpečnosti sítí a informačních systémů. Zejména povinnosti uložené členským státům zaručují odpovídající připravenost na vnitrostátní úrovni a připívají k vytvoření vzájemné důvěry, která je předpokladem efektivní spolupráce na úrovni EU. Nastavení mechanismů spolupráce na úrovni EU prostřednictvím kooperačních struktur by mělo umožnit předcházení přeshraničním rizikům a narušení bezpečnosti sítí a informačních systémů a reagovat na ně jednotným a koordinovaným způsobem. Zavedení povinného řízení rizik v oblasti bezpečnosti sítí a informačních systémů pro orgány veřejné správy a klíčové soukromé subjekty by bylo silným podnětem ke skutečně efektivnímu řízení rizik. Povinnost oznamovat narušení bezpečnosti sítí a informačních systémů s významným dopadem by posílila schopnost na taková narušení reagovat a zvýšila transparentnost. Kromě toho by celkové zvýšení bezpečnosti sítí a informačních systémů v ČR i EU přidalo na důvěryhodnosti tohoto společenství coby partnera pro dvoustrannou i mnohostrannou spolupráci. EU by tak mohla lépe prosazovat základní práva a své hodnoty v ostatních částech světa.

1.6.3 Riziko nečinnosti

Mezi další hlavní rizika spojená s nečinností se řadí nárůst kybernetických útoků, výrazné materiální škody, ohrožení základních služeb a v neposlední řadě i neplnění dalších mezinárodních závazků ČR

včetně závazků plynoucích ze smluv o ochraně investic. Neprovedení transpozice směrnice by znamenalo rezignaci státu na posílení ochrany základního práva, jehož důležitost v současné společnosti stále roste, tj. práva na informační sebeurčení. Zprostředkovaně by se pak jednalo též o rezignaci na primární odpovědnost státu za zajištění ochrany vlastnického práva (v tomto případě vlastnického práva k informační a komunikační infrastruktuře) a na odpovědnost státu vůči mezinárodnímu společenství (tj. o faktické porušení principu bdělosti – due dilligence) a odpovědnosti k zahraničním investorům v sektoru ICT.

1.6.4 Technická a ekonomická náročnost zavádění bezpečnostních opatření u povinných osob

Správci a provozovatelé informačních systémů základních služeb budou podle navrhované právní úpravy povinni zavádět bezpečnostní opatření, jejichž struktura je navržena v zákoně a obsah bude specifikován v prováděcím právním předpise. Část subjektů, které budou podle navrhované právní úpravy zavádět povinně bezpečnostní opatření, již má řešenu vlastní kybernetickou bezpečnost na úrovni mezinárodních standardů ISO/IEC 20000 a ISO/IEC 27000. Vzhledem k tomu, že navrhovaná právní úprava z těchto standardů vychází, neměla by být adaptace na zákonné povinnosti v takových případech otázkou prakticky žádných dodatečných investic. Tam, kde nově regulované subjekty doposud řešily kybernetickou bezpečnost jiným způsobem, než stanoví navrhovaný zákon, počítá právní úprava s přechodným obdobím.

Pro poskytovatele digitálních služeb pak bude platit mírnější režim regulace, který jim sice ukládá zavádět přiměřená bezpečnostní opatření, jejich strukturu si však budou moci určit tito poskytovatelé sami s ohledem na bezpečnostní rizika, postihující jejich sítě a informační systémy. V tomto ohledu je nutno zdůraznit, že směrnice má co nejvíce harmonizovat míru bezpečnostních opatření, kterou by měly tyto subjekty splňovat, aby nedocházelo k nežádoucí fragmentaci vnitřního trhu v této oblasti.

1.6.5 Zneužití dat z evidence kybernetických bezpečnostních incidentů a dalších evidencí

Vládní i národní dohledová pracoviště CERT již zpracovávají a budou i nadále zpracovávat data o výskytu a řešení kybernetických bezpečnostních incidentů, přičemž případný únik těchto dat by mohl ohrozit bezpečnostní zájmy ČR nebo práva orgánů a osob. Nadto NBÚ disponuje i evidencí kybernetických bezpečnostních incidentů, jejíž součástí jsou údaje o zdroji kybernetického bezpečnostního incidentu, údaje z hlášení o kybernetickém bezpečnostním incidentu, včetně identifikačních údajů systému, ve kterém se kybernetický bezpečnostní incident vyskytl, a informace o postupu při řešení kybernetického bezpečnostního incidentu a jeho výsledku. Data v evidenci jsou chráněna povinností mlčenlivosti a jejich předávání je možné jen v omezeném rozsahu na základě zmocnění k poskytování údajů. Zároveň jsou údaje obsažené v evidenci incidentů vyjmuty z povinnosti poskytování informací podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

Navrhovaná právní úprava je minimalistická co do struktury zpracovávaných dat. Součástí evidence kybernetických bezpečnostních incidentů nejsou obsahové údaje z informačních systémů, sítí nebo služeb elektronických komunikací; pro potřeby národního a vládního CERT jsou zpracovávána výlučně data o kybernetických bezpečnostních incidentech. Nejcitlivější z údajů tvořících evidenci

kybernetických bezpečnostních incidentů jsou statistická data o frekvenci útoků na jednotlivé systémy, sítě a služby elektronických komunikací a data o způsobu řešení kybernetických bezpečnostních incidentů.

1.6.6 Personální zajištění vládního CERT a NBÚ

Vzhledem k tomu, že specialistů na problematiku kybernetické bezpečnosti s náležitou kvalifikací a odpovídajícími zkušenostmi je v ČR v současné době nedostatek[29] a vzhledem ke skutečnosti, že NBÚ má velmi omezené možnosti co do jejich náležitého finančního ohodnocení, lze očekávat personální problémy při rozšiřování constituency vládního CERT o provozovatele základních služeb a správce a provozovatele informačních systémů základních služeb. S cílem předejít těmto problémům NBÚ systematicky spolupracuje se špičkovými českými univerzitami a podporuje vznik specializovaných studijních oborů zaměřených na kybernetickou bezpečnost. Současně NBÚ již v současné době propaguje činnost vládního CERT a formou spolupráce na vzdělávacích a výzkumných aktivitách univerzit zapojuje do aktivit vládního CERT studenty a doktorandy.

2. Návrh variant řešení

K hodnocení jednotlivých variant regulatorního modelu je třeba přistoupit prostřednictvím následujících premis:

1. Při naplňování transpoziční povinnosti, která pro ČR vyplývá z primárního práva EU, je závazný výsledek, kterého má být dosaženo, přičemž volba formy a prostředků se ponechává vnitrostátním orgánům.

2. K posílení kybernetické bezpečnosti a odpovídajícímu zajištění práva na informační sebeurčení prostřednictvím přístupu k fungujícím službám informační společnosti je nutno zpracovávat informace o výskytu kybernetických bezpečnostních incidentů z co největšího množství zdrojů. Kybernetické útoky velkého rozsahu totiž mají často v podmínkách sledování místních sítí a systémů charakter bagatelních incidentů, přičemž až vyhodnocení informací z větší části informační nebo komunikační infrastruktury může přinést adekvátní identifikaci závažného kybernetického útoku, případně může napomoci při určování jeho rozsahu a nebezpečnosti.

3. Jednotlivé informační a komunikační systémy včetně systémů kritického významu mají různé správce a fungují v různých právních režimech. Nelze tedy docílit jejich koordinovaného zabezpečení na národní úrovni jinak než prostřednictvím činnosti státu – žádný jednotlivý orgán veřejné moci, soukromé ani akademické sdružení nebo jiný spolek totiž nepokrývá tyto součásti v jejich souhrnu a není zde tak subjekt, který by mohl zajistit jejich koordinovanou ochranu před kybernetickými bezpečnostními incidenty. Úloha státu je tedy v tomto případě podobně jako v ostatních oblastech bezpečnostní politiky unikátní a nenahraditelná.

4. Státní moc lze uplatňovat výlučně na základě a v mezích zákona a soukromoprávním subjektům lze ukládat povinnosti jen zákonem. Transpozici směrnice je tedy třeba provést zákonem, s podrobným

[29] Je odhadováno, že na pracovním trhu ČR chybí asi 1 000 zaměstnanců s odpovídající kvalifikací.

rozdělením povinností subjektů, vymezením jejich rolí subjektů a sjednocením pojmů užívaných v oblasti kybernetické bezpečnosti.

Zároveň je nutno mít na paměti, že služby informační společnosti se vyznačují svým síťovým charakterem, tj. jsou vzájemně propojeny a navzájem se ovlivňují, přičemž i rozsahem nepatrný prvek sítě může závažným způsobem ovlivňovat její ostatní části, a to dokonce často i bez ohledu na geografickou blízkost.

2.1 Varianta 0 (bez specifické právní regulace)

Za nulovou variantu je možno považovat pokračování současného stavu, tj. neexistenci specifické zákonné úpravy pro provozovatele základní služby, respektive správce a provozovatele informačního systému základní služby, a poskytovatele digitální služby a neprovedení transpozice směrnice. V takové situaci je zajištění kybernetické bezpečnosti provozovatelů základních služeb, správců informačních systémů základních služeb, provozovatelů informačních systémů základních služeb a poskytovatelů digitálních služeb otázkou dobrovolné koordinace dohledových a ochranných činností mezi jednotlivými subjekty. Platí přitom, že v podstatě každý subjekt může svou liknavostí nebo neochotou účastnit se na systému kybernetické bezpečnosti poskytnout útočníkovi dostatek prostoru k závažnému ohrožení kybernetické bezpečnosti.

Z hlediska bezpečnostního by nulová varianta přinesla zvýšenou míru bezpečnostní rizikovosti následovanou absencí efektivních nástrojů k obraně před rozsáhlým kybernetickým útokem zásadního významu, který může mít značné dopady na ekonomické nebo společenské aktivity.

Z ekonomického hlediska nulová varianta zdánlivě šetří investice na rozšíření národních kybernetických schopností a kapacit. Rovněž by šetřila investice vybraných osob soukromého práva a orgánů veřejné moci do zabezpečení jejich systémů (tj. na zavedení povinných bezpečnostních opatření). Je však nutno zvážit, že nezavedením příslušných bezpečnostních opatření by zůstala nezabezpečena významná skupina subjektů, jejichž činnost a služby mají značné hospodářské a společenské dopady. V tomto ohledu by tedy případné incidenty mohly napáchat dalekosáhlejší ekonomické ztráty, než jsou náklady vzniklé implementací bezpečnostních opatření. Navíc značná část subjektů již odpovídající bezpečnostní opatření provádí dobrovolně, ekonomické náklady tudíž pro ně nebudou příliš vysoké. V případě správců kritické informační infrastruktury je tato povinnost dokonce plněna již na základě současné právní úpravy.

Zároveň je nutno zdůraznit, že neprovedení transpozice směrnice by mohlo ohrozit reputaci českých podnikatelů v digitálním sektoru, kteří by nebyli nuceni splňovat stejné požadavky, jako jsou nuceni splňovat jim podobné subjekty v ostatních členských státech EU. Je sice pravděpodobné, že velká část těchto subjektů již v současné době splňuje dokonce vyšší bezpečnostní standardy, přesto se však dá říci, že plošné zavedení bezpečnostních standardů a harmonizace této oblasti napříč EU povede, a to zejména v případě poskytovatelů digitálních služeb, ke zvýšení zabezpečení sítí a informačních systémů, čímž budou dány i vyšší garance pro spotřebitele a obchodníky. Neprovedení transpozice by tak mohlo vést až ke zhoršení konkurenceschopnosti českých podnikatelů, kteří by nebyli schopni garantovat stejnou míru zabezpečení, jako subjekty v jiných částech EU. Zároveň by způsobila fragmentaci vnitřního trhu EU, která je z hlediska celoevropské ekonomiky nežádoucí.

Z pohledu mezinárodních závazků ČR by pak nulová varianta znamenala nedodržení závazků vyplývajících pro ni z primárního práva EU, potažmo rezignaci státu na posílení ochrany základního práva, jehož důležitost v současné společnosti stále roste, tj. práva na informační sebeurčení. Zprostředkovaně by se pak jednalo též o rezignaci na primární odpovědnost státu za zajištění ochrany vlastnického práva (v tomto případě vlastnického práva k informačním a komunikačním systémům) a na odpovědnost státu vůči mezinárodnímu společenství (tj., jak již bylo uvedeno výše, o faktické porušení principu bdělosti – due dilligence) a odpovědnosti k zahraničním investorům v sektoru ICT. To by mohlo ve svém důsledku vést i ke snížení mezinárodní reputace ČR, která v současné době patří na evropské úrovni mezi lídry v oblasti kybernetické bezpečnosti a disponuje naprosto unikátní právní úpravou této oblasti. Rovněž na mezinárodní úrovni je ČR chápána jako rovnocenný a plnohodnotný partner, což vyplývá i z bohaté mezinárodní spolupráce, která probíhá v současnosti mezi jejími příslušnými orgány a orgány jiných států.

I s ohledem na současnou mezinárodní bezpečnostní situaci, která zahrnuje vznik nových hrozeb, jako jsou např. kyberterorismus nebo hybridní války, není možné ignorovat požadavek na zvýšení zabezpečení kyberprostoru EU.

Tolerance současného stavu spočívající v nerozšíření působnosti zákona o kybernetické bezpečnosti je tedy z hlediska nutnosti respektovat a plnit mezinárodní závazky neúnosná. Vzhledem k výše uvedeným okolnostem je tedy nulová varianta zásadně nevhodná a nepřijatelná.

2.2 Varianty podle zapojení subjektů

2.2.1 Varianta Ia (varianta spolupráce s osobami soukromého práva)

Varianta řešení kybernetické bezpečnosti za účasti osob soukromého práva zahrnuje regulaci sítí a informačních systémů, které dohromady tvoří kybernetický prostor a jejichž bezpečnost implikuje stav kybernetické bezpečnosti státu. Současně je tato varianta postavena na předpokladu, že podstatná část informačních a komunikačních systémů má soukromoprávní vlastníky, správce nebo provozovatele, se kterými musí stát spolupracovat.

Bezpečnost kybernetického prostoru má pro tyto osoby soukromého práva značný ekonomický význam, neboť jen fungující síť nebo informační systém jim může generovat náležitý zisk. Zároveň umožní dostatečné zabezpečení těchto sítí nebo informačních systémů předcházet kybernetickým bezpečnostním incidentům, a tím zamezit značným ztrátám, které mohou vzniknout nejenom přímo následkem incidentu, ale i ztrátou důvěry zákazníků v poskytované služby a poškozením dobré pověsti daného subjektu. Tyto osoby soukromého práva tedy aktivně investují do zabezpečení vlastní infrastruktury a mají ekonomicky motivovaný zájem podílet se na zajištění celkové kybernetické bezpečnosti, vzhledem k tomu, že to zároveň zlepšuje i jejich konkurenceschopnost na trhu. Na druhou stranu jsou však tyto osoby značně závislé na informacích a datech, s kterými tyto informační systémy operují. Z tohoto důvodu mohou vnímat jakoukoli ingerenci ze strany státu jako nežádoucí. Je tak z jejich hlediska vhodnější, aby jejich přímým partnerem byl rovněž soukromoprávní subjekt.

Nelze však opominout, že určitá část subjektů spravuje natolik důležité sítě a informační systémy, že

jejich narušením by mohlo dojít k ohrožení základních společenských nebo ekonomických funkcí, popřípadě dokonce národní bezpečnosti. V takovémto případě by měl mít stát možnost přímo spolupracovat s těmito subjekty, aby mohl zabránit případným škodlivým následkům kybernetických bezpečnostních incidentů. Spolupráce se soukromoprávním subjektem tak přichází v úvahu tehdy, kdy se nejedná o subjekty natolik významné, že by narušením jejich sítí nebo informačních systémů došlo k výraznému zásahu do základních společenských hodnot, případně se jedná o subjekty podléhající již obdobné právní regulaci.

Co se týče nákladů, předmětné subjekty budou v případě uplatnění této varianty povinny plnit jim předepsané zákonné povinnosti. Lze přitom předpokládat, že náklady vzniklé implementací bezpečnostních opatření a vytvářením příslušných pracovních pozic budou v přiměřené výši ve vztahu k chráněnému zájmu a jejich vynaložení bude ve srovnání s nulovou variantou efektivnější. Rovněž náklady na posílení národních schopností a kapacit budou úměrné vzhledem k vysoké míře zabezpečení, které by bylo touto variantou dosaženo. Dále lze konstatovat, že z výše uvedených důvodů již značná část subjektů částečně bezpečnostní opatření provádí, náklady na provedení bezpečnostních opatření tak budou u těchto subjektů fakticky nižší.

Spolupráce s osobami soukromého práva tak zahrnuje jejich přímé podílení se na vytváření systému kybernetické bezpečnosti, a to prostřednictvím soukromoprávního dohledového pracoviště.

Zejména svěření působnosti nad kategorií poskytovatelů digitálních služeb tomuto dohledovému pracovišti by reflektovalo významnost těchto subjektů, která je nepopiratelně nižší než významnost kritické informační infrastruktury, významných informačních systémů nebo provozovatelů základních služeb a správců a provozovatelů informačních systémů základních služeb. Možnou nevýhodou je v tomto případě však obecná povinnost ČR zajistit takovému bezpečnostnímu týmu jednak dostatečné zdroje a materiální, technické a personální prostředky, jednak nutnost zajistit účelné a účinné provádění kontroly a ukládání sankcí za porušení povinností.

Obecně by použitím této varianty došlo ke zvýšení bezpečnosti digitálního prostředí v ČR a tím i zlepšení její reputace pro investory, odbornou veřejnost, občany a mezinárodní partnery. Navíc povinnostní charakter právní regulace včetně sankcí pak má zajistit dodržení stejné úrovně bezpečnostních standardů u těch nejdůležitějších informačních systémů a sítí a služeb elektronických komunikací, čímž je zaručena stabilní a předvídatelná úroveň zabezpečení sítí a informačních systémů. Zároveň by však tato varianta umožnila rozdělení úkolů mezi veřejnoprávní (státní) dohledové pracoviště a soukromoprávní dohledové pracoviště, čímž by významné snížila nápad pracovní agendy pro stát a zefektivnila tak proces řešení kybernetických bezpečnostních incidentů.

Touto variantou by byla splněna transpoziční povinnost a dodrženy evropské závazky a zároveň závazky mezinárodně-právní týkající se ochrany základních lidských práv a svobod, zejména pak práva na informační sebeurčení a vlastnického práva. Rovněž by tedy bylo sníženo riziko fragmentace vnitřního trhu EU a jednalo by se i o adekvátní reakci na současnou světovou bezpečnostní situaci.

Vzhledem k bezproblémové ústavní konformitě, vysoké efektivitě a nízké nákladovosti se tato varianta jeví být pro zajištění kybernetické bezpečnosti ČR v současné situaci ideální.

2.2.2 Varianta Ib (varianta výlučné a přímé státní regulace)

Tato varianta je založena na předpokladu, že pouze stát prostřednictvím svých orgánů přímo spolupracuje s regulovanými subjekty a kontroluje a vynucuje plnění jim uložených povinností, přičemž v rámci této regulace není nijak zapojena součinnost se soukromoprávním dohledovým pracovištěm.

To by znamenalo zejména svěření kategorie poskytovatelů digitálních služeb do působnosti vládního CERT. NBÚ by tak přijímal a zpracovával bezpečnostní incidenty od podstatně širšího spektra subjektů[30], přičemž se dá předpokládat jejich nárůst v řádech až o tisíce. Vzhledem však ke svým omezeným kapacitám by NBÚ nebyl schopen dostatečně zlepšovat úroveň svých služeb, čímž by trpěly i ostatní kategorie orgánů a osob. Navíc by tato kategorie subjektů představovala pro NBÚ výraznou administrativní zátěž.

Z hlediska regulovaných subjektů by pak mohlo být problematické, že citlivé informace týkající se kybernetických bezpečnostních incidentů musejí poskytovat organizační složce ústředního správního úřadu. I s ohledem na fakt, že tyto subjekty velmi často spravují obsah generovaný přímo uživateli, případně jejich citlivá data, mohlo by dojít k poškození důvěryhodnosti ČR u jejích občanů i podnikatelů. Takovýto zásah by tak mohlo způsobit i obavy z kontrolování obsahu státem a poškodit tak podnikatelské prostředí v ČR, čímž by mohla být ohrožena i její mezinárodní konkurenceschopnost a především její pověst, což by mělo vliv i na atraktivitu ČR pro zahraniční investory.

Lze tedy říci, že vedle značně zvýšené míry technické a organizační náročnosti pro státní orgány se tato varianta zdá být především rizikem pro pověst ČR a její podnikatelské prostředí. Navíc, oproti variantám Ia nebo 0 je přímá regulace nejnáročnější co do přímých nákladů a požadavků na materiální, finanční a personální zajištění orgánů státní správy.

Z výše uvedených důvodů se varianta přímé regulace jeví být nevhodnou, a to i přes to, že by jinak odpovídala splnění transpoziční povinnosti, čímž by byla posílena harmonizace vnitřního trhu a zároveň zohledněna celosvětová bezpečnostní situace.

2.3 Varianty podle působnosti

2.3.1 Varianta IIa (varianta striktního následování směrnice NIS)

Tato varianta předpokládá, že by byly striktně regulovány pouze subjekty spadající pod působnost směrnice. Je nutno si však uvědomit, že ČR již v současné době patří mezi evropské lídry v oblasti kybernetické bezpečnosti a oproti ostatním členským státům i EU jako takové je již značně napřed. Zákonem o kybernetické bezpečnosti totiž zavedla regulaci orgánů a osob, které spravují kritickou informační infrastrukturu nebo významné informační systémy. V případě orgánů a osob provozujících nebo poskytujících služby a sítě elektronických komunikací pak rozšířila povinnosti těchto subjektů

[30] V 1Q 2016 bylo určeno 153 významných informačních systémů a 98 prvků kritické informační infrastruktury, které spadají do constituency vládního CERT.

nad rámec povinností stanovených zákonem o elektronických komunikacích. V tomto ohledu je již současná regulace, co se týče rozsahu, pravděpodobně širší nebo přinejmenším srovnatelná se směrnicí. Jejím omezením by došlo ke značnému zhoršení zabezpečení českého kyberprostoru. Navíc je stávající regulace značně ceněna i ze strany odborné veřejnosti, s níž byl zákon o kybernetické bezpečnosti důkladně diskutován již během legislativního procesu. Dá se tedy říci, že by se jednalo o značný krok zpět, který by způsobil nedostatečné zajištění významných nebo dokonce kritických subjektů v rámci českého kyberprostoru.

Je sice nutno podotknout, že by u mnohých subjektů došlo k určitému snížení nákladů na implementaci bezpečnostních opatření, stejně jako nákladů na plnění dalších povinnost podle zákona o kybernetické bezpečnosti. Tyto úspory by však byly spíše zdánlivé. Je totiž v samotném zájmu těchto subjektů, aby byly co nejlépe zabezpečeny. Případné škody vzniklé následkem kybernetických bezpečnostních incidentů by totiž mohly mnohonásobně převýšit tyto úspory. Navíc by tyto incidenty mohly způsobit i poškození pověsti těchto subjektů a ztrátu důvěru zákazníků, což by pro ně mohlo mít až likvidační následky. Rovněž úspory na straně státních orgánů odpovědných za bezpečnost sítí a informačních systémů jsou spíše marginální s ohledem na fakt, že směrnice ukládá vytvoření příslušných národních organizačních struktur odpovědných za tuto oblast.

Tato varianta by tak způsobila zejména značnou právní nejistotu pro regulované subjekty. Zároveň by mohla vést i k častým správním nebo soudním sporům, vzhledem k tomu, že současná regulace uložila povinným orgánům a osobám implementovat finančně, organizačně i personálně náročná bezpečnostní opatření. Na závěr by vedla k obecnému zhoršení podnikatelského prostředí v ČR a ke ztrátě důvěry zákazníků i zahraničních investorů. Vedle toho by poškodila i mezinárodní pověst ČR a snížila by ochranu základních práv, a ačkoli by vedla k harmonizaci vnitřního trhu EU, byla by nedostatečná i vzhledem k celosvětové bezpečnostní situaci.

Vzhledem k výše uvedeným rizikům se tato varianta jeví jako krajně nevhodná.

2.3.2 Varianta IIb (varianta doplnění zákona o kybernetické bezpečnosti o požadavky směrnice NIS)

Tato varianta předpokládá doplnění již stávajícího a fungujícího režimu zákona o kybernetické bezpečnosti o požadavky stanovené směrnicí.

Vzhledem k tomu, že směrnice a zákon se ve velké míře shodují, co do míry ukládaných povinností, mohlo by být nastavení zákona o kybernetické bezpečnosti zachováno. Ohledně některých povinností (např. vytvoření strategie bezpečnosti sítí a informačních systémů) by se jednalo pouze o formální doplnění litery zákona, protože tyto povinnosti jsou již v praxi plněny. Transpozicí směrnice by však došlo ke změně působnosti zákona, respektive k jejímu rozšíření o provozovatele základních služeb, správce a provozovatele informačních systémů základních služeb a poskytovatele digitálních služeb.

Tato varianta by bezpochyby dostačovala pro naplnění povinností stanovených unijním právem. Vzhledem k tomu, že ČR je již v současné době v oblasti kybernetické bezpečnosti velmi aktivní a zákon o kybernetické bezpečnosti je značně oceňován, zejména ze strany odborné veřejnosti, přičemž v evropském měřítku se jedná o unikátní právní úpravu, je vhodné stávající status quo

zachovat, aby nebyla poškozena pověst národních orgánů na národní i mezinárodní úrovni.

Právě naopak by mohla mít transpozice směrnice tímto způsobem velmi pozitivní efekt zejména v tom ohledu, že by ještě zvýšila úroveň bezpečnosti sítí a informačních systémů v ČR. Především by se pak jednalo o uložení povinností i těm subjektům, které ze současné regulace vlivem legislativních mezer vypadávají (např. v oblasti zdravotnictví). Zároveň by tak posílila důvěryhodnost českých podnikatelů a zlepšila jejich konkurenceschopnost, čímž by bylo zlepšené i české podnikatelské prostředí jako takové.

Samozřejmě by však tímto způsobem transpozice vznikly náklady nově regulovaným subjektům. V tomto ohledu by se jednalo zejména o náklady na zavádění bezpečnostních opatření spojené s administrativními náklady a náklady na personální obsazení nově vznikajících pozic, přičemž by mohla nastat i situace, že pracovní trh nebude schopen zajistit dostatek kvalifikovaných pracovníků v oblasti kybernetické bezpečnosti, protože se jedná o relativně mladý a teprve se rozvíjející obor. Zároveň však lze konstatovat, že velká část firem již z podstaty své činnosti bezpečnostní opatření uplatňuje. Nová by tedy pro ně byla zejména povinnost ohlašovat kybernetické bezpečnostní incidenty a vést bezpečnostní dokumentaci. Dá se tedy říci, že vzhledem k charakteru a významnosti regulovaných subjektů se zdají být výše uvedené náklady odůvodněné a přiměřené. Na druhou stranu totiž bude zejména implementací bezpečnostních opatření minimalizováno riziko kybernetických bezpečnostních incidentů, které by jinak mohly mít dalekosáhlé dopady. Obdobně to platí i pro náklady na rozšíření národních kapacit.

Vedle toho by byly nově regulované subjekty zapojeny do systému sdílení informací, které by je varovaly ohledně existujících hrozeb. Byla by tak posílena i akceschopnost těchto subjektů nejen při řešení již vzniklých kybernetických bezpečnostních incidentů, ale i při zavádění včasných preventivních opatření.

Při aplikaci této varianty[31] je však nutno zvážit samotný způsob začlenění provozovatelů základních služeb, potažmo správců a provozovatelů informačních systémů základních služeb, a poskytovatelů digitálních služeb do systému zákona o kybernetické bezpečnosti. V případě posledně zmíněné skupiny se jedná o množinu subjektů, které jsou značně odlišné od v současné době již regulovaných orgánů a osob, z tohoto důvodu by tato skupina měla být regulována samostatně, bez použití analogie k některé z již existujících kategorií orgánů a osob. Jinak je tomu však v případě provozovatelů základních služeb a správců informačních systémů základních služeb, případně provozovatele informačních systémů základních služeb, kteří jsou svojí povahou blízcí zejména správcům systémů kritické informační infrastruktury. Mnohdy je možno dokonce s jistotou konstatovat, že prvky kritické informační infrastruktury by prošly i kritérii pro určení provozovatelů základních služeb. Přesto je vhodné tyto tři skupiny dostatečně odlišit a zdůraznit tak spíše jejich regionální význam. V případě kritické informační infrastruktury se totiž jedná o subjekty, jejichž významnosti je zdůrazňována z hlediska státu, přičemž podle krizového zákona na ně dopadají i další povinnosti. Vynětím provozovatelů základních služeb a správců a provozovatelů informačních systémů základních služeb z režimu krizového zákona tak nebudou tyto subjekty zatíženy povinnostmi podle krizového zákona, přičemž však budou stále povinny zabezpečit své sítě

[31] Obdobně toto platí i pro variantu IIc.

a informační systémy na odpovídající úrovni. Rozšíření průřezových a odvětvových kritérií v nařízení vlády č. 432/2010 Sb. a určení všech provozovatelů základních služeb a správců a provozovatelů informačních systémů základních služeb jakožto prvků kritické informační infrastruktury je tak krajně nevhodné. Navíc, aby toto nařízení vlády zahrnovalo všechna odvětví uvedená ve směrnici, muselo by být rozšířeno i o sektory, které na úrovni ČR nejsou považovány za kritické (např. sektor vodní dopravy).

Koncepčnější řešení tak představuje zavedení provozovatelů základních služeb a správců a provozovatelů informačních systémů základních služeb coby nových kategorií povinných osob *sui generis* při současném zachování systému kritické informační infrastruktury.

Tato varianta by plně splňovala požadavky stanovené evropským právem. Rovněž by nebyla v rozporu ani s ústavním pořádkem ČR ani s mezinárodními závazky, které pro ČR vyplývají ze smluv o ochraně lidských práv. Právě naopak by ještě vedla k posílení ochrany práva na informační sebeurčení osob a s tím práv souvisejících. Zároveň by vedla k harmonizaci vnitřního trhu a i s ohledem na světovou bezpečnostní situaci by byla vyhovující. Tato varianta je tedy vhodná pro transpozici směrnice.

2.3.3 Varianta IIc (varianta doplnění zákona o kybernetické bezpečnosti nad rámec požadavků směrnice NIS)

Tato varianta předpokládá doplnění již stávajícího a fungujícího režimu zákona o kybernetické bezpečnosti o požadavky stanovené směrnicí, a zároveň jeho novelu v oblastech, které se v průběhu jeho aplikace ukázaly být problematickými.

Vzhledem k tomu, že směrnice a zákon o kybernetické bezpečnosti se ve velké míře co do míry ukládaných povinnosti shodují, mohlo by být nastavení zákona o kybernetické bezpečnosti zachováno. Ohledně některých povinností (např. vytvoření strategie bezpečnosti sítí a informačních systémů) by se jednalo pouze o formální doplnění litery zákona, protože tyto povinnosti jsou již v praxi plněny. Transpozicí směrnice by však došlo ke změně působnosti zákona, respektive k jejímu rozšíření o provozovatele základních služeb, správce a provozovatele informačních systémů základních služeb a poskytovatele digitálních služeb. Rovněž by však byl zákon o kybernetické bezpečnosti novelizován v dalších oblastech, které byly na základě konzultací s odbornou veřejností vytipovány jakožto problematické.

Je nutno si totiž uvědomit, že oblast informačních a komunikačních technologií se vyvíjí velmi rychle, což lze dobře prezentovat na základě Moorova zákona, který uvádí, že výkon technologie se zdvojnásobí každých osmnáct měsíců, což neplatí pouze o výkonu počítačů, ale i o přenosové rychlosti, přičemž se snižuje energetická náročnost výpočetních technologií.[32] S tím však souvisí i možnosti kybernetických hrozeb, které jsou čím dál sofistikovanější a zákeřnější, a narůstá jejich počet. Je přirozené, že právo za realitou zaostává, je však nutno se snažit jej pokud možno co nejvíce držet v aktuální podobě, aby odpovídalo reálným bezpečnostním hrozbám.

Dále by tato varianta bezpochyby dostačovala pro naplnění povinností stanovených unijním právem.

[32] Srov. Pilný, I.: Digitální Ekonomika: Žít nebo přežít. Brno: Bizbooks, 2016, 1. vyd. Str. 12.

Jejím využitím by byl zachován režim zákona o kybernetické bezpečnosti, který by byl ještě rozšířen na další povinné subjekty, a byly by odstraněny jeho mezery. Jednalo by se tedy o značné posílení ochrany českého kyberprostoru a zároveň o posílení důvěryhodnosti českých podnikatelů.

Jako u výše uvedené varianty IIb i tímto způsobem transpozice by vznikly náklady nově regulovaným subjektům, a to zejména z důvodu plnění nově uložených povinností a vytváření nových pracovních míst. Rovněž i zde však platí, že vzhledem k charakteru a významnosti regulovaných subjektů se zdají být výše uvedené náklady odůvodněné a přiměřené. Na druhou stranu totiž bude zejména implementací bezpečnostních opatření a zapojením nově regulovaných subjektů do systému sdílení informací minimalizováno riziko kybernetických bezpečnostních incidentů, které by jinak mohly mít dalekosáhlé dopady. Obdobně to platí i pro náklady na rozšíření národních kapacit.

Tato varianta by tedy rovněž plně splňovala požadavky stanovené evropským právem a přispěla by k harmonizaci vnitřního trhu EU. Zároveň by nebyla v rozporu ani s ústavním pořádkem ČR ani s mezinárodními závazky, které pro ČR vyplývají ze smluv o ochraně lidských práv.

Dalším nesporným přínosem této varianty by však bylo i odstranění legislativních mezer, které brání dostatečnému zabezpečení důležitých sítí a informačních systémů. S ohledem na současnou bezpečnostní situaci, kdy kybernetické bezpečnostní incidenty jsou často nedílnou součástí válečných konfliktů, a se zdůrazněním faktu, že se zde jedná o ochranu velmi významných subjektů, které jsou důležité nejenom pro členské státy, ale i pro EU jako takovou, je tato varianta považována za nejvhodnější i přes to, že zákon o kybernetické bezpečnosti je účinný poměrně krátkou dobu.

3. Vyhodnocení nákladů a přínosů

3.1 Identifikace nákladů a přínosů

Posuzovat přínosy jednotlivých variant na základě ekonomického hodnocení je poměrně obtížné zadání, neboť dominantní přínos, který je navrhovanou právní úpravou sledován, spočívá v eliminaci nebo omezení bezpečnostních rizik a posílení základních aspektů fungování informační společnosti. Nejedná se tedy v prvé řadě pouze o eliminaci ekonomických škod, které mohou následkem kybernetických bezpečnostních incidentů vzniknout, ale zároveň o zajištění nedistributivních práv (veřejných statků), k jejichž ochraně je legitimován a povinen stát.

Jen velmi těžko se tedy v ekonomických termínech dá vyjádřit zvýšení bezpečnosti např. v případě výkonu práva na svobodu projevu nebo práva na informační sebeurčení. Podobně obtížná je kvantifikace přínosů navrhované právní úpravy, pokud jde o subsidiární efekty např. o důvěru občana ve stát a jeho instituce, důvěru ve fungování moderních informačních a komunikačních technologií nebo udržení dobré pověsti ČR a jejích orgánů na mezinárodní úrovni. V situaci, kdy je stále větší část veřejné agendy, včetně kontaktu s občany, realizována prostřednictvím informačních a komunikačních technologií, pak je navíc bezpečnost kybernetického prostoru, v němž se tyto veřejnoprávní informační transakce odehrávají, tím přínosnější, čím větší procento veřejnoprávní komunikace je realizováno elektronicky.

Informační a komunikační technologie se kromě výkonu veřejné správy významně podílejí též na

fungování jiných společenských funkcionalit, z nichž některé mají pro život člověka a společnosti zásadní význam. Informační systémy, služby a sítě elektronických komunikací tedy zajišťují chod energetických sítí, zásobování obyvatelstva životně důležitými komoditami, fungování vitálně důležitých institucí např. v oblasti zdravotnictví nebo dopravy. Přínosem sledovaným u shora popsaných variant tedy nesporně může být též další posílení bezpečnosti klíčově důležitých společenských funkcionalit a rozšíření chráněné oblasti v kyberprostoru.

Právě uvedené samozřejmě neznamená, že by přínosy různých shora popsaných variant neměly vůbec ekonomický aspekt – pouze není vhodné předřazovat tyto ekonomické efekty před obecnější společenské přínosy. Mezi čistě ekonomické přínosy může v tomto směru patřit minimalizace následků kybernetických bezpečnostních incidentů, tj. snížení míry ekonomických škod, které tyto incidenty způsobují. Jako příklad tohoto typu přínosu lze uvést situaci, kdy z důvodu kybernetického bezpečnostního incidentu nefunguje nebo jen s omezením funguje např. e-shop. Čím kvalitnější bude ochrana kybernetického prostoru před výskytem takového incidentu, tím může být útok méně intenzivní a tím rychleji též dochází k vyrovnání se s jeho následky. Na druhou stranu při nedostatečném zabezpečení může dojít k významným finančním ztrátám dané společnosti a poškození její dobré pověsti, které může mít pro její chod až fatální následky. Navíc takovýto incident nemusí postihnout pouze provozovatele nebo správce daného e-shopu, ale i jeho zákazníky, kterým mohou být odcizeny citlivé osobní údaje vhodné například pro páchání další kybernetické trestné činnosti. Je tedy nutno konstatovat, že u služeb informační společnosti, respektive digitálních služeb realizovaných v kybernetickém prostoru platí, že kvůli jejich charakteru dochází k ekonomickým ztrátám vždy, pokud služba není pro své uživatele technicky dostupná.

Dalším ekonomickým efektem různých výše popsaných variant může být zlepšení českého podnikatelského prostředí a zvýšení konkurenceschopnosti českých podnikatelů v oblasti informačních a komunikačních technologií, kteří budou moci následkem povinného plnění určité míry zabezpečení garantovat vysokou míru kvality svých služeb. Je-li v dnešní době běžné, že čeští podnikatelé oslovují prostřednictvím služeb informační společnosti zákazníky v zahraničí, je nasnadě, že bezpečné a fungující služby informační společnosti v rámci ČR mají pro rozvoj takového podnikání pozitivní vliv. Státy s fungujícím systémem kybernetické bezpečnosti tedy mohou svým podnikatelům nabídnout v porovnání se státy, které tuto problematiku neřeší, bezpečnější prostředí nejen k realizaci tuzemských obchodů ale též k mezinárodní expanzi.

S tímto je spojena i zvýšená míra motivace tuzemských a zahraničních investic do informačních a komunikačních technologií. Díky tomu, že v ČR působí špičková univerzitní a vědecká pracoviště, je zde realizována celá řada úspěšných investičních či inkubačních projektů zaměřených na pokročilé informační a komunikační technologie. Adekvátní zabezpečení kybernetického prostoru může v tomto směru posloužit k další motivaci investorů (zatímco opomenutí této agendy může naopak investory přimět k názoru, že informační a komunikační technologie nepředstavují pro ČR odpovídající prioritu).

V situaci, kdy se stát rozhodne aktivně přispět ke kybernetické bezpečnosti, je pak možno sledovat i další ekonomický přínos, a to podporu tuzemských komerčních produktů buď přímo v oblasti kybernetické bezpečnosti, nebo nepřímo v oblasti dalších produktů a služeb, které jsou na zabezpečení informačních a komunikačních technologií závislé. Vedle toho, že stát má v takovém

případě ideálně tendenci primárně využít domácích zdrojů a technologií a příslušnými veřejnými investicemi podporuje jejich tvůrce a investory, má užití těchto technologií i významný marketingový efekt. V bezpečnostních oborech totiž platí, že užití určité bezpečnostní technologie na tuzemském trhu jejího dodavatele je vnímáno jako důležitý předpoklad úspěchu této technologie v zahraničí.

Přínos ve smyslu nepřímé podpory specifických investic do sektoru informačních a komunikačních technologií lze dále zobecnit na problematiku podpory investic jako takovou. Faktorem sledovaným mezinárodními investory při rozhodování o umístění investičních akcí tedy nejsou jen otázky daňové, finanční nebo otázky dopravní dostupnosti, vzdělanosti pracovních sil nebo bezpečnosti místního právního prostředí, ale též fungující informační a komunikační infrastruktura. Přestože tedy zřejmě není bezpečně fungující kybernetický prostor u investorů mimo obory ICT dominantním faktorem pro jejich rozhodování o místě, typu a výši investic, tvoří nesporně míra kybernetické bezpečnosti jeden z důležitých momentů příslušných ekonomických analýz.

Z právě uvedeného nepřímo plyne i další přínos, který je možno u shora popsaných variant sledovat a který se týká posílení důvěry spotřebitelů a obchodních partnerů.

Není však možno přehlížet i širší společenské přínosy, které ze shora uvedených variant vyplývají. ČR je totiž vnímána jako rovnocenný partner v rámci unijního i celosvětového společenství. Nepopiratelným přínosem je tedy i plnění závazků ČR vyplývajících z unijního a mezinárodního práva. ČR totiž v současné době patří v oblasti kybernetické bezpečnosti mezi nejvyspělejší státy, a to zejména díky kvalitní právní úpravě, kterou představuje zákon o kybernetické bezpečnosti. Tento zákon má velmi dobré jméno i u odborné veřejnosti, která byla zapojena již do jeho legislativního projednávání. Je tedy nutno zvažovat i následky, které by mohly vzniknout nesprávnou transpozicí směrnice, závažně nabourávající již stávající systém kybernetické bezpečnosti. V případě, že však bude zvolena varianta, jejímž následkem bude další posílení tohoto systému, bude to znamenat posílení dobrého jména jak státních orgánů odpovědných za tuto oblast, tak i posílení pověsti ČR jako takové. Není totiž možné přehlížet významné mezinárodní přesahy problematiky kybernetické bezpečnosti, a to mimo jiné i s ohledem na současnou světovou bezpečnostní situaci, kdy jsou státy nuceny se přizpůsobovat novým hrozbám jako je kyberterorismus nebo využívání prostředků kybernetické války.

Typologii přínosů sledovaných u jednotlivých shora popsaných variant lze tedy shrnout následovně podle tří základních hledisek:

a) Bezpečnostní hledisko – jedná se o přínosy přímo spojené se zajištěním bezpečnosti informačních a komunikačních technologií. Toto hledisko zahrnuje tyto konkrétní přínosy:

- Zvýšení míry zabezpečení významných nebo dokonce kriticky důležitých společenských funkcionalit

- Ochrana relevantní části kyberprostoru v ČR a v EU

b) Ekonomické hledisko – jedná se o přínosy přímo spojené s ekonomickými zisky, popřípadě úsporami. Toto hledisko zahrnuje tyto konkrétní přínosy:

- Omezení ekonomických škod jako důsledků kybernetických bezpečnostních incidentů

- Zvýšení atraktivity ČR pro zahraniční i tuzemské investory

- Zlepšení českého podnikatelského prostředí a konkurenceschopnosti českých podnikatelů

- Posílení důvěry spotřebitelů a obchodních partnerů českých podnikatelů

c) Politicko-právní hledisko – jedná se o přínosy přímo spojené s právními závazky ČR a celkovými dopady na společnost. Toto hledisko zahrnuje tyto konkrétní přínosy:

- Splnění povinností vyplývajících pro ČR z mezinárodního práva a práva EU (transpoziční povinnost, podpora harmonizace vnitřního trhu EU)

- Ochrana základních práv a svobod (práva na informační sebeurčení, práva na svobodu projevu a dalších práv)

- Posílení reputace státu a jeho institucí u odborné veřejnosti a zvýšení míry ochrany důvěry občanů

- Posílení mezinárodní reputace ČR a dodržení mezinárodně právních závazků

- Zohlednění celosvětové bezpečnostní situace a nově vznikajících hrozeb

Je však nutno si uvědomit, že zabezpečení informačních a komunikačních technologií je proces poměrně náročný organizačně, technicky i ekonomicky. S minimalizací a posilováním bezpečnostních opatření tak nedílně souvisejí nezbytné náklady vynaložené na investice do zabezpečení, provozu informačních systémů a personálního zajištění, přičemž tyto náklady nevznikají pouze u subjektů, které musí plnit povinnosti uložené jim zákonem, nýbrž i u státních orgánů odpovědných za výkon státní správy v této oblasti. S aplikací náležitých bezpečnostních opatření navíc souvisí i určitá míra technicko-organizační náročnosti, která je závislá zejména na znalosti informačních systémů a jejich specifik. V tomto ohledu je tedy nutno přihlížet spíše k důvodnosti a přiměřenosti takovýchto nákladů vzhledem právě například k možným škodám, které mohou následky kybernetických bezpečnostních incidentů vzniknout.

Náklady jednotlivých variant lze rozdělit podle jejich typu na:

- Pořízení, respektive provádění příslušných bezpečnostních opatření a plnění dalších povinností – soukromý sektor

- Pořízení, respektive provádění příslušných bezpečnostních opatření a plnění dalších povinností – veřejný sektor

- Náklady na personální obsazení příslušných pozic zahrnující i požadavky na vývoj pracovního

trhu a vzdělávání – soukromý sektor

- Náklady na zřízení a provoz dohledových pracovišť

- Náklady na rozšíření národních schopností a kapacit, tj. na personální a finanční zajištění státních institucí odpovědných za výkon státní správy v oblasti kybernetické bezpečnosti a institucí plnících další úkoly uložené zákonem o kybernetické bezpečnosti nebo jinými právními předpisy.

Náklady na pořízení bezpečnostních opatření se v závislosti na zvolené variantě mohou lišit zejména rozsahem a typem akvizic techniky. Následné náklady na provoz se pak rovněž v návaznosti na příslušné regulatorní variantě mohou lišit podle toho, zda je třeba pouze příslušné bezpečnostní opatření pořídit (a jeho provoz již pak je pouze otázkou jeho zapojení do systému a běžné údržby) nebo zda je nutno je průběžně financovat, popřípadě investovat do inovací.

S těmito náklady úzce souvisí i míra personálních výdajů, ať už jde o zařazení zcela nových pozic a nabírání nových zaměstnanců nebo o školení stávajícího obslužného personálu. S tím souvisí i obecná potřeba dostatečně kvalifikovaných zaměstnanců, která může vytvářet tlaky na pracovní trh a vzdělávací instituce, zejména na středoškolské a vysokoškolské úrovni.

Je nutno zdůraznit, že náklady na pořízení bezpečnostních opatřeních a personální výdaje se dotknou soukromého i veřejného sektoru, protože regulace nečiní rozdíly v povaze povinných subjektů.

V případě shora popsaných variant počítajících s aktivním zapojením státu pak je třeba na straně nákladů počítat navíc s nutností akvizic dohledových technologií v rozsahu podle nastavení příslušné varianty. Nezanedbatelnou položkou pak jsou náklady NBÚ na rozšíření národních schopností a kapacit, která zahrnují zejména náklady na personální aparát, ať už jde přímo o operátory dohledových technologií a bezpečnostních opatření nebo o administrativní aparát zajišťující úřední agendu, tj. přípravu prováděcích právních předpisů, vydávání individuálních právních aktů, běžnou úřední komunikaci, komunikaci s veřejností, realizaci oficiálních mezinárodních vztahů apod.

Obecně lze tedy říci, že varianty počítající s aktivním přístupem státu i soukromého sektoru, které spočívají v rozšíření chráněného kyberprostoru a posílení zabezpečení sítí a informačních systémů jsou nedílně spjaty s vyšší mírou technické a organizační náročnosti, kterou je však třeba nutno posuzovat proporcionálně k možným následkům kybernetických bezpečnostních incidentů.

3.2 Náklady

3.2.1 Nulová varianta (bez specifické právní regulace)

U této varianty je struktura předpokládaných nákladů následující:

- Náklady na pořízení a provádění bezpečnostních opatření a plnění dalších povinností – soukromý sektor – uplatněním této varianty by nevznikla žádná skupina nově regulovaných subjektů, které by musely plnit povinnost podle zákona o kybernetické bezpečnosti. Nevznikly by tedy ani žádné nové

náklady na zavádění bezpečnostních opatření a hlášení kybernetických bezpečnostních incidentů, popřípadě náklady spojené s plněním dalších povinností.

- Náklady na pořízení a provádění bezpečnostních opatření a plnění dalších povinností – veřejný sektor – informační systémy veřejného sektoru jsou již z velké míry regulovány podle současného nastavení zákona o kybernetické bezpečnosti. Neprovedením transpozice by nevznikly žádné nově regulované subjekty v rámci státní správy a nedošlo by tudíž ke vzniku nově vynaložených nákladů.

- Náklady na personální obsazení příslušných pozic zahrnující i požadavky na vývoj pracovního trhu a vzdělávání – soukromý sektor – vzhledem k absenci nově regulovaných subjektů by nevznikly další požadavky na obsazení nově vznikajících pozic.

- Náklady na zřízení a provoz dohledových pracovišť – vzhledem k tomu, že by nebyly nově regulovány žádné další subjekty, nebylo by nutné rozšiřovat působnost ani kapacity dohledových pracovišť.

- Náklady na rozšíření národních schopností a kapacit – nebyly by nově vytvářeny žádné pracovní pozice, ani by nebyla rozšiřována působnost orgánů odpovědných za výkon státní správy v oblasti kybernetické bezpečnosti.

K uvedenému výčtu je třeba na straně nákladů připočíst všechny výše označené negativní společenské dopady plynoucí ze skutečnosti, že stát rezignuje na transpozici směrnice a odstranění nedostatků současné právní úpravy.

3.2.2 Varianta Ia - spolupráce s osobami soukromého práva

U této varianty je struktura předpokládaných nákladů následující:

- Pořízení, respektive provádění příslušných bezpečnostních opatření a plnění dalších povinností – soukromý sektor – tyto náklady se realizují již z velké část podle zákona o kybernetické bezpečnosti. Vzhledem k založení povinnosti aplikace bezpečnostních opatření, by tato varianta znamenala pro nově regulované subjekty náklady na pořízení bezpečnostních opatření a jejich dokumentaci. Zároveň by znamenala náklady na plnění povinnosti hlášení kybernetických bezpečnostních incidentů. U většiny osob soukromého práva by však znamenala jen marginální nutnost investic, neboť bezpečnostně exponované osoby soukromého práva již příslušné investice realizovaly – jediné dodatečné náklady tedy ve většině případů souvisejí s napojením těchto opatření na dohledová pracoviště.

- Pořízení, respektive provádění příslušných bezpečnostních opatření a plnění dalších povinností – veřejný sektor – vzhledem k založení povinnosti aplikace bezpečnostních opatření, by tato varianta znamenala náklady na pořízení bezpečnostních opatření, jejich dokumentaci a hlášení kybernetických bezpečnostních incidentů. Významné informační systémy a prvky kritické informační infrastruktury provozované státními orgány jsou však již regulovány podle zákona o kybernetické bezpečnosti. Požadavky směrnice jsou tak již ze značné části ve veřejném sektoru plněny.

- Náklady na personální obsazení příslušných pozic zahrnující i požadavky na vývoj pracovního trhu a vzdělávání – soukromý sektor – tato varianta by znamenala tlak na vytváření nových pracovních pozic a ovlivnila by poptávku po kvalifikovaných zaměstnancích na pracovním trhu, kterých je v současné době nedostatek. Problém vzdělávání odborníků v oblasti kybernetické bezpečnosti je však již řešen koncepčními materiály, jako je Strategie kybernetické bezpečnosti ČR 2015-2020.

- Náklady na zřízení a provoz dohledových pracovišť – centrální dohledová pracoviště již plní úkoly na základě zákona o kybernetické bezpečnosti. Při aplikaci této varianty by jejich úkoly zůstaly téměř nezměněny, pouze by jejich působnost byla rozšířena na nově regulované subjekty, což by znamenalo nárůst pracovní zátěže a požadavky na rozšíření pracovních pozic. Rovněž by mohly vzniknout i náklady na prostory a na technické a materiální vybavení. Oproti následující variantě by tyto náklady byly však nižší díky omezenému rozsahu činností dohledových pracovišť a jejich vzájemné spolupráci. Směrnice rovněž požaduje zavést v rámci dohledových pracovišť službu 24/7, což znamená další navýšení rozpočtu dohledových pracovišť, aby byly pokryty i příplatky za noční a víkendové služby.

- Náklady na rozšíření národních schopností a kapacit – jednalo by se zejména o náklady spojené s rozšířením působnosti orgánů odpovědných za výkon státní správy v oblasti kybernetické bezpečnosti a dohledových pracovišť. Tyto náklady by zahrnovaly navýšení pracovních míst, případně další náklady, jako jsou náklady na prostory a na technické a materiální vybavení. Rovněž by tyto náklady obsahovaly kontinuální vzdělávání pracovníků.

Tato varianta počítá se zvýšenou mírou nákladů i technicko-organizační náročnosti. Tyto náklady jsou však přiměřené vůči škodám, které by mohly vzniknout neprovedením transpozice směrnice a neodstraněním legislativních nedostatků současné právní úpravy.

3.2.3 Varianta Ib – výlučná a přímá státní regulace

- Pořízení, respektive provádění příslušných bezpečnostních opatření a plnění dalších povinností – soukromý sektor – vzhledem k založení povinnosti zavádění bezpečnostních opatření, by tato varianta způsobila u nově regulovaných subjektů nutnost vynaložení nákladů na pořízení bezpečnostních opatření a na plnění dalších povinností.

- Pořízení, respektive provádění příslušných bezpečnostních opatření a plnění dalších povinností – veřejný sektor – ačkoli by v případě této varianty vznikly ve veřejném sektoru náklady na pořízení a provádění bezpečnostních opatření a plnění dalších povinností, jednalo by se v tomto ohledu o náklady spíše marginální, protože značná část povinností stanovených směrnicí je již ve veřejném sektoru plněna na základě zákona o kybernetické bezpečnosti.

- Náklady na personální obsazení příslušných pozic zahrnující i požadavky na vývoj pracovního trhu a vzdělávání – soukromý sektor – tato varianta by obdobně jako varianta předešlá znamenala tlak na vytváření nových pracovních pozic a ovlivnila by poptávku po kvalifikovaných zaměstnancích na pracovním trhu, kterých je v současné době nedostatek.

Náklady na zřízení a provoz dohledových pracovišť - centrální dohledová pracoviště již plní úkoly na základě zákona o kybernetické bezpečnosti. V případě národního CERT by byl zachován současný

status quo, u vládního CERT by však došlo ke značnému rozšíření jeho constituency, což by mohlo vést až ke zhoršení jím poskytovaných služeb. Tato varianta by tak znamenala výrazný nárůst pracovní zátěže pro vládní CERT, což by implikovalo velké požadavky na rozšíření pracovních pozic. Rovněž by vznikly i vysoké náklady na prostory a na technické a materiální vybavení. Směrnice rovněž požaduje zavést v rámci dohledových pracovišť službu 24/7, což znamená další navýšení rozpočtu, aby byly pokryty i příplatky za noční a víkendové služby.

Náklady na rozšíření národních schopností a kapacit - jednalo by se zejména o náklady spojené s rozšířením působnosti orgánů odpovědných za výkon státní správy v oblasti kybernetické bezpečnosti a dohledového pracoviště vládní CERT. Tyto náklady by zahrnovaly navýšení pracovních míst, případně další náklady, jako jsou náklady na prostory a na technické a materiální vybavení. Rovněž by tyto náklady obsahovaly kontinuální vzdělávání pracovníků.

K výše uvedenému rozpisu je třeba ještě doplnit rizika vyplývající z dané varianty pro reputaci ČR a jejích státních orgánů.

3.2.4 Varianta IIa – striktní následování směrnice NIS

U této varianty je struktura předpokládaných nákladů následující:

- Pořízení, respektive provádění příslušných bezpečnostních opatření a plnění dalších povinností – soukromý sektor – u části subjektů regulovaných podle současné právní úpravy zákona o kybernetické bezpečnosti by došlo ke zrušení všech povinností, což by však v důsledku mohlo vést ke správním a soudním sporům těchto subjektů se státem, protože tyto subjekty by byly v krátké době nuceny zavést nákladná bezpečnostní opatření a personálně a administrativně zabezpečit plnění dalších povinností, a následně by byly tyto jejich zákonné povinnosti zrušeny. Část subjektů, doposud neregulovaná podle zákona o kybernetické bezpečnosti (zdravotnictví, digitální služby), by však musela nově tyto povinnosti začít plnit. Lze tedy očekávat, že úroveň nákladů by se nijak výrazně nezměnila oproti současné právní úpravě.

- Pořízení, respektive provádění příslušných bezpečnostních opatření a plnění dalších povinností – veřejný sektor – u většiny orgánů veřejné moci regulovaných podle současné právní úpravy zákona o kybernetické bezpečnosti by došlo ke zrušení všech povinností, což by však bylo z hlediska již vynaložených nákladů neefektivní a nehospodárné.

- Náklady na personální obsazení příslušných pozic zahrnující i požadavky na vývoj pracovního trhu a vzdělávání – soukromý sektor – u této varianty lze očekávat obdobný tlak na personální obsazení příslušných pozic, jako je v současnosti. Vzhledem k tomu, že směrnice reguluje zásadní odvětví, jako je energetika nebo doprava, a zároveň bude regulovat nově doposud nezahrnutá odvětví, např. zdravotnictví nebo digitální služby, nedá se očekávat, že by došlo k výraznému poklesu poptávky po kvalifikovaných zaměstnancích. To znamená, že i z hlediska vzdělávání zde bude nutno vytvářet nové obory, které se této problematice budou intenzivně věnovat.

- Náklady na zřízení a provoz dohledových pracovišť – dohledová pracoviště jsou již zřízena podle zákona o kybernetické bezpečnosti. Vzhledem ke srovnatelnému rozsahu působnosti zákona

o kybernetické bezpečnosti a směrnice lze očekávat, že by administrativní, finanční i personální požadavky na provoz dohledových pracovišť zůstaly obdobné.

- Náklady na rozšíření národních schopností a kapacit – vzhledem ke srovnatelnému rozsahu působnosti zákona o kybernetické bezpečnosti a směrnice lze očekávat, že by administrativní, finanční i personální požadavky národních kapacit zůstaly obdobné.

Tato varianta by vzhledem ke srovnatelnému rozsahu působnosti zákona o kybernetické bezpečnosti a směrnice nevedla k žádnému výraznému zvýšení nákladů. V oblasti státní správy by naopak mohlo dojít k jejich snížení vzhledem ke zrušení povinnosti naplňovat požadavky zákona o kybernetické bezpečnosti pro orgány veřejné moci. Obecně by se však jednalo o velmi neefektivní a nehospodárné řešení vyvolávající právní nejistotu a zhoršující podnikatelské prostředí v ČR. Popřípadě by mohlo docházet až ke správním nebo soudním sporům. K uvedenému výčtu je navíc třeba na straně nákladů připočíst všechny výše označené negativní společenské dopady plynoucí ze skutečnosti, že stát výrazně zasáhne do již nastaveného a fungujícího systému zajišťování kybernetické bezpečnosti.

3.2.5 Varianta IIb – doplnění zákona o kybernetické bezpečnosti o požadavky směrnice NIS

- Pořízení, respektive provádění příslušných bezpečnostních opatření a plnění dalších povinností – soukromý sektor – tato varianta by vedla ke vzniku nákladů nově regulovaným subjektům. Jednalo by se zejména o náklady na zavádění bezpečnostních opatření a plnění dalších povinností.

- Pořízení, respektive provádění příslušných bezpečnostních opatření a plnění dalších povinností – veřejný sektor – ačkoli by v případě této varianty vznikly ve veřejném sektoru náklady na pořízení a provádění bezpečnostních opatření a plnění dalších povinností, jednalo by se v tomto ohledu o náklady spíše marginální, protože značná část povinností stanovených směrnicí je již ve veřejném sektoru plněna na základě zákona o kybernetické bezpečnosti.

- Náklady na personální obsazení příslušných pozic zahrnující i požadavky na vývoj pracovního trhu a vzdělávání – soukromý sektor – tato varianta by vedla k vytváření pracovních pozic u nově regulovaných subjektů. Důsledkem by tedy bylo i zvýšení poptávky po kvalifikovaných pracovnících na trhu práce. Zároveň však lze konstatovat, že velká část firem již z podstaty své činnosti bezpečnostní opatření uplatňuje. Nová by tedy pro ně byla zejména povinnost ohlašovat kybernetické bezpečnostní incidenty a vést bezpečnostní dokumentaci.

- Náklady na zřízení a provoz dohledových pracovišť – dohledová pracoviště jsou již zřízena podle zákona o kybernetické bezpečnosti. Vzhledem k nárůstu subjektů spadajících do působnosti dohledových pracovišť by musela být dohledová pracoviště rozšířena, což by znamenalo další náklady na nové prostory, pracovní pozice a technické a materiální vybavení. Směrnice rovněž požaduje zavést v rámci dohledových pracovišť službu 24/7, což znamená další navýšení rozpočtu dohledových pracovišť, aby byly pokryty i příplatky za noční a víkendové služby.

- Náklady na rozšíření národních schopností a kapacit – vzhledem k nárůstu subjektů spadajících do působnosti zákona o kybernetické bezpečnosti by musely být národní schopnosti a kapacity rozšířeny, což by znamenalo další náklady na nové prostory, pracovní pozice a technické a materiální

vybavení.

Tato varianta počítá se zvýšenou mírou nákladů i technicko-organizační náročnosti. Vzhledem k charakteru a významnosti regulovaných subjektů se zdají být však výše uvedené náklady odůvodněné a přiměřené. Na druhou stranu totiž bude zejména implementací bezpečnostních opatření minimalizováno riziko kybernetických bezpečnostních incidentů, které by jinak mohly mít dalekosáhlé dopady. Obdobně to platí i pro náklady na rozšíření národních kapacit.

3.2.6 Varianta IIc – doplnění zákona o kybernetické bezpečnosti nad rámec požadavků směrnice NIS

- Pořízení, respektive provádění příslušných bezpečnostních opatření a plnění dalších povinností – soukromý sektor – tato varianta by vedla ke vzniku nákladů nově regulovaným subjektům. Jednalo by se zejména o náklady na zavádění bezpečnostních opatření spojené s administrativními náklady.

- Pořízení, respektive provádění příslušných bezpečnostních opatření a plnění dalších povinností – veřejný sektor – ačkoli by v případě této varianty vznikly ve veřejném sektoru náklady na pořízení a provádění bezpečnostních opatření a plnění dalších povinností, jednalo by se v tomto ohledu o náklady spíše marginální, protože značná část povinností stanovených směrnicí je již ve veřejném sektoru plněna na základě zákona o kybernetické bezpečnosti.

- Náklady na personální obsazení příslušných pozic zahrnující i požadavky na vývoj pracovního trhu a vzdělávání – soukromý sektor – tato varianta by vedla k vytváření pracovních pozic u nově regulovaných subjektů. Důsledkem by tedy bylo i zvýšení poptávky po kvalifikovaných pracovnících na trhu práce. Zároveň však lze konstatovat, že velká část firem již z podstaty své činnosti bezpečnostní opatření uplatňuje. Nová by tedy pro ně byla zejména povinnost ohlašovat kybernetické bezpečnostní incidenty a vést bezpečnostní dokumentaci.

- Náklady na zřízení a provoz dohledových pracovišť – dohledová pracoviště jsou již zřízena podle zákona o kybernetické bezpečnosti. Vzhledem k nárůstu subjektů spadajících do působnosti dohledových pracovišť by musela být dohledová pracoviště rozšířena, což by znamenalo další náklady na nové prostory, pracovní pozice a technické a materiální vybavení. Směrnice rovněž požaduje zavést v rámci dohledových pracovišť službu 24/7, což znamená další navýšení rozpočtu dohledových pracovišť, aby byly pokryty i příplatky za noční a víkendové služby.

- Náklady na rozšíření národních schopností a kapacit – vzhledem k nárůstu subjektů spadajících do působnosti zákona o kybernetické bezpečnosti by musely být národní schopnosti a kapacity rozšířeny, což by znamenalo další náklady na nové prostory, pracovní pozice a technické a materiální vybavení.

Tato varianta počítá se zvýšenou mírou nákladů i technicko-organizační náročnosti. Vzhledem k charakteru a významnosti regulovaných subjektů se zdají být však výše uvedené náklady odůvodněné a přiměřené. Na druhou stranu totiž bude zejména implementací bezpečnostních opatření minimalizováno riziko kybernetických bezpečnostních incidentů, které by jinak mohly mít dalekosáhlé dopady. Obdobně to platí i pro náklady na rozšíření národních kapacit.

3.2.7 Přehled nákladů jednotlivých variant

V následující tabulce jsou označeny náklady, které byly identifikovány pro jednotlivé varianty.

Legenda:

A - ano, s těmito náklady je u dané varianty možno počítat
N - ne, tyto náklady se u dané varianty nepředpokládají
Č - tyto náklady se u dané varianty předpokládají pouze zčásti, a to v závislosti na její osobní působnosti

Kritéria	Var-0	Var-Ia	Var-Ib	Var-IIa	Var-IIb	Var-IIc
Náklady na pořízení, respektive provádění bezpečnostních opatření a plnění dalších povinností – soukromý sektor	**N**	**A**	**A**	**Č**	**A**	**A**
Náklady na pořízení, respektive provádění bezpečnostních opatření a plnění dalších povinností – veřejný sektor	**N**	**Č**	**Č**	**N**	**Č**	**Č**
Náklady na personální obsazení příslušných pozic zahrnující i požadavky na vývoj pracovního trhu a vzdělávání – soukromý sektor	**N**	**A**	**A**	**Č**	**A**	**A**
Náklady na zřízení a provoz dohledových pracovišť	**N**	**A**	**A**	**N**	**A**	**A**
Náklady na rozšíření národních schopností a kapacit	**N**	**A**	**A**	**N**	**A**	**A**

3.3 Přínosy

V následující tabulce jsou označeny přínosy, které byly identifikovány pro jednotlivé varianty.

Legenda:

A – ano, s tímto přínosem je u dané varianty možno počítat
N – ne, tento přínos se u dané varianty nepředpokládá
Č – tento přínos se u dané varianty předpokládá pouze zčásti

Kritéria	Var-0	Var-Ia	Var-Ib	Var-IIa	Var-IIb	Var-IIc
Zvýšení míry zabezpečení významných nebo dokonce kriticky důležitých společenských funkcionalit	**N**	**A**	**A**	**N**	**A**	**A**
Ochrana relevantní části kyberprostoru v ČR a v EU	**Č**	**A**	**A**	**Č**	**A**	**A**
Omezení ekonomických škod jako důsledku kybernetických bezpečnostních incidentů	**Č**	**A**	**A**	**Č**	**A**	**A**
Zvýšení atraktivity České republiky pro zahraniční i tuzemské investory	**N**	**A**	**N**	**N**	**A**	**A**
Zlepšení českého podnikatelského prostředí a konkurenceschopnosti českých podnikatelů	**N**	**A**	**N**	**N**	**A**	**A**
Posílení důvěry spotřebitelů a obchodních partnerů českých podnikatelů	**N**	**A**	**N**	**N**	**A**	**A**
Splnění povinností vyplývajících pro ČR z mezinárodního práva a práva EU (transpoziční povinnost, podpora harmonizace i vnitřního trhu EU)	**N**	**A**	**A**	**A**	**A**	**A**
Ochrana základních práv a svobod (práva na informační sebeurčení, práva na svobodu projevu a dalších práv)	**Č**	**A**	**A**	**Č**	**A**	**A**
Posílení reputace státu a jeho institucí u odborné veřejnosti a ochrana důvěry občanů	**N**	**A**	**N**	**N**	**A**	**A**
Posílení mezinárodní reputace ČR a dodržení mezinárodně právních závazků	**Č/N**	**A**	**Č/N**	**Č/N**	**A**	**A**
Zohlednění celosvětové bezpečnostní situace a nově vznikajících hrozeb	**Č/N**	**A**	**A**	**Č/N**	**A**	**A**

3.4 Vyhodnocení nákladů a přínosů variant

Poměr nákladů a přínosů lze u jednotlivých variant zhodnotit následovně:

- Nulová varianta (bez specifické právní regulace) – tato varianta nepočítá s žádnými náklady. Na druhou stranu ale nepřináší žádné přínosy, které indukuje aktivní činnost státu (zvýšení ochrany základních práv, zvýšení ochrany kyberprostoru, podpora investic apod.). Zároveň by tato varianta

jako jediná vedla k nesplnění transpoziční povinnosti, tím pádem k nedodržení závazků ČR stanovených evropským primárním právem, čímž by byla ČR vystavena riziku finančního postihu ze strany institucí EU a ohrožení své mezinárodní reputace.

- Varianta Ia (spolupráce s osobami soukromého práva) - tato varianta generuje největší počet přínosů. Její nákladovost je omezena tím, že je funkčně založena na spolupráci se soukromoprávním dohledovým pracovištěm a striktní zákonné povinnosti ukládá jen v absolutně nezbytném rozsahu k dosažení jejího účelu. Struktura nákladů na plnění povinností předpokládaných navrhovanou variantou je dána strukturou základních ochranných institutů. Nákladovost u různých typů subjektů pak je dána jejich zařazením do zákonných kategorií. Náklady přímo související s aplikací varianty budou u podstatné části z nich minimální nebo nulové – tato varianta totiž zavádí takový standard bezpečnostních opatření, který značná část správců nebo provozovatelů sítí a informačních systémů již dnes aplikuje. Navíc lze konstatovat, že tyto náklady jsou přiměřené vzhledem ke škodám, které by mohly vzniknout následkem kybernetického bezpečnostního incidentu.

- Varianta Ib (výlučná a přímá státní regulace) – tato varianta je vedle vysokých nákladů na výkon zákonných pravomocí orgány veřejné moci problematická též z hlediska definice rozsahu zákonných povinností a jejich svázáním s působností veřejnoprávního dohledového pracoviště. V situaci, kdy mezi osobami soukromého práva v sektoru ICT panuje určitá nedůvěra k fungování orgánů veřejné moci, by implementace této varianty kromě uvedených nákladů přinesla též riziko zvýšení společenského napětí.

- Varianta IIa (striktní následování směrnice NIS) - tato varianta by vzhledem ke srovnatelnému rozsahu působnosti zákona o kybernetické bezpečnosti a směrnice nevedla k žádnému výraznému zvýšení nákladů. V oblasti státní správy by naopak mohlo dojít k jejich snížení vzhledem ke zrušení povinnosti naplňovat požadavky zákona o kybernetické bezpečnosti pro orgány veřejné moci. Obecně by se však jednalo o velmi neefektivní a nehospodárné řešení vyvolávající právní nejistotu a zhoršující podnikatelské prostředí v ČR. Popřípadě by mohlo docházet až ke správním nebo soudním sporům. K uvedenému výčtu je navíc třeba na straně nákladů připočíst všechny výše označené negativní společenské dopady plynoucí ze skutečnosti, že stát výrazně zasáhne do již nastaveného a fungujícího systému zajišťování kybernetické bezpečnosti.

- Varianta IIb (doplnění zákona o kybernetické bezpečnosti o požadavky směrnice) - tato varianta počítá se zvýšenou mírou nákladů, které jsou však vzhledem k charakteru a významnosti regulovaných subjektů odůvodněné a přiměřené. Implementací bezpečnostních opatření a zapojením nově regulovaných subjektů do systému sdílení informací bude totiž minimalizováno riziko kybernetických bezpečnostních incidentů, které by jinak mohly mít dalekosáhlé dopady. Obecně by tato varianta vedla k posílení zabezpečení českého kyberprostoru i zlepšení podnikatelského prostředí.

- Varianta IIc (doplnění zákona o kybernetické bezpečnosti nad rámec požadavků směrnice) – tato varianta počítá s obdobnými náklady jako varianta IIb (tj. náklady na vzdělávání pracovníků, vytváření nových pracovních míst, zavádění bezpečnostních opatření a rozšiřování národních kapacit). Vzhledem však ke sledovanému cíli, kterým je minimalizace bezpečnostních rizik, jsou tyto náklady přiměřené a odůvodněné. Na druhou stranu bude totiž plněním povinností zabráněno ve většině

případů vzniku kybernetických bezpečnostních incidentů, popřípadě vzniku masivních škod následkem takovýchto incidentů. Tím bude posílena reputace ČR a zvýšena důvěryhodnost a zlepšena konkurenceschopnost českého podnikatelského prostředí. Odstraněním stávajících legislativních mezer navíc dojde ke zlepšení celého systému zajišťování kybernetické bezpečnosti jako takové.

Vzhledem k výše uvedenému je za nejvhodnější řešení předkladatelem považováno použití variant Ia a IIc, tj. doplnění zákona o kybernetické bezpečnosti nad rámec požadavků směrnice a výkon působnosti v oblasti kybernetické bezpečnosti ve spolupráci s osobami soukromého práva.

Z výše uvedeného plyne, že náklady na straně povinných subjektů lze rozdělit na náklady související se zavedením bezpečnostních opatření, které zahrnují mimo jiné náklady související s detekcí kybernetických bezpečnostních událostí a s hlášením kybernetických bezpečnostních incidentů, a náklady spojené s prováděním opatření. Úroveň výdajů spojených s povinností zavést bezpečnostní opatření v minimálním zákonném standardu se bude odvíjet od zařazení subjektů do nově zaváděných zákonných kategorií.

U provozovatelů základních služeb budou vznikat náklady související s hlášením významného dopadu na kontinuitu poskytování základní služby, hlášením kontaktních údajů a informováním správců a provozovatelů informačních systémů základních služeb. Tyto náklady budou provozovateli základní služby vznikat tehdy, není-li zároveň správcem informačního systému základní služby.

U správců a provozovatelů informačních systémů základních služeb půjde o náklady související s plněním povinnosti aplikovat standardní úroveň bezpečnostních opatření, povinnosti detekovat kybernetické bezpečnostní události, povinnosti hlásit kybernetické bezpečnostní incidenty, povinnosti provádět opatření vydaná NBÚ, případně další povinnosti uložené zákonem.

Náklady související s přípravou na výskyt mimořádné situace, tj. stavu kybernetického nebezpečí, kdy budou mít správci nebo provozovatelé informačních systémů základních služeb, povinnost reagovat na reaktivní opatření vydané NBÚ, lze jen velmi těžko odhadnout – je totiž zákonem ponecháno na jejich vlastním uvážení, jakým způsobem upraví svoji schopnost dostát za stavu kybernetického nebezpečí požadavkům opatření. Zákon v tomto směru nestanoví ani povinnost zpracovávat při stavu kybernetického nebezpečí např. krizové plány a ponechává subjektům v této kategorii prakticky úplnou volnost v rozhodování ohledně mimořádných postupů, což umožní v řadě případů snížit tyto marginální náklady na úplně minimum.

U poskytovatelů digitálních služeb půjde bezprostředně pouze o náklady související s oznámením kontaktních údajů národnímu CERT (tyto náklady jsou prakticky bezvýznamné) a se zaváděním přiměřených bezpečnostních opatření. Vzhledem k doporučenému charakteru bezpečnostních opatření však nelze u těchto subjektů odhadnout přesné náklady. Je ale možno konstatovat, že míra zabezpečení je obecně u těchto subjektů vysoká. Vysoké zabezpečení sítí a informačních systémů je totiž jedním ze základních předpokladů jejich fungování a důvěryhodnosti. Zlepšením kvality jejich služeb tak lze očekávat i nárůst jejich tržeb, což v současné době znamená důležitý moment v rozvoji

digitální ekonomiky.[33] Navíc, aby bylo zabráněno nepřiměřenému zatížení poskytovatelů digitálních služeb, jsou ze zákonných povinností vyloučeny mikropodniky a malé podniky ve smyslu doporučení Komise č. 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků.

Navrhovaná varianta bude mít dále dopad na státní rozpočet, neboť v souvislosti s rozšířením působnosti zákona o kybernetické bezpečnosti dojde k navýšení funkčních míst, jakož i k navýšení rozpočtu NBÚ. S takovýmto navyšováním pracovních mít je však v současné době již počítáno, přičemž vláda ve svém usnesení ze dne 1. července 2015 č. 520 schválila posílení kapacity NBÚ v oblasti kybernetické bezpečnosti o 8 funkčních míst v roce 2016, o 8 funkčních míst v roce 2017 a o 8 funkčních mít v roce 2018 a zvýšení rozpočtu kapitoly NBÚ o 48,9 mi. Kč v roce 2016, o 49 mil. Kč v roce 2017 a o 50 mil. Kč v roce 2018.

Lze odhadovat, že další dopady na státní rozpočet budou již menšího rozsahu. Orgány státní správy jsou totiž v současné době regulovány jako správci systémů kritické informační infrastruktury nebo významných informačních systémů.

Předpokládá se, že tato varianta bude mít tedy zejména dopad na podnikatelské prostředí, a to s ohledem na stanovení nových povinností provozovatelům základních služeb, správcům a provozovatelům informačních systémů základních služeb a poskytovatelům digitálních služeb. Z průzkumu provedeného mezi již regulovanými orgány a osobami vyplynulo, že průměrné náklady na zavádění bezpečnostních opatření pro jeden informační systém byly asi 1,5 mil. Kč[34]. Na základě dalšího průzkumu provedeného mezi členy pracovní skupiny II[35] bylo zjištěno, že při započítání dalších nákladů, jako jsou náklady na personální zajištění, náklady na investice a dále náklady na samotný provoz lze předpokládat, že tyto náklady mohou v průměru vyšplhat až na 24 mil Kč na jeden regulovaný subjekt. Je však nutno si uvědomit, že tato výše nákladů je závislá na počtu využívaných informačních systémů a současném stavu jejich zabezpečení, přičemž z uvedeného dotazníkového šetření bylo zjištěno, že toto zabezpečení je v průměru hodnoceno na velmi vysoké úrovni a subjekty ze značné části již bezpečnostní opatření provádějí. Vyšší náklady však mohou vzniknout v sektorech, které doposud nebyly předmětem žádné regulace a u kterých není na zabezpečení informačních systémů kladen velký důraz (např. zdravotnictví). Návrh tedy vychází z premisy, že dotčené subjekty již uvažovaná bezpečnostní opatření z velké části používají a náklady pokryjí z finančních prostředků vynakládaných na ICT. Dalším způsobem financování těchto nákladů je možné čerpáním finančních prostředků z fondů Evropské unie.

Vzhledem k tomu, že navrhovaná právní úprava počítá s novými povinnostmi pouze ve vztahu k provozovatelům základních služeb, správcům a provozovatelům informačních systémů základních služeb a poskytovatelům digitálních služeb, nebude mít její zavedení žádný dopad na finanční situaci sociálně slabých skupin obyvatelstva, národnostních menšin nebo osob se zdravotním postižením.

[33] Dopad internetové ekonomiky, tedy činností přímo spojených s internetem, odpovídá zhruba 3 % HDP. Je však nutné uvést, že digitální technologie mají velmi průřezový charakter a ovlivňují tím celou řadu dalších odvětví. Pokud vezmeme v potaz toto komplexní pojetí, odhaduje se, že fenomén internetu se do HDP promítá téměř 10 %. Srov. Akční plán pro rozvoj digitálního trhu

[34] Viz kapitola 7.6 Oslovení již regulovaných subjektů.

[35] Viz kapitola 7. 4 Pracovní skupina II.

4. Návrh řešení

4.1 Stanovení pořadí variant a výběr nejvhodnějšího řešení

Shora uvedených šest základních variant řešení se vzájemně liší mírou a rozsahem právní regulace a mírou ingerence státních orgánů. Analýza zahrnula též krajní varianty ponechání současného stavu regulace kybernetické bezpečnosti a na druhou stranu variantu striktní transpozice směrnice do národního právního řádu.

K výběru nejvhodnějšího řešení dospěl navrhovatel především komplexní analýzou předpokládaných dopadů jednotlivých variant řešení, a to zaprvé z hlediska bezpečnostního, které zahrnuje zejména možné dopady na zabezpečení sítí a informačních systémů a relevantní část kyberprostoru, která těmto požadavkům bude podléhat, zadruhé z hlediska ekonomického, zohledňujícího zejména následky pro ekonomiku ČR a pro regulované subjekty a vliv regulace na postavení českých podnikatelů na národním i mezinárodním trhu, a zatřetí z hlediska politicko-právního, které se zaměřuje na splnění závazků vyplývajících pro ČR z evropského i mezinárodního práva, stejně jako na vliv navrhované právní regulace na pověst ČR a přizpůsobení stávající právní regulace současným závažným bezpečnostním rizikům.

Výběr nejvhodnější varianty je tedy veden především racionálním zhodnocením potřeb, možností a závazků ČR, jakož i aktuálního stavu vědění v oboru práva informačních a komunikačních technologií, informatiky a bezpečnostních studií.

Výběr nejvhodnějšího řešení podle míry zapojení subjektů vedle shora uvedených faktorů zohledňuje i vlastnictví a správu informačních a komunikačních systémů, přičemž jejich značná část je vlastněna a spravována osobami soukromého práva. Tyto osoby mají zpravidla velmi solidní zkušenosti s jejich provozováním a mají též odpovídající technické kompetence a faktické možnosti aktivně se starat o bezpečnost vlastních systémů, služeb a sítí. Řešení kybernetické bezpečnosti prostřednictvím specifických povinností adresovaných těmto osobám, resp. prostřednictvím spolupráce a vzájemné podpory soukromého sektoru a státu se jeví jako ideální. Z tohoto důvodu je doporučenou variantou vybranou k legislativnímu řešení varianta spolupráce s osobami soukromého práva. Varianta výlučné a přímé státní regulace je v tomto ohledu krajně nevhodná, protože by značně zasáhla již do nastaveného a fungujícího modelu spolupráce vládního a národního CERT, přičemž každých z těchto týmů má vymezený okruh subjektů spadajících pod jejich působnost. Z hlediska organizačního by si navíc tato varianta vyžádala masivní veřejné investice do personálního aparátu, který by takovou regulaci implementoval, kontroloval a sankcionoval.

Mezi variantami dělenými podle působnosti právní úpravy je možno reálně zvažovat použití varianty doplnění režimu zákona o kybernetické bezpečnosti o požadavky směrnice, stejně jako použití varianty doplnění režimu zákona o kybernetické bezpečnosti nad rámec požadavků směrnice. Prvá z uvedených variant by plně stačila ke splnění transpoziční povinnosti, nezohledňovala by však nijak zjištěná bílá místa současné právní regulace ani nejnovější vývoj v oblasti bezpečnosti ICT. Rovněž není možné opomenout, že důležitým faktorem je současná světová bezpečností situace, v rámci níž se stávají útoky na klíčové sítě a informační systémy běžným prostředkem vedení agresivní propagandy nebo dokonce prostředkem pro podporu ozbrojených konfliktů. ČR si již několik let na

mezinárodní scéně buduje pověst spolehlivého a progresivního partnera a přinejmenším na evropské úrovni patří mezi lídry v této oblasti. Vzhledem k tomu, že tento současný stav by měl být zachován, byla zhodnocena navrhovatelem jako nejvhodnější druhá z uvedených variant, která nad rámec nutné transpozice směrnice provede i nezbytné úpravy stávajícího režimu vedoucí ke zlepšení nastavení celého systému kybernetické bezpečnosti v ČR.

5. Implementace doporučené varianty a vynucování

Jako nejvhodnější variantou se tedy jeví zajištění kybernetické bezpečnosti ČR formou novely již účinného zákona o kybernetické bezpečnosti. Tato novela bude navazovat na stávající režim a bude jej doplňovat o nově regulované subjekty – provozovatele základních služeb, správce a provozovatele informačních systémů základních služeb a poskytovatele digitálních služeb. S ohledem na smysl a účel regulace pak nelze tuto směrnici transponovat do jiného právního předpisu než do zákona o kybernetické bezpečnosti.

V tomto ohledu tedy bude stávající režim zákona o kybernetické bezpečnosti významně doplněn o subjekty, které poskytují klíčové základní služby, přičemž jejich důležitost není posuzována na státní úrovni, jako je tomu u kritické informační infrastruktury, ale spíše na úrovni regionální, což současná právní úprava nepokrývá. V případě, že provozovatelé základních služeb nejsou identičtí se správci nebo provozovateli informačních systémů základních služeb, vztahuje se plnění zákonných povinností především na správce a provozovatele informačních systémů základních služeb, ačkoli nebudou předmětem určování. Klíčové je v tomto ohledu zejména postavení správce informačního systému základní služby. Druhá skupina subjektů, poskytovatelé digitálních služeb, nebyla doposud předmětem žádné právní regulace. Vezmeme-li však v potaz jejich rychle narůstající počet i význam, není možné tuto sféru digitální ekonomiky již nadále ignorovat. Právě naopak je nutné se začít zabývat jak jejich zákonným vymezením, tak i mírou regulace, kterou by měli být zatíženi. Vzhledem k tomu, že se jedná o novou oblast, ukládá směrnice ČR zavést minimální povinnosti nutné pro zajištění bezpečnosti sítí a informačních systémů těchto subjektů, aby nedošlo ke zbytečnému ohrožení inovačního potenciálu a rozvoje této oblasti.

Zákon o kybernetické bezpečnosti tak bude doplněn o nový pojmový aparát a nové definice, z nichž některé však budou využívat pojmy z jiných právních předpisů (např. definice digitální služby). Nově regulovaným subjektům pak budou uloženy i specifické povinnosti. Pro provozovatele základních služeb, respektive správce a provozovatele informačních systémů základních služeb, i poskytovatele digitálních služeb stanoví směrnice zejména povinnost přijetí bezpečnostních opatření přiměřených vzhledem k míře existujících rizik, přijetí opatření předcházejících vzniku incidentů a hlášení významných kybernetických bezpečnostních incidentů. V oblasti kontroly pak mají povinné subjekty podle směrnice povinnost spolupracovat s národními orgány odpovědnými za kybernetickou bezpečnost a poskytovat jim nezbytné podklady.

S výkonem pravomocí příslušných orgánů souvisí i povinnost těchto subjektů hlásit kontaktní údaje. Správci a provozovatelé informačních systémů základních služeb budou dále ještě podléhat reaktivním a ochranným opatření, stejně jakou budou muset plnit povinnosti jim uložené za stavu kybernetického nebezpečí.

Naproti tomu budou poskytovatelé digitálních služeb obecně podléhat mírnější regulaci. Nebudou mít přesně nastavená bezpečnostní opatření a z hlediska vynucování budou podléhat pouze ex post kontrole. Vzhledem k jejich soukromoprávní povaze nebudou podléhat tyto subjekty pod dohledové pracoviště vládní CERT, který je organizační složkou NBÚ, nýbrž pod národní CERT, jehož úkoly jsou upraveny v § 17 zákona o kybernetické bezpečnosti. I toto ustanovení tedy musí být odpovídajícím způsobem doplněno. Na poskytovatele digitálních služeb se navíc nevztahuje stav kybernetického nebezpečí, protože to směrnice neukládá, přičemž ČR v tomto ohledu nemůže překročit míru opatření stanovenou evropskou regulací.

Jako orgán veřejné správy odpovědný za implementaci regulace je určen NBÚ, který je již v § 22 odst. 1 zákona o kybernetické bezpečnosti označen jako orgán odpovědný za výkon státní správy v oblasti kybernetické bezpečnosti, nestanoví-li zákon o kybernetické bezpečnosti jinak. Odstavec 2 tohoto paragrafu pak upravuje jednotlivé kompetence NBÚ. Vzhledem k požadavkům směrnice je však nutno tyto kompetence rozšířit. Směrnice totiž ukládá ČR povinnost vytvořit jednotné kontaktní místo, které má usnadnit přeshraniční spolupráci s dalšími členskými státy a postupovat souhrnnou zprávu o kybernetických bezpečnostních incidentech skupině pro spolupráci. Dále budou ve vztahu k nově regulovaným subjektům rozšířeny i rozhodovací, kontrolní a sankční povinnosti NBÚ, přičemž NBÚ bude určovat subjekty, které naplňují kritéria pro určení provozovatele základních služeb. Zároveň bude mít povinnost informovat veřejnost o významných kybernetických bezpečnostních incidentech, pokud je to ve veřejném zájmu.

Návrh zákona musí zohlednit i požadavky směrnice týkající se mezinárodní spolupráce mezi ČR, respektive NBÚ, a dalšími členskými státy a jejich příslušnými organizačními složkami. Tato spolupráce musí zahrnovat konzultace při určování provozovatelů základních služeb, jejichž služby mají přeshraniční dopad, a postupování informací o vzniklých významných kybernetických bezpečnostních incidentech. Dále je pak nutné zajištění účasti zástupců ČR v nově vytvořených unijních kooperačních strukturách, kterými jsou podle směrnice skupina pro spolupráci na strategické úrovni a síť CSIRT na operativní úrovni. Rovněž na národní úrovni bude posílena spolupráce mezi NBÚ a příslušnými orgány pro ochranu osobních údajů.

Pod působnost dohledového pracoviště vládní CERT, jehož úkoly jsou upraveny v § 20 zákona o kybernetické bezpečnosti, v současné době spadá kritická informační infrastruktura a významné informační systémy. Provozovatelé základních služeb a správci a provozovatelé informačních systémů základních služeb mají obdobný charakter jako tyto dvě uvedené skupiny a budou podléhat obdobným bezpečnostním požadavkům, z tohoto důvodu budou i oni spadat pod vládní CERT. Ustanovení § 20 tak bude muset být rozšířeno, aby odpovídalo požadavkům na zajištění bezpečnosti a řešení významných kybernetických bezpečnostních incidentů vzniklých u provozovatelů základních služeb nebo správců a provozovatelů informačních systémů základních služeb, přičemž vládní CERT bude těmto subjektům poskytovat potřebnou metodickou podporu a pomoc.

Nad rámec transpozice směrnice budou správci informačního nebo komunikačního systému kritické informační infrastruktury, správci významného informačního systému a správci a provozovatelé informačních systémů základních služeb povinni zachovávat mlčenlivost o jimi přijatých a prováděných bezpečnostních opatřeních (přičemž tato povinnost se vztahuje i na jejich zaměstnance). Konkrétní pravidla pro uplatňování této povinnosti budou uvedena v prováděcím

právním předpise k zákonu o kybernetické bezpečnosti. Dále pak budou správci kritické informační infrastruktury, správci významných informačních systémů a správci a provozovatelé informačních systémů základních služeb, kteří jsou zároveň orgánem veřejné moci, povinni ukládat svá data pouze v cloudových uložištích garantujících nepřetržitou fyzickou přístupnost jejich informací a dat. Nadto jsou navíc správcům informačních a komunikačních systémů kritické informační infastruktury a správcům významných informačních systémů uloženy informační povinnosti vůči provozovatelům informačních systémů a vůči subjektům zajišťujícím přímé připojení uvedených informačních nebo komunikačních systémů do sítě elektronických komunikací.

Povinnosti jsou tedy pro povinné orgány a osoby nastaveny následujícím způsobem:

- Povinnosti provozovatelů základních služeb a správců informačních systémů základních služeb – povinnosti vztahující se na provozovatele základních služeb jsou v případě, že se jedná o jeden subjekt, primárně plněny správci informačních systémů základních služeb. Pokud se však jedná o dva samostatné subjekty, musí správci informačních systémů základních služeb zavést a provádět bezpečnostní opatření a zachovávat o nich mlčenlivost; zajistit si ve smlouvě s poskytovatelem cloud computingových služeb možnost přístupu a kontroly informací a dat, které pro ně tento poskytovatel uchovává (platí pouze tehdy, jsou-li orgánem veřejné moci); detekovat kybernetické bezpečnostní události; hlásit významné kybernetické bezpečnostní incidenty; hlásit kontaktní údaje; provádět reaktivní a ochranná opatření vydaná NBÚ; plnit povinnosti uložené reaktivními opatřeními vydanými NBÚ za stavu kybernetického nebezpečí; poskytnout součinnost při kontrole NBÚ a odstranit nedostatky při ní zjištěné. Povinnosti provozovatelů základních služeb jsou v takovém případě omezené do té míry, aby byl zachován účel a smysl směrnice. Provozovatelé základních služeb tak musejí informovat správce nebo provozovatele informačního systému, na němž závisí základní služba, že byli určeni jakožto provozovatelé základní služby a že se na předmětného správce nebo provozovatele vztahují povinnosti stanovené zákonem o kybernetické bezpečnosti. Dále musí hlásit závažné dopady kybernetických bezpečnostních incidentů na poskytování základní služby, poskytovat kontaktní údaje a v případě veřejného zájmu jim může NBÚ nařídit, aby informovali veřejnost o probíhajícím kybernetickém bezpečnostním incidentu.

- Povinnosti provozovatelů informačních systémů základních služeb – v případě, že provozovatelé informačních systémů základních služeb nejsou zároveň jejich správci, vztahují se na ně obdobné povinnosti jako na správce informačních systémů základních služeb.

- Povinnost poskytovatelů digitálních služeb – zavést a provádět bezpečnostní opatření dle jejich uvážení, aby bylo dosaženo předepsaného cíle, hlásit významné kybernetické bezpečnostní incidenty, hlásit kontaktní údaje, poskytnout součinnost při kontrole NBÚ a odstranit nedostatky při ní zjištěné.

- Nové povinnosti správců informačních nebo komunikačních systémů kritické informační infrastruktury – zachovávat mlčenlivost o přijatých bezpečnostních opatřeních; v případě, že jsou orgánem veřejné moci, si ve smlouvě s poskytovatelem cloud computingových služeb zajistit možnost přístupu a kontroly k informacím a datům, které pro ně tento poskytovatel uchovává; informovat orgán nebo osobu zajišťující významnou síť o určení informačního nebo komunikačního systému jako prvku kritické informační infrastruktury; informovat provozovatele informačního nebo komunikačního systému o určení informačního nebo komunikačního systému jako prvku kritické

informační infrastruktury.

- Nové povinnosti správců významných informačních systémů – zachovávat mlčenlivost o přijatých bezpečnostních opatřeních; zajistit si ve smlouvě s poskytovatelem cloud computingových služeb možnost přístupu a kontroly k informacím a datům, které pro ně tento poskytovatel uchovává; informovat provozovatele informačního systému o identifikaci informačního systému jakožto významného informačního systému.

5.1 Vynucování

Kontrolní a sankční pravomoci ohledně plnění výše uvedených povinností náleží NBÚ. Vůči provozovatelům základních služeb a správcům a provozovatelům informačních systémů základních služeb má NBÚ kontrolní pravomoci ve stejném rozsahu, jako je tomu v případě správců informačních nebo komunikačních systémů kritické informační infrastruktury nebo významných informačních systémů. Vůči poskytovatelům digitálních služeb však může vykonávat NBÚ pouze kontrolní pravomoc ex post, a to v případě, že se dozvěděl o neplnění povinností, které jsou těmto subjektům uloženy zákonem o kybernetické bezpečnosti.

Kontrolní kompetence jsou upraveny v návaznosti na zákon č. 255/2012 Sb., o kontrole (kontrolní řád). Sankční aparát zahrnuje ukládání nápravných opatření a deliktní odpovědnost. Ustanovení týkající se správních deliktů byla rozšířena s ohledem na nově ukládané povinnosti. Rovněž byla navýšena maximální výše finanční sankce, která může být uložena. Stávající horní hranice, 100 tis. Kč, se ukázala být v praxi jako nedostatečná. Zavádění a dodržování bezpečnostních opatření je totiž finančně i administrativně náročný proces, jehož náklady se pohybují v řádech jednotek až desítek miliónů korun. Povinným subjektům by se tak za současné situace více mohlo vyplatit neplnění povinností a uhrazení uložených pokut, než zavádění a provádění bezpečnostních opatření. Navýšení horní hranice sankcí navíc odráží i požadavky směrnice, která ukládá členským státům povinnost stanovit sankce za porušení vnitrostátních právních předpisů, přičemž tyto sankce musí být účinné, přiměřené a odrazující.

Nad rámec výše uvedeného správního řízení budou uplatňovány i obecné trestně-právní předpisy (zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů, zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim, v znění pozdějších předpisů, a zákon č. 141/1961 Sb., o trestním řízení soudním (trestní řád), ve znění pozdějších předpisů).

6. Přezkum účinnosti regulace

Důkladné hodnocení a pravidelný přezkum účinnosti regulace je u předpisu upravujícího relativně novou zájmovou oblast podléhající navíc rychlému technickému a společenskému vývoji nutným předpokladem jeho efektivního uplatnění. K tomu, aby mohla navrhovaná právní úprava plnit svůj základní účel, je tedy třeba průběžně sledovat, do jaké míry odpovídají zákonné povinnosti aktuálním potřebám informační společnosti - vzhledem k tomu, že zákon o kybernetické bezpečnosti se týká skutečného fungování informačních systémů a služeb a sítí elektronických komunikací, nelze připustit situaci, kdy budou zákonné povinnosti formálně definovány a formálně plněny, avšak bez skutečného praktického efektu.

Přezkum účinnosti regulace lze u navrhované právní úpravy rozdělit do tří základních fází:

1. Sledování technického vývoje a okamžitý přezkum implementace bezpečnostních opatření a opatření
2. Hodnocení efektivity právní úpravy a přezkum struktury jednotlivých konkrétních parametrů zákonných povinností
3. Hodnocení věcného a osobního rozsahu regulace

Ad 1) NBÚ prostřednictvím činností vládního CERT, spolupráce s národním CERT a mezinárodní spolupráce permanentně sleduje a vyhodnocuje situaci v oblasti kybernetické bezpečnosti a reaguje na zjištěné nedostatky a bezpečnostní hrozby. Dojde-li k situaci vyžadující okamžité přehodnocení kvality bezpečnostních opatření (např. dojde ke zjištění tzv. bezpečnostní díry v určité technologii nebo ke snížení důvěryhodnosti určitého bezpečnostního mechanismu), bude k jejímu řešení užito opatření, popřípadě následně bude provedena změna prováděcích právních předpisů.

Ad 2) NBÚ provádí ve spolupráci s dotčenými rezorty, akademickými pracovišti a soukromým sektorem pravidelné hodnocení efektivity právní úpravy jako takové. Ukáže-li se, že některé zákonné povinnosti neplní dostatečně účel navrhované právní úpravy, bude iniciována příslušná změna právní úpravy. Navíc NBÚ pravidelně vyhodnocuje strukturu parametrů bezpečnostních opatření, a to zejména v návaznosti na vývoj průmyslových standardů a obecně akceptovaných doporučených postupů (best practices). V případě potřeby upravit parametry bezpečnostních opatření bude jako nástroje použito změny prováděcího právního předpisu, tj. vyhlášky NBÚ.

Ad 3) NBÚ přezkoumává rozsah působnosti zákona o kybernetické bezpečnosti a na základě hodnocení aplikace zákona o kybernetické bezpečnosti, analýzy rizik nebo srovnání s právními úpravami jiných států může vytipovávat nové oblasti nebo typy subjektů, které by měly být pod regulaci zahrnuty.

První hodnocení účinnosti právní úpravy proběhlo v březnu 2016, kdy NBÚ rozeslal na zástupce odborné veřejnosti žádost o zhodnocení stávající právní úpravy v návaznosti na její aplikační praxi.

Připomínky odborné veřejnosti směřovaly v tomto ohledu zejména k těmto oblastem:

- Problematika outsourcingu – je nutná potřeba dostatečného zajištění bezpečnosti provozovatelů informačních a komunikačních systémů, a to minimálně zvýšením požadavků na smlouvy s dodavateli, které mnohdy nepokrývají oprávnění správce přístupu k informacím, čímž vzniká tzv. lock-in efekt.
- Přísnější sankce.
- Technická a personální certifikace - zavedení zákonné procedury kontroly souladu zavedených bezpečnostních opatření s požadavky zákona o kybernetické bezpečnosti a technické certifikace konkrétních bezpečnostních technologií a certifikace odborníků na kybernetickou bezpečnost.
- Upřesnění definice správce - otázku odpovědnosti v případech, kdy správce informačního nebo komunikačního systému není současně jejich vlastníkem či provozovatelem a není

jasné nastavení dodavatelských vztahů.

- Rozšíření povinnosti mlčenlivosti – tato povinnost by se měla vztahovat na všechny zaměstnance, kteří se podílejí na zajišťování kybernetické bezpečnosti, resp. na informace související s řízením kybernetické bezpečnosti.
- Neveřejnost povahy informací o kybernetické bezpečnosti a kybernetických bezpečnostních incidentech – tyto informace by měly být vyjmuty z působnosti zákona č. 106/1998 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.
- Upravení vyhlášky o kybernetické bezpečnosti, aby byla v souladu s aktuálním zněním norem ISO/IEC řady 27 000.
- Vyjasnění vztahu zákona o kybernetické bezpečnosti k zákonu č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů.
- Specifikace okolnosti vyhlášení stavu kybernetického nebezpečí – která práva budou omezena a v jakém rozsahu, rozsah ukládaných povinností, územní a osobní rozsah.
- Rozšíření klasifikace informací a dat – o stupně „neveřejné“ a „pro služební potřebu“.

Připomínky ve vztahu k dodavatelům a sankcím jsou již řešeny návrhem zákona, kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony. Další připomínky, které se vztahují k neveřejnosti povahy informací o kybernetické bezpečnosti a kybernetických bezpečnostních incidentech, pak řeší předložený návrh zákona. Ostatní připomínky jsou spíše koncepční povahy a jejich zapracování je ke zvážení do budoucna.

K vyhláškám uplatnila odborná veřejnost připomínky především ohledně odvětvových určujících kritérií kritické informační infrastruktury a významných informačních systémů a rozšíření regulovaných oblastí (např. o zdravotnictví). Rovněž i tyto připomínky jsou řešeny cestou návrhu zákona, který zmiňované oblasti upravuje v odvětvových kritériích pro základní služby. Dále se připomínky vztahovaly k veřejnosti přílohy č. 1 k vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, ve znění vyhlášky č. 205/2016 Sb., a k procesu identifikace významných informačních systémů. Tyto připomínky však odporují celé koncepci identifikace významných informačních systémů.

7. Konzultace a zdroje dat

7.1 Konzultace během projednávání návrhu směrnice v legislativních orgánech EU

Již během projednávání návrhu směrnice v legislativních orgánech EU byli konzultováni zástupci odborné veřejnosti. Konkrétně se jednalo o společnosti CZ.NIC a Seznam.cz, které pomáhaly NBÚ při vypracovávání stanovisek k poskytovatelům digitální služeb a provozovatelům základních služeb v oblasti digitálních infrastruktur. Tyto společnosti kritizovaly navrhovanou regulaci, která podle nich může ovlivnit velké množství subjektů a znevýhodnit evropské podnikatele, což může vést až k přesunu sídel těchto podnikatelů mimo EU. Ve spolupráci s nimi tak NBÚ vypracovával národní pozice ČR, které pak prezentoval na půdě Rady Evropské unie společně se zástupci členských států, jejichž národní pozice byly obdobné. I díky tomuto tlaku bylo nakonec přistoupeno k mírnějšímu

režimu regulace poskytovatelů digitálních služeb, přičemž byl zúžen i jejich okruh spadající pod regulaci.

Rovněž byly jednotlivé národní pozice pravidelně zasílány ke schválení členům resortní koordinační skupiny, která byla zřízena interním aktem řízení NBÚ. Členy této pracovní skupiny byli vedle pracovníků NBÚ zástupci Úřadu vlády ČR, Ministerstva vnitra, Ministerstva zahraničních věcí, Ministerstva obrany, Ministerstva průmyslu a obchodu, Ministerstva dopravy, Českého telekomunikačního úřadu a Stálého zastoupení ČR při EU v Bruselu. Instrukce pro jednotlivá jednání byly rovněž vkládány do informačního systému DAP, kde se k nim mohly vyjádřit i další resorty, jejichž zástupci nebyli v resortní koordinační skupině. Vývoj projednávání směrnice a nejdůležitější pozice ČR byly taktéž pravidelně prezentovány na jednáních výboru pro EU na pracovní úrovni.

7.2 Stanovisko Evropské komise

Během přípravy návrhu zákona se NBÚ rovněž obrátil na Komisi se žádostí o výklad týkající se dvou problematických oblastí.

První se týkala uložení povinnosti poskytovatelům digitálních služeb poskytovat kontaktní údaje. Tato povinnost jim není uložena samotnou směrnicí. Příslušné vnitrostátní orgány, tedy NBÚ, mají mít však podle směrnice pravomoci a prostředky nezbytné pro vynucování plnění povinností uložených směrnicí. Komise se v tomto ohledu vyjádřila, že pokud je to náležitě zdůvodněno jako požadavek pro zajištění bezpečnosti, lze do národní legislativy zahrnout povinnost poskytovatele digitálních služeb oznámit kontaktní osobu, tedy poskytnout kontaktní údaje.

Druhá oblast se pak vztahovala k problematice cloud computingových služeb, konkrétně, zda by poskytovatelé těchto služeb mohli být určeni jako prvek kritické informační infrastruktury, čímž by podléhali přísnějším pravidlům, než dovoluje směrnice. Komise se v tomto ohledu vyjádřila, že směrnice umožňuje členským státům zavázat provozovatele základních služeb, kteří využívají služeb cloudu, k povinnosti sjednat si smluvně s poskytovatelem tohoto cloudu takové podmínky, aby byly splněny nezbytné požadavky, které provozovatelům základních služeb ukládá směrnice. Odpovědnost za incidenty však vždy nese provozovatel základních služeb, respektive správce informačního nebo komunikačního systému kritické informační infrastruktury.

7.3 Pracovní skupina I

V únoru 2016 byla vytvořena Pracovní skupina pro transpozici směrnice NIS na resortní úrovni (dále také „pracovní skupina I“). Tato pracovní skupina se scházela od března 2016 do července 2016. Hlavní úkoly této pracovní skupiny byly:

- Posouzení jednotlivých ustanovení směrnice a jejich soulad s již existujícími právními předpisy.
- Vytipování a vypracování novel předpisů (vyjma zákona o kybernetické bezpečnosti), které mohou být transpozicí směrnice ovlivněny.
- Diskuse a příprava nejdůležitějších bodů novely zákona o kybernetické bezpečnosti (zejména rozšíření působnosti v případě provozovatelů základních služeb a poskytovatelů digitálních

služeb).

- Průběžné informování členů pracovní skupiny o dopadech, které pro ně a pro subjekty spadající do jejich působnosti z transpozice směrnice do právního řádu ČR vyplynou.
- Informování NBÚ o dopadech vyplývajících z transpozice směrnice do právního řádu ČR, které členové pracovní skupiny očekávají v rámci jejich resortů a subjektů spadajících do jejich působnosti.

Členy této pracovní skupiny byli zástupci Ministerstva financí, Ministerstva zahraničních věcí, Ministerstva vnitra, Ministerstva průmyslu a obchodu, Ministerstva práce a sociálních věcí, Ministerstva dopravy, Ministerstva zdravotnictví, Ministerstva životního prostředí, Ministerstva pro místní rozvoj, Českého báňského úřadu, Energetického regulačního úřadu, Úřadu pro ochranu osobních údajů, Vojenského zpravodajství, Bezpečnostní informační služby, Českého telekomunikačního úřadu, Policejního prezidia ČR, Svazu průmyslu a dopravy ČR, Úřadu pro zastupování státu ve věcech majetkových, Hospodářské komory ČR, zájmového sdružení právnických osob CZ.NIC a Generálního ředitelství hasičského záchranného sboru.

Pracovní skupina I se kontinuálně scházela jednou až dvakrát měsíčně k projednání otázek souvisejících s transpozicí směrnice. V průběhu jednání byly rovněž členům pracovní skupiny zasílány k připomínkám vypracovávané dokumenty (právně-lingvistické revize textu a srovnávací tabulka). Rovněž s nimi byly konzultovány pracovní návrhy zákona, přičemž některé návrhy a připomínky členů pracovní skupiny byly do finální podoby návrhu zákona promítnuty.

Jako problematické se během jednání této pracovní skupiny také ukázalo zpracování dopadů navrhované právní úpravy. Na základě připomínek členů pracovní skupiny tak NBÚ vypracoval stručný dotazník, který byl v polovině května 2016 členům rozeslán.

V rámci činnosti pracovní skupiny I se pak ukázaly být nejvíce exponované tyto následující okruhy:

- vymezení provozovatelů základních služeb vůči kritické informační infrastruktuře,
- zohlednění důvěrnosti informací uvedených v bezpečnostní dokumentaci při výběru dodavatelů,
- postavení manažera kybernetické bezpečnosti v rámci organizační struktury,
- definování významného dopadu kybernetických bezpečnostních incidentů,
- rozšíření bezpečnosti informací o „pravost“,
- horní hranice sankcí,
- detekce kybernetických bezpečnostních událostí a uložení sankce za neplnění této povinnosti,
- vztah povinnosti mlčenlivosti k zákonu č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů a
- definice informačního systému.

Uplatněné připomínky byly se členy pracovní skupiny vypořádány v průběhu jednání, přičemž část z nich byla do návrhu zákona zapracována, respektive je počítáno s jejím zapracováním do prováděcích právních předpisů k zákonu o kybernetické bezpečnosti.

Rovněž byli členové pracovní skupiny I konzultováni i v otázce, zda podle nich existuje rozdíl mezi provozovatelem základní služby, správcem informačního systému základní služby a provozovatelem informačního systému základní služby, přičemž z jejich odpovědí vyplynulo, že hypoteticky zde takovýto rozdíl může existovat.

7.4 Pracovní skupina II

V rámci transpozice směrnice byla vytvořena i druhá pracovní skupina pro transpozici směrnice NIS, tentokráte však na úrovni odborné veřejnosti (dále také „pracovní skupina II“). Tato skupina byla vytvořena v dubnu 2016 a poprvé svolána v květnu 2016. Její činnost probíhala do července 2016.

Hlavním cílem této pracovní skupiny bylo hodnocení dopadů návrhu novely zákona o kybernetické bezpečnosti na soukromý sektor a informování odborné veřejnosti o přípravě transpozice směrnice. Její úkoly byly tedy následující:

- Diskuse a příprava nejdůležitějších bodů novely zákona o kybernetické bezpečnosti.
- Průběžné informování členů pracovní skupiny o dopadech, které pro ně a pro další subjekty z transpozice směrnice do právního řádu ČR vyplynou.
- Informování NBÚ o dopadech vyplývajících z transpozice směrnice do právního řádu ČR, které členové pracovní skupiny očekávají.
- Informování o průběhu projednávání prováděcích předpisů Komise.

Jako zástupci odborné veřejnosti byly vybrány osoby soukromého práva, které mohou být pod nově vytvářenou regulaci zařazeni, zástupci akademické sféry, subjekty, které se přímo zabývají bezpečnostní ICT, popřípadě prováděním auditů, a důležité ústřední správní úřady ČR. Konkrétně se jednalo o tyto společnosti: PricewaterhouseCoopers, NIX.CZ, ČIMIB, Google CZ, ISACA, Státní pokladna – Centrum sdílených služeb, Seznam.cz, CESNET, Řízení letového provozu, NSM Cluster, Deloitte, Svaz průmyslu a dopravy, ČEPS, Anect, České radiokomunikace, ČEZ ICT Services, Ředitelství silnic a dálnic, Ústřední vojenská nemocnice – fakultní nemocnice Praha, Fakultní nemocnice Brno, Fakultní nemocnice Motol, Český telekomunikační úřad, Masarykova univerzita v Brně a zájmové sdružení právnických osob CZ.NIC, které provozuje národní CERT.

V reakci na žádost NBÚ o obecné zhodnocení nákladů, které by mohly dotčeným subjektům vzniknout, členové této pracovní skupiny oponovali, že není možné vymezit náklady, pokud nevědí, jaká míra zabezpečení na ně bude dopadat, přičemž tato míra bude dána až samotnou novelou zákona o kybernetické bezpečnosti. Dále upozornili, že směrnice je v tomto ohledu velmi obecná, přičemž nejzřetelnější je tento problém u poskytovatelů digitálních služeb, pro něž budou doporučená bezpečnostní opatření vydána až prováděcími akty Komise v roce 2017. Za účelem zhodnocení nákladů byl tedy členům této pracovní skupiny rozeslán taktéž již výše uvedený dotazník.

Další požadavky přednesené členy pracovní skupiny byly tyto:

- novela zákona o kybernetické bezpečnosti by měla být co nejméně administrativně zatěžující,
- měla by se řídit principem „digital by default“,

- dotčeným subjektům by měly vzniknout co nejnižší náklady.

Členové pracovní skupiny byli rovněž požádání o vyjádření k návrhu zákona. I na této pracovní skupině byl zmíněn požadavek na organizační upevnění manažera kybernetické bezpečnosti, přičemž však část členů pracovní skupiny II byla proti tomuto opatření s ohledem na fakt, že rozhodování o organizační struktuře by mělo být ponecháno samotným firmám. Dále členové této pracovní skupiny uplatnili připomínky vztahující se k náležitostem strategie kybernetické bezpečnosti a definicím digitálních služeb, které by podle nich mohli být uvedeny spíše v prováděcím právním předpise. Na druhou stranu uvítali některé z navrhovaných změn (např. zavedení povinnosti mlčenlivosti ohledně bezpečnostních opatření nebo zvýšení horní hranice sankcí).

I v rámci této pracovní skupiny NBÚ vznesl dotaz, zda podle členů pracovní skupiny existuje rozdíl mezi provozovatelem základní služby, správcem informačního systému základní služby a provozovatelem informačního systému základní služby, přičemž i z odpovědí členů této pracovní skupiny vyplynulo, že přinejmenším hypoteticky takovéto rozdělení možné je.

7.5 Bilaterální jednání

Pracovníci NBÚ rovněž projednávali některé otázky se zástupci dalších resortů a dotčených subjektů bilaterálně. Jednalo se zejména o otázky překryvu režimu regulace směrnice NIS a na něj navazujícího návrhu zákona s dalšími právními předpisy.

Šlo především o nastavení režimu regulace právnických nebo fyzických osob zajišťujících veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací podle zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů. Ohledně této problematiky proběhlo jednání se zástupci Českého telekomunikačního úřadu, přičemž na tomto jednání bylo dohodnuto, že bude ponecháno současné nastavení regulace těchto subjektů a nebude v tomto ohledu provedena žádná legislativní změna.

Dále byla projednávána s Ministerstvem vnitra regulace poskytovatelů služeb vytvářejících důvěru podle nařízení (EU) č. 910/2014 Sb. (dále jen „nařízení eIDAS“).[36] I během tohoto jednání bylo dohodnuto, že úpravy podle nařízení eIDAS a směrnice budou fungovat paralelně vedle sebe, přičemž není nutno tuto otázku nijak v návrhu zákona specifikovat.

7.6 Oslovení již regulovaných subjektů

V rámci zjišťování údajů o případných nákladech na implementaci bezpečnostních opatření byly v průběhu dubna 2016 osloveny subjekty, které jsou již regulovány podle stávající právní úpravy zákona o kybernetické bezpečnosti.

Celkem bylo cestou elektronické komunikace osloveno 42 subjektů spravujících kritickou informační infrastrukturu nebo významné informační systémy, popřípadě spravujících oba typy systémů.

[36] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (Úř. věst. L 257, 28. 8. 2014, s. 73).

Odpověď zaslalo 20 subjektů. Vzhledem k charakteru poskytnutých informací a použitelnosti odpovědí bylo do výpočtu zahrnuto 17 subjektů spravujících celkem 77 systémů kritické informační infrastruktury a významných informačních systémů.

Ze získaných dat vyplynulo, že souhrnné náklady na zavádění technických opatření podle zákona o kybernetické bezpečnosti činily na 77 systémů kritické informační infrastruktury a významných informačních systémů téměř 95 milionů Kč. K provádění organizačních opatření podle zákona o kybernetické bezpečnosti pak bylo podle správců vydáno celkem 23 milionů Kč na zmíněných 77 systémů. Tyto náklady jsou počítány za první rok od určení, tj. ve lhůtě stanovené pro zavádění bezpečnostních opatření. V budoucnosti správci předpokládají další náklady spojené s údržbou systémů a výměnou technických zařízení. Je nutno zmínit, že jde o velmi hrubé odhady, neboť někteří správci nebyli schopni náklady na zavádění zákonných opatření přesně vyčíslit. Dále pak není zvážena počáteční úroveň zabezpečení a není vyloučeno, že některá opatření by správci zavedli sami o své vůli i bez existence zákonné úpravy. Některé subjekty také sdělily, že zákon o kybernetické bezpečnosti na ně neměl žádné finanční dopady, neboť by daná opatření stejně zavedly v rámci řízení rizik či zavádění ISMS.

Lze tedy uvést, že průměrně náklady na zavedení technických opatření na jeden významný informační systém nebo informační nebo komunikační systém kritické informační infrastruktury vycházejí přibližně na 1 233 tis. Kč a organizační opatření pak vycházejí na cca 300 tis. Kč.

Tabulka č. 3 – shrnutí nákladů na zavádění bezpečnostních opatření v informačních a komunikačních systémech kritické informační infrastruktury a významných informačních systémech podle stávajícího zákona o kybernetické bezpečnosti[37]

Počet uvažovaných systémů KII i VIS	Celkem technická opatření na 77 systémů KII a VIS	Celkem organizační opatření na 77 systémů KII a VIS	Průměrné náklady na technická opatření na jeden systém KII nebo VIS	Průměrné náklady na organizační opatření na jeden systém KII nebo VIS
77	94 939 839 Kč	23 226 539 Kč	1 232 985 Kč	301 643 Kč

7.7 Zdroje dat

- Důvodová zpráva k návrhu směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii, COM(2013) 048 final – 2013/0027 (COD).

- Důvodová zpráva k návrhu zákona o kybernetické bezpečnosti.

[37] Vzhledem k charakteru informací, které oslovené subjekty poskytly, není výpočet rozdělen na systémy kritické informační infrastruktury a významné informační systémy, neboť některá opatření a tedy i náklady jsou sdílené pro kritickou informační infrastrukturu i pro významné informační systémy.

- Strategie pro oblasti kybernetické bezpečnosti České republiky na období 2011 – 2015 (usnesení vlády č. 564 ze dne 20. července 2011).

- Strategie pro oblast kybernetické bezpečnosti České republiky na období let 2012 až 2015 (usnesení vlády č. 364 ze dne 23. května 2012).

- Akční plán opatření ke Strategii pro oblast kybernetické bezpečnosti České republiky na období let 2012 až 2015 usnesení vlády č. 364 ze dne 23. května 2012).

- Národní strategie kybernetické bezpečnosti České republiky na období let 2015 až 2020 (usnesení vlády č. 105 ze dne 16. února 2015).

- Akční plán k Národní strategii kybernetické bezpečnosti České republiky na období let 2015 až 2020 (usnesení vlády č. 382 ze dne 25. května 2015).

- 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.

- Usnesení vlády České republiky ze dne 30. Května 2012 č. 382 o věcném záměru zákona o kybernetické bezpečnosti.

- Akční plán pro rozvoj digitálního trhu (usnesení vlády č. 694 ze dne 26. srpna 2015).

- Sdělení Komise Evropskému parlamentu, Radě, Evropskému hospodářskému a sociálnímu výboru a Výboru regionů: Strategie pro jednotný digitální trh v Evropě, COM(2015) 192 final.

- Commission staff Working Document: A Digital Single Market Strategy for Europe – Analysis and Evidence, SWD(2015) 100 final.

- Pilný, I.: Digitální ekonomika: Žít nebo přežít, 1. vyd. Brno: Bizbooks, 2016, s. 2016. ISBN 978-80-265-0481-8

- Nález Spolkového ústavního soudu ze dne 15. prosince 1983, č. j. BVerfGE 65, 1.

- Nález Ústavního soudu ze dne 1. března 2000, č. j. II. ÚS 517/99, N 32/17 SbNU 229, nález Ústavního soudu ze dne 7. dubna 2010, č. j. I. ÚS 22/10 a nález Ústavního soudu ze dne 22.března 2011, sp. zn. Pl. ÚS 24/10, 94/2011 Sb.

- www.govcert.cz

- www.vlada.cz

8. Dopady navrhované úpravy

Dopady navrhované úpravy cílí obecně na ochranu základních práv a svobod a vnitřního trhu EU. V tomto ohledu se jedná zejména o ochranu práva na informační sebeurčení a nedistributivních práv ČR, konkrétně práva státu na zajištění vnitřní bezpečnosti, na ochranu základních funkcionalit státu a na ochranu před škodlivými následky výjimečných stavů. Směrnice za tímto účelem ctí zásady přiznávané především Listinou základních práv Evropské unie, zejména právo na respektování soukromého života a komunikace, ochranu osobních údajů, svobodu podnikání, právo na vlastnictví a právo na účinnou právní ochranu a spravedlivý proces.

Návrh zákona pak vychází z principu minimalizace státního donucení a principu autonomie vůle regulovaných subjektů. Navržená právní úprava resp. povinnosti z ní plynoucí tak nedopadá na veškeré informační systémy, ale zaměřuje se pouze na ty sítě a informační systémy, které mají zásadní význam, a nespadají doposud pod regulaci zákona o kybernetické bezpečnosti. Zabezpečení těchto systémů před běžnými formami kybernetických útoků tak je podle účelu navrhovaného zákona řešeno pouze ve vztahu k systémům a sítím, na nichž je závislé poskytování základních nebo digitálních služeb. Povinnost aplikace určitého standardního zabezpečení včetně povinnosti hlásit výskyt kybernetických bezpečnostních incidentů a odpovídajícím způsobem na ně reagovat je tedy obecně definována pouze pro systémy stanoveného společenského významu (tj. systémy, jejichž ochrana má ve shora uvedeném smyslu zásadní význam pro ochranu práv na informační sebeurčení a nedistributivních informačních práv státu). Lze tedy konstatovat, že věcný a osobní rozsah navrhované právní úpravy je minimalistický a sleduje dosažení shora uvedeného účelu za užití nejnižší možné míry právní regulace.

Vedle standardního povinného zapojení shora uvedených subjektů do systému ochrany před kybernetickými bezpečnostními incidenty počítá navrhovaná právní úprava s tím, že řada subjektů provozujících sítě a informační systémy projeví zájem o dobrovolné zapojení do národního systému kybernetické bezpečnosti. Zkušenosti z posledních let ukazují, že spolupráce s národními dohledovými pracovišti přináší podnikatelským subjektům i akademickému nebo neziskovému sektoru vysoce pozitivní efekty a že zájem o tuto spolupráci bývá velký - správci soukromých nebo akademických sítí a informačních systémů mají v takových případech možnost vzájemně sdílet poznatky o hrozbách v oblasti kybernetické bezpečnosti a díky metodickému působení národního dohledového pracoviště mohou vlastní infrastrukturu daleko účinněji bránit před kybernetickými bezpečnostními incidenty. Zákon tedy v tomto směru počítá s možností dobrovolného zapojení do systému národní kybernetické bezpečnosti i pro subjekty mimo okruh regulovaných orgánů a osob.

Vzhledem ke značné různorodosti regulovaných subjektů jde navrhovaná právní úprava cestou stanovení základních povinností a standardních bezpečnostních parametrů, přičemž je adresátům právních povinností ponechána volnost ve způsobech, jakými dosáhnou jejich naplnění. Není totiž vhodné ani potřebné direktivně určovat konkrétní technické a organizační postupy. Podobně jako navrhovaná právní úprava počítá s tím, že lze standardní zabezpečení informačních systémů a sítí řešit za užití různých zabezpečovacích technologií, je regulatorní řešení liberální i v konkrétních způsobech, jimiž bude na straně orgánů a osob zajištěno plnění zákonných povinností. Konkrétní organizační a technické postupy včetně např. školení zaměstnanců, interních kontrol apod. tedy ponechává navrhovaná právní úprava plně v diskreci orgánů a osob. Tím je zajištěno, že výsledné zabezpečení sítí a informačních systémů bude ve svém souhrnu spolehlivě funkční, přičemž

individualita jednotlivých partikulárních bezpečnostních řešení umožní efektivní využití příslušných zdrojů. Zjednodušeně řečeno se tedy princip autonomie vůle regulovaných subjektů v důsledku projeví tak, že prostředky vynaložené na zabezpečení příslušných sítí a informačních systémů budou použity v přímém vztahu ke konkrétním potřebám orgánů a osob, tj. zpravidla účelně a hospodárně.

8.1 Dopady na státní rozpočet a ostatní veřejné rozpočty

Významné dopady na státní rozpočet lze očekávat tehdy, kdy by regulované subjekty byly orgány státní správy, popřípadě by pod tyto orgány spadaly. Orgány veřejné moci jsou však již ve většině případů určenými orgány a osobami podle stávajícího režimu zákona o kybernetické bezpečnosti a plní povinnosti jím stanovené. Tím pádem by jim zavedením nové regulace neměly vzniknout významné náklady, jak rovněž vyplynulo z dotazníkového průzkumu provedeného mezi členy pracovní skupiny I. Ti v závislosti na provádění povinností uložených zákonem o kybernetické bezpečnosti hodnotili svoje zabezpečení jako poměrně vysoké, přičemž náklady na doplnění bezpečnostních opatření na úroveň stanovenou pro správce a provozovatele informačního systému základní služby by činily v průměru na jeden subjekt cca 6 mil. Kč, pokud by požadovaná úroveň zabezpečení byla nastavena na úrovni významných informačních systémů, nebo cca 11,5 mil. Kč [38], pokud by byla požadována stejná úroveň zabezpečení jako pro kritickou informační infrastrukturu.

Na druhou stranu lze očekávat zvýšení rozpočtových nákladů u orgánu státní správy odpovědného za výkon státní správy v oblasti kybernetické bezpečnosti, kterým je NBÚ. Směrnice totiž ukládá ČR, aby zajistila, že příslušné orgány a týmy CERT disponují odpovídajícími zdroji pro účinné plnění svěřených úkolů. V případě NBÚ tak bude nutné navýšit rozpočet na pokrytí personálního zajištění nově vzniklých agend, kterými budou určování provozovatelů základních služeb, výkon kompetencí jednotného kontaktního místa, výkon kontroly u provozovatelů základních služeb, správců a provozovatelů informačních systémů základních služeb a poskytovatelů digitálních služeb, a v případě vládního CERT pak podpora a pomoc při řešení incidentů provozovatelů základních služeb a správců a provozovatelů informačních systémů základních služeb a rozšíření provozu dohledového pracoviště na službu 24/7. V souvislosti s rozšiřováním stavu zaměstnanců by pak mohly vzniknout i nové požadavky na prostorové, technické a materiální vybavení.[39]

8.2 Dopady na podnikatelské prostředí ČR

Předmětný návrh zákona může potenciálně znevýhodnit menší subjekty, které nedisponují dostatečnými finančními prostředky pro zavedení a provádění všech uložených povinností. Toto platí především pro implementaci bezpečnostních opatření, která může být značně administrativně i finančně náročná, a to zejména pokud povinné subjekty zabezpečení svých sítí a informačních systémů doposud nijak neřešily. Pro zamezení tohoto efektu však mají sloužit nástroje selekce, kterými jsou u provozovatelů základních služeb určovací kritéria, a u poskytovatelů digitálních služeb

[38] Jedná se o souhrnnou částku, která se skládá z nákladů provozních, investičních a mzdových.

[39] V usnesení vlády České republiky ze dne 1. července 2015 č. 520 schválila vláda posílení kapacity NBÚ v oblasti kybernetické bezpečnosti o 8 funkčních míst v roce 2016, o 8 funkčních míst v roce 2017 a o 8 funkčních mít v roce 2018 a zvýšení rozpočtu kapitoly NBÚ o 48,9 mi. Kč v roce 2016, o 49 mil. Kč v roce 2017 a o 50 mil. Kč v roce 2018.

přesně nastavené definice a plošná výjimka pro mikropodniky a malé podniky ve smyslu doporučení Komise č. 2003/361/ES o definici mikropodniků, malých a středních podniků.

V praxi by tak z regulace měly být vyloučeny ty subjekty, které nedosahují stanoveného stupně významnosti, co se týče jejich dopadů, popřípadě nejsou dostatečně velké.

Obecně je však očekáváno spíše posílení podnikatelského prostředí. Návrhem zákona je totiž garantována určitá úroveň zabezpečení sítí a informačních systémů u přesně stanoveného okruhu subjektů. Zvýšení zabezpečení pak přispěje k budování důvěry spotřebitelů a obchodních partnerů, případně i zahraničních investorů, které může přilákat právě vysoká míra bezpečnosti českého ICT prostředí. Právě naopak nezavedením uvedených povinností by čeští podnikatelé zaostávali za podnikateli ostatních členských států, což by mohlo vést ke ztrátě jejich klientely a zhoršení konkurenceschopnosti jako takové.

Navíc není možno přehlédnout, že zavedením bezpečnostních opatření a plněním dalších povinností podnikatelé minimalizují riziko vzniku kybernetických bezpečnostních incidentů, které mohou značně narušit fungování jimi provozovaných a poskytovaných služeb. Tím bude tedy zabráněno i vzniku rozsáhlých finančních ztrát a poškození dobrého jména, které by mohlo být ve výjimečných případech až fatální.

8.3 Sociální dopady

Nepředpokládají se negativní sociální dopady, neboť nedochází ke snížení úrovně ochrany zaměstnanců.

8.4 Dopady na životní prostředí

Daný návrh zákona se zaměřuje zejména na posílení nastavení základních pilířů kybernetické bezpečnosti v ČR a rozšíření působnosti zákona o kybernetické bezpečnosti. Vzhledem k zásadě technologické neutrality, na které jsou zákon o kybernetické bezpečnosti i směrnice postaveny, nepředepisuje návrh zákon žádná konkrétní technologická řešení, nepředpokládají se tedy dopady na životní prostředí.

8.5 Dopady na územní samosprávné celky

Návrh zákona představuje transpoziční novelu směrnice, která je zaměřena na zabezpečení sítí a informačních systémů provozovatelů základních služeb (v případě návrhu zákona pak ještě správců a provozovatelů informačních systémů základních služeb) a poskytovatelů digitálních služeb. Územní samosprávné celky mohou být touto novou regulací zasaženy tehdy, pokud naplňují definice a určující kritéria výše uvedených subjektů. V takovém případě by musely plnit povinnosti stanovené pro danou kategorii orgánů a osob podle zákona o kybernetické bezpečnosti, přičemž náklady na zabezpečení sítí nebo informačních systémů by byly v podobné výši, jako je shora uvedeno u státních a soukromoprávních správců informačních nebo komunikačních systémů.

8.6 Dopady na spotřebitele

Navrhovaná právní úprava nepředpokládá žádné přímé dopady na spotřebitele. Co se týče dopadů, jež by se mohly spotřebitele dotknout nepřímo, bude zlepšením bezpečnosti zvýšena především kvalita poskytovaných služeb. Dále je nutno podotknout, že směrnice cílí na ochranu a podporu fungování vnitřního trhu. Splněním ukládaných povinností tedy dojde i ke zlepšení úrovně poskytovaných služeb ve všech základních sledovaných parametrech bezpečnosti informací, a to napříč všemi členskými státy. Občanům ČR, potažmo EU, tak bude garantována vysoká úroveň zabezpečení služeb v rámci celého prostoru EU.

Zároveň bude mít zlepšení zabezpečení sítí a informačních systémů pozitivní vliv na ochranu osobních údajů, které jsou mnohdy zejména v souvislosti s poskytováním digitálních služeb sítěmi a informačními systémy zpracovávány a uchovávány. Na druhou stranu se však vynaložené náklady mohou odrazit na cenách poskytovaných služeb, což však s ohledem na konkurenční prostředí nemusí nastat.

8.7 Dopady ve vztahu k zákazu diskriminace a ve vztahu k rovnosti žen a mužů

Navrhovaná právní úprava nepřináší rizika diskriminace a nerovného zacházení. Obecná definice a podmínky jejího naplnění se budou aplikovat u všech zaměstnanců shodně, bez snahy jakoukoliv určitou skupinu zaměstnanců zvýhodnit či znevýhodnit.

8.8 Dopady na ochranu soukromí a osobních údajů

Z hlediska ochrany soukromí a osobních údajů nebyly identifikovány žádné negativní dopady. Právě naopak směrnice ukládá povinnou spolupráci vnitrostátních příslušných orgánů (NBÚ) s orgány pro ochranu osobních údajů. Rovněž se dá očekávat, že posílení zabezpečení důležitých sítí a informačních systémů povede k posílení ochrany osobních údajů, a to zejména s ohledem na regulaci poskytovatelů digitálních služeb, kteří zpravidla osobní údaje v rámci poskytování svých služeb zpracovávají a uchovávají.

8.9 Dopady na výkon státní statistické služby

Navrhovaná úprava nebude mít dopad na výkon státní statistické služby.

9. Zhodnocení korupčních rizik – CIA

Navrhovaná právní úprava zasahuje do právních vztahů upravených správním právem a řeší veřejnoprávní instituty. Jedná se tedy o sféru práva, která je doménou rozhodování orgánů veřejné správy.

Předkladatel provedl zhodnocení korupčních rizik ve smyslu čl. 9 odst. 2 písm. i) Legislativních pravidel vlády. Předkládaný návrh je svým rozsahem přiměřený cílům, k nimž je předkládán.

9.1 Přiměřenost

Předložený návrh zákona je vyhotoven v intencích transponované směrnice. Zároveň obsahuje ještě řešení některých otázek, které v současné praxi vytvářejí problémy při aplikaci zákona o kybernetické bezpečnosti. Rozsah povinností a rozšíření působnosti zákona o kybernetické bezpečnosti jsou však přiměřené, zejména s ohledem na rizika a dopady, které by vznikly netransponováním směrnice a neodstraněním současných legislativních nedostatků. Předmětný návrh je tedy svým rozsahem přiměřený množině vztahů, které má upravovat.

Oblast kybernetické bezpečnosti byla dosud regulována zákonem o kybernetické bezpečnosti a částečně i dalšími právními předpisy. Zákon o kybernetické bezpečnosti se však doposud soustředil pouze na informační a komunikační systémy důležité pro fungování státu a veřejné správy, nikoli však na informační systémy, na nichž jsou závislé služby důležité spíše na regionální úrovni. Tím byla ze systému kybernetické bezpečnosti v ČR vyjmuta podstatná část informačních a komunikačních systémů, jejichž zasažení incidenty může mít významné dopady na společnost a ekonomiku.

Návrhem zákona je tudíž prohlouben rozsah zajištění kybernetické bezpečnosti v ČR a celkově dojde k posílení bezpečnosti sítí a informačních systémů. Opatření navrženého zákona tak odpovídají požadavku na přiměřenost zásahu do osobnostních práv, zejména do práva na informační sebeurčení a s ním souvisejících základních práv (např. vlastnické právo). Stále však platí v tomto ohledu jeden ze základních principů zákona o kybernetické bezpečnosti, tj. princip autonomie vůle regulovaných subjektů. Prostředky vynaložené na zabezpečení příslušných sítí a informačních systémů tak budou použity v přímém vztahu ke konkrétním potřebám orgánů a osob, tj. zpravidla účelně a hospodárně.

Kompetence státních orgánů nejsou návrhem zákona nijak významně rozšířeny. Rozsah úkolů orgánů státní správy zůstává z velké části nezměněn, významné je však rozšíření působnosti na nově regulované subjekty. Úřad by tak měl na základě návrhu zákona nově určovat provozovatele základních služeb a vykonávat funkci jednotného kontaktního místa. Podpora a pomoc při řešení incidentů provozovatelů základních služeb a správců a provozovatelů informačních systémů základních služeb pak připadne vládnímu CERT a u poskytovatelů digitálních služeb národnímu CERT.

9.2 Efektivita

Efektivní implementace povinností stanovených zákonem o kybernetické bezpečnosti je průběžně vyhodnocována NBÚ. V březnu 2016 byl rozeslán dopis ředitele NBÚ zástupcům odborné veřejnosti se žádostí o sdělení případných nedostatků, které byly zjištěny aplikací zákona o kybernetické bezpečnosti. Zároveň byl na NBÚ vytvořen dokument Bílá místa kybernetické bezpečnosti České republiky, jehož cílem bylo zmapovat nejenom oblasti problematické při aplikaci zákona o kybernetické bezpečnosti, ale i oblasti, které pod současný systém kybernetické bezpečnosti ČR vůbec nespadají, přičemž bylo mezinárodní komparací a konzultacemi s odbornou veřejností zjištěno, že by jejich regulace byla nanejvýše žádoucí.

Povinnosti stanovené návrhem zákona budou posléze implementovány, kontrolovány a vynucovány na základě přijatého zákona a jeho prováděcích právních předpisů. Kontrolování a vynucování dodržování regulace kybernetické bezpečnosti již v současné době funguje u kritické informační

infrastruktury a významných informačních systémů. V tomto ohledu lze tedy předpokládat, že pro provozovatele základních služeb, správce a provozovatele informačních systémů základních služeb a poskytovatele digitálních služeb bude systém nastaven obdobně. Za účelem dosažení odpovídajícího efektu finančních sankcí obsahuje návrh zákona i jejich zvýšení z původní horní hranice 100 tis. Kč až na 5 mil. Kč v případě neplnění povinnosti zavést a provádět bezpečnostní opatření a vést o nich bezpečnostní dokumentaci.

Pracovníci NBÚ navíc kontinuálně sledují a vyhodnocují účinnost bezpečnostních opatření v závislosti na vývoji průmyslových standardů a standardizovaných postupů v rámci řízení bezpečnosti informací a obecně akceptovaných doporučených postupů (best practices), jakož i hodnotí efektivitu právní úpravy jako celku.

Přezkum účinnosti samotné evropské směrnice pak spadá do pravomoci Komise, která bude přezkoumávat i konzistentnost určování provozovatelů základních služeb napříč členskými státy.

9.3 Odpovědnost

Podle zákona o kybernetické bezpečnosti náleží výkon státní správy v oblasti kybernetické bezpečnosti NBÚ, přičemž zákon jednoznačně stanoví jeho kompetence a postavení v této oblasti. Navrhovaným zákonem nedochází k hlubší změně vymezení odpovědnosti. NBÚ bude tedy rozhodovat o určení provozovatelů základních služeb. Rovněž bude disponovat kontrolní i donucovací pravomocí jak vůči provozovatelům základních služeb a správcům a provozovatelům informačních systémů základních služeb, tak i vůči poskytovatelům digitálních služeb. V neposlední řadě bude vykonávat i úkoly jednotného kontaktního místa.

V tomto ohledu nedochází k nadměrnému soustřední pravomocí u NBÚ. Vzhledem ke zkušenostem, které již pracovníci NBÚ se zajišťováním kybernetické bezpečnosti mají, k vysoké míře znalostí a zkušeností nutných pro efektivní spravování této agendy a k nedostatku nabídky pracovní síly těmito znalostmi a zkušenostmi disponující, je nanejvýše vhodné, aby tato agenda byla NBÚ ponechána, a nebyla zbytečně štěpena mezi vícero příslušných orgánů. V úvahu by připadalo pouze sektorové rozdělení působnosti, to však není nutné vzhledem k tomu, že povinné orgány a osoby jsou již v současné době rozděleny do působnosti dvou dohledových pracovišť CERT, která zajišťují podporu a pomoc při řešení kybernetických bezpečnostních incidentů, a navíc mezi sebou intenzivně spolupracují. Zároveň bude díky soustředění pravomoci v rámci NBÚ vždy snazší jednoznačně určit osobu zodpovědnou za konkrétní rozhodnutí. Tou bude téměř vždy zaměstnanec NBÚ.

9.4 Opravné prostředky

Zákon o kybernetické bezpečnosti ve spojení s obecnými právními předpisy upravujícími správní řízení a předpisy upravujícími výkon státní kontroly umožňuje orgánům a osobám účinnou obranu proti nesprávnému postupu orgánu veřejné správy a rovněž opravňuje orgány a osoby k podání řádných i mimořádných opravných prostředků proti závazným aktům vydaným NBÚ. Prokazatelné poučení o možnosti podat opravný prostředek pak vyplývá z obecného právního předpisu, zákona č. 500/2004 Sb., správního řádu, ve znění pozdějších předpisů (dále jen „správní řád“). Podle současného znění zákona o kybernetické bezpečnosti doplněného o návrh zákona bude NBÚ

oprávněn vydávat následující závazné právní akty, proti nimž lze podat tyto opravné prostředky:

a) Určení prvku kritické informační infrastruktury – určení prvku kritické infrastruktury, jehož provozovatelem není organizační složka státu, činí NBÚ opatřením obecné povahy, proti němuž mohou dotčené osoby uplatnit námitky nebo připomínky, a to po vydání jeho návrhu. Rovněž není vyloučena možnost obrátit se na soud se žádostí o soudní přezkum zákonnosti aktů vydaných NBÚ.

b) Určení provozovatele základních služeb – provozovatelé základních služeb budou obdobně jako prvky kritické informační infrastruktury určováni opatřením obecné povahy, proti kterému budou moci dotčené osoby podat námitky nebo připomínky, a to po zveřejnění návrhu opatření obecné povahy, přičemž nebude vyloučena ani možnost obrátit se na soud se žádostí o soudní přezkum zákonnosti aktů vydaných NBÚ.

c) Reaktivní opatření – reaktivní opatření bude vydáváno ve formě rozhodnutí (případně rozhodnutí na místě) nebo opatření obecné povahy. Proti rozhodnutí návrh zákona umožňuje podat rozklad, který z důvodu nutnosti účinné reakce na kybernetický bezpečnostní incident, jakož i z důvodu ochrany kybernetického prostoru nebude mít odkladný účinek. Před vydáním reaktivního opatření ve formě opatření obecné povahy sice nebude vedeno námitkové a připomínkové řízení podle správního řádu, připomínky však bude možno vůči vydanému opatření obecné povahy uplatnit po jeho vydání. Ochrana práv orgánů a osob je dále zajištěna možností obrátit se na soud s žádostí o soudní přezkum aktů vydaných NBÚ.

d) Ochranné opatření – ochranné opatření bude vydáváno ve formě opatření obecné povahy. Před vydáním opatření obecné povahy sice nebude vedeno námitkové a připomínkové řízení podle správního řádu, avšak připomínky bude možno vůči vydanému opatření obecné povahy uplatnit po jeho vydání. Ochrana práv orgánů a osob je dále zajištěna možností obrátit se na soud s žádostí o soudní přezkum zákonnosti aktů vydaných NBÚ.

e) Nápravná opatření – limity nápravných opatření jsou upraveny přímo v § 24 zákona o kybernetické bezpečnosti. Obsah a rozsah nápravných opatření přitom musí respektovat zásadu proporcionality. Nápravná opatření lze vydat pouze v rámci výkonu kontroly podle kontrolního řádu, který obsahuje ustanovení chránící práva orgánu a osoby při výkonu kontroly.

f) Rozhodnutí o správním deliktu – jedná se o typické rozhodnutí vydané podle správního řádu, proti kterému lze podat rozklad, jež má odkladný účinek, jakož i další opravné prostředky podle správního řádu. Rovněž nebude vyloučena možnost soudního přezkumu rozhodnutí vydaných NBÚ.

9.5 Kontrolní mechanismy

Zákon o kybernetické bezpečnosti rozlišuje pět kategorií orgánů a osob, kterým v závislosti na důležitosti jejich informačních systémů nebo služeb a sítí elektronických komunikací ukládá explicitně stanovené povinnosti. Návrh zákona dále rozšiřuje působnost zákona o kybernetické bezpečnosti o další tři kategorie orgánů a osob. V zákoně o kybernetické bezpečnosti i v návrhu zákona je jednoznačně stanovena odpovědnost provozovatelů základních služeb za kontinuitu poskytování těchto služeb, správců informačních nebo komunikačních systémů za bezpečnost jejich systémů (u

informačních systémů základních služeb se tato povinnost vztahuje i na provozovatele takového systému) a v případě digitálních služeb se pak jedná o poskytovatele těchto služeb.

Návrh zákona nastavuje funkční systém přezkoumávání rozhodnutí přijímaných na jeho základě (viz výše – možnost podat řádné i mimořádné opravné prostředky včetně možnosti soudního přezkumu). Návrh zákona dále stanoví skutkové podstaty správních deliktů spočívající v porušení povinností uložených tímto zákonem nebo na jeho základě. Sankce za správní delikty pak představují pokuty, jejichž výše je závislá na charakteru porušené povinnosti, přičemž správní delikty projednává a pokuty vybírá NBÚ. Právnické osoby a podnikající fyzické osoby pak za správní delikt neodpovídají, jestliže prokážou, že vynaložily veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránily.

Kontrolu činnosti NBÚ vykonává příslušná komise Poslanecké sněmovny Parlamentu České republiky podle § 145 až 147 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů.

9.6 Korupční rizika – poptávková a nabídková stránka

Návrh zákona zakládá nové povinnosti jasně vymezenému okruhu subjektů, v jejichž zájmu je ochrana a zajištění bezpečného kyberprostoru. Nelze proto předpokládat, že by prvotní reakcí regulovaných subjektů byla snaha o neplnění povinností stanovených zákonem nebo na jeho základě, neboť zabezpečení sítí a informačních systémů před kybernetickými bezpečnostními incidenty je zejména v jejich vlastním zájmu.

Povinnosti, které předmětný zákon primárně stanoví, spočívají v zavedení bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů, hlášení kontaktních údajů a provádění opatření, a to u správců a provozovatelů informačních systémů základních služeb v míře obdobné jako pro správce prvků kritické informační infrastruktury. Pro poskytovatele digitální služeb pak budou tyto povinnosti nastaveny v omezeném rozsahu a na provozovatele základních služeb se některé z nich nevztahují (např. aplikace bezpečnostních opatření).

U provozovatelů základních služeb a správců a provozovatelů informačních systémů základních služeb je celkově počítáno s desítkami až nižšími stovkami těchto subjektů. Vzhledem k tomu, že nejvýznamnější subjekty jsou již v současné době regulovány jakožto správci prvků kritické informační infrastruktury, není očekáváno, že by regulace dopadla na subjekty s významnou vyjednávací silou. Spíše se bude jednat o střední podnikatele, tj. subjekty zaměstnávající méně než 250 zaměstnanců, jejichž roční obrat nepřesahuje 50 milionů EUR nebo jejichž bilanční suma roční rozvahy nepřesahuje 43 milionů EUR, případně větší podnikatele a orgány veřejné moci regionální povahy. Provozovatelé základních služeb a správci a provozovatelé informačních systémů základních služeb se však mohou sdružovat, a mnohdy již sdružují, v asociacích, které intenzivně komunikují s veřejnou správou a vyvíjejí inciativy směřující k ovlivnění činnosti orgánů státní správy. Výše nákladů a rozsah změn vzniklých pro správce a provozovatele informačních systémů základních služeb pak závisí na míře bezpečnostních opatření, která již tyto subjekty přijaly dobrovolně, přičemž tato míra je napříč sektory značně rozdílná. Obecně lze však říci, že velká část klíčových subjektů již bezpečnostní opatření přijala a provádí, protože na bezpečnosti sítí a informačních systémů závisí kvalita

poskytování jejich služeb. Navíc je nutno zmínit, že bezpečnost jako taková je u části provozovatelů základních služeb a správců nebo provozovatelů informačních systémů základních služeb regulována i jinými právními předpisy. Zároveň je nutno zdůraznit, že nastavení bezpečnostních opatření vychází z principů mezinárodní normy ISO/IEC 27001, tj. z bezpečnostních pravidel, jimiž se již v současné době většina subjektů, které budou podléhat regulaci předmětného návrhu zákona, řídí. Zavedení bezpečnostních opatření přitom nebude podléhat (na rozdíl od předmětné normy) žádnému certifikačnímu nebo akreditačnímu řízení. Správci a provozovatelé informačních systémů základních služeb budou tedy vést o zavedených bezpečnostních opatřeních příslušnou bezpečnostní dokumentaci a jejich aplikace bude podléhat pouze kontrole ze strany NBÚ.

V případě poskytovatelů digitálních služeb se jedná o zcela novou regulaci, která dopadne na střední podniky, větší podniky regionální povahy, ale i na ty největší podniky a mezinárodní korporace, které disponují velkým kapitálem a značnou vyjednávací silou. Tyto subjekty tak mohou ovlivňovat proces rozhodování orgánů veřejné správy, ať už vlastními prostředky nebo prostřednictvím asociací. Rovněž míra transparence těchto subjektů může být značně rozdílná, vzhledem k jejich velké variabilitě. Poskytovatelé digitálních služeb jsou však zatíženi minimálními povinnostmi a kontrolní oprávnění NBÚ jsou vůči nim omezené. Navíc je možno předpokládat, že většina těchto subjektů již bezpečnost svých sítí a informačních systémů intenzivně řeší, a to v daleko větší míře, než požaduje návrh zákona. S garancí bezpečnosti totiž stojí a padá důvěra uživatelů digitálních služeb, kteří jsou velmi citliví zejména na zacházení s jejich osobními údaji. Možné dopady v případě kybernetického bezpečnostního incidentu by tak u těchto subjektů mohly být mnohonásobně vyšší, než náklady na zavádění bezpečnostních opatření a plnění dalších povinností podle návrhu zákona. V případě závažného narušení bezpečnosti by se pak mohlo jednat dokonce až o likvidační následky.

Povinnost hlásit kybernetické bezpečnostní incidenty a incidenty s významným dopadem na poskytování služeb je založena za účelem pomoci orgánům a osobám v případě výskytu kybernetického bezpečnostního incidentu a zároveň s cílem získat informace o takovém incidentu pro jeho další analýzu NBÚ, respektive vládním nebo národním CERT. NBÚ zde je v podstatě v roli pasivního příjemce s tím, že při příjmu hlášení kybernetických bezpečnostních incidentů nerozhoduje o právech a povinnostech orgánů a osob. Prostor pro vznik korupčního jednání zde tak reálně nemůže vzniknout.

Oproti tomu povinnost aplikovat reaktivní a ochranná opatření vydaná NBÚ by mohla být potenciální příčinou vzniku korupčního prostředí. Vzhledem ke skutečnosti, že tyto dva druhy opatření budou vydávaná formou rozhodnutí nebo opatření obecné povahy, které budou ukládat orgánům a osobám povinnosti, jež mohou představovat zvýšené náklady na bezpečnost jejich sítí a informačních systémů, případně omezení jejich činnosti a s tím spojené ztráty, lze předpokládat zvýšený zájem orgánů a osob na vydání takových opatření, která jejich případné finanční ztráty eliminují. V této rovině by tak povinné subjekty mohly vyvíjet snahu o ovlivnění některých opatření. Na řešení daného kybernetického bezpečnostního incidentu se však vždy bude podílet několik zaměstnanců NBÚ s odpovídající odbornou kvalifikací, což by mělo jednak přispět k vydání efektivních opatření, jakož i ke ztížení možného úmyslného ovlivňování jejich vydávání. Rozhodování pak není svěřeno nižším stupňům řízení a podílí se na něm pracovníci více organizačních celků NBÚ. Řešení kybernetických bezpečnostních incidentů je pak postaveno na porovnání vydaného opatření s jeho výsledkem po provedení orgánem a osobou, která je povinna zaslat NBÚ oznámení o provedení reaktivního

opatření a jeho výsledek. Tímto opatřením tak dojde k výraznému zvýšení efektivity opatření a ke stanovení systému kontroly.

Co se týče navrhované úpravy horní hranice sankcí za nezavedení bezpečnostních opatření, nevedení bezpečnostní dokumentace nebo neprovedení nápravných opatření vydaných v rámci kontroly, je v této oblasti zvýšené riziko vzniku prostředí podněcujícího ke korupčnímu jednání, ať už ze strany účastníků řízení nebo úředních osob. Je však nutno uvést, že reálná výše pokuty je vždy závislá na závažnosti správního deliktu, zejména pak na způsobu jeho spáchání, způsobeným následkům a okolnostem, za nichž byl správní delikt spáchán. Uložení sankce blížící se horní hranici pokuty tak bude zvažováno v opravdu výjimečně závažných situacích, přičemž u většiny případů lze očekávat uložení sankcí o několik řádů nižších. Horní hranice sankcí tak má mít zejména odstrašující efekt. Postup ve správním řízení pak bude probíhat podle správního řádu, tj. v rámci NBÚ se bude rozhodovat v prvním a druhém stupni, přičemž účastníci mají rovněž možnost uplatnění řádných i mimořádných opravných prostředků před soudem. Navíc bude do správního řízení vždy zapojeno několik zaměstnanců NBÚ s odpovídající odbornou kvalifikací, což by mělo jednak přispět k efektivitě celého procesu, jakož i ke ztížení možného úmyslného ovlivňování průběhu správního řízení.

9.7 Transparence a otevřená data

Na internetových stránkách vládního i národního CERT jsou již nyní zveřejňovány údaje o hrozbách a zranitelnostech v oblasti kybernetické bezpečnosti. Zákon o kybernetické bezpečnosti pak explicitně stanoví povinnost NBÚ zveřejňovat opatření vydávaná ve formě varování na internetových stránkách vládního CERT. Návrh zákona pak dále nově umožňuje informování veřejnosti o jednotlivých kybernetických bezpečnostních incidentech i v případech, že je to nezbytné k jejich řešení. Aby však byla co nejvíce zohledněna citlivá povaha těchto zveřejňovaných informací, může tak NBÚ učinit pouze po konzultaci s postiženým provozovatelem základních služeb, správcem nebo provozovatelem informačního systému základních služeb nebo poskytovatelem digitálních služeb.

Rovněž tak i určené prvky kritické informační infrastruktury a reaktivní a ochranná opatření vydaná ve formě opatření obecné povahy jsou zveřejňována na internetových stránkách a úřední desce NBÚ. Obdobný postup je předpokládán i v případě určování provozovatelů základních služeb.

Dále jsou zveřejňovány statistické údaje o kybernetických bezpečnostních incidentech, jakož i informace o uzavření veřejnoprávní smlouvy s provozovatelem národního CERT.

Naopak z důvodu ochrany oprávněných zájmů orgánů a osob, jakož i zajištění účinnosti vydaných opatření nebude NBÚ některé údaje povinen poskytovat (např. údaje, z nichž by bylo možné identifikovat orgán a osobu, která ohlásila kybernetický bezpečnostní incident). Ty údaje, které nebude možné poskytnout ke zveřejnění, budou chráněny v evidenci, kterou povede NBÚ, přičemž zaměstnanci NBÚ, kteří se podílejí na řešení kybernetických bezpečnostních incidentů, jsou vázáni institutem mlčenlivosti, který trvá i po ukončení pracovněprávního vztahu. Povinnosti mlčenlivosti pak mohou být zproštění pouze ředitelem NBÚ. Na takovéto údaje se pak podle zákona o kybernetické bezpečnosti vztahuje i výjimka podle § 11 odst. 4 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

Nově je pak stanovena návrhem zákona povinnost vládního CERT i provozovatele národního CERT zachovávat bezpečnost a obchodní zájmy ohlašujícího subjektu v případě předání informace o incidentu s významným dopadem na kontinuitu poskytování základní služby nebo digitální služby příslušnému orgánu jiného členského státu.

Vedle této obecné povinnost je však nově uložena povinnost mlčenlivosti i správcům prvků kritické informační infrastruktury, správcům významných informačních systémů a správcům a provozovatelům informačních systémů základních služeb ohledně jimi přijatých bezpečnostních opatření. Tato povinnost se vztahuje i na zaměstnance těchto orgánů a osob. Jedná se o opatření, které má zabránit vyzrazení citlivých údajů týkajících se zabezpečení sítí a informačních systémů. Únik takovýchto informací by totiž ohrozil provádění bezpečnostních opatření a představuje tak značné bezpečnostní riziko.

Údaje, které budou na základě návrhu zákona zveřejňovány, budou zveřejňovány ve formátech otevřených dat, s nimiž lze bez dalšího dále pracovat.

Postupy, procesy a sankce obsažené v navrhované právní úpravě vycházejí z aktuálních poznatků v oblasti kybernetické bezpečnosti, z vývoje budování vládního a národního CERT, jakož i z aktuálních bezpečnostních potřeb zacílených na ochranu kybernetického prostoru a z požadavků stanovených směrnicí. Právní úpravu, jejíž procesní postupy se až na odůvodněné odchylky řídí správním a kontrolním řádem, tak lze označit za přiměřenou.

Při přípravě tohoto návrhu zákona byl brán též zřetel na aktuální poznatky z praxe, společenský diskurz a především pak na názory odborné veřejnosti. Stávající právní úprava ve výše zmíněných diskutovaných oblastech byla pouze vhodně doplněna s ohledem na požadavky vyplývající z právních předpisů EU či na požadavky praxe a sociálních partnerů.

9.8 Shoda s dobrou praxí a srovnání se stávající legislativou

Současná právní úprava zákona o kybernetické bezpečnosti byla již během svého projednávání konzultována s odbornou veřejností, přičemž do ní byly zapracovány mnohé poznatky z praxe i již existující osvědčené postupy. Největší důraz byl pak na tento postup kladen při vypracovávání bezpečnostních standardů, které musí jednotlivé orgány a osoby splňovat. Tyto standardy vycházejí z normy ISO 27 001. V tomto ohledu zachovává návrh zákona standardy nastavené zákonem o kybernetické bezpečnosti a do vytvořeného režimu předcházení, detekce a řešení kybernetických bezpečnostních incidentů výrazněji nezasahuje.

Oproti současné právní úpravě je však navrhováno zvýšení sankcí, přičemž navrhovaná horní hranice činí až 5 mil. Kč. Podle zákona o kybernetické bezpečnosti bylo za neplnění některých povinností možno uložit pokutu v maximální horní výši 100 tis. Kč. Tato hranice se však ukázala být jako nedostačující. Vzhledem k poměrně náročnému a drahému zavádění bezpečnostních opatření by se mnohdy povinným orgánům a osobám mohlo spíše vyplatit tyto povinnosti nesplnit a zaplatit uloženou pokutu. Navíc je tato pokuta nepřiměřená i v poměru vůči obratu některých subjektů (např. v oblasti energetiky). Orgány státní správy by tak měly mít větší možnost diskrece při posuzování přiměřenosti pokuty vůči konkrétnímu subjektu, stejně jako vůči míře jeho provinění. Toho je nutno

dosáhnout i vzhledem k povinnosti uložené ČR směrnicí stanovit účinné, přiměřené a odrazující sankce.

Přiměřenost navrhované právní úpravy sankcí je možno v tomto ohledu porovnat s právní úpravou zákona o elektronických komunikacích. Ten v případě, že podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací nezajistí bezpečnost a integritu své sítě nebo bezpečnost služeb, které poskytuje, podle § 98 odst. 1 zákona o elektronických komunikacích, umožňuje uložení pokuty s horní hranicí až 20 mil. Kč.

Je tedy možno konstatovat, že návrh zákona bere zřetel na aktuální poznatky z praxe, společenský diskurz a na názory odborné veřejnosti, přičemž umožňuje správním orgánům naplnit účel příslušné legislativy EU.

9.9 Systematický sběr dat

Data o zjištěných korupčních rizicích budou systematicky sbírána. Zejména budou v tomto ohledu sledována korupční rizika vyplývající z ukládání opatření NBÚ a sankcí za porušení povinností stanovených zákonem o kybernetické bezpečnosti. Tato data budou dále průběžně vyhodnocována a na základě zjištěných výsledků budou využita v rámci mapování korupčních rizik.

9.10 Závěr

Vyhodnocením poznatků podle metodiky CIA bylo zjištěno, že vzhledem k charakteru právního předpisu, tj. návrhu zákona, kterým se mění zákon o kybernetické bezpečnosti a zákon o svobodném přístupu k informacím, který je veřejnoprávním předpisem, dojde k mírnému zvýšení korupčního rizika, a to zejména v oblasti ukládání opatření (reaktivních a ochranných) NBÚ a ukládání sankcí za porušení povinností stanovených v zákoně o kybernetické bezpečnosti doplněném u ustanovení návrhu zákona. Při existenci základních principů správního řízení, při důsledném uplatňování rozhodovacích a kontrolních mechanismům, při nezávislosti a nestrannosti justice a při zaměstnávání dostatečně kvalifikovaných zaměstnanců je zde však dán předpoklad, že dojde k minimalizaci těchto potenciálních korupčních rizik.

10. Dopady na bezpečnost nebo obranu státu

Vzhledem k povaze výše navrhovaných změn lze konstatovat, že návrh zákona má pozitivní dopady na bezpečnost a obranu státu. Zejména přispěje k posílení zabezpečení klíčových sítí a informačních systémů v ČR, čímž dojde k posílení zabezpečení českého kyberprostoru jako takového. Rovněž dojde k navázání bližší spolupráce mezi členskými státy EU, čímž bude zlepšena i možnost včasné a efektivní reakce při vzniku masivního kybernetického bezpečnostního incidentu.

Návrh zákona zároveň reflektuje připomínky získané zejména ze strany odborné veřejnosti, které se vztahují k problémovým oblastem zákona o kybernetické bezpečnosti. Tyto připomínky částečně vycházejí i z aplikace moderních technologií (např. cloudová řešení) do prvků kritické informační infrastruktury. Odstranění těchto zákonných nedostatků povede k dalšímu posílení zabezpečení ČR

proti kybernetickým hrozbám a zároveň plně zohlední současných technologický vývoj a vznikající bezpečnostní rizika.

11. Soulad navrhované právní úpravy s ústavním pořádkem ČR

Aplikací zákona o kybernetické bezpečnosti je zasahováno zejména do práva vlastnického a částečně též i z něj odvozovaného práva na podnikání. Povinnosti, které navrhovaná právní úprava stanoví vybraným subjektům (tj. orgánům a osobám), totiž v různé míře omezují tyto subjekty v neomezeném užívání sítí a informačních systémů, k nimž vykonávají vlastnická nebo obdobná práva.

Vzhledem k tomu, že byl při tvorbě zákona zvolen minimalistický přístup k ukládání povinností osobám soukromého práva, nezasahuje tento záměr do práva na ochranu soukromí, práva na ochranu osobních údajů, práva na soukromý život, práva na svobodu projevu ani do dalších práv souhrnně označovaných jako práva na informační sebeurčení člověka – ochrana těchto práv naopak tvoří dominantní teleologii navrhované právní úpravy.

Kybernetické bezpečnostní incidenty mají za následek vedle různých typů škod též omezení dostupnosti služeb informační společnosti nebo zásahy do informační diskrece člověka. Právo na informační sebeurčení, které bylo jako souborné základní právo identifikováno Spolkovým ústavním soudem[40] a od té doby též několikrát zmíněno i Evropským soudem pro lidská práva a Ústavním soudem České republiky[41], přitom sestává z pasivních a aktivních informačních práv člověka. Pasivní informační práva zahrnují především ochranu soukromí či obecně diskrétní informační sféry, zatímco aktivní informační práva mají charakter práv přístupu ke službám informační společnosti. Definice informačního sebeurčení tak vychází nejen z předpokládané nutnosti chránit diskrétní informace, ale též z předpokladu, že dnešní člověk může žít plnohodnotný život jen tehdy, pokud má možnost komunikovat s ostatními. Z toho plyne povinnost státu chránit pasivní i aktivní informační práva člověka ochranou kybernetického prostoru, kde se tato práva realizují.

Navrhovaná právní úprava omezí plošně provozovatele základních služeb, správce a provozovatele informačních systémů základních služeb a poskytovatele digitálních služeb. Plošné omezení vlastnického práva resp. práva na podnikání má v tomto případě formu zavedení povinnosti implementovat bezpečnostní opatření, oznámit provozovateli národního CERT nebo NBÚ kontaktní údaje a hlásit kybernetické bezpečnostní incidenty vládnímu nebo národnímu CERT. U správců nebo provozovatelů informačních systémů základních služeb se pak bude jednat i o plnění povinnosti detekce kybernetických bezpečnostních událostí a povinnosti provádět opatření vydaná NBÚ.

Navrhovaná úprava bezprostředně nezasahuje do práva na informační sebeurčení člověka, neboť primárně nezasahuje do obsahové stránky komunikace a nezakládá ani přímé pravomoci státu direktivně zasahovat do běžného života informační společnosti – návrh zákona tedy nepředpokládá

[40] Nález Spolkového ústavního soudu ze dne 15. prosince 1983, č. j. BVerfGE 65, 1.
[41] Nález Ústavního soudu ze dne 1. března 2000, č. j. II. ÚS 517/99, N 32/17 SbNU 229, nález Ústavního soudu ze dne 7. dubna 2010, č. j. I. ÚS 22/10 a nález Ústavního soudu ze dne 22.března 2011, sp. zn. Pl. ÚS 24/10, 94/2011 Sb.

žádný státní zásah do soukromí uživatelů ani do jejich možností komunikovat prostřednictvím služeb informační společnosti.

Právo na informační sebeurčení člověka je návrhem zákona zpracováno jako hodnota, k jejíž ochraně návrh zákona směřuje. V tomto případě má návrh zákona jasně vymezenou teleologii, která spočívá v zabezpečení části kybernetického prostoru, která nebyla dosud pokryta stávající úpravou zákona o kybernetické bezpečnosti, přičemž zejména prostřednictvím digitálních služeb lze svobodně realizovat právo na informační sebeurčení člověka.

Vedle závazků ČR plynoucích ze členství v EU představuje zásadní důvod k úpravě kybernetické bezpečnosti (to i včetně shora uvedeného omezení vlastnického práva) základní princip mezinárodního práva, tj. povinnost bdělosti (due diligence). Je v tomto směru jen otázkou času, kdy začne Mezinárodní soudní dvůr řešit odpovědnost státu za jednání, kterého se sice stát sám neúčastní, ale které je mu přičitatelné, neboť má původ v jeho suverénní doméně. Typicky dochází k situaci, kdy jsou zneužity počítače na území jednoho státu k útoku na cizí stát (takové případy se u rozsáhlých útoků vyskytují běžně) – předmětný stát, přestože útok neorganizuje ani se na něm nepodílí, může být popohnán k odpovědnosti za to, že takovému útoku, byť k tomu měl prostředky, účinně nezabránil.

Výše zmíněný zásah do vlastnického práva soukromoprávních provozovatelů základních služeb, správců a provozovatelů informačních systémů základních služeb a poskytovatelů digitálních služeb je tedy ve struktuře proporcionality odůvodněn ochranou

- práva na informační sebeurčení (tj. zejména práva na ochranu soukromí, soukromého života, na svobodu projevu, na přístup k informacím a dalších informačních práv člověka),

- bezpečnosti a integrity (nedistributivních práv) ČR a

- mezinárodních závazků ČR.

Vzhledem k tomu, že návrh zákona nezatěžuje nikterak právo na informační sebeurčení soukromoprávních osob (tj. nedává státním orgánům právo zasahovat do soukromí ani do aktivní komunikace uživatelů služeb informační společnosti) a naopak zvyšuje míru ochrany základních práv a nedistributivních veřejných statků, lze konstatovat, že bez problémů vyhovuje požadavkům ústavní proporcionality a je tedy ústavně konformní.

12. Slučitelnost navrhované právní úpravy s mezinárodním právem a právem EU

Problematika kybernetické bezpečnosti je v současné době na úrovni EU průřezově řešena pouze předmětnou směrnicí. V této oblasti se jednalo o první právní předpis EU týkající se kybernetické bezpečnosti. ČR již v tomto ohledu část povinností stanovených směrnicí naplňovala – např. povinnost vytvoření národní strategie pro bezpečnost sítí a informačních systémů. Zbývající povinnosti, které nejsou upraveny již stávajícím zákonem o kybernetické bezpečnosti, do něj budou doplněny předloženým návrhem zákona, který je v plném souladu s požadavky směrnice.

S touto problematikou však souvisejí i další právní předpisy EU, které jsou zaměřeny na konkrétní sektorové úpravy. Jedná se v tomto ohledu zejména o problematiku služeb elektronických komunikací, poskytovatelů služeb vytvářejících důvěru, oblast ochrany osobních údajů a kybernetickou trestnou činnost.

Předmětná směrnice, a tedy i návrh zákona, přímo souvisí s těmito právními předpisy EU:

- Směrnice Evropského parlamentu a Rady 2002/21/ES ze dne 7. března 2002 o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice), ve znění směrnice 2009/140/ES,
- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 z dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, ve znění nařízení č. 1007/2008,
- Nařízení Evropského parlamentu a Rady (EU) č. 526/2013 ze dne 21. května 2013 o Agentuře Evropské unie pro bezpečnost sítí a informací (ENISA) a o zrušení nařízení (ES) č. 460/2004,
- Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů),
- Směrnice Evropského parlamentu a Rady 2015/2366 ze dne 25. listopadu 2015 o platebních službách na vnitřním trhu, kterou se mění směrnice 2002/65/ES, 2009/110/ES a 2013/36/EU a nařízení (EU) č. 1093/2010 a zrušuje směrnice 2007/64/ES (dále jen „revidovaná směrnice o platebních službách“),
- Směrnice Rady 2008/114/ES ze dne 8. prosince 2008 o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu,
- Směrnice Evropského parlamentu a Rady 2011/93/EU ze dne 13. prosince 2011 o boji proti pohlavnímu zneužívání a pohlavnímu vykořisťování dětí a proti dětské pornografii, kterou se nahrazuje rámcové rozhodnutí Rady 2004/68/SVV,
- Směrnice Evropského parlamentu a Rady 2013/40/EU ze dne 12. srpna 2013 o útocích na informační systémy a nahrazení rámcového rozhodnutí Rady 2005/222/SVV,
- Směrnice Evropského parlamentu a Rady (EU) 2015/1535 ze dne 9. září 2015 o postupu při poskytování informací v oblasti technických předpisů a předpisů pro služby informační společnosti,
- Směrnice Evropského parlamentu a Rady 2013/11/EU ze dne 21. května 2013 o alternativním řešení spotřebitelských sporů a o změně nařízení (ES) č. 2006/2004 a směrnice 2009/22/ES (směrnice o alternativním řešení spotřebitelských sporů),
- Doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků, malých a středních podniků.

Ze shora uvedených dokumentů se kybernetické bezpečnosti přímo dotýká pouze rámcová směrnice, nařízení eIDAS a revidovaná směrnice o platebních službách. Tyto právní předpisy upravují oblast kybernetické bezpečnosti pro úzce vymezený okruh subjektů. V případě rámcové směrnice se tak úprava dotýká pouze podniků zajišťujících veřejné komunikační sítě nebo poskytující veřejně dostupné služby elektronických komunikací, v případě nařízení eIDAS poskytovatelů služeb vytvářejících důvěru a v případě revidované směrnice o platebních službách internetových platebních bran. Směrnice v tomto ohledu stanoví konkrétní výjimky pro subjekty regulované podle rámcové

směrnice a nařízení eIDAS, kdy tyto subjekty nebudou spadat pod regulaci směrnice, potažmo tedy návrhu zákona, nýbrž pod regulaci jednotlivých odvětvových právních předpisů. Pro ostatní subjekty, které jsou již regulovány zvláštní odvětvovou legislativou, platí obecná výjimka z režimu směrnice na základě klauzule lex specialis, která se ale uplatňuje pouze tehdy, pokud jsou požadavky odvětvového právního aktu EU co do účinku přinejmenším rovnocenné povinnostem stanoveným ve směrnici.

Ostatní uvedené dokumenty se problematiky kybernetické bezpečnosti dotýkají pouze v širších souvislostech a do návrhu zákona o kybernetické bezpečnosti proto nejsou transponovány.

Mezi další dokumenty EU, které upravují oblast kybernetické bezpečnosti a související otázky, patří Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor[42] a Strategie pro jednotný digitální trh v Evropě[43].

Na mezinárodní úrovni zatím žádná komplexní právní úprava kybernetické bezpečnosti neexistuje. Je však již k dispozici celá řada mezinárodních právních předpisů a koncepčních dokumentů upravujících buď partikulární aspekty kybernetické bezpečnosti, nebo oblasti s ní úzce související. Jedná se v tomto ohledu zejména o dokumenty týkající se problematiky kybernetické trestné činnosti a kybernetické války. Prvním z nich je Úmluva Rady Evropy o kybernetické kriminalitě[44], druhým je Tallinnský manuál, který se zabývá aplikovatelností principů mezinárodního práva na kybernetickou válku.

Na základě výše uvedených skutečnostní lze konstatovat, že navrhovaná právní úprava je plně v souladu s mezinárodními smlouvami, jimiž je ČR vázána, a je plně slučitelná s předpisy EU.

13. Kontakty na zpracovatele RIA

Mgr. Bc. Hana Valentová
Národní bezpečnostní úřad
Odbor právní a legislativní
Na Popelce 2/16, Praha 5, 150 00
tel.:+420 257 283 432
e-mail: h.valentova@nbu.cz, posta@nbu.cz

[42] JOIN(2013) 1 final.
[43] COM(2015) 192 final.
[44] Úmluva Rady Evropy o kybernetické kriminalitě č. 185 ze dne 23. listopadu 2001, publikovaná pod č. 104/2013 Sb.m.s.