Věcný záměr zákona o kybernetické bezpečnosti

(Návrh pro vnější připomínkové řízení)

Obsah

A: Závěrečná zpráva o hodnocení dopadů regulace

1. Důvod předložení

1.1 Vnější vlivy

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 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.). Se vzrůstající závislostí společnosti na informačních technologiích pak ale na straně druhé vzrůstá i riziko zneužívání těchto technologií, které má rozsáhlé dopady do činnosti subjektů, které s nimi pracují, a potencionálně může vést ke značným škodám.

Obecným trendem v celém světě je kvalitní ochrana těchto informačních technologií před zásahy, které mohou ohrozit jejich chod. Cílené útoky proti informačním technologiím jsou celosvětovým fenoménem a jejich dopad způsobuje rozsáhlé ekonomické škody ve veřejném i v soukromém sektoru a současně jsou schopny vyvolat negativní politické důsledky, a to jak v národním měřítku, tak v měřítku globálním. V případech, kdy je útok veden proti prvkům kritické infrastruktury, může být v konečném důsledku ohrožena bezpečnost nebo samotná existence státu.

Útoky proti informačním technologiím jsou stále sofistikovanější a komplexnější. Ze sféry přímého ekonomického prospěchu individuálních útočníků se útoky přesouvají do oblasti organizované kybernetické průmyslové špionáže a kybernetického terorismu. Útočníci se stále více zaměřují na prvky kritické infrastruktury, jako jsou energetické systémy, produktovody, zdravotnické informační systémy a informační systémy veřejné správy.

S ohledem na fakt, že kybernetický prostor nezná hranic a není tedy otázkou teritoriální, je nutné útoky na informační technologie řešit z pohledu mezinárodního společenství a s ohledem na závazky České republiky vůči státům Organizace Severoatlantické smlouvy (dále jen „NATO“) a Evropské unie (dále jen „EU“). V rámci

mezinárodní regulace tohoto fenoménu je vyvíjen na Českou republiku tlak, aby problematiku ochrany kybernetického prostoru řešila formou závazné právní regulace.

Zajištění kybernetické bezpečnosti státu je jednou z klíčových výzev současné doby. Lisabonský summit NATO uskutečněný v roce 2010 mimo jiné zdůraznil nutnost řešení této problematiky jak na mezinárodní úrovni, tak i na úrovni národní. Bezhraničnost a všudypřítomnost kybernetických hrozeb vyžaduje intenzivní mezinárodní spolupráci a také intenzivní úsilí při zajišťování kybernetické bezpečnosti jednotlivých států.

Oblast kybernetické bezpečnosti je a bude jedním z určujících aspektů bezpečnostního prostředí České republiky. Všechny vyspělé země, mezi něž Česká republika bezesporu patří, jsou již zcela závislé na správném fungování informačních a komunikačních systémů. Tyto systémy podmiňují vznik a rozvoj konkurenceschopné společnosti založené na využívání vyspělých technologiích a správnou funkci informační společnosti. Služby informační společnosti a související zařízení a činnosti jsou jedním z nejdynamičtěji se rozvíjejících sektorů každé moderní ekonomiky, na jejichž fungování závisí ekonomický úspěch řady podnikatelských subjektů a do jisté míry i kvalita života všech občanů. Bezpečnost kyberprostoru každé země se stává hodnotícím kritériem pro investory a významně ovlivňuje konkurenceschopnost dané země.

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.

Je zřejmé, že nejen ekonomické aktivity se přesouvají do kyberprostoru. Vznikem sociálních sítí, herních sítí a zájmových sítí se z nejznámější části kyberprostoru, z internetu, stává významný celospolečenský jev, jehož prostřednictvím lze společnost výrazně pozitivně nebo i negativně ovlivňovat.

1.2 Vnitřní vlivy

V České republice se ochrana kybernetického prostoru řeší prostřednictvím privátních subjektů bez regulace, prostřednictvím partikulárních pracovišť. Tato

pracoviště často řeší případné útoky na informační technologie nahodile ad hoc, bez kvalifikovaných doporučení z centrální úrovně; nemají tak ani poznatky o útocích, které již byly řešeny, a musí je řešit samostatně a zvyšují se tak zbytečně náklady na jejich řešení.

V oblasti veřejné správy neexistuje jednotný způsob stanovení bezpečnostních standardů, které by minimalizovaly potencionální škody vzniklé z kybernetických útoků. Rovněž chybí systém prevence a včasného varování před těmito útoky. V souvislosti s probíhající elektronizací veřejné správy je hrozba kybernetických útoků stále aktuálnější a je zcela nezbytné přijmout opatření, která by státu umožňovala v rámci veřejné správy reagovat na tuto celospolečenskou hrozbu z centrální pozice, tak jak to odpovídá zahraničním zkušenostem se závažnými útoky. Dalším vlivem je snaha o výrazné zefektivnění výkonu veřejné správy.

Vzhledem k tomu, že státní moc lze uplatňovat výlučně na základě a v mezích zákona a privátním subjektům lze ukládat povinnosti jen zákonem, je třeba regulaci oblasti kybernetické bezpečnosti provést zákonem, s podrobným rozdělením povinností subjektů, které jsou primárně důležité pro chod státu, a subjektů ostatních, vymezením rolí subjektů dotčených veřejnoprávní regulací a sjednocením pojmů užívaných v oblasti kybernetické bezpečnosti.

Mezi hlavní rizika spojená s nečinností se řadí nárůst kybernetických útoků, výrazné materiální škody, ohrožení kritické infrastruktury státu a v neposlední řadě i neplnění mezinárodních závazků České republiky včetně závazků plynoucích ze smluv o ochraně investic.

V neposlední řadě je významným vnitřním vlivem přijetí usnesení vlády České republiky ze dne 19. října 2011 č. 781 o ustavení Národního bezpečnostního úřadu (dále jen „NBÚ“) gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Tímto usnesení vlády bylo NBÚ mimo jiné uloženo vybudovat do konce roku 2015 plně funkční Národní centrum kybernetické bezpečnosti.

1.3 Popis cílového stavu v oblasti kybernetické bezpečnosti

Základním cílem zákona o kybernetické bezpečnosti je zvýšit bezpečnost kybernetického prostoru, nastavit mechanismus aktivní spolupráce mezi soukromým

sektorem a veřejnou správou za účelem vyšší efektivity při řešení kybernetických bezpečnostních událostí a v této souvislosti zavést do praxe soubor oprávnění a povinností. Nastavením předvídatelného transparentního postupu pro subjekty, které budou zatíženy regulací, spočívajícího v postupných krocích, které mají zajistit detailnější přehled o hrozbách a rizicích, která se vyskytují v kybernetickém prostoru, se zajistí možnost v rychlém sledu reagovat na nové hrozby, které v budoucnu nastanou. Věcný záměr si neklade za cíl postihnout a eliminovat všechna rizika, která se mohou dotknout všech uživatelů kybernetického prostoru, ale bude se snažit ochránit tu část infrastruktury, která je pro fungování státu významná a jejíž narušení by vedlo k poškození nebo ohrožení zájmu České republiky. Pro takové subjekty budou stanoveny konkrétní povinnosti, prostřednictvím kterých dojde ke zvýšení ochrany jejich informačních systémů, resp. sítí, které provozují. Tyto povinnosti lze vnímat jako v zásadě minimalistické avšak přesto zajišťující dosažení předpokládaného cíle. Pro tzv. běžné uživatele budou vydávána doporučení a bude přistoupeno k formulování závěrů nejlepší praxe.

Cíle jsou stanoveny v kategoriích:

- Konstituce práv a povinností orgánu státu, jemuž je svěřena konkrétní pravomoc v oblasti zajišťování kybernetické bezpečnosti v souvislosti s právy a povinnostmi dalších orgánů státu a soukromoprávních subjektů, které v této oblasti participují.
- Nastavení mechanismu přenosu informací nezbytných pro prevenci před kybernetickými hrozbami, které budou sloužit pro analýzu možných kybernetických útoků a pro způsoby jejich včasného rozpoznání.
- Vybudování systému včasného varování, prevence a osvěty včetně poskytování pomoci při zavádění preventivních opatření a protiopatření při hrozícím útoku.
- Standardizace nastavení bezpečnosti systémů nezbytných pro chod státu v rámci kritické komunikační a informační infrastruktury státu.
- Stanovení pravidel pro koordinaci činností pro odvrácení a při odvracení hrozícího útoku na prvky kritické komunikační a informační infrastruktury státu a k řešení situací, v nichž je potřeba přijímat opatření před možným následkem hrozícího útoku.

Konečným cílem uvedených aktivit je vytvoření a udržení důvěryhodné a konkurenceschopné informační společnosti, s důrazem na rozvoj svobodného a bezpečného využívání a sdílení informací a v neposlední řadě i zlepšení obrazu státu v této oblasti, a to jak v kontextu národním i mezinárodním.

1.4 Popis současného stavu a dílčích řešení kybernetické bezpečnosti

Dosavadní vývoj řešení národní kybernetické bezpečnosti byl v České republice především předmětem vládních koncepčních dokumentů a iniciativ soukromého a akademického sektoru. Lze jej shrnout následovně:

2000 - Aktualizovaná koncepce boje proti organizovanému zločinu[1)]

Tento dokument uložil Ministerstvu vnitra mimo jiné „průběžně koncepčně řešit potírání organizovaných zločineckých aktivit v oblasti informačních technologií".

2001 - Koncepce boje proti trestné činnosti v oblasti informačních technologií[2)]

Ta byla přijata v souladu s povinnostmi uloženými Ministerstvu vnitra Aktualizovanou koncepcí boje proti organizovanému zločinu, a představovala první podstatnější dokument, který obsahuje snahu o zajištění kybernetické bezpečnosti. Její Harmonogram opatření ukládá odboru bezpečnostní politiky Ministerstva vnitra, ve spolupráci také s odborem komunikačních a informačních služeb, odborem koncepcí a organizace, Policejním prezidiem a Úřadem vyšetřování za úkol mimo jiné:

- Zajistit podmínky pro další rozvoj (včetně materiálního a personálního posilování) struktur, přímo zapojených do potírání informační kriminality.
- Rozšiřovat a podporovat spolupráci policejních orgánů se zpravodajskými službami a nevládními neziskovými subjekty, zabývajícími se problematikou boje proti některým aspektům informační kriminality.
- Vypracovat principy plánu ochrany státních a některých strategicky důležitých nestátních informačních systémů.

---

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

2) Schválena ministrem vnitra dne 5. června 2001.

- Vypracovat projekt hlásného systému pro trestnou činnost v oblasti informačních technologií.
- Iniciovat vznik a podporovat činnosti skupiny typu CERT (Computer Emergency Response Team) jako nevládního sdružení kvalifikovaných odborníků informujících ostatní profesionály o bezpečnostních problémech a reagujících na probíhající útoky.
- Vypracovat projekt vzdělávání a doškolování orgánů činných v trestním řízení, s důrazem na objasňování trestné činnosti v oblasti informačních technologií (včetně přípravy výukových materiálů).
- Vyvíjet a zavádět forenzní standardy pro vyhledávání a ověřování elektronických dat při kriminálním vyšetřování a trestním řízení.
- Podporovat nezávislou výzkumnou, publicistickou a dokumentaristickou činnost, zabývající se kybernetickými incidenty.
- Provádět osvětu a propagaci náležitého chování nejširší i odborné veřejnosti, související s bojem proti informační kriminalitě.
- Sledovat aktivity mezinárodních a nadnárodních organizací v oblasti boje proti trestné činnosti v oblasti informačních technologií. Aktivně se zúčastňovat mezinárodních akcí, týkajících se boje proti informační kriminalitě.

2004 – Státní informační a komunikační politika e-Česko 2006[3)]

Tento dokument byl schválen v souvislosti s očekávaným vstupem České republiky do Evropské unie a za cíl si stanovil definovat „hlavní zásady a principy, které vláda hodlá uplatňovat při dalším rozvoji informační společnosti v České republice“. Mimo jiné stanovil čtyři prioritní oblasti Státní informační a komunikační politiky, přičemž jednou z nich jsou dostupné a bezpečné komunikační služby. V oblasti bezpečnosti elektronických komunikací si pak vláda stanovila za cíl aktivně podporovat zajištění bezpečnosti komunikační infrastruktury uvnitř státu a u bezpečnostních řešení, která mají mít oporu v zákoně, závazně specifikovat parametry, vlastnosti a podmínky, kterých musí dosahovat. I na základě tohoto dokumentu byly zpracovávány další strategické dokumenty týkající se informačních systémů v České republice

[3)] Připravena Ministerstvem informatiky a přijata usnesením vlády České republiky ze dne 24. března 2004 č. 265.

zpracovávány s cílem posílení informační bezpečnosti v oblasti komunikační a informační infrastruktury České republiky a v souladu s § 4 odst. 1 písm. b) zákona č. 365/2000 Sb., o informačních systémech veřejné správy.

2005 – Národní strategie informační bezpečnosti České republiky[4)]

Národní strategie informační bezpečnosti České republiky stanovila úkoly v oblasti vytváření důvěryhodných informačních a komunikačních systémů v podmínkách České republiky. Cíle této strategie jsou mimo jiné „zlepšení řízení informační bezpečnosti a řízení rizik“, „rozvoj znalostí o informační bezpečnosti“, „podpora národní a mezinárodní spolupráce v oblasti informační bezpečnosti“. Za účelem jejich dosažení jsou pak stanovena následující opatření:

- Zavedení nejlepší praxe (best practice) do systémů řízení informační bezpečnosti.
- Soustavné monitorování hrozeb.
- Realizace systému včasného varování a reakce (součástí tohoto opatření je také úkol ustavit národní centrum pro řízení, monitoring a analýzu bezpečnostního prostředí informačních a komunikačních systémů České republiky).
- Monitorování účinnosti navržených protiopatření.
- Zlepšení informační bezpečnosti orgánů veřejné správy.
- Ochrana kritické informační infrastruktury státu.
- Zvyšovat povědomí o informační bezpečnosti, bezpečnostních rizicích a možnostech obrany u občanů, subjektů komerční a nekomerční sféry a orgánů veřejné správy.
- Zavést školicí a vzdělávací programy.
- Podpořit celkový program národního povědomí o informační bezpečnosti.
- Zvýšit efektivnost školicích programů.

[4)] Usnesení vlády České republiky ze dne 19. října 2005 č. 1340, o Národní strategii informační bezpečnosti České republiky a o zřízení Výboru pro informační bezpečnost České republiky.

- Zvýšit povědomí uživatelů o důležitosti užívání bezpečnostně certifikovaných výrobků a služeb z oboru informačních a komunikačních technologií.
- Realizace efektivní spolupráce a koordinace na národní úrovni.
- Realizace aktivní mezinárodní spolupráce.
- Zlepšení spolupráce při národní obraně proti informačním hrozbám.

Na tento dokument navazuje Akční plán realizace opatření Národní strategie informační bezpečnosti České republiky a návrh nařízení vlády k realizaci úkolů stanovených Národní strategií informační bezpečnosti České republiky ze strany orgánů a organizací veřejné správy a subjektů kritické infrastruktury.

Současně v usnesení vlády České republiky ze dne 16. listopadu 2005 č. 1466, o Národním akčním plánu boje proti terorismu (aktualizované znění pro léta 2005 až 2007), je v oblasti kybernetické bezpečnosti definován úkol vytvořit komplexní dokument, který by zmapoval problematiku kybernetických hrozeb z hlediska bezpečnostních zájmů České republiky.

2007 - Akční plán realizace opatření Národní strategie informační bezpečnosti České republiky[5)]

Tento dokument navazoval na Národní strategii informační bezpečnosti České republiky a definoval konkrétní úkoly, které měly směřovat k zajištění informační bezpečnosti v České republice. Mimo jiné byla stanovena následující opatření:

- Realizace systému včasného varování a reakce. Ustavit národní centrum pro řízení, monitoring a analýzu bezpečnostního prostředí informačních a komunikačních systémů České republiky. Ustanovení „pracoviště“ typu CERT s národní gescí.
- Realizace aktivní mezinárodní spolupráce. Zapojit se do vytváření národních a mezinárodních pozorovacích a varovných sítí, které dokáží odhalit a zabránit elektronickým útokům v době vzniku. Zajištění uvedených činností prostřednictvím ustanovení „pracoviště“ typu CERT s národní gescí.

[5)] Usnesení vlády České republiky ze dne 18. června 2007 č. 677 o Akčním plánu plnění opatření Národní strategie informační bezpečnosti České republiky.

2010 – Zřízení Meziresortní koordinační rady pro oblast kybernetické bezpečnosti[6)]

Dne 15. března 2010 přijala vláda České republiky usnesení č. 205 o řešení problematiky kybernetické bezpečnosti České republiky. V tomto usnesení stanovila gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast Ministerstvo vnitra, kterému mimo jiné uložila zřídit Meziresortní koordinační radu pro oblast kybernetické bezpečnosti. Ta měla být hlavním koordinačním orgánem pro oblast kybernetické bezpečnosti v České republice, přičemž jejím cílem byla především podpora výkonu gesční a koordinační role Ministerstva vnitra v oblasti kybernetické bezpečnosti vyžadující součinnost státních institucí. Rada měla plnit zejména tyto úkoly:

- koordinovat činnost státních institucí v oblasti kybernetické bezpečnosti a přispívat k zajištění plnění úkolů meziresortní povahy,
- koordinovat státní instituce při plnění úkolů v oblasti kybernetické bezpečnosti, které vyplývají z členství České republiky v mezinárodních organizacích a koordinovat zastupování České republiky v mezinárodních organizacích a v dalších zahraničních aktivitách souvisejících s kybernetickou bezpečností,
- vyžadovat od státních institucí zastoupených v koordinační radě nezbytnou součinnost při plnění úkolů v oblasti kybernetické bezpečnosti,
- aktivně vytvářet podmínky pro hladké fungování spolupráce mezi svými členy,
- řešit aktuální otázky kybernetické bezpečnosti a předkládat odborné návrhy a doporučení ministru vnitra a jeho prostřednictvím podle potřeby vládě,
- sledovat plnění závěrů z jednání koordinační rady jejími členy,
- shromažďovat, analyzovat a vyhodnocovat údaje o stavu zajištění kybernetické bezpečnosti poskytované členy koordinační rady,
- připravovat návrh zprávy o stavu zajištění kybernetické bezpečnosti České republiky, která měla být pravidelně předkládána ministrem vnitra vládě jako výchozí dokument, který měl stanovovat priority a z nich vyplývající úkoly v oblasti kybernetické bezpečnosti pro nadcházející období,

[6)] Usnesení vlády České republiky ze dne 24. května 2010 č. 380 o zřízení Meziresortní koordinační rady pro oblast kybernetické bezpečnosti.

- spolupracovat s externími odbornými subjekty a využívat jejich výstupů v zájmu zajišťování kybernetické bezpečnosti České republiky.

Meziresortní koordinační rada pro oblast kybernetické bezpečnosti byla po přechodu gesce nad oblastí kybernetické bezpečnosti na NBÚ zrušena usnesením vlády České republiky ze dne 19. října 2011 č. 781.

2010 – Podpis Memoranda o Computer Security Incident Response Team (CSIRT) České republiky se sdružením CZ.NIC[7)]

V České republice existuje řada etablovaných i neformálních týmů typu CSIRT/CERT, které mají zkušenosti s útoky, tyto informace navzájem sdílí a kvalifikaci prokázaly zařazením do mezinárodních struktur. Tyto týmy v rámci České republiky kooperují na půdě pracovní skupiny CSIRT.CZ, která je koordinovaná sdružením CZ.NIC. Podpisem Memoranda o Computer Security Incident Response Team (CSIRT) České republiky došlo k dohodě Ministerstva vnitra a sdružení CZ.NIC, že sdružení CZ.NIC převezme agendu národního Computer security incident response teamu České republiky (CSIRT.CZ). CSIRT.CZ se má zejména podílet na řešení incidentů týkajících se kybernetické bezpečnosti v sítích provozovaných v České republice, poskytovat při řešení incidentů koordinační pomoc koncovým uživatelům, shromažďovat a vyhodnocovat data o oznámených incidentech, má také působit jako Point of Contact pro oblast informačních technologií a zajišťovat osvětu a vzdělávání v oblasti kybernetické bezpečnosti. Předpokládá se spolupráce s ostatními pracovišti typu CERT jak na národní, tak i na mezinárodní úrovni. Toto pracoviště plní do 30. června 2012 také roli vládního pracoviště typu CERT České republiky.

2011 – Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011 - 2015[8)]

[7)] Uzavřeno dne 9. prosince 2010 mezi ministerstvem vnitra a CZ.NIC, z.s.p.o. Dokument viz https://www.csirt.cz/files/nic/doc/Memorandum_CZ.NIC-MVCR.pdf.

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

Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015 navazuje na Bezpečnostní strategii České republiky a definuje záměry České republiky v oblasti kybernetické bezpečnosti. Za cíl si Strategie stanovila především ochranu před hrozbami, kterými jsou informační a komunikační systémy vystaveny, a snížení potenciálních škod způsobených v případě útoků na tyto informační a komunikační systémy. Tohoto cíle má být dosaženo prostřednictvím následujících opatření:

- Vytvoření legislativního rámce, který by měl zejména vymezit činnosti jednotlivých orgánů při koordinaci postupu veřejné moci v oblasti kybernetické bezpečnosti. Legislativními nástroji má být zejména dosaženo zajištění kybernetické bezpečnosti České republiky při respektování Ústavou zaručených práv a to tak, aby byla zajištěna prevence, detekce reakce a opatření vedoucí k potírání kybernetické kriminality. Předpokládá se také nastavení pravidel pro spolupráci se soukromým sektorem.
- Zajištění posilování kybernetické bezpečnosti kritické infrastruktury a v informačních systémech veřejné správy, zejména prostřednictvím definování bezpečnostních norem, jejich povinné implementace a kontroly jejich dodržování. Bezpečnostní normy by měly být definovány v metodických materiálech.
- Vybudování vládního pracoviště CERT, které bude součástí národního a mezinárodního systému včasného varování o kybernetických hrozbách. Vládní pracoviště CERT by mělo zajišťovat monitoring a detekci bezpečnostních incidentů, reakci na jejich vznik a preventivní opatření omezující jejich dopad.
- Podpora mezinárodní spolupráce v oblasti kybernetické bezpečnosti, zejména ve formě výměny informací a zkušeností v rámci mezinárodních organizací a posilování spolupráce se zahraničními subjekty.
- Spolupráce státu, soukromé a akademické sféry.
- Zvyšování povědomí o kybernetické bezpečnosti.

Současně se Strategií byl přijat také Akční plán, který je rozčleněn do jednotlivých oblastí. Každá oblast obsahuje úkoly k naplňování jednotlivých strategických cílů Strategie do projektů a úkolů orgánů veřejné správy, které jsou věcně v jejich gesci.

2011 – Přechod gesce nad kybernetickou bezpečností na NBÚ a zřízení Rady pro kybernetickou bezpečnost[9)]

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 jako jeho součást vládní koordinační místo pro okamžitou reakci na počítačové incidenty (neboli tzv. vládní 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 Národního bezpečnostního úřadu v oblasti kybernetické bezpečnosti. Členy rady jsou zástupci příslušných státních institucí, kterými jsou Ministerstvo vnitra, Ministerstvo obrany, Ministerstvo zahraničních věcí, Ministerstvo financí, Ministerstvo průmyslu a obchodu, Ministerstvo dopravy, Policie České republiky, Úřad pro zahraniční styky a informace, Bezpečnostní informační služba, Vojenské zpravodajství, Úřad pro ochranu osobních údajů a Český telekomunikační úřad.

Jak je vidět, v oblasti kybernetické bezpečnosti do současnosti vzniklo mnoho koncepčních a strategických dokumentů, avšak většina jejich cílů zatím nebyla splněna. Praktické zkušenosti s kybernetickou bezpečností však v České republice existují – zejména v soukromé a akademické sféře. Největší zkušenosti s řešením kybernetických bezpečnostních událostí mají týmy typu CERT, které již v České republice fungují na soukromé a akademické bázi. Aktuálně v České republice působí čtyři týmy, které jsou oficiálně uznané světovou infrastrukturou CERT/CSIRT týmů:

- CESNET-CERTS
- CSIRT.CZ
- CZ.NIC-CSIRT
- CSIRT-MU

[9)] 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.

Českým průkopníkem v této oblasti je sdružení CESNET z.s.p.o., které založily vysoké školy a Akademie věd České republiky v roce 1996. Jeho hlavní činností je provozování a rozvíjení páteřní akademické počítačové sítě České republiky. Současná verze této sítě se nazývá CESNET2 a je určena pro vědu, výzkum, vývoj a vzdělávání a jsou k ní připojeny subsítě členů organizace a některé střední školy, nemocnice, či knihovny. Na bezpečnost této sítě v rámci sdružení dohlíží tým CESNET-CERTS[10], který vznikl v lednu roku 2004. Tento tým přímo zodpovídá za řešení bezpečnostních incidentů strojů a služeb v rámci sítě CESNET2, stará se bezproblémový chod sítě a koordinuje řešení a prevenci bezpečnostních incidentů v rámci sítě, v neposlední řadě také podporuje členy sdružení a správce připojených sítí při tvorbě jejich bezpečnostní strategie týkající se provozu sítí a služeb. CESNET-CERTS mimo svoji hlavní aktivitu vyvíjí také osvětovou činnost v podobě školení pořádaných pro zástupce svých členů a věnuje se mezinárodní spolupráci se zahraničními týmy typu CERT. V prostředí sítě CESNET2 také působí dílčí bezpečnostní týmy jednotlivých členů, které pro danou subsíť plní roli CERT týmu:

- CSIRT tým počítačové sítě VŠB-TU[11] Ostrava, který byl založen v roce 2008, jehož hlavní aktivitou je řešení bezpečnostních incidentů VŠB-TU Ostrava.
- CSIRT-MU[12], vznikl v roce 2009 na Ústavu výpočetní techniky Masarykovy univerzity a jeho primárním účelem je řešení bezpečnostních incidentů v rámci univerzitní počítačové sítě. CSIRT-MU je veden v oficiálním seznamu evropských pracovišť CSIRT.
- CSIRT-VUT[13] je zodpovědný za řešení bezpečnostních incidentů v rámci počítačové sítě Vysokého učení technického v Brně.
- WIRT[14] (WEBnet incident response team) prošetřuje a řeší stížnosti či hlášení bezpečnostních incidentů v rámci univerzitní sítě Západočeské univerzity v Plzni.

V rámci Ministerstva obrany je prvkem kybernetické bezpečnosti středisko CIRC MO. Jeho úkolem je proaktivní identifikace bezpečnostních hrozeb a incidentů, jejich analýza a následné reportování zjištěných událostí a postupů řešení k relevantním partnerům.

[10] https://csirt.cesnet.cz/.

[11] http://idoc.vsb.cz/cs/okruhy/cit/tuonet/info/csirt/index.html.

[12] http://www.muni.cz/ics/services/csirt.

[13] http://www.vutbr.cz/cvis/sit/csirt.

[14] http://support.zcu.cz/index.php/WIRT_-_WEBnet_Incident_Response_Team.

Středisko CIRC MO napomáhá k ochraně informací a dat, která jsou uložena v informačních systémech a k ochraně technických prostředků pro velení a řízení v rámci plnění úkolů Ministerstva obrany.

Dalším klíčovým pracovištěm typu CERT je bezpečnostní tým sdružení CZ.NIC. CZ.NIC, z.s.p.o. je sdružení založené v roce 1998 předními poskytovateli internetových služeb (v dnešní době má 94 členů). Hlavní činností sdružení je provozování registru doménových jmen „.cz“, zabezpečení provozu domény a osvěta v oblasti doménových jmen. Jeho tým CZ.NIC-CSIRT je zodpovědný za řešení bezpečnostních incidentů na svojí síti a incidentů, které se dotýkají nameserverů domény „.cz“. Specifikem tohoto týmu, jako týmu správce národní domény, je to, že má možnost iniciovat deaktivaci konkrétní domény, z níž pochází bezpečnostní incident národního či mezinárodního významu. Tento incident může představovat například šíření škodlivého obsahu, předstírání obsahu jiné služby (tzv. phishing), nebo je hardware připojený prostřednictvím domény řídícím centrem sítě distribuující škodlivý obsah (např. botnet).

V roce 2008 byl spuštěn pilotní projekt pracoviště CSIRT.CZ[15)], který v té době zajišťoval tým CESNET-CERTS a jehož hlavním úkolem byla koordinace a pomoc při řešení bezpečnostních incidentů, které měly původ nebo cíl v sítích provozovaných v České republice a na jejichž oznámení správci dané sítě nereagovali, problém neřešili, nebo na ně nebyl k dispozici kontakt. CSIRT.CZ tedy působil jako „místo poslední záchrany“ v oblasti bezpečnostních útoků na českých sítích, suploval tedy v zásadě Národní CERT tým. Tento projekt skončil na konci roku 2010 a od 1.1. 2011 funguje CSIRT.CZ jako oficiální Národní CERT tým, který provozuje sdružení CZ.NIC. Role CSIRT.CZ jsou v současné době zejména:

- Udržování zahraničních vztahů – se světovou komunitou CERT/CSIRT týmů a organizacemi, které tuto komunitu podporují.
- Spolupráce se subjekty v rámci České republiky – ISP (poskytovatel internetových služeb), poskytovateli obsahu, bankami, bezpečnostními složkami, akademickým sektorem, státními orgány a dalšími institucemi.
- Poskytování služeb v oblasti bezpečnosti:
    - Řešení a koordinace řešení bezpečnostních incidentů.

15) http://www.csirt.cz/.

- Osvětová a školící činnost.
- Proaktivní služby v oblasti bezpečnosti.

V rámci své činnosti spolupracuje CSIRT.CZ také se zahraničními subjekty; zejména s nadnárodními organizacemi ENISA[16], TERENA[17] a FIRST[18].

2. Návrh variant řešení

K hodnocení jednotlivých variant regulatorního modelu je třeba přistoupit prostřednictvím následující faktické premisy:

K zajištění kybernetické bezpečnosti a odpovídajícímu zajištění práva na informační sebeurčení prostřednictvím přístupu k fungujícím službám informační společnosti je nutno zpracovávat informace o výskytu kybernetických bezpečnostních událostí z co největšího množství zdrojů. Kybernetické útoky velkého rozsahu totiž mají často v podmínkách sledování místních sítí a systémů charakter bagatelních incidentů – až vyhodnocení informací z větší části informační nebo komunikační infrastruktury může v takových případech přinést adekvátní identifikaci kybernetického útoku, jeho rozsahu a nebezpečnosti. Ze stejného důvodu je třeba koordinovat ochranná opatření. Služby informační společnosti se totiž vyznačují svým síťovým charakterem, přičemž i rozsahem nepatrný prvek sítě může závažným způsobem ovlivňovat její ostatní části, to dokonce často i bez ohledu na geografickou blízkost.

2.1 Nulová varianta (bez specifické právní regulace)

Za nulovou variantu je možno považovat pokračování současného stavu, tj. neexistenci specifické zákonné úpravy a absenci centrálního institucionálního zajištění kybernetické bezpečnosti určeným orgánem veřejné moci. V takové situaci je zajištění

[16] European Network and Information Security Agency zdroj: http: //www.enisa.europa.eu/.

[17] Trans European Research and Education Network Association. Tato organizace působí jako fórum pro spolupráce, inovace a sdílení znalostí za účelem rozvoje internetových technologií, infrastruktury a služeb pro výzkumnou a akademickou komunitu – zdroj: http://www.terena.org/.

[18] Forum for Incident Response and Security Teams. FIRST sdružuje různě týmy typu CERT ze státních, soukromých i akademických organizací. Cílem tohoto sdružení je spolupráce a koordinace v oblasti prevence bezpečnostních incidentů – zdroj: http://www.first.org/.

kybernetické bezpečnosti otázkou dobrovolné koordinace dohledových a ochranných činností mezi jednotlivými poskytovateli služeb elektronických komunikací resp. mezi subjekty zajišťujícími sítě elektronických komunikací. Platí přitom, že i relativně bezvýznamný poskytovatel služeb nebo subjekt zajišťující síť 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 značnou míru bezpečnostní rizikovosti následovanou absencí efektivních nástrojů k obraně před rozsáhlým kybernetickým útokem celospolečenského významu. Z ekonomického hlediska nulová varianta zdánlivě šetří přímé investice na zřízení a fungování národních kybernetických bezpečnostních opatření. Rovněž by šetřila investice soukromých subjektů a orgánů veřejné moci do zabezpečení jejich systémů (tj. na zavedení povinných bezpečnostních opatření). Současně by však došlo k výraznému zvýšení nákladovosti u partikulárních investic do zabezpečení konkrétních systémů tam, kde by se k němu příslušný správce odhodlal. Soukromoprávní i veřejnoprávní subjekty se zájmem o zabezpečení svých systémů (resp. subjekty, pro které bezpečnost jejich systémů představuje ekonomickou či politickou nutnost) by tedy byly nuceny do zabezpečení své infrastruktury investovat nepoměrně více prostředků, než kolik by bylo nutno v situaci, kdy by zákon upravil základní bezpečností standard a určil odpovídající jeho institucionální zajištění.

Situace je v tomto případě podobná jako v případě protipožární ochrany. Není-li stanoven základní standard a institucionální zajištění protipožární ochrany, musí subjekt se zájmem o ochranu svého objektu před požárem investovat nejen do vlastních ochranných opatření, ale též do opatření pro případ, že se požár rozšíří z nezajištěných sousedních objektů. Lze to vyjádřit i tak, že by nebyla efektivní, ale ve svých důsledcích ani hospodárná, protože by nutně přinesla fakticky větší tlak na jiné prostředky ochrany.

Snaha o účinnou reakci na vzrůstající počet kybernetických útoků a jim odpovídající přijetí opatření ze strany soukromých subjektů a orgánů veřejné moci vedla k přijetí partikulárních řešení již nyní, přičemž nákladnost těchto investic v rámci těchto partikulárních investic již vedla k určité kooperaci a centralizaci a vzniku CERT/CIRT týmů.

Z hlediska filozofického by pak nulová varianta znamenala rezignaci státu na ochranu 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 (informační a komunikační technologie). Tolerance současného stavu je i z hlediska nutnosti respektovat a plnit mezinárodní závazky neúnosná.

Jedinou situací, kdy by se nulová varianta zákona o kybernetické bezpečnosti mohla efektivně uplatnit, je tedy situace objektivně klesající frekvence a nebezpečnosti kybernetických útoků. Vzhledem k přesně opačnému trendu je tedy nulová varianta zásadně nevhodná. Současný vývoj rovněž potvrzuje, že nulová varianta ustupuje progresivnějším řešením, která jsou uvedena dále.

2.2 Varianta ochrany informačních systémů nakládajících s utajovanými informacemi

Varianta ochrany informačních systémů nakládajících s utajovanými informacemi je postavena na předpokladu, že právní regulace dopadne pouze na systémy a sítě, které nakládající s utajovanými informacemi. Partikulární ochrana jedné relativně malé součásti informační a komunikační infrastruktury České republiky by s sebou nesla relativně omezenou nutnost investic, to navíc za situace, kdy je bezpečnost utajovaných informací v současné době kvalitně řešena specifickou právní úpravou.

Utajované informace však představují v běžném životě informační společnosti jen jednu z mnoha kritických informačních agend. S rozvojem služeb informační společnost a přesunem podstatné části společenského života do prostředí Informačních technologií má pro současnou společnost kritický význam i celá řada dalších, byť na první pohled marginálních, informačních funkcionalit. Těžištěm práva na informační sebeurčení člověka tak v současné době nejsou utajované informace, ale běžné služby, jejichž prostřednictvím je zajišťován chod společnosti, a to včetně podstatné části politické a ekonomické aktivity.

Řešení kybernetické bezpečnosti v rámci věcné působnosti utajovaných informací by tedy bylo až příliš partikulární a v důsledku by nesplnilo svou funkci. Právní řád by v takovém případě sice ošetřoval problematiku zabezpečení informační společnosti na národní úrovni, neposkytoval by však prakticky žádné prostředky k efektivnímu

zajištění těch informační funkcionalit, které jsou pro fungování státu, společnosti i pro každého člověka v dnešní době v rámci informační společnosti zásadně důležité.

2.3 Varianta obecné působnosti vůči orgánům veřejné správy

Variantu řešení kybernetické bezpečnosti pouze v rámci regulace orgánů veřejné správy nelze realizovat z následujících důvodů. Informační systémy veřejné správy a jejich komunikační infrastruktura tvoří pouze část množiny informačních systému a služeb elektronických komunikací, které jsou nezbytné k fungování společnosti. Bez účasti soukromoprávních subjektů se pak jedná o partikulární řešení, které nesplňuje očekávání, neboť umožňuje reagovat pouze na útoky vedené vůči informačním systémům veřejné správy České republiky, ale neumožňuje případně reagovat na útoky na jiné informační systémy vzniklé z bezpečnostního incidentu v rámci informačních systémů veřejné správy. Tato varianta tedy neumožňuje plnit mezinárodní závazky České republiky vůči jejím spojencům z NATO a EU.

2.4 Varianta obecné působnosti a spolupráce se soukromoprávními subjekty

Varianta řešení kybernetické bezpečnosti za účasti soukromoprávních subjektů je postavena na předpokladu obecnosti. Zahrnuje tedy nejrůznější informační systémy, sítě a služby elektronických komunikací, které dohromady tvoří český kyberprostor a jejichž bezpečnost implikuje stav kybernetické bezpečnosti státu.

Současně je tato varianta postavena na předpokladu, že podstatná část kybernetické informační infrastruktury státu, a to včetně součástí kritického významu, má soukromoprávní vlastníky, správce nebo provozovatele. Služby informační společnosti značné společenské a ekonomické důležitosti, ať už je jejich uživatelem stát nebo soukromý sektor, tedy jsou z podstatné části poskytovány soukromoprávními subjekty, nejčastěji pak komerčním způsobem.

Bezpečnost českého kyberprostoru má pro tyto soukromoprávní subjekty značný ekonomický význam, neboť jen fungující síť jim může generovat náležitý ekonomický efekt. Tyto soukromoprávní subjekty tedy aktivně investují do zabezpečení vlastní infrastruktury a mají ekonomicky motivovaný zájem podílet se na zajištění celkové kybernetické bezpečnosti.

Varianta spolupráce se soukromoprávními subjekty je konečně založena na předpokladu, že tyto subjekty jsou technicky i právně nejlépe kompetentní řešit kybernetické bezpečnostní incidenty v rámci vlastní infrastruktury. To jim umožňuje detailní znalost příslušných systémů, jejich přímá technická kontrola a rovněž právní vztahy, jejichž jsou tyto systémy objektem. Informační a komunikační systémy jsou totiž buďto přímo ve vlastnictví příslušného subjektu nebo má nad nimi příslušný subjekt jiný typ právní či faktické kontroly. Stát pak v tomto případě nikdy nemůže ústavně konformním způsobem dosáhnout vzhledem k objektu právní regulace takových oprávnění, jakými tyto subjekty běžně disponují.

Lze přitom předpokládat, že vzniklá zátěž nebo další náklady budou v přiměřené výši ve vztahu k chráněnému zájmu a jejich vynaložení bude ve srovnání s nulovou variantou efektivnější. Dojde tak ke zvýšení bezpečnosti prostředí, v němž podnikají. Povinnostní charakter právní regulace včetně sankcí pak má zajistit dodržení stejné úrovně bezpečnostních standardů jen v rámci kritické informační a komunikační infrastruktury.

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

2.5 Varianta obecné působnosti a přímé regulace

Varianta přímé regulace je založena na předpokladu, že stát prostřednictvím svých orgánů přímo kontroluje a reguluje fungování služeb informační společnosti. Tato varianta vyžaduje založení takových kompetencí, aby mohl určený státní orgán (v tomto případě NBÚ) přímo aplikovat bezpečnostní a ochranná opatření. Takové řešení by vyžadovalo založit kompetence NBÚ přímo ve vztahu k uživatelům služeb informační společnosti, tzn. bezprostředně omezit jejich právo na informační sebeurčení. Současně by bylo nutno zasáhnout do vlastnického práva a dalším právům subjektů poskytujících služby respektive zajišťujících sítě elektronických komunikací, neboť by bylo třeba ošetřit bezprostřední možnost NBÚ přímo technicky zasahovat a ovlivňovat fungování sítí a služeb elektronických komunikací.

Vedle značné regulatorní zátěže soukromoprávních subjektů se varianta přímé regulace vyznačuje i velkou mírou technické a organizační náročnosti. Operátoři NBÚ by totiž museli zvládnout a obsáhnout obtížně evidovatelné a regulovatelné množství

informační a komunikačních systémů, do nichž by bylo nutno instalovat sondy respektive zařízení k přímé kontrole. Oproti ostatním variantám je tedy přímá regulace zdaleka nejnáročnější co do přímých nákladů a požadavků na personální zajištění.

Vzhledem k extrémní ekonomické a organizační náročnosti, jakož i k velmi problémové ústavní konformitě, se varianta přímé regulace jeví být v současné situaci nevhodnou a prakticky neproveditelnou.

2.6 Vyhodnocení nákladů a přínosů

Problematika, která má být upravena, je vzhledem ke své obecné aplikovatelnosti značně rozsáhlá co do počtu skupin subjektů a oblastí regulace, jichž se bude dotýkat. Současně však navrhované řešení vychází především z dosavadních zahraničních poznatků. V návrhu řešení je zohledněna též dlouhodobá strategie vlády v oblasti kybernetické bezpečnosti. Nová regulace přinese výrazné zvýšení úrovně bezpečnosti informační společnosti obecně. Centrální systém monitorování kybernetických útoků, systém varování a systém vhodně koncipovaných protiopatření přinese rovněž vyšší stabilitu sítí, sdílení informací povede k lepší prevenci a v konečném důsledku povede k zefektivnění výkonu veřejné správy i činnosti podnikatelů. Náklady na odstranění následků kybernetického bezpečnostního incidentu jsou vysoce individuální, protože zahrnují nejen sanaci škod způsobených vlastním incidentem, ale je nutné sem zahrnout i ztráty (např. v oblasti finančnictví či bezpečnosti státu).

Z těchto důvodů lze těžko vymezit konkrétní náklady a přínosy pro jednotlivé oblasti či skupiny, a proto se hodnocení variant v této fázi zabývá především komplexním zhodnocením nákladů a přínosů navrhovaných řešení, a to především z pohledu naplnění stanoveného cíle.

Kvantitativní vyhodnocení nákladů či přínosů, zejména jeho finanční ocenění, je v této fázi komplikované. Rovněž je velmi komplikované finančně vyjádřit hodnotu aktiv, která jsou chráněna a stejně tak finančně vyjádřit škody způsobené útokem. Navrhované varianty jsou vyhodnoceny z pohledu nákladů a přínosů pro jednotlivé dotčené skupiny i komplexního přínosu pro zlepšení a zjednodušení právního prostředí v České republice v oblasti kybernetické bezpečnosti.

V tomto stadiu lze přesně vyčíslit jen náklady potřebné na vybudování a provoz Národního centra kybernetické bezpečnosti. Podle usnesení vlády České republiky ze dne 19. října 2011 č. 781 je pro NBÚ stanoveno, že v oblasti personální bude průběžné navýšení, a to o 8 funkčních míst v roce 2012, o 10 funkčních míst v roce 2013, o 10 funkčních míst v roce 2014 a o 5 funkčních míst v roce 2015, a s tím související navýšení rozpočtu Národního bezpečnostního úřadu pro zajištění činnosti Národního centra kybernetické bezpečnosti o 51,5 mil. Kč v roce 2012, o 61 mil. Kč v roce 2013, o 61 mil. Kč v roce 2014 a o 65 mil. Kč v roce 2015.

3. Vymezení skupin a oblastí dotčených regulací

3.1 Osobní a věcná působnost

Zákon má plánovaně dopadat na takzvané definiční autority českého kyberprostoru, tj. na poskytovatele služeb a provozovatele sítí elektronických komunikací, jakož i na správce vybraných informačních systémů (tj. informačních systémů zařazených do kritické informační infrastruktury a informačních systémů veřejné správy). Zákon je založen na funkčním modelu, tj. rozlišuje subjekty na základě principu rovnosti nikoli prostřednictvím jejich povahy, ale prostřednictvím funkce, kterou pro český kyberprostor plní. Jedinou kategorií subjektů, kde zákon specificky dopadá pouze na veřejnoprávní korporace, je kategorie správců informačních systémů veřejné správy. Zákon tedy rozlišuje následující skupiny svých adresátů:

- Poskytovatelé služeb a provozovatelé sítí elektronických komunikací.
- Správci systémů kritické komunikační infrastruktury.
- Správci informačních systémů zařazených do kritické informační infrastruktury.
- Správci informačních systémů veřejné správy.

Zákon naopak ve své osobní působnosti nedopadá přímo na uživatele služeb a sítí elektronických komunikací, což je důležité z hlediska ochrany práva na informační sebeurčení, které je spojeno se základními lidskými právy na majetek a svobodu projevu.

Věcnou působností zákona jsou vztahy vznikající z nutnosti aplikovat bezpečnostní opatření k ochraně českého kyberprostoru. Obecně lze rozdělit věcnou působnost

zákona na problematiku hlášení výskytu a eliminaci kybernetických bezpečnostních událostí v sítích a službách elektronických komunikací, problematiku rozsahu zabezpečení informačních systémů velké důležitosti (tj. informačních systémů zařazených do kritické informační infrastruktury a vybraných informačních systémů veřejné správy) a na problematiku protiopatření prováděných k obraně před kybernetickým útokem.

Zákon se naopak ve své věcné působnosti netýká obsahové stránky služeb informační společnosti a nezasahuje do práva na informační sebeurčení. K určitému omezení služeb může dojít v rámci vyhlášení stavu kybernetického nebezpečí.

3.2 Derogace a novelizace jiných právních předpisů

Vzhledem k tomu, že věcná působnost zákona o kybernetické bezpečnosti je specifická, nepočítá záměr s výrazným zásahem do ostatních součástí právního řádu.

- Novelizován bude § 98 zákona č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů tak, aby mohl neplnění povinností poskytovateli služeb resp. subjekty zajišťujícími sítě elektronických komunikací sankcionovat Český telekomunikační úřad (dále jen „ČTÚ“).
- Novelizován bude zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů tak, aby byly posíleny požadavky na bezpečnost informačních systémů veřejné správy, ale zároveň aby zůstaly zachovány kompetence Ministerstva vnitra vůči správcům a provozovatelům těchto systémů a aby se nekřížily kompetence Ministerstva vnitra a NBÚ vztahující se k těm informačním systémům veřejné správy, které jsou zařazeny do kritické informační infrastruktury.
- Nelze vyloučit, že v průběhu příprav návrhu paragrafového znění zákona se objeví potřeba novelizace i dalších právních předpisů, ale jejich rozsah nebude nijak zásadní.

3.3 Současná legislativa a jiné dokumenty na úseku kybernetické bezpečnosti

Ústavní pořádek České republiky:

- Ústavní zákon č. 1/1993 Sb., Ústava České republiky, ve znění pozdějších předpisů,
- Listina základních práv a svobod,
- Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky.

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. 127/2005 Sb., 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. 419/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim.

Prováděcí předpisy

- Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznamy utajovaných informací, ve znění nařízení vlády č. 240/2008 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. 158/2005 Sb., kterou se stanoví minimální náležitosti návrhu smlouvy o přístupu nebo o propojení veřejných komunikačních sítí,
- Vyhláška č. 162/2005 Sb., o stanovení parametrů kvality univerzální služby a jejich mezních hodnot,
- Vyhláška č. 430/2005 Sb., kterou se stanoví kritéria pro posuzování, zda má více subjektů společnou významnou tržní sílu na relevantním trhu elektronických komunikací,
- Vyhláška č. 327/2006 Sb., kterou se stanoví charakteristiky přiměřených požadavků na připojení v pevném místě k veřejné telefonní síti a na přístup v pevném místě k veřejně dostupné telefonní službě a podmínky přístupu k internetu v rámci univerzální služby,
- 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).

Usnesení vlády

- Usnesení vlády České republiky ze dne 18. června 2007 č. 677 o Akčním plánu plnění opatření Národní strategie informační bezpečnosti České republiky,
- Usnesení vlády České republiky ze dne 20. července 2011 č. 564 o Strategii pro oblast kybernetické bezpečnosti České republiky na období 2011-2015,
- 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.

Primární právo EU:

- Listina základních práv Evropské unie.

Směrnice Evropského parlamentu a Rady:

- 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů, ve znění směrnice 98/48/ES,
- 1999/5/ES o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody,
- 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu),
- 2002/19/ES o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení (přístupová směrnice), ve znění směrnice 2009/140/ES,
- 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice), ve znění směrnice 2009/140/ES,
- 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice), ve znění směrnice 2009/140/ES,
- 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací (směrnice o univerzální službě), ve znění směrnice 2009/136/ES,
- 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací,
- 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí,
- 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu.

Nařízení Evropského parlamentu a Rady:

- 460/2004/ES o zřízení Evropské agentury pro bezpečnost sítí a informací ve znění nařízení č. 1007/2008,
- 1077/2011/ES kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva.

Rozhodnutí a stanoviska Rady:

- 92/242/EHS o bezpečnosti informačních systémů,
- 2002/465/JHA o společných vyšetřovacích týmech,
- 2002/C 43/02 o společném postoji a specifických činnostech v oblasti bezpečnosti sítí a informací,
- 2003/C48/01 o evropském postoji vůči kultuře bezpečnosti sítí a informací,
- 2005/222/SVV o útocích proti informačním systémům,
- 2009/C62/05 o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti,
- 2009/C321/01 o společném evropském přístupu k bezpečnosti sítí a informací,
- 2011/292/EU o bezpečnostních pravidlech na ochranu utajovaných informací EU.

Sdělení Komise:

- KOM/2000/890 o vytvoření bezpečnější informační společnosti zdokonalením bezpečnosti informační infrastruktury a bojem proti počítačovým trestným činům,
- KOM/2001/298 Bezpečnost sítí a informací – návrh evropského postoje,
- KOM/2006/251 Strategie pro bezpečnou informační společnost – „Dialog, partnerství a posílení účasti“,
- KOM/2006/688 boj proti spamu a špionážnímu a škodlivému softwaru,

- KOM/2007/267 k obecné politice v boji proti počítačové kriminalitě,
- KOM/2009/149 o ochraně kritické informační infrastruktury - „Ochrana Evropy před rozsáhlými počítačovými útoky a narušením: zvyšujeme připravenost, bezpečnost a odolnost“,
- KOM/2010/245 Digitální agenda pro Evropu,
- KOM/2010/673 Strategie vnitřní bezpečnosti Evropské unie: pět kroků směrem k bezpečnější Evropě,
- KOM/2011/163 o ochraně kritické informační infrastruktury – „Dosažené výsledky a další kroky: směrem ke globální kybernetické bezpečnosti“.

Dokumenty Rady Evropy:

- Úmluva Rady Evropy č. 185 o kybernetické kriminalitě,
- Úmluva Rady Evropy č. 196 o prevenci terorismu,
- Doporučení Parlamentního shromáždění č. 1706 (2005) o médiích a 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),
- 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-21.09.2011_2E ze dne 21. září 2011 o principech internet governance,
- 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.

Další dokumenty mezinárodních organizací:

- Akční plán Evropské unie pro boj s terorismem (INI/2004/2214); Evropský parlament,
- Bezpečnost informačních systémů a sítí: Směrem ke kultuře bezpečnosti; 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,
- Akční plán zemí G8 pro potírání „high-tech" zločinu.

4. Stav realizace kybernetické bezpečnosti v zahraničí

Do přehledu byly zahrnuty země, z nichž se podařilo ve fázi přípravy záměru získat ucelené informace, a to například za součinnosti diplomatických misí České republiky. Řada členských států Evropské unie i zemí mimo Evropskou unii v současné době připravuje legislativu k ochraně kybernetické bezpečnosti a informace o systému právní regulace a jeho implementaci tedy doposud chybí. Z dále podaného přehledu zřetelně plyne, že vyspělé státy věnují otázce kybernetické bezpečnosti značnou pozornost. To mimo jiné představuje důležitý impulz pro přijetí příslušného zákona, protože zahraniční investoři sledují bezpečnost prostředí státu globálně.

4.1 Belgie

Služby národního CERT v Belgii zajišťuje tým CERT.be[19], který je provozován belgickou Sítí národního výzkumu BELNET[20], které tuto odpovědnost předala Federální veřejná služba pro informační a komunikační technologie[21] ve spolupráci s Belgickým institutem pro poštovní služby a telekomunikace[22]. Jedná se o veřejnou službu, jejímž posláním je poskytování informací a koordinačních služeb za účelem zajištění informační bezpečnosti. CERT.be také poskytuje poradenství a vytváří návody a postupy pro podporu bezpečnosti informačních a komunikačních technologií v Belgii. Tyto služby jsou poskytovány nejen státním orgánům a provozovatelům kritické infrastruktury, ale také soukromým subjektům a široké veřejnosti. V současné době vyvíjí tento tým spíše osvětovou činnost.

4.2 Dánsko

V Dánsku figuruje tým pod názvem DK.CERT, který je vnímán jako národní na základě toho, že jde o jednoho z průkopníků. Založen byl již v roce 1991 podle vzoru amerických CERTů dánským Centrem informačních technologií pro vývoj a výzkum, jež je národní organizací spadající pod dánské Ministerstvo školství. Hlavním cílem tohoto týmu je získávání know-how a informací prostřednictvím spolupráce s FIRST. Na základě svých pozorování a informací pak publikuje informace o bezpečnostních incidentech a další informace související se zajištěním kybernetické bezpečnosti v Dánsku. Dále má za úkol koordinaci postupu dalších CERTů při vzniku bezpečnostního incidentu.

V Dánsku dále působí „Danish GovCERT“, který se označuje za „National“. Je provozován Ministerstvem obrany a je členem skupiny týmů s ověřeným vládním/národním mandátem při CERT/CC.

---

[19] Computer emergency response team Belgium(https://www.cert.be).

[20] www.belnet.be/en/about-us/who-are-we

[21] http://www.fedict.belgium.be/en.

[22] http://www.ibpt.be.

4.3 Litva

Kybernetická bezpečnost je v gesci Ministerstva vnitra, které koordinuje aktivity všech zainteresovaných orgánů státní správy[23)].

V poslední době v Litvě vznikl dokument Program rozvoje bezpečnosti elektronické informace (kybernetické bezpečnosti) na období 2011 - 2019[24)]. Ten se zaměřuje především na nebezpečné internetové fenomény, které ohrožují nejen soukromé uživatele, ale i státní správu. Cílem je zajistit důvěrnost služeb poskytovaných v kybernetickém prostoru, ochranu osobních údajů a zvýšení povědomí a znalosti o kybernetické bezpečnosti. Prioritními oblastmi v tomto ohledu jsou pak zejména:

- Zdokonalování koordinace a zvládání rizik kybernetické bezpečnosti.
- Zdokonalování legislativního rámce k posílení kybernetické bezpečnosti.
- Posilování kybernetické bezpečnosti veřejné správy a komunikační infrastruktury.
- Povzbuzení k uskutečňování projektu kybernetické bezpečnosti.
- Podpora mezinárodní spolupráce v oblasti kybernetické bezpečnosti.

K plnění tohoto plánu je legitimováno Ministerstvo vnitra a za jeho účelem jsou rozděleny úkoly mezi zainteresované orgány.

V Litvě je v současnosti ustaven tým CERT-LT, Lithuanian National Computer Emergency Response Team. Ten je provozován The Communications Regulatory Authority of the Republic of Lithuania.

4.4 Německo

Problematikou kybernetické bezpečnosti se v Německu zabývá Strategie pro kybernetickou bezpečnost[25)], která je postavena na činnosti dvou základních orgánů.

[23)] Jedná se zejména o Ministerstvo obrany, Ministerstvo dopravy a spojů, Státní inspekci ochrany osobních údajů a Úřad pro regulaci spojů (telekomunikační úřad).

[24)] Schváleno usnesením č. 796 ze dne 29. června 2011.

[25)] www.bmi.bund.de/SharedDocs/Downloads/DE/Themen/OED_Verwaltung/Informationsgesellschaft/cyber_eng.pdf?__blob=publicationFile.

Prvním z nich je Centrum pro kybernetickou obranu[26], které podléhá Spolkovému úřadu pro informační bezpečnost[27]. Tým bude tvořen celkem deseti členy, z nichž šest bude ze Spolkového úřadu pro informační bezpečnost, dva další experty dosadí Spolkový úřad pro ochranu ústavy a Spolkový úřad pro ochranu obyvatelstva a pomoc při živelních katastrofách. Zbytek týmu doplní hostující experti dosazení zejména Spolkovou kriminální policií, Spolkovou policií, Celním úřadem, Federální zpravodajskou službou, či Armádou. Toto centrum pak nebude mít ofenzivní nástroje pro ochranu kybernetického prostoru. Z dokumentu však není patrné, jaké budou úkoly a kompetence Centra, ani jaké nástroje bude k jejich plnění mít.

Druhým zmíněným orgánem je Rada kybernetické bezpečnosti[28], která by měla začít pracovat 1. dubna 2012. Rada bude součástí Kancléřství a jejími členy budou nejvyšší představitelé všech relevantních ministerstev – například ministerstva vnitra, obrany, spravedlnosti, financí a dalších podle potřeby, v jeho čele pak bude stát státní tajemník pro oblast IT. Rada se bude scházet za účelem řešení závažných kybernetických incidentů, které by mohly ohrožovat kritickou infrastrukturu Německa.

Německo je zemí s jedním z největších počtů oficiálně konstituovaných CERT/CSIRT týmů, které působí v různých sektorech – vládní, soukromý, průmyslový a akademický.

Roli vládního týmu plní tým CERT-BUND.

4.5 Nizozemsko

V Nizozemsku funguje tým NCSC-NL[29], jehož fungování v Nizozemsku zajišťuje Ministerstvo bezpečnosti a spravedlnosti, který provozuje službu pro zajištění kybernetické bezpečnosti Nizozemska a vystupuje jako Incident response team pro vládu Nizozemska. Pracuje zejména pro organizace zajišťující veřejné služby, typicky vládní organizace, a spolupracuje se subjekty, které jsou aktivní v rámci kritické infrastruktury Nizozemska. NCSC-NL také spolupracuje s mezinárodní sítí pracovišť

[26] Nationales Cyber-Abwehrzentrum (NCAZ).

[27] Bundesamt für Sicherheit in der Informationstechnik (BSI). Tento úřad vznikl v roce 1991, kdy se oddělil od jednotky pro kybernetické události německé Zpravodajské agentury (Bundesnachrichtendienst) https://www.bsi.bund.de/.

[28] Nationaler Cyber-Sicherheitsrat.

[29] www.govcert.nl/english/organisation.

typu CERT a získané znalosti a zkušenosti využívá při monitorování a řešení bezpečnostních incidentů. Tento tým zejména podporuje nizozemské vládní orgány při předcházení a řešení bezpečnostních incidentů v oblasti informačních a komunikačních technologií. Poskytují v tomto ohledu zejména službu oznamování rizik v oblasti kybernetické bezpečnosti, publikují informace o aktuálních hrozbách a známých incidentech a koordinují reakci na vzniknuvší incidenty. Kromě toho také komunikuje svoje poznatky a jiné důležité informace s koncovými uživateli a poskytuje odborné rady v oblasti prevence a řešení bezpečnostních incidentů.

4.6 Norsko

Vojenský i národní CERT jsou v podřízenosti Národního bezpečnostního úřadu. Národní CERT v Norsku vystupuje pod zkratkou NorCERT[30], a koordinuje preventivní činnosti v rámci zabezpečení informační a komunikační infrastruktury Norska. Má za úkol také koordinaci protiopatření pro případ bezpečnostních incidentů a ochranu kritické infrastruktury Norska. NorCERT vznikl v roce 2006 a je operačním oddělením Národního bezpečnostního úřadu Norska[31], které se skládá z dvou integrovaných sekcí – Norský systém pro upozornění a brzké varování systémů digitální infrastruktury, která zabezpečuje vydávání varovných zpráv o IT útocích v Norsku a Sekce pro Incident Handling, jež je národním centrem, které koordinuje reakce na útoky na kritické Norské informační a komunikační systémy.

Odpovědností NorCERTu je mimo jiné:

- Koordinace protiopatření pro případ IT bezpečnostních incidentů v kritické infrastruktuře.
- Sběr informací o závažných bezpečnostních incidentech.
- Koordinace vyplňování bezpečnostních děr v kritických počítačových systémech.
- Sdílení informací s ostatními CERTy o nových rizicích.
- Asistence pro ostatní CERTy a zajištění připravenosti na bezpečnostní incidenty.

[30] Norwegian Computer Emergency Response Team. https://www.nsm.stat.no/Arbeidsomrader/Internettsikkerhet-NorCERT/Internettsikkerhet---NorCERT/NorCERT/English/.

[31] Nasjonal sikkerhetsmyndighet (NSM).

- Point of contact pro zahraniční týmy typu CERT.

4.7 Rakousko

V Rakousku figuruje národní CERT tým pod názvem CERT.at[32)], který vznikl z iniciativy rakouského doménového registrátora nic.at. Vystupuje jako point of contact pro kybernetickou bezpečnost v národním kontextu, také koordinuje ostatní CERT týmy působící jak v rámci kritické infrastruktury Rakouska, tak i v rámci ostatních rakouských sítí. Mimo jiné má CERT.at za úkol informovat veřejnost o bezpečnostních rizicích a incidentech, a napovídat jak postupovat při jejich řešení a to formou varování, hlášení incidentů a koordinovaných postupů. V případě závažných incidentů proti rakouské kritické infrastruktuře koordinuje CERT.at reakci v podobě směrovaných opatření za pomoci lokálních bezpečnostních týmů.

[32)] http://www.cert.at/about/missionstatement/content_en.html.

4.8 Slovensko

Národní CERT tým vystupuje pod názvem CSIRT.SK[33)], který vznikl v roce 2009 v souladu s Národní strategií pro informační bezpečnost ve Slovenské republice z roku 2008. CSIRT.SK je zřízený jako specializovaný útvar DataCentra, které je rozpočtovou organizací Ministerstva financí SR. Tento tým má zejména iniciovat a koordinovat reakce státní správy, veřejného a soukromého sektoru na bezpečnostní incidenty, které ohrožují nejen Národní informační a komunikační infrastrukturu SR (NIKI). Hlavními cíli CSIRT.SK tedy jsou:

- Řešení informačně-bezpečnostním incidentů v SR ve spolupráci s vlastníky a provozovateli postižených částí NIKI, telekomunikačními operátory, poskytovateli internetových služeb a se státními orgány.
- Budování a rozšiřování znalostí veřejnosti ve vybraných oblastech informační a kybernetické bezpečnosti.
- Kooperace se zahraničními sesterskými organizacemi a reprezentace SR v oblasti informační bezpečnosti na mezinárodní úrovni.

Za účelem dosažení těchto cílů poskytuje CSIRT.SK služby jak aktivní, které zahrnují zejména analýzu, varování, reakci a koordinaci činností pro případ vzniku bezpečnostního incidentu, tak proaktivní, jako například vzdělávání, distribuce informací o incidentech a konzultační podporu v oblasti kybernetické bezpečnosti.

4.9 Spojené království

Britské ministerstvo vnitra nedávno zveřejnilo novou národní Strategii kybernetické bezpečnosti do roku 2015, ve které vymezuje základní cíle pro ochranu kybernetického prostoru a postupy, kterými jich chce dosáhnout. Cíle, které mají být do roku 2015 naplněny, jsou zejména:

- Vybudování schopnosti bránit se kybernetickým útokům.
- Dosažení mezinárodního konsensu o normách chování v kyberprostoru.
- Omezení zranitelnosti vládních systémů a kritické infrastruktury.

[33)] Computer incident response team Slovakia vznikl usnesením vlády Slovenské republiky č. 479/2009 ze dne 1. června 2009, viz http://www.csirt.gov.sk/.

- Podpora výuky profesionálů v oblasti kybernetické bezpečnosti.
- Posilování vymahatelnosti práva v oblasti kybernetické bezpečnosti.
- Zlepšení prevence a vybudování obecného povědomí.
- Zvýšení povědomí v privátním sektoru.

K dosažení těchto cílů vláda hodlá spolupracovat jak se soukromými subjekty, tak se subjekty mezinárodními. Byl také přijat Národní program kybernetické bezpečnosti s rozpočtem 650.000.000 GBP na čtyři roky. Tyto prostředky budou rozděleny především mezi zpravodajské služby, ministerstvo vnitra a ministerstvo obrany.

Primárně se politika kybernetické bezpečnosti UK zaměřuje na ochranu proti kyberterorismu, za tím účelem vzniká na Ministerstvu obrany nová Operační skupina pro kybernetickou obranu[34)], která bude ve spolupráci s Vládním velitelstvím pro komunikace[35)] vyvíjet nové taktiky a postupy v oblasti vojenské kybernetiky. Dále vzniklo Středisko globálních operací a bezpečnostní kontroly[36)], které se zaměřuje na vývoj kybernetické ochrany infrastruktury britských ozbrojených sil.

Důležitá je pochopitelné také ochrana kritické infrastruktury. Již nyní funguje Centrum pro ochranu národní infrastruktury, v jehož rámci vláda spolupracuje s firmami operujícími v oblasti kritické infrastruktury. Vláda chce touto cestou motivovat provozovatele prvků kritické infrastruktury k zavádění přísných standardů kybernetické bezpečnosti.

V neposlední řadě je cílem ochrany také bezpečný internet. Za účelem jeho dosažení má být zahájen zkušební provoz Centra sdílení informací[37)], které má zajišťovat výměnu a vyhodnocování informací o kybernetických útocích. Do budoucna doufá vláda v rámci tohoto centra v širokou spolupráci s velkými i menšími soukromými subjekty. K výměně informací by mělo docházet také se zpravodajskými službami.

K dalšímu zajištění kybernetické bezpečnosti hodlá vláda také v rámci policie zřizovat speciální oddělení boje proti kybernetickému zločinu. Budou také

34) Defence Cyber Operations Group.

35) Government Communication Headquarters (GCHQ).

36) Global Operation and Security Control Centre.

37) Public/private sector cyber security hub.

vypracovávány instrukce a pokyny pro orgány veřejné správy, policie a soudnictví, jak postupovat při potírání kybernetické kriminality.

Ve Spojeném království byl v roce 2008 ustaven GovCertUK, který je vládním týmem a jeho hlavním úkolem je pomáhat veřejnému sektoru při řešení bezpečnostních incidentů.

4.10 Španělsko

Kybernetická bezpečnost je ve Španělsku navýsost aktuální otázkou. Jejím zajištěním jsou pověřeny tři základní instituce. Tou hlavní je Národní kryptologické centrum (CCN)[38)], které patří pod Ministerstvo obrany a je součástí Národního zpravodajského centra[39)]. Tato agentura je zodpovědná za koordinační činnost jednotlivých státních orgánů, které používají šifrovací prostředky a postupy. Jejím hlavním cílem je zajistit bezpečnost informačních technologií, které jsou v tomto prostředí využívány. CCN je také členem Vysoké rady pro elektronickou správu[40)] a Národního centra pro ochranu kritické infrastruktury[41)]. Národní kryptologické centrum plní v rámci kybernetické bezpečnosti následující funkce:

- Rozvíjet a šířit standardy, pokyny a doporučení k zajištění bezpečnosti systémů informačních a komunikačních technologií veřejné správy.
- Vytváření personálu odborné správy v oblasti bezpečnostních systémů informačních a komunikačních technologií.

[38)] Centro Criptologico Nacional (CCN), vznik a fungování na základě zákona č. 421/2004 Sb., El Real Decreto.

[39)] Centro Nacional de Inteligencia (CNI).

[40)] Consejo Superior de Administración Electrónica. Kolegiální orgán v rámci Ministerstva veřejné správy. Zodpovědnost za přípravu, vývoj a rozvoj a realizaci vládní politiky a strategie v oblasti informačních technologií.

[41)] Centro Nacional de Proteccion de Infraestructuras Críticas. Toto centrum je odpovědné Ministerstvu vnitra a aktualizuje a dohlíží na Bezpečnostní plán (Plan de Seguridad) a Národní seznam krizového řízení (Catálogo Nacionbal de Infraestructuras Críticas).

- Vytváření certifikačního orgánu na národní úrovni pro hodnocení a certifikaci bezpečnosti informačních a komunikačních technologií, produktů a systémů v této oblasti.
- Posuzování a akreditování způsobilosti šifrovacích zařízení a informačních technologií, které zahrnují šifrovací prostředky k zpracování, ukládání, nebo přenosu informací bezpečným způsobem.
- Koordinace podpory, vývoje, nákupu, pořízení a používání bezpečnostní technologie výše zmíněných systémů.
- Dohled nad dodržováním normativy o ochraně utajovaných informací v rámci své působnosti.
- Vytváření nezbytných vztahů a podepisování smluv se zahraničními organizacemi podobného charakteru k rozvoji výše uvedených funkcí.

Druhou institucí zajišťující kybernetickou bezpečnost ve Španělsku jsou Computer Emergency Response Team (CERT) týmy. Ty jsou hlavním nástrojem boje s kybernetickými hrozbami a existují jak privátní, tak i národní. Nejvýše je v této hierarchii CCN-CERT. Ten vypracovává příručky a instrukce, nabízí podporu a spolupráci při vytváření personálního obsazení úřadů veřejné správy, uděluje bezpečnostní certifikáty produktům a akreditace bezpečnostním systémům, podporuje rozvoj národní bezpečnostní technologie a poskytuje informace a oznámení o zranitelnostech a nových hrozbách informačních systémů.

Třetím orgánem je Národní centrum pro ochranu kritické infrastruktury[42)], které je řízené Guardia Civil. Toto centrum se stará o bezpečnost kritické infrastruktury a to i v oblasti kybernetické bezpečnosti.

Dále ve Španělsku působí několik national (central government) týmů:

- IRIS-CERT - academic (Education Ministry)
- CCN-CERT - central administration (National Intelligence Center)
- INTECO-CERT - SMEs and citizens (Industry Ministry)

[42)] Centro Nacional de Protección de Infraestructuras Críticas.

- CESICAT - Catalonia goverment (regional) CERT
- CSIRT-GV - Valencia goverment (regional) CERT
- ANDALUCIA-CERT - Andalucia/goverment (regional) CERT

Je to dáno politickým uspořádáním Španělska, pole působnosti těchto týmů se částečně překrývají, ale tvoří funkční infrastrukturu. Jako "national" jsou komunitou nejsilněji vnímány týmy INTECO-CERT a CCN-CERT. Členy skupiny týmů s národním/vládním mandátem při CERT/CC jsou CCN-CERT, INTECO-CERT a IRIS-CERT.

4.11 Spojené státy americké (USA)

Oblasti kybernetické bezpečnosti je věnována ve Spojených státech amerických velká pozornost. V širší podobě je toto téma definováno ve strategických dokumentech, tj. prezidentově *Cyberspace Policy Review (2009)*, *Národně bezpečnostní strategii* (NSS z roku 2010) a O*branné doktríně* (QDR z roku 2010). Do oblasti kybernetické bezpečnosti je zapojeno několik agentur a ministerstev.

V dokumentu *Cyberspace Policy Review* z roku 2009 si administrativa prezidenta B. Obamy stanovila 10 krátkodobých cílů, jež také úspěšně do poloviny roku 2011 realizovala. V dubnu 2011 administrativa učinila další krok k zajištění kybernetické bezpečnosti zveřejněním tzv. *National Strategy for Trusted Identities in Cyberspace (NSTIC).* Strategií, jíž administrativa plní jeden ze základních cílů svého *Cyberspace Policy Review*, usiluje o zřízení „online prostředí" (tzv. „ekosystému identity"), ve kterém mohou jednotlivci a organizace provádět online transakce, aniž by se museli obávat o identitu. Klíčovým prvkem této strategie je její charakter zaměřený na uživatele, který by tímto získal větší kontrolu nad svými daty a schopnost sám prokazovat svou totožnost.

V květnu 2011 administrativa zveřejnila klíčovou *International Strategy for Cyberspace.* Třicetistránková strategie, do jejíhož vzniku byla zapojena řada ministerstev, především State Department a ministerstvo spravedlnosti, předkládá jednotnou vizi vlády pro kybernetický prostor. Jejím cílem je integrovat otázku „cyber" do širší politiky USA v oblasti diplomacie, ekonomické diplomacie, bezpečnosti, mezinárodní asistence. Strategie identifikuje 7 priorit, jimž se diplomacie USA hodlá věnovat – např. ekonomická spolupráce za účelem podpory inovace a obchodu,

kybernetická bezpečnost k ochraně sítí a posílení mezinárodní bezpečnosti, dohled nad dodržováním zákonů s cílem zlepšit schopnost odpovědi na kybernetický zločin a to např. posílením mezinárodních zákonů a posílením regulace v případě, že to bude vhodné, vojenská spolupráce se spojenci a podpora jejich schopnosti předcházet kybernetickým hrozbám.

Ministerstvo obrany povýšilo kybernetický prostor na svou pátou válečnou doménu vedle souše, vzduchu, moře a vesmíru. Dále zřídil separátní jednotné kybernetické velitelství, US Cyber Command, podřízené hlavnímu US velitelství (US Strategic Command). Jeho hlavním cílem je ochrana US vojenské sítě (tzv. „dot mil“). Pod US Cyber Command již svá velitelství sjednotily i jednotlivé US vojenské složky - námořnictvo, armáda a letectvo. Cyber Command má být k dispozici civilnímu vedení k podpoře jeho kritických operací a k podpoře civilní infrastruktury. Cyber Command sdílí řadu pravomocí s Department of Homeland Security (DHS - ministerstvo pro národní bezpečnost), které má výhradní dohled nad zajištěním kybernetické bezpečnosti civilních sítí USA a je hlavním koordinátorem přístupu ke kybernetické bezpečnosti.

V červenci 2011 zveřejnilo Ministerstvo obrany strategii administrativy k zajištění kybernetické bezpečnosti - *Defense Strategy for Cyberspace*. Zveřejněna byla pouze neklasifikovaná verze, která definuje nástroje k zajištění efektivnější kybernetické bezpečnosti. Při její přípravě se Pentagon zaměřil na několik aspektů kybernetické hrozby: externí aktéry, interní aktéry, citlivost dodavatelských kanálů a hrozbu představovanou pro operační schopnosti ministerstva obrany. Pentagon vidí ohrožení v následujících aktivitách nepřítele: krádež dat či zneužití dat, pokus o zamezení přístupu na US vojenskou síť a pokusy o zničení sítě a souvisejících systémů. Základním elementem strategie je zabránit či minimalizovat útok a co nejrychleji detektovat zdroj útoku. Strategie, jak toho dosáhnout, stojí na pěti pilířích:

1. „Cyber“ jako nová operační doména: Strategie podtrhává *cyberspace* jako pátou operační doménu vedle moře, souše, vzduchu a vesmíru;
2. Aktivní obrana: USA poprvé rozmístí aktivní obranu v podobě senzorů, softwaru a digitálních podpisů k zastavení škodlivých kódů;
3. Ochrana kritické infrastruktury: Pentagon definuje svou roli po boku Department of Homeland Security, dalších agentur a soukromého sektoru v zajištění ochrany

kritické infrastruktury a nevojenské sítě. Za tuto kritickou infrastrukturu považuje finanční sektor, transportní systém a přenosové sítě (*power grid*);

4. Vytvoření mezinárodní obrany: USA chtějí vytvořit kolektivní kybernetickou ochranu s mezinárodními partnery, spojenci, včetně NATO;
5. Technologie a výcvik: Pod tímto pilířem chtějí USA zásadním způsobem posílit finanční a materiální podporu výcviku a novým technologiím. Za tímto účelem Pentagon nově vyčlenil půl miliardy USD.

Další agenturou, která se zabývá kybernetickou bezpečností, je National Security Agency (NSA), která je součástí ministerstva obrany a je klíčovou složkou mezi zpravodajskou komunitou a zastává specifickou úlohu v oblasti kybernetické bezpečnosti danou především její zpravodajskou expertízou. Její úloha spočívá ve sběru informací a podpoře zpravodajských operací.

Hlavním roli uvnitř vlády v zabezpečení civilní neklasifikované sítě je Department of Homeland Security (známé také jako „dot gov"). Tzv. *Quadrennial Homeland Security Review*, vlastní koncepční dokument DHS, definovalo kybernetickou bezpečnost jako jednu z pěti klíčových misí DHS. Jeho role spočívá v poskytování technické expertízy soukromému sektoru a dalším aktérům, osvětě o kybernetické bezpečnosti u veřejnosti a koordinaci národní reakce na hlavní incidenty. Spravuje také hlavní národní „organizaci" zodpovědnou za reakci v kybernetických otázkách, tzv. US-CERT (US Computer Emergency Readiness Team).

Co se týče legislativního zakotvení, tak Kongres má dlouhodobě aktivní zájem ovlivňovat národní strategii v oblasti kybernetické bezpečnosti. Prozatím ale neexistuje žádná komplexní legislativa, jež by dostatečně efektivně definovala pravomoci vlády, její politiku či podobu kongresového dohledu nad kroky administrativy. Aktuální je snaha o přípravu jednotné komplexní legislativy ke kybernetické bezpečnosti.

Kybernetické bezpečnost obecně není otázkou, která by zásadním způsobem rozdělovala politické spektrum. Důkazem zájmu Kongresu o kybernetickou bezpečnost jsou enormní a stále rostoucí částky, jež jsou Kongresem alokovány na kybernetickou bezpečnost navzdory narůstajícímu deficitu a potřebě úsporných opatření. Americký think-tank *Center for New American Security* např. srovnává, že od roku 2002 US vláda do informačních technologií investovala jednou tolik, co na válku v Afghánistánu, téměř 650 mld USD. Na fiskální rok 2012 administrativa Kongres požádala o vyčlenění 936 mil

USD pro program DHS (třicetiprocentní nárůst od požadavku rozpočtu na rok 2010) a 3,2 mld USD pro iniciativy Pentagonu na zajištění kybernetické bezpečnosti (dvou procentní nárůst od rozpočtu na rok 2010).

4.12 Maďarsko

CERT- Hungary je vládní Reakční tým pro počítačové incidenty (*Computer Security Incident Response Team, CSIRT*), je vládním CERT týmem Maďarska. Funguje v rámci nadace Theodora Puskáse. CERT Maďarsko zahájil svoji činnost v lednu 2005. Od ledna 2010 CERT Maďarsko funguje, na základě vládního rozhodnutí, jako Centrum kybernetické bezpečnosti Maďarska. CERT Maďarsko koordinuje preventivní aktivity a odpovědi na porušení IT bezpečnosti zaměřené na kritickou infrastrukturu Maďarska. Nad činností CERT Maďarska dohlíží Úřad předsedy vlády.

Za účelem zajištění efektivní odpovědi proti kybernetickým hrozbám CERT Maďarsko aktivně spolupracuje s národními partnery, podílí se na snahách mezinárodních CSIRT a CIIP organizacích.

Právním rámcem v Maďarsku je vládní nařízení č. 223 z roku 2009 o bezpečnosti elektronické veřejné správy. Podle článku 8 nařízení č. 233 za účelem ochrany maďarské kritické informační struktury a bezpečnosti komunikace v rámci ústředního vládního systému a dále zmírnění virových a jiných útoků, maďarská vláda zřizuje Centrum kybernetické bezpečnosti. Centrum je akreditovaným členem mezinárodních organizací zaměřených na kybernetickou bezpečnost a ochranu kritické informační struktury, které ochraňuje služby ústředního vládního systému před útoky přicházejícími z internetu. V tomto rámci Centrum vykovává aktivity týkající se technické ochrany, prevence a zvyšování povědomí. Centrum navíc reprezentuje Maďarsko v mezinárodní spolupráci a organizacích specializujících se na kybernetickou bezpečnost a ochranu kritické informační infrastruktury. Centrum se také podílí na přípravě strategií a právních předpisů týkajících se informační bezpečnosti a bezpečnosti sítě a ochrany kritické informační infrastruktury.

Podle článku 9 nařízení č. 233 Centrum funguje na nepřetržitém základě jako Národní kontaktní místo pro maďarské a mezinárodní organizace zodpovědné za kybernetickou bezpečnost a ochranu kritické informační infrastruktury a dále jako

vládní síla rychlé reakce počítačové technologie (vládní CERT). Centrum zvládá incidenty, které využívají internet jako způsob útoku a koordinuje protiopatření pro maďarské a mezinárodní organizace zodpovědné za kybernetickou bezpečnost a kritické informační infrastruktury. Dále Centrum spravuje známé a publikované softwarové zranitelnosti pro maďarské a mezinárodní organizace zodpovědné za kybernetickou bezpečnost a kritické informační infrastruktury, publikuje softwarové zranitelnosti na svých internetových stránkách (www.cert-hungary.hu) v maďarštině a zpřístupňuje softwarové zranitelnosti dostupné v angličtině pro své mezinárodní partnery. Na základě informací získaných od operátorů ústředního vládního systému se souhlasem majitele ústředního vládního systému, Centrum kontinuálně monitoruje a analyzuje internetový provoz, hledá data, která by mohla nasvědčovat o závadných aktivitách a popřípadě informuje operátory ústředního vládního systému a maďarské a mezinárodní organizace zodpovědné za kybernetickou bezpečnost a kritické informační infrastruktury o závadných aktivitách prostřednictvím kontinuální služby.

Podle článku 10 nařízení č. 233 Centrum poskytuje služby popsané v článku 9 odst. 1 pro uživatele a operátory ústředního vládního systému na základě dohody o veřejné službě bezplatně. A aniž by bylo dotčeno plnění jeho úkolů obsažených v článku 9, Centrum je oprávněno poskytovat další služby s přidanou hodnotou za peníze způsobem popsaným ve zvláštní dohodě pro uživatele a operátory ústředního vládního systému a majitelům kritické informační infrastruktury. Tyto aktivity musí být odděleny od aktivit veřejné služby.

4.13 Estonsko

Estonsko nemá speciální právní úpravu problematiky kybernetické bezpečnosti, ale vychází ze Strategie v oblasti kybernetické bezpečnosti. Původně bylo gestorem v oblasti kybernetické bezpečnosti ministerstvo obrany, nyní má tuto problematiku na starosti ministerstvo hospodářství a dopravy, do jehož působnosti spadají komunikace.

V Estonsku mj. jako reakcí na kybernetický útok v roce 2007, bylo zřízeno NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Toto Centrum bylo založeno v květnu 2008 a v říjnu téhož roku bylo akreditováno jako NATO Centre of Excellence a má statut mezinárodní vojenské organizace, není však operační jednotkou ani součástí velitelské struktury NATO. Úkolem centra je vývoj aliančních kapacit na zajištění

kybernetické bezpečnosti, spolupráce a výměna informací v této oblasti v rámci NATO, to prostřednictvím výzkumu a vývoje, vzdělávání a expertních konzultací. Centrum v Tallinu je jedním z 16 center svého druhu na světě a jeho činnost zajišťuje a financuje zatím 10 členských zemí NATO – Litva, Lotyšsko, Německo, Itálie, Slovensko, Španělsko, Maďarsko, Polsko, Estonsko a USA. V současnosti má Centrum 35 zaměstnanců a do roku 2016 se počítá s navýšením počtu zaměstnanců na 60 – 65 osob. Činnost Centra je zaměřena na tři hlavní oblasti – legislativu a politické otázky, tvorbu koncepcí a strategií a na technické otázky a jejich řešení. Informace o činnosti a výstupech centra jsou přístupné na veřejném webovém portálu – www.ccdcoe.org.

V zemi působí tým CERT Estonia (CERT-EE). CERT-EE je Estonský Národní CERT, který spadá do gesce Ministerstva hospodářství a komunikací.

4.14 Polsko

Vládní tým pro řešení kybernetických incidentů v Polsku je CERT.GOV.PL. Poskytuje technickou podporu pro zajištění a rozvíjení ochrany státní správy a samosprávy Polské republiky před kybernetickými hrozbami. Působí v rámci oddělení teleinformatické bezpečnosti kontrarozvědné služby ABW.

Kybernetickou bezpečnost v Polské republice formálně upravuje vládní program ochrany kyberprostoru Polské republiky v letech 2009 až 2011. Na něj navazuje program na léta 2011 až 2016, který měl být v krátké době vládou schválen. Mezi hlavní cíle jednotky CERT.GOV.PL patří zvýšení bezpečnosti a zároveň snížení počtu bezpečnostních incidentů. Tento tým koordinuje činnosti při kybernetickém útoku, shromažďuje poznatky o rizikových aktivitách a relevantních bezpečnostních hrozbách, provádí jejich hodnocení a odpovídá za technickou i metodologickou podporu a odborné vzdělávání. Dále se zaměřuje na vzdělávání v oblasti dodržování bezpečnostních mechanismů a reakcí při identifikaci napadení, vydává varování a výstrahy před možnými hrozbami, nemá však přístup k obsahu informací, které v systému chrání. V systému se zobrazí pouze parametry příslušných souborů (metadata). Tento prvek vnitřní ochrany má zajišťovat bezpečnost chráněných informací v síti, před případným zneužitím.

Polsko již přijalo první z řady legislativních úprav, které jsou nezbytné k přípravě navazující legislativy ke kybernetické bezpečnosti. Cílem zákona je především úprava pojmu „kyberprostor“do právního rámce polské legislativy. Tento pojem je definován jako „prostředí informačních systémů, v nichž probíhá vytváření a výměna informací“. Přes tuto dílčí úpravu se polský systém ochrany kyberprostoru potýká s nedostatečnou legislativou, o níž by se polská strategie ochrany kyberprostoru mohla opřít.

5. Realizace, vynucování a přezkum účinnosti regulace

5.1 Realizace

Vzhledem k identickému objektu právní regulace a tím dané specifické věcné působnosti jeví se jako nejvhodnější variantou úprava ochranných opatření k zajištění kybernetické bezpečnosti České republiky formou zvláštního zákona a s ohledem na specifika navrhované regulace se tedy nejeví jako vhodné řešit situaci novelou zákona o ochraně utajovaných informací. Ten sice může převzít některé pojmy z jiných právních předpisů, musí však též, v návaznosti na pojmy a definice v právním řádu již zavedené, definovat vlastní pojmový aparát a rovněž tak upravit specifické povinnosti nově definovaným kategoriím subjektů (konkrétně subjektům spravujícím informační a komunikační systémy zařazené do kritické informační resp. kritické komunikační infrastruktury). S ohledem na účel a působení regulace nelze kybernetickou bezpečnost podřadit pod jiný právní předpis (například krizový zákon).

Vzhledem k charakteru NBÚ je rovněž nutno definovat formou zvláštního zákona specifické kompetence NBÚ jako ústředního orgánu státní správy na úseku kybernetické bezpečnosti včetně rozhodovacích, kontrolních a sankčních pravomocí a vymezit vztah NBÚ k dalším orgánům veřejné moci. Rovněž je nutno založit NBÚ možnost spolupráce se soukromoprávními a zahraničními subjekty, jakož i působit v oblasti kybernetické bezpečnosti metodicky a osvětově.

Aby bylo možno postihnout i výjimečné situace, kdy bude formou rozsáhlého kybernetického útoku závažným způsobem ohrožena nebo narušena bezpečnost České republiky, počítá záměr se zavedením zvláštního stavu fungování zákona o kybernetické bezpečnosti, tj. stavu kybernetického nebezpečí. Vzhledem k tomu, že v tomto případě nejde o zvláštní stav s obecnou osobní a věcnou působností (tj. vztahuje se jen na okruh

subjektů a vztahů, na něž běžně dopadá zákon o kybernetické bezpečnosti), není z důvodu zachování pravidel legislativní techniky vhodné upravovat tento stav v krizovém zákoně (tj. v předpise v obecnou věcnou a osobní působností).

Z uvedených důvodů byl pro implementaci zvolen model zvláštního zákona, jehož návrh bude v paragrafovém znění připraven ve vzájemné spolupráci NBÚ a dalších orgánů veřejné moci působících na úseku elektronických komunikací, bezpečnosti a krizového řízení.

5.2 Vynucování

Struktura povinností předpokládaných záměrem se vztahuje k soukromoprávním subjektům i veřejnoprávním korporacím, přičemž základní jejich rozlišení je podle typu infrastruktury, kterou příslušný subjekt spravuje či zajišťuje. Kontrolní a sankční pravomoci jsou pak rozděleny tak, aby reflektovaly současné postavení a kompetence ČTÚ na úseku elektronických komunikací následovně:

- Povinnost poskytovatelů služeb elektronických komunikací a subjektů zajišťující sítě elektronických komunikací hlásit kontaktní údaje pro předávání informací o kybernetických bezpečnostních událostech a povinnost vybraných poskytovatelů služeb elektronických komunikací a vybraných subjektů zajišťující sítě elektronických komunikací hlásit kybernetické bezpečnostní události: kontroluje a sankcionuje ČTÚ. Povinnost provádět protiopatření stanovená NBÚ ve stavu kybernetického nebezpečí: kontroluje a sankcionuje NBÚ.
- Povinnosti správců kritické komunikační infrastruktury hlásit kontaktní údaje pro předávání informací o kybernetických bezpečnostních událostech a hlásit kybernetické bezpečnostní události se vztahem ke kritické komunikační infrastruktuře: kontroluje a sankcionuje ČTÚ. Povinnost chránit systémy zařazené do kritické komunikační infrastruktury (tj. prvky kritické komunikační infrastruktury) bezpečnostními opatřeními: kontroluje a sankcionuje NBÚ. Povinnost provádět protiopatření stanovená NBÚ: kontroluje a sankcionuje NBÚ.
- Povinnosti správců informačních systémů kritické informační infrastruktury hlásit kontaktní údaje pro předávání informací o kybernetických bezpečnostních událostech, hlásit kybernetické bezpečnostní události se vztahem k informačním

systémům kritické informační infrastruktury a provádět protiopatření stanovená NBÚ: kontroluje a sankcionuje NBÚ. Povinnost chránit systémy zařazené do kritické informační infrastruktury (tj. prvky kritické informační infrastruktury) bezpečnostními opatřeními: kontroluje a sankcionuje NBÚ.

- Povinnosti správců informačních systémů veřejné správy hlásit kontaktní údaje pro předávání informací o kybernetických bezpečnostních událostech, hlásit kybernetické bezpečnostní incidenty a provádět protiopatření stanovená NBÚ: kontroluje a sankcionuje NBÚ.

Kontrolní kompetence budou upraveny v návaznosti na zákon o státní kontrole. Sankční aparát bude zahrnovat ukládání opatření k nápravě a pokuty.

5.3 Přezkum účinnosti regulace

Již samotný návrh zpracování nové právní úpravy vychází především s ohledem na potřeby praxe. Rovněž v případě přijetí nového zákona o kybernetické bezpečnosti bude k přezkumu účinnosti docházet nadále na základě provádění kontrolní činnosti a konzultací se subjekty, jichž se zákon o kybernetické bezpečnosti dotýká, bude sledováno uplatňování nově upravených procesních pravidel v praxi. V důsledku této činnosti bude následně zvažována případná novelizace či úplné odstranění těch ustanovení, jež se v praxi neosvědčí, a naopak zavedení nových mechanismů, které regulovanou činnost v praxi zefektivnily.

B: Návrh věcného řešení

6. Vymezení pojmů

Záměr vychází z pravidel legislativní techniky a předpokládá explicitní vymezení pouze u specifických pojmů nebo u pojmů, jejichž význam v běžném jazyce by mohl komplikovat následnou interpretaci. Legální definice zahrne následující pojmy vymezené v úvodních ustanoveních:

- Kybernetický prostor – digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními a komunikačními technologiemi, zahrnující připojení k veřejné síti (internet).
- Kybernetická bezpečnost – souhrn právních, organizačních, technických, fyzických a vzdělávacích opatření namířených na zajištění nerušeného a bezvadného fungování kybernetického prostoru.
- Kritická informační infrastruktura – prvek kritické informační infrastruktury nebo systém těchto prvků, narušení jehož funkce by mohlo způsobit poškození nebo ohrožení zájmu České republiky.
- Kritická komunikační infrastruktura - prvek kritické komunikační infrastruktury nebo systém těchto prvků, narušení jehož funkce by mohlo způsobit poškození nebo ohrožení zájmu České republiky.
- Zájmem České republiky zachování její ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob.
- Prvek kritické informační infrastruktury – informační systém se zvláštním významem pro kybernetickou bezpečnost České republiky, jehož dlouhodobá nefunkčnost bude mít za následek ohrožení nebo poškození konkrétního zájmu České republiky, a který je zařazený do seznamu prvků kritické informační infrastruktury. Seznam prvků kritické informační infrastruktury stanoví nařízením vláda.

- Prvek kritické komunikační infrastruktury – služba[43)] nebo síť elektronických komunikací[44)] se zvláštním významem pro kybernetickou bezpečnost České republiky, jejíž dlouhodobá nefunkčnost bude mít za následek ohrožení nebo poškození zájmu České republiky, a která je zahrnuta do seznamu prvků kritické komunikační infrastruktury. Seznam prvků kritické komunikační infrastruktury stanoví nařízením vláda.
- Kybernetická bezpečnostní událost – událost s dopadem na služby nebo sítě elektronických komunikací anebo na informační systémy, která představuje narušení jejich bezpečnosti a pravidel definovaných k jejich ochraně, která je způsobilá ohrozit nebo poškodit zájem České republiky, a jež je zařazena v seznamu typů kybernetických bezpečnostních událostí vydávaném formou vyhlášky NBÚ.
- Správce informačního systému kritické informační infrastruktury - subjekt, který určuje účel a prostředky zpracování informací a odpovídá za prvek kritické informační infrastruktury.
- Správce systému kritické komunikační infrastruktury – subjekt, který poskytuje službu elektronických komunikací nebo zajišťuje síť elektronických komunikací zařazenou do seznamu kritické komunikační infrastruktury.
- Národní centrum kybernetické bezpečnosti – útvar NBÚ působící na úseku kybernetické bezpečnosti, který je přímo podřízen řediteli NBÚ.
- Ústřední dohledové pracoviště (standardně mezinárodně užívaný termín „Národní CERT“) pracoviště provozované zpravidla soukromoprávním subjektem na základě veřejnoprávní smlouvy, které zajišťuje a zprostředkovává sdílení informací (hlášení bezpečnostních událostí, zranitelností a další) v národním i mezinárodním kontextu (i jako kontaktní místo poslední instance), a to zejména pro soukromoprávní subjekty, akademickou sféru, oblast samosprávy, neziskový sektor, za předpokladu, že subjekty z těchto oblastí nepodléhají zcela nebo v některých částech působnosti NBÚ. Ústřední dohledové pracoviště koordinuje svou činnost s NBÚ.

[43)] § 2 písm. n) zákona č. 127/2005 Sb., o elektronických komunikacích.

[44)] § 2 písm. h) zákona č. 127/2005 Sb.

- Národní dohledové pracoviště (standardně mezinárodně užívaný pojem „Vládní CERT“) – pracoviště provozované jako součást Národního centra kybernetické bezpečnosti za účelem ochrany služeb a sítí elektronických komunikací a informačních systémů před kybernetickými bezpečnostními událostmi.
- Stav kybernetického nebezpečí – stav vyhlašovaný předsedou vlády České republiky na základě návrhu ředitele NBÚ, je-li ve velkém rozsahu ohrožena bezpečnost služeb nebo sítí elektronických komunikací anebo informačních systémů, a tím dojde k porušení nebo ohrožení zájmu České republiky a ohrožení není možné odvrátit běžnou činností Národního centra kybernetické bezpečnosti.
- Protiopatření – úkony a činnosti, jichž je třeba k ochraně sítí elektronických komunikací nebo informačních systémů před negativním dopadem kybernetické bezpečnostní události (např. instalace nové verze antiviru, úprava bezpečnostních pravidel firewallu, instalace bezpečnostních záplat informačního systému).
- Bezpečnostní opatření – technologicky zcela neutrální opatření, která nejsou takového charakteru, aby určovala konkrétní technologii, konkrétního výrobce nebo poskytovatele služeb, aby nemohlo dojít k determinaci bezpečnostních řešení užívaných subjekty regulace. Uvedená opatření budou vydávána NBÚ ve formě vyhlášky a budou v souladu s mezinárodními standardy a normami.

7. Působnost úpravy

7.1 Věcná působnost

Smyslem a účelem zákona je ochrana českého kyberprostoru tak, aby bylo možno zajistit subjektům pod jurisdikcí České republiky odpovídající nástroje a standardy pro řešení kybernetické bezpečnosti jejich informačních systémů a elektronických komunikací a nerušený výkon jejich práva na informační sebeurčení. Tomu odpovídá i věcná působnost, jejímž předmětem jsou právní vztahy k informační a komunikační infrastruktuře.

Rozdělení věcné působnosti je dáno skutečností, že kyberprostor České republiky je možno z hlediska kybernetické bezpečnosti členit na část kritickou (tj. část se zvýšenou

důležitostí pro fungování státu) a část ostatní (tj. veškeré ostatní služby elektronických komunikací a služby informační společnosti). Z kritické infrastruktury českého kyberprostoru je předmětem záměru zákona jak segment sítí a služeb elektronických komunikací (tj. kritická komunikační infrastruktura), tak i segment informačních systémů (tj. kritická informační infrastruktura). Z ostatní informační a komunikační infrastruktury českého kyberprostoru dopadá záměr pouze na komunikační segment, tj. na služby a sítě elektronických komunikací. Specificky pak dopadá záměr na informační systémy veřejné správy, tj. na systémy podle zákona č. 365/2000 Sb., přičemž právní regulace nebude v celém rozsahu dopadat na všechny správce informačních systémů veřejné správy.

Definici kritické informační a kritické komunikační infrastruktury provede zákon o kybernetické bezpečnosti, seznam prvků stanoví vláda formou nařízení. Definice informačních systémů veřejné správy je provedena zákonem č. 365/2000 Sb.

Pojem „kritická“ je použit úmyslně, neboť vyjadřuje zvýšenou důležitost dotčené infrastruktury pro fungování státu a společnosti, ale jeho obsahem je jiná množina subjektů než v zákoně č. 240/2000 Sb., o krizovém řízení, ve znění pozdějších předpisů. Zákon o kybernetické bezpečnosti bude pracovat s jinými kritérii, na základě kterých se určují prvky kritické komunikační a kritické informační infrastruktury, než je tomu u krizového zákona a jeho prováděcích předpisů, jehož nastavená kritéria jsou pro oblast kybernetické bezpečnosti ne zcela vyhovující.

7.2 Osobní působnost

Nová právní úprava bude obecně dopadat na následující okruhy subjektů:

- *Poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací*. Tyto subjekty, budou mít nově povinnost oznámit ústřednímu dohledovému pracovišti kontaktní údaje pro předávání informací o kybernetických bezpečnostních událostech a vybraní poskytovatelé služeb elektronických komunikací a vybrané subjekty zajišťující sítě elektronických komunikací budou mít povinnost hlásit kybernetické bezpečnostní události, které se vyskytnou v jejich komunikační infrastruktuře ústřednímu dohledovému pracovišti. Při vyhlášení stavu kybernetického nebezpečí budou mít tyto subjekty rovněž povinnost provádět protiopatření nařízená NBÚ.

- *Správci systémů kritické komunikační infrastruktury*. Jedná se o podskupinu poskytovatelů služeb elektronických komunikací a subjektů zajišťujících sítě elektronických komunikací. Tyto subjekty budou mít povinnosti oznámit NBÚ kontaktní údaje pro nepřetržité předávání informací o kybernetických bezpečnostních událostech a hlásit NBÚ kybernetické bezpečnostní události se vztahem ke kritické komunikační infrastruktuře, které se vyskytnou v jejich komunikační infrastruktuře. Tyto subjekty budou mít povinnost chránit systémy zařazené do kritické komunikační infrastruktury (tj. prvky kritické komunikační infrastruktury) bezpečnostními opatřeními, jejichž parametry stanoví NBÚ vyhláškou. Na rozdíl od obecné kategorie poskytovatelů služeb elektronických komunikací resp. subjektů zajišťujících sítě elektronických komunikací budou mít správci systémů kritické komunikační infrastruktury povinnost aplikovat protiopatření stanovená NBÚ i v běžném režimu (tj. i mimo režim stavu kybernetického nebezpečí). Jejich rozsah bude vymezen rozhodnutím nebo opatřením obecné povahy.
- *Správci informačních systémů kritické informační infrastruktury.* Tyto subjekty budou mít povinnosti oznámit NBÚ kontaktní údaje pro nepřetržité předávání informací o kybernetických bezpečnostních událostech a hlásit NBÚ kybernetické bezpečnostní události se vztahem k informačním systémům kritické informační infrastruktury, které se vyskytnou v jejich informační infrastruktuře. Tyto subjekty budou mít povinnost chránit informační systémy zařazené do kritické informační infrastruktury (tj. prvky kritické informační infrastruktury) bezpečnostními opatřeními, jejichž parametry stanoví NBÚ vyhláškou. Rovněž budou mít tyto subjekty povinnost aplikovat protiopatření, která jim stanoví NBÚ. Jejich rozsah bude vymezen rozhodnutím nebo opatřením obecné povahy.
- *Správci informačních systémů veřejné správy*[45)]. Jedná se o ministerstva, jiné správní úřady a územní samosprávné celky, jakož i další orgány veřejné moci, které určují účel a prostředky zpracování informací a odpovídají za informační systémy podle zákona č. 365/2000 Sb. Bude stanovena povinnost chránit informační systémy veřejné správy bezpečnostními opatřeními, jejichž parametry stanoví NBÚ vyhláškou, a to jen u informačních systémů, jež jsou

[45)] § 2 písm. c) zákona č. 365/2000 Sb., o informačních systémech veřejné správy.

významné (nelze tyto požadavky vztahovat na nevýznamné informační systémy), přičemž zákon stanoví kritéria pro kategorizaci informačního systému. Na rozdíl od povinnosti aplikace bezpečnostních opatření, která se týkají užší množiny správců, musí všichni správci informačních systémů veřejné správy hlásit výskyt kybernetických bezpečnostních událostí NBÚ a provádět protiopatření, která jim NBÚ stanoví.

7.3 Místní působnost

Záměr nepočítá s explicitním stanovením místní působnosti zákona.

7.4 Časová působnost

Zákon plánovaně stanoví shora uvedeným subjektům nové typy povinností, zejm. povinnost aplikovat opatření ke hlášení kybernetických bezpečnostních událostí a opatření k zabezpečení informačních a komunikačních systémů. Je tedy nutno poskytnout soukromoprávním i veřejnoprávním subjektům dostatečný čas k implementaci těchto opatření. Lze však v tomto směru zohlednit skutečnost, že oznamovací resp. zabezpečovací technologie již řada subjektů, na něž dopadnou nové zákonné povinnosti, v současné době používá a adaptace na nová pravidla tedy nebude nijak náročná.

Lhůty ke splnění povinností budou zákonem stanoveny následovně:

- *Poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací* – povinnost hlásit kontaktní údaje pro předávání informací o kybernetických bezpečnostních událostech: 30 dnů ode dne nabytí účinnosti zákona, povinnost vybraných poskytovatelů služeb elektronických komunikací a vybraných subjektů zajišťující sítě elektronických komunikací zavést hlášení kybernetických bezpečnostních událostí: nejpozději (nejdéle) do 1 roku ode dne nabytí účinností zákona, povinnost provádět protiopatření stanovená NBÚ ve stavu kybernetického nebezpečí: nejpozději (nejdéle)do 1 roku ode dne nabytí účinnosti zákona.
- *Správci kritické komunikační infrastruktury* - povinnost hlásit kontaktní údaje pro předávání informací o kybernetických bezpečnostních událostech: 30 dnů ode

dne nabytí účinnosti zákona, povinnost zavést hlášení kybernetických bezpečnostních událostí: nejpozději (nejdéle) do 1 roku ode dne nabytí účinností zákona, povinnost bezodkladně provádět protiopatření stanovená NBÚ: nejpozději (nejdéle) do 1 roku ode dne nabytí účinnosti zákona.

- *Správci informačních systémů kritické informační infrastruktury* - povinnost hlásit kontaktní údaje pro předávání informací o kybernetických bezpečnostních událostech: 30 dnů ode dne nabytí účinnosti zákona, povinnost zavést hlášení kybernetických bezpečnostních událostí: nejpozději (nejdéle) do 1 roku ode dne nabytí účinností zákona, povinnost bezodkladně provádět protiopatření stanovená NBÚ: nejpozději (nejdéle) do 1 roku ode dne nabytí účinnosti zákona.
- *Správci informačních systémů veřejné správy* - povinnost hlásit kontaktní údaje pro předávání informací o kybernetických bezpečnostních událostech: 30 dnů ode dne nabytí účinnosti zákona, povinnost zavést hlášení kybernetických bezpečnostních událostí: nejpozději (nejdéle) do 1 roku ode dne nabytí účinností zákona, povinnost bezodkladně provádět protiopatření stanovená NBÚ: nejpozději (nejdéle) do 1 roku ode dne nabytí účinnosti zákona. Kontaktní údaje budou předávány do veřejného informačního systému, který obsahuje základní informace o dostupnosti a obsahu zpřístupněných informačních systémů veřejné správy (informační systém o ISVS), který na základě § 4 odst. 1 písm. h) zákona č. 365/2000 Sb. spravuje Ministerstvo vnitra. Obsah tohoto informačního systému bude doplněn o kontaktní údaje výslovně pro potřeby zákona o kybernetické bezpečnosti.

8. NBÚ, Národní centrum kybernetické bezpečnosti a dohledová pracoviště

Podle usnesení vlády České republiky ze dne 19. října 2011 č. 781 je ústředním orgánem státní správy na úseku kybernetické bezpečnosti NBÚ. Organizační řešení potřeby centralizovaného vyhodnocování informací o kybernetické bezpečnostní situaci České republiky bude postaveno na existenci dvou dohledových pracovišť, tj. národního (standardně mezinárodně užívaný pojem „Vládní CERT“) a ústředního (standardně mezinárodně užívaný pojem „Národní CERT“). Národní dohledové pracoviště bude

součástí Národního centra kybernetické bezpečnosti zřízeného jako součást organizační struktury NBÚ. Ústřední dohledové pracoviště bude provozováno soukromoprávním subjektem na základě veřejnoprávní smlouvy uzavřené s NBÚ.

Zákon v této souvislosti upraví:

- *NBÚ jako orgán státní správy na úseku kybernetické bezpečnosti.* NBÚ bude vyhodnocovat údaje o kybernetických bezpečnostních událostech získaných z dohledových pracovišť, vydávat prováděcí předpisy, kontrolovat a sankcionovat nedodržení povinností stanovených zákonem o kybernetické bezpečnosti, navrhovat vyhlášení stavu kybernetického nebezpečí, působit jako koordinační orgán ve stavu kybernetického nebezpečí a spolupracovat s ostatními státními orgány.
- *Národní centrum kybernetické bezpečnosti jako útvar NBÚ působící na úseku kybernetické bezpečnosti a přímo podřízený řediteli NBÚ.* Národní centrum kybernetické bezpečnosti bude součástí vnitřní organizační struktury NBÚ. Bude sestávat z národního dohledového pracoviště a z organizačních útvarů zajišťujících jeho činnost. Bude spolupracovat s ostatními dohledovými pracovišti (CERT/CSIRT), zajišťovat mezinárodní spolupráci, spolupráci s výzkumnými a vývojovými pracovišti, přípravu prováděcích předpisů, technických parametrů (standardů) a doporučení (best practices), prevenci a vzdělávání v oboru kybernetické bezpečnosti. Národní centrum kybernetické bezpečnosti bude zajišťovat výzkum a vývoj prostředků pro zajišťování a analýzu kybernetických hrozeb a incidentů, bude provádět analýzy zranitelnosti. Národní centrum kybernetické bezpečnosti bude provádět kontrolu plnění povinností správci informačních a komunikačních systémů kritické informační a komunikační infrastruktury a správci informačních systémů veřejné správy a zjištěné skutečnosti předávat k dalšímu řízení ostatním útvarům NBÚ (např. správní trestání). Stávající kompetence Ministerstva vnitra vůči správcům ISVS podle zákona č. 365/2000 Sb. zůstanou zachovány.
- *Národní dohledové pracoviště jako součást centra kybernetické bezpečnosti (standardně mezinárodně užívaný termín „Vládní CERT“)*. Národní dohledové pracoviště bude vyhodnocovat údaje z kritické informační a komunikační infrastruktury a z informačních systémů veřejné správy. V případě výskytu

kybernetické bezpečnostní události poskytne součinnost správci příslušného systému resp. sítě. Nebude-li na straně správce náležitá odezva, stanoví NBÚ protiopatření.

- Ústřední dohledové pracoviště (standardně mezinárodně užívaný termín „Národní CERT“) pracoviště provozované zpravidla soukromoprávním subjektem na základě veřejnoprávní smlouvy, které zajišťuje a zprostředkovává sdílení informací (hlášení bezpečnostních událostí a zranitelností) v národním i mezinárodním kontextu (i jako kontaktní místo poslední instance), a to zejména pro soukromoprávní subjekty, akademickou sféru, oblast samosprávy, neziskový sektor, za předpokladu, že subjekty z těchto oblastí nepodléhají zcela nebo v některých částech působnosti NBÚ. Ústřední dohledové pracoviště koordinuje svou činnost s NBÚ.

Národní centrum kybernetické bezpečnosti bude zpracovávat informace o kybernetických bezpečnostních událostech od:

- správců systémů kritické komunikační infrastruktury,
- správců informačních systémů zařazených do kritické informační infrastruktury,
- správců informačních systémů veřejné správy,
- dohledových pracovišť.

Současně bude shora uvedeným subjektům poskytovat informace o kybernetické bezpečnostní situaci, o vyhodnocených kybernetických bezpečnostních událostech a případně metodiku a součinnost k jejich řešení. Národní centrum kybernetické bezpečnosti bude rovněž spolupracovat s obdobnými útvary partnerských států (tj. států, s nimiž bude na úseku kybernetické bezpečnosti navázána rezortní nebo vyšší forma mezinárodní spolupráce), obdobnými pracovišti mezinárodních organizací, nevládních organizací, jakož i vydávat parametry bezpečnostních opatření a nezávazná doporučení (best practices) pro veřejný i soukromý sektor formou oznámení ve Věstníku NBÚ.

NBÚ bude formou rozhodnutí nebo opatření obecné povahy anebo právními předpisy přímo stanovovat konkrétní protiopatření k řešení bezpečnostních událostí:

- správcům systémů kritické komunikační infrastruktury,

- správcům informačních systémů zařazených do kritické informační infrastruktury,
- správcům informačních systémů veřejné správy,
- při vyhlášení stavu kybernetického nebezpečí též ostatním poskytovatelům služeb elektronických komunikací a subjektům zajišťujícím sítě elektronických komunikací.

9. Orgány veřejné moci

Z orgánů veřejné moci bude zákon ukládat povinnosti těm, které spravují informační systémy kritické informační nebo komunikační infrastruktury (tj. těm, které budou odpovídat definici správce informačního systému kritické informační infrastruktury nebo správce systému kritické komunikační infrastruktury podle zákona o kybernetické bezpečnosti) a dále pak v různé míře těm, které spravují informační systémy veřejné správy. Tyto orgány budou mít povinnost oznámit NBÚ kontaktní údaje pro nepřetržité předávání informací o kybernetických bezpečnostních událostech a chránit své informační systémy bezpečnostními opatřeními, jejichž náležitosti stanoví NBÚ vyhláškou. Rovněž budou mít tyto orgány povinnost hlásit výskyt kybernetických bezpečnostních událostí NBÚ a provádět protiopatření, která jim NBÚ stanoví.

Ke splnění povinností hlásit kybernetické bezpečnostní události resp. provádět protiopatření stanovená NBÚ, tj. k zavedení oznamovacích resp. bezpečnostních opatření, bude zákonem stanovena odpovídající lhůta (viz časová působnost).

10. Soukromoprávní subjekty

K tomu, aby bylo možno zajistit ochranu kyberprostoru České republiky, je nutno kromě orgánů veřejné moci stanovit též povinnosti soukromoprávním subjektům. Zákon je v tomto směru koncipován spíše jako minimalistický, přičemž nezasahuje do obsahu komunikace ani do jiné obsahové stránky fungování informační a komunikační infrastruktury. Rovněž zákon obecně nezahrnuje úpravu přímých výkonných pravomocí státu – stát tedy prostřednictvím činnosti Národního centra kybernetické bezpečnosti pouze vyhodnocuje informace o bezpečnostní situaci v českém kyberprostoru a přímo

působí jen ve vztahu k systémům, které mají pro kybernetickou bezpečnost České republiky kritický význam (tj. k prvkům kritické informační a komunikační infrastruktury) a ve vztahu k informačním systémům veřejné správy.

V běžném režimu zákona o kybernetické bezpečnosti budou mít soukromoprávní subjekty poskytující služby elektronických komunikací nebo zajišťující sítě elektronických komunikací pouze sankcionovatelnou povinnost oznámit ústřednímu dohledovému pracovišti kontaktní údaje pro předávání informací o bezpečnostních událostech a vybraní poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací sankcionovatelnou povinnost zavést hlášení kybernetických bezpečnostních událostí ústřednímu dohledovému pracovišti (podrobnosti k technické specifikaci kybernetických bezpečnostních událostí a formátu hlášení stanoví NBÚ prováděcím předpisem). Ústřední dohledové pracoviště bude vedle průběžného vyhodnocování kybernetické bezpečnostní situace v soukromém sektoru též poskytovat prostřednictvím předaných kontaktních údajů soukromoprávním subjektům metodickou podporu a pomoc. Až při vyhlášení stavu kybernetického nebezpečí budou mít soukromoprávní poskytovatelé služeb elektronických komunikací resp. subjekty zajišťující sítě elektronických komunikací povinnost provádět protiopatření stanovená NBÚ.

Ve vztahu ke kritické informační a komunikační infrastruktuře nebude zákon rozlišovat povahu subjektů spravujících příslušné systémy. Vzhledem ke kritické důležitosti těchto systémů tak zákon u soukromoprávních i veřejnoprávních správců počítá nejen s povinností hlásit výskyt kybernetických bezpečnostních událostí NBÚ, ale též s povinností aplikovat bezpečnostní opatření k ochraně těchto systémů a povinnost provádět protiopatření stanovená NBÚ.

Struktura povinností ukládaných soukromoprávním subjektům bude následující:

- *Poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací.* Tyto subjekty budou mít povinnost oznámit ústřednímu dohledovému pracovišti kontaktní údaje pro předávání informací o kybernetických bezpečnostních událostech a vybraní poskytovatelé služeb elektronických komunikací a vybrané subjekty zajišťující sítě elektronických komunikací budou mít povinnost hlásit kybernetické bezpečnostní události, které se vyskytnou v jejich komunikační infrastruktuře ústřednímu dohledovému

pracovišti. Při vyhlášení stavu kybernetického nebezpečí budou mít tyto subjekty rovněž povinnost provádět protiopatření nařízená NBÚ. Povinnosti oznámit ústřednímu dohledovému pracovišti kontaktní údaje a povinnost vybraných subjektů oznamovat mu výskyt kybernetických bezpečnostních událostí budou formou odkazu zahrnuty pod rozsah povinností k zajištění bezpečnosti a integrity sítí podle zákona č. 127/2005 Sb. a upraveny zákonem o kybernetické bezpečnosti a vyhláškou NBÚ – tyto povinnosti bude sankcionovat v rámci své kompetence ČTÚ. Povinnost provádět protiopatření nařízená NBÚ za stavu kybernetického nebezpečí bude založena zákonem o kybernetické bezpečnosti a nedodržení této povinnosti bude sankcionovat NBÚ.

- *Správci systémů kritické komunikační infrastruktury*. Tyto subjekty budou mít obecné povinnosti oznámit NBÚ kontaktní údaje pro nepřetržité předávání informací o bezpečnostních událostech a hlásit NBÚ kybernetické bezpečnostní události se vztahem ke kritické informační infrastruktuře, které se vyskytnou v jejich komunikační infrastruktuře a povinnost aplikovat protiopatření nařízená NBÚ. Povinnosti oznámit NBÚ kontaktní údaje a oznamovat mu výskyt kybernetických bezpečnostních událostí budou formou odkazu zahrnuty pod rozsah povinností k zajištění bezpečnosti a integrity sítí podle zákona č. 127/2005 Sb. a upraveny zákonem o kybernetické bezpečnosti a vyhláškou NBÚ – tyto povinnosti bude sankcionovat v rámci své kompetence ČTÚ. Tyto subjekty budou mít rovněž povinnost chránit systémy zařazené do kritické komunikační infrastruktury (tj. prvky kritické komunikační infrastruktury) bezpečnostními opatřeními, jejichž parametry stanoví NBÚ vyhláškou. Tato povinnost a povinnost provádět protiopatření nařízená NBÚ bude založena zákonem o kybernetické bezpečnosti a bude ji sankcionovat NBÚ.
- *Správci informačních systémů kritické informační infrastruktury (tj.* soukromoprávní subjekty, které spravují informační systémy zařazené do seznamu kritické informační infrastruktury). Tyto subjekty budou mít povinnosti oznámit NBÚ kontaktní údaje pro nepřetržité předávání informací o kybernetických bezpečnostních událostech a hlásit NBÚ kybernetické bezpečnostní události se vztahem k informačním systémům kritické informační infrastruktury, které se vyskytnou v jejich informační infrastruktuře. Tyto

subjekty budou mít povinnost chránit informační systémy zařazené do kritické informační infrastruktury (tj. prvky kritické informační infrastruktury) bezpečnostními opatřeními, jejichž parametry stanoví NBÚ vyhláškou. Rovněž budou mít tyto subjekty povinnost provádět protiopatření, která jim nařídí NBÚ. Tyto povinnosti budou založeny zákonem o kybernetické bezpečnosti a budou sankcionovány NBÚ.

Výše uvedené povinnosti mohou mít za následek u soukromoprávních subjektů poskytujících služby elektronických komunikací resp. u subjektů zajišťujících sítě elektronických komunikací nutnost aplikovat bezpečnostní opatření, které umožní identifikovat a oznamovat kybernetické bezpečnostní události. Investice v tomto směru nemusí být ve svém úhrnu podstatné, neboť uvedené subjekty již v současné době takových technologií běžně využívají. Z důvodu potřeby adresnosti uložení protiopatření za stavu kybernetického nebezpečí dojde ke sdílení kontaktních údajů mezi ústředním dohledovým pracovištěm a NBÚ.

NBÚ stanoví prováděcím předpisem minimální bezpečnostní opatření, které by jednotlivé subjekty podléhající regulaci měly dodržovat. Přes takto uloženou povinnost však může dojít ke vzniku škody. V rámci odpovědnosti za škodu bude postupováno standardní cestou, tedy, že tyto subjekty v případě nedodržení předepsaných bezpečnostních opatření budou odpovídat podle obecné odpovědnosti stanovené v občanském zákoníku. V případě, že dojde ke vzniku škody, přestože subjekty podléhající regulaci dodržely stanovenou povinnost aplikovat bezpečnostní opatření, nebudou standardně za takto vzniklou škodu odpovídat v případě prokázání skutečnosti, že vynaložily veškeré úsilí, které bylo možno po nich požadovat, aby vzniku škody zabránily. Povinnost orgánů státu za škodu se rovněž řídí obecně platnými právními předpisy (viz kap. 15).

11. Zpracování osobních údajů, provozních údajů a přístup k informacím veřejného sektoru

Navrhovaná úprava se přímo nedotýká zpracování osobních údajů[46)], provozních údajů[47)], lokalizačních údajů[48)] nebo přístupu k informacím veřejného sektoru. Veškeré údaje, které budou na základě navrhované úpravy předávány a zpracovávány NBÚ a ústředním dohledovým pracovištěm, se týkají výlučně kybernetických bezpečnostních událostí resp. opatření k jejich řešení a nemají vztah ke konkrétním uživatelům služeb elektronických komunikací ani k obsahu jejich vzájemné komunikace. NBÚ ani ústřední dohledové pracoviště tedy nebudou zpracovávat žádné informace, které by zasahovaly do práva na informační sebeurčení (viz dále) a byly chráněny zvláštními zákony. Pokud přesto dojde při zpracování hlášení kybernetických bezpečnostních událostí k předání údajů, které mají charakter údajů, které jsou chráněny zvláštními zákony, bude s nimi nakládáno v souladu s těmito příslušnými zákony.

NBÚ bude v rámci evidence kybernetických bezpečnostních událostí uchovávat identifikační údaje systémů, v nichž se odehrály kybernetické bezpečnostní události, a dále údaje o postupu a úspěšnosti jejich řešení. Tyto údaje mohou v případě zneužití poškodit zájmy České republiky nebo dotčených subjektů. Z tohoto důvodu budou chráněny formou institutu mlčenlivosti. Nejzávažnější informace s velkým významem pro kybernetickou bezpečnost České republiky budou chráněny jako utajované informace (viz kap. Evidence).

12. Evidence

Zpracování údajů o kybernetických bezpečnostních událostech je nutným předpokladem pro vyhodnocování kybernetických útoků, vývoj postupů a technik obrany i pro efektivní spolupráci se soukromým sektorem a mezinárodními organizacemi. Údaje o kybernetických bezpečnostních událostech mohou sloužit též k vývoji účinnějších ochranných technologií. Z tohoto důvodu počítá věcný záměr s tím, že NBÚ povede evidenci kybernetických bezpečnostních událostí.

---

46) § 4 písm. a) zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.

47) § 90 odst. 1 zákona č. 127/2005 Sb.

48) § 91 odst. 1 zákona č. 127/2005 Sb.

Hlášení o kybernetických bezpečnostních událostech, jakož i záznam o provedených protiopatřeních, jsou však rovněž informacemi velkého bezpečnostního i ekonomického významu. Mohou vést k identifikaci napadeného systému, odkrýt bezpečnostní postupy a protiopatření útočníkům, ukázat slabá místa informační a komunikační infrastruktury apod. Je tedy nutno tyto informace chránit před zneužitím a vyloučit možnost jejich úniku. Přitom je však třeba zachovat výhody sdílení informací o kybernetických bezpečnostních událostech s dalšími subjekty podílejícími se na ochraně českého kyberprostoru (včetně provozovatele ústředního dohledového pracoviště, provozovatelů místních dohledových pracovišť typu CERT/CSIRT apod.), jakož i umožnit standardní demokratickou kontrolu činnosti NBÚ prostřednictvím práva na informace.

Identifikační údaje systému, v němž došlo ke kybernetické bezpečnostní události, identifikační údaje původce kybernetické bezpečnostní události a záznam o řešení kybernetické bezpečnostní události ke každé z kybernetických bezpečnostních událostí budou mít charakter informací, k nimž bude vázána povinnost mlčenlivosti. Záznamy o řešení závažných kybernetických bezpečnostních událostí můžou mít charakter utajovaných informací[49)]. Informace z evidence kybernetických bezpečnostních událostí budou poskytovány orgánům činným v trestním řízení a dále pak jiným orgánům veřejné moci, bude-li to nezbytné pro plnění úkolů v rámci jejich působnosti.

13. Spolupráce

Spolupráce se soukromým sektorem, ostatními orgány veřejné moci a zahraničními subjekty je nutnou podmínkou praktické efektivity zákonných povinností k ochraně kybernetické bezpečnosti České republiky. Základem spolupráce při budování systému kybernetické bezpečnosti i při řešení konkrétních kybernetických bezpečnostních událostí je výměna informací. Vzájemnou spoluprací dohledových pracovišť (za součinnosti místních dohledových pracovišť státních orgánů, telekomunikačních operátorů, mezinárodních organizací) lze docílit efektivního řešení i rozsáhlých kybernetických útoků.

[49)] § 2 zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti.

13.1 Spolupráce se soukromoprávními subjekty

NBÚ bude oprávněn uzavřít veřejnoprávní smlouvu s provozovatelem ústředního dohledového pracoviště. Na základě této smlouvy bude subjekt s odpovídající technickou kompetencí zajišťovat sběr a vyhodnocování údajů z komunikační infrastruktury a poskytovat soukromoprávním poskytovatelům služeb elektronických komunikací a subjektům zajišťujícím sítě elektronických komunikací součinnost při řešení kybernetických bezpečnostních událostí. Zmocnění k této spolupráci bude provedeno explicitně, přičemž bude NBÚ uložena povinnost zveřejnit sjednanou veřejnoprávní smlouvu ve Věstníku NBÚ.

Vedle toho bude NBÚ oprávněn spolupracovat s dalšími soukromoprávními subjekty, typicky s provozovateli místních dohledových pracovišť, se subjekty provádějícími výzkum a vývoj.

13.2 Spolupráce s orgány veřejné moci a veřejnoprávními korporacemi

NBÚ bude ze zákona oprávněn spolupracovat s orgány veřejné moci a s veřejnoprávními korporacemi, které budou působit na úseku kybernetické bezpečnosti. Vedle bezpečnostních složek České republiky a orgánů krizového řízení půjde zejména o jednotlivé správce informačních systémů veřejné správy, veřejnoprávní správce kritické informační a komunikační infrastruktury, výzkumné a vývojové příspěvkové organizace státu, univerzity apod. Předmětem spolupráce bude zejména výměna informací, vzájemná součinnost při vývoji a testování bezpečnostních opatření a účast na cvičeních.

13.3 Mezinárodní spolupráce

Mezinárodní spolupráce, kterou bude NBÚ navazovat, bude mít charakter účasti v mezinárodních strukturách k ochraně kybernetické bezpečnosti (zpravidla formou účasti v mezinárodních organizacích a sdruženích zajišťujících výměnu informací o kybernetických bezpečnostních událostech a koordinaci ochranných opatření) a účasti na mezinárodních akcích. NBÚ bude oprávněn sjednávat na úseku kybernetické bezpečnosti rezortní mezinárodní smlouvy, zastupovat Českou republiku v mezinárodních organizacích a účastnit se mezinárodních akcí, tj. cvičení a simulací.

14. Kontrola a sankce

Efektivní ochrana kybernetické bezpečnosti vyžaduje implementaci odpovídajícího kontrolního a sankčního aparátu. Jeho struktura vychází ze systematiky záměru, tj. ze členění kyberprostoru na infrastrukturu kritickou a ostatní s přihlédnutím ke specifickému postavení správců informačních systémů veřejné správy. Současně je třeba zohlednit skutečnost, že poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací jsou nyní pod kontrolní a sankční pravomocí ČTÚ.

Vzhledem k tomu, že záměr je formulován jako minimalistický s ohledem na kompetence orgánů veřejné moci a nepočítá se zásadní změnou v organizaci kompetencí na úseku elektronických komunikací, vycházejí kontrolní a sankční pravomoci, zjednodušeně řečeno, z toho, že v segmentu komunikační infrastruktury kontroluje a sankcionuje ČTÚ, zatímco v segmentu informační infrastruktury a specifických povinností na úseku kybernetické bezpečnosti kontroluje a sankcionuje NBÚ, resp. u dílčí části Ministerstvo vnitra.

Záměr tedy počítá s následujícím rozdělením kontrolních a sankčních pravomocí:

NBÚ:

- Pravomoc kontrolovat správce informačních systémů zařazených do kritické informační infrastruktury (kontrole podléhá nasazení a používání předepsaných bezpečnostních opatření u prvků kritické informační infrastruktury) včetně ukládání opatření k nápravě a sankcí (s vyšší úrovní ve stavu kybernetického nebezpečí).
- Pravomoc ukládat opatření k nápravě a sankce při neprovedení protiopatření nařízeného správci informačního systému zařazeného do kritické informační infrastruktury (s vyšší úrovní ve stavu kybernetického nebezpečí).
- Pravomoc ukládat opatření k nápravě a sankce při neprovedení protiopatření nařízeného správcům informačních systémů veřejné správy (s vyšší úrovní ve stavu kybernetického nebezpečí).

- Pravomoc ukládat opatření k nápravě a sankce při neprovedení protiopatření nařízeného správci systému kritické komunikační infrastruktury (s vyšší úrovní ve stavu kybernetického nebezpečí).
- Pravomoc ukládat opatření k nápravě a sankce při neprovedení protiopatření nařízeného NBÚ poskytovateli služeb elektronických komunikací nebo subjektu zajišťujícímu síť elektronických komunikací ve stavu kybernetického nebezpečí.
- Pravomoc kontrolovat a sankcionovat správce informačních systémů veřejné správy, přičemž kontrole a sankcím podléhá oznámení kontaktních údajů pro předávání informací o kybernetických bezpečnostních událostech a povinnost hlásit kybernetické bezpečnostní incidenty a provádět protiopatření stanovená NBÚ.

ČTÚ (formou novely zákona č. 127/2005 Sb.):

- Pravomoc kontrolovat a sankcionovat správce systémů kritické komunikační infrastruktury (kontrole a sankcím podléhá oznámení kontaktních údajů pro předávání informací o kybernetických bezpečnostních událostech a povinnost hlásit kybernetické bezpečnostní události se vztahem ke kritické informační infrastruktuře).
- Pravomoc kontrolovat a sankcionovat poskytovatele služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací (kontrole podléhá oznámení kontaktních údajů pro předávání informací o kybernetických bezpečnostních událostech a u vybraných poskytovatelů služeb elektronických komunikací a vybraných subjektů zajišťujících sítě oznamování kybernetických bezpečnostních událostí formou předepsanou ve vyhlášce NBÚ).

MV (formou novely zákona č. 365/2000 Sb.):

- Pravomoc kontrolovat správce informačních systémů veřejné správy včetně ukládání opatření k nápravě a sankcí (kontrole podléhá nasazení a používání předepsaných bezpečnostních opatření).

Výkon kontrolních pravomocí bude probíhat podle obecných ustanovení zákona o státní kontrole[50)] s přihlédnutím k chystané právní úpravě. Informace o skutečnostech nasvědčujících tomu, že subjekty, jimž ukládají povinnosti zákon o kybernetické bezpečnosti a zákon č. 127/2005 Sb., tyto povinnosti neplní, budou mít nejčastěji povahu vadných nebo chybějících hlášení o kybernetických bezpečnostních událostech, které bude vyhodnocovat Národní centrum kybernetické bezpečnosti. Z tohoto důvodu bude zákon o kybernetické bezpečnosti explicitně upravovat možnost NBÚ dávat podněty ČTÚ k provedení kontroly.

15. Stav kybernetického nebezpečí

Pro případ rozsáhlého kybernetického útoku nebo jiné zvlášť závažné kybernetické bezpečnostní události, která bude mít potenciál bezprostředně ohrozit fungování služeb informační společnosti na území České republiky nebo v mezinárodním měřítku, počítá záměr se zvláštním režimem stavu kybernetického nebezpečí. Zákon o kybernetické bezpečnosti upraví způsob vyhlašování stavu kybernetického nebezpečí, jakož i související specifická práva a povinnosti.

Stav kybernetického nebezpečí bude vyhlašovat předseda vlády České republiky na návrh ředitele NBÚ, přičemž jeho rozhodnutí musí do 24 hodin schválit vláda (v opačném případě se rozhodnutí o vyhlášení stavu kybernetického nebezpečí ruší uplynutím této lhůty). Stav kybernetického nebezpečí bude možno vyhlásit nejvýše na dobu sedmi dnů. Prodloužení stavu kybernetického nebezpečí na dobu dalších sedmi dnů, a to i opakovaně, může provést vláda.

Po vyhlášení stavu kybernetického nebezpečí svolá ředitel NBÚ krizový štáb, který bude přijímat opatření k ochraně českého kyberprostoru a zajišťovat komunikaci s dotčenými tuzemskými a zahraničními subjekty. Krizový štáb bude průběžně vyhodnocovat svou činnost a informovat o ní vládu – pokud dosáhnou kybernetické bezpečnostní události takové intenzity, že dojde ve značném rozsahu k ohrožení životů, zdraví, majetku, vnitřního pořádku nebo bezpečnosti České republiky, informuje krizový štáb vládu o potřebě vyhlášení nouzového stavu[51)].

[50)] Zákon č. 552/1991 Sb., o státní kontrole, ve znění pozdějších předpisů.

[51)] Čl. 5 ústavního zákona č. 110/1998 Sb.

Jedinou podstatnou změnou pro soukromoprávní subjekty bude oproti normálnímu režimu podle zákona o kybernetické bezpečnosti zavedení povinnosti poskytovatelům služeb elektronických komunikací a subjektům zajišťujícím sítě elektronických komunikací provádět protiopatření stanovená NBÚ. Protiopatření budou oznamována prostřednictvím kontaktních údajů, které tito poskytovatelé sdělili ústřednímu dohledovému pracovišti, které jsou sdíleny NBÚ.

Vzhledem k tomu, že je stav kybernetického nebezpečí zvláštním režimem podle zákona o kybernetické bezpečnosti a nedotýká se práv a povinností subjektů mimo osobní působnost zákona (viz osobní působnost), bude jeho úprava systematicky zařazena v zákoně o kybernetické bezpečnosti.

V případě vzniku škody při realizaci protiopatření za stavu kybernetického nebezpečí je dána odpovědnost státu jen pokud budou naplněny podmínky stanovené zákonem č. 82/1998 Sb., o odpovědnosti za škodu způsobenou při výkonu veřejné moci rozhodnutím nebo nesprávným úředním postupem a o změně zákona České národní rady č. 358/1992 Sb., o notářích a jejich činnosti (notářský řád), ve znění pozdějších předpisů.

16. Prováděcí předpisy a doporučení

Záměr počítá s využitím prováděcích předpisů ke konkretizaci technických podrobností k povinnostem pro poskytovatele služeb elektronických komunikací, provozovatelé sítí elektronických komunikací, správce systémů kritické komunikační infrastruktury, správce informačních systémů kritické informační infrastruktury a pro správce ostatních informačních systémů veřejné správy. Vedle prováděcích předpisů záměr počítá též s využitím parametrů bezpečnostních opatření a nezávazných doporučení (best practices) vydávaných ve Věstníku NBÚ.

NBÚ bude formou vyhlášek vydávat:

- Technické podrobnosti pro identifikaci kybernetických bezpečnostních událostí (tj. typologii událostí) – a technické podrobnosti pro předávání informací o výskytu kybernetických bezpečnostních událostí.

- Technické podrobnosti pro zabezpečení informačních systémů kritické informační infrastruktury a technické podrobnosti pro zabezpečení systémů kritické komunikační infrastruktury.

Vláda bude formou nařízení vydávat:

- Seznam prvků kritické informační infrastruktury.
- Seznam prvků kritické komunikační infrastruktury.

17. Změny jiných právních předpisů

Záměr počítá se změnou § 98 zákona č. 127/2005 Sb., který bude nově konkretizovat povinnosti k zajištění bezpečnosti a integrity elektronických komunikací formou odkazu ke specifickým povinnostem poskytovatelů služeb elektronických komunikací a subjektů zajišťujících sítě elektronických komunikací upraveným zákonem o kybernetické bezpečnosti a vyhláškou NBÚ.

Novelizován bude zákon č. 365/2000 Sb.

- Bude navrženo zmocnění k vydání vyhlášky o bezpečnosti informačních systémů veřejné správy (s výjimkou informačních systémů spadajících do kritické informační infrastruktury).
- Budou upravena ustanovení o informačním systému o Informačních systémech veřejné správy (dále jen „ISVS“) tak, aby bylo možno předávat kontaktní údaje pro účely zákona o kybernetické bezpečnosti. Součástí záznamu o ISVS bude i příznak, že ISVS je prvkem kritické informační infrastruktury.

Nelze samozřejmě vyloučit, že v průběhu příprav návrhu paragrafového znění zákona se objeví potřeba novelizace i dalších předpisů, ale jejich rozsah nebude nijak zásadní.

18. Ústavní konformita

S ohledem na aktuální judikaturu Ústavní soudu České republiky[52)] je třeba posuzovat obsah tohoto záměru prostřednictvím standardní aplikace testu proporcionality. Základním právem, k jehož omezení dojde prostřednictvím zákonem o kybernetické bezpečnosti, je právo vlastnické a částečně též i z něj odvozované právo na podnikání. Vzhledem k tomu, že byl při tvorbě zákona zvolen minimalistický přístup k ukládání povinností soukromoprávním subjektům, 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.

Kybernetické bezpečnostní události 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[53)] a v poslední době též několikrát zmíněno i Evropským soudem pro lidská práva a Ústavním soudem České republiky[54)], 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 národního kyberprostoru, kde se tato práva realizují.

Zákon o kybernetické bezpečnosti omezí pouze soukromé vlastníky resp. provozovatele komunikační infrastruktury, tj. poskytovatele služeb a sítí elektronických komunikací. Omezení vlastnického práva resp. práva na podnikání má v tomto případě formu zavedení povinnosti oznámit ústřednímu dohledovému pracovišti kontaktní údaje k předávání informací o kybernetických bezpečnostních událostech a dále pak

[52)] Nálezem Ústavního soudu ze dne 12.října1994, sp. zn. Pl.ÚS 4/94, 214/1994 Sb., N 46/2 SbNU 57.

[53)] Nález Spolkového ústavního soudu ze dne 15. prosince 1983, č.j. BVerfGE 65, 1.

[54)] 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.

vybraným poskytovatelům služeb elektronických komunikací a vybraným správcům sítí elektronických komunikací povinnost tyto bezpečnostní události oznamovat. Tím je zasaženo do *iuris utendi* příslušné komunikační infrastruktury.

Specifické povinnosti jsou pak dále stanoveny subjektům, které provozují systémy zařazené vládou do seznamu kritické informační resp. kritické komunikační infrastruktury. Vedle povinnosti hlásit výskyt kybernetických bezpečnostních událostí (v tomto případě NBÚ) mají tyto subjekty rovněž povinnost aplikovat bezpečnostní opatření splňující předepsaný standard a reagovat na požadavky NBÚ na přijetí protiopatření.

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 – zákon tedy nepředpokládá žádný státní zásah do soukromí uživatelů ani do jejich možností komunikovat.

Právo na informační sebeurčení člověka je zákonem zpracováno jako hodnota, k jejíž ochraně zákon primárně směřuje. Bezpečnost totiž nemůže být brána za hodnotu *per se*, není-li jasné, co vlastně má být zabezpečeno. V tomto případě má zákon jasně vymezenou teleologii, která spočívá v zabezpečení českého kyberprostoru, tj. v zabezpečení fungování služeb informační společnosti, ať soukromých nebo veřejných. Právě prostřednictvím těchto služeb, tj. jejich dostupnosti, spolehlivosti a bezpečnosti, lze v době rostoucího významu informační společnosti svobodně realizovat právo na informační sebeurčení[55)].

Vedle závazků České republiky plynoucích ze členství v mezivládních organizacích 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 tak může dojít k situaci, kdy budou zneužity počítače na území České republiky k útoku na cizí stát (takové případy se u rozsáhlých útoků vyskytují běžně) – Česká

[55)] Zpráva Zvláštního zpravodaje Valného shromáždění OSN č. A/HRC/17/2.

republika, přestože útok neorganizuje ani se na něm nepodílí, může být pohnána k odpovědnosti za to, že takovému útoku, byť k tomu měla prostředky, účinně nezabránila.

Výše zmíněný zásah do vlastnického práva soukromoprávních poskytovatelů služeb elektronických komunikací respektive správců informačních a komunikačních systémů kritické infrastruktury je tedy ve struktuře proporcionality odůvodněn ochranou

- práva na informační sebeurčení (tj. zejm. práva na ochranu soukromí, soukromého života, na svobodu projevu, na přístup k informacím a dalších informačních práv člověka),
- bezpečnosti a integrity České republiky a
- mezinárodních závazků České republiky.

Z výše uvedeného lze formulovat následující stručné závěry ohledně ústavní proporcionality tohoto záměru:

- *Test vhodnosti* – záměr, tak, jak je formulován, nepochybně povede ke zvýšení míry kybernetické bezpečnosti České republiky a k ochraně shora zmíněných hodnot. Dosavadní zkušenosti ukazují, že výměna informací o kybernetických bezpečnostních incidentech a koordinace protiopatření představují nejúčinnější prostředky ochrany kyberprostoru. Záměr tedy vychází z aktuálních poznatků praxe v oboru ICT a vybírá nejefektivnější nástroje ochrany kyberprostoru při zachování minimální zátěže směrem k soukromoprávním subjektům.
- *Test potřebnosti* – provedenými studiemi nebylo zjištěno alternativní řešení, které by mohlo naplnit základní cíl záměru, tj. ochranu kyberprostoru České republiky. Byť je většina poskytovatelů služeb elektronických komunikací pozitivně motivována k účasti na zajištění kybernetické bezpečnosti státu prostřednictvím ekonomických motivů (jen fungující síť může generovat ekonomický efekt), je třeba formou zákonných povinností zajistit i pokrytí těch subjektů, které, ať už z neznalosti, neschopnosti nebo úmyslně, zanedbávají ochranu vlastní infrastruktury a ohrožují tak bezpečnost českého kyberprostoru jako celku – to s důrazem na subjekty, jejichž infrastruktura je pro stát kriticky důležitá.

- *Test poměrnosti* – Zásah do vlastnického práva je co do své intenzity ve zřejmém nepoměru s rizikem zásahu do distributivních i nedistributivních práv, k jejichž ochraně zákon vzniká. Povinnost oznamovat výskyt kybernetických bezpečnostních incidentů respektive povinnost aplikovat bezpečnostní opatření a realizovat případné bezpečnostní pokyny tak zdaleka nedosahují intenzity rizik ekonomických ztrát, společenských otřesů či ztráty mezinárodní důvěryhodnosti České republiky. Co do své intenzity jeví se v tomto směru mnohem závažnějšími příkladně i jen obdobné zásahy do vlastnického práva resp. práva svobodně podnikat např. na úseku požární ochrany. Navrhovaná úprava přitom nezasahuje do žádných informačních práv, tj. do jednotlivých komponent práva na informační sebeurčení. Povinnosti zamýšlené tímto zákonem jsou tedy plně odůvodněny chráněnými zájmy a omezují své adresáty jen v nezbytně nutné míře. Lze tedy konstatovat, že navrhovaná úprava je poměrná.

Vzhledem k tomu, že záměr, jak uvedeno shora, přináší jen minimum povinností soukromoprávním subjektům, nezatěžuje nikterak jejich právo na informační sebeurčení (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.

19. Zhodnocení souladu navrhované právní úpravy s mezinárodními smlouvami jimiž je Česká republika vázána, její slučitelnosti s předpisy Evropské unie

Problematika kybernetické bezpečnosti není komplexně řešena mezinárodním právem ani právem EU. Existuje zde celá řada mezinárodních dokumentů upravujících oblast kybernetické bezpečnosti, problematiku služeb elektronických komunikací, oblast kritické infrastruktury a oblast ochrany soukromí v odvětví elektronických komunikací. Návrh věcného záměru zákona o kybernetické bezpečnosti je plně v souladu s dosud uzavřenými mezinárodními smlouvami upravujícími shora uvedenou problematiku.

Jedná se zejména o Listinu základních práv Evropské unie, dále o směrnici Evropského parlamentu a Rady č. 98/34/ES o postupu při poskytování informací v oblasti norem a technických předpisů, ve znění směrnice 98/48/ES, směrnici č.

1999/5/ES o rádiových zařízeních a telekomunikačních koncových zařízeních a vzájemném uznávání jejich shody, č. 2000/31/ES o některých právních aspektech služeb informační společnosti, zejména elektronického obchodu, na vnitřním trhu (směrnice o elektronickém obchodu), směrnici č. 2002/19/ES o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení (přístupová směrnice), ve znění směrnice 2009/140/ES, směrnici č. 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací (autorizační směrnice), ve znění směrnice 2009/140/ES, směrnici č. 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací (rámcová směrnice), ve znění směrnice 2009/140/ES, směrnici č. 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací (směrnice o univerzální službě), ve znění směrnice 2009/136/ES, směrnici č. 2002/58/ES o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací, směrnici č. 2006/24/ES o uchovávání údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí a směrnici č. 2008/114/ES o určování a označování evropských kritických infrastruktur a o posouzení potřeby zvýšit jejich ochranu. Na poli práva Evropské unie se dále jedná o nařízení Evropského parlamentu a Rady č. 460/2004/ES o zřízení Evropské agentury pro bezpečnost sítí a informací ve znění nařízení č. 1007/2008 a o nařízení č. 1077/2011/ES kterým se zřizuje Evropská agentura pro provozní řízení rozsáhlých informačních systémů v prostoru svobody, bezpečnosti a práva a dále o rozhodnutí a stanoviska Rady č. 92/242/EHS o bezpečnosti informačních systémů, č. 2002/465/JHA o společných vyšetřovacích týmech, č. 2002/C 43/02 o společném postoji a specifických činnostech v oblasti bezpečnosti sítí a informací, č. 2003/C48/01 o evropském postoji vůči kultuře bezpečnosti sítí a informací, č. 2005/222/SVV o útocích proti informačním systémům, č. 2009/C62/05 o společné pracovní strategii a konkrétních opatřeních v oblasti boje proti počítačové trestné činnosti, č. 2009/C321/01 o společném evropském přístupu k bezpečnosti sítí a informací, č. 2011/292/EU o bezpečnostních pravidlech na ochranu utajovaných informací EU.

Danou oblast dále upravují dokumenty Rady Evropy, a to konkrétně 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.

Mezi další dokumenty mezinárodních organizací, které upravují oblast kybernetické bezpečnosti a související otázky, patří Akční plán Evropské unie pro boj s terorismem (INI/2004/2214); Evropský parlament, Bezpečnost informačních systémů a sítí: Směrem ke kultuře bezpečnosti; 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 a Akční plán zemí G8 pro potírání „high-tech" zločinu.

Návrh věcného záměru zákona o kybernetické bezpečnosti je plně v souladu s mezinárodními smlouvami, jimiž je Česká republika vázána, a je plně slučitelný s předpisy EU.

20. Předpokládaný hospodářský a finanční dopad navrhované právní úpravy, zejména nároky na státní rozpočet, ostatní veřejné rozpočty, na podnikatelské prostředí České republiky, sociální dopady a dopady na životní prostředí.

Návrh věcného záměru zákona o kybernetické bezpečnosti bude mít dopad na státní rozpočet, neboť v souvislosti se vznikem Národního centra kybernetické bezpečnosti dojde k navýšení funkčních míst, jakož i k navýšení rozpočtu Národního bezpečnostního úřadu. Vláda České republiky usnesením ze dne 19. října 2011 č. 781, o ustavení Národního bezpečnostního úřadu gestorem problematiky kybernetické bezpečnosti a národní autoritou pro tuto oblast, schválila převod 1 funkčního místa a příslušných mzdových a souvisejících výdajů z Ministerstva vnitra na Národní bezpečnostní úřad v roce 2011 a převod finančních prostředků ve výši 500 tis. Kč z kapitoly Ministerstva vnitra do kapitoly Národního bezpečnostního úřadu v roce 2011. V tomto usnesení vlády rovněž došlo ke schválení navýšení 8 funkčních míst v roce 2012, 10 funkčních míst v roce 2013, 10 funkčních míst v roce 2014 a 5 funkčních míst v roce 2015 Národního bezpečnostního úřadu a k navýšení rozpočtu Národního bezpečnostního úřadu pro zajištění činnosti Národního centra kybernetické bezpečnosti o 51,5 mil. Kč v roce 2012, o 61 mil. Kč v roce 2013, o 61 mil. Kč v roce 2014 a o 65 mil. Kč v roce 2015.

Předpokládá se, že návrh věcného záměru zákona bude mít další dopad na státní rozpočet i na ostatní veřejné rozpočty a podnikatelské prostředí, a to zejména s ohledem na stanovení nových povinností poskytovatelům služeb elektronických komunikací a provozovatelům sítí elektronických komunikací, správcům systémů kritické komunikační infrastruktury, správcům informačních systémů zařazených do kritické informační infrastruktury a správcům informačních systémů veřejné správy, avšak vzniklé náklady nebudou významné. Návrh vychází z premisy, že dotčené subjekty již uvažovaná bezpečnostní opatření používají a náklady tak lze spatřovat zejména v jejich sladění s technologiemi, které budou používat dohledová pracoviště.

Návrh věcného záměru zákona o kybernetické bezpečnosti nepřinese žádné negativní sociální dopady ani dopady na životní prostředí a nemá dopady na rovnost žen a mužů.