V l á d n í n á v r h

ZÁKON

ze dne …… 2014

o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ

KYBERNETICKÁ BEZPEČNOST

Hlava I
Základní ustanovení

§ 1

Předmět úpravy

(1) Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti.

(2) Tento zákon se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

Vymezení pojmů

§ 2

V tomto zákoně se rozumí

a) kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací[1)],
b) kritickou informační infrastrukturou prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy[2)] v oblasti kybernetické bezpečnosti,
c) bezpečností informací zajištění důvěrnosti, integrity a dostupnosti informací,
d) významným informačním systémem informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci,
e) správcem informačního systému orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního systému,
f) správcem komunikačního systému orgán nebo osoba, které určují účel komunikačního systému a podmínky jeho provozování a

---

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

2) § 2 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), ve znění pozdějších předpisů.
Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

g) významnou sítí síť elektronických komunikací[1)] zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře.

§ 3

Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací[1)], pokud není orgánem nebo osobou podle písmene b),
b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d),
c) správce informačního systému kritické informační infrastruktury,
d) správce komunikačního systému kritické informační infrastruktury a
e) správce významného informačního systému.

Hlava II
Systém zajištění kybernetické bezpečnosti

Bezpečnostní opatření

§ 4

(1) Bezpečnostním opatřením se rozumí souhrn úkonů, jejichž cílem je zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí elektronických komunikací[1)] v kybernetickém prostoru.

(2) Orgány a osoby uvedené v § 3 písm. c) až e) jsou povinny v rozsahu nezbytném pro zajištění kybernetické bezpečnosti zavést a provádět bezpečnostní opatření pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém a vést o nich bezpečnostní dokumentaci.

§ 5

(1) Bezpečnostními opatřeními jsou

a) organizační opatření a
b) technická opatření.

(2) Organizačními opatřeními jsou

a) systém řízení bezpečnosti informací,
b) řízení rizik,
c) bezpečnostní politika,
d) organizační bezpečnost,
e) stanovení bezpečnostních požadavků pro dodavatele,
f) řízení aktiv,
g) bezpečnost lidských zdrojů,
h) řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,
i) řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému,
j) akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,

k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
l) řízení kontinuity činností a
m) kontrola a audit kritické informační infrastruktury a významných informačních systémů.

(3) Technickými opatřeními jsou

a) fyzická bezpečnost,
b) nástroj pro ochranu integrity komunikačních sítí,
c) nástroj pro ověřování identity uživatelů,
d) nástroj pro řízení přístupových oprávnění,
e) nástroj pro ochranu před škodlivým kódem,
f) nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,
g) nástroj pro detekci kybernetických bezpečnostních událostí,
h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,
i) aplikační bezpečnost,
j) kryptografické prostředky,
k) nástroj pro zajišťování úrovně dostupnosti informací a
l) bezpečnost průmyslových a řídících systémů.

§ 6

Prováděcí právní předpis stanoví

a) obsah bezpečnostních opatření,
b) obsah a strukturu bezpečnostní dokumentace,
c) rozsah bezpečnostních opatření pro orgány a osoby uvedené v § 3 písm. c) až e) a
d) významné informační systémy a jejich určující kritéria.

Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident

§ 7

(1) Kybernetickou bezpečnostní událostí je událost, která může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací[1)].

(2) Kybernetickým bezpečnostním incidentem je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací[1)] v důsledku kybernetické bezpečnostní události.

(3) Orgány a osoby uvedené v § 3 písm. b) až e) jsou povinny detekovat kybernetické bezpečnostní události v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury nebo významném informačním systému.

§ 8

Hlášení kybernetického bezpečnostního incidentu

(1) Orgány a osoby uvedené v § 3 písm. b) až e) jsou povinny hlásit kybernetické bezpečnostní incidenty v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury nebo významném informačním systému, a to bezodkladně po jejich detekci; tím není dotčena informační povinnost podle jiného právního předpisu[3)].

(2) Orgány a osoby uvedené v § 3 písm. b) hlásí kybernetické bezpečnostní incidenty provozovateli národního CERT.

(3) Orgány a osoby uvedené v § 3 písm. c) až e) hlásí kybernetické bezpečnostní incidenty Národnímu bezpečnostnímu úřadu (dále jen „Úřad“).

(4) Prováděcí právní předpis stanoví

a) typy a kategorie kybernetických bezpečnostních incidentů a
b) náležitosti a způsob hlášení kybernetického bezpečnostního incidentu.

Evidence

§ 9

(1) Úřad vede evidenci kybernetických bezpečnostních incidentů (dále jen „evidence incidentů“), která obsahuje

a) hlášení kybernetického bezpečnostního incidentu,
b) identifikační údaje systému, ve kterém se kybernetický bezpečnostní incident vyskytl,
c) údaje o zdroji kybernetického bezpečnostního incidentu a
d) postup při řešení kybernetického bezpečnostního incidentu a jeho výsledek.

(2) Součástí evidence incidentů jsou údaje podle § 20 písm. f) až h).

(3) Úřad poskytuje údaje z evidence incidentů orgánům veřejné moci pro výkon jejich působnosti.

(4) Úřad může poskytovat údaje z evidence incidentů provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti v rozsahu nezbytném pro zajištění ochrany kybernetického prostoru.

§ 10

(1) Zaměstnanci České republiky zařazení k výkonu práce v Úřadu, kteří se podílejí na řešení kybernetického bezpečnostního incidentu, jsou vázáni povinností mlčenlivosti o údajích z evidence incidentů. Povinnost mlčenlivosti trvá i po skončení pracovněprávního vztahu k Úřadu.

(2) Ředitel Úřadu může osoby podle odstavce 1 zprostit povinnosti mlčenlivosti o údajích z evidence incidentů, s uvedením rozsahu údajů a rozsahu zproštění.

[3)] Například § 98 odst. 4 a § 99 odst. 4 zákona č. 127/2005 Sb., ve znění pozdějších předpisů.

§ 11

Opatření

(1) Opatřeními se rozumí úkony, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací[1)] před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu.

(2) Opatřeními jsou

a) varování,
b) reaktivní opatření a
c) ochranné opatření.

(3) Reaktivní opatření jsou povinny provádět

a) orgány a osoby uvedené v § 3 písm. a) a b) za stavu kybernetického nebezpečí nebo za nouzového stavu[4)] vyhlášeného na základě žádosti podle § 21 odst. 6 a
b) orgány a osoby uvedené v § 3 písm. c) až e).

(4) Ochranné opatření jsou povinny provádět orgány a osoby uvedené v § 3 písm. c) až e).

§ 12

Varování

(1) Úřad vydá varování, dozví-li se zejména z vlastní činnosti nebo z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o hrozbě v oblasti kybernetické bezpečnosti.

(2) Varování Úřad zveřejní na svých internetových stránkách a oznámí je orgánům a osobám uvedeným v § 3, jejichž kontaktní údaje jsou vedeny v evidenci podle § 16 odst. 4.

Reaktivní a ochranné opatření

§ 13

(1) Úřad vydá rozhodnutí, ve kterém uloží provést reaktivní opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací[1)] před kybernetickým bezpečnostním incidentem, které je prvním úkonem ve věci. Nepodaří-li se rozhodnutí adresátovi doručit do vlastních rukou do 3 dnů ode dne jeho vydání, doručí se mu tak, že se vyvěsí se na úřední desce Úřadu a tímto okamžikem je vykonatelné. Rozhodnutí podle věty první může Úřad vydat i v řízení na místě podle správního řádu.

(2) Rozklad podaný proti rozhodnutí podle odstavce 1 nemá odkladný účinek.

(3) Má-li se reaktivní opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací[1)] před kybernetickým bezpečnostním incidentem týkat blíže neurčeného okruhu orgánů nebo osob, vydá je Úřad formou opatření obecné povahy.

(4) Orgány a osoby uvedené v § 3 jsou povinny bez zbytečného odkladu oznámit Úřadu provedení reaktivního opatření a jeho výsledek. Náležitosti oznámení stanoví prováděcí právní předpis.

[4)] Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.

§ 14

(1) Úřad uloží za účelem zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací[1)], na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu, provést ochranné opatření formou opatření obecné povahy.

(2) Opatřením obecné povahy Úřad orgánům a osobám uvedeným v § 3 písm. c) až e) stanoví způsob zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací[1)] a lhůtu k jeho provedení.

§ 15

(1) Opatření obecné povahy podle § 13 nebo 14 nabývá účinnosti okamžikem jeho vyvěšení na úřední desce Úřadu; ustanovení § 172 správního řádu se nepoužije. O vydání opatření obecné povahy Úřad rovněž vyrozumí orgány a osoby uvedené v § 3, jejichž kontaktní údaje jsou vedeny v evidenci podle § 16 odst. 4.

(2) Připomínky k opatření obecné povahy vydanému podle § 13 nebo 14 lze uplatnit ve lhůtě 30 dnů ode dne jeho vyvěšení na úřední desce Úřadu. Úřad může na základě uplatněných připomínek opatření obecné povahy změnit nebo zrušit.

§ 16

Kontaktní údaje

(1) Kontaktními údaji jsou

a) u právnické osoby obchodní firma nebo název, adresa sídla, identifikační číslo osoby nebo obdobné číslo přidělované v zahraničí,
b) u podnikající fyzické osoby obchodní firma nebo jméno včetně odlišujícího dodatku nebo dalšího označení, adresa sídla a identifikační číslo osoby,
c) u orgánu veřejné moci jeho název, adresa sídla, identifikační číslo osoby, bylo-li přiděleno a identifikátor orgánu veřejné moci, pokud mu není přiděleno identifikační číslo osoby,

a údaje o fyzické osobě, která je za orgán nebo osobu uvedené v § 3 oprávněna jednat ve věcech upravených tímto zákonem, a to jméno, příjmení, telefonní číslo a adresa elektronické pošty.

(2) Kontaktní údaje a jejich změny oznamují

a) orgány a osoby uvedené v § 3 písm. a) a b) provozovateli národního CERT a
b) orgány a osoby uvedené v § 3 písm. c) až e) Úřadu.

(3) Orgány a osoby uvedené v § 3 písm. c) až e) oznamují změny pouze těch údajů podle odstavce 1, které nejsou referenčními údaji vedenými v základních registrech, a to neprodleně.

(4) Úřad vede evidenci kontaktních údajů, která obsahuje údaje uvedené v odstavci 1.

(5) Úřad je za stavu kybernetického nebezpečí oprávněn vyžadovat kontaktní údaje shromážděné provozovatelem národního CERT podle odstavce 2 písm. a).

(6) Vzor oznámení kontaktních údajů a jeho formu stanoví prováděcí právní předpis.

§ 17

Národní CERT

(1) Národní CERT zajišťuje v rozsahu stanoveném tímto zákonem sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti.

(2) Provozovatel národního CERT

a) přijímá oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. a) a b) a tyto údaje eviduje a uchovává,
b) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. b) a tyto údaje eviduje, uchovává a chrání,
c) vyhodnocuje kybernetické bezpečnostní incidenty u orgánů a osob uvedených § 3 písm. b),
d) poskytuje orgánům a osobám uvedeným v § 3 písm. a) a b) metodickou podporu a pomoc,
e) působí jako kontaktní místo pro orgány a osoby uvedené v § 3 písm. a) a b) a poskytuje těmto orgánům a osobám součinnost při výskytu kybernetického bezpečnostního incidentu,
f) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti,
g) předává Úřadu údaje o kybernetických bezpečnostních incidentech bez uvedení ohlašovatele kybernetického bezpečnostního incidentu a
h) předává na vyžádání Úřadu za stavu kybernetického nebezpečí kontaktní údaje orgánů a osob uvedených v § 3 písm. a) a b).

(3) Provozovatel národního CERT může vykonávat i další činnost v oblasti kybernetické bezpečnosti neupravenou tímto zákonem, pokud tato činnost nenaruší plnění povinností uvedených v odstavci 2.

(4) Provozovatel národního CERT při plnění povinností uvedených v odstavci 2 koordinuje svou činnost s Úřadem.

§ 18

Provozovatel národního CERT

(1) Provozovatelem národního CERT se může stát pouze právnická osoba,

a) která splňuje podmínky uvedené v odstavci 2 a
b) se kterou Úřad uzavřel veřejnoprávní smlouvu podle § 19.

(2) Provozovatelem národního CERT může být pouze právnická osoba, která

a) nevyvíjí ani nevyvíjela činnost proti zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací,
b) provozuje nebo spravuje informační systémy nebo služby a sítě elektronických komunikací[1)] anebo se na jejich provozu a správě podílí, a to nejméně po dobu 5 let,
c) má technické předpoklady v oblasti kybernetické bezpečnosti,
d) je členem nadnárodní organizace působící v oblasti kybernetické bezpečnosti,
e) nemá v evidenci daní u orgánů Finanční správy České republiky ani orgánů Celní správy České republiky ani v evidenci daní, pojistného na sociální zabezpečení a pojistného na veřejné zdravotní pojištění evidovány nedoplatky a
f) nebyla pravomocně odsouzena za spáchání trestného činu uvedeného v § 7 zákona o trestní odpovědnosti právnických osob a řízení proti nim.

(3) Zájemce prokazuje splnění podmínek předložením

a) čestného prohlášení v případě odstavce 2 písm. a) až d) a
b) potvrzení orgánu Finanční správy České republiky a Celní správy České republiky v případě odstavce 2 písm. e).

(4) Z obsahu čestného prohlášení podle odstavce 3 písm. a) musí být zřejmé, že uchazeč splňuje příslušné předpoklady. Potvrzení podle odstavce 3 písm. b), že uchazeč nemá v evidenci daní u orgánů Finanční správy České republiky ani orgánů Celní správy České republiky ani v evidenci daní, pojistného na sociální zabezpečení a pojistného na veřejné zdravotní pojištění nebo obdobných peněžitých plnění u příslušných orgánů státu, ve kterém má uchazeč sídlo, místo podnikání či bydliště, evidovány nedoplatky, nesmí být starší než 30 dnů. Za účelem prokázání podmínky uvedené v odstavci 2 písm. f) si Úřad vyžádá výpis z evidence Rejstříku trestů podle jiného právního předpisu[5)].

(5) Provozovatel národního CERT musí při plnění povinností uvedených v § 17 odst. 2 postupovat nestranně.

(6) Úřad zveřejní na svých internetových stránkách údaje o provozovateli národního CERT, a to jeho obchodní firmu nebo název, adresu sídla, identifikační číslo osoby, identifikátor datové schránky a adresu jeho internetových stránek.

§ 19

Veřejnoprávní smlouva

(1) Úřad uzavírá veřejnoprávní smlouvu (dále jen „smlouva“) s právnickou osobou vybranou postupem podle § 163 odst. 4 správního řádu za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění činností podle § 17 odst. 2. Řízení o výběru žádosti vyhlašuje Úřad.

(2) Smlouva obsahuje alespoň

a) označení smluvních stran,
b) vymezení předmětu smlouvy,
c) práva a povinnosti smluvních stran,
d) podmínky spolupráce smluvních stran,
e) způsob a podmínky odstoupení smluvních stran od smlouvy,
f) výpovědní lhůtu a výpovědní důvody,
g) zákaz zneužití údajů získaných v souvislosti s výkonem činností uvedených v § 17 odst. 2,
h) způsob financování činnosti národního CERT a
i) způsob předání a rozsah údajů předávaných Úřadu v případě zániku závazku.

(3) Smlouvu uzavřenou podle odstavce 1 Úřad zveřejňuje ve Věstníku Úřadu, s výjimkou těch částí smlouvy, jejichž zveřejnění neumožňuje jiný právní předpis.

(4) Není-li uzavřena smlouva podle odstavce 1, nebo v případě zániku závazku, vykonává činnost národního CERT Úřad.

[5)] Zákon č. 269/1994 Sb., o Rejstříku trestů, ve znění pozdějších předpisů.

§ 20

Vládní CERT

Vládní CERT jako součást Úřadu

a) přijímá oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. c) až e),
b) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. c) až e),
c) vyhodnocuje údaje o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech z kritické informační infrastruktury, z významných informačních systémů a dalších informačních systémů veřejné správy,
d) poskytuje orgánům a osobám uvedeným v § 3 písm. c) až e) metodickou podporu a pomoc,
e) poskytuje součinnost orgánům a osobám uvedeným v § 3 písm. c) až e) při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události,
f) přijímá podněty a údaje od orgánů a osob uvedených v § 3 a od jiných orgánů a osob a tyto podněty a údaje vyhodnocuje,
g) přijímá údaje od provozovatele národního CERT a tyto údaje vyhodnocuje,
h) přijímá údaje od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, a tyto údaje vyhodnocuje,
i) poskytuje podle § 9 odst. 4 provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraniční a jiným osobám působícím v oblasti kybernetické bezpečnosti údaje z evidence incidentů a
j) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti.

Hlava III

Stav kybernetického nebezpečí

§ 21

(1) Stavem kybernetického nebezpečí se rozumí stav, ve kterém je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost a integrita služeb nebo sítí elektronických komunikací[1)], a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky ve smyslu zákona upravujícího ochranu utajovaných informací.

(2) O vyhlášení stavu kybernetického nebezpečí rozhoduje ředitel Úřadu. Rozhodnutí o vyhlášení stavu kybernetického nebezpečí se vyhlašuje vyvěšením na úřední desce Úřadu. Informace o vyhlášení stavu kybernetického nebezpečí se zveřejňuje v celoplošném rozhlasovém a televizním vysílání. Provozovatel celoplošného televizního nebo rozhlasového vysílání je povinen bez náhrady nákladů na základě žádosti Úřadu neprodleně a bez úpravy obsahu a smyslu uveřejnit informace o vyhlášení stavu kybernetického nebezpečí.

(3) Rozhodnutí o vyhlášení stavu kybernetického nebezpečí nabývá účinnosti okamžikem, který se v rozhodnutí stanoví. Stav kybernetického nebezpečí se vyhlašuje na dobu nezbytně nutnou, nejdéle však na 7 dnů. Uvedenou dobu může ředitel Úřadu prodloužit; souhrnná doba trvání vyhlášeného stavu kybernetického nebezpečí nesmí být delší než 30 dnů.

(4) V průběhu vyhlášeného stavu kybernetického nebezpečí ředitel Úřadu informuje vládu o postupech při řešení stavu kybernetického nebezpečí a o aktuálním stavu hrozeb, které vedly k vyhlášení stavu kybernetického nebezpečí. Za stavu kybernetického nebezpečí a

za nouzového stavu[4)] v případech podle odstavce 6 je Úřad oprávněn vydat rozhodnutí nebo opatření obecné povahy podle § 13 rovněž orgánům a osobám uvedeným v § 3 písm. a) a b).

(5) Stav kybernetického nebezpečí nelze vyhlásit v případě, kdy ohrožení bezpečnosti informací v informačních systémech nebo bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací[1)] lze odvrátit činností Úřadu podle tohoto zákona.

(6) Není-li možné odvrátit ohrožení bezpečnosti informací v informačních systémech nebo bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací[1)] v rámci stavu kybernetického nebezpečí, ředitel Úřadu neprodleně požádá vládu o vyhlášení nouzového stavu[4)]. Rozhodnutí a opatření obecné povahy vydaná Úřadem podle § 13 před vyhlášením nouzového stavu zůstávají v platnosti, pokud tato opatření nejsou v rozporu s krizovými opatřeními vyhlášenými vládou.

(7) Stav kybernetického nebezpečí končí uplynutím doby, na kterou byl vyhlášen, pokud ředitel Úřadu nerozhodne o jeho zrušení před uplynutím této doby, nebo vyhlášením nouzového stavu[4)].

Hlava IV
Výkon státní správy

§ 22

(1) Státní správu v oblasti kybernetické bezpečnosti vykonává Úřad, nestanoví-li zákon jinak.

(2) Úřad

a) stanoví bezpečnostní opatření,
b) vydává opatření,
c) zajišťuje činnost Národního centra kybernetické bezpečnosti,
d) vede evidence podle tohoto zákona,
e) ukládá pokuty za správní delikty podle tohoto zákona,
f) působí jako koordinační orgán ve stavu kybernetického nebezpečí,
g) spolupracuje s orgány a osobami, které působí v oblasti kybernetické bezpečnosti, zejména s veřejnoprávními korporacemi, výzkumnými a vývojovými pracovišti a s ostatními pracovišti typu CERT,
h) zajišťuje mezinárodní spolupráci,
i) sjednává a uzavírá smlouvy o mezinárodní spolupráci,
j) zajišťuje prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti,
k) zajišťuje výzkum a vývoj v oblasti kybernetické bezpečnosti,
l) uzavírá veřejnoprávní smlouvu s provozovatelem národního CERT,
m) zasílá podle krizového zákona Ministerstvu vnitra návrh prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jejichž provozovatelem je organizační složka státu,
n) určuje podle krizového zákona prvky kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, pokud nejde o prvky uvedené v písmeni m) a
o) plní další úkoly v oblasti kybernetické bezpečnosti stanovené tímto zákonem.

Hlava V

Kontrola, nápravná opatření a správní delikty

§ 23

Kontrola

(1) Úřad vykonává kontrolu v oblasti kybernetické bezpečnosti. Při výkonu kontroly Úřad zjišťuje, jak orgány a osoby uvedené v § 3 plní povinnosti stanovené tímto zákonem a rozhodnutími a opatřeními obecné povahy vydanými Úřadem, a dodržují prováděcí právní předpisy v oblasti kybernetické bezpečnosti.

(2) Úřad kontroluje, jak

a) orgány a osoby uvedené v § 3 písm. a) a b) plní povinnosti uložené Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13 za stavu kybernetického nebezpečí,
b) orgány a osoby uvedené v § 3 písm. c) až e) plní povinnosti stanovené v § 4 odst. 2, § 8 odst. 3 a § 16 odst. 2 písm. b) a povinnosti uložené Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13 nebo 14.

§ 24

Nápravná opatření

(1) Zjistí-li Úřad při kontrole nedostatky, uloží kontrolovanému orgánu nebo osobě, aby je ve stanovené lhůtě odstranila, popřípadě určí, jakým způsobem.

(2) Pokud je informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém pro zjištěné nedostatky bezprostředně ohrožen kybernetickým bezpečnostním incidentem, který jej může významně poškodit nebo zničit, může kontrolní orgán zakázat kontrolovanému orgánu nebo osobě používání tohoto systému anebo jeho části do doby, než bude zjištěný nedostatek odstraněn.

Správní delikty

§ 25

(1) Právnická osoba nebo podnikající fyzická osoba uvedené v § 3 písm. a) nebo b) se dopustí správního deliktu tím, že

a) nesplní za stavu kybernetického nebezpečí povinnost uloženou Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13, nebo
b) nesplní některou z povinností uloženou nápravným opatřením podle § 24.

(2) Právnická osoba nebo podnikající fyzická osoba uvedené v § 3 písm. c) až e) se dopustí správního deliktu tím, že

a) v rozporu s § 4 odst. 2 nezavede nebo neprovádí bezpečnostní opatření anebo nevede bezpečnostní dokumentaci,
b) neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 3,
c) nesplní povinnost uloženou Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13 nebo 14,
d) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 16 odst. 2 písm. b) nebo
e) nesplní některou z povinností uloženou nápravným opatřením podle § 24.

(3) Za správní delikt se uloží pokuta do

a) 100 000 Kč, jde-li o správní delikt podle odstavce 1 písm. a) nebo b) anebo odstavce 2 písm. a) až c) nebo e),
b) 10 000 Kč, jde-li o správní delikt podle odstavce 2 písm. d).

§ 26

(1) Fyzická osoba se dopustí přestupku tím, že poruší povinnost uvedenou v § 10 odst. 1.

(2) Za přestupek podle odstavce 1 se uloží pokuta do 50 000 Kč.

§ 27

(1) Právnická osoba za správní delikt neodpovídá, jestliže prokáže, že vynaložila veškeré úsilí, které bylo možno požadovat, aby porušení právní povinnosti zabránila.

(2) Odpovědnost právnické osoby za správní delikt zaniká, jestliže Úřad o něm nezahájil řízení do 1 roku ode dne, kdy se o něm dozvěděl, nejpozději však do 3 let ode dne, kdy byl správní delikt spáchán.

(3) Při určení výměry pokuty právnické osobě se přihlédne k závažnosti správního deliktu, zejména ke způsobu jeho spáchání a jeho následkům a k okolnostem, za nichž byl spáchán.

(4) Správní delikty podle tohoto zákona projednává Úřad.

(5) Na odpovědnost za jednání, k němuž došlo při podnikání fyzické osoby nebo v přímé souvislosti s ním, se vztahují ustanovení tohoto zákona o odpovědnosti a postihu právnické osoby.

(6) Pokuty vybírá Úřad. Příjem z pokut je příjmem státního rozpočtu

(7) Pokuta je splatná do 30 dnů ode dne nabytí právní moci rozhodnutí o jejím uložení.

Hlava VI
Závěrečná ustanovení

§ 28
Zmocňovací ustanovení

(1) Úřad a Ministerstvo vnitra stanoví vyhláškou významné informační systémy a jejich určující kritéria podle § 6 písm. d).

(2) Úřad stanoví vyhláškou

a) obsah a strukturu bezpečnostní dokumentace, obsah bezpečnostních opatření a rozsah bezpečnostních opatření podle § 6 písm. a) až c),
b) typy a kategorie kybernetických bezpečnostních incidentů a náležitosti a způsob hlášení kybernetického bezpečnostního incidentu podle § 8 odst. 4,
c) náležitosti oznámení o provedení reaktivního opatření a jeho výsledku podle § 13 odst. 4 a
d) vzor oznámení kontaktních údajů a jeho formu podle § 16 odst. 6.

Přechodná ustanovení

§ 29

(1) Orgány a osoby uvedené v § 3 písm. a) a b) oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne nabytí účinnosti tohoto zákona.

(2) Orgány a osoby uvedené v § 3 písm. b) začnou plnit povinnost stanovenou v § 8 odst. 1 a 2 nejpozději do 1 roku ode dne nabytí účinnosti tohoto zákona.

§ 30

Orgány a osoby uvedené v § 3 písm. c) a d)

a) oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou,
b) začnou plnit povinnost stanovenou v § 8 odst. 1 a 3 nejpozději do 1 roku ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou a
c) zavedou bezpečnostní opatření podle § 4 odst. 2 nejpozději do 1 roku ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou.

§ 31

Orgány a osoby uvedené v § 3 písm. e)

a) oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne naplnění určujících kritérií významného informačního systému jejich informačních systémů,
b) začnou plnit povinnost stanovenou v § 8 odst. 1 a 3 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému a
c) zavedou bezpečnostní opatření podle § 4 odst. 2 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému.

§ 32

Činnost národního CERT vykonává do doby, než nabude účinnosti veřejnoprávní smlouva uzavřená podle § 19 ten, kdo přede dnem nabytí účinnosti tohoto zákona vykonával činnost, kterou podle tohoto zákona vykonává národní CERT, nejdéle však do 2 let ode dne nabytí účinnosti tohoto zákona.

§ 33

Společná ustanovení

(1) Tento zákon se vztahuje pouze na takové informační nebo komunikační systémy zpravodajských služeb, které splňují podmínky pro určení kritické informační infrastruktury, a to v rozsahu § 12 a 16; ustanovení § 4 se na tyto systémy použije přiměřeně a Úřad je jako prvky kritické infrastruktury podle § 22 odst. 2 písm. m) nenavrhuje.

(2) Na informační systém Policie České republiky pro analytickou činnost v trestním řízení se tento zákon vztahuje pouze v rozsahu § 12 a 16; ustanovení § 4 se na tento systém použije přiměřeně. To neplatí, pokud je tento systém kritickou informační infrastrukturou.

ČÁST DRUHÁ

Změna zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti

§ 34

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění zákona č. 119/2007 Sb., zákona č. 177/2007 Sb., zákona č. 296/2007 Sb., zákona č. 32/2008 Sb., zákona č. 124/2008 Sb., zákona č. 126/2008 Sb., zákona č. 250/2008 Sb., zákona č. 41/2009 Sb., zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 255/2011 Sb., zákona č. 420/2011 Sb., zákona č. 458/2011 Sb., zákona č. 167/2012 Sb. a zákona č. 303/2013 Sb., se mění takto:

1. V § 145 se na konci odstavce 5 tečka nahrazuje čárkou a doplňuje se písmeno f), které zní:

   „f) na vyžádání zprávu o jednotlivých kybernetických bezpečnostních incidentech z kritické informační infrastruktury.“.

2. V § 146 odst. 1 se za slova „bezpečnostního řízení“ vkládají slova „nebo v rámci správního řízení o vydání opatření podle zákona o kybernetické bezpečnosti“.

3. V § 146 odst. 2 se za slova „podle tohoto zákona“ vkládají slova „nebo podle zákona o kybernetické bezpečnosti“.

ČÁST TŘETÍ

Změna zákona o elektronických komunikacích

§ 35

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění zákona č. 290/2005 Sb., zákona č. 361/2005 Sb., zákona č. 186/2006 Sb., zákona č. 235/2006 Sb., zákona č. 310/2006 Sb., zákona č. 110/2007 Sb., zákona č. 261/2007 Sb., zákona č. 304/2007 Sb., zákona č. 124/2008 Sb., zákona č. 177/2008 Sb., zákona č. 189/2008 Sb., zákona č. 247/2008 Sb., zákona č. 384/2008 Sb., zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 153/2010 Sb., nálezu Ústavního soudu, vyhlášeného pod č. 94/2011 Sb., zákona č. 137/2011

Sb., zákona č. 341/2011 Sb., zákona č. 375/2011 Sb., zákona č. 420/2011 Sb., zákona č. 457/2011 Sb., zákona č. 458/2011 Sb., zákona č. 468/2011 Sb., zákona č. 18/2012 Sb., zákona č. 19/2012 Sb., zákona č. 142/2012 Sb., zákona č. 167/2012 Sb., zákona č. 273/2012 Sb., zákona č. 214/2013 Sb. a zákona č. 303/2013 Sb., se mění takto:

1. V § 89 se doplňuje odstavec 4, který včetně poznámky pod čarou č. 62 zní:

„(4) Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinen na žádost účastníka bezplatně a ve formě umožňující další elektronické zpracování dat poskytnout mu provozní a lokalizační údaje, které má k dispozici na základě tohoto zákona, pokud je nemohl účastník pro poruchu na jeho zařízení v důsledku kybernetického bezpečnostního incidentu[62)] zachytit nebo uložit. Údaje podnikatel předá, je-li to technicky možné bezodkladně, nejpozději však do 3 dnů ode dne doručení žádosti nebo v případě probíhající komunikace ode dne jejího uskutečnění.

[62)] § 7 odst. 2 zákona č. …/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).“.

2. V § 118 odst. 14 písm. y) se slovo „nebo“ zrušuje.

3. V § 118 se na konci odstavce 14 tečka nahrazuje slovem „, nebo“ a doplňuje se písmeno ad), které zní:

„ad) v rozporu s § 89 odst. 4 neposkytne údaje, nebo je poskytne opožděně.“.

4. V § 118 odst. 22 písm. a) se slovo „nebo“ nahrazuje čárkou a na konci textu písmene se doplňují slova „nebo odstavce 14 písm. ad)“.

ČÁST ČTVRTÁ

Změna zákona o svobodném přístupu k informacím

§ 36

V § 11 odst. 4 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění zákona č. 61/2006 Sb., se na konci písmene e) tečka nahrazuje čárkou a doplňuje se písmeno f), které zní:

„f) údajích vedených v evidenci incidentů podle zákona o kybernetické bezpečnosti, ze kterých bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila nebo jejichž poskytnutí by ohrozilo účinnost reaktivního nebo ochranného opatření podle zákona o kybernetické bezpečnosti.“.

ČÁST PÁTÁ

Změna zákona o provozování rozhlasového a televizního vysílání

§ 37

V § 32 odst. 1 písm. k) zákona č. 231/2001 Sb., o provozování rozhlasového a televizního vysílání a o změně dalších zákonů, ve znění zákona č. 274/2003 Sb., se za slova „válečného stavu,“ vkládají slova „stavu kybernetického nebezpečí,“.

ČÁST ŠESTÁ

ÚČINNOST

§ 38

Tento zákon nabývá účinnosti dnem 1. ledna 2015.

Důvodová zpráva

A. Obecná část

I. Závěrečná zpráva z hodnocení dopadů regulace (RIA)

1. Důvod předložení a cíle

Usnesení vlády České republiky ze dne 30. května 2012 č. 382 k návrhu věcného záměru zákona o kybernetické bezpečnosti, kterým byl tento návrh věcného záměru zákona schválen a řediteli Národního bezpečnostního úřadu (dále jen „NBÚ“) bylo uloženo zpracovat na základě předmětného věcného záměru zákona a předložit vládě do 31. července 2013 návrh zákona o kybernetické bezpečnosti.

1.1 Název

Zákon o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

1.2 Definice problému a nezbytnost právní úpravy

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 nebo útoky na tyto technologie, které mají rozsáhlé dopady do činnosti subjektů, které s nimi pracují, a potencionálně mohou 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.
Evropská unie rovněž reflektuje narůstající potřebu zajištění ochrany kybernetického prostoru. Za tímto účelem byla vypracována Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor, kterou předložila Vysoká představitelka Evropské unie pro zahraniční věci a bezpečnostní politiku. Současně s tímto dokumentem Evropská komise předložila dne 7. 2. 2013 návrh směrnice Evropského parlamentu a Rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii.
Návrh směrnice vyžaduje, aby každý členský stát přijal národní strategii pro bezpečnost sítí a informací, jmenoval vnitrostátní orgán odpovědný za bezpečnost sítí a informačních systémů a zřídil skupinu pro reakci na počítačové hrozby, tzv. CERT (Computer emergency response team). Návrh dále požaduje, aby odpovědné vnitrostátní orgány spolupracovaly v rámci sítě umožňující bezpečnou a efektivní spolupráci včetně koordinované výměny informací, odhalování incidentů a reakcí na úrovni EU. Směrnice počítá s ukládáním povinností subjektům regulace, kterými budou orgány veřejné správy a tzv. hospodářské subjekty definované směrnicí[1)].
Podle návrhu výše uvedené směrnice budou členské státy povinny zajistit, aby jejich orgány veřejné správy a hospodářské subjekty přijaly vhodná technická a organizační opatření k řízení bezpečnosti rizik jejich sítí a informačních systémů. Tato opatření by přitom měla vycházet z norem, respektive specifikací týkajících se bezpečnosti sítí a informací, které budou uvedeny v seznamu norem vypracovaným Evropskou komisí. Návrh směrnice dále předpokládá, že orgány veřejné správy a hospodářské subjekty budou povinny oznamovat odpovědnému orgánu incidenty, které budou mít významný dopad na bezpečnost jimi poskytovaných základních služeb. Vnitrostátní odpovědný orgán by pak měl disponovat prováděcími a donucovacími pravomocemi spočívajícími zejména v oprávnění vydávat závazné pokyny orgánům veřejné správy a hospodářským subjektům a v oprávnění požadovat od těchto subjektů informace potřebné k posouzení bezpečnosti jejich sítí a informačních systémů.
Předmětný návrh směrnice byl předložen Evropskému Parlamentu a Radě dne 7. 2. 2013. Evropský parlament o předmětném návrhu dosud nejednal. První jednání na úrovni Rady k návrhu výše uvedené směrnice proběhlo 11. dubna 2013. S ohledem na obecnost návrhu předmětné směrnice lze proto předpokládat, že shora uvedené základní povinnosti členských států a regulovaných subjektů mohou doznat změn.
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

[1)] Hospodářským subjektem se pro účely směrnice rozumí poskytovatel služeb informační společnosti, na nichž závisí poskytování dalších služeb informační společnosti, jejichž demonstrativní výčet je uveden v příloze II směrnice nebo provozovatel kritické infrastruktury, která má zásadní význam pro zachování životně důležitých ekonomických a společenských činností v oblasti energetiky, dopravy, bankovnictví, obchodování s cennými papíry a zdravotnictví, jejichž demonstrativní výčet je uveden v příloze II této směrnice.

kybernetického prostoru 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 kybernetického prostoru. Vznikem sociálních sítí, herních sítí a zájmových sítí se z nejznámější části kybernetického prostoru, z internetu, stává významný celospolečenský jev, jehož prostřednictvím lze společnost výrazně pozitivně nebo i negativně ovlivňovat.
V České republice se ochrana kybernetického prostoru řeší především prostřednictvím osob soukromého práva bez regulace, prostřednictvím partikulárních pracovišť.
Dále bylo na základě usnesení vlády č. 781 ze dne 19. října 2011 zřízeno Národní centrum kybernetické bezpečnosti jako součást NBÚ. Předmětné usnesení vlády uložilo řediteli NBÚ vybudovat do konce roku 2015 nejen plně funkční Národní centrum kybernetické bezpečnosti, ale i vládní koordinační místo pro okamžitou reakci na počítačové incidenty, tzv. vládní CERT, který bude součástí Národního centra kybernetické bezpečnosti, tj. součástí NBÚ. Soukromoprávní pracoviště často řeší případné útoky na informační technologie ad hoc. Proto je nezbytné, aby existovala pracoviště, která by útoky řešila z centralizované úrovně a následně by postiženým subjektům poskytovala kvalifikovaná doporučení. Poznatky o útocích, které již byly řešeny, pak mohou být následně poskytovány dalším postiženým subjektům. Tyto subjekty je tak nebudou muset řešit samostatně, čímž se sníží jejich náklady na odvracení a řešení kybernetických útoků.
Potřebu efektivní spolupráce mezi vládním CERT, soukromoprávními pracovišti řešící kybernetické útoky a postiženými subjekty potvrdily kybernetické útoky typu DDoS[2)] z počátku března letošního roku (4. – 7. 3. 2013). Předmětem těchto útoků byly zpravodajské servery, bankovní a finanční instituce, včetně České národní banky a Pražské burzy cenných papírů a internetové stránky některých mobilních operátů. Útoky směřovaly převážně na osoby soukromého práva, které pravděpodobně nebudou primárně podléhat regulaci návrhu zákona, a dále na informační systémy, z nichž pouze některé budou prvky kritické informační infrastruktury. NBÚ se společně se soukromoprávními pracovišti podílel na analýze tohoto útoku. V rámci zjišťování informací důležitých k rozboru DDoS útoku vyvstala potřeba spolupráce nejen s postiženými subjekty, ale i s poskytovateli služeb elektronických komunikací a se subjekty zajišťujícími sítě elektronických komunikací, kteří za trvajícího DDoS útoku jako jediní disponovali údaji o provozu napadeného serveru. Rozdílnými informacemi potřebnými k řešení kybernetického bezpečnostního incidentu tak disponovalo několik různých subjektů. Pro jeho řešení je přitom nezbytná rychlá a efektivní spolupráce, jakož i možnost sdílení potřebných údajů mezi NBÚ, soukromoprávními pracovišti řešícími kybernetické subjekty, subjekty postiženými kybernetickým útokem a poskytovateli služeb elektronických komunikací a subjektů zajišťující sítě elektronických komunikací. Mantinely této spolupráce pak musí být s ohledem na postavení NBÚ jakožto státního orgánu a charakter údajů předávaných mezi zainteresovanými subjekty upraveny zákonnou normou.
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

[2)] Útok typu DDoS (Distributed Denial of Service – distribuované odmítnutí služby) je technika útoku na internetové služby nebo stránky, při níž dochází k přehlcení požadavky a k pádu nebo nefunkčnosti a nedostupnosti systému pro ostatní uživatele, a to útokem mnoha koordinovaných útočníků.

elektronizací veřejné správy je hrozba kybernetických útoků stále aktuálnější a je zcela nezbytné přijmout opatření, která by státu umožňovala reagovat na tuto celospolečenskou hrozbu z centrální pozice, tak jak to odpovídá zahraničním zkušenostem se závažnými útoky. Osoby soukromého práva, které provozují systémy nebo technologie, které jsou důležité pro kritickou infrastrukturu, mají sice v převážné většině zavedeny bezpečnostní standardy, které vychází ze standardů ISO/IEC 20000 a ISO/IEC 27000, avšak ve vztahu k těmto subjektům stát v současné době nedisponuje žádnou pravomocí, v rámci níž by mohl přijmout opatření k odvracení kybernetických útoků.

Vzhledem k tomu, že státní moc lze uplatňovat výlučně na základě a v mezích zákona a soukromoprávním 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.

Nezbytnost právní úpravy je nutno řešit jednak vzhledem k materii společenské otázky, která je předmětem právní regulace, a dále pak vzhledem k nezbytnosti pokrytí této společenské otázky specifickou právní regulací. Je tedy třeba k odůvodnění navrhované právní úpravy odpovědět kladně na otázku, zda předmětný fenomén představuje aktuální společenský problém a rovněž je nutno odpovědět i na otázku, zda nestačí tento fenomén pokrýt stávajícími společenskými nástroji (tj. zda se společnost s tímto fenoménem nedokáže vypořádat bez regulatorního působení státu).

Ze shora uvedených vnějších a vnitřních důvodů pro regulaci fenoménu kybernetické bezpečnosti formou navrhované právní úpravy vyplývají tři základní problémové okruhy, jejichž řešení je na národní úrovni nezbytné, a to:

1) Ochrana existence a funkčnosti prostředí tvořeného informačními systémy a službami a sítěmi elektronických komunikací tak, aby v něm mohly subjekty pod jurisdikcí České republiky realizovat své právo na informační sebeurčení (k pojmu informačního sebeurčení viz část II., bod 1.2)
2) Ochrana existence a funkčnosti prostředí tvořeného informačními systémy a službami a sítěmi elektronických komunikací tak, aby kybernetické bezpečnostní incidenty nemohly ohrozit fungování základních společenských funkcionalit chráněných nedistributivními právy České republiky (k pojmu nedistributivních práv viz část II., bod 1.3)
3) Ochrana existence a funkčnosti prostředí tvořeného informačními systémy a službami a sítěmi elektronických komunikací tak, aby nebyla národní kybernetická infrastruktura zneužitelná k útokům mimo Českou republiku.

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

Při zajišťování kriticky důležitých společenských informačních funkcionalit nebo při zajišťování významných činností veřejné správy nelze spoléhat či pasivně čekat na to, že se všechny subjekty, jejichž činnost je pro fungování těchto systémů kriticky důležitá, vzájemně dohodnou na koordinovaném postupu nebo na jednotných pravidlech vzájemné spolupráce. Samoorganizační řešení spoléhající jen na aktivní prozíravost všech zúčastněných by totiž nikdy nebylo úplné a ve svém důsledku by tak mělo charakter provizoria do momentu, než

fakticky nastane bezpečnostní problém natolik závažný, aby všechny zúčastněné donutil aktivně spolupracovat (přičemž lze dokonce pochybovat o tom, že i pak by iniciativní řešení zahrnulo všechny rizikové faktory).

1.3 Popis existujícího právního stavu v oblasti kybernetické bezpečnosti

V současné době není problematika kybernetické bezpečnosti specificky řešena českým právním řádem. Dílčí aspekty ochrany České republiky před kybernetickými útoky jsou předmětem následujících právních předpisů, usnesení vlády a nadnárodních koncepčních dokumentů:

1.3.1 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.

1.3.2 Zákony

- Zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů,
- Zákon č. 240/2000 Sb., o krizovém řízení a změně některých zákonů, ve znění pozdějších předpisů,
- Zákon č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů,
- Zákon č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti), ve znění pozdějších předpisů,
- Zákon č. 127/2005 Sb., o elektronických komunikacích, ve znění pozdějších předpisů,
- Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů,
- Zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů,
- Zákon č. 40/2009 Sb., trestní zákoník, ve znění pozdějších předpisů,
- Zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů,
- Zákon č. 418/2011 Sb., o trestní odpovědnosti právnických osob a řízení proti nim.

1.3.3 Prováděcí předpisy

- Nařízení vlády č. 522/2005 Sb., kterým se stanoví seznamy utajovaných informací, ve znění nařízení vlády č. 240/2008 Sb.,
- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury,
- Vyhláška č. 523/2005 Sb., o bezpečnosti informačních a komunikačních systémů a dalších elektronických zařízení nakládajících s utajovanými informacemi a o certifikaci stínicích komor, ve znění vyhlášky č. 453/2011 Sb.,
- Vyhláška č. 529/2006 Sb., o požadavcích na strukturu a obsah informační koncepce a provozní dokumentace a o požadavcích na řízení bezpečnosti a kvality informačních

systémů veřejné správy (vyhláška o dlouhodobém řízení informačních systémů veřejné správy),
- Vyhláška 357/2012 Sb., o uchovávání, předávání a likvidaci provozních a lokalizačních údajů.

1.3.4 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,
- Usnesení vlády České republiky ze dne 23. května 2012 č. 364 o Strategii pro oblast kybernetické bezpečnosti České republiky na období let 2012 až 2015 a Akčním plánu opatření ke Strategii pro oblast kybernetické bezpečnosti České republiky na období let 2012 až 2015,
- Usnesení vlády České republiky ze dne 30. května 2012 č. 382 k návrhu věcného záměru zákona o kybernetické bezpečnosti.

1.3.5 Primární právo EU
- Listina základních práv Evropské unie.

1.3.6 Směrnice Evropského parlamentu a Rady
- 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),
- 2002/20/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,
- 2002/58/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.

1.3.7 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.

1.3.8 Rozhodnutí Rady

- 92/242/EHS o bezpečnosti informačních systémů,
- 2011/292/EU o bezpečnostních pravidlech na ochranu utajovaných informací EU.

1.3.9 Jiné dokumenty EU

- 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“.
- 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.

1.3.10 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.

1.3.11 Jiné 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.

1.3.12 Poziční a koncepční dokumenty veřejné správy České republiky

Vzhledem k tomu, že doposud v České republice chybí komplexní specifická úprava práv a povinností na úseku kybernetické bezpečnosti, byla potřeba ochrany České republiky před kybernetickými útoky doposud řešena zejména prostřednictvím následujících vládních koncepčních dokumentů, iniciativ soukromého a akademického sektoru a kooperativních aktivit technického charakteru s různou mírou zapojení státu:

Aktualizovaná koncepce boje proti organizovanému zločinu (2000)[3)]. Tento dokument uložil Ministerstvu vnitra mimo jiné „průběžně koncepčně řešit potírání organizovaných zločineckých aktivit v oblasti informačních technologií".

Koncepce boje proti trestné činnosti v oblasti informačních technologií (2001)[4)] 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 s dalšími organizačními celky a Policií České republiky za úkol mimo jiné:

- Zajistit podmínky pro další rozvoj (včetně materiálního a personálního posilování) struktur, přímo zapojených do potírání informační kriminality.

[3)] Usnesení vlády České republiky ze dne 23. října 2000 č. 1044 k Aktualizované Koncepci boje proti organizovanému zločinu.
[4)] Schválena ministrem vnitra dne 5. června 2001.

- 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.
- Vypracovat projekt hlásného systému pro trestnou činnost v oblasti informačních technologií.
- Iniciovat vznik a podporovat činnosti skupiny typu CERT 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.

Státní informační a komunikační politika e-Česko 2006 (2004)[5)] byla schválena v souvislosti s očekávaným vstupem České republiky do Evropské unie a za cíl si stanovila 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 vytvořeny další strategické dokumenty týkající se informačních systémů v České republice 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.

Národní strategie informační bezpečnosti České republiky (2005)[6)] 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

[5)] Připravena Ministerstvem informatiky a přijata usnesením vlády České republiky ze dne 24. března 2004 č. 265.
[6)] 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.

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.
- 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.

Akční plán realizace opatření Národní strategie informační bezpečnosti České republiky (2007)[7)] 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. Ustanovení národního centra 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.

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

Zřízení Meziresortní koordinační rady pro oblast kybernetické bezpečnosti (2010)[8]. 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,
- 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.

Memorandum o Computer Security Incident Response Team (CSIRT) České republiky se sdružením CZ.NIC (2010 a 2012)[9]. 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

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

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

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.
V roce 2012 nahradilo tento dokument nové dočasné Memorandum o CERT/CSIRT České republiky uzavřené mezi CZ.NIC a NBÚ s platností 1. 4. 2012 – 31. 12. 2012. Součástí memoranda je závazek CZ.NIC vykonávat funkce národního CERT/CSIRT týmu a rovněž plnit funkce vládního CERT týmu (to nejdéle do 31. 8. 2012). Fungování národního CERT/CSIRT na základě tohoto memoranda bylo ze strany NBÚ průběžně vyhodnocováno a získané zkušenosti budou využity při konstrukci a uzavírání veřejnoprávní smlouvy podle navrhované právní úpravy.
Toto dočasné memorandum bylo nahrazeno novým Memorandem o Computer Emergency Response Team/Computer Security Incident Response Team České republiky uzavřeným mezi CZ.NIC a NBÚ dne 12. 12. 2012. Memorandum nabylo účinnosti 1. 1. 2013 a platnosti pozbude 31. 12. 2015. Na základě tohoto memoranda bude sdružení CZ.NIC dále budovat a rozvíjet agendu národního „Computer Incident Security Response Team České republiky (CSIRT.CZ). CSIRT.CZ se bude jako národní tým podílet na řešení incidentů týkajících se kybernetické bezpečnosti v sítích provozovaných v České republice, bude poskytovat koordinační a metodickou pomoc při řešení incidentů a shromažďovat a vyhodnocovat data o oznámených incidentech. CSIRT.CZ bude rovněž působit jako národní Point of Contact pro oblast informačních technologií a jako centrum vzdělávání a šíření osvěty v oblasti kybernetické bezpečnosti. Při své činnosti by měl CSIRT.CZ úzce spolupracovat s NBÚ, respektive s vládním CERT, jakož i s dalšími CERT/CSIRT týmy na národní i mezinárodní úrovni.

Strategie pro oblast kybernetické bezpečnosti České republiky na období 2011 – 2015 (2011)[10)] 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

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

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.

Přechod gesce nad kybernetickou bezpečností na NBÚ a zřízení Rady pro kybernetickou bezpečnost (2011)[11]. 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 (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 NBÚ 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.

Schválení Věcného záměru zákona o kybernetické bezpečnosti (2012). NBÚ vypracoval v souladu s úkolem uloženým usnesením vlády ze dne 19. října 2011 č. 781 o ustanovení NBÚ gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast věcný záměr zákona o kybernetické bezpečnosti. Vláda České republiky schválila předložený věcný záměr zákona o kybernetické bezpečnosti dne 30. května 2012 svým usnesením č. 382 a současně uložila řediteli NBÚ zpracovat zákon o kybernetické bezpečnosti a předložit jej vládě do konce července 2013.

1.3.13 Zhodnocení současného právního stavu v oblasti kybernetické bezpečnosti v České republice

Jak plyne z výše uvedeného, je navrhovaná právní úprava první komplexní zákonnou úpravou reagující na objektivně existující potřebu zabezpečení České republiky a jejích národních zájmů před kybernetickými bezpečnostními incidenty. Aktuálně platná úprava totiž sice řeší některé aspekty kybernetické bezpečnosti, to však zpravidla formou specifických forem individuální odpovědnosti za informační delikty nebo formou certifikace zabezpečení informačních a komunikačních systémů nakládajících s utajovanými informacemi. Objektivní potřeba zabezpečení České republiky před kybernetickými bezpečnostními incidenty musela tedy, jak je uvedeno shora, mít doposud charakter užití soukromoprávních instrumentů, přičemž řadu zásadně důležitých funkcionalit nebylo možno kvůli absenci specifických zákonných povinností vůbec realizovat.

[11] 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.

1.4 Identifikace dotčených subjektů

Návrh zákona označuje dotčené subjekty jako orgány a osoby v oblasti kybernetické bezpečnosti (dále jen „orgány a osoby“). Vzhledem ke smyslu a účelu návrhu zákona, tj. k ochraně specifických informačních a komunikačních systémů před kybernetickými bezpečnostními incidenty, jakož i vzhledem k dominantní roli principu technologické neutrality (viz část II., kapitola 1.1) se zákon nedotýká uživatelů ani poskytovatelů obsahu ve službách informační společnosti. Orgány a osobami tak jsou v navrhované právní úpravě subjekty spravující specifické informační a komunikační systémy.

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

Navrhovaná právní úprava částečně přebírá definice subjektů z ostatních právních předpisů, a to zejména ze zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů a ze zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích). Nově jsou navrhovanou právní úpravou vytvořeny kategorie správců informačních a komunikačních systémů zařazených do kritické informační infrastruktury, správců významných informačních systémů a kategorie subjektů zajišťující významné sítě. Návrh zákona dále užívá dvou odlišných pojmů, a to služby a sítě elektronických komunikací a komunikační systémy. Pojem služby a sítě elektronických komunikací vychází ze zákona o elektronických komunikacích, zatímco pojem komunikační systémy v sobě zahrnuje jak tyto služby a sítě elektronických komunikací, tak i další, například neveřejné komunikační systémy.

Katalog povinností založených navrhovanou právní úpravou orgánům a osobám je uveden v tabulce níže:

Typ orgánu nebo osoby	**Základní povinnosti**	**Povinnosti – stav kybernetického nebezpečí**
Poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací	Hlásit kontaktní údaje národnímu CERT	Hlásit kontaktní údaje národnímu CERT, provádět reaktivní opatření vydaná NBÚ
Subjekty zajišťující významné sítě	Hlásit kontaktní údaje národnímu CERT, detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty národnímu CERT	Hlásit kontaktní údaje národnímu CERT, detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty národnímu CERT, provádět reaktivní opatření vydaná NBÚ
Správci významných informačních systémů	Hlásit kontaktní údaje NBÚ, zpracovávat bezpečnostní dokumentaci a zavádět	Hlásit kontaktní údaje NBÚ, zpracovávat bezpečnostní dokumentaci a zavádět

	bezpečnostní opatření, detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty NBÚ, provádět opatření vydaná NBÚ	bezpečnostní opatření, detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty NBÚ, provádět opatření vydaná NBÚ
Správci komunikačních Systémů zařazených do kritické informační infrastruktury	Hlásit kontaktní údaje NBÚ, zpracovávat bezpečnostní dokumentaci a zavádět bezpečnostní opatření, detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty NBÚ, provádět opatření vydaná NBÚ	Hlásit kontaktní údaje NBÚ, zpracovávat bezpečnostní dokumentaci a zavádět bezpečnostní opatření, detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty NBÚ, provádět opatření vydaná NBÚ
Správci informačních systémů zařazených do kritické informační infrastruktury	Hlásit kontaktní údaje NBÚ, zpracovávat bezpečnostní dokumentaci a zavádět bezpečnostní opatření, detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty NBÚ, provádět opatření vydaná NBÚ	Hlásit kontaktní údaje NBÚ, zpracovávat bezpečnostní dokumentaci a zavádět bezpečnostní opatření, detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty NBÚ, provádět opatření vydaná NBÚ

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

1.5 Popis cílového stavu

Cílovým stavem realizace navrhované právní úpravy je zajištění bezpečného fungování informační společnosti České republiky, tj. zajištění bezpečné realizace základního práva na informační sebeurčení prostřednictvím informačních systémů, služeb a sítí elektronických komunikací. Cílem navrhované právní úpravy je též ochrana nedistributivních práv státu, tj. zajištění veřejného zájmu na bezpečnosti kritické informační infrastruktury a významných informačních systémů.
Cílovým stavem je ve shora uvedeném smyslu fungující systém kybernetické bezpečnosti zahrnující:

- Bezpečnostní opatření
- Detekce kybernetických bezpečnostních událostí
- Hlášení kybernetických bezpečnostních incidentů
- Systém opatření k reakci na kybernetické bezpečnostní incidenty
- Činnost dohledových pracovišť (národní CERT a vládní CERT).

Jak plyne ze shora uvedeného a z principů v části II., není cílem navrhované právní úpravy obsah jednotlivých informačních transakcí. Navrhovaná právní úprava tedy nezasahuje do obsahového fungování informační společnosti, ale pouze si klade za cíl zabezpečit proti úmyslným nebo nahodilým kybernetickým bezpečnostním incidentům informační kanály, jimiž člověk realizuje své právo na informační sebeurčení a jimiž stát vykonává svá nedistributivní informační práva.
Cílem navrhované právní úpravy je především stanovit minimální požadavky na standardní zabezpečení kritické informační infrastruktury a významných informačních systémů a zajistit vládnímu dohledovému pracovišti v reálném čase přehled o kybernetické bezpečnostní situaci v kritické informační infrastruktuře a ve významných informačních systémech. Správcům kritické informační infrastruktury a významných informačních systémů zajistí navrhovaná právní úprava nepřetržitý kontakt s vládním dohledovým pracovištěm umožňující kvalitnější identifikaci kybernetických bezpečnostních rizik s původem mimo příslušný systém, službu nebo síť, efektivnější analýzu kybernetických bezpečnostních událostí a účinnější reakci na kybernetické bezpečnostní incidenty. Tato opatření bezprostředně povedou k řešení shora identifikovaného problému zabezpečení vitálních národních informačních funkcionalit, tj. k zabezpečení nejdůležitějších informačních systémů a zabezpečení nejdůležitějších služeb a sítí elektronických komunikací před kybernetickými bezpečnostními incidenty.
Ve vztahu k informačním a komunikačním systémům mimo shora uvedené vitálně důležité části zavádí navrhovaná právní úprava pouze povinnost oznamovat kontaktní údaje pro případ vyhlášení stavu kybernetického nebezpečí. Současně navrhovaná právní úprava počítá se spoluprací těchto subjektů se soukromoprávním národním dohledovým pracovištěm (národní CERT). Tyto subjekty tak budou moci využívat výhod vzájemné výměny informací o analýze kybernetických bezpečnostních událostí, o řešení kybernetických bezpečnostních incidentů, jakož i získávat metodickou podporu a pomoc odpovídající odborné úrovně. Cílem navrhované právní úpravy je tedy v tomto směru zvýšení bezpečnosti těchto informačních a komunikačních systémů prostřednictvím zajištění informačního a expertního servisu podporujícího přirozené snahy správců informačních systémů, podnikatelů v oboru elektronických komunikací a dalších subjektů po zvyšování bezpečnosti jejich vlastních systémů, sítí a služeb.

1.6 Zhodnocení rizika

1.6.1 Riziko nečinnosti

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. Nulová varianta by 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.

1.6.2 Technická a ekonomická náročnost zavádění bezpečnostních opatření u povinných osob

Orgány a osoby spravující kritickou informační infrastrukturu nebo významné informační systémy budou podle navrhované právní úpravy povinny zavádět bezpečnostní opatření, jejichž struktura je navržena v zákoně a obsah bude proveden v prováděcím právním předpise. Většina subjektů, které budou podle navrhované právní úpravy zavádět povinně bezpečnostní

opatření, již má řešenu vlastní kybernetickou bezpečnost na úrovni mezinárodních standardů ISO/IEC 20000 a ISO/IEC 27000. Vzhledem k tomu, že navrhovaná právní úprava z těchto standardů vychází, neměla by být adaptace na zákonné povinnosti v takových případech otázkou prakticky žádných dodatečných investic. U orgánů a osob, které se prokážou certifikací podle shora uvedených mezinárodních norem, se má za to, že splnily standardy bezpečnostních opatření podle zákona o kybernetické bezpečnosti. Tam, kde není u orgánů a osob s povinností zavádět bezpečnostní opatření dosud tato problematika řešena (což je vzhledem k důležitosti těchto systémů, služeb a sítí možno jednoznačně považovat za chybu na straně správce resp. poskytovatele), počítá navrhovaná právní úprava s přechodným obdobím.

1.6.3 Zneužití dat z evidence kybernetických bezpečnostních incidentů

Vládní CERT bude zpracovávat data o výskytu a řešení kybernetických bezpečnostních incidentů. Případný únik těchto dat by mohl ohrozit bezpečnostní zájmy České republiky nebo práva orgánů a osob. Součástí evidence kybernetických bezpečnostních incidentů budou údaje o zdroji kybernetického bezpečnostního incidentu, údaje z hlášení o kybernetickém bezpečnostním incidentu, včetně identifikačních údajů systému, ve kterém se kybernetický bezpečnostní incident vyskytl. Tato data budou chráněna povinností mlčenlivosti a jejich předávání bude možné jen v omezeném rozsahu na základě výslovného zákonného zmocnění k poskytování údajů.

Navrhovaná právní úprava je minimalistická co do struktury zpracovávaných dat o kybernetických bezpečnostních incidentech. Součástí evidence nebudou obsahové údaje z informačních systémů, sítí nebo služeb elektronických komunikací; pro potřeby národního a vládního CERT budou zpracovávána výlučně data o kybernetických bezpečnostních incidentech. Nejcitlivější z údajů tvořících evidenci kybernetických bezpečnostních incidentů budou statistická data o frekvenci útoků na jednotlivé systémy, sítě a služby elektronických komunikací a dále pak zejména data o způsobu řešení kybernetických bezpečnostních incidentů.

1.6.4 Neuzavření veřejnoprávní smlouvy s provozovatelem národního CERT

Zákon počítá s tím, že NBÚ uzavře veřejnoprávní smlouvu zajišťující provoz národního CERT soukromoprávním subjektem. Vzhledem k rigorózním požadavkům na uchazeče o uzavření takové smlouvy je možné, že se provozovatele národního CERT nepodaří vybrat. Navrhovaná právní úprava upravuje nouzovou variantu zajišťující fungování funkcionalit národního CERT po dobu do výběru soukromoprávního provozovatele tak, že funkce národního CERT bude dočasně vykonávat vládní CERT. Do doby výběru provozovatele národního CERT po účinnosti zákona o kybernetické bezpečnosti se předpokládá, že činnost národního CERT bude dočasně vykonávat soukromoprávní subjekt, který uzavřel s NBÚ smlouvu o spolupráci v oblasti kybernetické bezpečnosti.

1.6.5 Personální zajištění vládního CERT

Vzhledem k tomu, že specialistů na problematiku kybernetické bezpečnosti s náležitou kvalifikací a odpovídajícími zkušenostmi je v České republice v současné době nedostatek a vzhledem ke skutečnosti, že NBÚ má velmi omezené možnosti co do jejich náležitého finančního ohodnocení, lze očekávat personální problémy v počáteční fázi fungování vládního CERT. S cílem předejít těmto problémům NBÚ systematicky spolupracuje se špičkovými českými univerzitami a podporuje vznik specializovaných studijních oborů zaměřených na kybernetickou bezpečnost. Současně plánuje NBÚ prostřednictvím této spolupráce propagovat činnost vládního CERT a formou spolupráce na vzdělávacích a výzkumných aktivitách univerzit zapojovat do aktivit vládního CERT studenty a doktorandy.

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 incidentů 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 opatření. Služby informační společnosti se totiž vyznačují svým síťovým charakterem, přičemž i rozsahem nepatrný prvek sítě může závažným způsobem ovlivňovat její ostatní části, a to dokonce často i bez ohledu na geografickou blízkost.

2.1 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 kybernetické bezpečnosti otázkou dobrovolné koordinace dohledových a ochranných činností mezi jednotlivými správci informačních systémů nebo poskytovateli služeb elektronických komunikací resp. mezi subjekty zajišťujícími sítě elektronických komunikací. Platí přitom, že v podstatě každý správce informačního systému, 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 vybraných osob soukromého práva 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. Osoby soukromého práva a orgány veřejné moci 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 jeho odpovídající 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 osob soukromého práva 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 informačním a komunikačním systémům) a na odpovědnost státu vůči mezinárodnímu společenství (tj. o faktické porušení principu bdělosti – due dilligence) a odpovědnosti k zahraničním investorům v sektoru ICT. 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 informační a komunikační systémy, které nakládají s utajovanými informacemi. Partikulární ochrana pouze těchto systémů 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 a zajištěna relativně velmi dobrou úrovní technických standardů.
Utajované informace však představují v běžném životě informační společnosti jen jednu z mnoha kritických informačních agend. S rozvojem služeb informační společnosti a přesunem podstatné části společenského života do prostředí informačních technologií má pro současnou společnost kritický význam i celá řada dalších 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.
Přestože mají utajované informace důležité místo ve výkonu různých funkcí moderního státu, nelze rozhodně konstatovat, že by ochrana základního veřejného zájmu na fungování informačních a komunikačních systémů byla vyřešena zabezpečením systémů, které utajované informace zpracovávají. Řešení kybernetické bezpečnosti pouze v rámci věcné působnosti zákona č. 412/2005 Sb. by tedy bylo až příliš partikulární a v důsledku by nesplnilo svou funkci. Navrhovaná právní úprava by v takovém případě sice ošetřovala problematiku zabezpečení informační společnosti na národní úrovni, neposkytovala by však prakticky žádné prostředky k efektivnímu zajištění těch informačních funkcionalit, které jsou důležité nejen pro fungování státu, informační společnosti, ale i pro každého člověka.

2.3 Varianta ochrany veřejných informačních systémů

Varianta ochrany veřejných informačních systémů je založena na osobní působnosti pouze vůči správcům informačních systémů veřejné správy a dalších informačních systémů spravovaných orgány veřejné moci nebo jinými veřejnoprávními korporacemi. Výhodou této varianty by byl velmi omezený regulatorní efekt, přičemž by stát de facto zavazoval pouze sám sebe. Tato varianta by zřejmě nevyžadovala ani řešení formou zákonné úpravy, ale postačilo by technické řešení formou usnesení vlády.
Varianta ochrany veřejných informačních systémů by mohla být efektivní za předpokladu, že by kritická informační infrastruktura měla veřejnoprávní charakter. Ve skutečnosti však má část kritické informační infrastruktury soukromoprávní charakter a především kriticky důležité součásti veřejně dostupných služeb elektronických komunikací, na nichž životně závisí fungování informační společnosti, jsou vlastněny a provozovány osobami soukromého práva.

Tato situace samozřejmě nepředstavuje žádnou anomálii a ve své podstatě je pro rozvoj informační společnosti příznivá. Soukromý prospěch je v tomto směru ideálním motivačním faktorem k rozvoji systémů, sítí a služeb elektronických komunikací a situace, kdy jsou části kritické informační infrastruktury výhradně ovládány státem, je naopak běžná spíše ve státech s autoritářkou formou vlády. Není pak rovněž ničím zvláštním, pokud jsou soukromý systém, služba nebo síť pro fungování státu natolik důležité, že je jejich bezpečnost považována za důležitý národní zájem.
Z výše uvedeného plyne, že by řešení kybernetické bezpečnosti formou ochrany veřejných informačních systémů, tj. systémů spravovaných veřejnoprávními korporacemi, nepřineslo dostatečný efekt vzhledem ke smyslu a účelu navrhované právní úpravy. Partikulární ošetření informačních a komunikačních systémů spravovaných orgány veřejné moci by v důsledku vedlo pouze k ochraně veřejných informačních systémů, přičemž by nedošlo ke zkvalitnění v obecných otázkách zabezpečení možnosti výkonu práva na informační sebeurčení nebo ochrany zájmů státu na fungování informačních a komunikačních systémů, které nejsou státem vlastněny a provozovány.

2.4 Varianta obecné působnosti a spolupráce s osobami soukromého práva

Varianta řešení kybernetické bezpečnosti za účasti osob soukromého práva je postavena na předpokladu obecnosti. Zahrnuje tedy nejrůznější informační systémy, sítě a služby elektronických komunikací, které dohromady tvoří kybernetický prostor a jejichž bezpečnost implikuje stav kybernetické bezpečnosti státu.
Současně je tato varianta postavena na předpokladu, že podstatná část informačních a komunikačních systémů, 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 kybernetického prostoru má pro tyto osoby soukromého práva značný ekonomický význam, neboť jen fungující síť jim může generovat náležitý ekonomický efekt. Tyto osoby soukromého práva tedy aktivně investují do zabezpečení vlastní infrastruktury a mají ekonomicky motivovaný zájem podílet se na zajištění celkové kybernetické bezpečnosti.
Varianta spolupráce s osobami soukromého práva je konečně založena na předpokladu, že tyto osoby 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 příslušné osoby nebo má nad nimi příslušná osoba 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 osoby 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 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 založení 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 dalších práv správců informačních systémů a subjektů poskytujících služby respektive zajišťujících sítě elektronických komunikací, neboť by bylo třeba ošetřit bezprostřední možnost NBÚ přímo technicky zasahovat a ovlivňovat fungování informačních systémů, sítí a služeb elektronických komunikací.

Vedle značné regulatorní zátěže osob soukromého práva 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 informačních a komunikačních systémů, do nichž by bylo nutno instalovat 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.

3. Vyhodnocení nákladů a přínosů

3.1 Identifikace nákladů a přínosů

Ekonomické hodnocení přínosů jednotlivých variant představuje relativně obtížné zadání, neboť dominantní přínos, který je navrhovanou právní úpravou sledován, spočívá v eliminaci nebo omezení bezpečnostních rizik a posílení základních aspektů fungování informační společnosti. Tato rizika, tj. rizika plynoucí z kybernetických bezpečnostních incidentů, nemají dominantně ekonomický charakter, neboť spočívají v zajištění nedistributivních práv (veřejných statků), k jejichž ochraně je legitimován a povinen stát.

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

Informační a komunikační technologie se kromě výkonu veřejné správy významně podílejí též na fungování jiných společenských funkcionalit, z nichž některé mají pro život člověka a společnosti zásadní význam. Informační systémy, služby a sítě elektronických komunikací tedy zajišťují chod energetických sítí, zásobování obyvatelstva životně důležitými komoditami, fungování vitálně důležitých institucí např. v oborech ochrany veřejného zdraví, ochrany životního prostředí, dopravy. Přínosem sledovaným u shora popsaných variant tedy nesporně může být též zvýšení bezpečnosti kriticky důležitých společenských funkcionalit.

Právě uvedené samozřejmě neznamená, že by přínosy různých shora popsaných variant neměly vůbec ekonomický aspekt – pouze není vhodné předřazovat tyto ekonomické efekty před obecnější společenské přínosy. Mezi čistě ekonomické přínosy může v tomto směru

patřit snížení škodních následků kybernetických bezpečnostních incidentů, tj. snížení míry ekonomických škod, které tyto incidenty znamenají. Jako příklad tohoto typu přínosu lze uvést situaci, kdy z důvodu kybernetického bezpečnostního incidentu nefunguje nebo jen s omezením funguje např. e-shop nebo výměnný reklamní systém. Čím kvalitnější bude ochrana kybernetického prostoru před výskytem takového incidentu, tím může být útok méně intenzivní a tím rychleji též dochází k vyrovnání se s jeho následky. U služeb informační společnosti realizovaných v kybernetickém prostoru přitom platí, že kvůli jejich permanentnímu charakteru dochází k ekonomickým ztrátám vždy, pokud služba není pro své uživatele technicky dostupná.

Dalším ekonomickým efektem různých shora popsaných variant může být zvýšená míra motivace tuzemských a zahraničních investic do informačních a komunikačních technologií. Díky tomu, že v České republice působí špičková univerzitní a vědecká pracoviště, je zde realizována celá řada úspěšných investičních či inkubačních projektů zaměřených na pokročilé informační a komunikační technologie. Adekvátní zabezpečení kybernetického prostoru může v tomto směru posloužit k další motivaci investorů (zatímco opomenutí této agendy může naopak investory utvrzovat v názoru, že informační a komunikační technologie nepředstavují pro Českou republiku odpovídající prioritu).

V situaci, kdy se stát rozhodne aktivně přispět ke kybernetické bezpečnosti, je pak možno sledovat i další ekonomický přínos, a to nepřímou podporu tuzemských komerčních produktů v oblasti kybernetické bezpečnosti. Vedle toho, že stát má v takovém případě ideálně tendenci primárně využít domácích zdrojů a technologií a příslušnými veřejnými investicemi podporuje jejich tvůrce a investory, má užití těchto technologií i významný marketingový efekt. V bezpečnostních oborech totiž platí, že užití určité bezpečnostní technologie na tuzemském trhu jejího dodavatele je vnímáno jako důležitý předpoklad úspěchu této technologie v zahraničí. Stát, který se v oblasti kybernetické bezpečnosti buďto vůbec neangažuje nebo toto angažmá svěřuje zahraničním technologickým řešením, tedy vlastním vývojářům a investorům těchto technologií příliš nepomáhá.

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

Z právě uvedeného nepřímo plyne i další přínos, který je možno u shora popsaných variant sledovat a který se týká podpory konkurenceschopnosti tuzemských podniků působících na trhu služeb informační společnosti. Je-li v dnešní době běžné, že čeští podnikatelé oslovují prostřednictvím služeb informační společnosti zákazníky v zahraničí, je nasnadě, že bezpečné a fungující služby informační společnosti v rámci České republiky mají pro rozvoj takového podnikání pozitivní vliv. Státy s fungujícím systémem kybernetické bezpečnosti tedy mohou svým podnikatelům nabídnout v porovnání se státy, které tuto problematiku neřeší, bezpečnější prostředí nejen k realizaci tuzemských obchodů ale též k mezinárodní expanzi. Zcela banálně řečeno je totiž v mezinárodním obchodě zřejmě konkurenceschopnější podnikatel, kterému doma funguje e-mail a webové stránky.

Typologii přínosů sledovaných u jednotlivých shora popsaných variant lze tedy shrnout následovně:

- Zvýšení míry ochrany práva na informační sebeurčení, práva na svobodu projevu a dalších informačních práv člověka

- Zvýšení míry ochrany důvěry člověka ve stát a jeho instituce
- Zvýšení míry bezpečnosti kriticky důležitých společenských funkcionalit (tj. kritické informační infrastruktury)
- Omezení ekonomických škod jako důsledků kybernetických bezpečnostních incidentů
- Zvýšení atraktivity České republiky pro investory v oboru ICT
- Podpora českých dodavatelů bezpečnostních ICT technologií
- Obecné zvýšení atraktivity České republiky pro zahraniční a tuzemské investory
- Zvýšení konkurenceschopnosti tuzemských podnikatelů využívajících ICT k podnikání na evropském nebo mezinárodním trhu.

Náklady jednotlivých variant lze rozdělit podle jejich typu na pořízení respektive provoz příslušných bezpečnostních opatření a dále pak podle subjektů na veřejnoprávní a soukromoprávní sektor.

Náklady na pořízení bezpečnostních opatření se v závislosti na zvolené variantě mohou lišit rozsahem a typem akvizic techniky, jakož i mírou potřeby personálních výdajů, ať už jde o zařazení zcela nových profesí nebo o školení stávajícího rozsahu obslužného personálu. Následné náklady na provoz se pak rovněž v návaznosti na příslušné regulatorní variantě mohou lišit podle toho, zda je třeba pouze příslušné bezpečnostní opatření pořídit (a jeho provoz již pak je pouze otázkou jeho zapojení do systému a běžné údržby) nebo zda je nutno je průběžně financovat.

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

U variant, kde se počítá se zapojením státu, je rovněž možné v návaznosti na parametry příslušné regulatorní varianty počítat se zvláštními náklady na veřejnoprávní podporu výzkumu a vývoje bezpečnostních technologií a nástrojů, problematiky jejich používání, vývoje doporučených postupů aj., a to včetně podpory nebo jiné formy účasti na výzkumu v oborech informačních technologií, bezpečnostních studií, práva, sociologie, ergonomie, psychologie apod. S tím souvisí též kalkulace nákladů na osvětovou a vzdělávací činnost a nákladů na spolupráci s občanským, akademickým a neziskovým sektorem.

Typologii nákladů jednotlivých variant lze tedy shrnout následovně:

- Náklady na akvizici a provoz bezpečnostních opatření – soukromý sektor
- Náklady na akvizici a provoz bezpečnostních opatření – veřejný sektor
- Náklady na zřízení a provoz veřejnoprávního dohledového pracoviště
- Náklady na výzkum a vývoj v oblasti kybernetické bezpečnosti
- Náklady na preventivní činnost (vč. osvěty, vzdělávání).

3.2 Náklady

3.2.1 Nulová varianta (bez specifické právní regulace)

U této varianty je struktura předpokládaných nákladů následující:

- Náklady na akvizici a provoz bezpečnostních opatření – soukromý sektor – tyto náklady se realizují bez ohledu na zákonnou regulaci. Úspora spočívá v tom, že není nutno řešit náklady na hlášení kybernetických bezpečnostních incidentů centrálnímu dohledovému pracovišti.

- Náklady na akvizici a provoz bezpečnostních opatření – veřejný sektor - tyto náklady se realizují bez ohledu na zákonnou regulaci. Neexistence jednotné právní regulace této oblasti znamená různorodost řešení, které s sebou nese zvýšené náklady. Podle dosavadních zkušeností s budováním veřejných informačních systémů, kdy je velmi často problematika jejich zabezpečení podceněna nebo zcela opomenuta, lze očekávat, že by k založení povinnosti realizovat příslušné investice zřejmě muselo vzhledem k reálně existujícím bezpečnostním hrozbám a množícím se zkušenostem s kybernetickými bezpečnostními incidenty dojít.
- Náklady na zřízení a provoz veřejnoprávního dohledového pracoviště – vzhledem k absenci veřejnoprávního dohledového pracoviště v této variantě nebyly tyto náklady realizovány.
- Náklady na výzkum a vývoj v oblasti kybernetické bezpečnosti - vzhledem k absenci veřejnoprávního dohledového pracoviště v této variantě nebyly tyto náklady realizovány, resp. by se realizovaly na základě soukromých potřeb formou komerční činnosti.
- Náklady na preventivní činnost (vč. osvěty, vzdělávání) - vzhledem k absenci veřejnoprávního dohledového pracoviště v této variantě nebyly tyto náklady realizovány, resp. by se realizovaly na základě soukromých potřeb formou komerční činnosti.

K uvedenému výčtu je třeba na straně nákladů připočíst všechny výše označené negativní společenské dopady plynoucí ze skutečnosti, že stát rezignuje na řešení problému bezpečnosti informační a komunikační infrastruktury.

3.2.2 Varianta ochrany informačních systémů nakládajících s utajovanými informacemi

U této varianty je struktura předpokládaných nákladů následující:

- Náklady na akvizici a provoz bezpečnostních opatření – soukromý sektor – tyto náklady se u subjektů nakládajícími s utajovanými informacemi realizují na základě stávající úpravy zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Nad rámec těchto běžných nákladů by tato varianta přinesla potřebu investic představujících náklady na hlášení kybernetických bezpečnostních incidentů centrálnímu dohledovému pracovišti.
- Náklady na akvizici a provoz bezpečnostních opatření – veřejný sektor - tyto náklady se u subjektů nakládajícími s utajovanými informacemi realizují na základě stávající úpravy zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Nad rámec těchto běžných nákladů by tato varianta přinesla potřebu investic představující náklady na hlášení kybernetických bezpečnostních incidentů centrálnímu dohledovému pracovišti.
- Náklady na zřízení a provoz veřejnoprávního dohledového pracoviště – tato varianta počítá s náklady na zřízení centrálního dohledového pracoviště, tj. náklady na prostory a na technické a materiální vybavení. Oproti následujícím variantám by tyto náklady byly řádově nižší díky omezenému rozsahu činností dohledového pracoviště.
- Náklady na výzkum a vývoj v oblasti kybernetické bezpečnosti - vzhledem k tomu, že by veřejnoprávní dohledové pracoviště vykonávalo servis pouze pro systémy a sítě

zpracovávající utajované informace, byly by u této varianty náklady tohoto typu jen velmi omezené nebo žádné (obvykle by je nesly přímo povinné subjekty).

- Náklady na preventivní činnost (vč. osvěty, vzdělávání) - vzhledem k tomu, že by veřejnoprávní dohledové pracoviště vykonávalo servis pouze pro systémy a sítě zpracovávající utajované informace, byly by u této varianty náklady tohoto typu jen velmi omezené nebo žádné (obvykle by je nesly přímo povinné subjekty).

Podobně jako u předchozí varianty je třeba počítat s tím, že by náklady objevující se v důsledku aplikace této varianty zahrnovaly nejrůznější negativní dopady plynoucí z rezignace státu na ochranu kybernetického prostoru (ať už jde o náklady finanční či jiné).

3.2.3 Varianta ochrany veřejných informačních systémů

U této varianty je struktura předpokládaných nákladů následující:

- Náklady na akvizici a provoz bezpečnostních opatření – soukromý sektor – tyto náklady se realizují bez ohledu na zákonnou regulaci. Úspora spočívá v tom, že není nutno řešit náklady na hlášení kybernetických bezpečnostních incidentů centrálnímu dohledovému pracovišti.
- Náklady na akvizici a provoz bezpečnostních opatření – veřejný sektor – vzhledem k založení povinností k aplikaci bezpečnostních opatření, by tato varianta znamenala náklady na pořízení bezpečnostních opatření a jejich dokumentaci v souladu se zákonným standardem.
- Náklady na zřízení a provoz veřejnoprávního dohledového pracoviště – tato varianta počítá s náklady na zřízení centrálního dohledového pracoviště, tj. náklady na prostory a na technické a materiální vybavení. Oproti následujícím variantám by tyto náklady byly nižší díky omezenému rozsahu činností dohledového pracoviště pouze na veřejný sektor.
- Náklady na výzkum a vývoj v oblasti kybernetické bezpečnosti - vzhledem k tomu, že by veřejnoprávní dohledové pracoviště vykonávalo servis pouze pro systémy a sítě veřejnoprávních správců, byly by u této varianty náklady tohoto typu zaměřeny pouze do veřejného sektoru.
- Náklady na preventivní činnost (vč. osvěty, vzdělávání) - vzhledem k tomu, že by veřejnoprávní dohledové pracoviště vykonávalo servis pouze pro systémy a sítě veřejnoprávních správců, byly by u této varianty náklady tohoto typu zaměřeny pouze do veřejného sektoru.

K výše uvedenému je třeba doplnit, že by tato varianta neřešila ochranu dominantní soukromoprávní části kybernetického prostoru ani těch součástí kritické informační infrastruktury, které mají soukromé správce. Rovněž by touto variantou nebylo možno ošetřit kybernetické bezpečnostní incidenty velkého rozsahu, při nichž je třeba koordinovat činnost soukromoprávních i veřejnoprávní správců informačních a komunikačních systémů. Obojí by pak generovalo shora zmíněné náklady v rozsahu přímo závisejícím na aktuální bezpečnostní situaci.

3.2.4 Varianta obecné působnosti a spolupráce s osobami soukromého práva

U této varianty je struktura předpokládaných nákladů následující:

- Náklady na akvizici a provoz bezpečnostních opatření – soukromý sektor – vzhledem k založení povinností k aplikaci bezpečnostních opatření by tato varianta znamenala

náklady na pořízení bezpečnostních opatření a jejich dokumentaci v souladu se zákonným standardem pro malou skupinu osob soukromého práva. U většiny osob soukromého práva by však znamenala jen marginální nutnost investic, neboť bezpečnostně exponované osoby soukromého práva již příslušné investice realizovaly – jediné dodatečné náklady tedy ve většině případů souvisejí s napojením těchto opatření na dohledová pracoviště.

- Náklady na akvizici a provoz bezpečnostních opatření – veřejný sektor – vzhledem k založení povinností k aplikaci bezpečnostních opatření, by tato varianta znamenala náklady na pořízení bezpečnostních opatření a jejich dokumentaci v souladu se zákonným standardem.
- Náklady na zřízení a provoz veřejnoprávního dohledového pracoviště – tato varianta počítá s náklady na zřízení centrálního dohledového pracoviště, tj. náklady na prostory a na technické a materiální vybavení. Oproti následující variantě by tyto náklady byly nižší díky omezenému rozsahu činností dohledového pracoviště a spolupráci se soukromoprávním dohledovým pracovištěm.
- Náklady na výzkum a vývoj v oblasti kybernetické bezpečnosti - vzhledem k věcnému a osobnímu rozsahu této varianty by tento typ nákladů zahrnoval v omezené míře přímé náklady na výzkum a vývoj bezpečnostních nástrojů, standardních opatření, doporučených postupů apod. a dále pak náklady na podporu akademických a soukromých výzkumných a vývojových aktivit financovaných křížově nebo ze standardních grantových formátů. Část těchto nákladů by bylo možno realizovat též formou spoluúčasti na činnosti vládních institucí podporujících vědu a výzkum ve vybraných oborech.
- Náklady na preventivní činnost (vč. osvěty, vzdělávání) - vzhledem k věcnému a osobnímu rozsahu této varianty by tento typ nákladů zahrnoval v omezené míře přímé náklady na vzdělávání a preventivní osvětovou činnost (její součástí by byl např. provoz webových stránek veřejnoprávního dohledového pracoviště) a dále pak náklady na podporu konkrétních akademických a soukromých vzdělávacích a osvětových projektů.

3.2.5 Varianta obecné působnosti a přímé regulace

U této varianty je struktura předpokládaných nákladů následující:

- Náklady na akvizici a provoz bezpečnostních opatření – soukromý sektor – vzhledem k založení povinností k aplikaci bezpečnostních opatření, by tato varianta znamenala náklady na pořízení bezpečnostních opatření a jejich dokumentaci v souladu se zákonným standardem pro všechny osoby soukromého práva provozující informační a komunikační systémy. U většiny osob soukromého práva by však tato varianta znamenala nutnost rozsáhlých investic při zavedení bezpečnostních opatření v souladu se zákonným standardem a přímým napojením těchto systémů na dohledová pracoviště.
- Náklady na akvizici a provoz bezpečnostních opatření – veřejný sektor – vzhledem k založení povinností k aplikaci bezpečnostních opatření ve všech informačních systémech spravovaných orgány veřejné moci, by tato varianta znamenala enormní náklady na pořízení bezpečnostních opatření a jejich dokumentaci v souladu se

zákonným standardem a na přímé napojení příslušných systémů na dohledová pracoviště.

- Náklady na zřízení a provoz veřejnoprávního dohledového pracoviště – tato varianta počítá s náklady na zřízení centrálního dohledového pracoviště, tj. náklady na technické vybavení, náklady běžný provoz, náklady na administrativní servis apod. Oproti předchozím variantám by tyto náklady byly řádově vyšší, neboť dohledové pracoviště by muselo kompletně obsloužit bezpečnostní agendu v rámci věcné a osobní působnosti zákona.
- Náklady na výzkum a vývoj v oblasti kybernetické bezpečnosti - vzhledem k věcnému a osobnímu rozsahu této varianty by tento typ nákladů zahrnoval přímé náklady na výzkum a vývoj bezpečnostních nástrojů, standardních opatření, doporučených postupů apod. Oproti předchozí variantě by vzhledem k unikátní odpovědnosti státu za realizaci těchto aktivit nebylo možno spoléhat na finanční spoluúčast soukromého nebo akademického sektoru, resp. na externí zdroje projektového financování.
- Náklady na preventivní činnost (vč. osvěty, vzdělávání) - vzhledem k věcnému a osobnímu rozsahu této varianty by tento typ nákladů zahrnoval přímé náklady na vzdělávání a preventivní osvětovou činnost (její součástí by byl např. provoz webových stránek veřejnoprávního dohledového pracoviště) a dále pak náklady na veřejnoprávní vzdělávacích a osvětové projekty. Oproti předchozí variantě by vzhledem k unikátní odpovědnosti státu za realizaci těchto aktivit nebylo možno spoléhat na finanční spoluúčast soukromého nebo akademického sektoru, resp. na externí zdroje projektového financování.

K výše uvedenému rozpisu je třeba ještě doplnit hypotetickou úvahu ohledně nákladů státu generovaných předpokládanou neochotou podstatné části soukromého sektoru podrobit svou kybernetickou bezpečnost přímému státnímu dohledu. Tyto náklady by spočívaly v akvizici a provozu sankčního aparátu, který by s těžko odhadnutelnou mírou efektivity měl zajišťovat všeobecné plnění zákonných povinností.

3.3 Přínosy

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

Identifikovaný přínos	V1	V2	V3	V4	V5
Zvýšení míry ochrany práva na informační sebeurčení, práva na svobodu projevu a dalších informačních práv člověka	N	N	N	A	A
Zvýšení míry ochrany důvěry člověka ve stát a jeho instituce	N	N	N	A	Č
Zvýšení míry bezpečnosti kriticky důležitých společenských funkcionalit (tj. kritické informační infrastruktury)	N	Č	Č	A	A
Omezení ekonomických škod jako důsledků kybernetických bezpečnostních incidentů	N	N	Č	A	A
Zvýšení atraktivity České republiky pro investory v oboru ICT	N	N	N	A	Č
Podpora českých dodavatelů bezpečnostních ICT technologií	N	Č	A	A	A
Obecné zvýšení atraktivity České republiky pro zahraniční a tuzemské investory	N	N	Č	A	Č
Zvýšení konkurenceschopnosti tuzemských podnikatelů	N	N	Č	A	A

využívajících ICT k podnikání na evropském nebo mezinárodním trhu					

Legenda: V1 - Nulová varianta (bez specifické právní regulace)
V2 - Varianta ochrany informačních systémů nakládajících s utajovanými informacemi
V3 - Varianta ochrany veřejných informačních systémů
V4 - Varianta obecné působnosti a spolupráce s osobami soukromého práva
V5 - Varianta obecné působnosti a přímé regulace
A – ano, s tímto přínosem je u dané varianty možno počítat
N – ne, tento přínos se u dané varianty nepředpokládá
Č – tento přínos se u dané varianty předpokládá pouze zčásti, a to v závislosti na její věcné působnosti

K výše uvedenému je nutno doplnit vysvětlení skutečnosti, že míra investorské atraktivity by byla zvýšena při nasazení V5 pouze částečně (což platí pro atraktivitu pro investory obecně i pro investory v oboru ICT). Lze totiž předpokládat, že by na jedné straně sice investoři kladně hodnotili vyšší míru bezpečnosti zdejšího kybernetického prostoru, na druhé straně by mohla na některé investory negativně působit potřeba přímé spolupráce s veřejnoprávním dohledovým pracovištěm (tj. přímá kontrola státu nad zavedením a realizací bezpečnostních opatření).

3.4 Vyhodnocení nákladů a přínosů variant

Poměr nákladů a přínosu lze u jednotlivých variant zhodnotit následovně:

- Nulová varianta (bez specifické právní regulace) – tato varianta nepočítá s žádnými marginálními náklady ani jinými typy nákladů a předpokládá, že se kybernetický prostor, zjednodušeně řečeno, postará o svoji bezpečnost sám. Tato varianta tedy nepřináší žádné přínosy, které indukuje aktivní činnost státu (podpora právního vědomí, podpora investic apod.). Dynamika vývoje této varianty je jednoznačně negativní, což dokládá poslední vývoj kybernetické bezpečnostní situace v České republice (vedle kybernetického útoku z jara roku 2013 lze zmínit i mediálně nikoli zaznamenané ale přinejmenším stejně ekonomicky závažné útoky na vybrané e-shopy z podzimu 2012, útok na Českou poštu z podzimu 2011 aj.).
- Varianta ochrany informačních systémů nakládajících s utajovanými informacemi – tato varianta počítá jen s velmi částečným pozitivním efektem pro celkovou kybernetickou bezpečnostní situaci České republiky, neboť pokrývá jen nepatrný segment informačních a komunikačních systémů. Její potřebnost je navíc velmi diskutabilní, neboť bezpečnost těchto systémů je již řešena zákonem č. 412/2005 Sb. a stávající činností NBÚ.
- Varianta ochrany veřejných informačních systémů – tato varianta by již, jak plyne ze shora uvedené struktury nákladů a přínosů, částečně řešila ochranu veřejnoprávních informačních a komunikačních systémů a nesporně by vedla k částečnému vylepšení bezpečnostní situace České republiky v oblasti kybernetické bezpečnosti. Její zřejmou nevýhodou je opět základní premisa plynoucí z vlastnické analýzy kybernetického prostoru, tj. že podstatná část kybernetického prostoru nemá veřejnoprávní charakter, a to včetně funkcionalit zajišťujících vitální zájmy společnosti a státu.
- Varianta obecné působnosti a spolupráce s osobami soukromého práva – tato varianta generuje největší počet přínosů. Její nákladovost je omezena tím, že je funkčně

založena na spolupráci s osobami soukromého práva a striktní zákonné povinnosti ukládá jen v absolutně nezbytném rozsahu k dosažení jejího účelu. Struktura nákladů na plnění povinností předpokládaných navrhovanou variantou je dána strukturou základních ochranných institutů. Nákladovost u různých typů subjektů pak je dána jejich zařazením do zákonných kategorií. Náklady přímo související s aplikací varianty budou u podstatné části orgánů a osob minimální nebo nulové – tato varianta totiž zavádí takový standard bezpečnostních opatření, který podstatná část informačních systémů, služeb a sítí elektronických komunikací již dnes splňuje a správci těchto systémů a sítí, resp. poskytovatelé těchto služeb tak nebudou nuceni k žádným dodatečným investicím vyjma minimálních nákladů na hlášení kybernetických bezpečnostních incidentů dohledovým pracovištím.

Z výše uvedeného plyne, že náklady na straně orgánů a osob lze rozdělit na náklady související se zavedením bezpečnostních opatření, náklady související s detekcí kybernetických bezpečnostních událostí a s hlášením kybernetických bezpečnostních incidentů a náklady spojené s prováděním opatření. Úroveň výdajů spojených s povinností zavést bezpečnostní opatření v minimálním zákonném standardu se bude u orgánů a osob odvíjet od jejich zařazení do zákonných kategorií. U správců informačních a komunikačních systémů zařazených do kritické informační infrastruktury a u správců významných informačních systémů půjde o náklady související s plněním povinnosti aplikovat standardní úroveň bezpečnostních opatření, povinnosti detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty a povinnosti provádět opatření vydaná NBÚ.

U poskytovatelů služeb elektronických komunikací a subjektů zajišťujících sítě elektronických komunikací půjde bezprostředně pouze o náklady související s oznámením kontaktních údajů národnímu CERT (tyto náklady jsou prakticky bezvýznamné). U subjektů zajišťujících významné sítě půjde o náklady souvisejících s oznámením kontaktních údajů národnímu CERT, s povinností detekovat kybernetické bezpečnostní události a hlásit kybernetické bezpečnostní incidenty národnímu CERT.

Náklady související s přípravou na výskyt mimořádné situace, tj. stavu kybernetického nebezpečí, kdy budou mít tyto orgány a osoby povinnost reagovat na reaktivní opatření vydané NBÚ, lze u tohoto typu orgánů a osob jen velmi těžko předpokládat – je totiž zákonem ponecháno na jejich vlastním uvážení, jakým způsobem upraví svoji schopnost dostát za stavu kybernetického nebezpečí požadavkům opatření. Zákon v tomto směru nestanoví ani povinnost zpracovávat např. krizové plány a ponechává orgánům a osobám této kategorie prakticky úplnou volnost v rozhodování ohledně mimořádných postupů, což umožní v řadě případů snížit tyto marginální náklady na úplně minimum.

Navrhovaná varianta bude mít dále dopad na státní rozpočet, neboť v souvislosti se vznikem Národního centra kybernetické bezpečnosti, jehož součástí je vládní CERT, došlo a dojde k navýšení funkčních míst, jakož i k navýšení rozpočtu NBÚ. 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 NBÚ v roce 2011 a převod finančních prostředků ve výši 500 tis. Kč z kapitoly Ministerstva vnitra do kapitoly NBÚ 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 NBÚ a k navýšení rozpočtu NBÚ 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 tato varianta 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 komunikační infrastruktury zařazených do kritické informační 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 pokryjí z finančních prostředků vynakládaných na ICT. Dalším způsobem financování těchto nákladů je možné čerpáním finančních prostředků z fondů Evropské unie.
V souladu s usnesením vlády ze dne 28. listopadu 2012 č. 867, k přípravě programů spolufinancovaných z fondů Společného strategického rámce pro programové období let 2014 až 2020 v podmínkách České republiky, se v současné době zařazuje problematika kybernetické bezpečnosti do možností aktivit jednotlivých operačních programů u různých řídících orgánů. V květnu 2013 projednala vláda jednotlivé operační programy a přistoupí k návrhu Dohody o partnerství mezi Českou republikou a Evropskou komisí. Do konce měsíce října by měly být všechny operační programy finalizovány a měly by začít konkrétní rozhovory se zástupci Evropské komise nad již konkrétními body operačních programů.
Čerpání finančních prostředků ve Společném strategickém rámci by mělo dosahovat 85% podílu ze strany Evropské komise s 15 % účastí jednotlivých subjektů, i když v oblasti prioritní osy pro ICT by mohlo být stanoveno na podíl 50% - 50%. Po uzavření Dohody o partnerství by Česká republika měla do třech měsíců předložit prioritní osy jednotlivých dohodnutých operačních programů v definitivním znění.
V operačním programu Zaměstnanost, jehož řídícím orgánem je Ministerstvo práce a sociálních věcí, předkládá Ministerstvo vnitra na návrh NBÚ k zapracování popis problému a návrh aktivit a opatření v rámci Tematického cíle 11 Posilování institucionální kapacity a účinné veřejné správy pro investiční prioritu 4.1 v rámci prioritní osy 4 „Efektivní veřejná správa“. Čerpání z tohoto programu je pouze pro tzv. měkké aktivity, proto by umožňovalo zajistit kofinancování pro proškolování odborníků ICT jednotlivých budoucích orgánů a osob v rámci veřejné správy, a to jak jednorázově, tak v pravidelných cyklech, a umožňovalo by efektivnější odborné vazby k dohledovému pracovišti.
V rámci programu IROP v investiční prioritě 2 – „Zlepšení přístupu k ICT, využití kvality ICT, posilování aplikací v oblasti ICT určených pro elektronickou veřejnou správu, elektronické učení, elektronické začleňování a elektronické zdravotnictví“ předkládá Ministerstvo vnitra na návrh NBÚ k zapracování popis problémů a aktivit směřující k tomu, aby bylo umožněno čerpání finančních prostředků veřejné správě a složek Integrovaného záchranného systému pro zajištění příslušného technického vybavení pro splnění standardů požadovaných prováděcím předpisem a aby ke zvýšení efektivity odborných vazeb k dohledovému pracovišti došlo i v oblasti financování tzv. tvrdých aktivit.
Obdobně o zařazení problematiky kybernetické bezpečnosti jednal NBÚ s Ministerstvem školství, mládeže a tělovýchovy a s Ministerstvem práce a sociálních věcí, které zařadilo zástupce NBÚ do Pracovní skupiny pro programování, konkrétně do podskupiny, která se bude zabývat návrhy aktivit pro prioritní osu „Efektivní veřejná správa“.

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

- Varianta obecné působnosti a přímé regulace – tato varianta zajišťuje státu největší míru kontroly nad bezpečnostní situací v oblasti kybernetické bezpečnosti. Vedle vysokých nákladů na výkon zákonných pravomocí orgány veřejné moci je problematická též z hlediska definice rozsahu zákonných povinností a jejich svázáním s působností veřejnoprávního dohledového pracoviště. V situaci, kdy mezi osobami soukromého práva v sektoru ICT panuje určitá nedůvěra k fungování orgánů veřejné moci, by plná implementace této varianty kromě uvedených nákladů přinesla též riziko nikoli zcela důvodného zvýšení společenského napětí.

4. Návrh řešení

4.1 Stanovení pořadí variant a výběr nejvhodnějšího řešení

Shora uvedených pět základních variant řešení se vzájemně liší mírou resp. důkladností právní regulace a mírou ingerence státních orgánů. Analýza zahrnula též krajní varianty totální regulace resp. ponechání problematiky kybernetické bezpečnosti volnému vývoji.

K výběru nejvhodnějšího řešení dospěl navrhovatel především komplexní analýzou předpokládaných efektů jednotlivých variant řešení, a to z hlediska ústavní konformity resp. zatěžování jednotlivých subjektů novými typy povinností, z hlediska ekonomické a organizační výhodnosti a rovněž z hlediska objektivních technických možností informačních a komunikačních systémů. Výběr nejvhodnější varianty tedy není veden idealistickou touhou po dokonalém řešení nebo naivním spoléhání se na to, že problém kybernetické bezpečnosti zmizí stejně náhle, jako se objevil, ale pragmatickým zhodnocením potřeb a možností České republiky, jakož i aktuálního stavu vědění v oboru práva informačních a komunikačních technologií, informatiky a bezpečnostních studií.

Výběr nejvhodnějšího řešení vedle shora uvedených faktorů zohledňuje i vlastnictví a správu informačních a komunikačních systémů, přičemž jejich část je vlastněna a spravována osobami soukromého práva. Tyto osoby mají zpravidla velmi solidní zkušenosti s jejich provozováním a mají též odpovídající technické kompetence a faktické možnosti aktivně se starat o bezpečnost vlastních systémů, služeb a sítí. Řešení kybernetické bezpečnosti prostřednictvím specifických povinností adresovaných těmto osobám, resp. prostřednictvím spolupráce a vzájemné podpory těchto osob a státu se jeví jako ideální. Z tohoto důvodu je doporučenou variantou vybranou k legislativnímu řešení varianta obecné působnosti zákona a spolupráce s osobami soukromého práva.

Varianty partikulární věcné působnosti zákona je třeba z důvodu jejich nedostatečného věcného rozsahu vyloučit, neboť by při jistých nákladech nevedly k odpovídajícímu výslednému efektu. Problém kybernetické bezpečnosti má totiž z výše uvedených důvodů komplexní charakter a nemůže tak být logicky řešen partikulární právní regulací.

V pořadí smysluplných variant tedy z tohoto důvodu zůstává již pouze varianta obecné působnosti a přímé regulace. Přímá regulace bezpečnostních aspektů fungování informačních systémů a sítí a služeb elektronických komunikací by však byla jen velmi obtížně proveditelná z hlediska její ústavní konformity – zákonná omezení by se totiž z podstatné části týkala užívání soukromé informační a komunikační infrastruktury a nevyhnutně by se dotkla též práv a povinností koncových uživatelů. Z hlediska organizačního by si navíc tato

varianta vyžádala masivní veřejné investice do personálního aparátu, který by takovou regulaci implementoval, kontroloval a sankcionoval.

5. Implementace doporučené varianty a vynucování

Vzhledem k identickému objektu právní regulace a tím dané specifické věcné působnosti se jeví jako nejvhodnější variantou zajištění kybernetické bezpečnosti České republiky formou zvláštního zákona. Ten sice přebírá 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 souhrnně označeným jako orgány a osoby). S ohledem na smysl a účel regulace pak nelze kybernetickou bezpečnost podřadit pod jiný právní předpis.
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. U případů, u kterých je zřejmé, že by mohl být spáchán trestný čin, se bude postupovat podle jiných právních předpisů, zejména podle trestního řádu. Rovněž je nutno založit NBÚ možnost spolupráce s osobami soukromého práva 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 ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb a sítí elektronických komunikací, počítá navrhovaná právní úprava se zavedením zvláštního stavu - 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 s obecnou věcnou a osobní působností).
Struktura povinností se v navrhované právní úpravě vztahuje k osobám soukromého práva i orgánům veřejné moci, přičemž jejich základní rozlišení je podle typu informačního a komunikačního systému, kterou příslušný subjekt spravuje či zajišťuje. Kontrolní a sankční pravomoci jsou pak rozděleny následovně:

- Povinnost poskytovatelů služeb elektronických komunikací a subjektů zajišťujících sítě elektronických komunikací provádět opatření vydaná NBÚ ve stavu kybernetického nebezpečí: kontroluje a sankcionuje NBÚ.
- Povinnost subjektů zajišťujících významné sítě hlásit kybernetické bezpečnostní incidenty národnímu CERT a povinnost provádět opatření vydaná NBÚ ve stavu kybernetického nebezpečí: kontroluje a sankcionuje NBÚ,
- Povinnosti správců informačních a komunikačních systémů kritické informační infrastruktury zavádět a dokumentovat bezpečnostní opatření, oznamovat kontaktní údaje vládnímu CERT, hlásit kybernetické bezpečnostní incidenty vládnímu CERT a provádět opatření vydaná NBÚ: kontroluje a sankcionuje NBÚ.
- Povinnosti správců významných informačních systémů zavádět bezpečnostní opatření: kontroluje a sankcionuje MV. Povinnost správců významných informačních systémů provádět opatření vydaná NBÚ, oznamovat kontaktní údaje vládnímu CERT, hlásit kybernetické bezpečnostní incidenty vládnímu CERT: kontroluje a sankcionuje NBÚ.

Kontrolní kompetence jsou upraveny v návaznosti na kontrolní řád. Sankční aparát zahrnuje ukládání nápravných opatření a deliktní odpovědnost.

6. Přezkum účinnosti regulace

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

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

Ad 1. bude NBÚ prostřednictvím činností vládního CERT, spolupráce s národním CERT a mezinárodní spolupráce permanentně sledovat a vyhodnocovat situaci v oblasti kybernetické bezpečnosti a reagovat na zjištěné nedostatky a bezpečnostní hrozby. Dojde-li k situaci vyžadující okamžité přehodnocení kvality bezpečnostních opatření (např. dojde ke zjištění tzv. bezpečnostní díry v určité technologii nebo ke snížení důvěryhodnosti určitého bezpečnostního mechanismu), bude k jejímu řešení užito buďto opatření a následné změny prováděcích právních předpisů.
Ad 2. bude NBÚ pravidelně vyhodnocovat strukturu parametrů bezpečnostních opatření, a to zejména v návaznosti na vývoj průmyslových standardů a obecně akceptovaných doporučených postupů (best practices). V případě potřeby upravit parametry bezpečnostních opatření bude jako nástroje použito změny prováděcího právního předpisu, tj. vyhlášky NBÚ.
Ad 3. bude NBÚ provádět ve spolupráci s dotčenými rezorty, akademickými pracovišti a soukromým sektorem pravidelné hodnocení efektivity právní úpravy jako takové. Ukáže-li se, že některé zákonné povinnosti neplní dostatečně účel navrhované právní úpravy, bude iniciována příslušná změna právní úpravy. Skutečnost, že navrhovatel počítá s tím, že navrhovaná právní úprava může být v budoucnosti měněna a doplňována, však nelze vnímat jako nedostatek důvěry navrhovatele v její současnou kvalitu či jako důvod k pochybnostem o jejím aktuálním nastavení – potřeba změnit navrhovanou právní úpravu na zákonné úrovni může totiž být dána technickým vývojem a zejména pak výskytem nových typů kybernetických bezpečnostních incidentů, jejichž odpovídajícímu pokrytí nebude aktuálně navrhovaná struktura povinností dostačovat.

7. Konzultace a zdroje dat

Usnesením vlády ze dne 30. května 2012 č. 382 k návrhu věcného záměru zákona o kybernetické bezpečnosti byl věcný záměr zákona o kybernetické bezpečnosti schválen s tím, že bylo řediteli NBÚ uloženo vypracovat návrh zákona v termínu do konce července 2013. Na postulátech, které založil věcný záměr zákona o kybernetické bezpečnosti, tak bylo přistoupeno k tvorbě paragrafového znění zákona o kybernetické bezpečnosti. V rámci přípravy paragrafového znění bylo přistoupeno k široké prezentaci tezí, na kterých je právní regulace v oblasti kybernetické bezpečnosti postavena a k zapojení spektra subjektů orgánů veřejné moci a osob soukromého práva, se kterými byly zvolené teze a navržené postupy konzultovány.

7.1 Konference Brno

V rámci konzultací, kterých bylo využito při tvorbě návrhu zákona o kybernetické bezpečnosti, bylo uskutečněno ve dnech 20. a 21. září 2012 pracovní setkání s účastí celého spektra odborné veřejnosti, akademické sféry a zástupců veřejné správy. Toto setkání se uskutečnilo k prezentaci základní filosofie právní regulace v rámci konference „České právo a informační technologie 2012“ pořádané Ústavem práva a technologií Právnické fakulty Masarykovy univerzity v Brně. V rámci této konference byly představeny hlavní principy a instituty zákona o kybernetické bezpečnosti, k němuž následně proběhla plenární panelová diskuse. Odborná veřejnost přijala předložené principy zákona vstřícně, kdy diskuze směřovala hlavně k možnostem outsorcingu technologií a k dopadu regulace na takto přenesený výkon povinností.

7.2 Konzultace s akademickou sférou

Pro zajištění právní bezvadnosti zvolených řešení docházelo od července 2012 ke konzultacím s akademickou sférou, kde konzultovanými tématy byly vazby na správní řád, forma opatření na kybernetické bezpečnostní incidenty, podmínky pro výběr provozovatele národního CERT a prolomení povinnosti mlčenlivosti. Po konzultacích s akademickou sférou bylo upuštěno od snahy NBÚ reagovat na nastalý kybernetický bezpečnostní incident opatřením vydaným v režimu mimo rozhodování podle správního řádu anebo mimo opatření obecné povahy. Navržený institut opatření NBÚ, který by NBÚ dal možnost reagovat bezprostředně bez jisté svázanosti instituty správního řízení a který bylo možno přirovnat k opatření, jež umožňuje právní úprava v gesci ministerstva zdravotnictví a které bylo uplatněno v rámci opatření vydaných při metanolové aféře na sklonku roku 2012, byl jako nekonformní opuštěn a byl zvolen princip vydání opatření výlučně formou rozhodnutí podle správního řádu nebo ve formě opatření obecné povahy. V rámci snahy o efektivní možnost kontroly a o nezbytnou formalizaci došlo k inicializaci vytvoření povinnosti pro orgány a osoby, které budou muset aplikovat bezpečnostní opatření a o těchto bezpečnostních opatřeních vést bezpečnostní dokumentaci. Jako subjekt, vůči kterému budou směřovat povinnosti dané zákonem o kybernetické bezpečnosti, byl zvolen správce těchto systémů, a to z důvodu velké efektivity tohoto řešení. Odmítnuta byla myšlenka, že údaje z evidence kybernetických bezpečnostních incidentů by se měly předávat výhradně orgánům činným v trestním řízení.

7.3 Meziresortní pracovní skupina

V září 2012 byla vytvořena Meziresortní pracovní skupina k tvorbě paragrafového znění návrhu zákona o kybernetické bezpečnosti, jejímiž členy byly zástupci Ministerstva vnitra, Ministerstva obrany, Bezpečnostní informační služby, Úřadu pro zahraniční styky a informace, Českého telekomunikačního úřadu a Generálního ředitelství hasičského záchranného sboru, která se kontinuálně scházela k projednání otázek kybernetické bezpečnosti a s tím souvisejících aspektů, které promítla do jednotlivých verzí návrhu zákona o kybernetické bezpečnosti. Tato meziresortní pracovní skupina pracovala až do konce měsíce března 2013. V rámci své činnosti pak shledala potřebu určitých změn oproti předpokladům, které byly vytýčeny věcným záměrem. Jako nejvíce exponované byly vytipovány následující okruhy

- rozšíření pojmu kyberprostor i na systémy, které nejsou „on-line“,
- zákon se nebude vztahovat na informační a komunikační systémy, které nakládají s utajovanými informacemi,
- výjimka pro informační a komunikační systémy zpravodajských služeb z regulace zákona.

Oproti věcnému záměru zákona o kybernetické bezpečnosti se v důsledku připomínek upravila definice kybernetického prostoru. Terminologicky se nová definice vypořádává i s existencí kriticky důležitých systémů, které nemají přímé „on-line“ napojení k veřejné síti. Zákon tak bude nově dopadat i na ty informační a komunikační systémy, které nejsou připojeny k internetu a jejichž správu lze podřadit pod definice orgánů a osob. Pro specifické postavení zpravodajských služeb České republiky, kdy tyto služby spravují informační systémy velké důležitosti, avšak není z věcného hlediska (zájem zpravodajských služeb na utajení metod a forem práce) a současně z důvodu faktické nemožnosti v některých případech adekvátně dostát povinnostem návrhu zákona o kybernetické bezpečnosti možné o těchto systémech sdělovat konkrétní údaje a tyto systémy tak dekonspirovat či je podrobovat možné kontrole ze strany NBÚ byla stanovena výjimka pro tyto systémy. Aby byly do systému regulace vztaženy ty informační nebo komunikační systémy zpravodajských služeb, jejichž existence nespadá pod shora uvedená kritéria, není výjimka koncipována jako absolutní, ale některé systémy zpravodajských služeb budou do systému kybernetické bezpečnosti vztaženy, a to takovým způsobem, který respektuje specifika zpravodajských služeb a přispěje k větší bezpečnosti kybernetického prostoru. Současně bylo přistoupeno k výjimce z věcné působnosti, kdy regulaci nebudou podléhat informační a komunikační systémy nakládající s utajovanými informacemi. Takové systémy mají svou úroveň bezpečnosti jasně definovanou v certifikační zprávě, deklarovanou certifikátem vydaným NBÚ a dodržení podmínek certifikace je pravidelně kontrolováno.

V rámci tvorby paragrafového znění pak meziresortní pracovní skupina provedla dílčí úpravy, které vedly, v souladu s přijatým stanoviskem LRV k věcnému záměru k odstranění kompetenčních konfliktů. Kontrolní a sankční pravomoci byly upraveny tak, že kontrolu bude vykonávat NBÚ a jen oproti orgánům a osobám, které spravují významné informační systémy podle zákona o kybernetické bezpečnosti, bude kontrolu bezpečnostních opatření provádět Ministerstvo vnitra. Kontrolní mechanismy, kterými disponuje Český telekomunikační úřad, zůstávají nedotčeny.

Dále došlo tak k následujícím úpravám

- zpřesnění legální definice bezpečnosti informací a kritické informační infrastruktury,
- definiční vymezení významného informačního systému,
- předávání kontaktních údajů orgánů a osob, které jsou orgány veřejné moci.

V rámci vymezení definice významného informačního systému byla akcentována skutečnost, že právě pro tyto systémy, které budou podřazeny pod tvořenou definici, bude nastavena nižší úroveň bezpečnostních opatření. Charakter orgánů a osob, majících původ ve veřejné správě bylo nutné provázat s existující legislativou, zejména se základními registry. Systém hlášení kontaktních údajů a jejich změn byl nejprve nastaven tak, že ty orgány a osoby, které jsou orgány veřejné správy, by kontaktní údaje hlásily prostřednictvím informačního systému o informačním systému orgánů veřejné správy, avšak v průběhu dalších prací byl po konzultaci s Ministerstvem vnitra tento systém opuštěn a i pro tyto orgány a osoby byl zvolen systém hlášení kontaktních údajů dohledovému pracovišti.

Po rozsáhlé diskuzi uvnitř meziresortní skupiny došlo k některým úpravám návrhu zákona o kybernetické bezpečnosti, které zohledňují současný právní stav a reagují na vyjasnění potencionálních konfliktů. Změny se tak objevily zejména v těchto částech

- úprava povinnosti mlčenlivosti,
- předávání údajů orgánům veřejné moci a sdílení údajů v mezinárodním kontextu,
- úprava deliktní odpovědnosti,
- vymezení vztahu stavu kybernetického nebezpečí a nouzového stavu,
- definiční vymezení pojmu významná síť a opuštění pojmu páteřní síť.

Povinnost mlčenlivosti byla navázána na široký okruh osob, které se podílely na řešení kybernetického bezpečnostního incidentu nebo které se o něm dozvěděly. Tato široká varianta byla následně zúžena tak, že tuto povinnost návrh zákona ukládá zaměstnancům NBÚ, kteří se podílí na řešení kybernetického bezpečnostního incidentu. V důsledku zachování minimalizace dopadů do sféry osob soukromého práva došlo k upuštění od původně navržené koncepce deliktní odpovědnosti, kdy návrh zákona bude sankcionovat jen závažná porušení povinností ukládaných orgánům a osobám, které jsou osobami soukromého práva, typicky pak došlo k upuštění od sankce v případě neoznámení kontaktních údajů, resp. jejich změn v případě osob soukromého práva, které nejsou součástí kritické informační infrastruktury.
Stav kybernetického nebezpečí, jako stav mimořádný, který je koncipován jako stav mimo režim krizového zákona i mimo režim ústavního zákona o bezpečnosti České republiky, bylo nutno provázat na mimořádné stavy podle těchto právních předpisů. Ve spolupráci s Generálním ředitelstvím hasičského záchranného sboru byla navržena konstrukce, že v případě, že je zřejmé, že na odvrácení škodlivého následku, který vedl k vyhlášení stavu kybernetického nebezpečí, nedostačují postupy a prostředky přijaté podle návrhu zákona o kybernetické bezpečnosti, navrhne ředitel NBÚ vládě, aby byl vyhlášen nouzový stav s tím, že dosavadní opatření přijatá za stavu kybernetického nebezpečí zůstanou v platnosti, pokud tato opatření nebudou v rozporu s krizovými opatřeními vyhlášenými vládou.

7.4 Rada pro kybernetickou bezpečnost

Návrh zákona byl k dalším konzultacím předložen v listopadu 2012 Radě pro kybernetickou bezpečnost. Rada pro kybernetickou bezpečnost je koordinačním a poradním orgánem předsedy vlády pro oblast kybernetické bezpečnosti. Její členové (určení zástupci Ministerstva vnitra, Ministerstva obrany, Ministerstva zahraničních věcí, Ministerstva financí, Ministerstva průmyslu a obchodu, Ministerstva dopravy, Policie České republiky, Úřadu pro zahraniční styky a informace, Bezpečnostní informační služby, Vojenského zpravodajství, Úřadu na ochranu osobních údajů, Českého telekomunikačního úřadu) předložený návrh zákona o kybernetické bezpečnosti projednali a na základě jejich připomínek a doporučení byl materiál upraven a následně předložen ke konzultacím odborné veřejnosti.

7.5 Konzultace s odbornou veřejností

Pro hodnocení dopadů návrhu zákona o kybernetické bezpečnosti na soukromý sektor byla oslovena široká odborná veřejnost včetně zástupců technických oborů akademické sféry. Jako zástupci odborné veřejnosti byly vybrány osoby soukromého práva, které se účastnily diskuse nad věcným záměrem zákona o kybernetické bezpečnosti, zástupci akademické sféry – ČVUT, Fakulta informatiky Masarykovy univerzity v Brně, Ústav práva a technologií Právnické fakulty Masarykovy univerzity v Brně, zájmové sdružení právnických osob CZ.NIC, které provozuje oficiální národní CERT tým, zájmové sdružení AFCEA, poskytovatelé služeb elektronických komunikací, GTS Novera, T- Mobile, O2 Telefonica, správci sítí T-systems, zástupci bankovního sektoru ČNB a ČSOB, veřejná správa – Správa základních registrů, samospráva – Svaz měst a obcí, a ostatní subjekty, které na poli kybernetické bezpečnosti spolupracují Microsoft, Deloitte, Cesnet, T-soft. Oslovené subjekty dostaly k dispozici verzi paragrafového znění zákona vytvořenou meziresortní pracovní skupinou, a která byla odsouhlasena Radou pro kybernetickou bezpečnost. Současně byly pozvány na prezentaci zákona o kybernetické bezpečnosti, která se uskutečnila dne 22. ledna 2013 na NBÚ, kde jim byl zákon o kybernetické bezpečnosti představen a kde byly vyzvány k tomu, aby k předložené verzi uplatnily připomínky. Oslovené subjekty k předložené verzi zaslaly NBÚ více než 400 připomínek. Připomínky byly vypořádány na jednáních ve dnech 8. února 2013, 12. února 2013, 18. února 2013 a týkaly se následujících oblastí

- úprava definice bezpečnosti informací,
- zúžení orgánů a osob spadajících pod regulaci podle § 3 písm. b) návrhu zákona,
- vyjasnění dopadu regulace (na konkrétní informační nebo komunikační systémy, které budou prvkem kritické informační infrastruktury a významné informační systémy),
- detekce kybernetických bezpečnostních událostí,
- sdílení informací mezi vládním CERT a národním CERT a dalšími subjekty,
- úprava povinnosti mlčenlivosti,
- úprava opatření a příklady reaktivních opatření,
- úprava podmínek předávání kontaktních údajů národním CERT vládnímu CERT,
- nápravné opatření – zpřísnění a zpřesnění kritérií, za kterých lze zakázat provozování systému,
- jiné vymezení obsahu pojmů kybernetická bezpečnostní událost a kybernetický bezpečnostní incident,
- zrušení výjimky pro systémy nakládající s utajovanými informacemi,
- zvýšení sankcí,
- změna přechodných ustanovení,
- nutnost novelizace zákona o elektronických komunikacích.

Na základě uplatněných připomínek došlo k významné úpravě návrhu zákona o kybernetické bezpečnosti. Došlo k zúžení orgánů a osob, které podléhají národnímu CERT – z ustanovení návrhu zákona došlo k vypuštění kategorie tzv. významných poskytovatelů služeb elektronických komunikací. Povinnost detekce kybernetických bezpečnostních událostí se na základě uplatněných připomínek nebude dotýkat poskytovatelů služeb elektronických komunikací a subjektů zajišťující sítě elektronických komunikací, ale bude dopadat jen na ty orgány a osoby, kterým návrh zákona ukládá povinnost hlásit kybernetické bezpečnostní incidenty. Institut mlčenlivosti se váže pouze na zaměstnance NBÚ a byla opuštěna konstrukce, kdy by o porušení povinnosti mlčenlivosti nešlo v případě, kdyby osoba podílející se na řešení kybernetického bezpečnostního incidentu poskytla údaje z evidence orgánům veřejné moci. Všechny konkrétní údaje z evidence incidentů budou předávány výhradně NBÚ. Institut preventivního opatření se upravil do nově zaváděného pojmu varování, kdy tento nově zvolený pojem lépe vystihuje obsahovou stránku této formy opatření. Na základě požadavku větší předvídatelnosti právní úpravy byl akceptován požadavek, aby příklady opatření byly uvedeny v prováděcím právním předpisu. Současně došlo k úpravě přechodných ustanovení, kdy je okamžik vzniku povinností nově vázán nikoli na účinnost zákona, ale na určení prvku kritické informační infrastruktury, respektive významného informačního systému. Současně bylo vypuštěno přechodné ustanovení, které stanovilo přechodné období pro orgány a osoby na provedení opatření. Doplněno bylo ustanovení, které reaguje na existenci memoranda o spolupráci mezi NBÚ a sdružením CZ.NIC a stanoví, že po dobu než bude vybrán provozovatel národního CERT, vykonává jeho funkce subjekt, který uzavřel s NBÚ smlouvu o spolupráci. V neposlední řadě byla akcentována nutnost novelizovat zákon o elektronických komunikacích v ustanovení o důvěrnosti komunikací tak, aby došlo k zpřesnění povinnosti poskytovatelů služeb elektronických komunikací ve vztahu ke koncovým uživatelům s cílem výslovně zajistit možnost koncových účastníků vyžadovat od poskytovatele služeb údaje o uskutečněné komunikaci. Zamítnuty byly požadavky na jiné vymezení obsahu pojmů kybernetická bezpečnostní událost a kybernetický bezpečnostní incident, kdy obsah těchto pojmů plně odpovídá zavedené mezinárodní terminologii. Požadavek na podřazení informačních a komunikačních systémů nakládajících s utajovanými informacemi pod regulaci byl rovněž odmítnut, neboť bezpečnost těchto systémů je

dostatečně ošetřena platnou legislativou v oblasti utajovaných informací. Stejně tak nebylo vyhověno požadavku na zvýšení sankcí, které zákon o kybernetické bezpečnosti v rámci deliktní odpovědnosti stanoví, když regulace je postavena primárně na prevenci a vzájemné spolupráci v oblasti kybernetické bezpečnosti.

7.6 Podpora mezinárodní spolupráce v oblasti kybernetické bezpečnost

NBÚ zahájil ihned po ustavení gestorem problematiky kybernetické bezpečnosti a národní autoritou pro oblast kybernetické bezpečnosti odpovídající aktivity. Iniciovala se snaha o zapojení do mezinárodních organizací zabývajících se touto problematikou a začalo se s aktivním navazováním kontaktů s partnerskými úřady, především zahraničními vládními CERT. Již v listopadu 2011 se NBÚ účastnil jako pozorovatel NATO Cyber Coalition 2011, které bylo za Českou republiku vedeno Armádou České republiky a Ministerstvem obrany a následně se plně účastnil cvičení NATO Cyber Coalition 2012. Dne 14. března 2012 bylo podepsáno Memorandum o porozumění mezi NATO Cyber Defence Management Board a NBÚ o spolupráci v oblasti kybernetické obrany, které zakotvuje základní principy spolupráce mezi Českou republikou a NATO v oblasti kybernetické bezpečnosti a obrany. Memorandum se týká sdílení informací o aktuálních útocích a hrozbách a případné pomoci při řešení závažných kybernetických bezpečnostních událostí. Podpisem tohoto memoranda, které Česká republika podepsala jako osmnáctý členský stát NATO, došlo k plnému začlenění České republiky do struktur NATO v oblasti kybernetické obrany.

V průběhu roku 2012 a počátkem roku 2013 se uskutečnila řada návštěv partnerských úřadů v členských státech NATO a EU zaměřených především na sdílení informací o systému zajištění kybernetické bezpečnosti a získání zkušeností s provozováním vládních CERT. V této souvislosti pracovníci NBÚ navštívili Polsko, Španělsko, Lucembursko, Německo, Chorvatsko, Norsko a Velkou Británii. V průběhu května proběhla návštěva ředitele NBÚ ve Spojených státech amerických, v jejímž průběhu byla navázána spolupráce s představiteli Bílého domu, Ministerstva zahraničních věcí, Ministerstva obrany a Ústřední zpravodajské služby (CIA). Ve všech navštívených zemích byla představena filosofie návrhu zákona a byly konzultovány základní principy regulace.

NBÚ podnikl kroky k tomu, aby se Česká republika po zahájení funkčnosti vládního CERT zapojila do uznávaných mezinárodních organizací zabývajících se kybernetickou bezpečností. V této souvislosti byly navázány kontakty s organizací CERT Coordination Center působící pod záštitou Carnegie-Mellon University, stejně jako s organizací FIRST (Forum of Incident Response and Security Teams). V letošním roce Úřad také z větší části převzal agendu spojenou se spoluprací s organizací ENISA – European Network and Information Security Agency.

Zástupci NBÚ účastnili řady jednání a konferencí, kde prezentovali koncepci kybernetické bezpečnosti České republiky. Kromě navazování důležitých kontaktů zástupci NBÚ sbírali zpětnou vazbu k této koncepci a k dosavadní prezentované činnosti NBÚ týkající se problematiky kybernetické bezpečnosti. Reakce na celkovou koncepci a připravovanou legislativu je možno shrnout jako velmi pozitivní, zejména co se týče progresivního přístupu obsaženého v návrhu zákona. Jednalo se zejména o vystoupení na konferencích ke kybernetické bezpečnosti organizovaných AFCEA (Armed Forces Communications and Elecronics Association), Mezinárodní telekomunikační unií, ISACA (Information systems Audit and Control Association) a FIRST.

7.7 Technologická analýza a zdroje dat

Celková evidence důležitých systémů ICT pro fungování státu v kybernetickém prostoru je základem pro jejich efektivní zabezpečení. Vzhledem ke skutečnosti, že doposud neexistovala

žádná využitelná evidence, bylo nezbytné, aby byla vytvořena vlastní evidence pro potřeby kybernetické bezpečnosti a zvládání kybernetických bezpečnostních incidentů.
Pro vytvoření základního přehledu důležitých informačních a komunikačních systémů, tedy technologií pro fungování státu byla zvolena forma dotazníku rozesílaných na jednotlivé odpovědné subjekty. Tento způsob zjišťování stavu byl vybrán zejména z důvodu snahy minimalizovat finanční a časovou náročnost celého procesu výběru těchto důležitých systémů prováděného jak NBÚ, tak spolupracujícími subjekty.
Vlastní realizace celé evidence je rozdělena do dvou časově navazujících etap.
Cílem první etapy pro rok 2012 byla realizace evidence důležitých systémů pod správou veřejnoprávních subjektů a zjištění úrovně jejich základních bezpečnostních parametrů včetně analýzy rizik.
Cílem druhé etapy, která je v plánu na r. 2013, je evidence důležitých systémů pod správou osob soukromého práva a zjištění úrovně jejich základních bezpečnostních parametrů včetně analýzy rizik.
V lednu 2012 byl rozeslán na 44 subjektů první dotazník kybernetické bezpečnosti, jehož cílem bylo zejména určení celkového rozsahu důležitých systémů s připojením do veřejných sítí. Obsahoval deset základních evidenčních údajů jako je název informačního systému, kontaktní údaje na bezpečnostního manažera a správce informačního systému, připojení do KIVS, apod. Po vyhodnocení prvního dotazníku byl vytvořen základní přehled o cca 730 informačních systémech, které veřejnoprávní subjekty považovaly za důležité pro fungování státu. Tento seznam obsahoval i systémy, které nebyly důležité pro fungování státu, např. informační systémy Myslivecké a rybářské průkazy, Evidence restaurátorů, Evidence knihoven. Na druhé straně v seznamech u některých subjektů zjevně chyběly jejich kritické systémy podléhající krizovému zákonu. Z těchto zjištění vycházelo zpřesnění původní množiny důležitých systémů, které bylo zahrnuto v druhém dotazníku kybernetické bezpečnosti, jednalo se o vydefinování kritických a významných systémů vycházejících z krizového zákona a zákona o informačních systémech veřejné správy a vypuštění parametru nutného pro připojení těchto systémů do internetu.
V měsíci srpnu 2012 byl rozeslán druhý dotazník kybernetické bezpečnosti, který obsahoval 54 otázek s detailnějším zaměřením na popis vybraných bezpečnostních parametrů. Výsledkem je vytvoření seznamu s celkovým počtem cca 170 důležitých systémů státu. Přibližný počet je uváděn zejména z důvodu různého stupně agregace IS na úrovni hodnocení jednotlivých subjektů, které budou zpřesněny na plánovaných společných jednáních NBÚ a dotčených subjektů v následujícím období.

7.7.1 Vyhodnocení dotazníků

Konkrétní data získaná výše uvedenou dotazníkovou metodou byla předložena vládě ve formě utajovaného dokumentu stupně utajení Vyhrazené, a proto nelze tato data uvést v důvodové zprávě.

7.7.2 Shrnutí významných zjištění

Velmi pozitivním zjištěním je skutečnost, že metodika norem pro řízení informační bezpečnosti ISO/IEC 27001, 27002, z níž vychází návrh zákona, je již nyní využívána pro řízení informační bezpečnosti u 80% subjektů spravujících důležité informační a komunikační technologie státu, 98% subjektů spravujících důležité informační a komunikační systémy a technologie státu má již zcela nebo částečně zaveden systém evidence a zvládání bezpečnostních incidentů, a že 21% subjektů spravujících důležité informační a komunikační systémy a technologie státu má zavedeno certifikované řízení informační bezpečnosti. Z uvedeného je zřejmé, že vzhledem k rozšířenosti používání bezpečnostního standardu rodiny norem ISO IEC 27000 u subjektů spravujících důležité informační a komunikační systémy a

technologie státu, je výběr této metodologie pro návrh zákona správným rozhodnutím. Uvedená analýza bude podkladem, na základě kterého dojde k vymezení kritické informační infrastruktury ve smyslu definice zákona o kybernetické bezpečnosti s tím, že jednotlivé prvky budou určeny postupem podle krizového zákona. Zpracovaná analýza je tak podkladem, na základě kterého bude budováno technologické řešení, postavené na respektování maxima stávajícího technického řešení subjektů podléhajících regulaci s principiálně technologicky neutrálním řešením bezpečnostních opatření vycházejících z mezinárodně platných standardů.

II. Odůvodnění hlavních principů navrhované právní úpravy

Předmětem navrhované právní úpravy je založení práv a povinností nutných k zajištění bezpečnosti kybernetického prostoru. Jejím smyslem a účelem je tedy zabezpečit prostředí tvořené informačními systémy a službami a sítěmi elektronických komunikací tak, aby nebyla v důsledku kybernetických bezpečnostních incidentů ohrožena jeho samotná existence či celková funkčnost, tj. aby byl chráněn veřejný zájem na fungování služeb informační společnosti. Ve svém důsledku tedy navrhovaná právní úprava sleduje cíl zabezpečení existence a funkčnosti informačních kanálů, jimiž člověk realizuje svá práva na informační sebeurčení.
Smyslem a účelem se tedy navrhovaná právní úprava výrazně liší od shora cit. právních předpisů, jejichž předmětem je zpravidla založení konkrétní odpovědnosti za různé formy jednání poškozujícího informační práva jednotlivců nebo státu. Navrhovaná právní úprava totiž nezakládá civilní ani trestní odpovědnost pachatelů kybernetických útoků (ta je ostatně již pro většinu typických případů založena shora cit. předpisy), ale vytváří systém bezpečnostních opatření, která mají výskytu kybernetických bezpečnostních incidentů předcházet, resp. která mají zajistit, že případný kybernetický bezpečností incident neohrozí celkové fungování informačních a komunikačních systémů nebo fungování kriticky důležitých společenských informačních funkcionalit.
Svým zaměřením tedy lze navrhovanou právní úpravu přirovnat například k předpisům protipožární ochrany – jejich smyslem je rovněž zavázat určité subjekty k dodržování základních bezpečnostních pravidel a nastavit takové detekční a reaktivní mechanismy, aby případně vyskytnuvší se ohrožení bylo co nejdříve a co nejúčinněji zažehnáno (přičemž identifikace pachatelů a jejich následný postih řeší standardně předpisy práva soukromého, správního či trestního).

1. Specifické principy navrhované právní úpravy

Navrhovaná právní úprava je postavena na následujících specifických principech:

- Princip technologické neutrality
- Princip ochrany informačního sebeurčení člověka
- Princip ochrany nedistributivních práv
- Princip minimalizace státního donucení
- Princip autonomie vůle regulovaných subjektů
- Princip bdělosti ve vztahu k ostatním státům a k mezinárodnímu společenství

1.1 Princip technologické neutrality

Tento princip se v navrhované právní úpravě projevuje v první řadě striktním zaměřením zákonných povinností k technologickým aspektům fungování služeb informační společnosti

(tj. informačních systémů a služeb a sítí elektronických komunikací). Navrhovaná právní úprava důsledně odděluje bezpečnost fungování služeb informační společnosti od informačního obsahu a předmětem regulace tak zde není obsah přenášených informací. Předmětem navrhované právní úpravy tedy nejsou například projevy obsahové informační či počítačové kriminality, jako např. šíření dětské pornografie, stalking nebo porušování práv duševního vlastnictví. Práva a povinnosti založené navrhovanou právní úpravou budou postihovat pouze kybernetické bezpečnostní incidenty – žádná ze součástí navrhované právní úpravy tak neumožňuje státu nebo jeho orgánům provádět obsahovou cenzuru internetu nebo jiných informačních sítí či služeb.
Projevem principu technologické neutrality v navrhované právní úpravě je užití výhradně obecných kriterií pro standardní zabezpečení informačních systémů a služeb a sítí elektronických komunikací. Bezpečnostní opatření, k jejichž dodržování zaváže navrhovaná právní úprava vybrané subjekty (např. správce systémů kritické informační infrastruktury) jsou definovány tak, aby mohlo být jejich splnění řešeno za užití různých technologií a postupů. Subjekty, jimiž navrhovaná právní úprava zavede povinnosti aplikovat standardní bezpečnostní technologie, tedy budou moci dle vlastního uvážení volit konkrétní způsob zabezpečení jejich informačních struktur, a to včetně volby dodavatelů příslušných bezpečnostních řešení. V současné době je na českém trhu ICT běžně k dispozici celá řada tuzemských i zahraničních produktů způsobilých naplnit předpoklady navrhované právní úpravy – díky bezvýhradnému založení navrhované právní úpravy na principu technologické neutrality tedy nedojde k narušení standardních tržních mechanismů v oboru bezpečnostních ICT.

1.2 Princip ochrany informačního sebeurčení člověka

Bezpečnost nelze vnímat jako samostatně existující legitimní hodnotu. Legitimní jsou totiž jen ta bezpečnostní opatření, jejichž prostřednictvím je chráněn (zabezpečen) legitimní společenský zájem. Navrhovaná právní úprava je v tomto směru primárně založena na principu zabezpečení informačního sebeurčení člověka.
Pojem informačního sebeurčení člověka zavedl do právní praxe Spolkový ústavní soud[12)] jako souhrnné označení pro katalog absolutních informačních práv člověka. Původní chápání pojmu informačního sebeurčení zahrnovalo především jeho pasivní složku, tj. ochranu diskrétní informační sféry, a projevovalo se především ochranou soukromí a ochranou osobních údajů. Dalším rozvojem ústavní judikatury a judikatury Evropského soudu pro lidská práva dospěla právní doktrína k aktuálnímu chápání informačního sebeurčení, které kromě pasivní složky (tj. ochrany diskrétních informací) zahrnuje též aktivní složku, tj. právo aktivně přijímat, zpracovávat a komunikovat informace. Aktivní aspekt informačního sebeurčení přitom vychází z předpokladu, že člověk nemůže žít plnohodnotný soukromý život bez toho, aby měl možnost komunikovat s okolním světem[13)]. V tomto smyslu je právo na informační sebeurčení reflektováno navrhovanou právní úpravou jako její dominantní princip legitimující obecně legislativní zadání k řešení kybernetické bezpečnosti.
Zaměření navrhované právní úpravy k ochraně práva na informační sebeurčení se odráží též v konkrétní struktuře informací zpracovávaných dohledovými pracovišti, přičemž tvorba, zpracování ani archivace záznamů o výskytu a řešení kybernetických bezpečnostních incidentů nesměřují k identifikaci osob nebo k jiným zásahům do práva na soukromí nebo do práva na ochranu osobních údajů. Zjednodušeně řečeno je tedy navrhovaná právní úprava konstruována tak, aby detekčních nebo obranných mechanismů, s jejichž zavedením u vybraných služeb a sítí počítá, nebylo možno zneužít ke sledování uživatelů služeb informační společnosti.

[12)] Viz BVerfG, 15. prosince 1983, 1 BvR 209/83 u. a. – Volkszählung –, BVerfGE 65, 1.
[13)] K tomu srov. např. I.ÚS 22/10 ze dne 07.04.2010, N 77/57 SbNU.

Vedle dominantní úlohy informačního sebeurčení směřují partikulární součásti navrhované právní úpravy rovněž k zabezpečení informační infrastruktury k nerušenému výkonu dalších informačních práv člověka, tj. práva na svobodu projevu, práva na vzdělání, sdružovacího práva, práva na podnikání apod.

1.3 Princip ochrany nedistributivních práv

Navrhovaná právní úprava je vedle ochrany informačního sebeurčení člověka postavena též na principu ochrany nedistributivních (veřejných) práv, konkrétně práva státu na zajištění vnitřní bezpečnosti, na ochranu základních funkcionalit státu a na ochranu před škodlivými následky výjimečných stavů. Zařazení tohoto principu do struktury základních principů navrhované právní úpravy reflektuje skutečnost, že fungování státu je v současné době do značné míry závislé na existenci informačních struktur zajišťujících kriticky důležité společenské funkcionality. Kybernetický bezpečnostní incident může v tomto směru znamenat nejen shora zmíněný zásah do možnosti člověka realizovat právo na informační sebeurčení, ale může též vést k ohrožení nebo omezení těch vitálních společenských funkcionalit, pro něž zajišťují informační systémy nebo služby a sítě elektronických komunikací životně důležitou informační podporu. Kybernetický útok tak může v krajním případě ohrozit například energetický sektor, zásobování obyvatelstva esenciálními komoditami, sociální služby nebo dopravní obsluhu. Princip ochrany nedistributivních práv je navrhovanou právní úpravou reflektován zejména v otázce rozsahu kritické informační infrastruktury a v otázce úpravy stavu kybernetického nebezpečí.

1.4 Princip minimalizace státního donucení

Tento princip je v navrhované právní úpravě nejen důsledkem liberálního přístupu k předmětu právní regulace, ale zejména důsledkem pragmatického zhodnocení dosavadních zkušeností získaných analýzou současného stavu zabezpečení informačních systémů a služeb a sítí elektronických komunikací. Navržená právní úprava resp. povinnosti z ní plynoucí tak nedopadá na veškeré informační systémy resp. služby a sítě elektronických komunikací, ale zaměřuje se pouze na ty informační a komunikační systémy, které mají aktuálně vzhledem ke shora uvedenému účelu zákona zásadní význam. Zabezpečení těchto systémů před běžnými formami kybernetických útoků tak je řešeno pouze ve vztahu k systémům a sítím tvořících kritickou informační infrastrukturu a dále pak ve vztahu k významným informačním systémům. Povinnost aplikace standardního zabezpečení včetně povinnosti hlásit výskyt kybernetických bezpečnostních incidentů a odpovídajícím způsobem na ně reagovat je tedy obecně definována pouze pro správce systémů značného společenského významu (tj. systémů, jejichž ochrana má ve shora uvedeném smyslu zásadní význam pro ochranu práv na informační sebeurčení a nedistributivních informačních práv státu). Lze tedy konstatovat, že věcný a osobní rozsah navrhované právní úpravy je minimalistický a sleduje dosažení shora uvedeného účelu za užití nejnižší možné míry právní regulace.

Rozšíření rozsahu povinností poskytovatelů služeb elektronických komunikací a subjektů zajišťující sítě elektronických komunikací mimo kritickou informační infrastrukturu je zákonem předpokládáno pouze při vyhlášení stavu kybernetického nebezpečí. Procedura vedoucí k vyhlášení tohoto stavu je zákonem upravena tak, aby nemohlo dojít k jeho svévolnému zneužití (stav kybernetického nebezpečí je vyhlašován předsedou vlády České republiky a následně schválen exekutivním orgánem s nejvyšší úrovní politické legitimity, tj. vládou České republiky, to navíc pouze na návrh ředitele ústředního orgánu státní správy, tj. NBÚ).

Vedle standardního povinného zapojení shora uvedených subjektů do systému ochrany před kybernetickými bezpečnostními incidenty počítá navrhovaná právní úprava s tím, že řada subjektů provozujících informační systémy, sítě a služby projeví zájem o dobrovolné zapojení

do národního systému kybernetické bezpečnosti. Zkušenosti ze zahraničí ukazují, že spolupráce s národními dohledovými pracovišti přináší podnikatelským subjektům i akademickému nebo neziskovému sektoru vysoce pozitivní efekty a že zájem o tuto spolupráci bývá velký - správci soukromých nebo akademických informačních systémů, sítí nebo služeb mají v takových případech možnost vzájemně sdílet poznatky o hrozbách v oblasti kybernetické bezpečnosti a díky metodickému působení národního dohledového pracoviště mohou vlastní infrastrukturu daleko účinněji bránit před kybernetickými bezpečnostními incidenty. Zákon tedy v tomto směru počítá s možností dobrovolného zapojení do systému národní kybernetické bezpečnosti i pro subjekty mimo okruh orgánů a osob. Lze v této souvislosti předpokládat, že spíše než spolupráci s orgánem veřejné moci uvítají subjekty dobrovolně zapojené do národního systému kybernetické bezpečnosti raději možnost spolupracovat s právně rovnocennou osobou soukromého práva. Na základě skutečnosti, že k dobrovolné spolupráci není zapotřebí vykonávat nařizovací, kontrolní nebo sankční pravomoci a rovněž na základě pozitivních zkušeností ze zahraničí byl pro navrhovanou právní úpravu zvolen model provozu národního dohledového pracoviště osobou soukromého práva, a to na základě veřejnoprávní smlouvy. Designace provozovatele národního dohledového pracoviště formou veřejnoprávní smlouvy umožní nejen adekvátně realizovat autonomní vůli těch subjektů, které budou mít aktivní zájem podílet se na národním systému kybernetické bezpečnosti, ale též označí tohoto provozovatele jako partnera pro obdobně fungující národní dohledová pracoviště v zahraničí a pro jejich mezinárodní spolky. I osoby soukromého práva, které nejsou orgány a osobami, se budou moci zapojit do systému národní kybernetické bezpečnosti spoluprací s vládním CERT.

1.5 Princip autonomie vůle regulovaných subjektů

Analýzou aktuální situace bylo zjištěno, že kriticky důležité informační systémy a služby a sítě elektronických komunikací resp. významné informační systémy (tj. infrastruktura, k níž budou směřovat specifické zákonné povinnosti) mají zásadně různý charakter a jsou spravovány různými typy subjektů. Přestože lze i takto heterogenní skupině adresátů navrhované právní úpravy stanovit obecným způsobem příslušné povinnosti, není vhodné ani potřebné direktivně určovat konkrétní technické a organizační postupy. Navrhovaná právní úprava jde v tomto směru cestou stanovení základních povinností a standardních bezpečnostních parametrů, přičemž je adresátům právních povinností ponechána volnost ve způsobech, jakými dosáhnou jejich naplnění. Podobně, jako navrhovaná právní úprava podle shora uvedeného principu počítá s tím, že lze standardní zabezpečení informačních systémů a sítí řešit za užití různých zabezpečovacích technologií, je regulatorní řešení liberální i v konkrétních způsobech, jimiž bude na straně orgánů a osob zajištěno plnění zákonných povinností. Konkrétní organizační a technické postupy včetně např. řízení dodavatelů, školení zaměstnanců, interních kontrol apod. tedy ponechává navrhovaná právní úprava plně v diskreci orgánů a osob. Tím je zajištěno, že výsledné zabezpečení informačních a komunikačních systémů bude ve svém souhrnu spolehlivě funkční, přičemž individualita jednotlivých partikulárních bezpečnostních řešení umožní efektivní využití příslušných zdrojů. Zjednodušeně řečeno se tedy princip autonomie vůle regulovaných subjektů v důsledku projeví tak, že prostředky vynaložené na zabezpečení příslušných informačních systémů, služeb a sítí elektronických komunikací budou použity v přímém vztahu ke konkrétním potřebám orgánů a osob, tj. zpravidla účelně a hospodárně.

Významným projevem principu autonomie vůle je možnost dobrovolného zapojení subjektů mimo okruh orgánů a osob do systému kybernetické bezpečnosti.

1.6 Princip bdělosti ve vztahu k ostatním státům a k mezinárodnímu společenství

Přestože dominantním účelem navrhované právní úpravy je zajištění bezpečnosti informačních a komunikačních systémů, je navrhovaná právní úprava postavena též subsidiárně na respektu k mezinárodněprávnímu principu due dilligence, tj. k principu, na jehož základě je suverénní stát povinen v rámci své jurisdikce aktivně bránit škodám, které by mohly vzniknout ostatním státům nebo mezinárodnímu společenství. Specifická úprava, která na národní úrovni umožní zabezpečit informační a komunikační systémy před kybernetickými bezpečnostními incidenty, totiž ochrání tyto systémy i před tím, aby nebyla zneužita k útokům cíleným mimo českou jurisdikci.

Účinný národní systém detekce a řešení kybernetických bezpečnostních incidentů tak bude chránit české národní zájmy nejen bezprostředně, ale též formou ochrany před budoucí možnou mezinárodní odpovědností České republiky ostatním státům nebo mezivládním organizacím z titulu nedostatečného zabezpečení kybernetického prostoru před možností zneužití zdejších informačních systémů, sítí a služeb elektronických komunikací k útokům na zahraniční nebo mezinárodní infrastrukturu.

2. Základní instituty navrhované právní úpravy

Řešení kybernetické bezpečnosti v navrhované právní úpravě vycházející ze shora uvedených principů je postaveno na následujících základních institutech:

- Institut bezpečnostních opatření,
- Institut hlášení kybernetických bezpečnostních incidentů a
- Institut opatření

2.1 Bezpečnostní opatření

Navrhovaná právní úprava vychází z předpokladu, že zabezpečení informačních a komunikačních systémů před negativními následky kybernetických bezpečnostních incidentů může být efektivní pouze v případě, jsou-li jednotlivé jeho prvky aplikovány systematicky a ve vzájemných souvislostech. Jedním z předpokladů navrhované právní úpravy je rovněž faktická důležitost nejen technických řešení, ale též s nimi souvisejících organizačních opatření. Teprve kombinace kvalitní technologie s náležitě zorganizovaným personálním zajištěním totiž může ve výsledku poskytnout kýženou efektivitu.

Navrhovaná právní úprava počítá se zavedením povinností definovat a aplikovat systém opatření a postupů pro vybrané skupiny orgánů a osob, tj. správce kritické informační infrastruktury a správce významných informačních systémů souhrnně označovaný jako bezpečnostní opatření. Definice bezpečnostních opatření je v navrhované právní úpravě včetně prováděcích předpisů provedena genericky resp. teleologicky a předpokládá, že jednotlivá konkrétní řešení bezpečnostních opatření se mohou při současném splnění zákonných požadavků vzájemně odlišovat. Povinnosti týkající se zavedení systému bezpečnostních opatření vycházejí z mezinárodně uznaných standardů a týkají se nejen kategorií a funkčních parametrů jednotlivých typů bezpečnostních technologií (zejména zavedení přístupových práv, logovacích nástrojů, kryptografických nástrojů), ale rovněž organizace jednotlivých souvisejících procesů (zejména řízení lidských zdrojů, řízení akvizic nových technologií, organizační postupy pro řešení mimořádných událostí).

Z výše uvedeného plyne, že navrhovaná právní úprava předpokládá, že uvedené skupiny orgánů a osob provedou zhodnocení bezpečnostních charakteristik jimi spravovaných informačních systémů a služeb a sítí elektronických komunikací a na tomto základě si vytvoří

a zdokumentují vlastní systém bezpečnostních opatření sestávajících z opatření organizačních a technických v intencích navrhované právní úpravy.

2.2 Hlášení kybernetických bezpečnostních incidentů

Jedním ze základních účelů navrhované právní úpravy je zajistit detekci kybernetických bezpečnostních událostí a hlášení kybernetických bezpečnostních incidentů v kritické informační infrastruktuře a ve významných informačních systémech tak, aby na ně mohly v součinnosti s vládním CERT reagovat orgány a osoby s co nejmenší časovou prodlevou a co nejvyšší efektivitou. Navrhovaná právní úprava tedy počítá s tím, že budou mít vybrané skupiny orgánů a osob, tj. správci informačních nebo komunikačních systémů kritické informační infrastruktury a správci významných informačních systémů, povinnost nejen za užití shora uvedených bezpečnostních opatření detekovat výskyt kybernetických bezpečnostních událostí, ale že budou mít též povinnost předat údaje o zjištěných kybernetických bezpečnostních incidentech vládnímu CERT. Vládní CERT pak na základě vyhodnocení situace provedeného mj. i na základě zjištění, zda není incident hlášen současně z více součástí kritické informační infrastruktury nebo z významných informačních systémů, zvolí další postup adekvátní významu a rozsahu příslušného kybernetického bezpečnostního incidentu.

V této souvislosti je třeba zdůraznit, že předávané informace o detekovaných kybernetických bezpečnostních incidentech (resp. o detekovaných kybernetických bezpečnostních událostech vyhodnocených jako kybernetické bezpečnostní incidenty) nebudou mít charakter obsahových údajů, neboť jejich předmětem bude pouze identifikace kybernetického bezpečnostního incidentu.

Informace zpracovávané vládním CERT na základě hlášení kybernetických bezpečnostních incidentů budou vedeny v evidenci kybernetických bezpečnostních incidentů. Součástí této evidence budou informace, jejichž veřejná expozice by mohla poškodit buďto zájmy orgánů a osob nebo bezpečnostní zájmy České republiky – i jen pouhá statistická informace o tom, že se některá z orgánů a osob stává často terčem určitého typu kybernetických útoků, může být pro tento orgán a osobu citlivá a podobně problematická by byla například i veřejná dostupnost informací o postupech bezpečnostních týmů a vládního CERT při řešení hlášených kybernetických bezpečnostních incidentů. Z těchto důvodů budou informace zpracovávané v rámci evidence kybernetických bezpečnostních incidentů chráněny povinností mlčenlivosti a budou zpřístupněny vybraným orgánům veřejné moci k omezenému užití a národnímu CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným subjektům působícím v oblasti kybernetické bezpečnosti v rozsahu nezbytném pro zajištění ochrany kybernetického prostoru.

2.3 Opatření

Opatřením se v navrhované právní úpravě rozumí organizační nebo technický úkon či postup, jímž NBÚ uloží orgánu a osobě povinnost reagovat na kybernetický bezpečnostní incident. Za standardního režimu fungování navrhované právní úpravy (tj. není-li vyhlášen stav kybernetického nebezpečí) mají povinnost přímo aplikovat opatření jen vybrané typy orgánů a osob, tj. správci informačních a komunikačních systémů zařazených do kritické informační infrastruktury a správci významných informačních systémů. Pouze při vyhlášení stavu kybernetického nebezpečí se povinnost aplikovat opatření rozšíří i na ostatní orgány a osoby.

Opatření budou vydávána NBÚ v reakci na aktuální hrozbu v oblasti kybernetické bezpečnosti nebo v reakci na konkrétní kybernetické bezpečnostní incidenty. Budou mít buďto charakter varování před konkrétní hrozbou v oblasti kybernetické bezpečnosti, konkrétních opatření k bezprostřední reakci na probíhající nebo bezprostředně hrozící kybernetický bezpečnostní incident (typicky na hrozící nebo trvající kybernetický útok) nebo

závazných preventivních postupů k ošetření zdokumentovaných kybernetických bezpečnostních incidentů (např. k ošetření zjištěných bezpečnostních děr nebo prevenci nových penetračních technik).

3. Národní a vládní CERT

Navrhovaná právní úprava počítá se zřízením dvou dohledových pracovišť, a to národního a vládního CERT, jejichž úkolem bude vyhodnocování kybernetické bezpečnostní situace v informačních a komunikačních systémech a ochrana těchto systémů před kybernetickými bezpečnostními incidenty. Základním smyslem fungování obou dohledových pracovišť je vyhodnocování informací o výskytu kybernetických bezpečnostních incidentů z pokud možno co největšího množství informačních a komunikačních systémů. Jedině koncentrované a správně vyhodnocené informace o kybernetických bezpečnostních incidentech totiž mohou vést k odhalení nebezpečných forem kybernetických útoků, které se mohou na partikulárním systému nebo síti jevit jako bagatelní avšak při srovnání údajů z více zdrojů mohou indikovat závažný kybernetický bezpečnostní incident velkého významu.
Zřízení vládního a národního CERT rovněž umožní navázat spolupráci s obdobnými pracovišti fungujícími v ostatních státech a na mezinárodní úrovni a těžit tak ze vzájemné výměny údajů o řešení kybernetických bezpečnostních incidentů. Zapojení národního a vládního CERT do struktur vzájemně spolupracujících dohledových pracovišť umožní České republice těžit ze zkušeností získaných ve státech vystavených řádově závaznějším formám kybernetických bezpečnostních incidentů. Zkušenosti s řešením závažných kybernetických bezpečnostních incidentů získané obdobnými dohledovými pracovišti ve státech, které se ocitly takříkajíc v první linii kybernetických konfliktů, mají ve státech jako je Česká republika velký význam, neboť se zde podobné typy kybernetických hrozeb objevují zpravidla až s určitým časovým odstupem – namísto nákladných investic do vývoje vlastních bezpečnostních řešení tak lze v tomto případě úspěšně těžit z často nákladně nabytých zkušeností z ostatních států.
Model národního a vládního CERT byl zvolen k tomu, aby obě entity maximálně využily svoji institucionální povahu při ochraně národních zájmů v oblasti kybernetické bezpečnosti. Vládní CERT působící jako součást NBÚ, tj. jako orgán veřejné moci, může disponovat nařizovacími a sankčními pravomocemi a tím zajišťovat přímé uplatňování státní moci na úseku kybernetické bezpečnosti, a to včetně kontrolních a sankčních pravomocí. Vzhledem k základním principům navrhované právní úpravy (zejm. principu technologické neutrality a principu minimalizace státního donucení) však jsou pravomoci NBÚ v tomto směru maximálně omezeny, a to jak co do jejich rozsahu, tak i adresátů. Vládní CERT se svými nařizovacími a kontrolními pravomocemi tak bude primárně přímo působit pouze na vybrané informační a komunikační systémy, které mají pro národní zájmy České republiky vitální charakter, tj. na oblast kritické informační infrastruktury a významných informačních systémů.
Národní CERT naproti tomu reflektuje poptávku osob soukromého práva po centralizovaném soukromoprávním řešení sběru informací o kybernetické bezpečnostní situaci, jakož i potřebu metodiky a asistence při účinnému řešení různých typů kybernetických bezpečnostních incidentů ve většině informačních a komunikačních systémů stojících mimo shora uvedené vitální prvky. Národní CERT nebude disponovat nařizovacími ani jinými výkonnými pravomocemi, ale bude fungovat pouze k vyhodnocování a metodické podpoře subjektů, které aktivně projeví zájem o výhody kolektivní ochrany před kybernetickými bezpečnostními incidenty. Vzhledem k soukromoprávní povaze národního CERT bude především v nepředvídaných situacích vyžadujících kvalitativně zcela nová řešení nebo technické postupy možno využít toho, že jeho provozovatel může činit vše, co mu není zákonem

zakázáno (na rozdíl od situace, kdy by národní CERT provozoval orgán veřejné moci, jemuž je umožněno činit pouze to, co mu zákon výslovně ukládá nebo umožňuje). Národní CERT tedy bude moci v nepředvídaných problematických situacích reagovat operativně a nabízet kreativní řešení, jejichž jediným omezením bude zákonnost, a bude moci využít i širokých možností soukromoprávní spolupráce včetně spolupráce s obdobnými pracovišti na mezinárodní úrovni.
Právě v otázce těžení z výhod mezinárodní spolupráce je model národního a vládního CERT nanejvýš vhodný, neboť pro oba typy dohledových pracovišť existují specifické kooperativní struktury – zjednodušeně řečeno pak mají k některým kolaborativním aktivitám přístup jen dohledová pracoviště mající charakter orgánů veřejné moci a k jiným naopak jen soukromoprávní subjekty. Model dvou centrálních dohledových pracovišť zajistí České republice přísun a využití užitečných informací z obou uvedených sfér.
Navrhovaná právní úprava počítá se vzájemnou spoluprací národního a vládního CERTu, a to zejména formou výměny informací o řešení kybernetických bezpečnostních incidentů. Obě dohledová pracoviště pak budou vzájemně spolupracovat v otázkách výzkumu a vývoje, vzdělávání apod.

III. Soulad navrhované právní úpravy s ústavním pořádkem České republiky

S ohledem na judikaturu Ústavního soudu České republiky[14)] je třeba posuzovat obsah navrhované právní úpravy prostřednictvím standardní aplikace testu proporcionality. Základním právem, k jehož omezení dojde prostřednictvím zákona o kybernetické bezpečnosti, je právo vlastnické a částečně též i z něj odvozované právo na podnikání. Povinnosti, které navrhovaná právní úprava stanoví vybraným subjektům (tj. orgánům a osobám), totiž v různé míře omezuje tyto subjekty v neomezeném užívání informačních nebo komunikačních systémů, k nimž vykonávají vlastnická nebo obdobná práva.
Vzhledem k tomu, že byl při tvorbě zákona zvolen minimalistický přístup k ukládání povinností osob soukromého práva, nezasahuje tento záměr do práva na ochranu soukromí, práva na ochranu osobních údajů, práva na soukromý život, práva na svobodu projevu ani do dalších práv souhrnně označovaných jako práva na informační sebeurčení člověka – ochrana těchto práv naopak tvoří dominantní teleologii navrhované právní úpravy.
Kybernetické bezpečnostní incidenty mají za následek vedle různých typů škod též omezení dostupnosti služeb informační společnosti nebo zásahy do informační diskrece člověka. Právo na informační sebeurčení, které bylo jako souborné základní právo identifikováno Spolkovým ústavním soudem[15)] a v poslední době též několikrát zmíněno i Evropským soudem pro lidská práva a Ústavním soudem České republiky[16)], přitom sestává z pasivních a aktivních informačních práv člověka. Pasivní informační práva zahrnují především ochranu soukromí či obecně diskrétní informační sféry, zatímco aktivní informační práva mají charakter práv přístupu ke službám informační společnosti. Definice informačního sebeurčení tak vychází nejen z předpokládané nutnosti chránit diskrétní informace, ale též z předpokladu, že dnešní člověk může žít plnohodnotný život jen tehdy, pokud má možnost komunikovat s ostatními. Z toho plyne povinnost státu chránit pasivní i aktivní informační práva člověka ochranou kybernetického prostoru, kde se tato práva realizují.
Navrhovaná právní úprava omezí plošně poskytovatele služeb elektronických komunikací, subjekty zajišťující sítě elektronických komunikací, subjektů zajišťujících významnou síť a

[14)] Nález Ústavního soudu ze dne 12.října1994, sp. zn. Pl.ÚS 4/94, 214/1994 Sb., N 46/2 SbNU 57.
[15)] Nález Spolkového ústavního soudu ze dne 15. prosince 1983, č.j. BVerfGE 65, 1.
[16)] 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.

dále pak správce komunikačních systémů zařazených do kritické informační infrastruktury, správce informačních systémů zařazených do kritické informační infrastruktury a správce významných informačních systémů. Plošné omezení vlastnického práva resp. práva na podnikání má v tomto případě pouze formu zavedení povinnosti oznámit provozovateli národního CERT nebo vládního CERT kontaktní údaje, a to podle kategorií orgánů a osob.
Specifické povinnosti jsou pak dále stanoveny subjektům, které spravují systémy zařazené do kritické informační infrastruktury a správce významných informačních systémů. Konkrétně jde o povinnosti těchto orgánů a osob detekovat kybernetické bezpečnostní události, oznamovat vládnímu CERT výskyt kybernetických bezpečnostních incidentů a provádět opatření vydaná NBÚ. Vedle těchto povinností mají tyto orgány a osoby rovněž povinnost aplikovat bezpečnostní opatření splňující předepsaný standard.
Navrhovaná úprava bezprostředně nezasahuje do práva na informační sebeurčení člověka, neboť primárně nezasahuje do obsahové stránky komunikace a nezakládá ani přímé pravomoci státu direktivně zasahovat do běžného života informační společnosti – návrh zákona tedy nepředpokládá žádný státní zásah do soukromí uživatelů ani do jejich možností komunikovat prostřednictvím služeb informační společnosti.
Právo na informační sebeurčení člověka je návrhem zákona zpracováno jako hodnota, k jejíž ochraně návrh zákona primárně směřuje. V tomto případě má návrh zákona jasně vymezenou teleologii, která spočívá v zabezpečení kybernetického prostoru, 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[17)].
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 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 informační 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 (nedistributivních práv) České republiky a
- mezinárodních závazků České republiky.

Z výše uvedeného lze formulovat následující stručné závěry ohledně ústavní proporcionality návrhu zákona:

- *Test vhodnosti* – návrh zákona, 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 opatření představují nejúčinnější prostředky ochrany kybernetického prostoru. Návrh zákona tedy vychází z aktuálních poznatků praxe

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

v oboru ICT a vybírá nejefektivnější nástroje ochrany kybernetického prostoru při zachování minimální zátěže směrem k osobám soukromého práva.

- *Test potřebnosti* – provedenými studiemi nebylo zjištěno alternativní řešení, které by mohlo naplnit základní cíl záměru, tj. ochranu kybernetického prostoru. 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 kybernetického prostoru 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 případná opatření 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 zákon, jak uvedeno shora, přináší jen minimum povinností osobám soukromého práva, 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.

IV. Slučitelnost navrhované právní úpravy s mezinárodním právem a právem Evropské Unie

Problematika kybernetické bezpečnosti není komplexně řešena mezinárodním právem ani právem EU. Existuje zde však celá řada mezinárodních dokumentů upravujících partikulární aspekty kybernetické bezpečnosti, tj. problematiku služeb elektronických komunikací, oblast kritické infrastruktury a oblast ochrany soukromí v odvětví elektronických komunikací. Navrhovaná právní úprava 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 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.
Shora uvedené dokumenty se problematiky kybernetické bezpečnosti dotýkají pouze v širších souvislostech a do návrhu zákona o kybernetické bezpečnosti proto nejsou implementovány.
Evropská Komise zadala v březnu 2012 studii o kybernetické bezpečnosti, která byla publikována v červenci 2012 jako Special Eurobarometer 390/Wave EB77.2 – TNS Opinion & Social. V červenci 2012 rovněž Evropská komise zahájila veřejné konzultace k záměru legislativně upravit otázku kybernetické bezpečnosti v EU. Výsledkem je návrh směrnice Evropského parlamentu a rady o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v EU. Navrhovaná právní úprava je v plném souladu se základními legislativními tezemi ohledně plánovaného celoevropského systému detekce a ochrany před kybernetickými bezpečnostními incidenty. Návrh směrnice požaduje, aby každý členský stát jmenoval vnitrostátní orgán odpovědný za bezpečnost sítí a informačních systémů a zřídil skupinu pro reakci na počítačové hrozby, tzv. CERT. Tomu odpovídají ustanovení zákona, podle kterých bude působnost v oblasti kybernetické bezpečnosti vykonávat NBÚ a ustanovení zákona, podle nichž budou vytvořena dvě dohledová pracoviště, národní a vládní CERT, jejichž úkolem bude mimo jiné ochrana informačních a komunikačních systémů před kybernetickými incidenty. Návrh směrnice dále počítá s ukládáním povinností subjektům regulace, kterými budou orgány veřejné správy a tzv. hospodářské subjekty definované směrnicí. Tomu korespondují příslušná ustanovení návrhu zákona, který formuluje povinnosti pouze vybraným subjektům spravujícím specifické informační nebo komunikační systémy, a to v závislosti na jejich významu.
Podle návrhu Směrnice budou členské státy povinny zajistit, aby jejich orgány veřejné správy a hospodářské subjekty přijaly vhodná technická a organizační opatření k řízení bezpečnosti rizik jejich sítí a informačních systémů. Tato opatření by přitom měla vycházet z norem, respektive specifikací týkajících se bezpečnosti sítí a informací, které budou uvedeny v seznamu norem vypracovaným Evropskou komisí. Podle návrhu zákona budou orgány a osoby spravující informační nebo komunikační systémy zařazené do kritické informační infrastruktury nebo spravující významné informační systémy povinny zavádět za účelem zajištění bezpečnosti informací v informačních systémech a dostupnosti a spolehlivosti služeb a sítí v kybernetickém prostoru tzv. bezpečnostní opatření. Tato bezpečnostní opatření přitom

budou vycházet z mezinárodních standardů a měly by tak být v souladu se standardy stanovenými na základě směrnice prováděcími akty. Návrh směrnice dále předpokládá, že orgány veřejné správy a hospodářské subjekty budou povinny oznamovat odpovědnému orgánu incidenty, které budou mít významný dopad na bezpečnost jimi poskytovaných základních služeb a vnitrostátní odpovědný orgán bude disponovat pravomocí spočívající v oprávnění vydávat závazné pokyny orgánům veřejné správy a hospodářským subjektům. Podle návrhu zákona budou vybrané orgány a osoby povinny hlásit kybernetické bezpečnostní incidenty NBÚ nebo národnímu CERT a NBÚ bude oprávněn vydávat opatření ve formě nezávazného varování nebo závazných právních aktů formou rozhodnutí nebo opatření obecné povahy. Rovněž v této části je návrh zákona v souladu s příslušnými ustanoveními návrhu směrnice.
Navrhovaná právní úprava je rovněž v plném souladu s aktuálně připravovanými legislativními změnami shora uvedených sekundárních pramenů práva EU týkajících se okrajově věcné působnosti navrhované právní úpravy, konkrétně nařízení o ochraně osobních údajů (COM(2012) 11 final a nařízení o elektronické identifikaci a autentizaci elektronických transakcí na vnitřním trhu (COM(2012) 238/2).
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, Akční plán zemí G8 pro potírání „high-tech" zločinu a Strategie kybernetické bezpečnosti Evropské unie: Otevřený, bezpečný a chráněný kyberprostor ze dne 7. 2 2013.
Navrhovaná právní úprava je plně v souladu s mezinárodními smlouvami, jimiž je Česká republika vázána, a je plně slučitelná s předpisy EU.

V. Zhodnocení korupčních rizik

1. Přiměřenost

Předložený návrh zákona o kybernetické bezpečnosti je vyhotoven v intencích vládou schváleného věcného záměru zákona o kybernetické bezpečnosti a svým rozsahem je

přiměřený množině vztahů, které má upravovat. Oblast kybernetické bezpečnosti nebyla dosud regulována právními předpisy a do listopadu 2011 spadala pod gesci Ministerstva vnitra. Usnesením vlády č. 781 ze dne 19. října 2011 byl Úřad ustanoven gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast. Návrh zákona tak upravuje zcela novou materii a zakládá Úřadu kompetence, které doposud neměl, avšak v rozsahu nezbytném pro zajištění kybernetické bezpečnosti České republiky.

2. Efektivita

Efektivní implementace povinností stanovených předmětným návrhem zákona bude průběžně vyhodnocována Úřadem, který bude především pravidelně vyhodnocovat účinnost bezpečnostních opatření v závislosti na vývoji průmyslových standardů a standardizovaných postupů v rámci řízení bezpečnosti informací a obecně akceptovaných doporučených postupů (best practices), jakož i hodnotit efektivitu právní úpravy jako celku. V případě potřeby pak dojde k novelizaci předmětného zákona nebo jeho prováděcích právních předpisů. Kontrolu a případné vynucování dodržování povinností stanovených návrhem zákona, především kontrolu zavedení bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů a provádění opatření bude plošně vykonávat Úřad. Dodržování dílčí povinnosti (zavedení bezpečnostních opatření) uložené správcům významných informačních systémů bude kontrolováno Ministerstvem vnitra, které již v současné době vykonává kontrolu nad dodržováním právních předpisů upravujících oblast informačních systémů veřejné správy. Takto dělená pravomoc by měla přispět k vyšší účinnosti kontroly v oblasti kybernetické bezpečnosti.

3. Odpovědnost

Ústředním správním úřadem, do jehož působnosti spadá oblast kybernetické bezpečnosti, bude Úřad. Zákon jednoznačně stanoví jeho kompetence a postavení v této oblasti. Pouze dílčí oblast kontroly dodržování povinnosti spočívající v zavedení bezpečnostních opatření správci významných informačních systémů je svěřena Ministerstvu vnitra, do jehož působnosti již nyní spadá regulace informačních systémů veřejné správy.

4. Opravné prostředky

Návrh zákona ve spojení s obecnými právními předpisy upravujícími správní řízení a předpisy upravujícími výkon státní kontroly umožňuje orgánům a osobám účinnou obranu proti nesprávnému postupu orgánu veřejné správy a rovněž opravňuje orgány a osoby k podání řádných i mimořádných opravných prostředků proti závazným aktům vydaným Úřadem. Prokazatelné poučení o možnosti podat opravný prostředek pak vyplývá z obecného právního předpisu, správního řádu. Podle návrhu zákona bude Úřad oprávněn vydávat následující závazné právní akty, proti nimž lze podat tyto opravné prostředky:

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

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

c) Nápravné protiopatření – limity nápravných opatření jsou upraveny přímo v § 28 návrhu zákona. Obsah a rozsah nápravných opatření přitom musí respektovat zásadu proporcionality výslovně uvedenou v tomto ustanovení. Nápravná opatření lze vydat pouze v rámci výkonu kontroly podle kontrolního řádu (zákon č. 255/2012 Sb.), který obsahuje ustanovení chránící práva orgánu a osoby při výkonu kontroly (např. právo namítat podjatost kontrolujícího, právo podávat námitky).

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

5. Kontrolní mechanismy

Návrh zákona rozlišuje pět kategorií orgánů a osob, kterým v závislosti na důležitosti jejich informačních systémů nebo služeb a sítí elektronických komunikací ukládá explicitně stanovené povinnosti. Návrh zákona přitom jednoznačně stanoví odpovědnost správců informačních nebo komunikačních systémů za bezpečnost jejich systémů a tyto subjekty současně definuje jako orgány a osoby za účelem eliminace případných odpovědnostních sporů mezi správci a smluvními provozovateli těchto systémů.
Návrh zákona nastavuje funkční systém přezkoumávání rozhodnutí přijímaných na jeho základě (viz výše – možnost podat řádné i mimořádné opravné prostředky včetně možnosti soudního přezkumu). Návrh zákona dále stanoví skutkové podstaty správních deliktů spočívající v porušení nejdůležitějších povinností uložených tímto zákonem nebo na jeho základě. Sankce za správní delikty pak představují pokuty, jejichž výše je závislá na charakteru porušené povinnosti.

6. Korupční rizika

Návrh zákona o kybernetické bezpečnosti zakládá nové povinnosti jasně vymezenému okruhu subjektů, v jejichž zájmu je ochrana a zajištění bezpečného kybernetického prostoru. Nelze proto předpokládat, že by prvotní reakcí regulovaných subjektů byla snaha o neplnění zákonem nebo na jeho základě stanovených povinností, neboť je zejména v jejich zájmu zabezpečení vlastních informačních systémů a služeb a sítí elektronických komunikací před kybernetickými bezpečnostními incidenty.
Povinnosti, které předmětný zákon primárně stanoví, spočívají v zavedení bezpečnostních opatření, hlášení kybernetických bezpečnostních incidentů, hlášení kontaktních údajů a provádění opatření.
Bezpečnostní opatření vychází z principů mezinárodní normy ISO/IEC 27001, tj. z bezpečnostních pravidel, jimiž se již v současné době většina subjektů, které budou podléhat regulaci předmětného návrhu zákona, řídí. Zavedení bezpečnostních opatření přitom nebude

podléhat (na rozdíl od předmětné normy) žádnému certifikačnímu nebo akreditačnímu řízení. Orgány a osoby budou vést o zavedených bezpečnostních opatřeních příslušnou bezpečnostní dokumentaci a jejich aplikace bude podléhat pouze kontrole ze strany Úřadu, respektive Ministerstva vnitra. Vzhledem k výši sankcí za nezavedení bezpečnostních opatření, nevedení bezpečnostní dokumentace nebo neprovedení nápravných opatření vydaných v rámci kontroly, se nepředpokládá v této oblasti vznik prostředí podněcujícího ke korupčnímu jednání ať už ze strany účastníků řízení nebo úředních osob.
Povinnost hlásit kybernetické bezpečnostní incidenty je založena za účelem pomoci orgánům a osobám v případě výskytu kybernetického bezpečnostního incidentu a zároveň s cílem získat informace o takovém incidentu pro jeho další analýzu Úřadem, respektive národním CERT. Úřad zde je v podstatě v roli pasivního příjemce s tím, že při příjmu hlášení kybernetických bezpečnostních incidentů nerozhoduje o právech a povinnostech orgánů a osob. Prostor pro vznik korupčního jednání zde tak reálně nemůže vzniknout.
Oproti tomu povinnost aplikovat reaktivní a ochranná opatření vydaná Úřadem by mohla být potenciální příčinou vzniku korupčního prostředí. Vzhledem ke skutečnosti, že tyto dva druhy opatření budou vydávaná formou rozhodnutí nebo opatření obecné povahy, které budou ukládat orgánům a osobám povinnosti, jež mohou představovat zvýšené náklady na bezpečnost jejich informačních systémů nebo služeb a sítí elektronických komunikací, případně omezení jejich činnosti a s tím spojené ztráty, lze předpokládat zvýšený zájem orgánů a osob na vydání takových opatření, která jejich případné finanční ztráty eliminují. V této rovině by tak některé orgány a osoby (především podnikatelské subjekty) mohly vyvíjet snahu o ovlivnění některých opatření. Na řešení daného kybernetického bezpečnostního incidentu se však vždy bude podílet několik zaměstnanců Úřadu s odpovídající odbornou kvalifikací, což by mělo jednak přispět k vydání efektivních opatření, jakož i ke ztížení možného úmyslného ovlivňování jejich vydávání. Řešení kybernetických bezpečnostních incidentů je pak dále postaveno na porovnání vydaného opatření s jeho výsledkem po provedení orgánem a osobou, která je povinna zaslat Úřadu oznámení o provedení reaktivního opatření a jeho výsledek. Tímto opatřením tak dojde k výraznému zvýšení efektivity opatření a ke stanovení systému kontroly.
Určitý prostor pro korupční jednání by mohl vzniknout v oblasti rozhodování o správních deliktech při porušení povinností stanovených návrhem předmětného zákona nebo na jeho základě. Jak už však bylo uvedeno shora, vzhledem k výši sankcí za správní delikty se nepředpokládá v této oblasti vznik prostředí podněcujícího ke korupčnímu jednání ať už ze strany účastníků řízení nebo úředních osob.

7. Transparence a otevřená data

Návrh zákona obecně předpokládá zveřejňování údajů týkajících se kybernetické bezpečnosti. Na internetových stránkách vládního CERT jsou již nyní zveřejňovány údaje o hrozbách a zranitelnostech v oblasti kybernetické bezpečnosti. Návrh zákona explicitně stanoví povinnost Úřadu zveřejňovat opatření vydávané ve formě varování na internetových stránkách vládního CERT. Rovněž tak i reaktivní a ochranná opatření vydaná ve formě opatření obecné povahy budou zveřejňována na těchto internetových stránkách. Dále se předpokládá zveřejňování statistických údajů o kybernetických bezpečnostních incidentech, jakož i obsahu veřejnoprávní smlouvy uzavřené s provozovatelem národního CERT, s výjimkou těch částí, jejichž zveřejnění by bylo v rozporu s právními předpisy (např. z důvodu ochrany obchodního tajemství). Naopak z důvodu ochrany oprávněných zájmů orgánů a osob, jakož i zajištění účinnosti vydaných opatření nebude Úřad některé údaje povinen poskytovat (např. údaje, z nichž by bylo možné identifikovat orgán a osobu, která ohlásila kybernetický bezpečnostní incident) Ty údaje, které nebude možné poskytnout ke zveřejnění, budou chráněny

v evidencích, které povede Úřad a odpovídajícím způsobem ochráněny včetně institutu povinnosti mlčenlivosti pro zaměstnance Úřadu, kteří se podíleli na řešení KBI.
Údaje, které budou na základě návrhu zákona zveřejňovány, budou zveřejňovány ve formátech otevřených dat, s nimiž lze bez dalšího dále pracovat.
Postupy, procesy a sankce obsažené v navrhované nové právní úpravě vycházejí ze zahraničních poznatků v oblasti kybernetické bezpečnosti, z vývoje budování vládních pracovišť týmu rychlé reakce na počítačové incidenty, jakož i z aktuálních bezpečnostních potřeb zacílených na ochranu kybernetického prostoru. Navrhovanou právní úpravu, jejíž procesní postupy se až na odůvodněné odchylky řídí správním a kontrolním řádem, tak lze ve srovnání se stávající legislativou označit za přiměřenou.

B. Zvláštní část

K § 1

Věcná působnost zákona je vymezena obecně pro oblast kybernetické bezpečnosti s výjimkou informačních a komunikačních systémů nakládajících s utajovanými informacemi. Pojmu kybernetické bezpečnosti je užito k odlišení od pojmu informační bezpečnosti resp. počítačové bezpečnosti a ke zdůraznění specifického zaměření zákona na ochranu funkčnosti síťového prostředí umožňujícího vznik, zpracování, uchovávání a komunikaci informací, které je tvořeno informačními systémy a službami a sítěmi elektronických komunikací.
Specifické omezení působnosti zákona vztahující se k informačním a komunikačním systémům nakládajícím s utajovanými informacemi je důsledkem toho, že úprava povinných bezpečnostních parametrů těchto systémů včetně navazujících právních povinností, kompetencí orgánů veřejné moci, kontroly, sankcí apod., je komplexně provedena zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Do této právní úpravy není v současné době důvod zasahovat, neboť tyto systémy podléhají certifikaci, tj. vyšší formě regulace.

K § 2

Pojem kybernetického prostoru je definován jako informační prostředí k realizaci informačních transakcí, které je vytvořeno technologiemi, jejichž definice a podmínky užívání upravují zvláštní zákony, tj. informačními systémy, službami a sítěmi elektronických komunikací. Jedná se přitom i o takové informační systémy, služby a sítě elektronických komunikací, které nejsou připojeny k veřejné síti, tj. k internetu.
Definice pojmu kritická informační infrastruktura vychází z právních předpisů upravujících oblast krizového řízení. Vychází se přitom z předpokladu, že kritická informační infrastruktura bude součástí kritické infrastruktury, která je vymezena zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) ve znění pozdějších předpisů („dále jen krizový zákon“)[18)]. Aby mohl být určitý informační systém nebo služba a síť elektronických komunikací zařazena do kritické informační infrastruktury, bude muset splnit definiční kritéria kritické infrastruktury, jakož i prvku kritické infrastruktury[19)], vymezené krizovým zákonem a dále pak i průřezová[20)] a odvětvová kritéria stanovená nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. V odvětvových kritériích pro určení prvku kritické infrastruktury se předpokládá doplnění bodu VI. „Komunikační a informační systémy“ o oblast kybernetické bezpečnosti, v níž budou stanovena odvětvová kritéria pro určení daného informačního systému, služby nebo sítě elektronických komunikací kritickou informační infrastrukturou. Těmito kritérii bude především skutečnost, že daný informační systém, služba nebo síť elektronických

---

[18)] Kritickou infrastrukturou se rozumí prvek kritické infrastruktury nebo systém prvků kritické infrastruktury narušení, jehož funkce by mělo závažný dopad na bezpečnost státu, zabezpečení základních životních potřeb obyvatelstva, zdraví osob nebo ekonomiku státu.

[19)] Prvkem kritické infrastruktury se rozumí stavba, zařízení, prostředek nebo veřejná infrastruktura určená podle průřezových a odvětvích kritérií, která jsou stanovena nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.

[20)] Průřezovým kritériem pro určení prvku kritické infrastruktury je hledisko

a) obětí s mezní hodnotou více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací po dobu delší než 24 hodin,

b) ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo

c) dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.

komunikací bude zajišťovat provoz již určeného prvku kritické infrastruktury a bude pro tento prvek nenahraditelný, anebo že daný informační systém, služba nebo síť elektronických komunikací bude zajišťovat jinou významnou činnost nebo službu sám o sobě, aniž by byl spojen s již určeným prvkem. Pokud jednotlivé informační systémy, služby a sítě elektronických komunikací splní všechny shora uvedené podmínky, budou určeny prvkem kritické infrastruktury standardním postupem podle krizového zákona. Pokud bude provozovatelem daného prvku organizační složka státu, bude prvek určen usnesením vlády, v ostatních případech pak opatřením obecné povahy vydaným NBÚ a tímto postupem se tyto systémy, služby nebo sítě stanou kritickou informační infrastrukturou podle zákona o kybernetické bezpečnosti.
Pojem bezpečnosti informací vychází ve své definici z významu tohoto pojmu v odvětví informačních věd a týká se důvěrnosti (tj. diskrece), jednoty (tj. integrity) a dostupnosti informace. Pojem se netýká obsahu informace, ale pouze funkčnosti prostředí, v němž je informace tvořena, zpracovávána, uchovávána a komunikována. To odpovídá principu technologické neutrality, na němž zákon spočívá a má za následek důsledné vyčlenění kriteria obsahu informací z věcné působnosti zákona.
Pojem významného informačního systému odkazuje k systémům, jejichž správcem je orgán veřejné moci a které mají zásadní význam pro fungování veřejné správy. V tomto případě není použito rozdělení na informační a komunikační systém, neboť z definice plyne, že do pojmu informačního systému spadá vždy i jeho vnitřní komunikační složka. Významným informačním systémem podle zákonné definice může být i systém, který neodpovídá definici obsažené v § 3 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, jehož správcem je orgán veřejné moci a jehož důležitost odůvodnila jeho zařazení mezi významné informační systémy.
Pojem správce informačního, respektive komunikačního systému je definován obdobně jako v zákoně č. 365/2000 Sb., přičemž definice je založena na faktickém stanovení účelu příslušného systému a podmínek jeho provozování. Pro účely tohoto zákona je třeba vymezit pojem správce, neboť ten bude především orgánem a osobou, na níž bude dopadat právní regulace. Pokud by tento pojem vymezen nebyl, mohly by vznikat interpretační obtíže s tím, kdo ponese odpovědnost za neplnění povinností stanovených tímto zákonem. Orgánem a osobu by tak podle navrhované definice měl být ten, kdo určuje účel daného systému, respektive podmínky jeho provozování (typicky jeho vlastník), nikoliv ten, kdo se smluvně zavázal k provozu daného systému.
Pojem významné sítě je definován tak, aby zahrnoval páteřní sítě, jejichž prostřednictvím je kybernetický prostor na území České republiky propojen do zahraničí. Vzhledem k důležitosti kritické informační infrastruktury je jako významná síť označena touto legální definicí též síť, která sama o sobě není prvkem kritické informační infrastruktury, ale která zajišťuje připojení kritické informační infrastruktury ke kybernetickému prostoru. Relativně menší bezpečnostní expozice významné sítě v porovnání s kritickou informační infrastrukturou se projevuje v dalších ustanoveních zákona omezeným katalogem povinností ukládaných zákonem jejich správcům.

K § 3

Vymezení okruhu orgánů a osob je částečně založeno na užití stávajících pojmů zákona o elektronických komunikacích.
Orgány a osoby lze v zásadě rozdělit do dvou skupin. První z nich tvoří poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací vymezené v zákoně o elektronických komunikacích, a subjekty zajišťující tzv. významné sítě, na něž bude regulace tohoto zákona dopadat pouze minimálně, a to v rozsahu povinnosti oznámit kontaktní údaje a jejich změny národnímu CERT, respektive v povinnosti provádět opatření

za stavu kybernetického nebezpečí. Subjekty zajišťující významné sítě budou nadto povinny detekovat kybernetické bezpečnostní události a hlásit kybernetické bezpečnostní incidenty. Druhou skupinu pak budou tvořit správci informačních systémů kritické informační infrastruktury, správci komunikačních systémů kritické informační infrastruktury, a správci významných informačních systémů, na něž bude dopadat regulace tohoto zákona v plném rozsahu. Tato skupina orgánů a osob tak bude povinna oznámit kontaktní údaje a jejich změnu vládnímu CERT, zavést bezpečnostní opatření, detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty a provádět opatření.
Toto rozdělení orgánů a osob s následným omezením rozsahu zákonných povinností na nezbytné minimum v závislosti na významnosti informačních a komunikačních systémů, které orgány a osoby spravují, odpovídá principu minimalizace státních zásahů, na němž je tento zákon založen. Shora uvedená klasifikace orgánů a osob má kaskádovitý charakter. Typicky tedy např. subjekt zajišťující významnou síť, která bude zařazena do kritické informační infrastruktury, bude mít ve vztahu k této síti na úseku kybernetické bezpečnosti povinnosti odpovídající správci komunikačního systému zařazeného do kritické informační infrastruktury.

K § 4

Návrh ustanovení zakládá povinnost vybraným typům orgánů a osob zavést a provádět v jimi spravovaných informačních a komunikačních systémech bezpečnostní opatření a vést o tom příslušnou bezpečnostní dokumentaci. Účelem zavedení bezpečnostních opatření je zajištění určité úrovně bezpečnosti informačních a komunikačních systémů. Zavedení standardů má tak zejména preventivní význam, neboť systém, v němž budou příslušná bezpečnostní opatření aplikována, by měl být odolnější vůči kybernetickým útokům a současně by měl být připraven na efektivní zvládání kybernetických bezpečnostních událostí a incidentů.
Výběr typů orgánů a osob podléhajících povinnosti zavést bezpečnostní opatření je veden zákonným principem minimalizace zásahu do autonomie vůle orgánů a osob. Ze zákona tak plyne povinnost k zabezpečení vlastních informačních a komunikačních systémů jen těm osobám soukromého práva a orgánům veřejné moci, jejichž systémy mají zásadní význam pro kybernetickou bezpečnost České republiky, tj. správcům informačních systémů nebo komunikačních systémů kritické informační infrastruktury a správcům významných informačních systémů.

K § 5

Toto ustanovení podrobněji specifikuje obsah bezpečnostních opatření, k jejichž zavedení mají povinnost správci informačních nebo komunikačních systémů kritické informační infrastruktury a správci významných informačních systémů. Bezpečnostní opatření jsou rozdělena do dvou skupin, a to na organizační opatření a technická opatření. Organizační opatření zahrnují povinnost pořizovat plány a aplikovat řídící, organizační a kontrolní postupy k ošetření procesů souvisejících se zaváděním a provozem informačních a komunikačních systémů spravovaných orgány a osobami. Technická opatření specifikují jednotlivé okruhy technických řešení týkajících se zabezpečení informačních a komunikačních systémů včetně detekce, vyhodnocování a řešení kybernetických bezpečnostních událostí a incidentů. K povinnostem zavést bezpečnostní opatření se váže též povinnost zpracovat jejich bezpečnostní dokumentaci.

K § 6

Z důvodu zachování právní jistoty orgánů a osob je třeba dále jednotlivé komponenty bezpečnostních opatření konkretizovat. Rovněž je třeba zajistit, aby byla tato konkretizace

dostatečně flexibilní ve vztahu k budoucímu vývoji techniky. V tomto ustanovení je tedy provedeno zmocnění k realizaci podmíněné omezené legislativní kompetence správní orgánu, tj. v tomto případě NBÚ, ke specifikaci obsahu a rozsahu bezpečnostních opatření, přičemž se předpokládá stanovení úrovně bezpečnostních opatření v závislosti na důležitosti a bezpečnostní expozici příslušné kategorie informačních nebo komunikačních systémů. V zásadě platí, že správci informačních nebo komunikačních systémů kritické informační infrastruktury budou v těchto systémech zavádět bezpečnostní opatření v širším rozsahu než správci významných informačních systémů, u nichž bude rozsah zavedení bezpečnostních opatření v jimi spravovaných systémech užší.
Rovněž je tímto ustanovením založeno právo a povinnost NBÚ upravit prováděcím předpisem obsah a strukturu bezpečnostní dokumentace. Účelem technické specifikace náležitostí bezpečnostní dokumentace je usnadnit orgánům a osobám její zpracování a zefektivnit její následné užití včetně kontroly.
Toto ustanovení dále zmocňuje NBÚ k vydání prováděcího právního předpisu, jímž budou upraveny významné informační systémy a jejich určující kritéria.

K § 7

Rozdělení skutkových stavů, na něž zákon reaguje konstrukcí specifických povinností, na kybernetické bezpečnostní události a kybernetické bezpečnostní incidenty, sleduje účel odlišení potenciálně problematických situací vykazujících stanovené formální znaky a situací, které na základě vyhodnocení formálních podmínek v kontextu aktuálních okolností, představují reálné bezpečnostní riziko. Zatímco kybernetickou bezpečnostní událostí je událost bez reálného negativního následku pro daný komunikační nebo informační systém, kybernetickým bezpečnostním incidentem je pak samotné narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací, tj. narušení informačního nebo komunikačního systému s negativním dopadem. Detekční povinnosti zákon váže ke kybernetickým bezpečnostním událostem, oproti tomu povinnosti reagovat formou hlášení příslušnému pracovišti CERT resp. formou provedení opatření jsou navázány až k situaci, kdy je příslušná událost vyhodnocena orgánem a osobu jako kybernetický bezpečnostní incident.
Toto ustanovení zakládá vybraným orgánům a osobám detekční povinnost vzhledem ke kybernetickým bezpečnostním událostem, které se vyskytly v jejich významné síti, informačním nebo komunikačním systému kritické informační infrastruktury anebo ve významném informačním systému. Povinnost hlásit kybernetický bezpečností incident je pak založena v následujícím ustanovení.
Cizojazyčný pojem „incident“ byl použit z důvodu zachování souladu zákonného pojmového aparátu s mezinárodní technickou terminologií. Ze stejného důvodu je použit i pojem „detekovat,“ jehož český ekvivalent, tj. „odhalovat“ nebo „zjišťovat“ navíc není sémanticky zcela adekvátní.

K § 8

Navržené ustanovení zakládá vybraným orgánům a osobám povinnost hlásit kybernetické bezpečnostní incidenty. Účelem tohoto ustanovení je umožnit NBÚ (respektive jeho součásti – vládnímu CERT) a národnímu CERT vykonávat jejich primární funkci, tj. koordinovat ochranu kritické informační infrastruktury, významných informačních systémů a významných sítí.
Vybrané orgány a osoby budou povinny hlásit kybernetické bezpečnostní incidenty, které se vyskytly v jejich významné síti, informačním nebo komunikačním systému kritické informační infrastruktury anebo ve významném informačním systému, bezodkladně po jejich zjištění, tj. po vyhodnocení kybernetické bezpečnostní události jako kybernetického

bezpečnostního incidentu. Toto ustanovení je komplementární úpravou k existujícím informačním a ohlašovacím povinnostem, tj. splněním ohlašovací povinnosti podle toho ustanovení se orgány a osoby nezbavují informačních povinností založených jinými právními předpisy např. zákonem o elektronických komunikacích.
Vzhledem k zásadní důležitosti informačních a komunikačních systémů zařazených do kritické informační infrastruktury a významných informačních systémů jsou jejich správci povinni hlásit výskyt kybernetických bezpečnostních incidentů NBÚ, respektive jím provozovanému vládnímu CERT. Kybernetické bezpečnostní incidenty ve významných sítích jsou vybrané orgány a osoby povinny hlásit národnímu CERT.
Účelem tohoto ustanovení je založit povinnost hlásit kybernetické bezpečnostní incidenty detekované na základě povinnosti založené v předchozím ustanovení. Tato ustanovení však nevylučují možnost hlášení kybernetických bezpečnostních událostí nebo možnost obracet se na národní CERT nebo NBÚ (respektive jeho součást – vládní CERT) s podněty anebo jinými oznámeními souvisejícími s kybernetickou bezpečností nemajícími charakter kybernetického bezpečnostního incidentu.
Vzhledem k tomu, že je třeba upravit technické podrobnosti k výkonu povinnosti hlásit kybernetické bezpečnostní incidenty, tj. zejména je třeba v návaznosti na technický vývoj a na aktuální poznatky z oboru informatiky průběžně definovat konkrétní technické parametry typů a kategorií hlášených kybernetických bezpečnostních incidentů, jakož i stanovovat technické náležitosti a způsob jednotlivých hlášení, je v tomto ustanovení rovněž provedeno zákonné zmocnění NBÚ k vydání prováděcího předpisu.

K § 9

Účelem tohoto ustanovení je založit právo a povinnost NBÚ vést evidenci kybernetických bezpečnostních incidentů. Struktura údajů taxativním výčtem je zvolena tak, aby umožňovala evidovat údaje nutné k následné formální a obsahové analýze kybernetických bezpečnostních incidentů. Výstupy této analýzy budou sloužit jako důležitý podklad pro činnosti NBÚ v oblasti kybernetické bezpečnosti upravenými tímto zákonem.
Údaje v evidenci kybernetických bezpečnostních incidentů mají velkou vypovídací hodnotu o činnosti pracovišť CERT a o kybernetické bezpečnostní situaci České republiky, jakož i o jednotlivých orgánech a osobách. Současně mohou být tyto údaje vysoce důležité pro výkon funkcí orgánů veřejné moci, národního CERT nebo pro činnost zahraničních spolupracujících soukromoprávních nebo veřejnoprávních institucí působících v oblasti kybernetické bezpečnosti. Předávání údajů z evidence kybernetických bezpečnostních incidentů je proto zákonem regulováno, respektive omezeno. Orgánům veřejné moci (typicky např. orgánům činným v trestním řízení, Českému telekomunikačnímu úřadu, zpravodajským službám) lze údaje z evidence kybernetických bezpečnostních incidentů poskytnout pouze pro plnění úkolů v rámci jejich působnosti. Předávání těchto údajů dalším subjektům, (např. národnímu CERT, zahraničním subjektům působícím v oblasti kybernetické bezpečnosti) pak lze na základě správního uvážení NBÚ, a to pouze v rozsahu nezbytném pro ochranu kybernetického prostoru.
Nezbytnou zákonnou podmínkou nakládání s evidencí podle navrhovaného ustanovení bude i vedení elektronických záznamů, které umožní určit a ověřit, kdy, kým a z jakého důvodu byly údaje shromážděné podle § 10 zpracovány, vč. toho, jak dlouho a pro jaký účel byly uchovávány, nevyjímaje protokoly o likvidaci. Jedná se účinné a technologicky přiměřené opatření k zabezpečení ochrany osobních údajů stanovené v § 13 zákona o ochraně osobních údajů. Opatření vytváří podmínky pro případný dozor a vymahatelnost zákonné povinnosti zachovávat mlčenlivost.

K § 10

Návrh ustanovení upravuje individuální povinnost mlčenlivosti zaměstnanců NBÚ vzhledem k údajům tvořícím evidenci kybernetických bezpečnostních incidentů. Účelem tohoto ustanovení je zamezit možnému úniku těchto údajů prostřednictvím zaměstnanců NBÚ, kteří s nimi budou přicházet do styku, a tím umožnit předávání a další užití těchto údajů výlučně způsoby upravenými v předchozích ustanoveních. V odůvodněných případech je ředitel NBÚ oprávněn zbavit zaměstnance mlčenlivosti, a to ve vztahu ke konkrétně určeným údajům a ke konkrétním způsobům jejich dalšího užití.

K § 11

Ustanovení upravuje definici opatření jako součásti systému k zajištění kybernetické bezpečnosti. Definice opatření je provedena za užití obsahového kriteria, tj. účelu ochrany kybernetického prostoru před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení kybernetického bezpečnostního incidentu, který již nastal.

Cílem takto stanovené struktury opatření je pokrýt jednak formou varování potřebu oficiálního preventivního působení NBÚ vzhledem k aktuálním kybernetickým bezpečnostním hrozbám ještě před tím, než se tyto hrozby projeví v kybernetickém prostoru. Smyslem reaktivních opatření pak je působit k dosažení smyslu a účelu zákona v situaci trvajícího kybernetického bezpečnostního incidentu a účelem ochranných opatření je dodatečně reagovat na zkušenosti z řešení nastalých kybernetických bezpečnostních incidentů.

Zákon ukládá orgánům a osobám povinnost provádět reaktivní a ochranná opatření. Orgány a osoby jsou vzhledem k této povinnosti rozděleny do dvou skupin, přičemž bezprostředně tato povinnost zavazuje správce informačních a komunikačních systémů zařazených do kritické informační infrastruktury a správce významných informačních systémů, tj. subjekty zajišťující chod informačních systémů, služeb a sítí vitálně důležitých pro fungování základních společenských funkcionalit státu. Ostatní orgány a osoby, tj. poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací včetně subjektů zajišťujících významné sítě, mají povinnost provádět reaktivní opatření jen výjimečně, a to za vyhlášeného stavu kybernetického nebezpečí anebo za nouzového stavu.

Rozdělení orgánů a osob vzhledem k povinnostem provádět reaktivní a ochranná opatření odpovídá principu minimalizace zásahu do autonomie vůle orgánů a osob a zakládá možnost NBÚ autoritativně regulovat chování orgánů a osob jen v nezbytně nutné míře. Za běžné kybernetické bezpečnostní situace by totiž k ochraně vitálních zájmů státu na fungování základních funkcionalit informační společnosti před kybernetickými bezpečnostními incidenty měla postačit implementace opatření správců informačních nebo komunikačních systémů kritické informační infrastruktury anebo správců významných informačních systémů. Až v případě, že dojde k výjimečné kybernetické bezpečnostní situaci, kterou nebude možno řešit standardními prostředky zákona, a v jejímž důsledku bude vyhlášen stav kybernetického nebezpečí nebo nouzový stav, je důvod zavázat k dodržování opatření stanovených NBÚ též ostatní orgány a osoby.

K § 12

Účelem varování podle tohoto ustanovení je oficiální publikace informací o bezpečnostní hrozbě, tj. preventivní informování orgánů a osob. Vzhledem k technickému charakteru některých kybernetických bezpečnostních hrozeb lze očekávat, že v některých případech bude možno takovou hrozbu ze strany NBÚ po obdržení informací o její existenci pro účely okamžitého vydání varování pouze popsat. Bude-li mít NBÚ k dispozici též informace o technickém řešení, může tyto informaci připojit k varování.

Varování bude publikováno prostřednictvím internetových stránek NBÚ (respektive jeho součásti – vládního CERT), aby byla zajištěna informovanost dotčených subjektů, včetně široké veřejnosti. Orgánům a osobám bude varování rovněž oznamováno formou kontaktních údajů, které mají orgány a osoby povinnost hlásit do evidence kontaktních údajů.

K § 13

Účelem reaktivního opatření je okamžitá reakce na výskyt kybernetického bezpečnostního incidentu. Obsahem opatření tedy mohou být povinnosti provést konkrétní úkony nutné k odvrácení kybernetického bezpečnostního incidentu nebo ke zmírnění jeho následků.

Zákon rozlišuje dvě formy reaktivních opatření, a to rozhodnutí a opatření obecné povahy. Smyslem tohoto dělení je pokrýt oba typické případy vyskytující se při ochraně před kybernetickými bezpečnostními incidenty. První možností je výskyt kybernetického bezpečnostního incidentu v určitém informačním nebo komunikačním systému. Reaktivní opatření lze v takovém případě vydat formou rozhodnutí konkrétně specifikujícím povinnosti pro určeného adresáta – orgán nebo osobu. Druhou možností je výskytu incidentu, jehož rozsah je větší nebo jehož rozsah nelze kvůli složitosti incidentu nebo jeho rychlému vývoji přesně určit – takový incident pak je možno řešit vydáním reaktivního opatření formou opatření obecné povahy, v němž budou specifikovány konkrétní povinnosti k jeho odvrácení neurčitému okruhu orgánů a osob definovanému za užití generických znaků odpovídajících jeho charakteru.

Charakter kybernetických bezpečnostních incidentů vyžaduje k úspěšnosti reaktivního opatření reakci v co nejkratším čase. Jakákoli časová prodleva, byť v řádu hodin, může znamenat exponenciální rozvoj kybernetického bezpečnostního incidentu a násobení jeho škodlivého účinku. Z tohoto důvodu je explicitně stanoveno, že rozhodnutí je prvním úkonem ve věci, současně je zákonem speciálně upraven způsob doručování takového rozhodnutí a jeho vykonatelnost a dále je výslovně založena možnost vydání rozhodnutí v řízení na místě podle správního řádu. Z téhož důvodu nelze přiznat odkladný účinek rozkladu podanému proti rozhodnutí.

Z důvodu potřeby zpětné vazby pro vyhodnocení efektivnosti vydaných opatření se formuluje orgánům a osobám povinnost informovat NBÚ o provedených opatřeních a o jejich účinku. Pro zjednodušení této povinnosti a nezatěžování orgánů a osob přílišnými administrativními povinnostmi pak NBÚ stanoví prováděcím právním předpisem náležitosti tohoto oznámení.

K § 14

Důvodem vydání ochranného opatření je nutnost reagovat na vyřešený kybernetický bezpečnostní incident a na základě získaných zkušeností obecně zvýšit kvalitu ochrany informačních systémů, služeb a sítí elektronických komunikací u orgánů a osob. Vzhledem k tomu, že ochranné opatření směřuje k obecnému zvýšení rezistence kybernetického prostoru vůči kybernetickým bezpečnostním incidentům, je vydáváno formou opatření obecné povahy, kterým je možno uložit konkrétní povinnosti (tj. povinnosti vedoucí ke zvýšení ochrany před určitým typem kybernetického bezpečnostního incidentu) neurčitému okruhu subjektů. Okruh adresátů tedy bude v tomto případě určen podle toho, u kterých orgánů a osob spadajících pod možný rozsah osobní působnosti ochranného opatření je nutno zlepšení ochrany realizovat, vždy však půjde o orgány a osoby zavádějící standardizaci, tj. o správce informačních nebo komunikačních systémů kritické informační infrastruktury anebo o správce významných informačních systémů.

Oproti bezpečnostním opatřením se v tomto případě jedná o řešení prováděné v bezprostřední návaznosti na poznatky získané řešením konkrétního kybernetického bezpečnostního incidentu. Ochranného opatření tedy bude použito v situaci, kdy nelze z legislativně-technických důvodů realizovat požadavek na zvýšení úrovně zabezpečení informačních

systémů, sítí nebo služeb elektronických komunikací formou aktualizace prováděcích předpisů stanovících technické parametry bezpečnostních opatření.

K § 15

Toto ustanovení je společné pro opatření obecné povahy, jejichž prostřednictvím se vydávají reaktivní nebo ochranná opatření. Z důvodu naléhavé nutnosti reagovat na probíhající nebo vyřešený kybernetický bezpečnostní incident v co nejkratším čase je upravena účinnost těchto opatření obecné povahy okamžikem jeho vyvěšení na úřední desce NBÚ, přičemž vydání těchto opatření obecné povahy nebude předcházet řízení o návrhu opatření obecné povahy podle § 172 správního řádu, při němž by mohly být proti návrhu podávány oprávněnými orgány a osobami námitky nebo připomínky. Orgánům a osobám je oprávnění uplatnit připomínky podle § 172 odst. 4 správního řádu modifikováno, a to tak, že budou oprávněny podat připomínky směřující přímo proti vydanému opatření obecné povahy, a to ve lhůtě 30 dnů od jeho vyvěšení na úřední desce NBÚ. V případě vyhodnocení připomínek jako důvodných, lze příslušné opatření obecné povahy změnit nebo zrušit.

Z důvodu zajištění co možná nejrychlejšího a nejefektivnějšího informování orgánů a osob o opatřeních vydaných formou opatření obecné povahy NBÚ vyrozumí orgány a osoby o vydání těchto opatření prostřednictvím kontaktních údajů, které mají orgány a osoby povinnost hlásit do evidence kontaktních údajů.

K § 16

Návrh ustanovení vymezuje kontaktní údaje orgánů a osob, upravuje podmínky jejich evidence vedené NBÚ a notifikační povinnost orgánů a osob. Poskytovatelé služeb elektronických komunikací, subjekty zajišťující sítě elektronických komunikací a subjekty zajišťující významné sítě jsou povinny oznamovat kontaktní údaje a jejich změny provozovateli národního CERT. Správci informačních a komunikačních systémů kritické informační infrastruktury a správci významných informačních systémů pak tyto údaje oznamují NBÚ. Vzhledem k tomu, že za stavu kybernetického nebezpečí se okruh orgánů a osob, které mohou být povinny provádět reaktivní a ochranná opatření, rozšiřuje též o osoby, které kontaktní údaje oznamují provozovateli národního CERT, upravuje se pro tento případ předání kontaktních údajů těchto osob NBÚ.

Institut kontaktních údajů slouží kromě jmenovité evidence orgánů a osob též ke komunikaci neformálních informací, oficiálních informací (např. varování) a závazných individuálních právních aktů vydávaných NBÚ (ochranných a reaktivních opatření). Komunikace prostřednictvím kontaktních údajů má zajistit nikoli jen formální informovanost orgánů a osob, ale i skutečný kontakt pracovišť CERT na konkrétní pracovníky fakticky odpovídající u orgánů a osob za otázky kybernetické bezpečnosti – prostřednictvím těchto kontaktních údajů tedy bude možno vedle oficiální komunikace řešit též neformální kontakt výkonných pracovníků orgánů a osob s pracovišti CERT, běžnou neformální metodiku, technické konzultace apod.

S ohledem na právní úpravu základních registrů, podle které není žádný orgán veřejné moci až na zákonem formulované výjimky oprávněn vyžadovat od osob referenční údaje vedené v základních registrech, byly z notifikační povinnosti orgánů a osob oznamujících kontaktní údaje NBÚ vyňaty změny referenčních údajů evidovaných v základních registrech.

Vzhledem k tomu, že je třeba zajistit efektivní zpracování velkého množství kontaktních údajů orgánů a osob, počítá zákon s vydáním formulářového vzoru oznámení kontaktních údajů prováděcím právním předpisem, který bude reflektovat shora uvedenou úpravu základních registrů, tj. nebude vyžadovat od orgánů a osob referenční údaje vedené v základních registrech.

K § 17

Toto ustanovení definuje instituci národního CERT a vymezuje jeho činnost. Zákon předpokládá, že národní CERT bude provozován zpravidla osobou soukromého práva, která uzavře s NBÚ veřejnoprávní smlouvu, a bude sloužit zejména jako společné kontaktní a koordinační místo pro osoby soukromého práva. Vůči národnímu CERT budou poskytovatelé služeb elektronických komunikací, subjekty zajišťující sítě elektronických komunikací a subjekty zajišťující významné sítě realizovat svou zákonnou notifikační povinnost.

Model standardně soukromoprávního výkonu funkcí národního CERT usnadňuje komunikaci mezi národním CERT a orgány a osobami využívajícími jej povinně jako kontaktní místo. Tyto orgány a osoby budou mít totiž rovněž zpravidla soukromoprávní povahu. Národní CERT se bude také moci zapojit do mezinárodních sítí obdobných soukromoprávních pracovišť typu CERT a těžit z poznatků, které se v rámci těchto sítí neformálně předávají.

Předpokládaný soukromoprávní charakter národního CERT je vzhledem ke smyslu a účelu zákona vhodný i z toho důvodu, že provozovatel národního CERT může, jedná-li se o osobu soukromého práva, vyvíjet iniciativně k dosažení účelu zákona též aktivity na základě tacitního dovolení, tj. libovolné aktivity podle své soukromé vůle neporušující zákonné povinnosti. Provozovatel národního CERT tak bude moci například poskytovat metodickou a informační pomoc i subjektům stojícím mimo osobní působnost zákona, tj. osobám mimo definice jednotlivých kategorií orgánů a osob, které o to projeví zájem. Národní CERT bude moci dále vyvíjet vlastní vzdělávací, publikační, výzkumnou nebo vývojovou činnost apod. Podmínkou omezující iniciativně vykonávané činnosti národního CERT k dosažení účelu tohoto zákona je jejich bezrospornost s plněním povinností vyčtených v zákoně taxativně.

K § 18

Toto ustanovení stanoví obecné podmínky pro výběr provozovatele národního CERT a způsob jejich prokázání. Současně je upraven způsob založení jeho závazku k provozování národního CERT formou veřejnoprávní smlouvy uzavřené s NBÚ. Užití institutu veřejnoprávní smlouvy odpovídá předpokladu, že provozovatelem národního CERT bude osoba soukromého práva. Závazky provozovatele národního CERT vykonávat činnosti uvedené v tomto zákoně mají sice převážně charakter soukromoprávní, ve vztahu k poskytovatelům služeb elektronických komunikací, subjektům zajišťující sítě elektronických komunikací a subjektům zajišťující významné sítě však bude provozovatel národního CERT vystupovat jako subjekt, prostřednictvím jehož činnosti tyto orgány a osoby plní některé své zákonné povinnosti, typicky povinnost oznamovat kontaktní údaje a v případě subjektů zajišťujících významné sítě též povinnost hlásit výskyt kybernetických bezpečnostních incidentů.

Vzhledem k tomu, že národní CERT je pracovištěm velkého významu pro systém kybernetické bezpečnosti České republiky, vyžaduje se, aby provozovatel nevyvíjel činnost proti zájmům České republiky ve smyslu zákona č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Bezúhonnost a neexistence splatných finančních závazků vůči státu jsou v případě spolupráce státu a osoby soukromého práva standardně požadovanými formálními podmínkami. Zákon rovněž formuluje materiální podmínky výkonu funkce provozovatele národního CERT, přičemž se požaduje, aby provozovatel národního CERT prokázal faktické schopnosti a zkušenosti s provozem a správou informačních systémů nebo služeb a sítí elektronických komunikací, a to po dobu nejméně 5 let, dále technické předpoklady k výkonu činnosti uložené mu tímto zákonem, jakož i schopnost pracovat v součinnosti se zahraničními subjekty působícími na úseku kybernetické bezpečnosti. Zákon dále požaduje, aby provozovatel národního CERT plnil povinnosti svěřené mu tímto zákonem nestranně.

K § 19

Toto ustanovení upravuje způsob výběru provozovatele národního CERT, účel a podstatné náležitosti veřejnoprávní smlouvy, kterou bude NBÚ uzavírat s provozovatelem národního CERT. Zákon předpokládá, že tato veřejnoprávní smlouva bude zveřejněna ve Věstníku NBÚ. Zveřejní obsahu této smlouvy společně s institutem výběru provozovatele národního CERT v řízení o výběru žádosti podle správního řádu a institutem zveřejnění výsledku výběru přitom představuje projev principu transparentnosti výkonu veřejné správy.

Vzhledem k tomu, že může dojít k situaci, kdy nebude uzavřena veřejnoprávní smlouva s provozovatelem národního CERT nebo kdy uzavřená veřejnoprávní smlouva pozbude účinnosti (např. pokud provozovatel národního CERT přestane splňovat zákonné podmínky), je třeba pro tento výjimečný případ upravit provizorní fungování národního CERT. V takovém případě pak bude funkce národního CERT vykonávat NBÚ.

K § 20

Usnesení vlády č. 781 ze dne 19. října 2011 uložilo řediteli NBÚ vybudovat do konce roku 2015 plně funkční Národní centrum kybernetické bezpečnosti, jakož i vládní koordinační místo pro okamžitou reakci na počítačové incidenty, tzv. vládní CERT, který bude jeho součástí. Návrh zákona plně respektuje toto vládní usnesení a obecně upravuje působnost NBÚ v oblasti kybernetické bezpečnosti, přičemž touto problematikou se v rámci NBÚ bude zabývat Národní centrum kybernetické bezpečnosti jakožto organizační celek NBÚ a vládní CERT, který bude součástí Národního centra kybernetické bezpečnosti a jehož činnost bude toto centrum zajišťovat. Vládní CERT je koncipován jako centrální veřejnoprávní pracoviště a veřejnoprávní „single point of contact“ pro oblast kybernetické bezpečnosti. Jeho činnost zahrnuje příjem kontaktních údajů od vybraných orgánů a osob, příjem informací o kybernetické bezpečnostní situaci, a to zejména příjem povinných a iniciativních hlášení kybernetických bezpečnostních incidentů a dalších údajů o kybernetické bezpečnostní situaci od tuzemských a zahraničních orgánů veřejné moci a spolupracujících subjektů a jejich vyhodnocování. Vládní CERT dále poskytuje součinnost vybraným typům orgánů a osob při výskytu kybernetického bezpečnostního incidentu, zajišťuje součinnost s ostatními orgány a subjekty zajišťujícími kybernetickou bezpečnost v České republice a ve spolupracujících nebo spojeneckých státech a rovněž provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti, jehož předmětem je zkoumání známých zranitelností.

K § 21

Toto ustanovení upravuje vyhlašování stavu kybernetického nebezpečí. Vzhledem k tomu, že zákon je postaven na principu minimalizace zásahu do autonomie vůle subjektů působících v kybernetickém prostoru, jsou zákonné povinnosti týkající se zavádění a dokumentace bezpečnostních opatření, provádění opatření, hlášení kybernetických bezpečnostních incidentů a spolupráce s vládním resp. národním CERT za normální situace ukládány pouze těm orgánům a osobám, jejichž systémy jsou vysoce bezpečnostně exponovány, tj. správcům informačních nebo komunikačních systémů kritické informační infrastruktury a správcům významných informačních systémů a v omezeném případě pak subjektům zajišťujícím významné sítě. Zahraniční zkušenosti však ukazují, že může dojít k tak masivnímu ohrožení nebo narušení kybernetické bezpečnosti, že v jeho důsledku mohou být ohroženy nebo dokonce poškozeny fundamentální národní zájmy. Nelze-li takový incident zvládnout za užití standardních mechanismů zákona, může ředitel NBÚ rozhodnout o vyhlášení stavu kybernetického nebezpečí, v němž dojde k rozšíření osobní působnosti zákona na poskytovatele služeb elektronických komunikací, subjekty zajišťující sítě elektronických komunikací a subjekty zajišťující významné sítě, které budou za stavu kybernetického nebezpečí povinny provádět reaktivní opatření vydaná NBÚ.

Vyhlášení stavu kybernetického nebezpečí se netýká uživatelů informačních systémů, sítí a služeb elektronických komunikací a ve stavu kybernetického nebezpečí rovněž nedochází ani k rozšíření kompetencí orgánů veřejné moci působících na úseku kybernetické bezpečnosti. Vyhlášením stavu kybernetického nebezpečí dojde pouze k rozšíření okruhu orgánů a osob uvedených výše, které budou povinny provádět reaktivní opatření vydaná NBÚ. Vzhledem k tomu, že se stav kybernetického nebezpečí nedotýká práv nebo povinností občanů, není vhodné jej z legislativně-technických důvodů upravovat v obecném předpisu týkajícím se krizového řízení, tj. v krizovém zákoně.
Proces vyhlašování stavu kybernetického nebezpečí je upraven analogicky s krizovým zákonem. O vyhlášení stavu kybernetického nebezpečí rozhoduje ředitel NBÚ, který rovněž rozhoduje o prodloužení stavu kybernetického nebezpečí, přičemž ten může být prodloužen i opakovaně nejdéle však tak, aby souhrnná doba vyhlášeného stavu kybernetického nebezpečí nepřekročila dobu 30 dnů.
Pro vyhlášení i prodloužení stavu kybernetického nebezpečí platí vedle obecných právních principů též konkrétní materiální omezení uvedená v tomto ustanovení. Stav kybernetického nebezpečí lze vyhlásit, respektive prodloužit pouze ze zákonného důvodu, na dobu nezbytně nutnou k vyřešení ohrožení, které bylo důvodem jeho vyhlášení, a pouze tehdy, nelze-li důvod jeho vyhlášení řešit běžnou činností Úřadu podle tohoto zákona.
Za situace, kdy nebude možno zajistit bezpečnost informací v informačních systémech nebo bezpečnost služeb nebo sítí elektronických komunikací v rámci vyhlášeného stavu kybernetického nebezpečí, je ředitel NBÚ povinen požádat předsedu vlády o vyhlášení nouzového stavu podle ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb. V rámci takto vyhlášeného nouzového stavu lze vedle opatření stanovených krizovým zákonem nadále vydávat reaktivní opatření NBÚ se shora uvedenou rozšířenou osobní působností. Ačkoliv vyhlášením nouzového stavu končí stav kybernetického nebezpečí, rozhodnutí a opatření obecné povahy, která byla v jeho rámci vydána, zůstávají v platnosti, pokud nebudou v rozporu s krizovými opatřeními vydanými vládou v rámci vyhlášeného nouzového stavu.

K § 22
Tímto ustanovením je obecně svěřen NBÚ výkon státní správy na úseku kybernetické bezpečnosti. Ve výčtu činností, k jejichž výkonu má NBÚ právo a povinnost jsou vedle správních, evidenčních, kontrolních a legislativních kompetencí s ohledem na povahu NBÚ jako orgánu veřejné moci, pro který nepůsobí tacitní zákonné dovolení, explicitně uvedeny i činnosti nemající autoritativní povahu, tj. činnosti výzkumné a vývojové, koordinační, kooperační, preventivní a činnosti vedoucí k realizaci mezinárodní spolupráce na úseku kybernetické bezpečnosti.

K § 23
Kontrolní pravomoci specifikované tímto ustanovením vykonává NBÚ. Předmětem kontroly, při jejímž výkonu se primárně postupuje podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), je dodržování povinností stanovenými tímto zákonem, reaktivními a ochrannými opatřeními, jakož i dodržování prováděcích právních předpisů. Rozsah kontrolovaných povinností se liší v závislosti na typu orgánu a osoby, u které je kontrola vykonávána. Ve vztahu k poskytovatelům služeb elektronických komunikací, subjektům zajišťujícím sítě elektronických komunikací a subjektům zajišťujícím významné sítě kontroluje NBÚ pouze dodržování povinností stanovených reaktivními opatřeními za stavu kybernetického nebezpečí. Nad správci informačních nebo komunikačních systémů kritické informační infrastruktury a správci významných informačních systémů je výkon kontroly prováděný NBÚ nejširší. Předmětem kontroly těchto orgánů a osob je plnění povinností spočívajících v

zavedení bezpečnostních opatření, vedení bezpečnostní dokumentace, hlášení kybernetických bezpečnostních incidentů NBÚ, provádění reaktivních a ochranných opatření a oznamování kontaktních údajů a jejich změn NBÚ.

K § 24

Toto ustanovení upravuje podmínky, za nichž lze uložit orgánům a osobám nápravná opatření. Účelem nápravných opatření je odstranění nedostatků zjištěných při kontrole, tj. především dodatečné řádné splnění některé z povinností stanovených tímto zákonem nebo na jeho základě (typicky doplnění nedostatečně vedené bezpečnostní dokumentace, aktualizace kontaktních údajů). Obsahem nápravných opatření však mohou být i jiné povinnosti, a to v závislosti na charakteru zjištěných nedostatků a jejich možných následků. Pokud by pro zjištěné nedostatky byl informační nebo komunikační systém kritické informační infrastruktury anebo významný informační systém bezprostředně ohrožen kybernetickým bezpečnostním incidentem, který by jej mohl poškodit či zničit, byl by kontrolní orgán oprávněn orgánu a osobě uložit povinnost zabezpečit takový systém, v krajním případě pak dočasně zakázat jeho používání či používání jeho části, a to do doby, než budou zjištěné nedostatky odstraněny.

Nesplnění některé z povinností uložených nápravným opatřením pak zakládá skutkovou podstatu správního deliktu podle tohoto zákona, za nějž lze uložit pokutu do výše 100 000 Kč. Zákon dále výslovně stanoví, že náklady spojené s provedením nápravných opatření uložených NBÚ nese orgán a osoba, kterým byla nápravná opatření uložena.

K § 25 a 26

Ustanovení § 25 formuluje jednotlivé skutkové podstaty správních deliktů právnických a podnikajících fyzických osob v oblasti kybernetické bezpečnosti. Obecně platí, že orgán a osoba se správního deliktu podle tohoto zákona dopustí, neplní-li některé povinnosti stanovené tímto zákonem anebo na jeho základě. Rozsah skutkových podstat správních deliktů poskytovatelů služeb elektronických komunikací, subjektů zajišťujících sítě elektronických komunikací a subjektů zajišťujících významné sítě je přitom užší, než u ostatních orgánů a osob, neboť tato skupina orgánů a osob je právní regulací zatížena nejméně. Poměrně nízká výše pokuty za správní delikty byla stanovena zejména z toho důvodu, že zákon o kybernetické bezpečnosti je založen na principu prevence a principu autonomie vůle regulovaných subjektů. Vychází se přitom z předpokladu, že zájmem orgánů a osob je bezpečnost informací v jejich informačních systémech a dostupnost a spolehlivost služeb a sítí elektronických komunikací. Zákon si proto neklade za cíl působit represivně na orgány a osoby s cílem nutit je plnit povinnosti stanovené tímto zákonem pod hrozbou vysokých finančních pokut.

V závislosti na charakteru a závažnosti správních deliktů je dále výše pokuty diferenciovaná tak, že nesplnění povinnosti oznámit kontaktní údaje nebo jejich změnu NBÚ je sankcionováno pokutou výrazně nižší, než jakou lze uložit za jiné správní delikty.

V § 26 je dále formulována skutková podstata přestupku, jehož se dopustí fyzická osoba, pokud poruší povinnost mlčenlivosti o údajích vedených v evidenci incidentů podle § 9 návrhu zákona.

K § 27

Vzhledem ke skutečnosti, že neexistuje obecná právní úprava odpovědnosti právnických, respektive podnikajících fyzických osob za správní delikty, zákon v tomto ustanovení formuluje obecný liberační důvod z jejich odpovědnosti za jimi spáchané správní delikty. Dále je zde samostatně upravena promlčecí doba správního deliktu, a to jak subjektivní (1

rok), tak i objektivní (3 roky) a stanoví se zde obecná kritéria pro výměru výše pokuty za správní delikty.
Pokuty uložené za správní delikty, které jsou příjmem státního rozpočtu, vybírá NBÚ. Orgánem oprávněným k jejich vymáhání v případě jejich neuhrazení v zákonem stanovené lhůtě je pak příslušný celní úřad.

K § 28
Toto ustanovení upravuje zmocnění NBÚ a Ministerstva vnitra k vydání prováděcích právních předpisů ve formě vyhlášky k provedení příslušných ustanovení návrhu zákona.

K § 29
Lhůta ke splnění povinnosti hlásit kontaktní údaje je navázána na počátek účinnosti zákona. Vzhledem k tomu, že k předání kontaktních údajů bude formou prováděcího předpisu stanoven formulář a jednoduchý technický postup, nemělo by její dodržení činit povinným subjektům žádné obtíže.
Lhůta ke splnění povinnosti subjektů zajišťujících významné sítě hlásit kybernetické bezpečnostní incidenty je stanovena tak, aby měly tyto subjekty dostatečnou časovou rezervu k organizačním opatřením umožňující kontakt s národním dohledovým pracovištěm.

K § 30
Lhůty ke splnění povinností správců informačních a komunikačních systémů kritické informační infrastruktury oznámit kontaktní údaje a hlásit kybernetické bezpečnostní incidenty jsou stanoveny analogicky se lhůtami ve výše uvedeném ustanovení s tím rozdílem, že rozhodným dnem pro počátek běhu lhůty je den, kdy byl příslušný informační nebo komunikační systém orgánu a osoby určen kritickou informační infrastrukturou, respektive jejím prvkem. Dalším rozdílem oproti předchozímu ustanovení je stanovení přechodného období pro implementaci a dokumentaci bezpečnostních opatření. U obou typů orgánů a osob, jichž se týká toto ustanovení, lze očekávat, že již bezpečnostními opatřeními na úrovni zákonného standardu, respektive technického standardu stanoveného prováděcím předpisem vzhledem k důležitosti příslušné informační a komunikační infrastruktury disponují, a proto je v jejich případě roční lhůta stanovena s dostatečnou časovou rezervou.

K § 31
Lhůty k přizpůsobení se novým zákonným povinnostem jsou u správců významných informačních systémů stanoveny analogicky s předchozím ustanovením s tím, že počátek jejich běhu je stanoven ke dni, kdy příslušný informační systém nabyl parametry významného informačního systému stanovené prováděcím právním předpisem.

K § 32
V současnosti je potřeba národního soukromoprávního „single point of contact“ řešena při absenci zákonného právního rámce, tj. bez založení kompetencí nebo stanovení povinností třetím stranám, spoluprací se soukromoprávním subjektem provizorně provozujícím pracoviště typu CERT, a to na základě neformálního inominátního memoranda o spolupráci uzavřeného s NBÚ. Teprve po nabytí účinnosti tohoto zákona bude moci být vypsáno řízení o výběru žádosti podle správního řádu, v jehož rámci bude vybrána právnická osoba, která bude vykonávat činnost provozovatele národního CERT a s níž NBÚ uzavře příslušnou veřejnoprávní smlouvu. Mohlo by zde tak dojít k určité časové prodlevě mezi nabytím účinnosti návrhu zákona a uzavřením veřejnoprávní smlouvy, kdy by činnost národního CERT do vybrání jeho provozovatele měl podle dikce zákona vykonávat NBÚ, avšak současně by zde byl subjekt, který tuto činnost dlouhodobě vykonával a má k ní vytvořeny

odpovídající podmínky. Z hlediska zachování kontinuity činnosti, jakož i efektivnosti se jeví jako vhodnější řešení, podle kterého by tento subjekt po dobu účinnosti shora uvedeného memoranda vykonával činnost, provozovatele národního CERT podle návrhu zákona, avšak s časovým omezením. Maximální lhůta dvou let pro toto provizorní řešení umožní provést adekvátní výběrové řízení a bez technických nebo organizačních obtíží předat provoz národního CERT řádně vybranému subjektu.

K § 33

Účelem tohoto ustanovení je partikulární vynětí informačních a komunikačních systémů používaných zpravodajskými službami z působnosti tohoto zákona. Vzhledem k charakteru těchto systémů není žádoucí ani technicky možné, aby byly informace o jejich bezpečnostní situaci zpracovávány národním nebo vládním CERT, neboť by to vyžadovalo technické i personální oddělení veškerých evidencí a postupů, a to by indukovalo neúměrné personální, organizační i transakční náklady. Zabezpečení těchto systémů je přitom dostatečně řešeno na úrovni jednotlivých zpravodajských služeb, takže tyto systémy nepředstavují pro národní kybernetickou bezpečnost žádné podstatné riziko. Z těchto důvodů zákon předpokládá pouze základní vzájemnou komunikaci mezi správci těchto systémů, a vládním dohledovým pracovištěm. Zpravodajské služby tak budou povinny oznámit NBÚ kontaktní údaje systémů, které splňují formální požadavky pro zařazení do kritické informační infrastruktury a prostřednictvím těchto kontaktních údajů jim budou zasílána varování před hrozbami v oblasti kybernetické bezpečnosti s případnými doporučeními, jak těmto hrozbám čelit. V těchto informačních nebo komunikačních systémech by rovněž měla být zavedena bezpečnostní opatření, nikoliv však v plném rozsahu, ale přiměřeně s ohledem na jejich technické vlastnosti a účel jejich provozu. Z důvodů uvedených výše nebudou rovněž tyto systémy navrhovány do příslušného seznamu prvků kritické infrastruktury. Z důvodu specifického postavení Policie České republiky v rámci trestního řízení se navrhuje výjimka pro informační systém Policie České republiky pro analytickou činnost v trestním řízení. Z povahy regulace zákona nelze výjimku koncipovat jako absolutní, ale základní povinnosti spočívající v zabezpečení informačního systému, hlášení kontaktních údajů a reakce na varování se budou vztahovat i na tento informační systém. Tak bude zajištěna ochrana informačního systému při zachování specifik využívaných Policií České republiky.

K § 34

Činnost NBÚ vymezená zákonem č. 412/2005 Sb., podléhá kontrole, kterou je oprávněna vykonávat Poslanecká sněmovna Parlamentu České republiky. Protože se podle návrhu zákona kompetence NBÚ rozšíří o oblast kybernetické bezpečnosti, je třeba upravit příslušná ustanovení zákona č. 412/2005 Sb. tak, aby Poslanecká sněmovna, respektive jí zřízený zvláštní kontrolní orgán, mohl vykonávat kontrolu činnosti NBÚ rovněž v oblasti kybernetické bezpečnosti.

K § 35

Návrh zákona chrání kybernetický prostor, primárně se však zaměřuje na strategické a významné prvky a subjekty, a to z hlediska ochrany zájmů České republiky. Kybernetické bezpečnostní incidenty však mohou mít zásadní dopady i do práv osob soukromého práva, které tento status nemají. Je tedy třeba, aby i tyto osoby měly možnost řešit případné napadení sdílením informací, a to ve spolupráci s podnikateli v oblasti elektronických komunikací, jejichž prostřednictvím jsou jim poskytovány příslušné služby elektronických komunikací. Tato kooperace pomůže nejen identifikovat problém a tím přispět k jeho účinnému odstranění, ale umožní i do budoucna vytvářet potřebné ochranné mechanismy k zamezení či odvrácení případných dalších kybernetických bezpečnostních incidentů. Vzhledem k závažnosti maření

této nutné spolupráce je třeba takové jednání považovat za správní delikt. Sankce se však navrhuje v nejnižším pásmu.

K § 36

Údaje v evidenci kybernetických bezpečnostních incidentů mají velkou vypovídací hodnotu o činnosti pracovišť CERT a o kybernetické bezpečnostní situaci České republiky, jakož i o jednotlivých orgánech a osobách. Předávání údajů z evidence kybernetických bezpečnostních incidentů je proto zákonem regulováno, respektive omezeno. Toto ustanovení omezuje poskytování údajů z evidence kybernetických bezpečnostních incidentů ze strany NBÚ v případech, kdy je NBÚ povinným subjektem podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, který je povinen poskytovat informace vztahující se k jeho působnosti, tj. i k oblasti kybernetické bezpečnosti. Jak je uvedeno výše, údaje vedené v evidenci kybernetických bezpečnostních incidentů mají mimo jiné též velký význam pro bezpečnostní reputaci a pro fungování bezpečnostních opatření jednotlivých orgánů a osob. Aby nedošlo k nedůvodnému zásahu do oprávněných zájmů orgánů a osob nebo ke zmaření účelu bezpečnostních opatření, je poskytování těchto údajů omezeno jen na takové, z nichž nelze určit totožnost oznamovatele a dále je omezeno poskytování takových údajů, jejichž poskytnutí by představovalo riziko pro faktickou realizaci reaktivních nebo ochranných opatření.

K § 37

V návaznosti na ustanovení § 21 odst. 2 upravující informování veřejnosti o vyhlášení stavu kybernetického nebezpečí se rovněž doplňuje povinnost provozovatele rozhlasového nebo televizního vysílání poskytnout Národnímu bezpečnostnímu úřadu vysílací čas v rozsahu nezbytném pro důležitá a neodkladná oznámení související s vyhlášením stavu kybernetického nebezpečí.

K § 38

Účinnost předmětného zákona se navrhuje dnem 1. ledna 2015. Tento termín dává dostatečný prostor k projednání návrhu zákona v Parlamentu České republiky a současně dostatečný prostor pro orgány a osoby připravit se na novou právní regulaci.

V Praze dne 2. ledna 2014

předseda vlády

Ing. Jiří Rusnok, v. r.

ředitel Národního bezpečnostního úřadu

Ing. Dušan Navrátil, v. r.