Návrh

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 fyzických a právnických osob a působnost a pravomoc orgánů veřejné moci a jejich vzájemnou spolupráci v oblasti kybernetické bezpečnosti.

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

§ 2

Vymezení pojmů

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) kybernetickou bezpečností souhrn právních, organizačních, technických a vzdělávacích prostředků k zajištění ochrany kybernetického prostoru,
c) kritickou informační infrastrukturou prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy[2)] v oblasti kybernetické bezpečnosti,
d) bezpečností informací zajištění důvěrnosti, integrity a dostupnosti informace,
e) významným informačním systémem informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může ohrozit nebo výrazně omezit výkon činnosti veřejné správy; významné informační systémy a jejich určující kritéria stanoví prováděcí právní předpis,

[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 zákona č. 320/2002 Sb. a zákona č. 430/2010 Sb.

f) správcem informačního systému subjekt, který určuje účel zpracování informací a podmínky provozování informačního systému,
g) správcem komunikačního systému subjekt, který určuje účel komunikačního systému a podmínky jeho provozování a
h) významnou sítí síť elektronických komunikací[1)] zajišťující přímé zahraniční připojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře.

§ 3

Povinné osoby v oblasti kybernetické bezpečnosti

Povinnými osobami v oblasti kybernetické bezpečnosti jsou

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací[1)], pokud nespadá pod písmeno b),
b) subjekt zajišťující významnou síť, pokud nespadá pod písmeno d),
c) správce informačního systému kritické informační infrastruktury,
d) správce komunikačního systému kritické informační infrastruktury a
e) správce významného informačního systému.

HLAVA II

SYSTÉM K ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI

§ 4

Systém zajištění kybernetické bezpečnosti tvoří bezpečnostní opatření, hlášení kybernetických bezpečnostních incidentů, protiopatření, oznamování kontaktních údajů a činnost Národního bezpečnostního úřadu (dále jen „Úřad“) a dohledových pracovišť.

Bezpečnostní opatření

§ 5

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

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

§ 6

(1) Bezpečnostními opatřeními jsou

a) organizační opatření a
b) technická opatření.

(2) Organizační opatření jsou zejména

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) Technická opatření jsou zejména

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 správců,
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.

§ 7

Prováděcí právní předpis stanoví

a) obsah bezpečnostních opatření,
b) obsah, strukturu a formu bezpečnostní dokumentace a
c) rozsah zavedení bezpečnostních opatření pro povinné osoby uvedené v § 3 písm. c) až e).

Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident a jejich detekce

§ 8

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

(2) Kybernetickým bezpečnostním incidentem je kybernetická bezpečnostní událost, která představuje narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb a sítí elektronických komunikací[1)].

(3) Povinné 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.

§ 9

Hlášení kybernetického bezpečnostního incidentu

(1) Povinné 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) Povinné osoby uvedené v § 3 písm. b) hlásí kybernetické bezpečnostní incidenty národnímu dohledovému pracovišti (dále jen „národní CERT“).

(3) Povinné osoby uvedené v § 3 písm. c) až e) hlásí kybernetické bezpečnostní incidenty Úřadu.

(4) Prováděcí právní předpis stanoví

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

Evidence

§ 10

(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 řešení kybernetického bezpečnostního incidentu, jeho výsledek a použitá protiopatření.

(2) Součástí evidence incidentů mohou být údaje podle § 22 písm. e) až g).

(3) Úřad poskytuje údaje z evidence incidentů orgánům veřejné moci pouze pro plnění úkolů v rámci jejich působnosti.

(4) Úřad může poskytovat údaje z evidence incidentů 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.

[3)] § 98 zákona č. 127/2005 Sb., ve znění zákona č. 153/2010 Sb. a zákona č. 468/2011 Sb.

§ 11

(1) Úřad neposkytne údaje z evidence incidentů, pokud by z nich bylo možné identifikovat povinnou osobu, která kybernetický bezpečnostní incident ohlásila; to neplatí v případě postupu podle § 10 odst. 3 nebo 4.

(2) Úřad může omezit poskytnutí údaje z evidence incidentů, pokud by jejich poskytnutí ohrozilo účinnost protiopatření podle § 15 nebo 16; to neplatí v případě postupu podle § 10 odst. 3 nebo 4.

§ 12

(1) Zaměstnanci 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.

Protiopatření

§ 13

(1) Protiopatřeními se rozumí úkony Úřadu, 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) Protiopatřeními jsou

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

(3) Reaktivní protiopatření jsou povinny provádět

a) povinné osoby uvedené v § 3 písm. a) a b) za stavu kybernetického nebezpečí nebo za nouzového stavu[4)] v případech podle § 24 odst. 6 a
b) povinné osoby uvedené v § 3 písm. c) až e).

(4) Ochranné protiopatření jsou povinny provádět povinné osoby uvedené v § 3 písm. c) až e).

§ 14

Varování

(1) Úřad vydá varování, dozví-li se zejména z vlastní činnosti nebo z podnětu 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 internetových stránkách vládního dohledového pracoviště (dále jen „vládní CERT“) a oznámí jej povinným osobám prostřednictvím údajů vedených v evidenci kontaktních údajů. Součástí varování může být doporučení, jak čelit hrozbě v oblasti kybernetické bezpečnosti.

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

§ 15

Reaktivní protiopatření

(1) Úřad vydá reaktivní protiopatření rozhodnutím k řešení kybernetického bezpečnostního incidentu a doručí jej povinné osobě. Rozhodnutí je vykonatelné doručením. Nepodaří-li se rozhodnutí do 24 hodin od jeho vydání doručit do vlastních rukou adresáta, je vykonatelné vyvěšením na úřední desce Úřadu. Rozhodnutí může Úřad vydat v řízení na místě[5)].

(2) Proti rozhodnutí lze podat rozklad. Podání rozkladu nemá odkladný účinek.

(3) Úřad vydá reaktivní protiopatření opatřením obecné povahy, kterým povinné osobě uloží zabezpečit informační systémy nebo sítě a služby elektronických komunikací[1)] před kybernetickým bezpečnostním incidentem.

(4) Povinná osoba je povinna bez zbytečného odkladu oznámit Úřadu provedení reaktivního protiopatření a jeho výsledek. Náležitosti oznámení stanoví prováděcí právní předpis.

(5) Prováděcí právní předpis stanoví příklady reaktivních protiopatření.

§ 16

Ochranné protiopatření

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

(2) Opatřením obecné povahy Úřad povinným 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.

§ 17

(1) Při vydání protiopatření opatřením obecné povahy podle § 15 nebo 16 postupuje Úřad podle správního řádu. Opatření obecné povahy nabývá účinnosti dnem zveřejnění na úřední desce Úřadu, a to před postupem podle § 172 správního řádu. Současně se opatření obecné povahy zveřejní na internetových stránkách vládního CERT. O vydání opatření obecné povahy se povinná osoba rovněž vyrozumí prostřednictvím kontaktních údajů.

(2) Připomínky k opatření obecné povahy vydaného podle odstavce 1 lze uplatnit ve lhůtě 15 dnů ode dne jeho zveřejnění na úřední desce Úřadu. Úřad může na základě uplatněných připomínek opatření obecné povahy změnit anebo zrušit.

(3) O opatření obecné povahy nelze vést přezkumné řízení.

Kontaktní údaje

§ 18

(1) Kontaktní údaje povinné osoby jsou

a) u právnické osoby obchodní firma nebo název včetně odlišujícího dodatku nebo dalšího označení, adresa sídla, identifikační číslo osoby nebo obdobné číslo přidělované v zahraničí,

[5)] § 143 správního řádu.

b) u podnikající fyzické osoby obchodní firma nebo název včetně odlišujícího dodatku nebo dalšího označení, adresa místa podnikání 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 povinnou osobu pověřena jednat ve věcech upravených tímto zákonem, v rozsahu jméno, příjmení, telefonní číslo a adresa elektronické pošty.

(2) Kontaktní údaje a jejich změny oznamují

a) povinné osoby uvedené v § 3 písm. a) a b) národnímu CERT a
b) povinné osoby uvedené v § 3 písm. c) až e) Úřadu.

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

(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 národním CERT podle odstavce 2 písm. a).

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

Dohledová pracoviště

§ 19

Národní CERT

(1) Národní CERT je pracoviště provozované zpravidla osobou soukromého práva, které zajišťuje sdílení informací na národní a mezinárodní úrovni v oblasti kybernetické bezpečnosti, a to zejména pro osoby soukromého práva.

(2) Národní CERT

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

(3) Národní CERT může vykonávat i další činnost v oblasti kybernetické bezpečnosti pokud tato činnost nenaruší plnění povinností uvedených v odstavci 2.

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

§ 20

Provozovatel národního CERT

(1) Provozovatelem národního CERT je právnická osoba,

a) která splňuje podmínky uvedené v odstavci 2 a
b) se kterou Úřad uzavřel veřejnoprávní smlouvu podle § 21.

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

a) má zkušenosti s provozem informačních systémů nebo služeb a sítí elektronických komunikací[1)],
b) má technické, technologické a personální zázemí,
c) se podílí na mezinárodní spolupráci s organizacemi působícími v oblasti kybernetické bezpečnosti v zahraničí,
d) má transparentní vlastnickou strukturu,
e) plní finanční povinnosti vůči státu, fyzickým a právnickým osobám,
f) je bezúhonná a
g) má sídlo na území České republiky.

(3) Vztah mezi provozovatelem národního CERT a povinnou osobou nesmí mít vliv na jeho nestrannost při plnění povinností uvedených v § 19 odst. 2.

(4) Úřad zveřejní údaje o provozovateli národního CERT na internetových stránkách vládního CERT.

§ 21

Veřejnoprávní smlouva

(1) Úřad uzavírá veřejnoprávní smlouvu (dále jen „smlouva“) s právnickou osobou vybranou v řízení o výběru žádosti podle správního řádu za účelem spolupráce v oblasti kybernetické bezpečnosti a zajištění činností podle § 19 odst. 1 a 2.

(2) Smlouva obsahuje

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) způsob financování činnosti národního CERT a
h) způsob předání a rozsah údajů předávaných Úřadu v případě pozbytí účinnosti smlouvy.

(3) Smlouvu uzavřenou podle odstavce 1 Úřad zveřejňuje ve Věstníku Úřadu, umožňuje-li to obsah smlouvy.

(4) Není-li uzavřena smlouva podle odstavce 1, nebo pozbyla-li účinnosti, vykonává činnost národního CERT Úřad.

§ 22

Vládní CERT

Vládní CERT je pracoviště Úřadu, které

a) přijímá oznámení kontaktních údajů od povinných osob uvedených v § 3 písm. c) až e),
b) přijímá hlášení o kybernetických bezpečnostních incidentech od povinných 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 součinnost povinným osobám uvedeným v § 3 písm. c) až e) při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události,
e) přijímá podněty a údaje od povinných osob a od subjektů, které nejsou uvedeny v § 3, a tyto podněty a údaje vyhodnocuje,
f) přijímá údaje od národního CERT a tyto údaje vyhodnocuje,
g) přijímá údaje od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, a tyto údaje vyhodnocuje,
h) poskytuje národnímu CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraniční a jiným subjektům působícím v oblasti kybernetické bezpečnosti údaje z evidence incidentů a
i) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti.

§ 23

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 § 14 a 18; ustanovení § 5 se na tyto systémy použije přiměřeně a Úřad je jako prvky kritické infrastruktury podle § 26 odst. 2 písm. n) nenavrhuje.

HLAVA III

STAV KYBERNETICKÉHO NEBEZPEČÍ

§ 24

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

(2) Stav kybernetického nebezpečí vyhlašuje na návrh ředitele Úřadu předseda vlády. Rozhodnutí o vyhlášení stavu kybernetického nebezpečí se zveřejňuje v hromadných informačních prostředcích a vyhlašuje se stejně jako zákon. Účinnosti nabývá okamžikem, který se v rozhodnutí stanoví. Rozhodnutí o vyhlášení stavu kybernetického nebezpečí vláda do 24 hodin schválí nebo zruší.

(3) Stav kybernetického nebezpečí se vyhlašuje na dobu nezbytně nutnou, nejdéle na dobu 7 dnů. Uvedená doba se může prodloužit jen po předchozím souhlasu vlády; souhrnná doba trvání vyhlášeného stavu kybernetického nebezpečí nesmí být delší než 30 dnů.

(4) V průběhu vyhlášeného stavu kybernetického nebezpečí ředitel Úřadu informuje předsedu vlády 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 protiopatření podle § 15 rovněž povinným 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 nebo sítí elektronických komunikací[1)] lze odvrátit činností vládního CERT.

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

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

§ 25

(1) Komise pro kybernetickou bezpečnost je poradním orgánem ředitele Úřadu pro předcházení a řešení stavu kybernetického nebezpečí.

(2) Předsedou Komise pro kybernetickou bezpečnost je ředitel Úřadu, který jmenuje její další členy z řad zástupců orgánů veřejné moci, zástupců veřejnoprávních korporací a zástupců osob soukromého práva působících v oblasti kybernetické bezpečnosti nebo v oblasti elektronických komunikací.

HLAVA IV

VÝKON STÁTNÍ SPRÁVY

§ 26

(1) Výkon státní správy v oblasti kybernetické bezpečnosti vykonává Úřad, nestanoví-li tento zákon nebo jiný právní předpis jinak.

(2) Úřad jako ústřední správní úřad

a) stanoví bezpečnostní opatření,
b) vydává protiopatření,
c) zajišťuje činnost Národního centra kybernetické bezpečnosti,
d) vede evidence podle tohoto zákona,
e) kontroluje plnění povinností stanovených tímto zákonem,
f) ukládá pokuty za správní delikty podle tohoto zákona,
g) působí jako koordinační orgán ve stavu kybernetického nebezpečí,
h) spolupracuje s orgány veřejné moci, veřejnoprávními korporacemi, výzkumnými a vývojovými pracovišti a s ostatními dohledovými pracovišti,
i) zajišťuje mezinárodní spolupráci v součinnosti s Ministerstvem zahraničních věcí,
j) sjednává a uzavírá smlouvy o mezinárodní spolupráci v součinnosti s Ministerstvem zahraničních věcí,
k) zajišťuje prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti,
l) zajišťuje výzkum a vývoj v oblasti kybernetické bezpečnosti,
m) uzavírá veřejnoprávní smlouvu s provozovatelem národního CERT,

n) 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,
o) určuje podle krizového zákona prvky kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, pokud nejde o prvky uvedené v písmenu n) a
p) plní další úkoly v oblasti kybernetické bezpečnosti stanovené tímto zákonem.

(3) Ministerstvo vnitra kontroluje plnění povinnosti stanovené v § 5 odst. 2 u povinných osob uvedených v § 3 písm. e).

HLAVA V

KONTROLA, DOHLED A SPRÁVNÍ DELIKTY

Kontrola

§ 27

(1) Úřad vykonává kontrolu v oblasti kybernetické bezpečnosti. Při výkonu kontroly Úřad zjišťuje, jak povinné osoby plní povinnosti stanovené tímto zákonem, rozhodnutími a opatřeními obecné povahy vydanými Úřadem a dodržují prováděcí právní předpisy. Kontrolu v oblasti kybernetické bezpečnosti dále vykonává Ministerstvo vnitra, a to podle odstavce 4.

(2) Při výkonu kontroly se postupuje podle kontrolního řádu, nestanoví-li tento zákon jinak.

(3) Úřad vykonává kontrolu

a) povinné osoby uvedené v § 3 písm. a) a b) nad plněním povinností stanovených protiopatřením vydaným podle § 15 za stavu kybernetického nebezpečí,
b) povinné osoby uvedené v § 3 písm. c) a d) nad plněním povinností stanovených v § 5 odst. 2, § 9 odst. 3, protiopatření vydaném podle § 15 nebo 16 a § 18 odst. 2 písm. b) a
c) povinné osoby uvedené v § 3 písm. e) nad plnění povinností stanovených v § 9 odst. 3, protiopatření vydaném podle § 15 nebo 16 a § 18 odst. 2 písm. b).

(4) Ministerstvo vnitra vykonává kontrolu povinné osoby uvedené v § 3 písm. e) nad plněním povinností stanovených v § 5 odst. 2.

§ 28

Nápravná opatření

(1) Zjistí-li kontrolní orgán při kontrole prováděné podle § 27 nedostatky, uloží povinné osobě, aby ve stanovené lhůtě zjednala nápravu zjištěných nedostatků, a případně určí, jaká opatření k odstranění nedostatků je tato povinná osoba povinna přijmout.

(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 povinné osobě používání tohoto systému anebo jeho části do doby, než bude zjištěný nedostatek odstraněn.

(3) Náklady spojené s provedením nápravných opatření hradí povinná osoba.

Správní delikty právnických a podnikajících fyzických osob

§ 29

(1) Povinná osoba uvedená v § 3 písm. a) nebo b) se dopustí správního deliktu tím, že

a) neprovede za stavu kybernetického nebezpečí protiopatření vydané Úřadem podle § 15, nebo
b) nesplní některou z povinností uloženou nápravným opatřením podle § 28.

(2) Povinná osoba uvedená v § 3 písm. c) až e) se dopustí správního deliktu tím, že

a) v rozporu s § 5 odst. 2 nezavede bezpečnostní opatření nebo nevede bezpečnostní dokumentaci,
b) neohlásí kybernetický bezpečnostní incident Úřadu podle § 9 odst. 3,
c) neprovede protiopatření vydané Úřadem podle § 15 nebo 16,
d) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 18 odst. 2 písm. b) nebo
e) nesplní některou z povinností uloženou nápravným opatřením podle § 28.

(3) Za správní delikt se uloží pokuta do

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

§ 30

(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 zaniká 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

§ 31
Zmocňovací ustanovení

(1) Úřad a Ministerstvo vnitra stanoví vyhláškou významné informační systémy a jejich určující kritéria podle § 2 písm. e).

(2) Úřad stanoví vyhláškou

a) obsah, strukturu a formu bezpečnostní dokumentace, obsah bezpečnostních opatření a rozsah zavedení bezpečnostních opatření podle § 7,

b) typy a kategorie kybernetických bezpečnostních incidentů a náležitosti a formu hlášení kybernetického bezpečnostního incidentu podle § 9 odst. 4,

c) náležitosti oznámení o provedení reaktivního protiopatření a jeho výsledku podle § 15 odst. 4,

d) příklady reaktivních protiopatření podle § 15 odst. 5 a

e) vzor oznámení kontaktních údajů a jeho formu podle § 18 odst. 6.

Přechodná ustanovení

§ 32

(1) Povinné osoby uvedené v § 3 písm. a) a b) jsou povinny oznámit kontaktní údaje podle § 18 do 30 dnů ode dne nabytí účinnosti tohoto zákona.

(2) Povinné osoby uvedené v § 3 písm. b) jsou povinny plnit povinnost hlásit kybernetické bezpečnostní incidenty podle § 9 odst. 3 nejpozději do 1 roku ode dne nabytí účinnosti tohoto zákona.

§ 33

Povinné osoby uvedené v § 3 písm. c) a d) jsou povinny

a) oznámit kontaktní údaje podle § 18 do 30 dnů ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou,
b) plnit povinnost hlásit kybernetické bezpečnostní incidenty podle § 9 odst. 3 nejpozději do 1 roku ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou a
c) zavést bezpečnostní opatření podle § 5 odst. 2 do 1 roku ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou.

§ 34

Povinné osoby uvedené v § 3 písm. e) jsou povinny

a) oznámit kontaktní údaje podle § 18 do 30 dnů ode dne naplnění určujících kritérií významného informačního systému,
b) plnit povinnost hlásit kybernetické bezpečnostní incidenty podle § 9 odst. 3 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému a

c) zavést bezpečnostní opatření podle § 5 odst. 2 do 1 roku ode dne naplnění určujících kritérií významného informačního systému.

§ 35

Činnost národního CERT vykonává do doby, než nabude účinnosti veřejnoprávní smlouva uzavřená podle § 21, subjekt, který uzavřel s Úřadem smlouvu o spolupráci před nabytím účinnosti tohoto zákona, nejdéle však do doby 2 let ode dne nabytí účinnosti tohoto zákona.

ČÁST DRUHÁ

Změna zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti

§ 36

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. a zákona č. 167/2012 Sb., se mění takto:

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

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

2. V § 146 odst. 1 se za slova „bezpečnostního řízení“ vkládají slova „nebo v rámci správního řízení o vydání protiopatření 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

§ 37

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. a zákona č. 273/2012 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 údaje k uskutečněné nebo probíhající komunikaci, 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 bezodkladně, nejpozději však do 3 dnů ode dne doručení žádosti nebo v případě probíhající komunikace ode dne jejího uskutečnění.

[62)] § 8 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 písmeno aa), které zní:

„aa) 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. aa)“.

ČÁST ČTVRTÁ

ÚČINNOST

§ 38

Tento zákon nabývá účinnosti dnem 1. ledna 2015.