181/2014 Sb.

ZÁKON

ze dne 23. července 2014

o kybernetické bezpečnosti a o změně souvisejících zákonů

(zákon o kybernetické bezpečnosti)

Ve znění zákonů č.: 111/2019 Sb., 35/2018 Sb., 205/2017 Sb., 104/2017 Sb., 183/2017 Sb.

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 zapracovává příslušné předpisy Evropské unie[6] a upravuje zajišťování bezpečnosti sítí elektronických komunikací a informačních systémů.

(3) 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 a dat,

d) významným informačním systémem informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby 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,

g) provozovatelem informačního nebo komunikačního systému orgán nebo osoba zajišťující funkčnost technických a programových prostředků tvořících informační nebo komunikační systém

h) významnou sítí síť elektronických komunikací1 zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře,

i) základní službou služba, jejíž poskytování je závislé na sítích elektronických komunikací[7] nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví

   1. energetika,
   2. doprava,
   3. bankovnictví,
   4. infrastruktura finančních trhů,
   5. zdravotnictví,
   6. vodní hospodářství,
   7. digitální infrastruktura,
   8. chemický průmysl,

j) informačním systémem základní služby informační systém, na jehož fungování je závislé poskytování základní služby,

k) provozovatelem základní služby orgán nebo osoba, která poskytuje základní službu a která je určena Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „Úřad“) podle § 22a; pro účely plnění informační povinnosti podle příslušného předpisu Evropské unie[8] se za provozovatele základní služby považují též orgány a osoby uvedené v § 3 písm. c) a d),

l) digitální službou služba informační společnosti podle zákona upravujícího některé služby informační společnosti[9], která spočívá v provozování

   1. on-line tržiště, které spotřebiteli nebo prodávajícímu umožňuje on-line uzavírat s prodávajícím podnikatelem[10] kupní smlouvu nebo smlouvu o poskytnutí služeb, a to prostřednictvím internetové stránky on-line tržiště nebo prostřednictvím internetové stránky prodávajícího, který využívá službu poskytovanou on-line tržištěm,
   2. internetového vyhledávače, který umožňuje provádět vyhledávání v zásadě na všech internetových stránkách, a to na základě dotazu uživatele na jakékoliv téma v podobě klíčového slova, sousloví nebo jiného zadání, přičemž služba poskytuje odkazy, na nichž lze nalézt informace související s požadovaným obsahem, nebo

3. cloud computingu, který umožňuje přístup k rozšířitelnému a přizpůsobitelnému úložišti nebo výpočetním zdrojům, které je možné sdílet, a

m) příslušným orgánem orgán vykonávající působnost v oblasti kybernetické bezpečnosti.

§ 3

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

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací1, pokud není orgánem nebo osobou podle písmene b),

b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem nebo provozovatelem komunikačního systému podle písmene d),

c) správce a provozovatel informačního systému kritické informační infrastruktury,

d) správce a provozovatel komunikačního systému kritické informační infrastruktury,

e) správce a provozovatel významného informačního systému,

f) správce a provozovatel informačního systému základní služby, pokud nejsou správcem nebo provozovatelem podle písmene c) nebo d),

g) provozovatel základní služby, pokud není správcem nebo provozovatelem podle písmene f), a

h) poskytovatel digitální služby.

§ 3a
Zástupce poskytovatele digitálních služeb

(1) Poskytovatel digitální služby, který poskytuje tuto službu v České republice, nemá sídlo v Evropské unii a neustavil si svého zástupce v jiném členském státě Evropské unie (dále jen „jiný členský stát“), je povinen ustavit si svého zástupce v České republice. Zástupcem poskytovatele digitální služby je osoba, která je usazená v České republice a která je poskytovatelem digitální služby na základě plné moci zmocněná jej zastupovat ve vztahu k povinnostem podle tohoto zákona.

(2) V případě, že poskytovatel digitální služby má sídlo mimo Evropskou unii a ustavil si svého zástupce v České republice, má se za to, že je usazen v České republice a vztahují se na něj povinnosti podle tohoto zákona.

(3) V případě, že je poskytovatel digitální služby usazen v České republice nebo zde má ustaveného zástupce, ale jím využívané sítě elektronických komunikací a informační systémy se nacházejí v jiném členském státu, Úřad při výkonu státní správy spolupracuje s příslušným orgánem dotčeného členského státu.

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 komunikací1 v kybernetickém prostoru.

(2) Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury, informačního systému základní služby a významného informačního systému a vést o nich bezpečnostní dokumentaci.

(3) Poskytovatel digitální služby je povinen zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby, přičemž tato bezpečnostní opatření zohledňují zajištění bezpečnosti informací, zvládání kybernetických bezpečnostních incidentů, řízení kontinuity činností, monitorování, audit, testování a soulad s mezinárodními předpisy.

(4) Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

(5) Orgány a osoby uvedené v § 3 písm. c) až g), které jsou orgány veřejné moci, jsou povinny si ve smlouvě s poskytovatelem služeb cloud computingu zejména zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu stanovená Úřadem, a že budou mít na základě své žádosti bez zbytečného odkladu k dispozici informace a data, která pro ně poskytovatel služeb cloud computingu uchovává včetně možnosti kontroly uchovávaných informací a dat v reálném čase. Dalšími nezbytnými náležitostmi smlouvy jsou

a) zakotvení povinnosti poskytovatele služeb respektovat bezpečnostní politiku odběratele služeb,

b) stanovení úrovně poskytovaných služeb,

c) systém schvalování subdodavatelů služby cloud computingu,

d) podmínky ukončení smluvního vztahu z pohledu bezpečnosti,

e) řízení kontinuity činností v souvislosti s poskytovanou službou cloud computingu,

f) určení vlastníka uchovávaných dat,

g) dohoda o důvěrnosti smluvního vztahu,

h) stanovení úrovně ochrany dat z pohledu důvěrnosti, dostupnosti a integrity,

i) pravidla zákaznického auditu,

j) stanovení povinnosti poskytovatele služeb informovat odběratele o kybernetických bezpečnostních incidentech souvisejících s plněním smlouvy.

(6) Poskytovatel služby cloud computingu a orgány a osoby uvedené v § 3 písm. c) až g), které jsou orgány veřejné moci, si ve smlouvě dále dohodnou způsob a výši úhrady účelně vynaložených nákladů na zavedení bezpečnostních pravidel.

(7) Zohlednění požadavků vyplývajících z bezpečnostních pravidel, bezpečnostních opatření a dalších podmínek sjednaných ve smlouvě podle odstavce 5, které jsou nezbytné pro splnění povinností podle tohoto zákona, nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

§ 4a

(1) Orgány a osoby, které se staly správci informačních nebo komunikačních systémů kritické informační infrastruktury nebo správci významných informačních systémů, a nejsou provozovateli tohoto systému, jsou povinny neprodleně a prokazatelně informovat provozovatele systému o této skutečnosti a o tom, že se tento provozovatel stal orgánem nebo osobou podle § 3 písm. c), d) nebo e).

(2) Orgány a osoby, které se staly správci nebo provozovateli informačních nebo komunikačních systémů kritické informační infrastruktury, jsou povinny neprodleně a prokazatelně informovat subjekt zajišťující síť elektronických komunikací, ke které je jejich předmětný informační nebo komunikační systém kritické informační infrastruktury připojen, o této skutečnosti a o tom, že se tento subjekt stal orgánem nebo osobou podle § 3 písm. b).

(3) Orgány a osoby, které byly podle § 22a určené provozovateli základní služby a nejsou zároveň správci nebo provozovateli svých informačních systémů základní služby, jsou povinny správce nebo provozovatele tohoto informačního systému základní služby neprodleně a prokazatelně informovat o svém určení a o tom, že se dotčený správce nebo provozovatel stal orgánem nebo osobou podle § 3 písm. f).

§ 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 f),

d) významné informační systémy a jejich určující kritéria,

e) obsah a rozsah bezpečnostních pravidel pro orgány veřejné moci využívající služby poskytovatelů cloud computingu.

§ 6a

(1) Správce informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému může pověřit provozováním informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému jiný orgán nebo osobu, pokud to jiný zákon nevylučuje.

(2) Provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému předá na vyžádání správce tohoto systému bez zbytečného odkladu a v dohodnutém formátu data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému. Ustanovení právního předpisu upravujícího práva k duševnímu vlastnictví nejsou předáním dat, provozních údajů a informací dotčena.

(3) Pokud provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému nebude tento systém nadále provozovat, předá správci tohoto systému data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému a které jsou nezbytné pro případné další provozování tohoto informačního systému nebo jeho jiné využití a bezpečně zlikviduje ve svém digitálním prostředí jejich kopie. Způsob likvidace dat, provozních údajů, informací a jejich kopií stanoví prováděcí právní předpis.

(4) Provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému má nárok na úhradu účelně vynaložených nákladů za předání dat, provozních údajů a informací podle odstavců 2 a 3; náklady provozovateli uhradí správce takového systému.

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 f) jsou povinny detekovat kybernetické bezpečnostní události v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému.

§ 8

Hlášení kybernetického bezpečnostního incidentu

(1) Orgány a osoby uvedené v § 3 písm. b) až f) jsou povinny hlásit kybernetické bezpečnostní incidenty v jejich významné síti, informačním systému kritické informační infrastruktury, komunikačním systému kritické informační infrastruktury, informačním systému základní služby nebo významném informačním systému, a to bezodkladně po jejich detekci; tím není dotčena informační povinnost podle jiného právního předpisu[3] nebo přímo použitelného předpisu Evropské unie upravujícího ochranu osobních údajů[11]. V případě, že kybernetický bezpečnostní incident má významný dopad na kontinuitu poskytování základní služby, oznámí to provozovatel základní služby Úřadu.

(2) Poskytovatel digitální služby je povinen bez zbytečného odkladu hlásit kybernetický bezpečnostní incident s významným dopadem na poskytování jeho služeb, pokud má přístup k informacím nezbytným pro posouzení významnosti tohoto dopadu.

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

(4) Orgány a osoby uvedené v § 3 písm. c) až g) hlásí kybernetické bezpečnostní incidenty Úřadu.

(5) Povinnost podle odstavce 1 je správcem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému splněna i tehdy, pokud byl kybernetický bezpečnostní incident hlášen provozovatelem tohoto systému. Provozovatel informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému informuje správce tohoto systému o hlášených kybernetických bezpečnostních incidentech bez zbytečného odkladu.

(6) Orgány a osoby neuvedené v § 3 mohou hlásit kybernetické bezpečnostní incidenty provozovateli národního CERT, nebo Úřadu.

(7) Prováděcí právní předpis stanoví

a) typy, kategorie a hodnocení významnosti dopadu kybernetického bezpečnostního incidentu a

b) náležitosti a způsob hlášení kybernetického bezpečnostního incidentu.

(8) Pokud má kybernetický bezpečnostní incident, který postihnul poskytovatele digitální služby, významný dopad na kontinuitu poskytování základní služby, je její provozovatel povinen tuto skutečnost Úřadu nahlásit.

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) a l).

(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.

§ 10a

Informace, jejichž zpřístupnění by mohlo ohrozit zajišťování kybernetické bezpečnosti nebo účinnost opatření vydaného podle tohoto zákona, nebo informace, které jsou vedené v evidenci incidentů, ze kterých by bylo možné identifikovat orgán nebo osobu, která kybernetický bezpečnostní incident ohlásila, se podle předpisů upravujících svobodný přístup k informacím neposkytují.

§ 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 f).

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

§ 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.

(3) Úřad je z důvodu ochrany vnitřního pořádku a bezpečnosti, ochrany života a zdraví osob nebo ochrany ekonomiky státu oprávněn po konzultaci s orgánem nebo osobou uvedenými v § 3 písm. c), d), f), g) nebo h), které jsou dotčeny kybernetickým bezpečnostním incidentem, veřejnost o tomto incidentu informovat nebo dotčenému orgánu nebo osobě uložit, aby tak učinil sám.

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 komunikací1 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 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 písm. a) až f) jsou povinny bez zbytečného odkladu oznámit Úřadu provedení reaktivního opatření a jeho výsledek. Náležitosti oznámení stanoví prováděcí právní předpis.

§ 14

Úřad za účelem zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací[1] a na základě analýzy již vyřešeného kybernetického bezpečnostního incidentu jako ochranné opatření vydá opatření obecné povahy, ve kterém orgánům a osobám uvedeným v § 3 písm. c) až f) stanoví způsob zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací[1] a přiměřenou 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.

§ 15a

(1) Úřad může v případě hrozícího kybernetického bezpečnostního incidentu na návrh správce informačního systému, který marně vyzval provozovatele ke splnění povinnosti předat správci data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému, rozhodnutím uložit provozovateli tohoto systému povinnost předat správci data, provozní údaje a informace, které má k dispozici v souvislosti s provozováním tohoto systému; návrh musí obsahovat odůvodnění požadavku s ohledem na hrozící kybernetický bezpečnostní incident, podrobný popis předchozího jednání mezi provozovatelem a správcem tohoto systému zejména s ohledem na nesplnění smluvní povinnosti provozovatele a možné následky, pokud nedojde k předání požadovaných dat, provozních údajů a informací.

(2) Rozhodnutí o uložení povinnosti předat data, provozní údaje a informace podle odstavce 1 je prvním úkonem v řízení, je vykonatelné dnem doručení rozhodnutí a rozklad proti němu nemá odkladný účinek.

(3) Pro úhradu nákladů vynaložených provozovatelem informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému na předání dat, provozních údajů a informací podle odstavce 1 se ustanovení § 6a odst. 4 použije obdobně.

§ 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), b) a h) provozovateli národního CERT a

b) orgány a osoby uvedené v § 3 písm. c) až g) Úřadu.

(3) Orgány a osoby uvedené v § 3 písm. c) až g) 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) Úřad je dále oprávněn si pro účely kontroly vyžádat od provozovatele národního CERT kontaktní údaje orgánů a osob uvedených v § 3 písm. h).

(7) 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), b) a h) a tyto údaje eviduje a uchovává,

b) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. b) a h) a tyto údaje eviduje, uchovává a chrání,

c) vyhodnocuje kybernetické bezpečnostní incidenty u orgánů a osob uvedených v § 3 písm. b) a h),

d) poskytuje orgánům a osobám uvedeným v § 3 písm. a), b) a h) metodickou podporu, pomoc a součinnost při výskytu kybernetického bezpečnostního incidentu,

e) působí jako kontaktní místo pro orgány a osoby uvedené v § 3 písm. a), b) a h),

f) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti,

g) předává Úřadu údaje o kybernetických bezpečnostních incidentech ohlášených podle § 8 odst. 3, bez uvedení ohlašovatele,

h) předává Úřadu na vyžádání údaje podle § 16 odst. 5 a 6,

i) plní roli týmu CSIRT podle příslušného předpisu Evropské unie[12],

j) informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu s významným dopadem na

kontinuitu poskytování základní nebo digitální služby v tomto členském státě a zároveň o tom informuje Úřad, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele,

k) spolupracuje s týmy CSIRT jiných členských států a

l) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob neuvedených v § 3, a pokud to jeho kapacity umožňují, zpracovává je a poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost.

(3) Provozovatel národního CERT může vlastním jménem a na vlastní odpovědnost vykonávat i další hospodářskou 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.

(5) Provozovatel národního CERT musí při plnění povinností podle odstavce 2 postupovat nestranně.

§ 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,

f) nebyla pravomocně odsouzena za spáchání trestného činu uvedeného v § 7 zákona o trestní odpovědnosti právnických osob a řízení proti nim,

g) není zahraniční osobou podle jiného právního předpisu a

h) nebyla založena nebo zřízena výlučně za účelem dosažení zisku; tím není dotčena možnost provozovatele národního CERT postupovat podle § 17 odst. 3.

(3) Zájemce prokazuje splnění podmínek předložením

a) čestného prohlášení v případě odstavce 2 písm. a) až d), g) a h) 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 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 vykonává činnosti podle podle § 17 odst. 2 písm. a) až c), e) a g) až l) bezúplatně. Provozovatel národního CERT je povinen vynaložit k řádnému a účelnému výkonu činností uvedených v § 17 odst. 2 nezbytné náklady.

(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) vymezení podmínek pro výkon činnosti národního CERT podle § 17 odst. 3 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.

§ 20
Vládní CERT

Vládní CERT jako součást Úřadu

a) přijímá oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. c) až g),

b) přijímá hlášení o kybernetických bezpečnostních incidentech od orgánů a osob uvedených v § 3 písm. c) až g),

c) vyhodnocuje údaje o kybernetických bezpečnostních událostech a kybernetických bezpečnostních incidentech z kritické informační infrastruktury, informačního systému základní služby, významných informačních systémů a dalších informačních systémů veřejné správy,

d) poskytuje orgánům a osobám uvedeným v § 3 písm. c) až g) metodickou podporu a pomoc,

e) poskytuje součinnost orgánům a osobám uvedeným v § 3 písm. c) až g) 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 zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti údaje z evidence incidentů,

j) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti,

k) informuje bez uvedení identifikačních údajů ohlašovatele příslušný orgán jiného členského státu o kybernetickém bezpečnostním incidentu, který má významný dopad na kontinuitu poskytování základních služeb v tomto členském státě nebo se dotýká poskytování digitálních služeb v tomto členském státě, přičemž zachovává bezpečnost a obchodní zájmy ohlašovatele,

l) přijímá hlášení o kybernetickém bezpečnostním incidentu od orgánů a osob neuvedených v § 3; vládní CERT hlášení zpracovává, a pokud to jeho kapacity umožňují a jedná se o kybernetický bezpečnostní incident s významným dopadem, poskytuje orgánům nebo osobám dotčeným kybernetickým bezpečnostním incidentem metodickou podporu, pomoc a součinnost,

m) plní roli týmu CSIRT podle příslušného předpisu Evropské unie[12] a

n) spolupracuje s týmy CSIRT jiných členských států.

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 služeb elektronických komunikací anebo bezpečnost a integrita 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 komunikací1 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

Úřad

§ 21a

(1) Zřizuje se Úřad se sídlem v Brně jako ústřední správní úřad pro oblast kybernetické bezpečnosti a pro vybrané oblasti ochrany utajovaných informací podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti. Příjmy a výdaje Úřadu tvoří samostatnou kapitolu státního rozpočtu.

(2) V čele Úřadu je ředitel, kterého jmenuje po projednání ve výboru Poslanecké sněmovny příslušném ve věcech bezpečnosti vláda, která ho též odvolává.

(3) Ředitel Úřadu je odpovědný předsedovi vlády nebo pověřenému členovi vlády.

§ 22

Úřad

a) stanoví bezpečnostní opatření,

b) vydává opatření,

c) plní stanovené úkoly ve vybraných oblastech ochrany utajovaných informací,

d) vede evidence podle tohoto zákona a podle zákona o ochraně utajovaných informací,

e) ukládá správní tresty za nedodržení povinností stanovených tímto zákonem a zákonem o ochraně utajovaných informací a o bezpečnostní způsobilosti,

f) působí jako koordinační orgán ve stavu kybernetického nebezpečí,

g) spolupracuje s orgány a osobami, které působí v oblasti kybernetické bezpečnosti a kybernetické obrany, zejména s veřejnoprávními korporacemi, výzkumnými a vývojovými pracovišti a s ostatními pracovišti typu CERT, a s orgány a osobami, které působí ve vybraných oblastech ochrany utajovaných informací,

h) zajišťuje mezinárodní spolupráci v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,

i) sjednává a uzavírá smlouvy o mezinárodní spolupráci v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,

j) zajišťuje prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,

k) zajišťuje výzkum a vývoj v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací,

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),

o) ověřuje každé 2 roky aktuálnost určení prvků kritické infrastruktury podle písmen m) a n),

p) určuje provozovatele základní služby a informační systém základní služby,

q) zpracovává a vládě ke schválení předkládá národní strategii kybernetické bezpečnosti[13] a akční plán k jejímu naplňování a tuto strategii aktualizuje nejméně každých 5 let,

r) je jednotným kontaktním místem pro zajištění přeshraniční spolupráce v oblasti kybernetické bezpečnosti v rámci Evropské unie,

s) je příslušným orgánem v České republice a plní informační povinnosti vůči Evropské komisi a skupině pro spolupráci podle příslušného předpisu Evropské unie[14],

t) informuje veřejnost o kybernetickém bezpečnostním incidentu podle § 12 odst. 3,

u) provádí analýzu a monitoring kybernetických hrozeb a rizik,

v) vykonává působnost v oblasti veřejné regulované služby Evropského programu družicové navigace Galileo,

w) vydává Věstník Úřadu, který zveřejňuje na svých internetových stránkách,

x) plní další úkoly v oblasti kybernetické bezpečnosti stanovené tímto zákonem a ve vybraných oblastech ochrany utajovaných informací podle zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti.

§ 22a

Určení provozovatele základní služby a informačního systému základní služby

(1) Úřad rozhodnutím určí provozovatele základní služby a informační systém základní služby, pokud naplní odvětvová a dopadová kritéria, která zohledňují významnost

a) služeb poskytovaných v jednotlivých odvětvích uvedených v § 2 písm. i) a

b) dopad kybernetického bezpečnostního incidentu zejména na

1. rozsah a kvalitu poskytování základní služby uživatelům, kteří jsou na ní závislí,

2. ekonomické a společenské činnosti a veřejnou bezpečnost,

3. vzájemnou závislost odvětví uvedených v § 2 písm. i).

Dopadová a odvětvová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností stanoví prováděcí právní předpis.

(2) V případě, že Úřad zjistí, že orgán nebo osoba, které hodlá určit podle odstavce 1 jako provozovatele základní služby, poskytují danou službu i v jiném členském státě, provede před rozhodnutím ve věci konzultaci s příslušným orgánem dotčeného členského státu.

(3) Proti rozhodnutí Úřadu o určení provozovatele základní služby a informačního systému základní služby není rozklad přípustný.

(4) Úřad ověřuje nejméně každé 2 roky ode dne vydání rozhodnutí o určení provozovatele základní služby, zda jsou splněny podmínky pro určení provozovatele základní služby a informačního systému základní služby.

§ 22b

(1) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona ze základního registru obyvatel referenční údaje, kterými jsou

a) příjmení,

b) jméno, popřípadě jména,

c) adresa místa pobytu,

d) datum, místo a okres narození; u subjektu údajů, který se narodil v cizině, datum, místo a stát, kde se narodil,

e) datum, místo a okres úmrtí; jde-li o úmrtí subjektu údajů mimo území České republiky, datum úmrtí, místo a stát, na jehož území k úmrtí došlo,

f) státní občanství, popřípadě více státních občanství,

g) záznam o zřízení datové schránky a identifikátor datové schránky, je-li tato datová schránka zpřístupněna.

(2) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona z agendového informačního systému evidence obyvatel o státních občanech České republiky údaje, kterými jsou

a) jméno, popřípadě jména, příjmení, včetně předchozích příjmení, rodné příjmení,

b) rodné číslo, pokud není přiděleno, datum narození,

c) adresa místa trvalého pobytu, včetně předchozích adres místa trvalého pobytu, popřípadě adresa, na kterou mají být doručovány písemnosti podle jiného právního předpisu,

d) omezení svéprávnosti, jméno, popřípadě jména, příjmení a rodné číslo opatrovníka; nebylo-li opatrovníkovi rodné číslo přiděleno, datum, místo a okres narození; je-li opatrovníkem ustanoven orgán místní správy, název a adresa sídla,

e) datum, místo a okres úmrtí; jde-li o úmrtí občana mimo území České republiky, datum úmrtí, místo a stát, na jehož území k úmrtí došlo,

f) den, který byl v rozhodnutí soudu o prohlášení za mrtvého uveden jako den smrti, popřípadě jako den, který občan prohlášený za mrtvého nepřežil.

Údaje, které jsou vedeny jako referenční údaje v základním registru obyvatel, se využijí z agendového informačního systému evidence obyvatel, pouze pokud jsou ve tvaru předcházejícím současný stav.

(3) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona z informačního systému cizinců o cizincích údaje, kterými jsou

a) jméno, popřípadě jména, příjmení, rodné příjmení,

b) datum narození,

c) rodné číslo,

d) státní občanství, popřípadě více státních občanství,

e) druh a adresa místa pobytu,

f) číslo a platnost oprávnění k pobytu,

g) omezení svéprávnosti,

h) datum, místo a okres úmrtí; jde-li o úmrtí mimo území České republiky, stát, na jehož území k úmrtí došlo, popřípadě datum úmrtí,

i) den, který byl v rozhodnutí soudu o prohlášení za mrtvého uveden jako den smrti, popřípadě jako den, který cizinec prohlášený za mrtvého nepřežil.

Údaje, které jsou vedeny jako referenční údaje v základním registru obyvatel, se využijí z informačního systému cizinců, pouze pokud jsou ve tvaru předcházejícím současný stav.

(4) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona z registru rodných čísel o fyzických osobách, kterým bylo přiděleno rodné číslo, avšak nejsou vedeny v agendovém informačním systému evidence obyvatel, údaje, kterými jsou

a) jméno, popřípadě jména, příjmení, popřípadě rodné příjmení,

b) rodné číslo,

c) v případě změny rodného čísla původní rodné číslo,

d) den, měsíc a rok narození,

e) místo a okres narození; u fyzické osoby narozené v cizině stát, na jehož území se narodila.

(5) Úřadu jsou poskytovány pro výkon působnosti podle tohoto zákona ze základního registru právnických osob, podnikajících fyzických osob a orgánů veřejné moci údaje, kterými jsou

a) obchodní firma nebo název právnické osoby nebo jméno, popřípadě jména, a příjmení podnikající fyzické osoby,

b) datum vzniku nebo datum zápisu do evidence podle zvláštních právních předpisů,

c) datum zániku nebo datum výmazu z evidence podle zvláštních právních předpisů,

d) právní forma,

e) záznam o zřízení datové schránky a identifikátor datové schránky, je-li tato datová schránka zpřístupněna,

f) statutární orgán vyjádřený referenční vazbou na registr obyvatel anebo na registr osob nebo údajem o jménu, popřípadě jménech, příjmení a bydlišti u zahraniční fyzické osoby,

g) právní stav,

h) adresa sídla právnické osoby nebo adresa místa podnikání fyzické osoby ve formě referenční vazby (kódu adresního místa) na referenční údaj o adrese v registru územní identifikace.

(6) K údajům podle odstavců 2 až 5 vedeným v agendových informačních systémech jsou Úřadu poskytovány i jejich předchozí změny.

(7) Z poskytovaných údajů lze v konkrétním případě použít vždy jen takové údaje, které jsou nezbytné ke splnění daného úkolu.

§ 22c
Zpracování osobních údajů

(1) Úřad a provozovatel národního CERT zpracovávají osobní údaje, jsou-li nezbytné pro výkon jejich působnosti. Tyto údaje Úřad a provozovatel národního CERT předávají orgánům veřejné moci nebo osobám, je-li to nezbytné pro plnění jejich úkolů.

(2) Úřad a provozovatel národního CERT při zpracování osobních údajů, na které se vztahuje nařízení Evropského parlamentu a Rady (EU) 2016/679,

a) nemusí omezit zpracování osobních údajů v případě, že subjekt údajů popírá jejich přesnost nebo vznesl námitku proti tomuto zpracování, a

b) může v rámci výkonu své působnosti využít osobní údaje i pro jiné účely, než pro které byly shromážděny.

(3) Pokud Úřad nebo provozovatel národního CERT v rámci činnosti, na kterou se vztahuje nařízení Evropského parlamentu a Rady (EU) 2016/679, při řešení kybernetického bezpečnostního incidentu nebo kybernetické bezpečnostní události anebo při prevenci kybernetických hrozeb nebo rizik obdrží osobní údaje, které zpracovává pouze za účelem plnění povinností podle tohoto zákona, po dobu plnění těchto povinností dále nemusí

a) poskytovat subjektu údajů informace o opravách nebo výmazech osobních údajů nebo omezení jejich zpracování,

b) zajistit přístup subjektu údajů k osobním údajům, nebo

c) opravit či doplnit osobní údaje na žádost subjektu údajů.

Hlava V
Kontrola, nápravná opatření a přestupky

§ 23
Kontrola

(1) Úřad vykonává kontrolu v oblasti kybernetické bezpečnosti. Při výkonu kontroly Úřad zjišťuje, jak orgány a osoby uvedené v § 3 písm. a) až g) plní povinnosti stanovené tímto zákonem a rozhodnutími a opatřeními obecné povahy vydanými Úřadem podle tohoto zákona, a dodržují prováděcí právní předpisy v oblasti kybernetické bezpečnosti. Je-li důvodné podezření, že poskytovatel digitální služby neplní povinnosti stanovené tímto zákonem, provede u něj Úřad kontrolu.

(2) Při výkonu kontroly se postupuje přiměřeně podle kontrolního řádu.

(3) Kontrolu vykonávají pověření zaměstnanci Úřadu.

§ 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, informační systém základní služby 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.

Kontrola činnosti Úřadu

§ 24a

(1) Kontrolu činnosti Úřadu vykonává Poslanecká sněmovna, která k tomuto účelu zřizuje zvláštní kontrolní orgán (dále jen „kontrolní orgán“).

(2) Kontrolní orgán se skládá nejméně ze 7 členů. Poslanecká sněmovna stanoví počet členů tak, aby byl zastoupen každý poslanecký klub ustavený podle příslušnosti k politické straně nebo politickému hnutí, za něž poslanci kandidovali ve volbách; počet členů je vždy lichý. Členem kontrolního orgánu může být pouze poslanec Poslanecké sněmovny.

(3) Pokud tento zákon nestanoví jinak, vztahuje se na jednání kontrolního orgánu a na práva a povinnosti jeho členů přiměřeně jiný právní předpis[15].

(4) Členové kontrolního orgánu mohou vstupovat v doprovodu ředitele Úřadu nebo jím pověřeného zaměstnance do objektů Úřadu.

(5) Ředitel Úřadu předkládá kontrolnímu orgánu

a) zprávu o činnosti Úřadu,

b) návrh rozpočtu Úřadu,

c) podklady potřebné ke kontrole plnění rozpočtu Úřadu,

d) vnitřní předpisy Úřadu,

e) na vyžádání zprávu o jednotlivých kybernetických bezpečnostních incidentech z kritické informační infrastruktury, významných informačních systémů a informačních systémů základní služby.

§ 24b

(1) Má-li kontrolní orgán za to, že činnost Úřadu nezákonně omezuje nebo poškozuje práva a svobody občanů nebo že rozhodovací činnost Úřadu v rámci správního řízení je stižena vadami, je oprávněn požadovat od ředitele Úřadu potřebné vysvětlení.

(2) Každé porušení zákona zaměstnancem Úřadu při plnění povinností podle tohoto zákona a ve vybraných oblastech podle zákona o ochraně utajovaných informací a o bezpečnostní

způsobilosti, které kontrolní orgán zjistí při své činnosti, je povinen oznámit řediteli Úřadu a předsedovi vlády.

§ 24c

Povinnost zachovávat mlčenlivost uložená členům kontrolního orgánu podle zákona se nevztahuje na případy, kdy kontrolní orgán podává oznámení podle § 24b odst. 2.

Přestupky

§ 25

(1) Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací nebo orgán nebo osoba zajišťující významnou síť se dopustí přestupku 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) Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury nebo správce nebo provozovatel významného informačního systému se dopustí přestupku 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 4,

c) nesplní povinnost uloženou Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13 nebo 14,

d) nesplní povinnost uloženou Úřadem v rozhodnutí podle § 15a odst. 1,

e) nepředá data, provozní údaje a informace podle § 6a odst. 2,

f) nepředá data, provozní údaje a informace podle § 6a odst. 3,

g) nezničí kopie dat, provozních údajů a informací podle § 6a odst. 3,

h) neumožní správci dohled nad průběhem zničení dat, provozních údajů a informací podle § 6a odst. 3,

i) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 16 odst. 2 písm. b) nebo

j) nesplní některou z povinností uloženou nápravným opatřením podle § 24.

(3) Správce informačního nebo komunikačního systému kritické informační infrastruktury nebo významného informačního systému se dopustí přestupku tím, že neinformuje provozovatele systému podle § 4a odst. 1.

(4) Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že neinformuje subjekt zajišťující síť elektronických komunikací podle § 4a odst. 2.

(5) Provozovatel informačního nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že

a) nesplní povinnost uloženou Úřadem v rozhodnutí podle § 15a odst. 1,

b) nepředá data, provozní údaje a informace podle § 6a odst. 2,

c) nepředá data, provozní údaje a informace podle § 6a odst. 3,

d) nezničí kopie dat, provozních údajů a informací podle § 6a odst. 3, nebo

e) neumožní správci dohled nad průběhem zničení dat, provozních údajů a informací podle § 6a odst. 3.

(6) Orgán nebo osoba zajišťující významnou síť se dopustí přestupku tím, že neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 3.

(7) Správce a provozovatel informačního systému základní služby se dopustí přestupku tím, že

a) v rozporu s § 4 odst. 2 nezavede nebo neprovádí bezpečnostní opatření nebo nevede bezpečnostní dokumentaci,

b) neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 4,

c) nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3,

d) nesplní povinnost uloženou Úřadem podle § 13 nebo 14,

e) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 16 odst. 2 písm. b), nebo

f) nesplní některou z povinností uloženou nápravným opatřením podle § 24.

(8) Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury, správce nebo provozovatel významného informačního systému, správce nebo provozovatel informačního systému základní služby a provozovatel základní služby, kteří jsou orgánem veřejné moci, se dopustí přestupku tím, že uzavřou smlouvu s poskytovatelem služeb cloud computingu v rozporu s § 4 odst. 5.

(9) Správce nebo provozovatel informačního nebo komunikačního systému kritické informační infrastruktury se dopustí přestupku tím, že nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3.

(10) Provozovatel základní služby se dopustí přestupku tím, že

a) neinformuje správce nebo provozovatele informačního systému základní služby podle § 4a odst. 3,

b) nenahlásí významný dopad na kontinuitu poskytování základní služby podle § 8 odst. 1 a 4,

c) nenahlásí významný dopad na kontinuitu poskytování základní služby způsobený kybernetickým bezpečnostním incidentem podle § 8 odst. 8,

d) nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3, nebo

e) neoznámí kontaktní údaje nebo jejich změnu Úřadu podle § 16 odst. 2 písm. b).

(11) Poskytovatel digitální služby se dopustí přestupku tím, že

a) neustaví svého zástupce podle § 3a odst. 1,

b) v rozporu s § 4 odst. 3 nezavede nebo neprovádí bezpečnostní opatření,

c) neohlásí kybernetický bezpečnostní incident podle § 8 odst. 2 a 3,

d) nesplní povinnost informovat veřejnost uloženou Úřadem podle § 12 odst. 3, nebo

e) neoznámí kontaktní údaje nebo jejich změnu podle § 16 odst. 2 písm. a).

(12) Za přestupek lze uložit pokutu do

a) 5 000 000 Kč, jde-li o přestupek podle odstavce 2 písm. a), odstavce 7 písm. a) nebo odstavce 11 písm. b),

b) 1 000 000 Kč, jde-li o přestupek podle odstavce 1 písm. a) nebo b), odstavce 2 písm. b), c) nebo e), odstavce 3, odstavce 4, odstavce 5 písm. a), c) nebo d), odstavce 6, odstavce 7 písm. b) až d) nebo f), odstavce 8, odstavce 9, odstavce 10 písm. a) až d) nebo odstavce 11 písm. a), c) nebo d),

c) 200 000 Kč, jde-li o přestupek podle odstavce 5 písm. b) nebo e),

d) 10 000 Kč, jde-li o přestupek podle odstavce 2 písm. d), odstavce 7 písm. e), odstavce 10 písm. e) nebo odstavce 11 písm. e).

§ 26

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

(2) Za přestupek podle odstavce 1 lze uložit pokutu do 50 000 Kč.

§ 27
Společné ustanovení k přestupkům

Přestupky podle tohoto zákona projednává a pokuty vybírá Úřad.

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) a obsah a rozsah bezpečnostních pravidel podle § 6 písm. e),

b) typy, kategorie a hodnocení významnosti kybernetických bezpečnostních incidentů a náležitosti a způsob hlášení kybernetického bezpečnostního incidentu podle § 8 odst. 7,

c) náležitosti oznámení o provedení reaktivního opatření a jeho výsledku podle § 13 odst. 4,

d) vzor oznámení kontaktních údajů a jeho formu podle § 16 odst. 7,

e) dopadová a odvětvová kritéria pro určení provozovatele základní služby a vymezení významnosti dopadu narušení základní služby na zabezpečení společenských nebo ekonomických činností podle § 22a odst. 1,

f) způsob likvidace dat, provozních údajů, informací a jejich kopií.

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 4 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 4 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 a Generální inspekce bezpečnostních sborů 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.

(3) Tento zákon se vztahuje pouze na poskytovatele digitální služby, který je právnickou osobou a není mikropodnikem nebo malým podnikem[16].

(4) Tento zákon se nevztahuje na poskytovatele digitální služby, který má sídlo v jiném členském státě.

ČÁST DRUHÁ

zrušena (§ 34)

§ 34

zrušen

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. 181/2014 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 a) se doplňují slova „nebo odstavce 14 písm. ad)“.

ČÁST ČTVRTÁ

zrušena (§ 36)

§ 36

zrušen

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.

Hamáček v. r.

Zeman v. r.

Sobotka v. r.

Poznámky pod čarou:

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.
3) Například § 98 odst. 4 a § 99 odst. 4 zákona č. 127/2005 Sb., ve znění pozdějších předpisů.
4) Ústavní zákon č. 110/1998 Sb., o bezpečnosti České republiky, ve znění ústavního zákona č. 300/2000 Sb.
5) Zákon č. 269/1994 Sb., o Rejstříku trestů, ve znění pozdějších předpisů.
6) Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii.
7) § 2 písm. h) zákona č. 127/2005 Sb., ve znění pozdějších předpisů.
8) Čl. 5 odst. 7 směrnice Evropského parlamentu a Rady (EU) 2016/1148.
9) § 2 písm. a) zákona č. 480/2004 Sb., o některých službách informační společnosti a o změně některých zákonů (zákon o některých službách informační společnosti).
10) § 2 odst. 1 písm. a) a b) zákona č. 634/1992 Sb., o ochraně spotřebitele, ve znění pozdějších předpisů. § 419 a 420 zákona č. 89/2012 Sb., občanský zákoník.
11) Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).
12) Čl. 9 směrnice Evropského parlamentu a Rady (EU) 2016/1148.
13) Čl. 7 směrnice Evropského parlamentu a Rady (EU) 2016/1148.
14) Například čl. 5 odst. 3, čl. 7 odst. 3 a čl. 8 směrnice Evropského parlamentu a Rady (EU) 2016/1148.
15) Zákon č. 90/1995 Sb., o jednacím řádu Poslanecké sněmovny, ve znění pozdějších předpisů.
16) Příloha doporučení Komise 2003/361/ES ze dne 6. května 2003 o definici mikropodniků a malých a středních podniků.