# 181/2014 Sb.

## ZÁKON

ze dne 23. července 2014

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

Parlament se usnesl na tomto zákoně České republiky:

## ČÁST PRVNÍ

## KYBERNETICKÁ BEZPEČNOST

### HLAVA I

### ZÁKLADNÍ USTANOVENÍ

§ 1

**Předmět úpravy**

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

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

**Vymezení pojmů**

§ 2

V tomto zákoně se rozumí

a) kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací[1)],

b) kritickou informační infrastrukturou prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy[2)] v oblasti kybernetické bezpečnosti,

c) bezpečností informací zajištění důvěrnosti, integrity a dostupnosti informací,

d) významným informačním systémem informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci,

e) správcem informačního systému orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního systému,

f) správcem komunikačního systému orgán nebo osoba, které určují účel komunikačního systému a podmínky jeho provozování, a

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

§ 3

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

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací[1)], pokud není orgánem nebo osobou podle písmene b),

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

c) správce informačního systému kritické informační infrastruktury,

d) správce komunikačního systému kritické informační infrastruktury a

e) správce významného informačního systému.

# HLAVA II

# SYSTÉM ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI

**Bezpečnostní opatření**

§ 4

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

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

(3) Orgány a osoby uvedené v § 3 písm. c) až e) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatelů pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury nebo významný informační systém. 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

(1) Bezpečnostními opatřeními jsou

a) organizační opatření a

b) technická opatření.

(2) Organizačními opatřeními jsou

a) systém řízení bezpečnosti informací,

b) řízení rizik,

c) bezpečnostní politika,

d) organizační bezpečnost,

e) stanovení bezpečnostních požadavků pro dodavatele,

f) řízení aktiv,

g) bezpečnost lidských zdrojů,

h) řízení provozu a komunikací kritické informační infrastruktury nebo významného informačního systému,

i) řízení přístupu osob ke kritické informační infrastruktuře nebo k významnému informačnímu systému,

j) akvizice, vývoj a údržba kritické informační infrastruktury a významných informačních systémů,

k) zvládání kybernetických bezpečnostních událostí a kybernetických

bezpečnostních incidentů,

l) řízení kontinuity činností a

m) kontrola a audit kritické informační infrastruktury a významných informačních systémů.

(3) Technickými opatřeními jsou

a) fyzická bezpečnost,

b) nástroj pro ochranu integrity komunikačních sítí,

c) nástroj pro ověřování identity uživatelů,

d) nástroj pro řízení přístupových oprávnění,

e) nástroj pro ochranu před škodlivým kódem,

f) nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů,

g) nástroj pro detekci kybernetických bezpečnostních událostí,

h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí,

i) aplikační bezpečnost,

j) kryptografické prostředky,

k) nástroj pro zajišťování úrovně dostupnosti informací a

l) bezpečnost průmyslových a řídících systémů.

§ 6

Prováděcí právní předpis stanoví

a) obsah bezpečnostních opatření,

b) obsah a strukturu bezpečnostní dokumentace,

c) rozsah bezpečnostních opatření pro orgány a osoby uvedené v § 3 písm. c) až e) a

d) významné informační systémy a jejich určující kritéria.

§ 6a

**neplatil**

**Kybernetická bezpečnostní událost a kybernetický bezpečnostní incident**

§ 7

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

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

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

§ 8

**Hlášení kybernetického bezpečnostního incidentu**

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

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

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

(4) Prováděcí právní předpis stanoví

a) typy a kategorie kybernetických bezpečnostních incidentů a

b) náležitosti a způsob hlášení kybernetického bezpečnostního incidentu.

**Evidence**

§ 9

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

a) hlášení kybernetického bezpečnostního incidentu,

b) identifikační údaje systému, ve kterém se kybernetický bezpečnostní incident vyskytl,

c) údaje o zdroji kybernetického bezpečnostního incidentu a

d) postup při řešení kybernetického bezpečnostního incidentu a jeho výsledek.

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

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

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

§ 10

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

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

§ 11

**Opatření**

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

(2) Opatřeními jsou

a) varování,

b) reaktivní opatření a

c) ochranné opatření.

(3) Reaktivní opatření jsou povinny provádět

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

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

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

§ 12

**Varování**

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

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

**Reaktivní a ochranné opatření**

§ 13

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

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

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

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

§ 14

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

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

§ 15

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

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

§ 15a

**neplatil**

§ 16

**Kontaktní údaje**

(1) Kontaktními údaji jsou

a) u právnické osoby obchodní firma nebo název, adresa sídla, identifikační číslo osoby nebo obdobné číslo přidělované v zahraničí,

b) u podnikající fyzické osoby obchodní firma nebo jméno včetně odlišujícího dodatku nebo dalšího označení, adresa sídla a identifikační číslo osoby,

c) u orgánu veřejné moci jeho název, adresa sídla, identifikační číslo osoby, bylo-li přiděleno, a identifikátor orgánu veřejné moci, pokud mu není přiděleno identifikační číslo osoby, a údaje o fyzické osobě, která je za orgán nebo osobu uvedené v § 3 oprávněna jednat ve věcech upravených tímto zákonem, a to jméno, příjmení, telefonní číslo a adresa elektronické pošty.

(2) Kontaktní údaje a jejich změny oznamují

a) orgány a osoby uvedené v § 3 písm. a) a b) provozovateli národního CERT a

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

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

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

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

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

§ 17

**Národní CERT**

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

(2) Provozovatel národního CERT

a) přijímá oznámení kontaktních údajů od orgánů a osob uvedených v § 3 písm. a) a b) a tyto údaje eviduje a uchovává,

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

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

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

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

f) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti,

g) předává Úřadu údaje o kybernetických bezpečnostních incidentech bez uvedení ohlašovatele kybernetického bezpečnostního incidentu a

h) předává na vyžádání Úřadu za stavu kybernetického nebezpečí kontaktní údaje orgánů a osob uvedených v § 3 písm. a) a b).

(3) Provozovatel národního CERT může 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 § 17 odst. 2 písm. a), b), c), e), g) a h) bezúplatně.

(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 e),

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

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

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

e) poskytuje součinnost orgánům a osobám uvedeným v § 3 písm. c) až e) při výskytu kybernetického bezpečnostního incidentu a kybernetické bezpečnostní události,

f) přijímá podněty a údaje od orgánů a osob uvedených v § 3 a od jiných orgánů a osob a tyto podněty a údaje vyhodnocuje,

g) přijímá údaje od provozovatele národního CERT a tyto údaje vyhodnocuje,

h) přijímá údaje od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, a tyto údaje vyhodnocuje,

i) poskytuje podle § 9 odst. 4 provozovateli národního CERT, orgánům vykonávajícím působnost v oblasti kybernetické bezpečnosti v zahraničí a jiným osobám působícím v oblasti kybernetické bezpečnosti údaje z evidence incidentů a

j) provádí hodnocení zranitelností v oblasti kybernetické bezpečnosti.

## HLAVA III

## STAV KYBERNETICKÉHO NEBEZPEČÍ

### § 21

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

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

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

(4) V průběhu vyhlášeného stavu kybernetického nebezpečí ředitel Úřadu informuje vládu o postupech při řešení stavu kybernetického nebezpečí a o aktuálním stavu hrozeb, které vedly k vyhlášení stavu kybernetického nebezpečí. Za stavu kybernetického nebezpečí a za nouzového stavu[4)] v případech podle odstavce 6 je Úřad oprávněn vydat rozhodnutí nebo opatření obecné povahy podle § 13 rovněž orgánům a osobám uvedeným v § 3 písm. a) a b).

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

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

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

## HLAVA IV

## VÝKON STÁTNÍ SPRÁVY

### § 22

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

(2) Úřad

a) stanoví bezpečnostní opatření,
b) vydává opatření,
c) zajišťuje činnost Národního centra kybernetické bezpečnosti,
d) vede evidence podle tohoto zákona,
e) ukládá pokuty za správní delikty podle tohoto zákona,
f) působí jako koordinační orgán ve stavu kybernetického nebezpečí,
g) spolupracuje s orgány a osobami, které působí v oblasti kybernetické bezpečnosti, zejména s veřejnoprávními korporacemi, výzkumnými a vývojovými pracovišti a s ostatními pracovišti typu CERT,
h) zajišťuje mezinárodní spolupráci,
i) sjednává a uzavírá smlouvy o mezinárodní spolupráci,

j) zajišťuje prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti,

k) zajišťuje výzkum a vývoj v oblasti kybernetické bezpečnosti,

l) uzavírá veřejnoprávní smlouvu s provozovatelem národního CERT,

m) zasílá podle krizového zákona Ministerstvu vnitra návrh prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, jejichž provozovatelem je organizační složka státu,

n) určuje podle krizového zákona prvky kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti, pokud nejde o prvky uvedené v písmeni m), a

o) plní další úkoly v oblasti kybernetické bezpečnosti stanovené tímto zákonem.

## HLAVA V

## KONTROLA, NÁPRAVNÁ OPATŘENÍ A SPRÁVNÍ DELIKTY

### § 23

### Kontrola

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

(2) Úřad kontroluje, jak

a) orgány a osoby uvedené v § 3 písm. a) a b) plní povinnosti uložené Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13 za stavu kybernetického nebezpečí,

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

### § 24

### Nápravná opatření

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

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

## Správní delikty

§ 25

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

a) nesplní za stavu kybernetického nebezpečí povinnost uloženou Úřadem v rozhodnutí nebo v opatření obecné povahy podle § 13, nebo

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

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

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

b) neohlásí kybernetický bezpečnostní incident podle § 8 odst. 1 a 3,

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

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

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

(3) Za správní delikt se uloží pokuta do

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

b) 10 000 Kč, jde-li o správní delikt podle odstavce 2 písm. d).

§ 26

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

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

§ 27

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

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

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

(4) Správní delikty podle tohoto zákona projednává Úřad.

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

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

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

# HLAVA VI

# ZÁVĚREČNÁ USTANOVENÍ

§ 28

**Zmocňovací ustanovení**

(1) Úřad a Ministerstvo vnitra stanoví vyhláškou významné informační systémy

a jejich určující kritéria podle § 6 písm. d).

(2) Úřad stanoví vyhláškou

a) obsah a strukturu bezpečnostní dokumentace, obsah bezpečnostních opatření a rozsah bezpečnostních opatření podle § 6 písm. a) až c),

b) typy a kategorie kybernetických bezpečnostních incidentů a náležitosti a způsob hlášení kybernetického bezpečnostního incidentu podle § 8 odst. 4,

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

d) vzor oznámení kontaktních údajů a jeho formu podle § 16 odst. 6.

## Přechodná ustanovení

### § 29

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

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

### § 30

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

a) oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou,

b) začnou plnit povinnost stanovenou v § 8 odst. 1 a 3 nejpozději do 1 roku ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou a

c) zavedou bezpečnostní opatření podle § 4 odst. 2 nejpozději do 1 roku ode dne určení jejich informačního systému nebo komunikačního systému kritickou informační infrastrukturou.

### § 31

Orgány a osoby uvedené v § 3 písm. e)

a) oznámí kontaktní údaje podle § 16 nejpozději do 30 dnů ode dne naplnění určujících kritérií významného informačního systému jejich informačních systémů,

b) začnou plnit povinnost stanovenou v § 8 odst. 1 a 3 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému a

c) zavedou bezpečnostní opatření podle § 4 odst. 2 nejpozději do 1 roku ode dne naplnění určujících kritérií významného informačního systému.

§ 32

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

§ 33

**Společná ustanovení**

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

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

# ČÁST DRUHÁ

# Změna zákona o ochraně utajovaných informací a o bezpečnostní způsobilosti

§ 34

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní

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

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

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

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

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

# ČÁST TŘETÍ

## Změna zákona o elektronických komunikacích

§ 35

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění zákona č. 290/2005 Sb., zákona č. 361/2005 Sb., zákona č. 186/2006 Sb., zákona č. 235/2006 Sb., zákona č. 310/2006 Sb., zákona č. 110/2007 Sb., zákona č. 261/2007 Sb., zákona č. 304/2007 Sb., zákona č. 124/2008 Sb., zákona č. 177/2008 Sb., zákona č. 189/2008 Sb., zákona č. 247/2008 Sb., zákona č. 384/2008 Sb., zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 153/2010 Sb., nálezu Ústavního soudu, vyhlášeného pod č. 94/2011 Sb., zákona č. 137/2011 Sb., zákona č. 341/2011 Sb., zákona č. 375/2011 Sb., zákona č. 420/2011 Sb., zákona č. 457/2011 Sb., zákona č. 458/2011 Sb., zákona č. 468/2011 Sb., zákona č. 18/2012 Sb., zákona č. 19/2012 Sb., zákona č. 142/2012 Sb., zákona č. 167/2012 Sb., zákona č. 273/2012 Sb., zákona č. 214/2013 Sb. a zákona č. 303/2013 Sb., se mění takto:

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

„(4) Podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinen na žádost účastníka

bezplatně a ve formě umožňující další elektronické zpracování dat poskytnout mu provozní a lokalizační údaje, které má k dispozici na základě tohoto zákona, pokud je nemohl účastník pro poruchu na jeho zařízení v důsledku kybernetického bezpečnostního incidentu[62)] zachytit nebo uložit. Údaje podnikatel předá, je-li to technicky možné, bezodkladně, nejpozději však do 3 dnů ode dne doručení žádosti nebo v případě probíhající komunikace ode dne jejího uskutečnění.

62) § 7 odst. 2 zákona č. 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

## Změna zákona o svobodném přístupu k informacím

§ 36

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

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

## ČÁST PÁTÁ

## Změna zákona o provozování rozhlasového a televizního vysílání

§ 37

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

## ČÁST ŠESTÁ

## ÚČINNOST

§ 38

Tento zákon nabývá účinnosti dnem 1. ledna 2015.

**Hamáček v. r.**

**Zeman v. r.**

**Sobotka v. r.**

## Vybraná ustanovení novel

### Čl.IV zákona č. 104/2017 Sb.

**neplatil**

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.