ZÁKON
č. 181/2014 Sb.

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.

Z důvodové zprávy:

Věcná působnost zákona je vymezena obecně pro oblast kybernetické bezpečnosti s výjimkou informačních a komunikačních systémů nakládajících s utajovanými informacemi. Pojmu kybernetické bezpečnosti je užito k odlišení od pojmu informační bezpečnosti resp. počítačové bezpečnosti a ke zdůraznění specifického zaměření zákona na ochranu funkčnosti síťového prostředí umožňujícího vznik, zpracování, uchovávání a komunikaci informací, které je tvořeno informačními systémy a službami a sítěmi elektronických komunikací.

Specifické omezení působnosti zákona vztahující se k informačním a komunikačním systémům nakládajícím s utajovanými informacemi je důsledkem toho, že úprava povinných bezpečnostních parametrů

těchto systémů včetně navazujících právních povinností, kompetencí orgánů veřejné moci, kontroly, sankcí apod., je komplexně provedena zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. Do této právní úpravy není v současné době důvod zasahovat, neboť tyto systémy podléhají certifikaci, tj. vyšší formě regulace.

K odst. 1

1. V úvodním ustanovení je vymezena věcná působnost zákona č. 181/2014, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), dále jen „zák. o kyber. bezpečnosti", a to jak pozitivně, tak negativně. Pozitivní vymezení působnosti zákona je obsaženo v odstavci 1. Zákon o kybernetické bezpečnosti upravuje práva a povinnosti osob, jakož i pravomoc a působnost orgánů veřejné moci, a to v oblasti kybernetické bezpečnosti.

2. Orgány veřejné moci obecně představují orgány moci zákonodárné, výkonné a soudní, jakož i orgány samosprávy. Subjekt vystupuje jako orgán veřejné moci, pokud rozhoduje o právech a povinnostech jiných osob a tato rozhodnutí jsou státní mocí vynutitelná, přičemž stát může do těchto práv a povinností zasahovat.[1] Nejdůležitějším orgánem veřejné moci, který vykonává státní správu v oblasti kybernetické bezpečnosti, je Národní bezpečnostní úřad. Významné úkoly jsou svěřeny i národnímu CERT, se kterým Národní bezpečnostní úřad uzavírá veřejnoprávní smlouvu, a vládnímu CERT, který je součástí Národního bezpečnostního úřadu.

3. Kybernetickou bezpečností rozumíme souhrn prostředků směřujících k zajištění ochrany kybernetického prostoru.[2] Tyto prostředky mohou být různého charakteru – právní, organizační, vzdělávací, technické apod. Pro účely zákona o kybernetické bezpečnosti je však nutno termín „kybernetická bezpečnost" chápat především ve smyslu právních prostředků zajišťujících ochranu kybernetického prostoru, které jsou obsaženy v tomto zákoně. Hlavním smyslem zákona o kybernetické bezpečnosti je ochrana funkčnosti kybernetického prostoru. Kybernetickým prostorem označujeme digitální prostředí, které slouží ke zpracování a výměně informací a tvoří jej informačními systémy a služby a sítě elektronických komunikací.[3] Ty umožňují vznik, zpracování, uchovávání a komunikaci informací.

K odst. 2

4. Negativní vymezení věcné působnosti zákona o kybernetické bezpečnosti je obsaženo v odstavci 2. Z působnosti zákona jsou vyňaty informační nebo komunikační systémy, které nakládají s utajovanými informacemi. Důvodem pro toto vynětí je, že tyto systémy jsou regulovány zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti (dále jen „zák. o ochraně utaj. informací").

---

1 KLÍMA, K. *Státověda.* Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2006, s. 177.

2 Srov. JIRÁSEK, P, NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. 2., aktualiz. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013, s. 57 [cit. 2014-12-30]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.

3 Tamtéž, s. 59.

5. Jako utajovaná je souladu s § 2 zák. o ochraně utaj. informací označována informace zaznamenaná v jakékoliv podobě a na libovolném nosiči, jejíž vyzrazení nebo zneužití je způsobilé zapříčinit újmu zájmu České republiky. Mezi zájmy České republiky patří především zachování jejích základních atributů coby svrchovaného, jednotného a demokratického právního státu [srov. čl. 1 odst. 1 ústavního zákona č. 1/1993 Sb., Ústava České republiky (dále jen „Ústava")], jakož i zajištění vnitřní a vnější bezpečnosti státu. Chráněna je i ekonomika státu a život a zdraví fyzických osob. Dle závažnosti újmy, kterou by mohlo vyzrazení či zneužití informace způsobit chráněnému zájmu, jsou utajované informace klasifikovány stupni utajení. Stupně utajení jsou v § 4 zák. o ochraně utaj. informací rozlišovány čtyři – přísně tajné, tajné, důvěrné a vyhrazené. Informační systém, který nakládá s utajovanými informacemi, podléhá certifikaci Národním bezpečnostním úřadem. Komunikační systém, který zajišťuje přenos těchto informací mezi koncovými uživateli, lze provozovat pouze na základě projektu bezpečnosti komunikačního systému schváleného Národním bezpečnostním úřadem.

Související ustanovení:
§ 3 – povinné subjekty, § 22 – státní správa, § 33 – společná ustanovení

Související předpisy:
§ 2, § 4 zák. o ochraně utaj. informací

Vymezení pojmů

§ 2
(Definice pojmů)

V tomto zákoně se rozumí

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

b) 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.

[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.

Z důvodové zprávy:

Pojem kybernetického prostoru je definován jako informační prostředí k realizaci informačních transakcí, které je vytvořeno technologiemi, jejichž definice a podmínky užívání upravují zvláštní zákony, tj. informačními systémy, službami a sítěmi elektronických komunikací. Jedná se přitom i o takové informační systémy, služby a sítě elektronických komunikací, které nejsou připojeny k veřejné síti, tj. k internetu.

Definice pojmu „kritická informační infrastruktura" vychází z právních předpisů upravujících oblast krizového řízení. Vychází se přitom z předpokladu, že kritická informační infrastruktura bude součástí kritické infrastruktury, která je vymezena zákonem č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon) ve znění pozdějších předpisů („dále jen krizový zákon")[4]. Aby mohl být určitý informační systém nebo služba a síť elektronických komunikací zařazena do kritické informační infrastruktury, bude muset splnit definiční kritéria kritické infrastruktury, jakož i prvku kritické infrastruktury[5], vymezené krizovým zákonem a dále pak i průřezová[6] a odvětvová kritéria stanovená nařízením vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury. V odvětvových kritériích pro určení prvku kritické infrastruktury se předpokládá doplnění bodu VI. „Komunikační a informační systémy" o oblast kybernetické bezpečnosti, v níž budou stanovena odvětvová kritéria pro určení daného informačního systému, služby nebo sítě elektronických komunikací kritickou informační infrastrukturou. Těmito kritérii bude především skutečnost, že daný informační systém, služba nebo síť elektronických komunikací bude zajišťovat provoz již určeného prvku kritické infrastruktury a bude pro tento prvek nenahraditelný, anebo že daný informační systém, služba nebo síť elektronických komunikací bude zajišťovat jinou významnou činnost nebo službu sám o sobě, aniž by byl spojen s již určeným prvkem. Pokud jednotlivé informační systémy, služby a sítě elektronických komunikací splní všechny shora uvedené podmínky, budou určeny prvkem kritické infrastruktury standardním postupem podle krizového zákona. Pokud bude provozovatelem daného prvku organizační složka státu, bude prvek určen usnesením vlády, v ostatních případech pak opatřením obecné povahy vydaným NBÚ

---

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

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

[6] Průřezovým kritériem pro určení prvku kritické infrastruktury je hledisko
a) obětí s mezní hodnotou více než 250 mrtvých nebo více než 2 500 osob s následnou hospitalizací po dobu delší než 24 hodin,
b) ekonomického dopadu s mezní hodnotou hospodářské ztráty státu vyšší než 0,5 % hrubého domácího produktu, nebo
c) dopadu na veřejnost s mezní hodnotou rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.

a tímto postupem se tyto systémy, služby nebo sítě stanou kritickou informační infrastrukturou podle zákona o kybernetické bezpečnosti.

Pojem bezpečnosti informací vychází ve své definici z významu tohoto pojmu v odvětví informačních věd a týká se důvěrnosti (tj. diskrece), jednoty (tj. integrity) a dostupnosti informace. Pojem se netýká obsahu informace, ale pouze funkčnosti prostředí, v němž je informace tvořena, zpracovávána, uchovávána a komunikována. To odpovídá principu technologické neutrality, na němž zákon spočívá a má za následek důsledné vyčlenění kritéria obsahu informací z věcné působnosti zákona.

Pojem významného informačního systému odkazuje k systémům, jejichž správcem je orgán veřejné moci a které mají zásadní význam pro fungování veřejné správy. V tomto případě není použito rozdělení na informační a komunikační systém, neboť z definice plyne, že do pojmu informačního systému spadá vždy i jeho vnitřní komunikační složka. Významným informačním systémem podle zákonné definice může být i systém, který neodpovídá definici obsažené v § 3 zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, jehož správcem je orgán veřejné moci a jehož důležitost odůvodnila jeho zařazení mezi významné informační systémy.

Pojem správce informačního, respektive komunikačního systému je definován obdobně jako v zákoně č. 365/2000 Sb., přičemž definice je založena na faktickém stanovení účelu příslušného systému a podmínek jeho provozování. Pro účely tohoto zákona je třeba vymezit pojem správce, neboť ten bude především orgánem a osobou, na níž bude dopadat právní regulace. Pokud by tento pojem vymezen nebyl, mohly by vznikat interpretační obtíže s tím, kdo ponese odpovědnost za neplnění povinností stanovených tímto zákonem. Orgánem a osobu by tak podle navrhované definice měl být ten, kdo určuje účel daného systému, respektive podmínky jeho provozování (typicky jeho vlastník), nikoliv ten, kdo se smluvně zavázal k provozu daného systému.

Pojem významné sítě je definován tak, aby zahrnoval páteřní sítě, jejichž prostřednictvím je kybernetický prostor na území České republiky propojen do zahraničí. Vzhledem k důležitosti kritické informační infrastruktury je jako významná síť označena touto legální definicí též síť, která sama o sobě není prvkem kritické informační infrastruktury, ale která zajišťuje připojení kritické informační infrastruktury ke kybernetickému prostoru. Relativně menší bezpečnostní expozice významné sítě v porovnání s kritickou informační infrastrukturou se projevuje v dalších ustanoveních zákona omezeným katalogem povinností ukládaných zákonem jejich správcům.

K písm. a)

1. Ustanovení § 2 je věnováno vymezení pojmů, se kterými je v zákoně dále pracováno. Kybernetickým prostorem dle zákonné definice označujeme digitální prostředí, které slouží ke zpracování a výměně informací, a tvoří jej informační systémy a služby a sítě elektronických komunikací.[7] Kybernetický prostor představuje virtuální prostředí uměle vytvořené člověkem, ve kterém dochází ke zpracování a uchování informací a také především k jejich výměně a sdílení.

2. Vzhledem ke stále větší závislosti moderní společnosti na informačních technologiích je v kybernetickém prostoru manipulováno i s důvěrnými informacemi. Riziko jejich

[7] Srov. JIRÁSEK, P., NOVÁK, L., POŽÁR, J. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary* [online]. 2., aktualiz. vyd. Praha: Policejní akademie ČR a Česká pobočka AFCEA, 2013, s. 59 [cit. 2014-12-30]. Dostupné z: https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovnik-kyberneticke-bezpecnosti---druhe-vydani/.

zneužití je značné. Kybernetický prostor vnímá Severoatlantická aliance jako tzv. pátou zónu války (vedle země, vody, vzdušného prostoru a vesmíru).[8]

3. Pojmy „síť elektronických komunikací" a „služba elektronických komunikací" jsou definovány v zákoně č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), dále jen „zák. o elektronických komunikacích".

4. Síť elektronických komunikací je dle § 2 písm. h) zák. o elektronických komunikacích systém přenosu informací, který umožňuje přenos signálů po vedení, a to rádiovými, optickými nebo jinými elektromagnetickými prostředky. Síť elektronických komunikací zahrnuje družicové sítě, pevné sítě s komutací okruhů nebo paketů, mobilní zemské sítě, sítě pro rozvod elektrické energie, sítě pro rozhlasové a televizní vysílání a sítě kabelové televize.

5. Službou elektronických komunikací je definována v § 2 písm. n) zák. o elektronických komunikacích jako služba poskytovaná obvykle za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací. Služby elektronických komunikací zahrnují telekomunikační a přenosové služby v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize. Naopak sem nespadají služby, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi.

K písm. b)

6. Pojem kritické informační struktury koresponduje s platnou právní úpravou v zákoně č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon), dále jen „krizový zákon", a dalších souvisejících předpisech.

7. Kritickou informační infrastrukturou obecně rozumíme dle § 2 písm. g) krizového zákona prvek nebo systém prvků kritické infrastruktury. Pokud by byla narušena funkce tohoto prvku nebo systému prvků, mělo by to zásadní dopad na zdraví osob nebo zabezpečení jejich základních životních potřeb, či na ekonomiku nebo bezpečnost státu.

8. Bezpečnost státu je třeba chápat v kontextu ústavního zákona č. 110/1998 Sb., o bezpečnosti České republiky (dále také „úst. zák. o bezpečnosti ČR"), jakož i aktuální Bezpečnostní strategie České republiky. Bezpečnost státu lze chápat jako stav, za kterého jsou hrozby a rizika jsou eliminovány na minimum, tudíž systému objektivně nehrozí závažnější újma. Jedná se o ideální stav, ke kterému se stát snaží směřovat prostřednictvím realizace bezpečnostní politiky.

9. Aby mohl být nějaký prostředek či zařízení označen jako prvek kritické infrastruktury, musí splňovat tzv. průřezová a odvětvová kritéria, která stanoví nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury (dále jen „nařízení č. 432/2010 Sb."). Průřezová kritéria, která jsou společná pro prvky kritické infrastruktury ve všech oblastech, představují hlediska:

[8] SEDLÁK, J. NATO posouvá kybernetickou ochranu mezi priority a na nejvyšší úroveň. *E15.cz* [online]. 05. 09. 2014 [cit. 2015-01-02]. Dostupné z: http://e-svet.e15.cz/internet/nato-posouva-kybernetickou-ochranu-mezi-priority-a-na-nejvyssi-uroven-1116140.

a) obětí, a to s počtem více než 250 mrtvých nebo více než 2 500 osob s hospitalizací po dobu delší než 24 hodin,
b) ekonomického dopadu s hospodářskými ztrátami státu vyššími než 0,5 % hrubého domácího produktu,
c) dopadu na veřejnost v podobě rozsáhlého omezení poskytování nezbytných služeb nebo jiného závažného dopadu do každodenního života postihujícího více než 125 000 osob.

10. Odvětvová kritéria se v jednotlivých oblastech liší a jsou stanovena v příloze k nařízení č. 432/2010 Sb. Pro účely zákona o kybernetické bezpečnosti je nejdůležitější stanovení odvětvových kritérií v kategorii komunikačních a informačních systémů. Aby byl informační nebo komunikační systém označen jako prvek kritické infrastruktury v oblasti kybernetické bezpečnosti, musí se jednat o:

a) informační systém, který významně ovlivňuje činnost prvku kritické infrastruktury a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období delším než 8 hodin;
b) komunikační systém, který významně ovlivňuje činnost prvku kritické infrastruktury a který je nahraditelný jen při vynaložení nepřiměřených nákladů nebo v časovém období delším než 8 hodin;
c) informační systém spravovaný orgánem veřejné moci, který obsahuje osobní údaje více než 300 000 osob;
d) komunikační systém, který zajišťuje připojení nebo propojení prvku kritické infrastruktury, s kapacitou garantovaného datového přenosu nejméně 1 Gbit/s;
e) ostatní informační a komunikační systémy, pokud je ochrana prvku nezbytná pro zajištění kybernetické bezpečnosti.

K písm. c)

11. Dalším z pojmů, který zákon o kybernetické bezpečnosti definuje, je „bezpečnost informací". Ta je chápána jako zajištění důvěrnosti, integrity a dostupnosti informací. Bezpečností informací se zabývá poměrně mladý vědní obor, který se označuje jako informační bezpečnost (Information Security). Předmětem jeho zkoumání je zabezpečení informací v informačních a komunikačních technologiích.

12. Informační bezpečnost musí řešit veškerou ochranu informací organizace, tedy celého informačního systému. To zahrnuje ochranu informací v mluvené i psané formě a zejména jejich ochranu při zpracování a přenosu.[9]

13. Pro zajištění důvěrnosti, integrity a dostupnosti informací je nutné především vybudovat systém ochrany dat a informací během jejich vzniku, zpracování, ukládání a přenášení. Ochrana dat a informací je zajišťována především pomocí logických, fyzických, technických, programových a organizačních opatření.[10]

14. Důvodová zpráva k zákonu o kybernetické bezpečnosti zdůrazňuje u pojmu bezpečnosti informací princip technologické neutrality. Předmětem regulace zákona o kybernetické bezpečnosti není obsah přenášených informací.

---

[9] SMEJKAL, V., RAIS, K. *Řízení rizik ve firmách a jiných organizacích*. 2., aktualiz. a rozš. vyd. Praha: Grada, 2006, s. 197.

[10] POŽÁR, J. *Manažerská informatika*. Plzeň: Aleš Čeněk, 2010, s. 252.

K písm. d)

15. Pojem „významný informační systém" je pozitivně vymezen jako informační systém, který spravuje orgán veřejné moci a u něhož narušení bezpečnosti informací může významně omezit či ohrozit výkon působnosti tohoto orgánu.

16. Používání informačních systémů orgány veřejné moci je právně regulováno zákonem č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, (dále jen „zák. o inf. systémech veř. správy"). Dle § 3 zák. o inf. systémech veř. správy se jako informační systém veřejné správy označuje informační systém, který slouží pro výkon veřejné správy. Z působnosti zákona o informačních systémech veřejné správy je však řada důležitých informačních systémů veřejné správy vyňata. Jedná se o systémy vedené např. zpravodajskými službami, Policií České republiky, celními orgány, orgány činnými v trestním řízení, Národním bezpečnostním úřadem apod.

17. Negativně je významný informační systém vymezen tak, že se nejedná o kritickou infrastrukturu.

18. Co je významný informační systém, konkrétně vymezuje vyhláška č. 317/2014 Sb. ze dne 15. prosince 2014, o významných informačních systémech a jejich určujících kritériích. Významné informační systémy jsou konkrétně označeny v příloze č. 1 k této vyhlášce. Jedná se především o informační systémy vedené ministerstvy a dalšími ústředními správními úřady. Kromě systémů uvedených v seznamu může být za významný informační systém považován i systém, o kterém tak určí správce. Učiní tak v případě, že daný informační systém naplní tzv. určující kritéria, která jsou definována ve vyhlášce č. 317/2014 Sb. ze dne 15. prosince 2014, o významných informačních systémech a jejich určujících kritériích. Rozlišujeme dopadová a oblastní určující kritéria.

19. Mezi dopadová určující kritéria lze zařadit skutečnost, že úplná nebo částečná nefunkčnost informačního systému na základě narušení bezpečnosti informací by mohla negativně ovlivnit fungování nebo hospodaření orgánu veřejné moci, který je jeho správcem. Dále sem patří negativní vliv na poskytování služeb nebo informací veřejnosti správcem významného informačního systému či omezení provozu informačního systému, který je s významným informačním systémem propojen.

20. Dopadovým určujícím kritériem je i skutečnost, že úplná nebo částečná nefunkčnost informačního systému kvůli narušením bezpečnosti informací by mohla způsobit:

a) ohrožení či narušení prvku kritické infrastruktury;
b) oběti na životech v počtu více než 10 mrtvých nebo 100 zraněných osob vyžadujících lékařské ošetření;
c) finanční či materiální ztráty ve výši více než 0,5 % stanoveného rozpočtu orgánu veřejné moci;
d) zásah do soukromého života nebo do práv nejméně 50 000 osob;
e) výrazné ohrožení nebo narušení veřejného zájmu, přičemž následky podle bodů 1 až 4 nedosáhnou hodnot pro určení prvku kritické infrastruktury.

21. Do oblastních určujících kritérií lze zařadit oblasti v rámci výkonu přenesené působnosti krajem zařadit oblasti: vedení správního řízení, databáze obsahující osobní údaje, hospodaření orgánu veřejné moci, státní dozor, inspekční činnost, příprava na krizové stavy, elektronická pošta, vedení internetových stránek, mezinárodní spolupráce, zadávání veřejných zakázek. Stejná oblastní kritéria platí i pro činnosti ostatních orgánů

veřejné moci, přičemž navíc jsou u nich zařazeny oblasti spisové služby, tvorby právních předpisů a mezirezortní spolupráce.

22. Dle přílohy č. 1 k vyhlášce č. 317/2014 Sb. jsou významnými informační systémy především informační systémy spravované ministerstvy a jinými ústředními správními úřady. Jedná se například o tyto instituce:
- Česká inspekce životního prostředí
- Česká národní banka
- Česká správa sociálního zabezpečení
- Český hydrometeorologický ústav
- Český statistický úřad
- Český telekomunikační úřad
- Český úřad zeměměřičský a katastrální
- Energetický regulační úřad
- Generální finanční ředitelství
- Generální ředitelství cel
- Ministerstvo dopravy
- Ministerstvo financí
- Ministerstvo obrany
- Ministerstvo práce a sociálních věcí
- Ministerstvo pro místní rozvoj
- Ministerstvo průmyslu a obchodu
- Ministerstvo spravedlnosti
- Ministerstvo školství, mládeže a tělovýchovy
- Ministerstvo vnitra
- Ministerstvo zahraničních věcí
- Ministerstvo zdravotnictví
- Ministerstvo zemědělství
- Ministerstvo životního prostředí
- Národní bezpečnostní úřad
- Nejvyšší kontrolní úřad
- Probační a mediační služba
- Rada pro rozhlasové a televizní vysílání
- Správa státních hmotných rezerv
- Správa základních registrů
- Státní úřad pro jadernou bezpečnost
- Státní úřad pro kontrolu léčiv
- Úřad pro civilní letectví
- Úřad pro ochranu osobních údajů
- Úřad pro zastupování státu ve věcech majetkových
- Úřad průmyslového vlastnictví
- Úřad vlády České republiky
- Vězeňská služba České republiky
- Všeobecná zdravotní pojišťovna České republiky.

Přehled významných informačních systémů:

PČ	Správce	Název
1	Česká inspekce životního prostředí	Centrální informační systém – CIS
2	Česká národní banka	CERTIS (Czech Express Real Time Interbank Gross Settlement systém)
3	Český hydrometeorologický ústav	Automatizovaný meteorologický informační systém – AMIS
4	Český hydrometeorologický ústav	AWOS AVIMET
5	Český hydrometeorologický ústav	Radarová síť CZRAD
6	Český hydrometeorologický ústav	EUMETSAT
7	Český hydrometeorologický ústav	Informační systém kvality ovzduší – ISKO
8	Český statistický úřad	Registr ekonomických subjektů – RES
9	Český statistický úřad	Registr statistických obvodů a budov – RSO
10	Český statistický úřad	Soustava statistických registrů – SSREG
11	Český telekomunikační úřad	Automatizovaný systém monitorování kmitočtového spektra – ASMKS
12	Český telekomunikační úřad	Spectra plus
13	Český úřad zeměměřičský a katastrální	Informační systém územní identifikace
14	Český úřad zeměměřičský a katastrální	Informační systém veřejné správy pro správu a vedení katastru nemovitostí
15	Český úřad zeměměřičský a katastrální	Informační systém veřejné správy zeměměřictví
16	Energetický regulační úřad	Jednotný informační systém Energetického regulačního úřadu
17	Generální finanční ředitelství	Automatizovaný daňový informační systém – ADIS
18	Generální ředitelství cel	Centrální registr subjektů – CRS
19	Generální ředitelství cel	Globální záruky – GLZ
20	Ministerstvo dopravy	Centrální registr dopravců – CRD
21	Ministerstvo dopravy	Centrální registr řidičů – CRŘ
22	Ministerstvo dopravy	Centrální registr vozidel
23	Ministerstvo dopravy	Informační systém o silniční a dálniční síti ČR – ISSDS ČR
24	Ministerstvo dopravy	Projekt správy informací o vozidlech (DAVOZ)
25	Ministerstvo dopravy	Přeprava nebezpečných věcí (IS ADR)

26	Ministerstvo dopravy	Systém elektronického mýta
27	Ministerstvo financí	Administrativní registr ekonomických subjektů – ARES
28	Ministerstvo financí	Automatizovaný rozpočtový infomační systém – ARIS
29	Ministerstvo financí	Evidenčně dotační systém a správa majetku ve vlastnictví státu – EDS/SMVS
30	Ministerstvo financí	Integrovaný informačního systém Státní pokladny – IISSP
31	Ministerstvo financí	Informační systém programového financování ISPROFIN
32	Ministerstvo financí	Informační systém VIOLA
33	Ministerstvo obrany	Informační systém mobilizačních příprav
34	Ministerstvo obrany	Informační systém Vojenské policie
35	Ministerstvo obrany	Informační systém o veřejných zakázkách – IS VZ
36	Ministerstvo obrany	Štábní informační systém Armády ČR
37	Ministerstvo práce a sociálních věcí	Informační systém hmotná nouze a sociální služby
38	Ministerstvo práce a sociálních věcí	Informační systém OK služby registr
39	Ministerstvo práce a sociálních věcí	Informační systém služeb zaměstnanosti
40	Ministerstvo práce a sociálních věcí	Informační systém státní sociální podpory
41	Ministerstvo průmyslu a obchodu	Informační systém Registru živnostenského podnikání
42	Ministerstvo spravedlnosti	Centrální evidence stíhaných osob
43	Ministerstvo spravedlnosti	Evidence znalců a tlumočníků – prezentační část
44	Ministerstvo spravedlnosti	Informační systém Rejstříku trestů – RT
45	Ministerstvo spravedlnosti	Informační systém registru obchodního rejstříku – ISROR
46	Ministerstvo spravedlnosti	Informační systém insolvenčního rejstříku – ISIR
47	Ministerstvo školství, mládeže a tělovýchovy	Informační systém pro kvalifikace a autorizace – ISKA
48	Ministerstvo vnitra	Agendový informační systém cizinců
49	Ministerstvo vnitra	Agendový informační systém ZBRANĚ
50	Ministerstvo vnitra	Agendový informační systém Modelovací
51	Ministerstvo vnitra	Agendový informační systém Policie ČR
52	Ministerstvo vnitra	Agendový informační systém Registru práv a povinností Působnostní
53	Ministerstvo vnitra	Czech POINT – systém kontaktních míst veřejné správy
54	Ministerstvo vnitra	Evidence občanských sdružení, jejich organizačních jednotek s právní subjektivitou, odborových organizací a organizací
55	Ministerstvo vnitra	Informační systém datových schránek – ISDS
56	Ministerstvo vnitra	Informační systém evidence cestovních dokladů – ISECD

57	Ministerstvo vnitra	Informační systém evidence mezinárodních nevládních organizací a jejich organizačních jednotek, které jsou oprávněny jednat svým jménem
58	Ministerstvo vnitra	Informační systém evidence občanských průkazů – ISEOP
59	Ministerstvo vnitra	Informační systém evidence obyvatel – ISEO
60	Ministerstvo vnitra	Informační systém o datových prvcích
61	Ministerstvo vnitra	Informační systém o informačních systémech veřejné správy
62	Ministerstvo vnitra	Portál veřejné správy – PVS
63	Ministerstvo vnitra	Rejstřík politických stran a politických hnutí
64	Ministerstvo vnitra	Ústřední evidence nabytí a pozbytí státního občanství České republiky
65	Ministerstvo zahraničních věcí	Víza ČR (EVC2)
66	Ministerstvo zahraničních věcí	Systém na pořizování, přenos a zpracování žádostí o cestovní doklad s biometrickými prvky – ePasy
67	Ministerstvo zdravotnictví	Ochrana veřejného zdraví
68	Ministerstvo zdravotnictví	Zdravotní služby
69	Ministerstvo zemědělství	Informační systém VODA
70	Ministerstvo zemědělství	Integrovaný zemědělský registr – IZR
71	Ministerstvo zemědělství	Společný zemědělský registr – SZR
72	Ministerstvo životního prostředí	Integrovaný registr znečišťování životního prostředí
73	Ministerstvo životního prostředí	Integrovaný systém plnění ohlašovacích povinností
74	Ministerstvo životního prostředí	Jednotný informační systém pro životní prostředí – JISŽP
75	Ministerstvo životního prostředí	Informační systém SEA
76	Ministerstvo životního prostředí	Informační systém EIA (Environmental Impact Assessment)
77	Národní bezpečnostní úřad	Iinformační systém GovCERT
78	Nejvyšší kontrolní úřad	Kontrolní informační software
79	Probační a mediační služba	Agendový informační systém AIS Probační a mediační služby
80	Rada pro rozhlasové a televizní vysílání	Intranet Rady pro rozhlasové a televizní vysílání
81	Správa státních hmotných rezerv	Informační systém pro plánování civilních zdrojů ARGIS (PCZ ARGIS)
82	Správa státních hmotných rezerv	Informačního systém k podpoře řízení a koordinace využívání věcných zdrojů za krizových situací – KRIZKOM
83	Správa základních registrů	Dohledový systém WILY Správy základních registrů

84	Správa základních registrů	Formulářový agendový informační systém – FAIS
85	Správa základních registrů	Informační systém základních registrů
86	Správa základních registrů	Provozní agendový informační systém – PAIS
87	Správa základních registrů	Service desk manager Správy základních registrů
88	Správa základních registrů	SharePoint Správy základních registrů
89	Státní úřad pro jadernou bezpečnost	Registr externích adres – REA
90	Státní úřad pro kontrolu léčiv	Centrální úložiště elektronických receptů
91	Státní úřad pro kontrolu léčiv	Registr léčivých přípravků s omezením
92	Úřad pro civilní letectví	IS úřadu pro civilní letectví – IS ÚCL
93	Úřad pro ochranu osobních údajů	Informační systém Úřadu pro ochranu osobních údajů – IS ÚOOÚ
94	Úřad pro zastupování státu ve věcech majetkových	Informační systém majetku státu – ISMS
95	Úřad průmyslového vlastnictví	Informační systém duševního vlastnictví – ISDV
96	Úřad vlády České republiky	Elektronická knihovna legislativního procesu – eKLEP
97	Vězeňská služba České republiky	Vězeňský informační systém – VIS
98	Všeobecná zdravotní pojišťovna České republiky	Informační systém Všeobecné zdravotní pojišťovny České republiky – IS VZP ČR

K písm. e) a f)

23. Jako správce informačního a komunikačního systému označuje ustanovení osobu, která určuje účel zpracování informací či komunikačního systému, jakož i podmínky provozování tohoto systému. Definice správce informačního a komunikačního systému koresponduje s právní úpravou v zákoně o informačních systémech veřejné správy.

24. Tento pojem je definován především proto, že správcům jsou v zákonu o kybernetické bezpečnosti ukládány povinnosti, jejichž plnění je stěžejní pro zajištění kybernetické bezpečnosti státu (zejména dodržování bezpečnostních opatření). Je tedy nutné jasně stanovit, kdo je k plnění těchto povinností zavázán. Z vymezení pojmu správce informačního a komunikačního systému jasně plyne, že odpovědnost vždy ponese ten, kdo určuje, proč a jak bude daný systém fungovat. V případě orgánů veřejné moci bude za plnění povinností stanovených zákonem o kybernetické bezpečnosti vždy odpovídat tento orgán veřejné moci, a nikoliv např. subjekt, který systém vytvořil či který jej provozuje.

K písm. g)

25. Posledním z pojmů, který je definován v § 2 zák. o kyber. bezpečnosti, je „významná síť elektronických komunikací“. Jedná se o síť elektronických komunikací ve smyslu ustanovení zákona o elektronických komunikacích, která buď zajišťuje propojení

kybernetického prostoru České republiky do zahraničí, nebo zajišťuje připojení ke kritické informační infrastruktuře.

Související ustanovení:
§ 3 – povinné subjekty, § 4 – organizační a technická opatření

Související předpisy:
úst. zák. o bezpečnosti ČR, – krizový zákon, – zák. o inf. systémech veř. správy, – zák. o elektronických komunikacích, – vyhláška č. 317/2014 Sb., – nařízení č. 432/2010 Sb.

§ 3
(Povinné subjekty)

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.

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

Z důvodové zprávy:

Vymezení okruhu orgánů a osob je částečně založeno na užití stávajících pojmů zákona o elektronických komunikacích.

Orgány a osoby lze v zásadě rozdělit do dvou skupin. První z nich tvoří poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací vymezené v zákoně o elektronických komunikacích, a subjekty zajišťující tzv. významné sítě, na něž bude regulace tohoto zákona dopadat pouze minimálně, a to v rozsahu povinnosti oznámit kontaktní údaje a jejich změny národnímu CERT, respektive v povinnosti provádět opatření za stavu kybernetického nebezpečí. Subjekty zajišťující významné sítě budou nadto povinny detekovat kybernetické bezpečnostní události a hlásit kybernetické bezpečnostní incidenty. Druhou skupinu pak budou tvořit správci informačních systémů kritické informační infrastruktury, správci komunikačních systémů kritické informační infrastruktury, a správci významných informačních systémů, na něž bude dopadat regulace tohoto zákona v plném rozsahu. Tato skupina orgánů a osob tak bude povinna oznámit kontaktní údaje a jejich změnu vládnímu CERT, zavést bezpečnostní opatření, detekovat kybernetické bezpečnostní události, hlásit kybernetické bezpečnostní incidenty a provádět opatření.

Toto rozdělení orgánů a osob s následným omezením rozsahu zákonných povinností na nezbytné minimum v závislosti na významnosti informačních a komunikačních systémů, které orgány a osoby spravují, odpovídá principu minimalizace státních zásahů, na němž je tento zákon založen. Shora uvedená klasifikace orgánů a osob má kaskádovitý charakter. Typicky tedy např. subjekt zajišťující významnou síť, která bude zařazena do kritické informační infrastruktury, bude mít ve vztahu k této síti