(platí od 1. 71. 2015 do 30. 6. 2017)

181/2014 Sb.

ZÁKON

ze dne 23. července 2014

o kybernetické bezpečnosti a o změně souvisejících zákonů

(zákon o kybernetické bezpečnosti)

ve znění zákona č. 104/2017 Sb.

(zkráceno - text neobsahující změny byl vypuštěn)

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

h~~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 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 a

e) správce a provozovatel významného informačního systému.

HLAVA II

SYSTÉM ZAJIŠTĚNÍ KYBERNETICKÉ BEZPEČNOSTI

Bezpečnostní opatření

§ 4

(zkráceno - text neobsahující změny byl vypuštěn)

§ 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.

(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.

(zkráceno - text neobsahující změny byl vypuštěn)

§ 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) 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.

(5~~(4~~) Prováděcí právní předpis stanoví

(zkráceno - text neobsahující změny byl vypuštěn)

Reaktivní a ochranné opatření

§ 13

(zkráceno - text neobsahující změny byl vypuštěn)

§ 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.

(zkráceno - text neobsahující změny byl vypuštěn)

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

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

(3) Za správní delikt se uloží pokuta do

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

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

c) 200 000 Kč, jde-li o správní delikt podle odstavce 2 písm. e) a h~~d~~).

(zkráceno - text neobsahující změny byl vypuštěn)

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. 5~~4~~,

(zkráceno - text neobsahující změny byl vypuštěn)