HR. 2012

Výbor pro národní bezpečnost

Výbor pro vědu, vesmír a technologie

Český model amerického kongresu 2020

zahájen a konán v městě Plzeň v neděli,
šestého září roku dvoutisícího dvacátého

V zájmu zajištění bezpečnosti Spojených států amerických a jejich občanů před vnějšími i vnitřními hrozbami v kyberprostoru se Senát a Sněmovna reprezentantů Spojených států amerických v Kongresu usnesly na tomto zákonu:

ZÁKON

O ochraně kritické infrastruktury před kybernetickými hrozbami

Hlava I. – Úvodní ustanovení

Par. 101.

(a) KRITICKOU INFRASTRUKTUROU se rozumí jakékoliv fyzické nebo elektronické systémy nebo objekty, které by v případě ohrožení nebo zničení měly podstatný dopad na bezpečnost, národní hospodářské zájmy Spojených států amerických, zdraví nebo život občanů Spojených států amerických, jejich bezpečnost nebo kombinaci výše uvedeného.

(b) KRITICKOU INFRASTRUKTUROU I. STUPNĚ se rozumí kritická infrastruktura podle Par. 101 odst. a) tohoto zákona, která se vyskytuje v oblasti obranné nebo bezpečnostní infrastruktury nebo veřejných financí.

(c) KRITICKOU INFRASTRUKTUROU II. STUPNĚ se rozumí kritická infrastruktura podle Par. 101 odst. a) tohoto zákona, která se vyskytuje v oblasti energetiky, průmyslové výroby nebo zdravotnictví.

(d) KRITICKOU INFRASTRUKTUROU III. STUPNĚ se rozumí kritická infrastruktura podle Par. 101 odst. a) tohoto zákona, která se vyskytuje v oblasti zemědělství, životního prostředí včetně zajištění pitné vody nebo infrastruktura týkající se národních památek, muzeí nebo jiných obdobných zařízení.

(e) MINISTERSTVEM se rozumí Ministerstvo vnitřní bezpečnosti;

(f) SOUKROMÝM SEKTOREM se rozumí všechny právnické osoby mající své sídlo ve Spojených státech amerických a všechny fyzické osoby mající ve Spojených státech americké občanství nebo povolen trvalý pobyt;

(g) VEŘEJNÝM SEKTOREM se rozumí jakékoliv federální složky výkonné moci Spojených států, které ve svém souhrnu vytvářejí státní správu, včetně všech ministerstev a jím podřízených správních orgánů;

(h) KYBERNETICKOU HROZBOU se rozumí potenciální kybernetický útok na kritickou infrastrukturu, který se vzhledem ke všem okolnostem daného případu jeví jako vysoce pravděpodobný nebo možný;

(i) KYBERNETICKÝM ÚTOKEM se rozumí neoprávněné jednání či zásah do elektronické počítačové sítě, která je součástí kritické infrastruktury, mající za cíl změnit, zničit nebo ukrást jakýkoliv prvek této sítě nebo tuto síť jakýmkoliv jiným způsobem negativně ovlivnit.

Par. 102.

(a) Teroristé a teroristické organizace směřují ke zničení kritické infrastruktury Spojených států amerických za účelem ochromení ekonomiky, ohrožení života a zdraví občanů Spojených států amerických a zničení morálky a sebejistoty společnosti.

(b) Současný globalizovaný svět přináší nové vnitřní i vnější hrozby, na které je nutné příslušnými prostředky reagovat. Obrana před kybernetickými hrozbami a kybernetickými útoky je v současné době s ohledem na kritickou infrastrukturu klíčová a prioritní.

(c) Veřejný a soukromý sektor musí s ohledem na kybernetické hrozby a kybernetické útoky postupovat koordinovaně a poskytovat si nezbytnou součinnost.

Hlava II. – Sektorové šetření

Par. 201.

Ministerstvo zajistí v koordinaci s veřejným a soukromým sektorem sektorové šetření za účelem identifikace kybernetických hrozeb, přičemž vyhodnotí způsoby a možnosti, jak na tyto hrozby reagovat.

Par. 202.

Sektorové šetření podle Par. 201 tohoto zákona bude provedeno dle následujícího harmonogramu:

(a) sektorové šetření v případě kritické infrastruktury I. stupně bude provedeno v prvních šestí měsících roku 2021;

(b) sektorové šetření v případě kritické infrastruktury II. stupně bude provedeno v 6 měsících následujících po provedení sektorového šetření podle Par. 202 odst. a) tohoto zákona;

(c) sektorové šetření v případě infrastruktury III. stupně bude provedeno nejpozději do konce roku 2022.

Par. 203.

V rámci sektorového šetření je ministerstvo oprávněno vyžádat si od jakéhokoliv subjektu veřejného nebo soukromého sektoru jakékoliv informace, podklady nebo dokumenty, které shledá nezbytné pro přesné vyhodnocení sektorového šetření.

Par. 204.

Subjekty soukromého sektoru jsou povinny poskytnout pravdivé a přesné údaje podle Par. 203. tohoto zákona ministerstvu do 30 dnů od okamžiku, kdy o ně ministerstvo požádá. Subjekty soukromého sektoru jsou dále povinny v rámci sektorového šetření poskytovat jakoukoliv nezbytnou součinnost, kterou si ministerstvo vyžádá.

Par. 205.

Výsledky sektorového šetření budou s ohledem na bezpečnost Spojených států neveřejné. Veřejnost se nemůže domáhat jejich zpřístupnění podle jiného právního předpisu.

Hlava III. – Povinnosti soukromého sektoru

Par. 301

Subjekty soukromého sektoru jsou povinny postupovat tak, aby:

(a) s ohledem na obecnou povinnost prevence předcházely kybernetickým hrozbám a kybernetickým útokům;

(b) v případě kybernetické hrozby nebo kybernetického útoku postupovaly tak, aby došlo k minimalizaci škod.

Par. 302.

Subjekty soukromého sektoru jsou dále povinny oznámit kybernetickou hrozbu nebo kybernetický útok ministerstvu, způsobem, který stanoví prováděcí právní předpis, a to:

(a) v případě kritické infrastruktury I. stupně do 1 hodiny;

(b) v případě kritické infrastruktury II. stupně do 24 hodin;

(c) v případě kritické infrastruktury III. stupně do 48 hodin;

od okamžiku, kdy se příslušný subjekt o kybernetické hrozbě nebo kybernetickém útoku dozví.

Par. 303.

Ministerstvo je oprávněno v souladu s jinými právními předpisy vyvlastnit ty systémy nebo objekty kritické infrastruktury I. nebo II. stupně, které bude považovat za nezbytné pro zajištění bezpečnosti Spojených států amerických.

Hlava IV. – Sankce

Par. 401.

V případě, že subjekt soukromého sektoru poruší svou povinnost stanovenou v Par. 204 tohoto zákona, bude mu uložena peněžitá pokuta až do výše:

(a) 10 000 000 amerických dolarů v případě, že půjde o informace týkající se kritické infrastruktury I. stupně;

(b) 1 000 000 amerických dolarů v případě, že půjde o informace týkající se kritické infrastruktury II. stupně;

(c) 500 000 amerických dolarů v případě, že půjde o informace týkající se kritické infrastruktury III. stupně.

Par. 402.

V případě, že subjekt soukromého sektoru poruší svou povinnost stanovenou v Par. 301 tohoto zákona, bude mu uložena peněžitá pokuta až do výše 1 000 000 amerických dolarů.

Par. 403.

V případě, že subjekt soukromého sektoru poruší svou povinnost stanovenou v Par. 302 tohoto zákona, bude mu uložena peněžitá pokuta až do výše 10 000 000 amerických dolarů.

Par. 404.

Spáchá-li osoba jakýkoliv kybernetický útok proti kritické infrastruktuře nebo jakýkoliv trestný čin spojený s kritickou infrastrukturou, bude tato okolnost považována za přitěžující okolnost podle jiného právního předpisu.

Hlava V. – Závěrečná ustanovení

Par. 501.

Tento zákon nabývá účinnosti dne 1. 1. 2021.