**NÁRODNÁ RADA SLOVENSKEJ REPUBLIKY**

VIII. volebné obdobie

**Návrh**

**zákon**

z ... 2022

**ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov**

Národná rada Slovenskej republiky sa uzniesla na tomto zákone:

**Čl. I**

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti v znení zákona č. 373/2018 Z. z., 287/2021 Z. z., 452/2021 Z. z. sa mení a dopĺňa takto:

1. V § 3 sa dopĺňa písmeno q až s, ktoré znejú:

„q) hybridnou hrozbou súbor nátlakových a podvratných činností, ktoré môžu štátne aj neštátne subjekty koordinovaným spôsobom využívať s cieľom oslabenia kritickej infraštruktúry, prehĺbenia nezdravej polarizácie na národnej a medzinárodnej úrovni, ohrozenie základných hodnôt demokratickej spoločnosti, zisku geopolitického vplyvu a moci prostredníctvom poškodzovania ostatných, ovplyvňovania demokratických rozhodovacích procesov a šírenia závažných dezinformácií,

r) závažnou dezinformáciou taký nepravdivý alebo zmanipulovaný text, obrázok, video alebo zvuk, ktorý skutočnosť a informácie, ktoré sú objektívne dané značne a dokázateľne skresľujú, a ktorý môže byť použitý na šírenie pochybností, diskreditáciu pravdivých informácií, jednotlivcov či organizácií, pričom jeho charakter, okolnosti za ktorých bol šírený, doba a forma šírenia, prípadné následky šírenia, či okruh subjektov, ktorí sú ovplyvnení týmito informáciami, je rozsiahly,

s) kritickou infraštruktúrou zariadenia, služby a informačné systémy životne dôležité pre obyvateľov a riadenie štátu, ktorých nefunkčnosť alebo zničenie môže ohroziť bezpečnostné záujmy štátu, do ktorej patria najmä objekty osobitnej dôležitosti, ďalšie dôležité objekty, vybrané informačné a komunikačné prostriedky, zariadenia na výrobu a zásobovanie vodou, elektrickou energiou, ropou a zemným plynom a ďalšie časti majetku štátu a podnikateľských právnických a fyzických osôb určené vládou SR alebo iným kompetentným orgánom štátnej správy, ktoré sú nevyhnutné na zvládnutie krízových situácií, ochranu obyvateľstva a majetku, na zaistenie minimálneho chodu ekonomiky a správy štátu, ako aj jeho vonkajšej a vnútornej bezpečnosti a ktoré treba špeciálne ochraňovať.“.

1. § 27b znie:

„§ 27b

* 1. Úrad z vlastnej iniciatívy rozhoduje o blokovaní, spôsobe blokovania a vykonáva blokovanie, ak § 27c neustanovuje inak.
  2. Rozhodnutie o blokovaní obsahuje najmä

1. identifikáciu úradu,
2. identifikáciu osoby, ktorá prevádzkuje infraštruktúru, na ktorej je blokovanie potrebné vykonať,
3. identifikáciu škodlivého obsahu alebo škodlivej aktivity,
4. dôvod blokovania,
5. spôsob blokovania,
6. lehotu na vykonanie blokovania, trvanie blokovania a možnosti jeho odblokovania,
7. poučenie.
   1. Škodlivým obsahom sa rozumie programový prostriedok alebo údaj, ktorý zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident. Škodlivou aktivitou sa rozumie akákoľvek činnosť, ktorá zapríčiňuje alebo môže zapríčiniť kybernetický bezpečnostný incident, ako podvodná činnosť, odcudzenie osobných údajov alebo citlivých údajov a hybridná hrozba.
   2. Blokovaniu predchádza:
8. informovanie Národnej jednotky CSIRT o zistení škodlivého obsahu na dotknutej doméne,
9. evidovanie a riešenie incidentu Národnou jednotkou CSIRT podľa zákona a interných postupov, vrátane eskalačných a komunikačných mechanizmov medzi jednotlivými zložkami, ktorých účasť na riešení incidentu vyžaduje zákon,
10. komunikácia Národnej jednotky CSIRT s držiteľom a prevádzkovateľom infraštruktúry, na ktorej je blokovanie potrebné vykonať,
11. umožnenie držiteľovi alebo prevádzkovateľovi infraštruktúry odstránenie škodlivého obsahu z dotknutej domény v určenej lehote, ktorá nesmie byť kratšia ako 72 hodín.
    1. Ak dôjde k odstráneniu škodlivého obsahu pred uplynutím určenej lehoty v súčinnosti s držiteľom alebo prevádzkovateľom infraštruktúry sa pokračuje v ďalších fázach riešenia a koordinácie riešenia kybernetického bezpečnostného incidentu.
    2. Ak škodlivý obsah nie je odstránený do určenej lehoty, vydá sa rozhodnutie o blokovaní. Rozhodnutie o blokovaní hybridnej hrozby podľa odseku 3 je možné až po súhlase vecne príslušného krajského súdu.
    3. Úrad rozhodne o spôsobe blokovania podľa pravidiel blokovania tak, aby bolo účinné, účelné a primerané vo vzťahu k možným rizikám spojeným s blokovaním.
    4. Rozhodnutie o blokovaní doručí úrad osobe, ktorá prevádzkuje infraštruktúru, na ktorej je blokovanie potrebné vykonať a ktorá je povinná vykonať blokovanie, a zabezpečí jeho vykonanie; na riadne zistenie takejto osoby je úrad oprávnený požiadať o spoluprácu orgán verejnej moci alebo inú osobu, ktorá je povinná tejto žiadosti bezodkladne vyhovieť.
    5. Rozhodnutie o blokovaní zverejní úrad na svojom webovom sídle.
    6. Osoba, ktorá prevádzkuje infraštruktúru, na ktorej je blokovanie potrebné vykonať, je povinná na základe rozhodnutia o blokovaní zamedziť prevádzku spôsobom podľa rozhodnutia o blokovaní, inak blokovanie vykoná úrad; úrad je oprávnený požiadať o spoluprácu orgán verejnej moci alebo inú osobu, ktorá je povinná tejto žiadosti bezodkladne vyhovieť.
    7. Rozhodnutím o blokovaní nie sú dotknuté postupy riešenia kybernetického bezpečnostného incidentu a postupy orgánov činných v trestnom konaní. Rozhodnutie o blokovaní je preskúmateľné súdom a správna žaloba nemá odkladný účinok, okrem prípadu podľa odseku 6.
    8. Štátne orgány sú povinné bez meškania oznamovať úradu škodlivý obsah a škodlivé aktivity, ktoré zistia pri svojej činnosti.
12. V § 27c odsek 9 znie:

„Na vykonanie blokovania sa ustanovenia § 27b ods. 4 až 11 použijú primerane.“.

**Čl. II**

Tento zákon nadobúda účinnosť 1. júla 2022.