

Manažerské shrnutí

Vyhláška o kritériích rizikovosti dodavatele navazuje na obsah nového Zákona o kybernetické bezpečnosti hned několika způsoby a týká se výhradně potřeb mechanismu prověřování bezpečnosti dodavatelského řetězce (Část První, Hlava II zákona).

Mechanismus se uplatní pouze na ty poskytovatele regulované služby v režimu vyšších povinností, o jejichž službách je to výslovně uvedeno ve Vyhlášce o regulovaných službách (§ 6). Mechanismus se pak použije jen v případě těch aktiv, které jsou v zákonem stanoveném rozsahu řízení bezpečnosti a jsou tzv. kritickou částí aktiv. Kritickou částí jsou aktiva, u kterých poskytovatel regulované služby v režimu vyšších povinností postupem podle Vyhlášky o bezpečnostních opatřeních pro poskytovatele regulované služby v režimu vyšších povinností (příloha č. 1 vyhlášky) ohodnotil dopad narušení bezpečnosti informací na stanovený rozsah úrovní vysoká nebo kritická, nebo jsou to aktiva, která zajišťují nepominutelné funkce stanoveného rozsahu podle Vyhlášky o nepominutelných funkcích. V rámci takto daných aktiv je potřeba zohledňovat u mechanismus také tzv. „bezpečnostně významnou dodávku“. Dodavatel takové dodávky je pak tím, na koho směřuje Mechanismus prověřování bezpečnosti dodavatelského řetězce svůj pohled nejvíce. Zda je tento dodavatel rizikový, a plnění může probíhat bez omezení uvedených v Zákoně o kybernetické bezpečnosti, je potřeba zhodnotit na základě kritérií daných touto vyhláškou.

Tento dokument slouží jako rozpracované teze budoucí vyhlášky a je proto podkladem k další diskuzi. Může se měnit a to v závislosti jak na obsahu připomínek odborné veřejnosti, tak na obsahu připomínek v průběhu legislativního procesu..

Návrh

VYHLÁŠKA

ze dne dd.mm.rrrr,

o kritériích rizikovosti dodavatele

Národní úřad pro kybernetickou a informační bezpečnost stanoví podle X zákona č. X, o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti):

§ 1

Předmět právní úpravy

Tato vyhláška upravuje podle § X odst. 4 [*Prověřování rizik spojených s dodavatelem*] zákona o kybernetické bezpečnosti (dále jen „zákon“) kritéria rizikovosti dodavatele a způsob jejich vyhodnocení.

§ 2

Země mající vliv na dodavatele

Pro účely této vyhlášky se země mající vliv na dodavatele rozumí

- a) země sídla dodavatele,
- b) země, ve které jsou převážně činěna jednání ve vztahu k řízení dodavatele nebo ve které se pravidelně schází vedení dodavatele,
- c) země pobytu skutečného majitele dodavatele ve smyslu právního předpisu upravujícího evidenci skutečných majitelů¹,
- d) země, ve které má sídlo či pobyt osoba ovládající dodavatele ve smyslu právního předpisu upravujícího obchodní korporace², nebo země, ze které je dodavatel převážně ovládán, nebo
- e) země, která může i svévolně, přímo či nepřímo, na dodavatele efektivně vyvíjet nátlak, rozhodujícím významným způsobem jej ovlivnit či uplatňovat rozhodující vliv ve smyslu právního předpisu upravujícího obchodní korporace³.

¹ Zákon č. 37/2021 Sb., o evidenci skutečných majitelů, ve znění pozdějších předpisů.

² Zákon č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů..

³ Zákon č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), ve znění pozdějších předpisů..

§ 3

Kritéria rizikivosti dodavatele

Kritéria rizikivosti dodavatele podle § X odst. 4 *[Prověřování rizik spojených s dodavatelem]* zákona jsou uvedena v příloze k této vyhlášce.

§ 4

Způsob vyhodnocení kritérií rizikivosti dodavatele

Pro vyhodnocení kritérií rizikivosti dodavatele podle § X odst. 4 *[Prověřování rizik spojených s dodavatelem]* zákona se dle zjištěných poznatků o naplnění jednotlivých kritérií dodavatelem určí hodnota rizikivosti dodavatele, která stanoví možnou kybernetickou hrozbu spojenou s dodavatelem nebo možné ohrožení bezpečnosti České republiky nebo vnitřního či veřejného pořádku. Relevance jednotlivých kritérií pro výslednou hodnotu rizikivosti dodavatele se posuzuje podle míry naplnění jednotlivých kritérií ve vztahu k míře naplnění ostatních kritérií a k jiným informacím a datům shromážděným a vyhodnoceným podle § X odst. 1 *[Prověřování rizik spojených s dodavatelem]* zákona.

§ 5

Účinnost

Tato vyhláška nabývá účinnosti dnem dd.mm.rrrr.

Ředitel:

Ing. Lukáš Kintr v. r.

Příloha k vyhlášce č. XX/XXXX Sb.

Kritéria rizikosti dodavatele

Číslo kritéria	Popis kritéria
1.	V zemi mající vliv na dodavatele není demokratický politický systém.
2.	V zemi mající vliv na dodavatele neexistuje dělba moci.
3.	V zemi mající vliv na dodavatele není vykonávána státní moc pouze na základě zákona a v zemi neexistuje nezávislý soudní přezkum výkonu veřejné moci.
4.	Právní předpisy země mající vliv na dodavatele ukládají povinnost spolupráce se zpravodajskými službami, a to bez nezávislého soudního dohledu či přezkumu.
5.	Země mající vliv na dodavatele fakticky vynucuje spolupráci se zpravodajskými službami a v zemi neexistuje nezávislý soudní přezkum.
6.	Země mající vliv na dodavatele zaměřuje svou kybernetickou strategii či doktrínu na útočné operace v kyberprostoru proti České republice nebo jiným členským státům Evropské unie, Evropského hospodářského prostoru, Severoatlantické aliance či Organizace pro hospodářskou spolupráci a rozvoj.
7.	Země mající vliv na dodavatele aktivně působí proti zájmům České republiky nebo jiným členským státům Evropské unie, Evropského hospodářského prostoru, Severoatlantické aliance či Organizace pro hospodářskou spolupráci a rozvoj.
8.	Na zemi mající vliv na dodavatele došlo k uvalení mezinárodních sankcí či existuje vysoká pravděpodobnost, že na danou zemi budou tyto mezinárodní sankce uvaleny.
9.	Dodavatel byl pravomocně odsouzen pro úmyslný trestný čin spáchaný ve spojitosti s předmětem podnikání nebo úmyslný trestný čin spočívající ve významném porušení nebo ohrožení bezpečnosti nebo vnitřního či veřejného pořádku České republiky nebo jiných členských států Evropské unie, Evropského hospodářského prostoru, Severoatlantické aliance či Organizace pro hospodářskou spolupráci a rozvoj.
10.	Ekonomická aktivita dodavatele vykazuje znaky rozporu s pravidly hospodářské soutěže.
11.	Jednání zástupců dodavatele vykazuje znaky porušování povinnosti péče řádného hospodáře, popřípadě jsou známy jiné skutečnosti, na základě kterých lze předpokládat budoucí značně nepříznivý ekonomický vývoj dodavatele.
12.	Došlo k uvalení mezinárodních sankcí na dodavatele ve smyslu zákona č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů.
13.	Dodavatel dobrovolně spolupracuje se zpravodajskými službami země mající na něj vliv, aniž by jej k tomu zavazoval právní předpis takové země.