NÚKIB

METODIKA K VAROVÁNÍ ZE DNE 17. PROSINCE 2018

Verze 1.0 ze dne 04.01.2019

Obsah

Úvod

Národní úřad pro kybernetickou a informační bezpečnost vydal dne 17. prosince 2018 varování před použitím technických nebo programových prostředků společností Huawei Technologies Co., Ltd., a ZTE Corporation. Na základě četných dotazů odborné i laické veřejnosti Národní úřad pro kybernetickou a informační bezpečnost přistoupil k vydání této metodiky.

Metodika konkretizuje možné postupy správců informačních a komunikačních systémů spadajících pod zákon o kybernetické bezpečnosti a je určena primárně odborníkům zabývajícím se kybernetickou bezpečností.

Metodika vysvětluje institut varování, popisuje princip řízení rizik a nastiňuje možnosti při zajištění plnění povinností podle zákona o kybernetické bezpečnosti v souladu s předpisy regulujícími zadávání veřejných zakázek.

V případě odborných dotazů k této metodice se prosím obracejte na odbor regulace Národního úřadu pro kybernetickou a informační bezpečnost na e-mailovou adresu regulace@nukib.cz.

Komunikaci s médii zajišťuje tiskový mluvčí Národního úřadu pro kybernetickou a informační bezpečnost na e-mailové adrese dotazy.media@nukib.cz.

Upozornění:

Tento dokument slouží jako podpůrné vodítko. Právo změny tohoto dokumentu vyhrazeno.

1 Manažerské shrnutí

Prostřednictvím varování Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB") upozorňuje na existenci hrozby v oblasti kybernetické bezpečnosti, na kterou je nutné bezprostředně reagovat. Subjekty, které spadají pod zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) (dále jen „ZKB"), jsou povinny se touto hrozbou dále zabývat a zohlednit ji v analýze rizik, kterou v souladu s požadavky ZKB a příslušné vyhlášky již pravidelně provádí. Varování tedy neznamená bezpodmínečný zákaz používání daných technických a programových prostředků, ale nutnost zvážit případné bezpečnostní riziko související s jejich užíváním. Dovolí-li to výsledky analýzy rizik, uvedené technické nebo programové prostředky je možné i nadále používat.

Orgánům a osobám, kterým ZKB neukládá povinnost zavést a provádět bezpečnostní opatření, stejně tak jako široké veřejnosti, nezakládá varování NÚKIB žádnou povinnost, a to ani zprostředkovaně. Tyto subjekty tedy nejsou podle ZKB povinny varování NÚKIB zohlednit.

2 Institut varování

2.1 Kdy NÚKIB vydá varování

NÚKIB je zřízen jako ústřední správní úřad pro oblast kybernetické bezpečnosti. Mezi jeho základní poslání patří v souladu s § 22 ZKB, vydávat opatření, zajišťovat prevenci, vzdělávání a metodickou podporu v oblasti kybernetické bezpečnosti a ve vybraných oblastech ochrany utajovaných informací a plnit další úkoly v oblasti kybernetické bezpečnosti stanovené ZKB. Jedním z těchto úkolů je v souladu s § 12 ZKB vydávání varování o hrozbě v oblasti kybernetické bezpečnosti. V souladu se ZKB tedy NÚKIB vydá varování, dozví-li se zejména z vlastní činnosti, z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, o hrozbě v oblasti kybernetické bezpečnosti.

V souladu s výše uvedeným tedy NÚKIB musí k vydání varování přistoupit, pokud se dozví o hrozbě v oblasti kybernetické bezpečnosti. Na základě toho NÚKIB varování vydal.

2.2 Co představuje institut varování

Dle § 12 ZKB prostřednictvím varování NÚKIB upozorňuje na existenci hrozby v oblasti kybernetické bezpečnosti, na kterou je nutné bezprostředně reagovat. Dá se předpokládat, že hrozba se dotýká většiny povinných subjektů podle ZKB. Ty se na základě zmíněného varování musí hrozbou dále zabývat a zohlednit ji v analýze rizik, kterou tyto subjekty v souladu s požadavky ZKB a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti) (dále jen „VKB"), již pravidelně provádí.

Varování tedy neznamená bezpodmínečný zákaz používání daných technických a programových prostředků. Samotné označení technických a programových prostředků určité společnosti za hrozbu, jak to NÚKIB ve svém varování učinil, znamená, že je nutné tuto hrozbu zvážit a rozhodnout o výši rizika, které z používání zmíněných technických nebo programových prostředků pro konkrétní prostředí konkrétní organizace plyne. Dovolí-li to tedy výsledky analýzy rizik, lze uvedené technické nebo programové prostředky nadále používat.

3 Co varování znamená pro jednotlivé subjekty

3.1 Povinné orgány nebo osoby podle § 3 písm. c) až f) ZKB

Správci nebo provozovatelé informačních a komunikačních systémů kritické informační infrastruktury, správci nebo provozovatelé významných informačních systémů a správci nebo provozovatelé informačních systémů základních služeb jsou povinni podle § 5 VKB pro informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém a informační systém základní služby provádět pravidelnou analýzu rizik, identifikovat rizika a identifikovaná rizika řídit.

Na základě vyhodnocení rizik potom výše uvedené subjekty zavádějí a provádějí bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti v souladu s § 4 odst. 2 ZKB. Bezpečnostní opatření jsou blíže specifikována ve VKB. V souvislosti s řízením rizik musejí podle § 5 odst. 1 písm. h) bod 3 VKB tyto subjekty zohlednit mimo jiné i opatření podle § 11 ZKB, tedy i varování vydané podle § 12 ZKB.

S ohledem na přechodné ustanovení v § 35 VKB, které stanoví, že v případě informačních systémů kritické informační infrastruktury a komunikačních systémů kritické informační infrastruktury, které byly určeny přede dnem nabytí účinnosti VKB, a v případě významných informačních systémů, u kterých došlo k naplnění určujících kritérií přede dnem nabytí účinnosti VKB, se do jednoho roku ode dne nabytí účinnosti VKB pro obsah a strukturu bezpečnostní dokumentace a obsah a rozsah zavedených bezpečnostních opatření použijí namísto ustanovení VKB ustanovení vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Datem účinnosti VKB byl 28. květen 2018. Po dobu jednoho roku, tedy do 28. května 2019, tyto povinné osoby zohlední hrozby a zranitelnosti v souvislosti s řízením rizik podle § 4 odst. 1 písm. c) a odst. 2 písm. c) vyhlášky č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti). Po uplynutí této přechodné lhůty, tedy po 28. květnu 2019, již postupují podle § 5 odst. 1 písm. h) bod 3 VKB.

Na základě vydaného varování tedy musejí výše zmíněné povinné osoby v rámci zavedeného řízení rizik provést analýzu rizik, ve které zohlední hrozbu, a následně na riziko reagovat přijetím bezpečnostních opatření, která musí být v souladu s nastavenými metrikami pro akceptovatelnost rizika a hodnotou daného rizika.

Výše zmíněné povinné osoby jsou současně povinny podle § 8 VKB stanovit pravidla pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací (jehož nedílnou

součástí je i vyhodnocení rizik), seznamovat s nimi tyto dodavatele a vyžadovat po dodavatelích plnění těchto pravidel.

Na informační nebo komunikační systémy orgánů nebo osob podle § 3 písm. c) až f) ZKB, které nejsou uvedeny v prvním odstavci této podkapitoly, se výše uvedené povinnosti nevztahují.

3.2 Povinné orgány nebo osoby podle § 3 písm. h) ZKB - poskytovatelé digitálních služeb

Poskytovatel digitální služby podle § 29 VKB zavádí bezpečnostní opatření podle prováděcího nařízení Komise (EU) 2018/151 ze dne 30. ledna 2018. Toto nařízení poskytovateli digitální služby ukládá pro informační systém nebo síť elektronických komunikací, které využívá poskytovatel digitálních služeb v souvislosti se zajišťováním digitální služby podle ZKB, povinnost zavést a provádět vhodná a přiměřená bezpečnostní opatření k řízení bezpečnostních rizik. Mimo jiné mu toto prováděcí nařízení Komise v čl. 2 ukládá, aby v rámci řízení bezpečnosti informací provedl analýzu rizik a řídil dodavatele.

Z praktického pohledu by tedy i poskytovatelé digitální služby měli vydané varování vzít v úvahu při provádění analýzy rizik i při řízení dodavatelů, a to na základě povinností, které jim stanovuje výše zmíněné prováděcí nařízení Komise.

Na informační systémy nebo sítě elektronických komunikací, které poskytovatel digitálních služeb nevyužívá v souvislosti se zajišťováním digitální služby podle ZKB, se výše uvedená povinnost nevztahuje.

3.3 Orgány nebo osoby, které nespadají pod ZKB

Orgánům a osobám, kterým ZKB neukládá povinnost zavést a provádět bezpečnostní opatření, stejně tak jako široké veřejnosti, nezakládá varování žádnou povinnost ani zprostředkovaně. Je tedy na jejich zvážení, jak budou s hrozbou, na kterou varování upozorňuje, dále pracovat.

4 Řízení rizik u orgánů a osob podle ZKB

4.1 Řízení rizik

Obecně lze riziko definovat jako možnost či pravděpodobnost, že určitá hrozba využije zranitelnosti aktiva a způsobí škodu.

Řízení rizik je souhrn činností vedoucích k nalezení a eliminaci rizik. K tomu je zapotřebí nejdříve stanovit rozsah aktiv, kterých se řízení rizik týká. Následným krokem je ohodnocení těchto aktiv a přiřazení a ohodnocení hrozeb a zranitelností pro tato konkrétní aktiva.

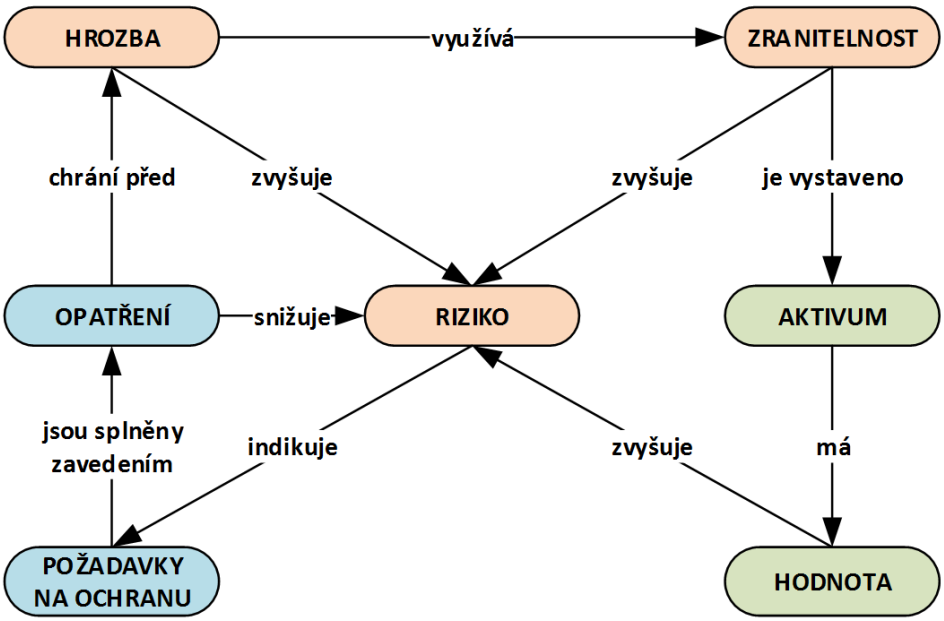
Jako aktivum je obecně vnímáno cokoliv, co má pro organizaci hodnotu. Ve VKB jsou rozlišována primární a podpůrná aktiva, přičemž je nutné je vždy zvažovat ve vztahu ke konkrétní organizaci a konkrétnímu informačnímu nebo komunikačnímu systému.

Primárním aktivem je informace nebo služba, kterou zpracovává nebo poskytuje informační nebo komunikační systém. Podpůrným aktivem jsou pak technická aktiva (technické vybavení, komunikační prostředky a programové vybavení informačního nebo komunikačního systému a objekty, ve kterých jsou tyto systémy umístěny, jejichž selhání může mít dopad na informační nebo komunikační systém), zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního nebo komunikačního systému.

Každé aktivum má zpravidla jednu či více zranitelností (např. nevhodnou bezpečnostní architekturu, nedostatečnou míru nezávislé kontroly, nevhodně nastavená přístupová oprávnění apod.). Těchto zranitelností využívají hrozby jako např. škodlivý kód (viry, spyware, trojské koně apod.), zneužití nebo neoprávněná modifikace údajů, cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik apod. Více viz níže uvedená přehledová tabulka hrozeb.

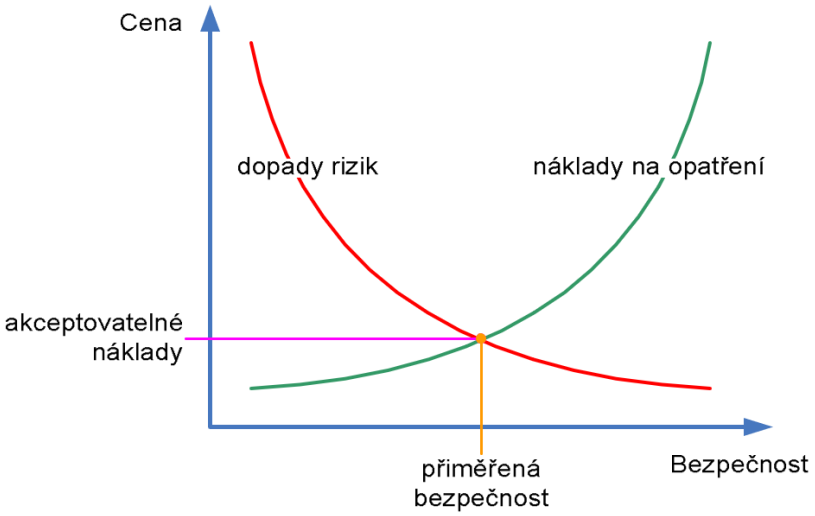
Jakmile je známa hodnota aktiva (viz příloha č. 1 k VKB) a hodnota s ním spojených hrozeb a zranitelností (viz příloha č. 2 k VKB), je nutné určit hodnotu rizika. Riziko je kombinací hrozby, zranitelnosti a dopadu na aktivum (dopad bude vycházet z hodnoty aktiva).

Výsledná míra rizika následně indikuje požadavky na ochranu, tedy na konkrétní bezpečnostní opatření, která je nutné zavést a tím snížit velikosti rizika naplnění hrozby. To znamená, že bezpečnostní opatření snižují možnost naplnění nežádoucích jevů.



Obrázek č. 1 Přehledové schéma k řízení rizik[1]

Náklady na bezpečnostní opatření by však měly být vždy přiměřené a neměly by převýšit náklady spojené s následky realizace rizika. Toto ilustruje následující schéma.



Obrázek č. 2 Akceptovatelné náklady[2]

[1] Vladimír SMEJKAL a Karel RAIS. Řízení rizik ve firmách a jiných organizacích. 4., aktualiz. a rozš. vyd. Praha: Grada, 2013. Expert (Grada). ISBN 978-80-247-4644-9.
[2] Viktor ONDRÁK, Petr SEDLÁK a Vladimír MAZÁLEK. *Problematika ISMS v manažerské informatice*. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

4.2 Co mají orgány a osoby povinné podle ZKB činit

Vydané varování povinné orgány a osoby zohlední v souladu s požadavkem § 5 písm. h) VKB v rámci procesu řízení rizik.

Zjednodušeně lze celý proces postupu shrnout v následujících krocích:

1. Analýza prostředí a prošetření, zda a kde jsou dané technické nebo programové prostředky v rámci informačních a komunikačních systémů využívány (např. v seznamu podpůrných aktiv nebo v seznamu majetku organizace).

2. U aktiv souvisejících s vydaným varováním je potřeba provést aktualizaci analýzy rizik a zohlednit nové hrozby plynoucí z vydaného varování. V rámci tohoto kroku je důležitá spolupráce manažera kybernetické bezpečnosti, který má znalost procesu analýzy rizik, s garantem aktiva, který je schopný ohodnotit aktivum, jehož je garantem.

3. Výsledkem aktualizace analýzy rizik je nová hodnota rizika. V případě, že je překročena akceptovatelná míra rizika, kterou má povinná osoba stanovenu v souladu s požadavky § 5 VKB, je nutné přistoupit k zavedení bezpečnostních opatření a tím k snížení rizika.

4. Jedním z možných opatření může být např. postupná náhrada daných technických a programových prostředků a jejich vyloučení z výběrového řízení. Další možností je např. úprava pravidel pro dodavatele, která zohledňují požadavky systému řízení bezpečnosti informací organizace, seznámení dodavatelů s těmito pravidly a vyžadování plnění těchto pravidel po dodavatelích. Bezpečnostní opatření definuje VKB.

Ze skutečností uvedených ve vydaném varování vyplývá, že hrozbu, na kterou varování upozorňuje, je v souladu s tabulkou č. 1 přílohy č. 2 VKB potřeba hodnotit jako velmi pravděpodobnou až více méně jistou. V případě užití jiné stupnice hodnocení hrozby, jak umožňuje § 5 odst. 3 VKB, je nutno tuto hrozbu ohodnotit způsobem odpovídajícím příslušné úrovni podle VKB.

4.3 Přehledová tabulka hrozeb

Přehledová tabulka hrozeb slouží pouze jako demonstrativní výčet, který je potřeba přizpůsobit prostředí konkrétní organizace. Níže uvedené informace nenahrazují VKB a nejedná se tedy o úplný seznam všech možných hrozeb.

Tabulka č. 1: Přehledová tabulka hrozeb

Výskyt hrozby	Projev hrozby
na úrovni telekomunikačních komponent	zaznamenávání hovorů
	kontrola nad obsahem přenášených dat
	lokalizace uživatelů
	deaktivace telekomunikačních služeb (nefunkční hlasové a datové služby)
na úrovni serverových řešení a infrastruktury	přístup k veškerým datům
	kontrola nad obsahem přenášených dat
	možnost odepření služby
na koncových zařízeních	přístup k uloženým datům (šifrování na zařízení není ochranou)
	pořizování záznamu (audio, video)
	získání geolokačních dat
	podvrhnutí identity

4.4 Bezpečnostní opatření

Konkrétní bezpečnostní opatření musejí reagovat na individualizované riziko. Vzhledem k velké diverzitě informačních a komunikačních systémů, které spadají pod ZKB, nelze konkrétní bezpečnostní opatření paušálně specifikovat, ale je třeba zohledňovat příslušné prostředí a technologie. Zákonem požadovaná bezpečností opatření specifikuje VKB.

5 Zohlednění varování při řízení dodavatelů

Výše popsaný proces analýzy a řízení rizik je potřeba v souladu s § 4 odst. 4 ZKB provést také v rámci výběru dodavatele a výsledná opatření promítnout do smluv, které budou s dodavateli uzavřeny.

Za dodavatele se v tomto případě považují nejen společnosti Huawei Technologies Co., Ltd., a ZTE Corporation, uvedené v samotném varování, ale i všechny další společnosti, které technické nebo programové prostředky zmiňovaných společností přeprodávají nebo které dodávají technické celky, jejichž součástí jsou prostředky zmiňovaných společností. Je však potřeba mít na paměti, že vydané varování se týká pouze technických a programových prostředků, nikoli osoby samotného dodavatele podle písm. e) přílohy č. 7 VKB musí každý dodavatel zajistit, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem a nebudou jednat v rozporu s požadavky povinné osoby na dodavatele.

6 Zajištění souladu postupu podle ZKB se zákonem o zadávání veřejných zakázek

NÚKIB upozorňuje, že níže uvedené nastiňuje možnosti správců systémů při zajištění splnění povinností podle ZKB v souladu s předpisy regulujícími zadávání veřejných zakázek. Aplikaci níže nastíněných postupů je však třeba vždy zvažovat ve světle skutkových okolností konkrétního případu. K rozhodování o tom, zda je postup zadavatele souladný s pravidly obsaženými v zákoně o zadávání veřejných zakázek, je pak příslušný Úřad pro ochranu hospodářské soutěže, nikoli NÚKIB.

Obecně musí zadavatel při zadávání veřejných zakázek postupovat podle zákona č. 134/2016 Sb., o zadávání veřejných zakázek (dále jen „ZZVZ“). Tento zákon v § 36 odst. 1 stanoví, že zadavatel nesmí vytvářet při stanovování zadávacích podmínek “*bezdůvodné překážky hospodářské soutěže*“. V případě, že oprávněná autorita (zde NÚKIB), která k tomuto kroku disponuje zákonným zmocněním (zde v § 22 písm. b) ZKB), vydává akt (zde varování), který může v konkrétních případech vést k omezení hospodářské soutěže, nemůže být dodržení tohoto omezení při tvorbě zadávacích podmínek považováno za vytváření bezdůvodné překážky hospodářské soutěže. Tedy hospodářskou soutěž v tomto případě lze omezit již při stanovení zadávacích podmínek a nejedná se tím o porušení ZZVZ.

Nadto ve vztahu k orgánům a osobám uvedeným v § 3 písm. c) až f) ZKB ustanovení § 4 odst. 4 ZKB stanoví, že jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační systém kritické informační infrastruktury, komunikační systém kritické informační infrastruktury, významný informační systém nebo informační systém základní služby a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle ZKB nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Je však potřeba zvolit odpovídající postupy ve vztahu k tomu, v jaké fázi se dané výběrové řízení nachází:

- Fáze přípravy na veřejnou zakázku.
- Fáze probíhajícího zadávacího řízení.
- Fáze po skončení zadávacího řízení a zadání zakázky uchazeči.

6.1 Fáze přípravy na veřejnou zakázku (příprava zadávací dokumentace/zadávacích podmínek vč. smluvních podmínek)

V souladu s § 8 odst. 1 písm. e) VKB musí povinná osoba řídit rizika spojená s dodavateli. Je tedy nutné provedení analýzy rizik podle § 5 VKB a následné zapracování jejího výsledku přímo do zadávací dokumentace.

6.2 Fáze probíhajícího zadávacího řízení

a) V rámci zadávacího řízení neuplynula lhůta pro podání žádosti o účast, předběžných nabídek nebo nabídek

V takovém případě lze po provedení analýzy rizik v souladu s ustanovením § 99 ZZVZ změnit nebo doplnit zadávací podmínky obsažené v zadávací dokumentaci. Změna nebo doplnění zadávací dokumentace musí být uveřejněna nebo oznámena dodavatelům stejným způsobem jako zadávací podmínka, která byla změněna nebo doplněna (zpravidla uveřejněním na profilu zadavatele, ve Věstníku veřejných zakázek, resp. Úředním věstníku Evropské unie).

Zde NÚKIB upozorňuje na povinnost vyplývající z druhého odstavce výše citovaného ustanovení ZZVZ, kdy je zadavatel povinen přiměřeně prodloužit lhůtu pro podání žádostí o účast, předběžných nabídek nebo nabídek. ZZVZ v tomto ustanovení dále ukládá zadavateli povinnost prodloužit lhůtu tak, aby od odeslání změny nebo doplnění zadávací dokumentace činila nejméně celou svou původní délku v případě takové změny nebo doplnění zadávací dokumentace, která může rozšířit okruh možných účastníků zadávacího řízení. Byť úpravou zadávacích podmínek podle varování dochází *de facto* spíše k omezení okruhu možných účastníků, NÚKIB vycházeje ze zásad uvedených v ustanovení § 6 ZZVZ doporučuje prodloužit lhůtu pro podání žádostí o účast, předběžných nabídek nebo nabídek tak, aby činila nejméně celou svou původní délku, a to z důvodu, že by uchazeči za změněných podmínek mohli nabídnout i jiné produkty než původně zamýšleli, příp. z kterých vycházeli při zvažování, zda v daném zadávacím řízení podají žádost o účast, předběžnou nabídku nebo nabídku, a k učinění této úvahy je třeba uchazečům poskytnout adekvátních prostor.

b) V rámci zadávacího řízení již uplynula lhůta pro podání nabídek

Po provedení analýzy rizik lze buď pokračovat v zadávacím řízení a případně přijmout bezpečnostní opatření ke snížení rizika (aniž by tím byl dotčen postup v zadávacím řízení), nelze-li, pak zrušit zadávací řízení z důvodů podle § 127 odst. 2 písm. d) ZZVZ. Důvodem pro tento krok pak je, že v průběhu zadávacího řízení se podle názoru NÚKIB vyskytly důvody hodné zvláštního zřetele (bylo vydáno varování národní autoritou k tomu oprávněnou), pro které nelze po zadavateli požadovat, aby v zadávacím řízení pokračoval (nedostal by plnění odpovídající všem podmínkám, kterými je povinen se řídit vč. varování NÚKIB) a nadto

zadavatel tyto důvody nezpůsobil (je tak donucen činit na základě objektivních skutečností vzniklých vně zadavatele).

NÚKIB zde upozorňuje, že vydání varování nelze automaticky považovat za důvod pro vyloučení uchazeče ze zadávacího řízení. I nadále platí, že zadavatel je oprávněn vyloučit uchazeče ze zadávacího řízení pouze z důvodů stanovených v ZZVZ (zadavatel by tedy musel varování NÚKIB, resp. důsledky plynoucí z jeho vydání, podřadit pod některý z důvodů uvedených v § 48 ZZVZ).

6.3 Fáze po skončení zadávacího řízení a zadání zakázky uchazeči

V souladu s § 8 odst. 1 písm. e) VKB musí povinná osoba řídit rizika spojená s dodavateli. Je tedy nutné provedení analýzy rizik podle § 5 VKB a na základě jejího výsledku provést jedno z následujících:

a) **V případě potřeby zvážit nasazení bezpečnostních opatření ke snížení rizik.**

NÚKIB upozorňuje v této souvislosti na ustanovení § 222 odst. 1 ZZVZ, podle něhož zadavatel nesmí umožnit podstatnou změnu závazku ze smlouvy na veřejnou zakázku po dobu jeho trvání bez provedení nového zadávacího řízení podle ZZVZ.

V případě plnění realizovaných na základě rámcové dohody NÚKIB upozorňuje na ustanovení § 131 ZZVZ, podle něhož zadavatel nesmí umožnit podstatnou změnu podmínek rámcové dohody po dobu jejího trvání bez provedení nového zadávacího řízení podle ZZVZ, přičemž zadavatel nesmí umožnit ani podstatnou změnu podmínek uvedených v rámcové dohodě při zadávání veřejných zakázek na základě této rámcové dohody.

Co je podstatnou změnou závazku podle ZZVZ je třeba vždy posuzovat individuálně vzhledem k charakteru původní veřejné zakázky a jednotlivých učiněných změn a toto posouzení vždy přísluší zadavateli.

b) **V případě, že není možné přijmout bezpečnostní opatření ke snížení rizika, nahradit technické a programové prostředky na základě nového zadávacího řízení.**

V této souvislosti NÚKIB uvádí, že možnost ukončení smlouvy je v ZZVZ řešena v ustanovení § 223. Podle tohoto ustanovení může zadavatel závazek ze smlouvy na veřejnou zakázku vypovědět nebo od ní odstoupit v případě, že v jejím plnění nelze pokračovat, aniž by byla porušena pravidla uvedená v § 222 ZZVZ. Současně tím není dotčeno právo zadavatele ukončit závazek ze smlouvy na veřejnou zakázku podle jiných právních předpisů (typicky občanského zákoníku) či smluvních ujednání v uzavřených smlouvách.

Vše uvedené se vztahuje na zadavatele ve smyslu § 4 ZZVZ, tedy nejen na veřejné zadavatele ale mimo jiné též na jiné osoby, které při výkonu relevantní činnosti zadávají sektorovou zakázku podle ustanovení § 151 a násl. ZZVZ, a to v míře dané jednotlivými ustanoveními ZZVZ.

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
04.01.2019	1.0	NÚKIB	Vytvoření dokumentu