Specifika a zadávání VZ v oblasti ICT a KB

NÚKIB

Národní úřad pro kybernetickou a informační bezpečnost

23. října 2024, Zlín
TLP:CLEAR

Jan Hénik
Oddělení regulace veřejného sektoru
Odbor regulace

Zadávání veřejných zakázek v oblasti ICT a KB

Hlavní problémy:

- **způsoby zohlednění požadavků vyplývajících z vyhlášky o kybernetické bezpečnosti (VKB) v zadávacím řízení,**
- **omezování rizikových technologií,**
- zamezení šíření bezpečnostní či jinak citlivé dokumentace v rámci zadávacího řízení,
- správné nastavení kvalifikačních předpokladů a jejich kontrola,
- kontrola a řízení poddodavatelů,
- plánování a náklady životního cyklu.

Hodnocení rizik a požadavky ZKB a VKB (současné)

§ 4 odst. 2 ZKB: Povinnost zavádět bezpečnostní opatření

§ 4 odst. 4 věta první ZKB: Povinnost zohlednit bezpečnostní opatření při výběru dodavatele a zahrnout je do smlouvy.

§ 4 odst. 4 věta druhá ZKB: Zohlednění požadavků vyplývajících z bezpečnostních opatření v míře nezbytné pro splnění povinností podle ZKB nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

§ 5 odst. 2 písm. b) ZKB: Organizačními opatřeními jsou (…) řízení rizik.

§ 3 písm. c) VKB: Povinná osoba v rámci systému řízení bezpečnosti informací pro stanovený rozsah systému řízení bezpečnosti informací na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a hodnocení rizik zavede přiměřená bezpečnostní opatření.

§ 36 odst. 1 ZZVZ: Zadávací podmínky nesmí být stanoveny tak, aby určitým dodavatelům bezdůvodně přímo nebo nepřímo zaručovaly konkurenční výhodu nebo vytvářely bezdůvodné překážky hospodářské soutěže.

Hodnocení rizik a požadavky ZKB a VKB

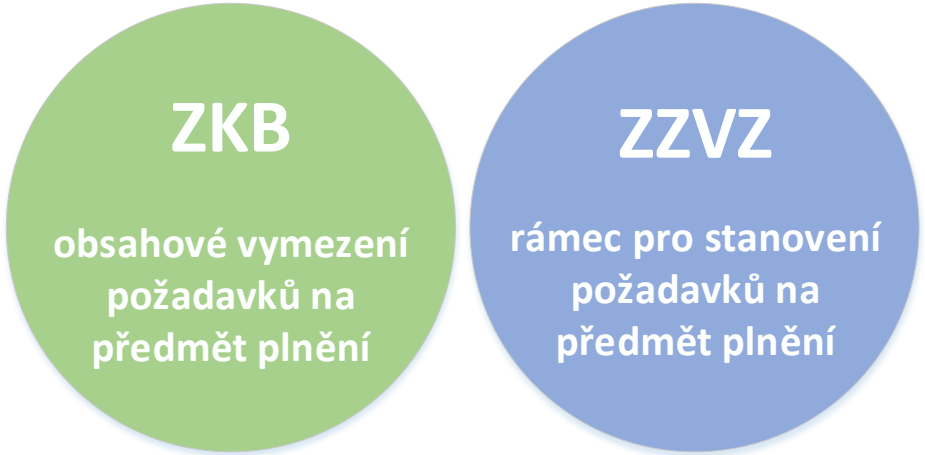
- Všechna bezpečnostní opatření z VKB jsou podřaditelná pod některý z institutů upravených ZZVZ

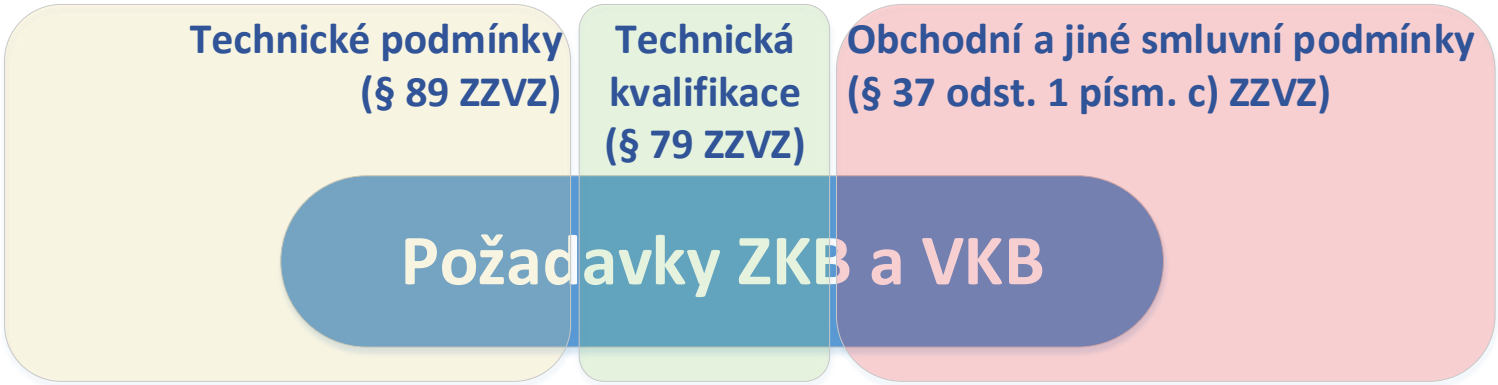
  - kvalifikaci dodavatele,
  - požadavky na předmět plnění
  - kritéria pro hodnocení nabídek.

⇒ Záleží pouze na potřebách zadavatele, jeho schopnosti řádně nadefinovat všechny podmínky pro přístup dodavatelů k zakázce a jeho kreativitě při využití možností, které mu ZZVZ nabízí.

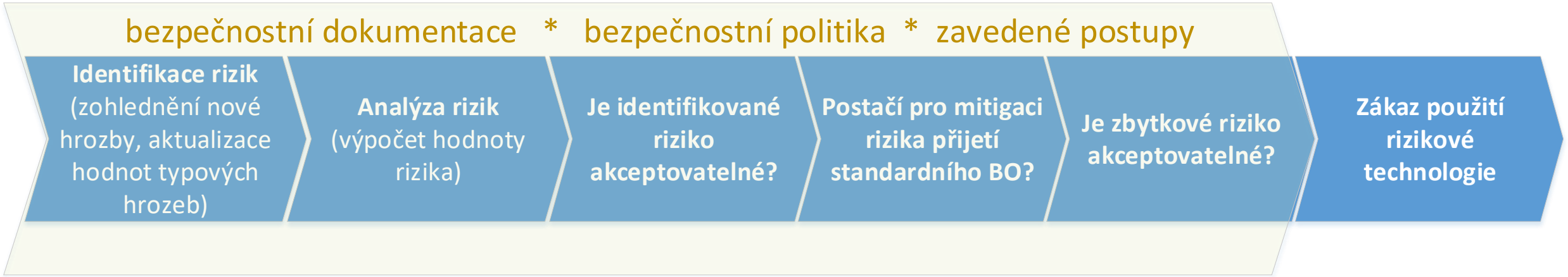
- Volba konkrétní úrovně zabezpečení systémů a konkrétních bezpečnostních opatření musí být založena na řádně provedené analýze aktiv a s nimi souvisejících rizik.

Hodnocení rizik a požadavky ZKB a VKB





Hodnocení rizik a požadavky ZKB a VKB



Scénáře zpracování výsledku hodnocení rizik

1. hodnota rizika nedosáhne neakceptovatelné míry rizika, kterou má zadavatel stanovenu
   - zadavatel tedy nemusí přijímat dodatečná bezpečnostní opatření, která by byl v souladu se ZKB povinen zohlednit v zadávací dokumentaci
2. hodnota rizika dosáhne neakceptovatelné míry rizika, kterou má zadavatel stanovenu
   a) mitigace rizika pomocí standardních (mírnějších) bezpečnostních opatření (např. redundance)
   b) mitigace rizika pomocí úplného zákazu rizikové technologie

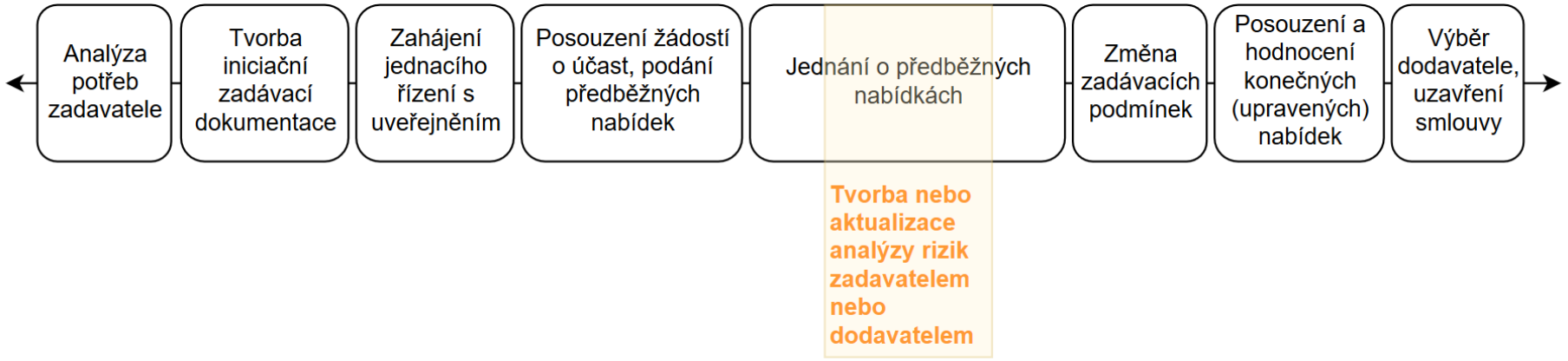
Hodnocení rizik a požadavky ZKB a VKB

Otevřené a užší řízení

- Předpokladem schopnost definovat v podrobnostech předmět VZ
- Pokud může zadavatele výsledné řešení “překvapit“ (nebo black-box), nelze bez dalšího rizikové technologie zakazovat → zvážit jiný druh ZŘ

Jednací řízení s uveřejněním

- Pokud zadavatel plánuje o konkrétní podobě výsledného řešení jednat (+ podmínky ZZVZ) – ne off-the-shelf řešení



Tvorba zadávacích podmínek

§ 36 odst. 1 ZZVZ: *„Zadávací podmínky nesmí být stanoveny tak, aby určitým dodavatelům bezdůvodně přímo nebo nepřímo zaručovaly konkurenční výhodu nebo vytvářely bezdůvodné překážky hospodářské soutěže.“*

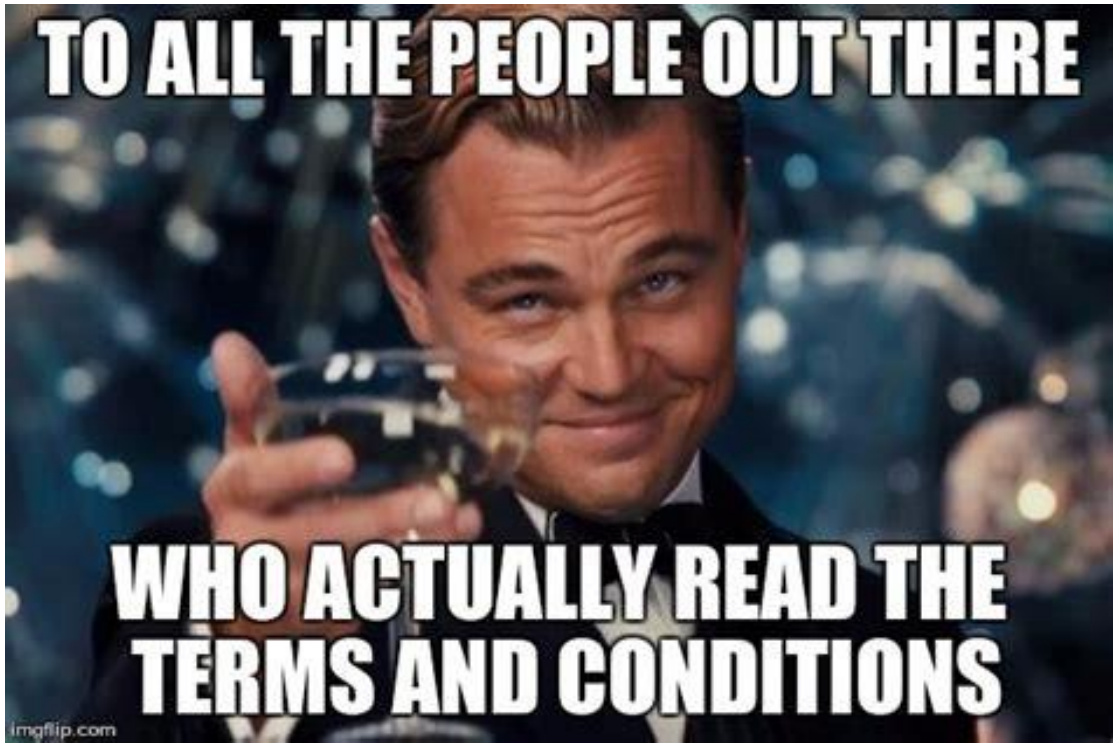
§ 36 odst. 3 ZZVZ: *„Zadávací podmínky zadavatel stanoví a poskytne dodavatelům v podrobnostech nezbytných pro účast dodavatele v zadávacím řízení. Zadavatel nesmí přenášet odpovědnost za správnost a úplnost zadávacích podmínek na dodavatele.“*

- ✓ Požadavky plynoucí z právních předpisů
- ✓ Požadavky plynoucí ze závazných dokumentů nadřízeného orgánu (nikoli vlastních interních) nebo uzavřených smluv
- ✓ Požadavky odůvodněné potřebami zadavatele
- × Požadavky neodůvodněné
- × Požadavky protizákonné

Tvorba zadávacích podmínek

- Problém je primárně v neschopnosti nadefinovat zadávací podmínky v nezbytných podrobnostech
- Výsledek – desítky až stovky stran požadavků

- ✓ Nadefinovat všechny požadavky v co největších podrobnostech (srozumitelně)
- ✓ Všechny požadavky mít odůvodněny (mimo ZD)
- ✓ Neodůvodněně nediskriminovat
- ✓ Lze počítat s určitou úrovní oborové znalosti (nenahrazuje povinnost stanovit podmínky řádně)
- ✓ Jednoznačně stanovit, jaká nabídka bude hodnocena jako nejvýhodnější



Tvorba zadávacích podmínek

Požadavky na osobu dodavatele

- Kvalifikace – základní, profesní, ekonomická, technická (taxativní vymezení)
- Obligatorní důvody pro vyloučení vybraného dodavatele – předložení nepravdivých dokumentů, a.s. s listinnými akciemi, skutečný majitel ve střetu zájmů (min. 25 % účast veřejného funkcionáře)
- Fakultativní důvody pro vyloučení uchazeče – profesní pochybení, pochybení při plnění dřívějšího smluvního vztahu, sociální aspekty, střet zájmů, narušení hospodářské soutěže předchozí účastí účastníka při přípravě zadávacího řízení, pokus o neoprávněné ovlivnění výsledku zadávacího řízení, uzavření kartelové dohody

Technické podmínky (požadavky na předmět plnění)

- parametry vyjadřujících požadavky na výkon nebo funkci
- popis účelu nebo potřeb, které mají být naplněny
- odkazy na normy nebo technické dokumenty (možnost nabídnout rovnocenné řešení)
- odkazy na štítky, zkušební protokoly, osvědčení, další doklady o shodě
- ! odkazy na určité dodavatele nebo výrobky (výjimečně, možnost nabídnout rovnocenné řešení)

Omezení hospodářské soutěže je možné pokud lze obhájit objektivními skutečnostmi, tzn. že použití určité technologie je prokazatelně rizikovější, než použití jiné.

Hodnocení nabídek

Hodnocení nabídek podle jejich **ekonomické výhodnosti**

- Nejvýhodnější poměr ceny a kvality včetně poměru nákladů životního cyklu a kvality
- Nejnižší nabídková cena (v řízení se soutěžním dialogem, v řízení o inovačním partnerství a u některých služeb zakázáno)
- Nejnižší náklady životního cyklu

Pravidla pro hodnocení nabídek (nutno stanovit v ZD)

- kritéria hodnocení (vyjadřující kvalitativní, environmentální nebo sociální hlediska spojená s předmětem VZ)
- metoda vyhodnocení nabídek v jednotlivých kritériích
- váha nebo jiný matematický vztah mezi kritérii (nebo jiný význam, který jednotlivým hodnotícím kritériím přisuzuje)

Hodnocení nabídek

Co lze např. hodnotit:

- technická úroveň
- estetické nebo funkční vlastnosti
- uživatelská přístupnost
- sociální, environmentální nebo inovační aspekty
- organizace, kvalifikace nebo zkušenost osob, které se mají přímo podílet na plnění veřejné zakázky v případě, že na úroveň plnění má významný dopad kvalita těchto osob (nad rámec minimálních požadavků)
- úroveň servisních služeb včetně technické pomoci
- podmínky a lhůta dodání nebo dokončení plnění
- **bezpečnostní aspekty**!!!

Co nelze hodnotit:

- smluvní podmínky utvrzující povinnost dodavatele (smluvní pokuta)
- platební podmínky

Obecná doporučení - shrnutí

- **Využívejte plně možnosti, které ZZVZ dává**
- **Každý krok zadávacího řízení si odůvodněte**
  - ZZVZ zadavatele pouze nesvazuje, ale dává mu možnosti, jak chránit své zájmy
  - tyto zájmy však musí zadavatel odůvodnit logickými a pevnými argumenty
  - každý krok zadavatele by měl být proto odůvodněný, odůvodnitelný a řádně zdokumentovaný
  - takový postup poskytuje značnou výhodu u případného přezkumu
- **Plňte řádně povinnosti vyplývající ze ZKB**
  - ZZVZ stanovuje „jak“ a nikoliv „co“ mají zadavatelé poptávat
  - ZKB a prováděcí předpisy naopak stanovují kvalitativní stránku IS a zařízení, tedy „co“

Pokud je předmět VZ založen na řádném plnění povinností vyplývajících ze ZKB, zejm. na řádně provedeném procesu řízení rizik a výběru bezpečnostních opatření k zajištění požadované úrovně KB, pak nemohou být z podstaty věci považovány za neodůvodněné.

Aplikace VAROVÁNÍ v zadávacím řízení

Zohlednění varování při tvorbě zadávací dokumentace

Obecná východiska

- **Zákon o kybernetické bezpečnosti (ZKB) a vyhláška o kybernetické bezpečnosti (VKB)**
  - Povinnosti jsou ukládány pouze povinným osobám, ty zavádí systém řízení bezpečnosti informací (ISMS)
  - ISMS se povinně nevztahuje na celou určenou organizaci, pouze na určené IS a KS
- **Risk based approach**
  - Přístup založený na riziku
  - **ZKB a VKB ukládají povinnosti – zavádění bezpečnostních opatření (ISMS)**
    - Jejich výběr a zavedení závisí na výsledku analýzy rizik
  - Hodnota rizika aktiva je vypočítána prostřednictvím funkce:
    - **Riziko = Dopad (hodnota aktiva) x Zranitelnost x Hrozba**
      - Výsledná míra rizika indikuje požadavky na ochranu, tedy na konkrétní bezpečnostní opatření, která jsou způsobilá snížit možnost naplnění nežádoucích jevů.
    - Konkrétní hodnoty prvků funkce volí subjekt obvykle na základě subjektivního hodnocení

Institut varování

- Jedno z protiopatření podle § 20 nZKB
  - = úkony, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu
  - = varování, výstraha, reaktivní protiopatření
- Projev zákonné pravomoci NÚKIB analyzovat a monitorovat kybernetické hrozby a rizika
- **Nenahrazuje, pouze doplňuje** obecnou povinnost regulovaných subjektů identifikovat hrozby

- **§ 22 nZKB – Varování**

(1) Úřad vydá varování, dozví-li se o závažné hrozbě nebo zranitelnosti v oblasti kybernetické bezpečnosti.

(2) Varování Úřad oznámí dotčeným poskytovatelům regulované služby prostřednictvím Portálu Úřadu a zveřejní jej na úřední desce Úřadu. Úřad varování nezveřejní, pokud by zveřejnění mohlo ohrozit zajišťování kybernetické bezpečnosti, jiné oprávněné zájmy státu nebo by na jeho základě bylo možné identifikovat toho, kdo hrozbu, zranitelnost nebo s tím související kybernetický bezpečnostní incident nahlásil.

Co varování znamená

- Prostřednictvím varování NÚKIB **upozorňuje na existenci hrozby** v oblasti kybernetické bezpečnosti, na kterou je nutné bezprostředně reagovat
- Varování je závazné pro regulované subjekty, neregulované subjekty mohou varování zohlednit dobrovolně
- Varování nic nezakazuje ani nepřikazuje – ZKB však stanoví povinnost s informací obsaženou ve varování dále pracovat
  - Např. pokud jsou varováním za hrozbu označeny technické nebo programové prostředky určitých společností, **neznamená to bezpodmínečný zákaz používání** daných 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

Význam varování pro regulované subjekty

- **Subjekty,** které spadají pod 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
- V rámci analýzy rizik je nutno aktualizovat katalog hrozeb o tuto hrozbu
  - Formulace hrozby – podle obsahu varování
  - Typová hrozba x konkrétní hrozba x definice z varování
- Hodnota hrozby – podle obsahu varování (dá se předpokládat, že nejčastěji půjde o hodnotu 4 ze 4)

Význam varování pro neregulované subjekty

- **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
- Další kroky s tím spojené jsou pouze na nich, jsou dobrovolné a nemohou být NÚKIB kontrolovány a sankcionovány
- Varování však může být zohledněno v analýze rizik (ISO 27001 a ISO 27005) – postup analogický s postupem regulovaných subjektů

Implementace varování

- Proces řízení rizik – povinnost **zohlednit mj. i protiopatření**, tedy i varování
- Na základě vyhodnocení rizik – **zavedení a provedení bezpečnostních opatření** v rozsahu nezbytném pro zajištění kybernetické bezpečnosti
  - Akceptovatelná úroveň rizika x přiměřená bezpečnostní opatření x akceptace rizika
- Bezpečnostní opatření – blíže specifikována ve vyhlášce
  - Organizační – bezpečnostní role, řízení dodavatelů, bezpečnost lidských zdrojů, řízení provozu a komunikací atd., technická – fyzická bezpečnost, správa a ověřování identit, řízení přístupových oprávnění, logování přístupů, kryptografické prostředky atd.
- **Na základě vydaného varování tedy musejí 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**

Zohlednění varování při zadávání veřejných zakázek

Konkrétní postup se odvíjí od fáze výběrového řízení (vždy založeno na výsledcích analýzy rizik):

1. Fáze přípravy zadávacího řízení
   - Zapracování výsledku analýzy rizik do **zadávací dokumentace**
2. Fáze probíhajícího zadávacího řízení
   a. Neuplynula lhůta pro podání žádosti o účast, předběžných nabídek nebo nabídek
      - **Změna / doplnění zadávacích podmínek** + prodloužení lhůty
   b. Lhůta uplynula
      - **Pokračování v zadávacím řízení** + **přijetí** takových **bezpečnostních opatření**, kterými nebude dotčen postup v ZŘ (např. organizační opatření uvnitř zadavatele)
      - **Zrušení zadávacího řízení**, pokud nelze pokračovat bez změny zadávacích podmínek (tj. přijetí jiných bezpečnostních opatření není možné)
3. Fáze po skončení zadávacího řízení a zadání zakázky uchazeči
   - Řízení rizik spojených s dodavateli
      - Nasazení **bezpečnostních opatření** ke snížení rizik
      - Postupné **nahrazení HW a SW** (podle možností)

Zohlednění varování ze 17. prosince 2018

- Vydání varování **nelze automaticky považovat za důvod pro vyloučení uchazeče** ze zadávacího řízení
  - Nejde o kvalifikační požadavky, ale o požadavky na předmět plnění (technické podmínky)
  - Nejde o vyloučení konkrétního dodavatele – prakticky se zadávacího řízení může účastnit i společnost, jejíž technické a programové prostředky jsou varováním označeny za hrozbu, nicméně nemůže nabídnout vlastní výrobky
- Vyloučit technické a programové prostředky uvedené ve varování je možné cestou **technické specifikace**
  - Půjde o stanovení technických podmínek (srov. § 89 ZZVZ)
  - Případné vyřazení nabídky obsahující prostředky uvedené ve varování bude odůvodněno nesplněním zadávacích podmínek
- **Vyloučení technických a programových prostředků je nutné odůvodnit**
  - Odůvodnění poskytne analýza rizik

Zohlednění varování ze 17. prosince 2018

- Máme již pravomocné rozhodnutí ÚOHS ze dne 19. 2. 2024 (sp. zn. ÚOHS-S0628/2023/VZ), kdy **neregulovaný subjekt na základě správně provedené AR vyloučil HUA a ZTE**, přičemž návrh HUA proti postupu tohoto zadavatele byl zamítnut, jelikož ÚOHS neshledal důvody pro uložení nápravného opatření.

Aplikace OOP v zadávacím řízení

Zohlednění OOP při tvorbě zadávací dokumentace

Aplikace OOP v zadávacím řízení

1. příprava před zahájením zadávacího řízení

- Zadavatel upraví připravované zadávací podmínky tak, aby byly v souladu s opatřením obecné povahy. Pokud v následujícím zadávacím řízení nebude tato zadávací podmínka splněna, může zadavatel dodavatele vyloučit podle § 48 odst. 2 ZZVZ. Reakce zadavatele na opatření obecné povahy bude tudíž obdobné jako v případě bezpečnostních opatření vyplývajících z právních předpisů obecně.

- Teoreticky lze stanovit zadávací podmínka, která by reflektovala i dosud nevydané OOP
  - Např. *„nabídka a účast v zadávacím řízení nesmí být v rozporu s opatřením obecné povahy stanovícím podmínky nebo zakazujícím využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, které vydal NUKIB podle § … zákona o kybernetické bezpečnosti“.*

Aplikace OOP v zadávacím řízení

Takováto zadávací podmínka by byla:

- stanovena zadavatelem předem v zadávací dokumentaci (transparentnost, § 6 odst. 1 ZZVZ),
- reagovala by na bezpečnostní hrozby (přiměřenost, § 6 odst. 1 ZZVZ) a
- nebyla založena na libovůli zadavatele (rovný přístup a zákaz diskriminace, § 6 odst. 2 ZZVZ).

Zároveň by byla:

- důvodná (§ 36 odst. 1 ZZVZ) a
- poskytnutá v podrobnostech nezbytných pro účast v zadávacím řízení (§ 36 odst. 3 ZZVZ).

Přihlížíme k tomu, že k návrhu opatření obecné povahy bude probíhat připomínkové řízení, a tak jeho vydání nebude pro zadavatele a dodavatele zcela překvapivé a bez možnosti obrany.

Aplikace OOP v zadávacím řízení

2. průběh zadávacího řízení před podáním nabídky (žádosti o účast, předběžné nabídky)

- Zadavatel může zadávací podmínky změnit (§ 99 ZZVZ) tak, aby dosáhl souladu s opatřením obecné povahy. Pokud nebude změněná zadávací podmínka splněna může dojít k vyloučení dodavatele podle § 48 odst. 2 ZZVZ.

Aplikace OOP v zadávacím řízení

3. průběh zadávacího řízení po podání nabídky

- Pokud již uplynula lhůta pro podání nabídek, není možné zadávací podmínky změnit. Smlouva musí být uzavřena v souladu s nabídkou (§ 51 odst. 3 ZZVZ). Pokud by uzavření smlouvy v souladu s nabídkou mělo vést k porušení opatření obecné povahy, **může zadavatel zadávací řízení zrušit**, protože v průběhu zadávacího řízení se vyskytly **důvody hodné zvláštního zřetele, pro které nelze po zadavateli požadovat, aby v zadávacím řízení pokračoval** (§ 127 odst. 2 písm. d) ZZVZ).

Aplikace OOP v zadávacím řízení

4. po uzavření smlouvy

- Zadavatel bude moci využít nového ustanovení (§ 32 nZKB) a závazek vypovědět. Případně může být smlouva změněna podle § 222 ZZVZ tak, aby bylo dosaženo souladu mezi smlouvou a opatřením obecné povahy.

Vyloučení účastníka ze zadávacího řízení

- **Vyloučení musí proběhnout přes § 48 odst. 2 ZZVZ**, podle kterého zadavatel může vyloučit účastníka zadávacího řízení, pokud údaje, doklady, vzorky nebo modely předložené účastníkem zadávacího řízení

(a) nesplňují zadávací podmínky nebo je účastník zadávacího řízení ve stanovené lhůtě nedoložil,
(b) nebyly účastníkem zadávacího řízení objasněny nebo doplněny na základě žádosti podle § 46.

- V § 48 odst. 1 ZZVZ je stanoveno, že zadavatel může vyloučit účastníka zadávacího řízení **pouze z důvodů stanovených tímto zákonem**, a to kdykoliv v průběhu zadávacího řízení.

- ZZVZ nestanovuje, že by v případě OOP mohlo dojít k vylučování bez promítnutí do zadávací podmínky.

- Jedná se o transpoziční právní úpravu, a tak není pro rozšiřování důvodů vyloučení ze zadávacího řízení prostor (čl. 56 směrnice 2014/24/EU).

Děkuji za pozornost!

nis2.nukib.gov.cz

regulace@nukib.gov.cz