Požadavky zadavatele v oblasti kybernetické bezpečnosti

Zadavatel je v postavení provozovatele základní služby dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „**ZKB**“).

Účelem těchto podmínek je zajistit splnění povinností, které zadavateli ve vztahu k předmětu veřejné zakázky vyplývají ze ZKB a jeho prováděcích předpisů, resp. k té části předmětu veřejné zakázky, která má povahu hardware a/nebo software, tj. technických a/nebo programových prostředků (taková část předmětu veřejné zakázky dále též souhrnně jen „**nabízené řešení**“).

Pojmy užité v těchto zadávacích podmínkách se vykládají dle ZKB, případně, neobsahuje-li ZKB jejich definici, pak se vykládají podle těchto zadávacích podmínek.

Požadavky zadavatele ve vztahu k rizikovým technologiím

Zadavatel stanovil maximální přípustnou úroveň rizika spojeného s narušením důvěrnosti, integrity nebo dostupnosti, tj. kybernetické bezpečnosti, každé jednotlivé součásti nabízeného řešení **na úroveň nízká** na škále uvedené v příslušné příloze vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti (dále jen „**maximální přípustná hodnota rizika**“ a „**VKB**“). Pro stanovení úrovní zranitelnosti, aktiv, hrozeb, dopadů, rizik, důvěrnosti, integrity, dostupnosti, případně dalších veličin použitých při hodnocení rizik dle této zadávací dokumentace jsou použity škály uvedené v přílohách VKB. Pro účastníka zadávacího řízení je použití těchto škál při zpracování nabídky povinné[1]. Pro účastníka zadávacího řízení je dále povinné při zpracování nabídky použít funkci, resp. vzorec pro výpočet hodnoty rizika uvedený v přílohách VKB[2].

Osobní údaje v nabízeném řešení zpracovávané[3], tj. rovněž údaje o zdravotním stavu pacientů zadavatele, včetně dalších uživatelských dat, považuje zadavatel za primární aktiva (tato uživatelská dále jen „**data**“ nebo „**uživatelská data**“). Tato primární aktiva zadavatel ohodnotil na škálách uvedených ve VKB takto:

- důvěrnost: **vysoká**,
- integrita: **kritická**,
- dostupnost: **střední**.

Služby poskytované nabízeným řešením považuje zadavatel za primární aktiva (tyto služby dále jen „**služby**“; data a služby dále souhrnně též pouze „**primární aktiva**“). Tato primární aktiva zadavatel ohodnotil na škálách uvedených ve VKB takto:

- důvěrnost: **střední**,
- integrita: **kritická**,
- dostupnost: **střední**.

[1] A to i v případě, že v je ve VKB použití určité škály označeno jen jako doporučené nebo jen jako příklad.
[2] A to i v případě, že v je ve VKB použití tohoto vzorce označeno jen jako doporučené nebo jen jako příklad.
[3] Pojmy „osobní údaje“ a „zpracování osobních údajů“ se vykládají podle nařízení Evropského parlamentu a Rady (EU) ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů).

Systémová data nezbytná pro řádné a bezpečné fungování nabízeného řešení považuje zadavatel za technická aktiva (dále jen „**systémová data**“; systémová data, uživatelská data a služby dále souhrnně jen „**aktiva**“). Tato technická aktiva zadavatel ohodnotil na škálách uvedených ve VKB takto:

- důvěrnost: **střední**,
- integrita: **kritická**,
- dostupnost: **střední**.

Zadavatel je povinen v zadávacím řízení zohlednit následující akty Národního úřadu pro kybernetickou a informační bezpečnost vztahující se k určitým technickým a/nebo programovým prostředkům (dále jen „**NÚKIB**“; technické a programové prostředky, ke kterým se tyto akty vztahují, resp. veškeré výrobky výrobců v těchto aktech stanovených, dále jen „**rizikové prostředky**“):

- varování NÚKIB ze dne 17. 12. 2018, sp. zn. 110-536/2018, č. j. 3012/2018-NÚKIB-E/110; a
- varování NÚKIB ze dne 10. 7. 2025, sp. zn. 350-544/2025-E, č. j. 4417/2025-NÚKIB-E/350 (veškeré tyto akty dále souhrnně jen „**varování NÚKIB**“).

Zadavatel je povinen v zadávacím řízení zohlednit rovněž následující akty NÚKIB vztahující se k určitým chováním technických a/nebo programových prostředků (technické a programové prostředky dále souhrnně též pouze „**systémy**“), které stanovují jako hrozbu vymezená chování vyplývající z vlastností umožňujících narušení kybernetické bezpečnosti technických a/nebo programových prostředků (tyto vlastnosti dále jen „**backdoor**“):

- varování NÚKIB ze dne 3. 9. 2025, sp. zn. 350-647/2025-E, č. j. 6159/2025-NÚKIB-E/350.

Zadavatel považuje, rovněž s ohledem na uvedené akty NÚKIB, následující státy za rizikové (dále jen „**rizikové státy**“):

- Čínská lidová republika včetně zvláštních administrativních oblastí.

Zadavatel je však povinen stanovit rizika spojená s narušením kybernetické bezpečnosti primárních aktiv **ve vztahu ke všem systémům** tvořícím předmět veřejné zakázky a ve vztahu ke všem chováním těchto systémů narušujících kybernetickou bezpečnost nabízeného řešení, a to bez ohledu na to, zda tyto systémy nebo tato chování spadají do působnosti výše uvedených aktů NÚKIB. Zadavatel proto pojem „backdoor“ pro účely této zadávací dokumentace vymezuje, vedle vymezení vyplývajících z výše uvedených aktů NÚKIB, jako vlastnost systému, která:

- umožňuje předávat uživatelská a/nebo systémová data do rizikových států nebo subjektům tam usídleným;
- umožňuje provádět vzdálenou správu technických aktiv vykonávanou z rizikových států nebo ze strany subjektů tam usídlených;
- umožňuje osobám odlišným od zadavatele vzdáleně narušovat kybernetickou bezpečnost aktiv[4];
- spočívá v tom, že systém narušuje kybernetickou bezpečnost aktiv automaticky;
- spočívá v tom, že systém umožňuje akceptovat povely osoby odlišné od zadavatele.

[4] Např. tento systém umožňuje provádění neoprávněného zpracování osobních údajů, neoprávněnou vzdálenou správu technických aktiv, neoprávněné odesílání i jen části osobních údajů nebo systémových dat mimo nabízené řešení, neoprávněné změny osobních údajů nebo systémových dat, neoprávněné omezování dostupnosti služby.

Avšak chování systémů, které je výslovně stanoveno zadávací dokumentací nebo je výslovně sjednáno ve smlouvě na veřejnou zakázku, nebo které je zjevně nezbytné k plnění této smlouvy nebo právních předpisů platných v České republice, se nepovažuje za narušení kybernetické bezpečnosti, ledaže ze správních aktů NÚKIB vyplývá, že je hrozbou.

Za samostatný systém tvořící nabízené řešení pro účely hodnocení rizik podle těchto požadavků zadavatele v oblasti kybernetické bezpečnosti, se považuje každá ucelená část nabízeného řešení, která se samostatně, tj. odděleně od ostatních takových částí, připojuje do datové sítě, tj. je samostatným síťovým zařízením.

Zadavatel pro účely hodnocení rizik v souvislosti s hrozbou spočívající v přítomnosti backdoor v systémech, které jsou součástí předmětu veřejné zakázky, rozlišuje následující případy:

a) případ, kdy výrobce takového systému má sídlo v rizikovém státě;
b) případ, kdy výrobce systému nemá sídlo v rizikovém státě, ale obsahuje digitální komponenty[5], jejichž výrobce má sídlo v rizikovém státě;
c) případ, kdy výrobce systému nemá sídlo v rizikovém státě, ani neobsahuje digitální komponenty, jejichž výrobce má sídlo v rizikovém státě.

Povinné hodnoty a podmínky povinně vstupující do hodnocení rizik jsou s ohledem na skutečnost, že zadavatel je mimo své postavení dle ZKB významným poskytovatelem zdravotních služeb, stanoveny takto:

- zneužití rizikového prostředku v nabízeném řešení znamená hrozbu v úrovni vyplývající ze správního aktu NÚKIB, nebo, nevyplývá-li úroveň takové hrozby z žádného správního aktu NÚKIB, v úrovni: **kritická**;
- zneužití backdoor v systému obsaženém v nabízeném řešení znamená hrozbu v úrovni vyplývající ze správního aktu NÚKIB, nebo, nevyplývá-li úroveň takové hrozby z žádného správního aktu NÚKIB, v úrovni: **nízká**;
- přítomnost každého rizikového prostředku v nabízeném řešení znamená zranitelnost v úrovni dle následující tabulky:

Správní akt NÚKIB ze dne	**Stručné vymezení rizikových prostředků**	**Úroveň zranitelnosti**
17. 12. 2018	Huawei, ZTE	Kritická
10. 7. 2025	DeepSeek	Kritická

- přítomnost následujících systémů, mimo jiné s ohledem na uvedené správní akty NÚKIB, v nabízeném řešení znamená zranitelnost v úrovni dle následující tabulky:

Správní akt NÚKIB ze dne; tyto úrovně zranitelnosti se však použijí na všechny systémy zahrnuté v nabízeném řešení bez ohledu na to, zda jsou uvedeny ve správním aktu NÚKIB	**Druh systému**	**Úroveň zranitelnosti**
3. 9. 2025	Systémy, jejichž výrobce má sídlo v rizikovém státě	Kritická
3. 9. 2025	Systém, jehož výrobce nemá sídlo v rizikovém státě, ale	Střední

[5] Digitální komponentou se rozumí rovněž programové vybavení (software) včetně middleware, firmware aj.

	obsahuje digitální komponenty, jejichž výrobce má sídlo v rizikovém státě	
3. 9. 2025	Systém, jehož výrobce nemá sídlo v rizikovém státě, ani neobsahuje digitální komponenty, jejichž výrobce má sídlo v rizikovém státě	Nízká

Není-li některá hodnota vstupující do hodnocení rizik výše stanovena ani z výše uvedeného nevyplývá, resp. ji pouze základě výše uvedeného nelze určit, určí ji účastník zadávacího řízení podle skutečnosti, přičemž určení takové hodnoty uvede a řádně a přezkoumatelně odůvodní ve zprávě o hodnocení rizik.

Tyto podmínky stanoví dvě možnosti, jak splnit výše uvedené požadavky zadavatele týkající se rizikových prostředků:

- **buď provedením hodnocení rizik, nebo**
- **čestným prohlášením, že nabízené řešení žádný rizikový prostředek neobsahuje.**

Tyto podmínky stanoví dvě možnosti, jak splnit výše uvedené požadavky zadavatele týkající se backdoor v případě, že výrobce žádného systému obsaženého v nabízeném řešení nemá sídlo v rizikovém státě, ani neobsahuje digitální komponenty, jejichž výrobce má sídlo v rizikovém státě:

- **buď provedením hodnocení rizik, nebo**
- **čestným prohlášením, že nabízené řešení žádný backdoor neobsahuje.**

Pokud má výrobce kteréhokoli systému obsaženého v nabízeném řešení sídlo v rizikovém státě nebo pokud kterýkoli systém obsažený v nabízeném řešení obsahuje digitální komponenty, jejichž výrobce má sídlo v rizikovém státě, musí účastník zadávacího řízení provést hodnocení rizik vždy.

Hodnocení rizik

Zadavatel požaduje, aby účastník zadávacího řízení ve vztahu ke všem výskytům rizikových prostředků v nabízeném řešení[6], ve vztahu ke všem hrozbám definovaným správními akty NÚKIB a ve vztahu ke všem backdoor v systémech tvořících nabízené řešení[7] **provedl hodnocení rizik** ve smyslu § 2 písm. d) VKB, a to postupy a s využitím škál dle příloh VKB, přičemž i to, co je v těchto přílohách VKB uvedeno jako pouhé doporučení nebo jako pouhý příklad, je pro účastníky tohoto zadávacího řízení povinné (toto hodnocení rizik dále jen „**hodnocení rizik**“).

Zadavatel proto požaduje, aby součástí nabídky byla podrobná a přezkoumatelná zpráva o provedení hodnocení rizik spojených s využitím rizikových prostředků v předmětu veřejné zakázky, s hrozbami definovanými správními akty NÚKIB a s výskytem backdoor v nabízeném

[6] V případě, že nabízené řešení má povahu služby nebo jiného plnění, které není dodávkou technických ani programových prostředků (resp. v rozsahu, ve kterém je takové plnění je součástí nabízeného řešení), rozumí se výskytem rizikového prostředku v nabízeném řešení využívání rizikového prostředku pro poskytování takové služby, resp. plnění.

[7] V případě, že nabízené řešení má povahu služby nebo jiného plnění, které není dodávkou technických ani programových prostředků (resp. v rozsahu, ve kterém je takové plnění je součástí nabízeného řešení), rozumí se výskytem backdoor v nabízeném řešení využívání technického nebo programového prostředku, který má backdoor, pro poskytování takové služby, resp. plnění.

řešení, která zadavateli umožní ve všech nezbytných detailech ověřit řádnost provedení tohoto hodnocení rizik a která bude mít minimálně následující náležitosti (dále a výše jen „**zpráva o hodnocení rizik**“):

- schéma, ze kterého vyplyne, z jakých systémů ve smyslu výše uvedené definice systému, a jak síťově zapojených, se nabízené řešení skládá, ledaže je nabízené řešení tvořeno jediným takovým systémem (zpracovává-li účastník zadávacího řízení na základě jiných požadavků zadávací dokumentace blokové komunikační schéma, které požadavek podle této odrážky splní, postačí ve zprávě o hodnocení rizik na toto blokové komunikační schéma odkázat),
- podrobnou identifikaci všech rizikových prostředků vyskytujících se v nabízeném řešení, a to včetně obchodního názvu, typu nebo verze, roku výroby, výrobce a sídla výrobce (postačuje stát),
- podrobnou identifikaci všech backdoor vyskytujících se v nabízeném řešení,
- hodnoty vstupních parametrů, které nejsou zadány těmito požadavky zadavatele v oblasti kybernetické bezpečnosti ani správními akty NÚKIB,
- zdůvodnění volby hodnoty každého z těchto parametrů, které nejsou výslovně zadány touto zadávací dokumentací, a to mimo jiné s ohledem na roli jednotlivých systémů v nabízeném řešení,
- ve vztahu ke všem rizikovým prostředkům, hrozbám uvedeným ve správních aktech NÚKIB a backdoor určení výsledné hodnoty rizik, a
- podrobný popis technických bezpečnostních opatření za účelem trvalého snížení hodnot zjištěných rizik na úroveň maximální přípustné hodnoty rizika nebo na nižší úroveň (dále jen „**bezpečnostní opatření**“)[8], a to včetně řádného zdůvodnění účinnosti těchto bezpečnostních opatření, přičemž (**zpráva o hodnocení rizik bude obsahovat výslovné prohlášení o splnění následujících odrážek**):
    - tato bezpečnostní opatření nesmí vyžadovat vyšší složitost obsluhy nabízeného řešení, než jaká by byla v případě, kdyby nabízené řešení neobsahovalo žádný rizikový prostředek ani žádný backdoor,
    - tato bezpečnostní opatření nesmí zvyšovat požadavky na personální zajištění obsluhy nabízeného řešení, a
    - nabízené řešení včetně těchto bezpečnostních opatření musí jako celek splňovat veškeré požadavky zadavatele.

V případě, že bude dle zprávy o hodnocení rizik hodnota rizika ve vztahu ke kterémukoli systému vyšší než maximální přípustná hodnota rizika, **požaduje zadavatel, aby součástí nabízeného řešení byla výše uvedená technická bezpečnostní opatření, která hodnotu rizik zjištěných při hodnocení rizik sníží** na úroveň maximální přípustné hodnoty rizika nebo na nižší úroveň.

Veškeré náklady na tato technická bezpečnostní opatření, včetně nákladů na jejich provoz a na udržování jejich účinnosti a úrovně kybernetické bezpečnosti po celou dobu trvání smlouvy, musí být součástí nabídkové ceny, což účastník zadávacího řízení ve vhodné a přezkoumatelné formě uvede ve své nabídce.

Neúplnost, nesprávnost nebo nepřezkoumatelnost zprávy o hodnocení rizik, případně jiné její nedostatky, **může být důvodem pro vyloučení účastníka zadávacího řízení z další účasti v zadávacím řízení.**

[8] Pouze u rizik, jejichž zjištěná hodnota přesahuje úroveň maximální přípustné hodnoty rizika.

Pokud bude dle zprávy o hodnocení rizik hodnota kteréhokoli rizika zjištěného při hodnocení rizik i po aplikaci bezpečnostních opatření vyšší než maximální přípustná hodnota rizika, nesplní nabídka účastníka zadávacího řízení zadávací podmínky. Zadavatel je v takovém případě **oprávněn účastníka zadávacího řízení vyloučit z další účasti v zadávacím řízení**.

Možnost čestného prohlášení

Za výše uvedených podmínek může účastník zadávacího řízení namísto provedení hodnocení rizik učinit v nabídce na veřejnou zakázku čestné prohlášení.

Zadavatel však upozorňuje, že v případě, že po uzavření smlouvy vyjde najevo, že toto čestné prohlášení neodpovídá skutečnosti, bude oprávněn odstoupit od smlouvy. Současně zadavatel v této souvislosti upozorňuje, že bude provádět testování (skenování) nabízeného řešení za účelem zjištění jeho kybernetických bezpečnostních zranitelností, které bude popisovat pomocí údajů z databáze CVE (Common Vulnerabilities and Exposures; dostupná z https://cve.mitre.org/), případně jiným vhodným způsobem.

Další požadavky zadavatele v oblasti kybernetické bezpečnosti

Za účelem trvalého udržování vysoké úrovně kybernetické bezpečnosti předmětu veřejné zakázky zadavatel požaduje, aby dodavatel:

- po celou dobu plnění smlouvy prováděl pravidelná technická a bezpečnostní školení osob na jeho straně **přímo** se podílejících na plnění smlouvy;
- po celou dobu plnění smlouvy dokumentoval změny přístupových oprávnění, které bude na své straně provádět;
- určil a průběžně aktualizoval havarijní kontaktní údaje pro zvládání kybernetických bezpečnostních událostí a incidentů, které bez zbytečného odkladu po nabytí účinnosti smlouvy poskytne zadavateli, a bude zadavateli oznamovat jakoukoliv jejich změnu bez zbytečného odkladu;
- poskytoval zadavateli součinnost při testování havarijního plánu vztahujícího se k předmětu veřejné zakázky, jakož i součinnost při provádění bezpečnostních, penetračních testů a testování zranitelností předmětu veřejné zakázky;
- při plnění předmětu veřejné zakázky využíval napojení na jednotnou adresářovou službu provozovanou na technologii Microsoft Active Directory zadavatele;
- využíval pro správu organizační struktury napojení na modul Identity Managementu informačního systému Enterprise Service Bus zadavatele;
- poskytovat součinnost při identifikaci a vyhodnocování potenciálních kybernetických bezpečnostních událostí v předmětu veřejné zakázky;
- zadavatel za účelem naplnění § 22 VKB provozuje systém log managementu systém TeskaLabs Logman.io; dodavatel poskytne veškerou nezbytnou součinnost pro napojení předmětu veřejné zakázky na tento systém log managementu tak, aby zadavatel rovněž ve vztahu k předmětu veřejné zakázky mohl plnit ustanovení § 22 VKB;
- za účelem naplnění § 18 VKB poskytne dodavatel zadavateli:
    - kompletní komunikační schéma předmětu veřejné zakázky v rozsahu a míře detailu nezbytných pro jeho zapojení do síťové infrastruktury zadavatele za podmínek vysoké úrovně kybernetické bezpečnosti, a
    - veškerou nezbytnou součinnost pro řádnou konfiguraci systému pokročilých síťových analýz zadavatele GreyCortex Mendel.