Vysvětlení a doplnění zadávací dokumentace č. 2

Dotaz č 1: Zadávací dokumentace dělí zakázku na dvě samostatné části, přičemž první část zahrnuje Asset Management, ServiceDesk, IPAM a Risk Asset Management, zatímco druhá část zahrnuje firewall, NAC, IDM, SIEM, PAM, MFA/SSO, WAF/LB a PKI. Tyto systémy jsou vzájemně úzce provázané a vyžadují integraci (např. IPAM s NAC a firewallem, Asset Management se SIEM, ServiceDesk s IDM/PAM). Jakým způsobem bude zadavatel zajišťovat technickou integraci mezi oběma částmi zakázky v případě, že vyhrají dva různí dodavatelé? Kdo ponese odpovědnost za celkovou funkčnost integrovaného řešení a za řešení integračních problémů mezi oběma částmi?

Odpověď zadavatele na dotaz č. 1: Každý dodavatel ponese odpovědnost za bezchybnou funkčnost a integritu své části dodávky v rozsahu stanoveném smlouvou. Vzhledem ke komplexnosti a provázanosti systémů bude architektura definována především v rámci části *„Kybernetická bezpečnost“*, přičemž dodavatel části *„Asset Management“* bude povinen zajistit kompatibilitu svého řešení s rozhraními a standardy stanovenými touto architekturou.Zadavatel zároveň doporučuje, aby se návrhové fáze integrace účastnili zástupci obou dodavatelů, čímž se předejde duplicitám a rizikům nesouladu.

Dotaz č 2: Požaduje zadavatel předložení celkového technického architektonického návrhu zahrnujícího všechna opatření z obou částí zakázky? Pokud ano, má tuto povinnost pouze dodavatel části 2, dodavatel části 1, oba dodavatelé samostatně, nebo se předpokládá společný návrh? Pokud ne, jak bude zajištěna konzistence celkové IT architektury kybernetické bezpečnosti nemocnice?

Odpověď zadavatele na dotaz č. 2: Zadavatel požaduje, aby byla architektura každé části zpracována samostatně, avšak v souladu s koncepčním rámcem a architektonickými zásadami kybernetické bezpečnosti nemocnice. Primární architektonický návrh bude tvořen v rámci části *„Kybernetická bezpečnost“.* Návrh části *„Asset Management“* musí být následně přizpůsoben této hlavní architektuře. Tím bude zajištěna konzistence a provázanost celkové IT architektury bez nutnosti předkládat jednotný návrh od všech dodavatelů.

Dotaz č 3: V případě, že zakázku realizují dva různí dodavatelé, mohou nastat situace, kdy nebude jednoznačné, který dodavatel odpovídá za vzniklý problém (např. nefunkční synchronizace dat mezi Asset Managementem a SIEM, problémy s automatizací v ServiceDesk kvůli integraci s IDM). Jak bude zadavatel řešit situace, kdy oba dodavatelé budou tvrdit, že problém je na straně druhého dodavatele? Kdo bude finálním arbitrem při určování odpovědnosti?

Odpověď zadavatele na dotaz č. 4: V případě sporných situací bude finálním arbitrem při určování odpovědnosti za vzniklý problém určený architekt a manažer kybernetické bezpečnosti Jihomoravské zdravotní, a.s. Tento subjekt disponuje odbornou způsobilostí i mandátem k rozhodování v oblasti kybernetické bezpečnosti v rámci krajského zdravotnictví a zajistí objektivní a nestranné posouzení. Rozhodnutí tohoto orgánu bude pro oba dodavatele závazné.

Dotaz č. 5: První část má termín realizace max. 90 dnů, druhá část do 31.3.2026. V případě dvou různých dodavatelů bude třeba koordinovat implementaci (přístup do sítě, instalaci agentů, konfiguraci AD, sdílení dokumentace). Kdo bude odpovědný za celkovou koordinaci obou projektů a řešení konfliktu priorit při společných aktivitách? Bude na straně zadavatele jmenován jeden hlavní projektový manažer odpovědný za celou zakázku (obě části)?

Odpověď zadavatele na dotaz č. 5 Zadavatel se s názorem tazatele ztotožňuje a je očekáváno, že vítězný účastník druhé části bude zapojen do zahájení obou části veřejné zakázky. K samotné

výzvě k zahájení činnosti dle uzavřené smlouvy dojde až ve vhodný termín, který bude předběžně stanoven v rámci uvodního setkání s oběma účastníky

Dotaz č. 6: První část zahrnuje ServiceDesk a procesy ITIL, druhá část zahrnuje technické nástroje, které tyto procesy podporují (IDM, PAM, SIEM). Kdo bude odpovědný za návrh a implementaci end-to-end procesů, které zasahují do obou částí zakázky (např. proces onboardingu zaměstnance zahrnuje ServiceDesk z části 1 i IDM z části 2)? Pokud vyhrají dva dodavatelé, bude každý navrhovat procesy pouze pro svou část, nebo se očekává společný procesní návrh?

Odpověď zadavatele na dotaz č. 6: Návrh procesů bude vycházet z architektury a procesních standardů definovaných v části *„Kybernetická bezpečnost“*. Dodavatel části *„Asset Management“* zajistí, že jeho řešení a procesy budou s těmito standardy v plném souladu. Zadavatel doporučuje, aby se zástupci obou dodavatelů účastnili společných konzultací při návrhu klíčových procesů (např. onboarding, správa oprávnění), čímž se zajistí jejich efektivní propojení a využití funkcionalit obou systémů.

Dotaz č. 7: Bude zadavatel při hodnocení nabídek zohledňovat výhody komplexního řešení od jednoho dodavatele (jedna architektura, jednotná odpovědnost, jednodušší integrace) oproti řešení od dvou dodavatelů? Pokud ano, jakým způsobem bude tato výhoda ohodnocena, když jediným hodnotícím kritériem je nabídková cena bez DPH? Budou nabídky na obě části od jednoho dodavatele hodnoceny samostatně, nebo bude hodnocena i celková ekonomická výhodnost komplexního řešení?

Odpověď zadavatele na dotaz č. 7: Zadavatel nebude při hodnocení nabídek zohledňovat případné výhody komplexního řešení od jednoho dodavatele. Jednotlivé části zakázky budou hodnoceny samostatně v souladu s definovanými hodnoticími kritérii.Tento přístup zajišťuje rovné podmínky pro všechny účastníky a odpovídá záměru rozdělit zakázku na samostatné, na sobě nezávislé části.

Dotaz č. 8: V případě dvou různých dodavatelů, jak bude zajištěna podpora pro integrované funkcionality, které zasahují do obou částí? Kdo bude řešit incidenty, kde příčina může být v jedné části, ale projev v druhé (např. selhání automatizace v ServiceDesk kvůli problému v IDM)? Bude zadavatel vyžadovat společné SLA dokumenty nebo eskalační procedury mezi oběma dodavateli?

Odpověď zadavatele na dotaz č. 8: Incidenty a servisní zásahy budou řešeny podle odpovědnosti vyplývající ze smluvního vztahu – tj. dodavatel odpovídá za závady v rozsahu své dodávky.V případech, kdy nelze jednoznačně určit příčinu incidentu, bude rozhodnutí o rozdělení odpovědnosti a případných nákladů učiněno architektem kybernetické bezpečnosti Jihomoravské zdravotní, a.s. Zadavatel doporučuje, aby mezi dodavateli vznikla minimální dohoda o součinnosti v rámci SLA (zejména o komunikačních postupech, eskalacích a termínech řešení incidentů zasahujících do obou částí).

Dotaz č. 9: Jak bude zajištěn budoucí rozvoj řešení, pokud bude vyžadovat změny v obou částech zakázky současně? Budou oba dodavatelé povinni konzultovat a koordinovat své změny s druhým dodavatelem? Kdo ponese náklady na integrační práce při budoucích rozšířeních nebo změnách, které budou vyžadovat úpravy v obou částech?

Odpověď zadavatele na dotaz č. 9: Budoucí rozvoj řešení bude probíhat ve spolupráci obou dodavatelů pod koordinací manažera kybernetické bezpečnosti nemocnice.Pokud půjde o nové požadavky zadavatele nebo rozšíření nad rámec původního projektu, budou integrační práce hrazeny zadavatelem.V případě legislativních nebo bezpečnostních změn budou dodavatelé

povinni provést nezbytné úpravy v souladu se smlouvou; hrazeny budou pouze případné implementační práce na straně zadavatele. Zadavatel si vyhrazuje právo schvalovat ve spolupráci s architektem kybernetické bezpečnosti kraje všechny zásahy do architektury tak, aby byla zachována její celistvost a bezpečnostní konzistence.

Dotaz č.10: Trváte na zachování stávající kombinace požadavků, anebo připouštíte nabídku technicky a funkčně ekvivalentní platformy od jiného výrobce, která obecně splní požadované parametry a účel projektu, ale využívá odlišná dílčí řešení, která s ohledem na různé technologie a architekturu jednotlivých výrobců nemusí odpovídat všem uvedeným minimálním požadavkům, nicméně požadavky daného projektu tato platforma celkově splní na stejné nebo vyšší bezpečnostní a výkonové úrovni.

Odpověď zadavatele na dotaz č. 10: Zadavatel uvádí, že technická specifikace byla vytvořena tak, aby odpovídala dlouhodobé bezpečnostní strategii organizace, požadované míře integrace jednotlivých bezpečnostních prvků a provozním podmínkám nemocniční infrastruktury. Z tohoto důvodu jsou některé požadavky definovány podrobněji – jejich cílem je zajistit dosažení požadované úrovně kybernetické bezpečnosti, nikoli zvýhodnit konkrétní řešení nebo výrobce.

Současně potvrzujeme, že zadavatel připouští nabídku technicky a funkčně ekvivalentní platformy jiného výrobce. Takové řešení však musí být prokazatelně a plnohodnotně kompatibilní s požadovanou architekturou projektu jako celku, a to zejména z hlediska:
- jednotného řízení bezpečnostních politik,
- integrace mezi jednotlivými komponentami,
- provozní spolehlivosti v prostředí nemocnice,
- kapacitních a výkonnostních parametrů,
- celkového dopadu na správu, dohled a incident management.

Posouzení ekvivalence bude provedeno komplexně, nikoli pouze podle jednotlivých samostatných funkcí. Ekvivalentní nabídka bude považována za přípustnou tehdy, pokud uchazeč jednoznačně doloží, že jeho řešení zajišťuje stejnou nebo vyšší úroveň bezpečnosti, integrace a funkční celistvosti bez negativního dopadu na provozní řízení či správu prostředí nemocnice. V případě, že tyto podmínky nebudou splněny, nebude možné nabídku považovat za ekvivalentní.

Dotaz č.11 V zadávací dokumentaci není jasně uveden požadavek na redundanci technologie WAF. Z povahy celkového poptávaného řešení předpokládáme, že navržené řešení WAF musí být redundantní. Je tento předpoklad správný?

Odpověď zadavatele na dotaz č. 11: V ideálním případě by bylo výborné mít WAF redundantně. V této zakázce to však není podmínkou z finančních důvodů.Důležité však je, aby se s případným dokoupením v budoucnu počítalo již při přípravě návrhu řešení.

Dotaz č. 12: V zadávací dokumentaci není jasně uveden požadavek na redundanci technologie NGFW č.1, ale pouze na NGFW č.2. Poptávané vlastnosti i celková povaha poptávaného řešení k tomuto ale vedou. Předpokládáme, že se jedná o nepřesnou formulaci a zadavatel požaduje redundantní řešení u technologie NGFW č.1 i NGFW č.2. Je tento předpoklad správný?

Odpověď zadavatele na dotaz č. 12 Firewall je potřeba mít redundantně.

Dotaz č. 13 První část má termín realizace max. 90 dnů, druhá část do 31.3.2026. V případě dvou různých dodavatelů bude třeba koordinovat implementaci (přístup do sítě, instalaci

agentů, konfiguraci AD, sdílení dokumentace). Kdo bude odpovědný za celkovou koordinaci obou projektů a řešení konfliktu priorit při společných aktivitách? Bude na straně zadavatele jmenován jeden hlavní projektový manažer odpovědný za celou zakázku (obě části)?

Odpověď zadavatele na dotaz č. 13

Je očekáváno, že vítězný účastník druhé části bude zapojen do zahájení obou části veřejné zakázky. K samotné výzvě k zahájení činnosti dle uzavřené smlouvy dojde až ve vhodný termín, který bude předběžně stanoven v rámci úvodního setkání s oběma účastníky. Zadavatel disponuje zkušeným týmem, který bude jednotlivé případné části zadávacího řízení řídit.

Zadavatel nevnímá výše uvedené vysvětlení ZD jako změnu zadávacích podmínek, která by rozšiřovala okruh jednotlivých účastníků a z toho důvodu prodlužuje lhůtu pro podání nabídek přiměřeně i ve vazbě na vysvětlení ZD č.1

Lhůta pro podání nabídek je tímto prodloužena do 1.12.2025 10:00 Hod