NEMOCNICE BŘECLAV, příspěvková organizace
U Nemocnice 3066/1, 690 02 Břeclav
telefon: +420 519 315 111, fax +420 519 372 112, www.nembv.cz
IČO: 00 390 780, DIČ: CZ00390780, zapsaná v obchodním rejstříku vedeném u Krajského soudu v Brně, pod sp. zn. Pr. 1233

Č.j.: 66/SŘ/2026 V Břeclavi dne 16. 2. 2026

Vysvětlení zadávací dokumentace č. 7

Název zakázky:
„Kybernetická bezpečnost Nemocnice Břeclav“

Údaje o zadavateli:

Název: Nemocnice Břeclav, příspěvková organizace
Právní forma: Příspěvková organizace
Sídlo: U Nemocnice 3066/1, 690 02 Břeclav
IČO: 003 90 780
DIČ: CZ00390780
Zastoupen: Ing. Petr Baťka, ředitel
Kontaktní osoba: Ing. Michal Ragan, MBA
Tel: 606711237
E-mail: ragan@nembv.cz

(dále jen ***„zadavatel“***)

I.

Dne 12. 2. 2026 byla zadavateli doručena žádost o vysvětlení zadávací dokumentace k výše uvedené veřejné zakázce (dále jen ***„Dotaz“***). Žádost byla doručena včas a zadavatel tak sděluje následující:

Dotazy:

Realizace perimetrového a centrálních firewallů

Dotaz č. 23:

Skrytý odkaz na konkrétního výrobce (Hardwarový Lock)

„Zadavatel v technické specifikaci v části 'Obecné minimální požadavky na NGFW' stanovil striktní požadavek na fyzické rozhraní zařízení: 16x GE RJ 45, 8x GE SFP a 4x 10 GE SFP+, a to vše v šasi o velikosti 1 RU.

Tato specifická kombinace portů je unikátní technickou vlastností jediného konkrétního modelu od výrobce Fortinet (modelová řada 200F). U jiných předních světových výrobců bezpečnostních technologií je tato portová hustota řešena buď modulárně, nebo v souladu s moderní architekturou 'Spine-Leaf' oddělením bezpečnostní vrstvy (NGFW) a přístupové vrstvy (Switch).

Dle ZZVZ nesmí technické podmínky obsahovat přímý nebo nepřímý odkaz na určité dodavatele nebo výrobky, pokud to není odůvodněno předmětem veřejné zakázky. Trvání na této specifické hardwarové konfiguraci bez připuštění ekvivalentního řešení (např. kombinace NGFW + L2 Switch) je bezdůvodným omezením hospodářské soutěže, neboť technicky neexistuje důvod, proč by firewall musel fungovat jako access switch s 28 porty.

Žádáme zadavatele o potvrzení, že v souladu s ZZVZ (zásada zákazu diskriminace) bude akceptovat jako splnění technické kvalifikace i řešení, které zajistí požadovanou konektivitu a počet portů pomocí kombinace vysoce výkonného NGFW a kompatibilního L2 přepínače (switche) zahrnutého v ceně dodávky, při zachování všech ostatních bezpečnostních a výkonnostních parametrů?“

Dotaz č. 24:

Metodika testování (Útok na ASIC vs. CPU)

„Zadavatel si vyhrazuje právo testovat shodu parametrů mimo jiné testem 'UDP PPS' a 'propustnost UDP/64B'. Upozorňujeme zadavatele, že tato metodika syntetického testování, zaměřená na zpracování paketů na nízkoúrovňové vrstvě (packet forwarding), zvýhodňuje konkrétní hardwarovou architekturu založenou na ASIC čipech, avšak je zcela irelevantní pro posouzení bezpečnostního výkonu NGFW v prostředí nemocnice.

Reálný provoz moderní nemocniční sítě je tvořen převážně šifrovaným provozem na aplikační vrstvě (HTTPS, DICOM, HL7), nikoliv záplavou malých UDP paketů (charakteristické spíše pro DDoS útoky, které mají být řešeny na úrovni ISP, nikoliv perimetrového firewallu). Testování UDP PPS nevypovídá nic o schopnosti zařízení provádět inspekci malwaru, IPS či dešifrování SSL, což jsou klíčové požadavky této zakázky.

Zadavatel se tímto dotazuje, zda bude při případném ověřování parametrů akceptovat (nebo preferovat) metodiku měření na reálném aplikačním provozu (HTTP/HTTPS mix), která prokazatelněji ověřuje schopnost zařízení chránit infrastrukturu před kybernetickými hrozbami (Threat Prevention), a upustí od diskriminačního požadavku na UDP PPS hodnoty, které nemají souvislost s požadovanou funkcí NGFW?“

Dotaz č. 25:

Doba podpory

„V zadávací dokumentaci existuje zásadní rozpor v požadavcích na délku podpory. Bod [5] vyžaduje aktualizaci reputačních a jiných databází 'po dobu minimálně 5-ti let', zatímco bod [7] požaduje podporu výrobce a aktualizace bezpečnostních funkcí 'po dobu minimálně 2 let'.

Tento rozpor znemožňuje stanovení srovnatelné nabídkové ceny, neboť náklady na bezpečnostní subskripce (NGTX/ATP) a HW support na 3 roky navíc tvoří významnou část ceny plnění. Ponechání této nejasnosti by mohlo vést ke spekulativnímu nacenění pouze kratšího období některými uchazeči, což by narušilo transparentnost řízení.

Zadavatel se táže: Požaduje zadavatel závazně nacenit kompletní bezpečnostní licence (IPS, Antivirus, Sandbox, Application Control, URL Filtering) a plnou podporu výrobce (HW replacement, software updates) na celou dobu 5 let (60 měsíců) tak, aby zařízení bylo po celou tuto dobu plně funkční a chráněné bez dalších investic?“

Dotazy k smluvním podmínkám dle Přílohy č. 5

Dotaz č. 26:

Příloha č. 5 - Smlouva o dodávce HW a SW a o poskytování souvisejících služeb, článek II. Předmět plnění, bod. č.1 – „Poskytovatel se zavazuje poskytnout objednateli plnění podrobně specifikované v přílohách č. 1 a č. 2 této Smlouvy spočívající v dodávce, instalaci a implementaci bezpečnostních technologií, HW a SW komponent včetně licencí, jakož i vzájemné funkční provázání těchto komponent a poskytnutí požadované servisní

podpory, včetně dalších činností (dále jen „Dodávka“). Poskytovatel odevzdá věci, které jsou předmětem Dodávky, a umožní objednateli nabýt vlastnické právo k nim.“

Dotaz: výše uvedený článek odkazuje na podrobně specifikované plnění v přílohách č.1 a č. 2. Ani jedna z uvedených příloh neobsahuje část, kde je možné prokázat splnění požadovaných parametrů. Jakým způsobem má být doložen fakt, že podmínky zadávací dokumentace byly splněny?

Dotaz č. 27:

Příloha č. 5 - Smlouva o dodávce HW a SW a o poskytování souvisejících služeb, článek III. Termíny a místo plnění, bod. č 1 – „Nevyplývá-li z této smlouvy výslovně jinak, je poskytovatel povinen provést Dodávku nejpozději do 250 kalendářních dnů od nabytí účinnosti této smlouvy, dle harmonogramu uvedeného v příloze č. 1“.

Dotaz: příloha č. 1 nedefinuje harmonogram plnění. Jaký je předpokládaný harmonogram plnění, jakým způsobem jsou definovány termíny plnění pro jednotlivé části předmětu plnění dle přílohy č. 2?

Dotazy k smluvním podmínkám dle Přílohy č. 3

Dotaz č. 28:

V Příloze č.3 zadávací dokumentace – Servisní služby je na straně 5 v kapitole Lhůty uvedena tato formulace: V případě, že se čeká na součinnost objednatele nebo tzv. třetí strany (např. dodavatele jiného HW) se běh lhůty přerušuje do doby zajištění součinnosti. Dotaz: Vztahuje se tato klausule i na přímou součinnost výrobce dotčené technologie v rámci výměny vadného hardware (RMA), případně součinnost jeho centra technické podpory (TAC)?

Realizace nástroje pro vysokou dostupnost aplikací

Dotaz č. 29:

Dotaz k bodu "Služba Web Application Firewall (WAF)" – Bezpečnostní rizika konsolidace

„Zadavatel v technické specifikaci požaduje, aby služba WAF byla *'provozována na zmíněných NGFW'*. Tento požadavek na konsolidaci kritických bezpečnostních vrstev (Perimetrový Firewall + Aplikační WAF) do jednoho hardwarového zařízení představuje v kontextu moderní kybernetické bezpečnosti nepřijatelné bezpečnostní riziko (Single Point of Failure).

Při vedení DDoS útoků na aplikační vrstvě (L7) nebo při náročné SSL inspekci dochází u 'All-in-One' řešení k vyčerpání systémových zdrojů (CPU/RAM) sdílených pro firewalling. To vede ke kolapsu síťové propustnosti i pro ostatní, neaplikační provoz organizace.

Dotaz: Trvá zadavatel na tomto technicky nebezpečném řešení, které snižuje odolnost infrastruktury, nebo bude v souladu se zásadou efektivního vynakládání prostředků akceptovat (a hodnotit jako rovnocenné či lepší) řešení architektury 'Defense-in-Depth', kde je WAF realizován jako dedikovaná hardwarová appliance oddělená od NGFW? Toto řešení prokazatelně eliminuje riziko výpadku firewallu při aplikačním útoku a je standardem pro vysokou dostupnost, kterou zadavatel názvem zakázky poptává.“

Dotaz č. 30:

Dotaz k bodu "Minimální počty požadovaných síťových rozhraní" – Bezdůvodné omezení soutěže

„Zadavatel v dokumentaci požaduje u zařízení NGFW přesnou kombinaci rozhraní: *16x GE RJ45, 8x GE SFP a 4x 10 GE SFP+* v šasi 1U. Tato specifická konfigurace je unikátním technickým otiskem produktu jediného výrobce na trhu a neodpovídá standardům Enterprise Security, kde firewall plní bezpečnostní funkci a není degradován do role přístupového switche s vysokým počtem legacy 1G portů.

Trváním na tomto specifickém počtu portů přímo na šasi firewallu zadavatel skrytě diskriminuje ostatní přední světové výrobce, kteří tuto 'switch' funkcionalitu řeší architektonicky čistěji.

Dotaz: Bude zadavatel akceptovat řešení, které splní či překročí požadovanou portovou kapacitu dodáním externího managovatelného switche (v ceně plnění), připojeného k NGFW vysokorychlostním linkem? Pokud zadavatel odpoví záporně, žádáme o technické zdůvodnění, proč je pro plnění veřejné zakázky nezbytné mít porty fyzicky na šasi firewallu, když funkčně je externí switch s firewallem ekvivalentní a servisně výhodnější řešení.“

Dotaz č. 31:

Dotaz k požadavku "Proxy-based inspekce" – Diskriminační terminologie

Znění dotazu: „Zadávací dokumentace opakovaně vyžaduje *'proxy-based inspekci'* jako podmínku pro aplikaci WAF profilů. Tento termín je specifickou marketingovou nomenklaturou operačního systému jednoho konkrétního výrobce a není průmyslovým standardem definujícím kvalitu ochrany.

Použití této terminologie bezdůvodně zvýhodňuje jednoho dodavatele a porušuje zásadu zákazu diskriminace.

Dotaz: Potvrdí zadavatel, že pro splnění kvalifikačních předpokladů postačuje, aby nabízené řešení zajišťovalo plnou inspekci obsahu (Deep Packet Inspection), terminaci SSL a ochranu proti webovým útokům, bez ohledu na to, zda technologie využívá marketingové označení 'proxy-based', nebo technicky přesnější termíny jako 'reverse-proxy' (standard u dedikovaných WAF) či 'stream-based' inspekce?“

LAN a WLAN

Dotaz č. 32:

Porušení zákazu uvádění konkrétních značek

"V dokumentaci (např. 'Tabulka rozmístění akt. prvků' a bod 'Jádro sítě') jsou explicitně uvedeny proprietární názvy modelů 'C9300-24UX' a 'C9300L-48P-4X'. Dle ZZVZ nesmí zadavatel zvýhodňovat určité výrobce, pokud to není odůvodněno předmětem zakázky. Žádáme o jednoznačné potvrzení, že tyto odkazy jsou pouze ilustrativní a zadavatel bude akceptovat technicky rovnocenné řešení jiného výrobce, které splní funkční požadavky, nikoliv přesnou kopii katalogového listu referenčního zařízení."

Dotaz č. 33:

Proprietární "Blue Beacon" (Vendor Lock)

"Zadavatel v technické specifikaci požaduje funkci 'Blue Beacon' pro identifikaci zařízení. Jedná se o marketingový název pro modrou LED diodu specifického výrobce (Cisco). Trvání na této specifické barvě a názvu je diskriminační. Potvrdí zadavatel, že pro splnění požadavku na fyzickou lokalizaci zařízení v rozvaděči postačuje standardní funkce 'Locator LED' (blikání systémové diody), kterou disponují všichni přední výrobci enterprise technologií?"

Dotaz č. 34:

Technologie stohování (Stacking)

"Zadavatel požaduje stohování 'speciálním stohovacím modulem' na zadní straně šasi. Tento požadavek kopíruje starší architekturu konkrétního výrobce (Cisco StackWise) a vylučuje moderní řešení využívající vysokorychlostní VIM moduly nebo dedikované QSFP/SFP28 porty na čelním panelu, které nabízejí stejnou nebo vyšší propustnost (např. 80-400 Gbps) a nižší latenci. Bude zadavatel akceptovat stohování pomocí vysokorychlostních portů, které zajistí požadovanou funkcionalitu jedné logické entity a redundanci, bez nutnosti použití proprietárních zadních kabelů?"

Dotaz č. 35:

WLAN Rádia (3+1 vs. 3+Sensor)

"Požadavek na 'Samostatné rádio pro monitorování' (3 klientská + 1 monitorovací rádio) je napsán na míru specifickému modelu AP. Moderní přístupové body využívají buď dedikovaný multi-funkční senzor, nebo softwarově definovaná rádia s adaptivním skenováním, která zajišťují WIPS a spektrální analýzu efektivněji a s nižší energetickou náročností. Akceptuje zadavatel řešení s

dedikovaným bezpečnostním senzorem nebo tri-radio AP s funkcí kontinuálního monitoringu, které splní bezpečnostní požadavky na detekci útoků a rušení?"

Dotaz č. 36:

Šifrovaný provoz (ETA)

"Požadavek na 'Application Visibility' v šifrovaném provozu odkazuje na technologii ETA (Encrypted Traffic Analytics). Žádáme o potvrzení, že zadavatel akceptuje i jiná technologická řešení založená na behaviorální analýze toků (NetFlow/IPFIX) a DPI (Deep Packet Inspection), která poskytnou srovnatelný přehled o aplikacích a hrozbách bez nutnosti dešifrování payloadu, což je v souladu s principy ochrany soukromí?"

NAC

Dotaz č. 37:

K protokolu SXP (Proprietární omezení)

Dotaz: V požadavcích zadavatel požaduje podporu protokolu SXP (Scalable Group Tag Exchange Protocol). Tento protokol je uzavřenou, proprietární technologií společnosti Cisco Systems. Dle § 89 odst. 5 zákona č. 134/2016 Sb. o zadávání veřejných zakázek nesmí technické podmínky odkazovat na konkrétní výrobce nebo postupy, pokud to není nezbytné.

Otázka: Bude zadavatel akceptovat i jiné, na standardech založené metody přenosu informací o politikách a segmentaci (např. VXLAN-GBP, standardní RADIUS atributy VSA nebo Role-Based Policy), které zajistí identický bezpečnostní výsledek bez nutnosti použití proprietárního protokolu jednoho výrobce?

Dotaz č. 38:

K protokolu EAP-FAST (Proprietární omezení)

Dotaz: V požadavcích je požadována podpora protokolu EAP-FAST. Tento protokol byl vyvinut společností Cisco a není průmyslovým standardem pro moderní NAC systémy (na rozdíl od EAP-TLS nebo EAP-TEAP).

Otázka: Postačí zadavateli pro splnění požadavku na „EAP-Chaining“ (současné ověření stroje i uživatele) podpora otevřeného standardu EAP-TEAP (dle RFC 7170), který je nativně podporován v operačních systémech bez nutnosti instalace softwaru třetích stran?

Dotaz č. 39:

K Multi-vendor podpoře (Ekonomická efektivita)

Dotaz: Zadavatel v požadavcích požaduje řízení přístupu na všech portech síťových přepínačů.

Otázka: Požaduje zadavatel, aby nabízené řešení NAC poskytovalo plnou a garantovanou funkcionalitu (včetně hloubkového profilování IoT a změny autorizace CoA) i na aktivních prvcích jiných výrobců, než je výrobce samotného NAC serveru?

Vyžadujeme potvrzení, že zadavatel preferuje otevřené řešení, které neznehodnocuje jeho stávající investice do sítě a umožňuje budoucí rozvoj bez technologického uzamčení (Vendor Lock-in).

Nástroj pro zabezpečení zdravotnických zařízení

Dotaz č. 40:

Omezení architektury: Zadavatel v bodě striktně vyžaduje dodání "HW sondy". Považuje zadavatel za splnění požadavku i řešení, kde funkci sondy (sběr a analýzu specifických OT protokolů jako Modbus/PROFINET) vykonává přímo aktivní prvek sítě (switch) vybavený dedikovaným analytickým enginem? Trvání na externím HW zařízení (sondě) v situaci, kdy identickou funkci plní síťový prvek nativně, se jeví jako bezdůvodná překážka hospodářské soutěže a v rozporu se zásadou technologické neutrality.

Dotaz č. 41:

"neviditelnost" systému: Bod vyžaduje, aby systém nebyl detekovatelný. U externích sond připojených přes SPAN port hrozí detekce skrze chyby v konfiguraci portu. Akceptuje zadavatel jako bezpečnější a technologicky vyspělejší variantu monitoring integrovaný přímo v ASIC čipech přepínačů, který je z principu své fyzické podstaty (vnitřní sběrnice) pro zbytek sítě absolutně neviditelný?

Dotaz č. 42:

Propojitelnost a bezpečnost: Zadavatel požaduje "vzájemnou propojitelnost jednotlivých technologií". Je si zadavatel vědom, že integrace NAC systému a monitoringu od různých výrobců (např. Flowmon + jiný NAC) zvyšuje bezpečnostní riziko prodlevy při automatické reakci na incident? Připouští zadavatel jako preferované řešení jeden ucelený ekosystém, kde NAC a monitoring sdílejí společnou databázi identit v reálném čase, čímž dochází k okamžité izolaci útočníka bez nutnosti API integrace třetích stran?

Dotaz č. 43:

Dokument vyžaduje připojení sondy přes SPAN/mirroring port. Tento způsob je však nespolehlivý při vysokém zatížení (dochází k zahazování paketů na monitorovacím portu). Nabídne-li uchazeč řešení založené na distribuované analytice (každý port je senzorem), které zaručuje 100% viditelnost i při plném vytížení 25G linek, bude toto hodnoceno jako technicky nadřazené?

Dotaz č. 44:

Požadavek na 2 TB úložné kapacity pro archivaci obohacených dat po dobu 6 měsíců je vázán na "virtuální řešení kolektoru". Je přípustné, aby tato kapacita byla součástí širšího management systému, který kromě logů a toků spravuje i politiky přístupu, čímž splní požadavek na jednotný celek dle bodu?

Vysoká dostupnost virtualizační vrstvy a diskových polí

Dotaz č. 45:

Proprietární název služby "AMS"

Zadavatel v bodě 4.4 vyžaduje absenci konkrétního SW produktu "AMS (Agentless Management Service)". Jde o přímé porušení zákazu používání obchodních názvů.

Dotaz: „V části 4.3 (Management a vzdálená správa) zadavatel striktně vyžaduje: *'OS se musí kompletně obejít bez AMS (Agentless Management Service)'*. Upozorňujeme zadavatele, že AMS je registrovaný obchodní název pomocné služby konkrétního výrobce (HPE). Tímto požadavkem zadavatel nepřípustně zvýhodňuje jednoho výrobce a porušuje ZZVZ. Žádáme zadavatele o odstranění tohoto názvu a potvrzení, že za ekvivalentní bude považováno jakékoli řešení umožňující plnohodnotný monitoring hardware bez nutnosti instalace agentů třetích stran do OS.“

Dotaz č. 46:

OOB Management skupina (iLO Federation)

Požadavek na správu bez externí aplikace a databázi na dvou místech je technicky omezující.

Dotaz: „Zadavatel vyžaduje, aby OOB karta tvořila management skupinu bez externí aplikace a aby databáze byla minimálně na dvou místech. Žádáme zadavatele o odborné zdůvodnění, v čem spatřuje vyšší míru dostupnosti u tohoto řešení oproti standardnímu průmyslovému postupu, kdy je správa clusteru realizována pomocí bezplatné virtuální appliance, která disponuje vyšším výkonem a lepší bezpečností. Trvání na tomto specifickém HW rysu (typickém pro iLO Federation) považujeme za diskriminační."

Dotaz č. 47:

Škálování řadičů vs. Scale-out

Bod 4.8 vyžaduje škálování přidáváním řadičů do jedné konfigurace (Scale-up), což znevýhodňuje modernější Scale-out architektury.

Dotaz: „Zadavatel vyžaduje škálování výkonu přidáváním řadičů do min. čtyř-řadičové konfigurace a zakazuje řešení pomocí 'podvěšení dalšího pole'. Upozorňujeme, že moderní architektury využívají pro lineární škálování výkonu a kapacity metodu Scale-out clusteru, kdy jsou jednotlivé nody logicky sjednoceny do jednoho celku. Tento přístup je technologicky vyspělejší než prosté přidávání řadičů do jedné šasi. Žádáme o úpravu bodu 4.8 tak, aby byla přípustná i Scale-out architektura tvořící jeden funkční logický celek se společnou správou."

Dotaz č. 48:

Proprietární termíny pro snapshoty a klony

Požadavky na „přechod snapshotu v klon" a „reverzní snapshoty" jsou terminologií konkrétního FW.

Dotaz: „V sekci 'Kopírovací funkce' zadavatel používá specifické termíny jako *'snapshot se po určité době může automaticky stát klonem'*. Žádáme zadavatele o potvrzení, že tento požadavek bude považován za splněný i u architektur, které díky logickému uspořádání dat na bázi metadat nerozlišují mezi snapshotem a klonem z hlediska výkonu a umožňují okamžitý zápis do jakékoli kopie (writable snapshot) bez nutnosti její transformace na jiný typ objektu. Trvání na doslovném postupu transformace objektu je technicky neopodstatněné a diskriminační."

Dotaz č. 49:

Potvrzení o trhu EU/ČR

Požadavek na potvrzení od lokálního zastoupení výrobce pro český trh.

Dotaz: „Zadavatel vyžaduje potvrzení, že řešení je určeno pro český (EU) trh. Žádáme zadavatele o vyjasnění, zda bude akceptováno i čestné prohlášení uchazeče, že zboží pochází z oficiální distribuce v rámci Evropského hospodářského prostoru (EHP). Požadavek na potvrzení přímo od lokálního zastoupení konkrétního výrobce může být v rozporu se zásadou volného pohybu zboží v rámci vnitřního trhu EU a může vytvářet bariéry pro uchazeče, kteří odebírají zboží z jiných členských států EU."

Implementace systému pro zálohování dat

Dotaz č. 50:

"V části 'Síťové úložiště určené pro zálohování PACS' zadavatel v parametru 'Podpora interního systému souborů' striktně vyžaduje souborový systém 'EXT4, Btrfs'. Tento požadavek je z technického hlediska neodůvodněný a diskriminační, neboť souborový systém je interní záležitostí architektury úložiště a nemá vliv na kompatibilitu s okolním prostředím (protokoly SMB/NFS).

Požadavek na konkrétní souborový systém Btrfs přímo vylučuje renomované Enterprise výrobce, kteří používají vlastní, často výkonnější a bezpečnější souborové systémy, a naopak přímo definuje řešení jediného výrobce (Synology/QNAP).

Domáhá se zadavatel dodání low-end/SMB zařízení (typ Synology), nebo bude akceptovat i profesionální Enterprise úložiště s proprietárním filesystémem, který zajišťuje shodnou či vyšší míru integrity dat? Žádáme o úpravu zadání vypuštěním požadavku na konkrétní interní souborový systém, případně jeho doplnění o formulaci 'nebo jiný ekvivalentní enterprise souborový systém'."

Dotaz č. 51:

"V technické specifikaci serverů v části 'Management a vzdálená správa' zadavatel požaduje: *'OOB karta serveru musí být schopna utvořit management skupinu... bez nutnosti instalace externí management aplikace... v režimu master-slave'*. Tato definice přesně kopíruje proprietární funkcionalitu jednoho výrobce (HPE iLO Federation).

Současně zadavatel uvádí požadavek, že *'OS se musí kompletně obejít bez AMS (Agentless Management Service)'*, což je opět specifická obchodní terminologie společnosti HPE.

Trvá zadavatel na těchto specifických parametrech, čímž vědomě omezuje soutěž pouze na dodavatele technologie HPE, nebo bude akceptovat i rovnocenné technické řešení jiných výrobců, které dosahuje stejného cíle (hromadná správa a monitoring) jinými technickými prostředky či s využitím bezplatné virtuální appliance? Žádáme o odstranění specifických obchodních názvů (AMS) a zobecnění požadavku na skupinový management."

Dotaz č. 52:

"Zadavatel požaduje osazení serverů disky o kapacitě 24TB. Upozorňujeme, že disky této kapacity představují absolutní technologickou novinku, která může být u některých Enterprise výrobců nedostupná nebo vázána na extrémně dlouhé dodací lhůty, což může ohrozit plnění zakázky.

Z důvodu rozšíření hospodářské soutěže a zajištění ekonomické výhodnosti se tážeme: Bude zadavatel akceptovat i nabídku řešení osazeného disky s kapacitou 22TB, pokud uchazeč navýšením počtu disků nebo expanzních polic dorovná celkovou požadovanou netto kapacitu úložiště?"

Dotaz č. 53:

"V části 'Zálohovací software - Licencování' zadavatel požaduje, aby licence nebyla závislá na objemu dat ani počtu VM. Tento požadavek reflektuje zastaralé licenční modely (Per Socket), od kterých většina předních světových výrobců softwaru v Enterprise segmentu upustila.

Trváním na tomto požadavku zadavatel de facto vylučuje dodání moderních softwarových platforem, které přešly na univerzální licenční modely (např. Veeam Universal License).

Bude zadavatel akceptovat i moderní licenční model (např. per instance/capacity), pokud uchazeč v nabídce zahrne dostatečný počet licencí pokrývající celý rozsah zadání (všechny popsané VM a kapacity) s rezervou např. 20 % pro budoucí růst po dobu trvání podpory?"

Emailová brána

Dotaz č. 54:

Požadavek na *"možnost nasazení v režimu gateway (MTA), server i transparent"* a specifikace *"v režimu server je možno vytvořit až 1500 schránek"* je pro jiné výrobce nesplnitelný. Bezpečnostní brána má filtrovat provoz, nikoliv hostovat uživatelská data a nahrazovat poštovní server. Toto je unikátní vlastnost FortiMailu, která zde slouží jako "vendor-lock"

"V části 'Obecné požadavky na platformu' zadavatel požaduje možnost nasazení v režimu 'server' a schopnost 'vytvořit až 1500 schránek'.

Tento požadavek směšuje dvě technologicky odlišné role: bezpečnostní bránu (Security Gateway) a poštovní server (Mail Server). Požadavek na hosting 1500 schránek přímo na bezpečnostním prvku je v rozporu s moderními principy kybernetické bezpečnosti (princip

segregace služeb) a v prostředí nemocnice nedává smysl, pokud již existuje stávající SMTP server, jak je uvedeno v úvodu dokumentu.

Tento parametr bezdůvodně diskriminuje všechna moderní bezpečnostní řešení, která fungují jako čisté MTA/API security vrstvy, a je ušit na míru jedinému řešení (Fortinet FortiMail).

Trvá zadavatel na požadavku, aby bezpečnostní brána suplovala funkci poštovního serveru a hostovala schránky, čímž vědomě omezuje soutěž pouze na jednoho výrobce, nebo bude akceptovat profesionální řešení 'Secure Email Gateway', které se soustředí výhradně na inspekci provozu a doručuje zprávy na stávající mailserver zadavatele? Žádáme o vypuštění požadavku na 'režim server' a 'počet schránek'."

Dotaz č. 55:

Režim "Transparent" (L2 bridging) a "IBE" (Identity Based Encryption) jsou další specifika Fortinetu. Běžná řešení používá MTA (změna MX záznamu) nebo API. IBE je specifická implementace, obecně ostatní výrobci používá jiné metody šifrování (PDF, Web Portal).

"Zadavatel v technické specifikaci požaduje podporu nasazení v režimu 'transparent' a dále vyžaduje specifickou metodu šifrování 'IBE' (Identity Based Encryption).

1. Režim 'transparent' je zastaralý způsob nasazení na L2 vrstvě, který neumožňuje pokročilé funkce ochrany dostupné v režimu MTA (Mail Transfer Agent). Standardem pro nasazení Email Security je úprava MX záznamu (MTA) nebo API integrace.

2. Zkratka 'IBE' odkazuje na specifickou marketingovou terminologii a technologickou implementaci konkrétního výrobce (Fortinet).

Zadavatel tímto porušuje ZZVZ použitím odkazů na specifické technologie jednoho dodavatele bez připuštění ekvivalentního řešení. Bude zadavatel akceptovat i řešení, které pracuje v standardním režimu MTA (MTA mode) a zajišťuje šifrování emailů jinou bezpečnou metodou (např. CRES, PDF encryption, Web Portal), která splňuje účel ochrany obsahu zprávy?"

Dotaz č. 56:

Požadavek *"podpora SMTP autentizace min. pomocí protokolů LDAP, RADIUS, POP3 a IMAP"* opět implikuje, že brána má sloužit jako koncový bod pro uživatele (mail server). Bezpečnostní brána (MTA) ověřuje obvykle jen relay (IP/Auth) nebo LDAP pro kontrolu existence příjemce, ale neřeší přístup uživatelů k poště přes IMAP.

"Zadavatel požaduje podporu autentizace pomocí protokolů POP3 a IMAP. Tyto protokoly slouží k přístupu koncových uživatelů k poštovním schránkám (čtení pošty), nikoliv k zabezpečení SMTP přenosu (odesílání/příjem mezi servery).

Pokud je předmětem plnění 'Emailová brána' pro ochranu komunikace (jak plyne z názvu zakázky), je požadavek na klientské přístupové protokoly (POP3/IMAP) irelevantní a technicky neodůvodněný, ledaže by zadavatel poptával náhradu celého poštovního serveru (Exchange/Lotus).

Může zadavatel potvrdit, že hledá bezpečnostní řešení (MTA Gateway) a nikoliv náhradu poštovního serveru? Pokud ano, žádáme o odstranění požadavku na podporu POP3 a IMAP autentizace, jelikož tyto protokoly bezpečnostní brána v režimu MTA pro svou funkci nepotřebuje."

Dotaz č. 57:

Požadavek *"propustnost řešení je min. 220 000 email/h"* je podezřele konkrétní číslo.

"Zadavatel stanovil minimální propustnost na přesně 220 000 email/h. Tato hodnota neodpovídá standardizovaným metrikám (např. dle RFC) a jeví se jako prostý opis z datasheetu konkrétního modelu virtuální appliance jednoho výrobce.

Z jaké metodiky zadavatel při stanovení této hraniční hodnoty vycházel? Bude zadavatel akceptovat i řešení s jinou nominální propustností (např. udávanou v počtu zpráv za den nebo Mbps), pokud uchazeč doloží, že navržené řešení s dostatečnou rezervou pokryje reálný provoz nemocnice (který je pravděpodobně řádově nižší než 220 tisíc emailů za hodinu)?“

Odpověď zadavatele na Dotazy:

Realizace perimetrového a centrálních firewallů

Ad. Dotaz č. 23

Na trhu je více zařízení plnící požadované parametry, tj. tvrzení dodavatele je účelové.
Zadavatel tedy trvá na tom, že se nejedná o diskriminační požadavky, nicméně připouští možnost splnit požadavky dvěma zařízeními s max. velikostí 2U.

Ad. Dotaz č. 24

Zadavatel nesouhlasí s tvrzením dodavatele, že uvedené testy „jsou irelevantní pro posouzení bezpečnostního výkonu NGFW“.

UDP PPS je test důležitý pro výkon NGFW u využívání DDoS ochrany, VoIP, DNS provozu a IoT sítí, což jsou důležité služby v rámci nemocnice.

Propustnost UDP/64B ukazuje skutečný packet processing výkon a tedy reálně ověřuje skutečný výkon NGFW.

HTTP/HTTPS mix posuzuje výkop NGFW jen v omezeném rozsahu služeb NGFW, tj. je nedostatečný.

Dodavatel bude muset zvolit zařízení, které bude plnit požadavky ZD, a to i po ověření těmito testy, zařízení je trhu více, tj. nejedná se o diskriminační požadavek.

Ad. Dotaz č. 25

Nesoulad opraven v předchozím vysvětlení.

Zadavatel požaduje podporu výrobce min. na 2 roky, v rámci nabídky může dodavatel nabídnout delší dobu.

Dotazy k smluvním podmínkám dle Přílohy č. 5

Ad. Dotaz č. 26

Dodavatel prokáže splnění podmínek podáním nabídky a podpisem smlouvy.
Pokud se ukáže, že některá část neplní požadavky ZD, bude po dodavateli vyžadováno, aby dodal plnění, které je splní, případně bude sankcionován.

Ad. Dotaz č. 27

Opraveno znění smlouvy.

Dotazy k smluvním podmínkám dle Přílohy č. 3

Ad. Dotaz č. 28

Ne, klauzule se nevztahuje na součinnost výrobce, ale pouze na součinnost Objednatele.

Realizace nástroje pro vysokou dostupnost aplikací

Ad. Dotaz č. 29

Dodavatel bude akceptovat i řešení navrhované dodavatelem, tj. oddělení WAF od NGFW.

Ad. Dotaz č. 30

Zadavatel specifikoval minimální požadavky, tj. uvedený počet portů je minimální, nikoliv exaktní. Zadavatel samozřejmě bude akceptovat řešení se stejným nebo vyšším počtem portů a dalšími „lepšími“ parametry.
Zadavatel připouští splnění požadavků dvěma zařízeními.

Ad. Dotaz č. 31

Na trhu je více výrobců, kteří splní požadavek na „Proxy-based inspekce“, tj. nejedná se o plnění jediného dodavatele.

LAN a WLAN

Ad. Dotaz č. 32

Zadavatel upozorňuje, že uvedené značky nedefinují požadavek na dodávku, ale identifikují stávající zařízení, které zůstane zachováno a bude součástí síťového prostředí.

Na tuto situaci se nevztahuje zákaz uvádění značek a modelů, protože se jedná o výchozí stav a prostředí objednatele, do něhož bude dodávka realizována.

Ad. Dotaz č. 33

Zadavatel akceptuje řešení formou LED.

Ad. Dotaz č. 34

Zadavatel akceptuje propojení se stejnými nebo lepšími parametry bez ohledu na umístění (zadní nebo přední).

Ad. Dotaz č. 35

Na trhu je více výrobců, kteří splní uvedené podmínky.
Zadavatel připouští „tri-radio AP s funkcí kontinuálního monitoringu“.

Ad. Dotaz č. 36

Zadavatel připouští i řešení uváděná dodavatelem.

NAC

Ad. Dotaz č. 37

Zadavatel bude akceptovat i řešení navrhované dodavatelem.

Ad. Dotaz č. 38

Zadavatel akceptuje i EAP-TEAP.

Ad. Dotaz č. 39

Ano.
Zadavatel preferuje otevřené řešení, tj. v souladu se zněním požadavku.

Nástroj pro zabezpečení zdravotnických zařízení

Ad. Dotaz č. 40

Zadavatel bude akceptovat i jiné než HW řešení sondy, pokud budou splněny všechny ostatní požadavky uvedené v TS.

Ad. Dotaz č. 41

Zadavatel akceptuje řešení navrhované dodavatelem.

Ad. Dotaz č. 42

Zadavatel akceptuje ucelené řešení / ekosystém, nicméně neomezuje tímto soutěž v rámci VZ, trvá tedy jen na splnění požadavků ZD bez ohledu na výrobce.

Ad. Dotaz č. 43

Řešení dodavatele bude posuzováno jako plnící zadávací podmínky.

Ad. Dotaz č. 44

Požadavek na úložnou kapacitu mlže být součástí širšího řešení, ale musí být zajištěno, že požadovaná kapacita bude vždy dostupná pro požadovaný účel.

Vysoká dostupnost virtualizační vrstvy a diskových polí

Ad. Dotaz č. 45

Zadavatel nezvýhodňuje žádného výrobce ani nikoho nediskriminuje.
Systém AMS není požadován pro dodávku, ale je vyloučena jeho dodávka z důvodu zajištění bezpečnosti.
OS je jistě možné dodat bez proprietárních technologií konkrétního výrobce, čímž je naopak rozšířena možnost hospodářské soutěže.

Ad. Dotaz č. 46

Zadavatel nepožaduje přímo „iLO Federation“, ale řešení plní technické podmínky uvedené v TS. Dodavatel může nabídnout ekvivalentní řešení, ale musí toto odůvodnit.

Ad. Dotaz č. 47

Zadavatel připouští „Scale-out“ architekturu.

Ad. Dotaz č. 48

Zadavatel trvá na funkčním splnění požadavků, nikoliv na stejné terminologii. Terminologie slouží pro ilustraci funkčnosti.

Ad. Dotaz č. 49

Zadavatel není schopen zjistit, zda výrobce nerozlišuje dodávané produkty a související služby dle země v EU, z tohoto důvodu žádá o toto potvrzení.

Dodavatel toto může prokázat prohlášením zastoupení jiné země EU, že dodávaný výrobek a služby jsou plnohodnotně dostupné v ČR, a to včetně služeb.

Implementace systému pro zálohování dat

Ad. Dotaz č. 50

Zadavatel bude akceptovat i ekvivalentní enterprise souborový systém, pokud budou splněny ostatní požadavky uvedené v TS.

Ad. Dotaz č. 51

Zadavatel nepožaduje přímo „iLO Federation“, ale řešení plní technické podmínky uvedené v TS.
Dodavatel může nabídnout ekvivalentní řešení, ale musí toto odůvodnit.

Ad. Dotaz č. 52

Zadavatel bude akceptovat i 22TB disky při zajištění celkové požadované kapacity.

Ad. Dotaz č. 53

Zadavatel bude akceptovat i licenční model navrhovaný dodavatelem, pokud bude obsahovat rezervu min. 30 %.

Emailová brána

Ad. Dotaz č. 54

Zadavatel trvá na splnění všech požadavků na řešení.
Zadavatel připouští, aby byly požadavky splněny více technologiemi.

Ad. Dotaz č. 55

Zadavatel bude akceptovat řešení navrhované dodavatelem.

Ad. Dotaz č. 56

Zadavatel odkazuje dodavatele na odpověď na první dotaz v této části.

Ad. Dotaz č. 57

Zadavatel bude akceptovat řešení s propustností min. 50 tis. emailů / hodinu.

II.

Zadavatel poskytl výše uvedené vysvětlení zadávací dokumentace v zákonné lhůtě ve smyslu § 98 zákona č. 134/2016 Sb., o zadávání veřejných zakázek. Lhůta k podání nabídek byla dosud třikrát prodloužena, přičemž k poslednímu prodloužení došlo dne 12. 2. 2026. Aktuálně stanovená lhůta je nadále delší než minimální lhůta podle § 57 odst. 1 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, pro podání nabídek v nadlimitním otevřeném řízení.

S ohledem na uvedené zadavatel lhůtu k podání nabídek dále neprodlužuje.

Ing. Petr Baťka

Digitálně podepsal Ing. Petr Baťka
Datum: 2026.02.16 14:44:56 +01'00'

Ing. Petr Baťka
ředitel