Název dokumentu	Vysvětlení zadávací dokumentace č. 6
Zadavatel	***ČEPRO, a.s.*** *Praha 7, Dělnická 213/12, Holešovice, PSČ 170 00* *IČ: 60193531* *zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 2341* *Zastoupena:* *Mgr. Jan Duspěva, předseda představenstva* *Ing. František Todt, člen představenstva*
Název veřejné zakázky	Privileged Identity Management/ Privileged Access Management (PIM/PAM)
Ev. č. veřejné zakázky	
Druh zadávacího řízení	ZPŘ
Ev. č. zadavatele	178/20/OCN

Zadavatel shora uvedené veřejné zakázky poskytuje dle § 98 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „zákon“) následující vysvětlení zadávací dokumentace.

Objednatel obdržel dne 24.11.2020 prostřednictvím profilu zadavatele žádosti dodavatele o vysvětlení zadávací dokumentace zakázky, na základě čehož se zadavatel rozhodl poskytnout odpovědi na předložené dotazy k nadepsané zakázce formou zveřejnění tohoto vysvětlení zadávací dokumentace.

Dotaz č. 38	VoKB stanovuje požadavek na řízení zranitelností tak, že je nutné využít nástrojů typu Vulnerability Management, v této oblasti není nástroj PIM/PAM dostačující. Dále stanovuje požadavek na omezení „přidělování privilegovaných oprávnění na úroveň nezbytně nutnou k výkonu náplně práce“. Tento požadavek přesně splňuje PIM/PAM nástroj. Z výše uvedeného vyplývá, že uvedený požadavek na „porovnávání aktuálního stavu s anonymními údaji tisíců zákazníků po celém světě“ nevyplívá z VOKB, je požadavkem Zadavatele, a současně diskriminuje ostatní výrobce, neboť je znám pouze jeden výrobce, který tuto funkcionalitu poskytuje. Žádáme tedy o úpravu tohoto požadavku, neboť jeho ponechání znamená pro ostatní dodavatele zamezení možnosti podat nabídku do VŘ.
Odpověď č. 38	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Cílem daného požadavku na porovnání stavu bezpečnosti s jinými společnostmi je snaha odhadnout a optimálně řídit bezpečnostní rizika, získat informace pro rozhodování na taktické a strategické úrovni organizace. Porovnání s dosaženou úrovní bezpečnosti je klíčový vstup pro řízení dalších investice do oblasti PIM/ PAM ve společnosti. V této souvislosti odkazuje Zadavatel na své odpovědi k dotazům č. 9 a 24.

Dotaz č. 39	Dle veřejného věstníku smluv již Zadavatel disponuje nástrojem SIEM dle VVŘ, Systémové číslo: P16V00000002 Evidenční číslo zadavatele: 095/16/OCN, odkaz na profilu zadavatele: https://zakazky.ceproas.cz/contract_display_2.html v hodnotě 2 600 000,- Kč, kde vyhlásil vítěze soutěže společnost AXENTA a.s. Je tedy možné splnit požadavek integrací na vlastněný SIEM, který toto již splňuje a požadavky by se tak dublovaly, tzn. Zadavatel by jen díky tomuto požadavku měl více SIEM nástrojů? Technicky daný požadavek splňuje samostatně (bez využití integrací) pouze jedno řešení PAM na trhu a jakékoli řešení dokoupení dalšího systému, jehož součástí by byl výše uvedený požadavek, zásadně navyšuje cenu ostatním potencionálním dodavatelům Jelikož se zadavatel několikrát vyhradil proti zvýhodňování jednoho výrobce, dovoluje si tímto dotazem upozornit, že neumožněním výše zmíněného, by Zadavatel možná i nechtěně jednoho konkrétního výrobce zvýhodnil a

	nechoval se v mezích zodpovědného hospodáře, jelikož by požadoval nasazení stejného systému (SIEM) 2x.
Odpověď č. 39	Cílem požadavku zadavatele je zajistit bezpečné práci s privilegovanými účty, které přistupují do kritické infrastruktury státu. Za tímto účelem poptává Zadavatel nástroj PIM/ PAM v rozsahu, který umožní zadavateli splnit požadavky ZoKB. Zadavatel ve snaze zajistit tuto klíčovou bezpečnostní oblast jistě nechce odmítnout řešení, které by mohlo požadavků zadavatele dosáhnout integrací vícero produktů. Z tohoto důvodu nástroj SIEM není v rámci zadávací dokumentace požadován, je však připuštěn. Zadavatel rozumí snaze tazatele využít existující prvky bezpečnostního dohledu zadavatele. Integrace s existujícím nástrojem SIEM by byla možná, současně by však znamenala dodatečné náklady na straně zadavatele spojené s investicemi do licencí, hardwaru současného řešení SIEM a případná integrace by též znamenala riziko narušení existujících smluvních ujednání o podpoře řešení a odpovědnosti za škody, což považuje za nepřípustné. Zadavatel tyto rizika při přípravě zadávací dokumentace zvážil a z uvedeného důvodu se rozhodl integraci s existujícím řešením nerealizovat. Dále, integrací jakéhokoli řešení PIM/PAM do nástroje SIEM Zadavatele, který provozuje za účelem splnění podmínek ZoKB by musel dále zpřísnit zadávací podmínky požadavkem např. na certifikaci vybraného dodavatele pro integraci do stávajícího řešení SIEM apod. Zadavatel má zato, že svým přístupem učinil zadávací řízení přístupnější pro vícero dodavatelů. Na základě všech výše uvedených důvodů Zadavatel nepřipustil integraci na existující SIEM řešení Zadavatele jako splnění požadavků této veřejné soutěže.

Dotaz č. 40	Dle veřejného věstníku smluv již Zadavatel nástrojem SIEM dle VVŘ disponuje, Systémové číslo: P16V00000002 Evidenční číslo zadavatele: 095/16/OCN, odkaz na profilu zadavatele: https://zakazky.ceproas.cz/contract_display_2.html v hodnotě 2 600 000,- Kč, kde vyhlásil vítěze soutěže společnost AXENTA a.s. Technicky tento daný požadavek splňuje samostatně pouze jedno řešení PAM na trhu. Zadavatel uvádí možnost splnění požadavku integrací s nástrojem SIEM, avšak musí být kompletně součástí dodávky. Je možné splnit požadavek integrací na Zadavatelem již vlastněný nástroj SIEM? Neuvolnění by pro všechny dodavatele mimo jediného znamenalo značné finanční navýšení a nekonkurenceschopnost z důvodu zahrnutí i další licencí SIEM, mimo již Zadavatelem vlastněných a v kontextu komplexního fungování kybernetické bezpečnosti by nedávalo smysl.
Odpověď č. 40	Odpověď viz dotaz 39

Dotaz č. 41	Dle veřejného věstníku smluv již Zadavatel disponuje nástrojem SIEM dle VVŘ, Systémové číslo: P16V00000002 Evidenční číslo zadavatele: 095/16/OCN, odkaz na profilu zadavatele: https://zakazky.ceproas.cz/contract_display_2.html v hodnotě 2 600 000,- Kč, kde vyhlásil vítěze soutěže společnost AXENTA a.s. Je tedy možné splnit požadavek integrací na vlastněný SIEM, který toto již splňuje a požadavky by se tak dublovaly, tzn. Zadavatel by jen díky tomuto požadavku měl více SIEM nástrojů? Technicky daný požadavek splňuje samostatně (bez využití integrací) pouze jedno řešení PAM na trhu a jakékoli řešení dokoupení dalšího systému, jehož součástí by byl výše uvedený požadavek, zásadně navyšuje cenu ostatním potencionálním dodavatelům
Odpověď č. 41	Zadavatel odkazuje na odpověď č. 39. V této souvislosti se Zadavatel se velice podivuje nad tím, že tazatel disponuje informací o vnitřním prostředí Zadavatele, tedy zda jím vlastněný SIEM ve své implementované podobě splňuje nebo nesplňuje požadavky stanovené v zadávacích podmínkách k této veřejné zakázce. Zadavatel dále připomíná, že nemá přístup k informacím o obchodních politikách a strategii výrobců PIM/ PAM a/nebo ujednáním mezi výrobci a jejich partnery a nemůže tedy posoudit účelovost/ pravdivost uvedeného tvrzení tazatele. Zadavatel má zato, že jeho požadavky jsou legitimní a zcela v souladu se zákonem.

Dotaz č. 42	Chápe tedy dodavatel správně, že může nabídnout i takové řešení, které pro splnění základních funkcionalit vyžaduje licence MS CAL, ale nemusí je dodat v rámci nabídky, i když to znamená, že bez nich není systém funkční? Dodavatel dále uvádí, že se může jednat o funkcionality řízení SSH relací k serverům, kde Zadavatel uvedl že musí být dodány všechny licence pro provoz serverové části. Může tedy Zadavatel blíže objasnit, jak je to s externími licencemi nezbytnými pro provoz základních funkcionalit PAM? Dodavatel se chce vyhnout situaci kdy dodá řešení, které nebude schopné základního provozu, protože Zadavatel nepožadoval externí licence MS CAL, nezbytné pro jeho provoz.
Odpověď č. 42	Cílem veřejné zakázky je zabezpečit správu existujících systémů v současném rozsahu správy. Správa serverů v prostředí zadavatele již vyžaduje vlastnictví MS CAL licencí bez ohledu na jakékoli implementované PIM/PAM řešení. Dle existujících smluvních ujednání je zadavatele oprávněn využít existující licence MS CAL bez jakýkoli dodatečných nákladů, rizika nebo nutnosti zásahu do vnitřního prostředí zadavatele. Z uvedeného důvodu se tedy zadavatel v rámci dodání PIM/ PAM řešení rozhodl dodání těchto licencí nepožadovat, jelikož má zato, že opětovné zakoupení těchto licencí by pouze uměle zvýšilo celkovou cenu zakázky bez přidané hodnoty pro Zadavatele (došlo by ke zdvojení licenční pozice, nedošlo by však ke zdvojnásobení počtu správců těchto systémů). Z výše popsaného důvodu proto Zadavatel od začátku zadávacího řízení požaduje dodání těch licencí, které souvisí s implementací dodaného PIM/ PAM.

Dotaz č. 43	Zadavatel uvedl v odpovědi na dotaz ohledně detekce útoků na zranitelnosti Kerberos, že tento požadavek splňuje více výrobců řešení PAM. Předkladatel se pohybuje na trhu kybernetické bezpečnosti řadu let a s tímto tvrzením nesouhlasí. Naopak mnoho řešení PAM využívá napojení na systémy SIEM či obdobné, které tuto funkcionalitu standardně zajišťují. Pokud však Zadavatel bude trvat na svém tvrzení, že případný SIEM musí být součástí dodávky, bude se jednat o účelové navýšení ceny. Je Zadavatel ochoten dle výše uvedených skutečností požadavek buď upravit tak, aby bylo možné splnit na základě již vlastněných systémů Zadavatele, např. SIEM, či zcela vypustit a umožnit tak možnost podání nabídky více výrobcům řešení PAM? VoKB tím samozřejmě není nijak porušena či dotčena.
Odpověď č. 43	Pro vyloučení všech pochybností, zadavatel nezpochybňuje tvrzení, že některá řešení na trhu nástrojů PIM/ PAM využívá napojení na nástroj SIEM, současně však dodává, že na trhu existuje vícero řešení, které daný požadavek řeší jiným způsobem. Je navíc možné danou funkcionalitu zajistit integrací na jiné nástroje, které popsanou detekci na zranitelnosti Kerberos řeší, nástroj musí však být dodán jako součást řešení včetně veškerých potřebných licencí. Zadavatel by rád doplnil, že protokol Kerberos slouží pro bezpečné prokázání identity uživatele, na základě které jsou danému uživateli přidělována přístupová oprávnění do systémů KII. Zneužití známých zranitelností může vést ke krádeži identity administrátora systému, které je v prostředí KII zcela nepřípustné – ochrana před tímto typem útoku je jedním z hlavních důvodů, proč Zadavatel projekt realizuje. Neodborný zásah a/ nebo kybernetický útok v prostředí KII může mít za následek ztráty na životech, majetku a/ nebo způsobit závažnou ekologickou havárii. Zadavatel dále připomíná, že nemá přístup k informacím o obchodních politikách a strategii výrobců PIM/ PAM a/nebo ujednáním mezi výrobci a jejich partnery a nemůže tedy posoudit účelovost/ pravdivost uvedeného tvrzení tazatele. Zadavatel má zato, že jeho požadavky jsou legitimní a zcela v souladu se zákonem.

Dotaz č. 44	Zadavatel v dotazu směřovanému na PAS Assessment tool výrobce uvedl odvolání na plnění souladu vyhláškou o kybernetické bezpečnosti č. 82/2018 Sb. (dále v tomto vysvětlení jen „VoKB“), která jasně požaduje zajištění procesu řízení zranitelností. Ano, toto tvrzení je pravdivé, nicméně v aktuální zakázce je řešen systém pro řízení privilegovaných přístupů. Někteří výrobci PAM mají jako součást PAM řízení zranitelností, avšak vázané primárně k privilegovaným účtům nikoli kompletní plný vulnerability scanner. Je takovéto řešení dostačující? Je možné tento požadavek upravit tak, aby splňovalo více výrobců řešení? V současné době odpovídá řešení pouze

	variantě od společnosti CyberArk CyberArk Privileged Access Managment Assessment Tool | CyberArk. Tento požadavek nemá jakýkoli vliv na plnění VoKB v oblasti řízení privilegovaných přístupů. Mnoho Zadavatelů spadajících pod VoKB má jiný systém než výše uvedený a VoKB plní.
Odpověď č. 44	Zadavatel se ohrazuje proti náznaku protěžování jakéhokoli konkrétního výrobce řešení. Zadavatel nepožaduje a nikdy nepožadoval „kompletní plný vulnerability scanner“ v rámci této zadávací dokumentace. Pokud tazatel tento požadavek v zadávací dokumentaci nalezl, žádá zadavatel o informaci o umístění požadavku, který bude neprodleně odstraněn. Zadavatel již v odpovědi č. 9 uvedl, že v rámci tohoto bodu požaduje metodiku, dle které může zadavatel na pravidelné bázi ověřit způsob používání nástroje vzhledem k privilegovaným účtům a best-practice výrobce. Cílem požadavku je rozšíření existujícího procesu řízení zranitelností o část PIM/PAM tak, aby provozování tohoto řešení v prostředí Zadavatele naplňovalo podstatu ZoKB.

Dotaz č. 45	Zadavatel v odpovědích uvádí že maximální počet současných relací je vztažen k maximálnímu počtu souběžně pracujících uživatelů. Výše uvedené tvrzení tedy počítá, že každý uživatel může provozovat maximálně s 1 relací? Případně že maximální počet relací je pouze 15 tzn. 1 spojení má neomezený počet relací? Někteří dodavatelé mají tyto relace licencované zvlášť, proto případné podcenění může mít za následek následné značné vícenáklady.
Odpověď č. 45	Zadavatel specifikoval maximální počet současně probíhajících relací na maximálně 15 v současné konfiguraci, čímž měl na mysli maximálně 15 současně připojených uživatelů. Zadavatel však nedisponuje statistikou počtu spojení na uživatele a nemá tuto informaci k dispozici. Pro odstranění všech pochybností, Zadavatel slovem relace míní přihlášení 1 uživatele a slovem spojení míní jedno komunikační spojení mezi zdrojovým a cílovým systémem.

Zadavatel s ohledem na povahu dotazů k zadávací dokumentaci a skutečnost, že obdržel šestou a sedmou žádost o vysvětlení ZD dne 24.11.2020 a na tuto žádosti podal vysvětlení v den uveřejnění tohoto vysvětlení, tedy 10 pracovních dnů poté, **prodlužuje v souladu s § 98 odst. 4 zákona lhůtu pro podání nabídek do 17. 12. 2020 do 10:00 hodin.**

V Praze

Milan Trnka

Digitálně podepsal Milan Trnka
Datum: 2020.12.08 13:48:15 +01'00'

ČEPRO, a.s.
oddělení centrálního nákupu