Zadavatel:

Pardubický kraj
se sídlem: Komenského nám. 125, 532 11 Pardubice
IČO: 70892822

Název veřejné zakázky:

„Bezpečnost komunikační infrastruktury"

veřejná zakázka na dodávky zadávaná v jednacím řízení s uveřejněním dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů

VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE IV

dle ust. § 98 a 99 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „*ZZVZ*")

Zadavatel obdržel v níže uvedeném termínu žádost dodavatele o písemné vysvětlení zadávací dokumentace. V návaznosti na obdrženou žádost zadavatel níže uvádí přesné znění žádosti a připojuje k ní písemné vysvětlení zadávací dokumentace.

Písemné vysvětlení zadávací dokumentace zadavatel uveřejnil, včetně přesného znění žádosti, na profilu zadavatele.

Žádost o vysvětlení zadávací dokumentace č. 4 (obdržena dne 27. 11. 2018):

Dotaz 1)

V části plnění 7 – Centrální logovací nástroj je obsažen požadavek:

Kapacita úložného prostoru (Disková kapacita appliance/pole, případně dedikovaná kapacita v rámci DC) pro systémem uložená data (logy, události /incidenty přijaté systémem) je 100TB.

Integrovaná systémová databáze má čistou velikost nejméně 100 TB s možností aktivace komprese ukládaných dat.

- Žádáme zadavatele o vysvětlení, zda toto znamená, že zadavatel požaduje čistou diskovou kapacitu pro ukládání logů 100TB?
- Lze v případě nabídky řešení, které poskytuje nativní kompresi uložených logů, bez dopadu na výkonnost, dodat kapacitu úložiště, která umožňuje ekvivalent 100TB raw logů bez komprese?

- V případě požadavku čisté kapacity úložiště 100TB se jedná o cca 1000TB nekomprimovaných dat. To při požadované licenci 518GB/day znamená dobu ukládání skoro 1950 dní. Opravdu zadavatel požaduje takovou dobu retence?

Informace zadavatele:

Zadavatel rozumí názoru účastníka zadávacího řízení tykajícího se využití kapacity úložiště, ale domnívá se, že tento požadavek vychází z předpokladu logování pouze na úrovni infrastruktury. Zadavatel ale v rámci řešení předpokládá i logování na aplikační úrovni, které je z kapacitního hlediska náročnější. Zároveň je z důvodu následné škálovatelnosti počítáno s rezervou pro využití v rámci doby udržitelnosti a po jejím uplynutí. Z těchto důvodů zadavatel trvá na parametru 100TB raw logů bez komprese.

Dotaz 2)

V části plnění 7 – Centrální logovací nástroj je uveden požadavek:

Systém umožňuje stálý příjem min. 10 tis událostí /s při průměrné velikosti události 600 Byte. Systém umožňuje nejméně po dobu 10 minut špičkový příjem minimálně 20 tis událostí/incidentů / s, v případě vyššího počtu událostí/incidentů jsou tyto ukládány systémem do bufferu k pozdějšímu zpracování.

Námi nabízené řešení je licencované v objemu GB/day. V tomto případě zadavatel požaduje licenci na zpracování cca 518GB logů denně a případně 1036GB logů ve špičce. Tento objem logů je nezvykle vysoký, a to vzhledem k velikosti infrastruktury zadavatele.

Skutečně je poptávaná licence shora uvedené kapacity?

Informace zadavatele:

Ano, zadavatel trvá na uvedené kapacitě logovacího nástroje.

Dotaz 3)

V části plnění 7 – Centrální logovací nástroj je uveden požadavek:

Systém nemá licenčně omezený počet zařízení zasílajících události, ani jinak licenčně omezený počet událostí za den.

Druhá část požadavku je v rozporu s kapacitními požadavky na minimální licenční objem požadované licence, která je přímo určena.

Žádáme zadavatele o vyjasnění rozporu.

Informace zadavatele:

Zadavatel v tuto chvíli trvá na parametrech uvedeného technického opatření, s tím, že konkrétní způsob splnění požadavku zadavatele může být předmětem jednání o předběžné nabídce.

Dotaz 4)

V kapitole 1 dokumentu:

"*PK_Bezpecnost_SML_P02_Specifikace_sluzeb_podpory_provozu.docx*" je mimo jiné uvedeno:

„pokud vyžaduje norma nebo legislativa, pod kterou spadá zadavatel, nějaké povinné úpravy předmětu plnění, je takováto úprava funkční dnem platnosti dané normy nebo legislativy a je na minimálně stejné administrátorské i uživatelské úrovni ovládání (legislativní update/upgrade)"

Tato formulace požadavků na změny plnění podle úpravy legislativy je legitimní, nicméně vzhledem k nemožnosti tyto změny a jejich rozsah predikovat bývá obvyklou praxí, že Zadavatel takovéto požadavky ohraničí maximální pracností nebo jiným způsobem. Jedině tak může zadavatel získat smysluplné nabídky.

Žádáme zadavatele o ohraničení tohoto požadavku například maximálním počtem MD/rok.

Informace zadavatele:

Zadavatel je subjektem veřejné správy, proto musí naplňovat všechny legislativní požadavky, z tohoto důvodu na tomto požadavku trvá.

Dotaz 5)

V kapitole 2 dokumentu:

"*PK_Bezpecnost_SML_P02_Specifikace_sluzeb_podpory_provozu.docx*" je mimo jiné uvedeno:

Provedení rekonfigurace kompletního opatření v druhém a pátém roce Služby podpory provozu dle požadavků zadavatele, provedení konzultačních služeb zhotovitelem před zadáním požadavků zadavatelem, vypracování prováděcí dokumentace. Na dané práce nelze využít jednotlivé hodiny konzultačních ani konfiguračních prací.

Stejně jako v předchozím dotazu žádáme zadavatele o ohraničení tohoto požadavku například maximálním počtem MD/rok.

Informace zadavatele:

Zadavatel nemůže předjímat časovou náročnost prací dodavatele při prvotní implementaci, a tedy ani při provedení rekonfigurace v druhém a pátém roce.

Dotaz 6)

V příloze 3 – Specifikace školení dokumentu *„PK_Bezpecnost_ZD_P01_Zavazny navrh smlouvy.docx*" je mimo jiné uveden požadavek na školení kritických částí díla.

Jelikož není jasné, které části považuje Zadavatel za kritické, žádáme o specifikace těchto částí tak, aby mohla být příslušná školení součástí nabídky a naplnila tak požadavek

zadavatele.

Informace zadavatele:

Školeními kritických částí díla je míněno:

1) Implementace Webového aplikačního firewallu a Loadbalanceru (2 osoby)

2) Zabezpečení počítavých sítí (2 osoby)

Bližší informace jsou uvedeny v příloze č. 3 daného dokumentu.

Dotaz 7)

V příloze 3 – Specifikace školení dokumentu „*PK_Bezpecnost_ZD_P01_Zavazny navrh smlouvy.docx*" je mimo jiné uveden požadavek na školení „*Zabezpečení počítačových sítí*":

ZABEZPEČENÍ POČÍTAVÝCH SÍTÍ (2 OSOBY)

Osnova školení 2

- Navazující na znalosti cca CompTIA Security+
- Identifikace hrozeb porušení bezpečnosti v počítačové síti s Active Directory, principy a fáze napadení sítě, typy bezpečnostních rizik
- Základy kryptografie
- Implementace opatření pro ochranu koncových stanic, serverů, sítě a dat v síti s Active Directory a operačním systémem Microsoft Windows
- hardening operačního systému Microsoft Windows
- Nastavení zabezpečení DNS, DHCP, NAC, PKI, SSO, VPN, Firewall, DMZ, sledování bezpečnosti Kerberos/NTLM a SSL/TLS provozu
- Zabezpečení bezdrátových sítí
- Využití pokročilých technik k ochraně sítě - IDS/IPS, logování, honeypot
- Ochrana proti malware
- Implementace opatření testování zranitelnosti sítě, detekce zranitelností
- Principy fyzického zabezpečení
- Ochrana a zálohování dat

Předpokládáme, že zadavatel při specifikaci výše uvedené osonovy vycházel již z nějakého známého školení, se kterým má vlastní zkušenost. Žádáme zadavatele o informaci, z obsahu jakého školení při specifikaci výše uvedené osnovy vycházel.

Informace zadavatele:

Zadavatel očekává, že účastník zadávacího řízení v předběžné nabídce navrhne jedno nebo více školení, které svým obsahem pokryjí kapitoly zmiňované v požadavku na dodávku školení „Zabezpečení počítačových sítí", dle svého uvážení. Svou povahou se může jednat např. o školení obdobná k EC – Council Certified Network Defender.

Dotaz 8)

V dokumentu "*5_datove_centrum_redig.docx*", který je součásti archivu "*PK_Bezpecnost_SML_P01_Technicka_specifikace.zip*", je v seznamu požadovaných

implementačních služeb i položka „*Instalace zálohovacího řešení KrÚ Pk pro celý nově dodaný cluster VMware*".

Vzhledem k tomu, že dodávka hardware a software pro zálohovací server není předmětem plnění této veřejné zakázky, předpokládáme, že instalaci zálohovacího řešení připraví zadavatel (hardware včetně D2D2 úložišť, OS, instalace zálohovacího SW, ověření funkčnosti).

V rámci plnění této zakázky pak bude provedena rekonfigurace pro potřeby této zakázky, tj. konfigurace zálohovacích politik pro VMware, nastavení a konfigurace páskové knihovny a akceptační testy překonfigurovaného zálohovacího řešení.

Žádáme zadavatele o potvrzení našeho shora uvedeného předpokladu a případně jeho upřesnění. Dále žádáme o informaci, jaký zálohovací software má být použit.

Informace zadavatele:

Zadavatel potvrzuje předpoklad účastníka zadávacího řízení. Jako zálohovací SW bude použit Veeam Backup & Replication Enterprise Plus.

Dotaz 9)

Ve stejném dokumentu (viz předchozí dotaz) je i požadavek na implementační služby „*Návrh migrace Oracle databáze na nově realizovaný Oracle cluster*" a „*Implementace Oracle clusteru*".

Vzhledem k nedostatku informací o stávajícím řešení žádáme o popis současného stavu Oracle prostředí, tzn.:

- počet Oracle serverů a jejich verze,
- zda se jedná o fyzickou nebo virtuální instalaci,
- jakým způsobem je dnes řešena vysoká dostupnost,
- počet a velikost Oracle databází,

a případně další detaily k současné infrastruktuře Oracle, které mohou být pro Dodavatele vstupem k návrhu provedení požadovaných služeb.

Informace zadavatele:

Detailnější informace o požadavku zadavatele tak, jak je uvedeno v zadávací dokumentaci veřejné zakázky, představují interní informace, které zadavatel poskytne účastníkům zadávacího řízení na počátku prvního jednání o předběžné nabídce oproti podpisu dohody o mlčenlivosti v souladu s odst. 1.6 zadávací dokumentace veřejné zakázky. Zadavatel současně

uvádí, že konkrétní způsob splnění požadavku zadavatele a doplnění dalších informací může být předmětem jednání o předběžné nabídce.

Zadavatel dále uvádí, že v rámci parametrů zejména požaduje:

1) Návrh migrace Oracle databáze na nově realizovaný Oracle cluster – podrobná dokumentace k dodanému VMware clusteru.
2) Implementace Oracle clusteru – převod jedné současné Oracle databáze (Zadavatel jich provozuje několik) do nového prostředí.

Dotaz 10)

K požadavkům, uvedeným v dokumentu "*10_Redundatni_proxy_redig.docx*", který je součásti archivu "*PK_Bezpecnost_SML_P01_Technicka_specifikace.zip*", žádáme o zodpovězení následujících dotazů:

- Je možné poskytnout informace o současném průměrném vytížení stávající Blue Coat proxy?
- Jaká je propustnost linky do Internetu (aktuální, případně plánovaná)?
- Pro kolik uživatelů má být systém redundantní proxy navržen? Lze počítat s počtem 400 uživatelů (uvedeno v jiném dokumentu)?

Odpovědi na tyto otázky jsou pro Dodavatele vstupem pro navržení správné konfigurace cílového řešení.

Informace zadavatele:

V pracovních dnech je průměrné vytížení 60-70GB, ve špičkách přesahujeme i 100GB za den.

Stávající propustnost linky do internetu je v převodu z 100 na 300 Mbps, plánované navýšení propustnosti linky je v úhrnu2,3 Gbps.

Zadavatel má v současné době 400 zaměstnanců, kteří aktivně využívají prostředky počítačové sítě úřadu. Navýšení počtu uživatelů nelze vyloučit.

Dotaz 11)

Ve stejném dokumentu (viz předchozí dotaz) jsou v seznamu Požadavků na funkcionalitu uvedeny následující položky:

- Rozšíření stávající konfigurace o dešifrování SSL provozu,
- Rozšíření stávající konfigurace o řízení šířky pásma pro vybraný typ provozu (např. video, zvuk),
- Rozšíření stávající konfigurace o inspekci veškerého webového provozu koncových zařízení,
- Rozšíření stávající konfigurace o hodnocení typu obsahu (YouTube),
- Rozšíření stávající konfigurace o inspekce dle typu webové aplikace (např. Google

Docs) a použité metody přenosu (GET, POST),
- Rozšíření stávající konfigurace o integraci se sandbox appliances,
- Rozšíření stávající konfigurace o řízení aplikací a protokolů, které mají povolen internetový provoz. A to i na základě velikosti a typu stahovaného souboru.

Ke správnému navržení cílové řešení včetně konfigurací a migrací, žádáme zadavatele o informaci, které ze shora uvedených funkcionalit jsou již nyní zadavatelem využívány a případně v jaké míře. Dodavateli není zcela zřejmé, zda se jedná o nové nasazení těchto funkcionalit, nebo pouze o rozšíření již používaných.

Informace zadavatele:

Nyní jsou zadavatelem využívány funkcionality:

1) dešifrování SSL provozu
2) inspekci vybraného webového provozu koncových zařízení
3) řízení aplikací a protokolů na základě velikosti a typu stahovaného souboru

U výše zmíněných funkcionalit se jedná o jejich rozšíření, případnou úpravu. U zbývajících se jedná o nové nasazení.

Dotaz 12)

K požadavkům, uvedeným v dokumentu "*12_loadbalancer_WAF_redig.docx*", který je součásti archivu "*PK_Bezpecnost_SML_P01_Technicka_specifikace.zip*", žádáme o zodpovězení následujících dotazů:

- Je poptávané řešení zcela nové, nebo nahrazuje nějaké jiné, stávající?
- Je možné odhadnout přibližný počet aplikací, které bude WAF chránit?
- Existuje požadavek na využívaní dynamických směrovacích protokolů na WAF?

Důvodem dotazů je optimalizace nabídky a cílového řešení.

Informace zadavatele:

Zadavatel konstatuje, že poptávaná technologie nahrazuje stávající zastarávající řešení. Počet webových aplikací není plně relevantní pro škálování výkonu dodávaného řešení, tím je spíše požadavek na propustnost nebo množství zpracovávaných requestů. Zadavatel konstatuje, že pro chod Krajského úřadu využívá/bude v budoucnu využívat přibližně 100 webových aplikací. Zadavatel konstatuje, že neuvažuje využívat dynamické směrovací protokoly.

Dotaz 13)

Ve stejném dokumentu (viz předchozí dotaz) jsou dále v seznamu Požadavků na funkcionalitu uvedeny následující položky:

- Podpora hardwarové SSL akcelerace,

- Podpora akcelerace.

Pro optimální návrh cílového řešení žádáme zadavatele o informaci, zda uvedené funkcionality požaduje dodat/zprovoznit v rámci implementace a nebo vyžaduje pouze podporu těchto funkcionalit na straně nabízené platformy, ale akceptuje odemčení těchto funkcionalit až po dokoupení patřičné SW licence.

Informace zadavatele:

Zadavatel konstatuje, že součástí plnění je i dodávka a zprovoznění výše uvedených funkcionalit.

Dotaz 14)

Ve stejném dokumentu (viz dotaz č. 5) jsou uvedeny konkrétní požadavky na metody load balancingu a perzistence. Dodavatel uvažuje o řešení, které je zaměřené více na bezpečnost, ale zároveň mírně omezené právě v možnostech metod load balancingu a perzistence; výhodou jsou potom pokročilé funkce WAF.

Dodavatel proto žádá o informaci, zda Zadavateli budou postačovat následující metody load balancingu (bez omezení na počet IP adres v poolu):

- Round Robin,
- Ratio (member),
- Ratio (node),
- Least Connections (member),
- Least Connections (node),
- Weighted Least Connection (member),
- Weighted Least Connection (node),
- Ratio Least Connection (member),
- Ratio Least Connection (node).

A perzistence:

- Cookie Persistency,
- Source Address,
- Host,
- Destination Address.

S ohledem na rozsah a složitost dotazů a předpokládaných upřesnění zadávacích podmínek vás žádáme o přiměřené prodloužení lhůty pro podání nabídek, a to minimálně o celou původní lhůtu.

Informace zadavatele:

Zadavatel trvá na všech technických parametrech load balancingu uvedených v dokumentu *„12_loadbalancer_WAF_redig.docx“* zadávací dokumentace veřejné zakázky.

Vzhledem k charakteru odpovědí zadavatele a na základě skutečnosti, že zadavatel v rámci vysvětlení zadávací dokumentace IV nepřistoupil ke změně nebo doplnění zadávací dokumentace ve smyslu § 99 ZZVZ, zadavatel neprodlužuje lhůtu pro podání předběžných nabídek.

V Praze dne 30. 11. 2018

Pardubický kraj
i.s. MT Legal s.r.o., advokátní kancelář
JUDr. Petr Novotný, LL.M., jednatel