Veřejná zakázka na dodávky

zadávaná v otevřeném řízení podle ustanovení § 3 písmeno b), § 14 odstavec (1), § 15 odstavec (1) a (2), § 25, § 56 souvisejících zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění platném ke dni zahájení tohoto zadávacího řízení (dále rovněž jen „Zákon“) s názvem:

„ZVÝŠENÍ KYBERNETICKÉ BEZPEČNOSTI VE FN BRNO“

ve vztahu k Zákonu se jedná o veřejnou zakázku nadlimitní

NADLIMITNÍ REŽIM
OTEVŘENÉ ŘÍZENÍ

Veřejná zakázka bude realizována na základě podpory projektu s názvem „Zvýšení kybernetické bezpečnosti ve FN Brno“, registrační číslo projektu č. CZ.06.3.05/0.0/0.0/15_011/0006912 v rámci Integrovaného regionálního operačního programu, prioritní osy 3, specifického cíle 3.2, výzvy č. 10 – „Kybernetická bezpečnost“ a bude spolufinancována z prostředků EU v rámci IROP.

VYSVĚTLENÍ ZADÁVACÍ DOKUMENTACE – SOUBOR ČÍSLO 04

Vysvětlení zadávací dokumentace poskytuje zadavatel v souladu s ustanovením § 98 Zákona.

Vysvětlení zadávací dokumentace podle § 98 Zákona či změna zadávací dokumentace podle § 99 Zákona poskytované zadavatelem bez požadavku dodavatele (označená jako Informace č.xx) je zveřejňována na elektronickém nástroji zadavatele ve lhůtách stanovených Zákonem.

Ve vysvětlení zadávací dokumentace poskytované zadavatelem podle § 98 Zákona na základě požadavku dodavatele je uvedeno přesné znění požadavku (označené jako Dotaz č.xx), kde formulace požadavku je doslovně převzata z požadavku dodavatele, a vlastní text vysvětlení (označené jako Odpověď zadavatele).

Dotaz č. 5:

K dokumentu „01 FNB KB - ZP - čistopis z 4_4_2019.pdf“ kapitola 9.7.2, totéž v dokumentu „04a FNB KB – Kupni smlouva - čistopis z 2_4_2019“ čl. III. odst. 5.1

Zadavatel zde uvádí požadavek na servis, cit.: „Úplné, řádné a bezvadné provádění komplexního záručního servisu (full service) dodaného systému pro zvýšení kybernetické bezpečnosti ve FN Brno včetně veškerého jeho dodaného příslušenství po celou dobu trvání 24měsíční záruční doby v rozsahu dle Smlouvy na zvýšení kybernetické bezpečnosti ve FN Brno.“

Žádáme tímto o upřesnění, co Zadavatel rozumí pojmem *úplné, řádné a bezvadné provádění komplexního záručního servisu (full service) dodaného systému.* V dokumentaci není nikde blíže specifikován pojem „full service" ani blíže rozveden rozsah požadovaného servisu a podmínky jeho poskytování. Tato skutečnost neumožňuje dodavateli řádně připravit svoji nabídku a současně Zadavateli hrozí riziko, že v důsledku obdrží neporovnatelné nabídky, když si každý dodavatel může rozsah servisu vysvětlit odlišně.

Odpověď zadavatele:

Zadavatel v článku III. a v článku XIV. Smlouvy na zvýšení kybernetické bezpečnosti ve FN Brno doslovně uvádí (mimo jiného) i následující text:

„3. Dodavatel se zavazuje, že **celý dodaný, nainstalovaný a zprovozněný systém včetně veškerých jeho součástí a příslušenství bude plně funkční, odpovídat zadávací dokumentaci, nabídce Dodavatele, platným právním předpisům a technickým normám a bude v souladu s požadavky uvedenými v této Smlouvě.** Prvky tvořící systém musí být dodány jako nové

a nepoužité; dodání repasovaných prvků, prvků z výstav či jakékoliv demoverze není přípustné. Prvky a tím i celý systém budou dodány prosty jakýchkoliv nevypořádaných práv třetích osob.

...

5. Předmětem této smlouvy je rovněž **závazek Dodavatele provádět či zajistit záruční servis dodaného systému včetně veškerých jeho prvků, součástí a příslušenství (tedy včetně software) včetně pravidelných servisních prohlídek, kontrol a revizí předepsaných výrobcem/ci dodaného systému, zajišťující řádnou funkci dodaného systému včetně veškerých jeho prvků, součástí a příslušenství (přičemž výraz "zajistit" znamená provést veškeré nutné a vhodné úkony či jiné kroky, byť by jejich uskutečnění bylo spojeno s vynaložením nákladů, nebo naopak se zdržet určitého jednání, v rozsahu povoleném příslušným právními předpisy tak, aby bylo dosaženo určitého výsledku)** v rozsahu dle této Smlouvy.

   5.1. úplné, řádné a bezvadné provádění komplexního záručního servisu (full service) celého implementovaného systému včetně veškerých jeho součástí a příslušenství po dobu 24 měsíců ode dne uvedení implementovaného systému včetně veškerých jeho součástí a příslušenství do plného provozu v rozsahu dle této Smlouvy;

...

1. Dodavatel garantuje, že **předmět této smlouvy má vlastnosti a bude fungovat v souladu s podmínkami dle této Smlouvy a zavazuje se odstranit** vady Díla, jež bude mít v době jeho předání zadavateli, a dále **vady, které se vyskytnou v průběhu záruční doby.**
2. Délka záruční doby dodaného systému včetně veškerých jeho součástí a příslušenství (tedy včetně software) je podle § 2113 ObčZ 24 měsíců ode dne podpisu Protokolu o předání a převzetí dodaného systému včetně veškerých jeho součástí a příslušenství (tedy včetně software) Objednatelem.
3. **Záruka se vztahuje na všechny části předmětu plnění včetně jeho příslušenství a dále na funkčnost předmětu plnění, jakož i na jeho vlastnosti, definované touto Smlouvou.**
4. **Veškeré vady dodaného systému včetně veškerých jeho součástí a příslušenství (tedy včetně software), které se vyskytnou v záruční době, je Dodavatel povinen bezplatně odstranit bez zbytečného odkladu po jejich oznámení Objednatelem,** není-li v příloze č.1 této Smlouvy s názvem TECHNICKÁ SPECIFIKACE stanoveno jinak.
5. Dodavatel odpovídá Objednateli za případnou škodu, která mu vznikne z titulu neodstranění vady na předmětu plnění ve sjednaném termínu.“

Z výše uvedeného má zadavatel za prokázané, že rozsah komplexního záručního servisu (full service) dodaného systému i podmínky jeho provádění jednoznačně vymezil v souladu s § 36 Zákona tak, že jeho předmětem je:

- **Provádění či zajištění záručního servisu dodaného systému,**
- **provádění či zajištění záručního servisu všech prvků dodaného systému,**
- **provádění či zajištění záručního servisu všech součástí dodaného systému,**
- **provádění či zajištění záručního servisu veškerého příslušenství dodaného systému,**
- **provádění či zajištění záručního servisu veškerého dodaného software,**
- **provádění či zajištění pravidelných servisních prohlídek,**

- **provádění či zajištění kontrol a revizí předepsaných výrobcem/ci dodaného systému**

vše výše uvedené tak, že bude zajištěna řádná a úplná funkce dodaného systému včetně veškerých jeho prvků, součástí a příslušenství po dobu 24 měsíců ode dne uvedení implementovaného systému včetně veškerých jeho součástí a příslušenství do plného provozu.

Dodaný systém musí být po tuto dobu plně funkční bez jakéhokoliv zásahu ze strany zadavatele, což zabezpečuje právě komplexní záruční servis (full service).

Vzhledem ke skutečnosti, že zadavatel plně respektuje ustanovení § 36 a § 89 odstavec (5) Zákona a není tedy oprávněn blíže specifikovat požadavky na komplexní záruční servis (full service) aniž by využil údajů jednotlivých konkrétních dodavatelů, vymezil jednoznačně, transparentně a všem dodavatelům shodně rozsah komplexního záručního servisu (full service) dodaného systému i podmínky jeho provádění tak, jak je uvedeno výše.

Dotaz č. 6:

K dokumentu „02 FNB KB - PZK - čistopis z 2_4_2019.pdf" - str. 10 / odst. 6.2.

Zadavatel ve shora označené části zadávací dokumentace uvádí, že způsobilým k účasti v tomto zadávacím řízení je dodavatel, cit.:

„Který v souladu s ustanovením § 79 odstavec (2) písmeno c) Zákona předloží seznam techniků nebo technických útvarů, které se budou podílet na plnění veřejné zakázky, a to zejména těch, které zajišťují kontrolu kvality, bez ohledu na to, zda jde o zaměstnance dodavatele nebo osoby v jiném vztahu k dodavateli (jedná se funkce Projektový manažer • Bezpečnostní architekt • Senior síťový specialista na switching a routing • Senior síťový specialista na Next Generation Firewally • SIEM architekt • SIEM specialista • SIEM analytik • Bezpečnostní specialista na hardening • Auditor kybernetické bezpečnosti • Senior bezpečnostní analytik)".

Současně s tím zadavatel stanovil v dokumentu „01 FNB KB - ZP - čistopis z 4_4_2019.pdf“ ZADÁVACÍ PODMÍNKY / Str. 18 / odst. 11.7.2., že cit.:

„11.7.2. Zadavatel v souladu s ustanovením § 105 odstavec (2) Zákona požaduje, aby zadavatelem dále určené významné činnosti při plnění veřejné zakázky byly plněny přímo vybraným dodavatelem (bez poddodavatelů):

výkony funkce Projektového manažera

výkony funkce Bezpečnostního architekta

výkony funkce Senior síťový specialista na Next Generation Firewally

výkony funkce SIEM architekta

výkony funkce SIEM specialisty

výkony funkce SIEM analytika

výkony funkce Bezpečnostní specialista na hardening

výkony funkce Auditor kybernetické bezpečnosti

výkony funkce Senior bezpečnostní analytik"

Ustanovení § 105 odst. 2 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, umožňuje Zadavateli, aby vymezil, že plnění určité významné činnosti musí být zajištěno přímo vybraným dodavatelem. Zadavatel v tomto případě vymezil činnosti pouze paušální odkazem na pozice osob, které však budou vykonávat cca 2/3 objemu zakázky, aniž by zohlednil konkrétní skutečně významné činnosti. Tím významně omezil možnost zapojení subdodavatelů do plnění, které je však v rámci trhu v obdobných případech s ohledem na dané specializace velmi obvyklé. Dodavatel proto vznáší dotaz, zda Zadavatel může upřesnit, které konkrétní části plnění nemohou být zajištěny subdodavatelsky a které Zadavatel považuje i s ohledem na zvyklosti trhu a zásadu přiměřenosti za významné. Skladba uvedených

pozic zaměstnanců může v důsledku zvýhodnit konkrétního dodavatele.

Odpověď zadavatele:

„Zadavatel uvádí, že v souladu s ustanovením 105 odstavec (2) Zákona vymezil pro zadavatele významné činnosti, které mají být plněny přímo vybraným dodavatelem (tj. bez využití poddodavatele) věcným vymezením, které je obsaženo v odst. 11.7.2. ZADÁVACÍCH PODMÍNEK. Zadavatel přitom vycházel ze svých legitimních požadavků kladených na bezpečnostně infrastrukturní projekt požadovaného rozsahu, s důrazem na vysokou kvalitu plnění.

Zadavatel pak přesto ve vazbě na žádost dále zvážil rozsah omezení poddodávek a pro posílení zásad stanovených v § 6 Zákona zadávací podmínky upravil tak, jak následuje.

Zadavatel ruší dále uvedené znění odstavce 11.7.2. ZADÁVACÍCH PODMÍNEK

„11.7.2. Zadavatel v souladu s ustanovením § 105 odstavec (2) Zákona požaduje, aby zadavatelem dále určené významné činnosti při plnění veřejné zakázky byly plněny přímo vybraným dodavatelem (bez poddodavatelů):

- výkony funkce Projektového manažera – je odpovědný za řízení zdrojů na projektu, jejich koordinaci, dodání jednotlivých výstupů projektu dle stanovených milníků;
- výkony funkce Bezpečnostního architekta – je odpovědný za návrh architektury celého řešení a dohled nad její implementací;
- výkony funkce Senior síťový specialista na Next Generation Firewally – je odpovědný za návrh řešení, segmentaci sítě včetně definice prostupů a ochranu vnějšího perimetru;
- výkony funkce SIEM architekta – je odpovědný za návrh SIEM řešení, včetně identifikace informačních zdrojů, jejich připojení a definici procesů okolo zpracování výstupů ze SIEMu;
- výkony funkce SIEM specialisty – je odpovědný za implementaci SIEM řešení včetně optimalizace výkonu (počet generovaných událostí);
- výkony funkce SIEM analytika – je odpovědný za analytické práce před nasazením SIEMu, identifikace datových zdrojů;
- výkony funkce Bezpečnostní specialista na hardening – je odpovědný za přípravu hardeningových politik dle jednotlivých platforem, jejich nasazení v provozním prostředí a ověření nastavení formou skeneru zranitelností;
- výkony funkce Auditor kybernetické bezpečnosti – je odpovědný za interní audit dle zákonu 181/2014 Sb. Zákon o kybernetické bezpečnosti a ISO/IEC 27001 a příprava na certifikaci dle ISO/IEC 27001;
- výkony funkce Senior bezpečnostní analytik – Senior bezpečnostní analytik – je odpovědný za analýzu současného stavu informační bezpečnosti, identifikaci a ohodnocení aktiv, hrozeb a zranitelností, Návrh a implementaci bezpečnostních opatření pro získání certifikace dle ISO/IEC 27001.

Účastník předloží v nabídce k zákazu poddodávek čestné prohlášení, které bude podepsáno oprávněnou osobou účastníka v souladu se způsobem jednání právnické či fyzické osoby podle občanského zákoníku a způsobu jednání podle výpisu z obchodního rejstříku.“

a nahrazuje jej novým zněním odstavce 11.7.2. ZADÁVACÍCH PODMÍNEK takto:

„11.7.2. Zadavatel v souladu s ustanovením § 105 odstavec (2) Zákona požaduje,

aby zadavatelem dále určené významné činnosti při plnění veřejné zakázky byly plněny přímo vybraným dodavatelem (bez poddodavatelů).

U výkonů funkce Projektového manažera se jedná o tyto činnosti:

- **Řízení zdrojů na projektu pro Zvýšení kybernetické bezpečnosti ve FN Brno,**
- **koordinace zdrojů na projektu pro Zvýšení kybernetické bezpečnosti ve FN Brno,**
- **předávání jednotlivých výstupů projektu pro Zvýšení kybernetické bezpečnosti ve FN Brno dle stanovených milníků.**

U výkonů funkce Bezpečnostního architekta se jedná o tyto činnosti:

- **návrh architektury celého řešení projektu pro Zvýšení kybernetické bezpečnosti ve FN Brno,**
- **dohled nad implementací architektury celého řešení projektu pro Zvýšení kybernetické bezpečnosti ve FN Brno.**

U výkonů funkce Senior síťový specialista na Next Generation Firewally se jedná o tyto činnosti:

- **návrh řešení,**
- **návrh segmentace sítě včetně definice prostupů,**
- **návrh ochrany vnějšího perimetru.**

U výkonů funkce SIEM architekta se jedná o tyto činnosti:

- **návrh SIEM řešení,**
- **identifikace informačních zdrojů, jejich připojení**
- **definici procesů okolo zpracování výstupů ze SIEMu.**

U výkonů funkce Bezpečnostní specialista na hardening se jedná o tyto činnosti:

- **přípravu hardeningových politik dle jednotlivých platforem**
- **nasazení hardeningových politik dle jednotlivých platforem v provozním prostředí,**
- **ověření nastavení hardeningových politik dle jednotlivých platforem formou skeneru zranitelností.**

U výkonů funkce Auditor kybernetické bezpečnosti se jedná o tyto činnosti:

- **provedení interního auditu dle zákona 181/2014 Sb. Zákon o kybernetické bezpečnosti a ISO/IEC 27001,**
- **zpracování přípravy projektu pro Zvýšení kybernetické bezpečnosti ve FN Brno na certifikaci dle ISO/IEC 27001.**

U výkonů funkce Senior bezpečnostní analytik se jedná o tyto činnosti:

- **analýza současného stavu informační bezpečnosti,**
- **identifikace a ohodnocení aktiv, hrozeb a zranitelností,**
- **návrh a implementace bezpečnostních opatření pro získání certifikace dle ISO/IEC 27001.**

Na jiné, než výše uvedené významné činnosti při plnění veřejné zakázky, se tento požadavek zadavatele nevztahuje.

Účastník předloží v nabídce k zákazu poddodávek čestné prohlášení, které bude podepsáno oprávněnou osobou účastníka v souladu se způsobem jednání právnické či fyzické osoby podle občanského zákoníku a způsobu jednání podle

výpisu z obchodního rejstříku.“

Zadavatel dále v odstavci 6.2. POŽADAVKŮ ZADAVATELŮ NA KVALIFIKACI ruší znění pododstavce 6.2.2.

„6.2.2. Zadavatel v souladu s ustanovením § 73 odstavec (6) písmeno b) Zákona stanovuje minimální úroveň pro splnění tohoto kritéria technické kvalifikace vzhledem ke složitosti a rozsahu předmětu této veřejné zakázky takto:

a)	Projektový manažer	minimálně 2 osoby;
b)	Bezpečnostní architekt	minimálně 1 osoba;
c)	Senior síťový specialista na switching a routing	minimálně 3 osoby;
d)	Senior síťový specialista na Next Generation Firewally	minimálně 3 osoby;
e)	SIEM architekt	minimálně 1 osoba;
f)	SIEM specialista	minimálně 2 osoby;
g)	SIEM analytik	minimálně 1 osoba;
h)	Bezpečnostní specialista na hardening	minimálně 1 osoba;
i)	Auditor kybernetické bezpečnosti	minimálně 2 osoby;
j)	Senior bezpečnostní analytik	minimálně 1 osoba.

a nahrazuje jej novým zněním pododstavce 6.2.2. takto:

„6.2.2. Zadavatel v souladu s ustanovením § 73 odstavec (6) písmeno b) Zákona stanovuje minimální úroveň pro splnění tohoto kritéria technické kvalifikace vzhledem ke složitosti a rozsahu předmětu této veřejné zakázky takto:

a)	**Projektový manažer**	**minimálně 1 osoba;**
b)	**Bezpečnostní architekt**	**minimálně 1 osoba;**
c)	**Senior síťový specialista na switching a routing**	**minimálně 1 osoba;**
d)	**Senior síťový specialista na Next Generation Firewally**	**minimálně 1 osoba;**
e)	**SIEM architekt**	**minimálně 1 osoba;**
f)	**SIEM specialista**	**minimálně 1 osoba;**
g)	**SIEM analytik**	**minimálně 1 osoba;**
h)	**Bezpečnostní specialista na hardening**	**minimálně 1 osoba;**
i)	**Auditor kybernetické bezpečnosti**	**minimálně 1 osoba;**
j)	**Senior bezpečnostní analytik**	**minimálně 1 osoba.“**

Příloha č.3 Kupní smlouvy, kterou uchazeči doloží jako součást své nabídky, bude doplněna pouze v rozsahu nového znění pododstavce 6.2.2.

Tabulka č.5 s názvem „Seznam dokladů k prokázání splnění kvalifikace“, bude doplněna pouze v rozsahu nového znění pododstavce 6.2.2.

Tabulka č.7 s názvem „Realizační tým“, bude doplněna pouze v rozsahu nového znění pododstavce 6.2.2.

Dotaz č. 7:

Zadavatel v kapitole 11.8.7. Zadávací dokumentace požaduje předložení osvědčení o Gold partnerství v 8 různých úrovních. Dodavatel se touto cestou dotazuje na opodstatněnost tohoto požadavku, neboť se domnívá, že tento požadavek je nepřiměřený a může být potenciální diskriminační. Partnerství v takovémto rozsahu na úrovni Gold vylučuje z možné účasti další potenciální zájemce, kteří by byli jinak schopni

veřejnou zakázku realizovat. Dodavatel proto žádá Zadavatele o úpravu tohoto požadavku v rozsahu, v jakém jsou dané certifikáty relevantní a obvyklé vzhledem k povaze tohoto výběrového řízení.

Odpověď zadavatele:

Gold partnerství garantuje vysokou kvalitu a odbornost dodavatele. Součástí projektu pro Zvýšení kybernetické bezpečnosti ve FN Brno je (mimo jiného) rovněž dodávka a nasazení Microsoft produktů a souvisejících implementačních prací, jako například výstavba PKI infrastruktury, různé integrační práce.

Proto je zadavatel přesvědčen, že tento požadavek není ve vztahu k předmětu veřejné zakázky požadavkem diskriminačním.

Navíc se jedná o otevřené řízení v nadlimitním režimu, které je otevřené v rámci všech členských států EU a i proto tento požadavek zadavatele nelze označit za jakkoliv diskriminační a zadavatel na něm i nadále trvá.

Dotaz č. 8:

Zadavatel v kapitole 6.3.2., bodě d), e), f), Kvalifikační dokumentace požaduje „Expertní certifikace na poptávané technologie“. Dodavatel disponuje různými úrovněmi certifikovaných techniků/certifikací. Mohl by Zadavatel specifikovat přesněji tento požadavek? (podobně jako je tomu např. v bodě a) Prince 2 nebo ekvivalentní, bodě c) – certifikace CCNA, CCNP či v bodě j) - CISSP)

Odpověď zadavatele:

Dodavatel dle nabízených technologií musí disponovat expertními kompetencemi, které je nutné prokázat expertními certifikacemi, přičemž za expertní certifikaci se považuje:

- **Next generation firewall na úrovni NSE6 (Fortinet), CCSE (CheckPoint), CCNP Security (Cisco),**
- **SIEM na úrovni ArcSight Certified Integrator/Administrator (ACIA), IBM Certified Deployment Professional, RSA NetWitness® Logs & Network Certified Administrator.**

Dotaz č. 9:

Dotazy ke kvalifikaci

V rámci požadavků technické kvalifikace zadavatel požaduje u role Auditor kybernetické bezpečnosti (2 osoby) doložit mimo jiné certifikaci CISA a akreditaci Auditor ZKB. Ze zadání není jasné, zda zadavatel požaduje, aby každá z osob v roli Auditora kybernetické bezpečnosti disponovala certifikátem CISA a akreditací Auditor ZKB současně nebo zda postačuje, aby jedna osoba v roli Auditora kybernetické bezpečnosti disponovala certifikací CISA a druhá v téže roli akreditací Auditor ZKB. Může zadavatel vysvětlit, jak je požadavek míněn?

Odpověď zadavatele:

Zadavatel požaduje, aby každá z osob v roli Auditora kybernetické bezpečnosti disponovala certifikátem CISA a akreditací Auditor ZKB současně.

Dotaz č. 10:

Dotazy ke kapitolám 1 a 14 (TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY)

Z textu není zcela jasné, zda předmětem dodávky je i zajištění organizace, která provede certifikaci dle ISO 27001 (certifikaci dle IS027000 považujeme za překlep (?)) nebo součástí dodávky je jen asistence v rámci 1 a 2 stupně certifikačního auditu?

Odpověď zadavatele:

Předmětem dodávky je jen příprava k certifikaci dle ISO 27001. Zadavatel očekává aktivní spoluúčast dodavatele na certifikačním procesu.

Dotaz č. 11:

Vzhledem k tomu, že v zadání k provedení analýzy rizik je i požadavek souladu s VyKB je nutné pro nacenění znát alespoň rámcově počet primárních a podpůrných aktiv, což má podstatný vliv na rozsah a pracnost analýzy rizik a následný systém řízení rizik. Může zadavatel tyto údaje doplnit a upřesnit?

Odpověď zadavatele:

Od vybraného dodavatele zadavatel požaduje v analýze rizik identifikaci primárních i podpůrných aktiv. Zadavatel předpokládá minimální počet 80 primárních aktiv a 250 podpůrných aktiv.

Dotaz č. 12:

Jeden z požadavků na zpracování dokumentace na str. 3 je: „Organizace bezpečnosti práce" což je termín z oblasti BOZP (bezpečnost a ochrana zdraví při práci), neměl zadavatel na mysli spíše „Systém řízení bezpečnosti informací"? Může zadavatel upřesnit, co je míněno požadavkem „Organizace bezpečnosti práce"?

Odpověď zadavatele:

Zadavatel má na mysli se Organizace bezpečnosti informací.

Dotaz č. 13:

Obecně struktura požadované dokumentace neodpovídá ani požadavkům ISO 27001 (ISMS), respektive její přílohy A, ani zákonu č. 181 /2014 Sb. (ZoKB), respektive vyhlášce č. 81 /2018 Sb. (VyKB). Je možné, aby dodavatel v rámci návrhu systému bezpečnostní dokumentace navrhl jinou strukturu, která by lépe vyhovovala oběma normám a usnadnila tak i následující certifikační audit?

Odpověď zadavatele:

Od vybraného dodavatele zadavatel požaduje dodat strukturu dokumentace v minimálním rozsahu dle původní specifikace. Dodavatel může tuto strukturu rozšířit tak, aby splnila požadavky norem a ZoKB.

Dotaz č. 14:

K dokumentu „03 FNB KB - TS - čistopis z 2_4_2019.pdf“ - TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY, kapitola 17. LAN a WiFi instrastruktura, odstavec „WiFi síť“ (str. 149-151) - k dokumentu Dle přílohy „06 FNB KB - TAB.2 KLNC - čistopis z 2_4_2019.xlsx“.

Dodavatel vznáší níže uvedený dotaz ke kapitole 17. LAN a WiFi instrastrukturav části WiFi síť (str. 149 – 151) dokumentu „TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY". Dle názoru dodavatele není v této části technická dokumentace zpracována v dostatečné míře tak, aby bylo možné připravit nabídku do veřejné zakázky.

Dle přílohy „06 FNB KB - TAB.2 KLNC - čistopis z 2_4_2019.xlsx“ požaduje Zadavatel uvést u většiny kategorií „Nabídkovou cenu včetně implementace". Pokud má být předmětem plnění kategorie „LAN a WiFi infrastruktura" i montáž WiFi přístupových bodů a instalace nezbytné kabeláže, pro správný návrh a nacenění tímto žádáme Zadavatele o poskytnutí přesných informací k umístění přístupových bodů ve formě výstupů z provedené WiFi Site Survey analýzy. Dále požadujeme upřesnění typu metalické kabeláže (stíněná / nestíněná, kategorie) a požadovaný způsob zakončení kabeláže na straně přístupových bodů (zásuvka s RJ45 keystone nebo krimpovací konektor RJ45 na kabelu).

Případně žádáme Zadavatele o potvrzení, že montáž WiFi přístupových bodů a instalace nezbytné kabeláže není požadována jako součást předmětu plnění.

Pro srovnání dále dodavatel uvádí, že Zadavatel měl v roce 2015 vypsánu veřejnou zakázku: „Rozvoj WiFi infrastruktury ve FN Brno" (viz https://ezak.fnbrno.cz/contract display 880.html). kde je realizace WiFi sítě svým rozsahem v podstatě totožná s aktuální veřejnou zakázkou (675 vs. 673 ks přístupových bodů).

Součástí zadávací dokumentace pro tuto předchozí veřejnou zakázku byla detailní technická specifikace, včetně studie proveditelnosti a WiFi Site Survey s výkresy s umístěním všech 673 ks WiFi přístupových bodů – rozsah dokumentace 230 stran pro PMDV, 145 stran pro PDM, 42 stran pro PRM + 26 stran technických požadavků na dodaná zařízení.

Odpověď zadavatele:

Zadavatel v rámci posílení dodržení zásad, stanovených v § 6 Zákona, z předmětu zadávané veřejné zakázky vypouští v kapitole 17. LAN a WiFi instrastruktura celou část s názvem „WiFi síť“ (str. 149–151) v dokumentu „TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY".

Dotaz č. 15:

S ohledem na rozsah veřejné zakázky a značnou náročnost přípravy nabídky rovněž vznášíme dotaz, zda by bylo možné lhůtu pro podání nabídek prodloužit na nejméně dvojnásobnou délku s ohledem na ustanovení § 57 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, kde je lhůta pro podání nabídek v délce 30 dní stanovena jako minimální s tím, že Zadavatel musí vždy ad hoc zvážit i s ohledem na specifika zadání a zvyklosti na daném trhu, zda je minimální lhůta dostatečná a zda naplňuje zásadu přiměřenosti ve smyslu § 6 citovaného zákona.

Opět pro srovnání uvádíme, že ve veřejné zakázce „Rozvoj WiFi infrastruktury ve FN Brno" z roku 2015 byla Zadavatelem lhůta pro podání nabídek stanovena v rozmezí 1. července - 18. srpna 2015, přičemž šlo o pouhou část plnění ve srovnání s aktuální veřejnou zakázkou. Mimo to byla součástí zadání detailní technická specifikace, která dodavatelům umožnila lépe zpracovat své nabídky.

Odpověď zadavatele:

Zadavatel lhůtu pro podání nabídky prodlužuje – viz. Informace 7.

Dotaz č. 16:

K dokumentu „01 FNB KB - ZP - čistopis z 4_4_2019.pdf" - str. 20, odstavec 11.8.7.

Zadavatel ve shora označené části zadávací dokumentace požaduje, aby byl vybraný dodavatel partnerem společnosti Microsoft. Vybraný dodavatel je povinen před podpisem smlouvy předložit zadavateli prostou platnou kopii osvědčení o partnerství vybraného dodavatele se společnosti Microsoft, a to na úrovni:

- Gold Application Development,
- Gold Cloud Platform,
- Gold Cloud Productivity,
- Gold Collaboration and Content,
- Gold Datacenter,
- Gold Enterprise Resource Planning,
- Gold Messaging,
- Gold Small and Midmarket Cloud Solutions.

Dodavatel vznáší dotaz, zda je s ohledem na předmět veřejné zakázky dostačující, pokud předloží Silver nebo Gold Datacenter, kterým lze zajistit splnění téhož cíle. Požadavek na partnerství se společností Microsoft na nejvyšší úrovni partnerství v oblastech, které nesouvisí s předmětem veřejné zakázky může v důsledku nedůvodně omezit hospodářskou soutěž a může být považován za diskriminační, když předmětná část plnění je ve vztahu k celkovému plnění marginální. Mimo to společnost Microsoft není jediným a ani klíčovým dodavatelem technologií kybernetické bezpečnosti.

Odpověď zadavatele:

Viz. odpověď na dotaz číslo 7.

Dotaz č. 17:

Dotazy ke kapitolám 9, 10 a 12 (TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ

ZAKÁZKY)

Musí být řešení ochrany proti DDoS útokům v režimu vysoké dostupnosti? V technických požadavcích na hardware DDoS ochrany je uvedena pouze "Možnost nasazení páru zařízení (aktivní - záložní)", ale v úvodu kapitoly 9 je věta, která vyžaduje redundanci - "Nabízené řešení musí být od jednoho výrobce a realizované v režimu vysoké dostupnosti."

Odpověď zadavatele:

Systém musí splňovat vysokou dostupnost, to je automatické přepnutí na záložní řešení.

Dotaz č. 18:

Rozporuplné požadavky na DDoS řešení na stranách 25 a 31 jsou i v oblasti rozhraní — na str. 25 je uvedeno „Rozhraní: 4x 1 0 GBASE-T / SFP+ a možnost rozšířeni, 8x 1 GBASE-T RJ45 — internal fail-close for SFP and XFP ports“. Na straně 31 jsou požadavky následující: „Minimálně 8x 1 Gbps metalické rozhraní“ a „Minimálně 2x 10Gbps SFP+ rozhráni”. Žádáme zadavatele o potvrzení, které parametry jsou směrodatné pro návrh řešení. Dále žádáme o zdůvodnění požadavku na 8x 1 GBASE-T RJ45 rozhraní. Máme v úmyslu nabídnout plně vyhovující zařízení s 6x 1 GBASE-T RJ45 rozhraním a zadavatelem požadovaná hodnota by mohla směřovat na konkrétní zařízení jednoho výrobce.

Odpověď zadavatele:

Správný počet portů je:

a. Minimálně 2x 10Gbps SFP+ rozhraní s hardware bypass

b. Minimálně 6x 1Gbps metalické rozhraní s hardware bypass

c. Minimálně 2x 1Gbps metalické rozhraní - management

Dotaz č. 19:

V dokumentu jsou rozporuplné požadavky na DDoS řešení na stranách 25 a 31, tyto požadavky vedou ke zcela odlišným řešením. Např. jsou uvedeny 2 rozdílné požadavky na minimální hodnotu paketů za vteřinu. V tabulce na str. 25 je požadováno 10 000 000 pps, v tabulce na str. 31 už je to jen 5 500 000 pps (?).Také požadavek na propustnost a počet současných spojení řešení DDoS ochrany je uveden ve dvou různých hodnotách - v jedné tabulce je 35 Gbps a ve druhé jen 1 Gbps při DDoS útocích. Totéž k počtu současných spojení — 4 mil. vs. 3 mil. Žádáme o vysvětlení, která hraniční hodnota je pro návrh řešení směrodatná.

Odpověď zadavatele:

Správné minimální hodnoty jsou:

a. počet paketů za vteřinu je 5 500 000 pps

b. požadavek na propustnost 6 Gbits

c. počet současných spojení 3 mil.

Dotaz č. 20:

Musí DDoS řešení podporovat Jumbo rámce? Jumbo rámce jsou podporovány až u modelu vyšší řady. Toto nevím — ve specifikaci je to jednoznačně požadováno.

Odpověď zadavatele:

Zadavatelem není požadována podpora jumbo rámců.

Dotaz č. 21:

Můžete sdělit od jakého výrobce je stávající řešení perimetrového a interního firewallu, jaké funkce používá a jak obsáhlá je bezpečnostní politika (kolik bezpečnostních a NAT pravidel obsahuje)?

Odpověď zadavatele:

Podrobnosti o stávajícím Firewallu, včetně všech konfigurací budou sděleny vybranému dodavateli po podpisu NDA.

Dotaz č. 22:

Pro virtuální interní firewall předpokládáme využití stávající virtualizační platformy VMware. Z důvodu přesné specifikace licencí pro virtuální firewall potřebujeme znát přesný počet CPU socketů na VMware NSX. Jedná se o 48 CPU socketů nebo jde o 48 CPU core?

Odpověď zadavatele:

Nabízené řešení musí licenčně podporovat ESX prostředí pro 48 CPU soketů.

Dotaz č. 23:

V požadavcích v kapitole 10. Web aplikační firewall je požadavek na 48GB RAM Žádáme zadavatele o zdůvodnění, proč požaduje tuto konkrétní hodnotu ? V našem návrhu řešení chceme nabídnout zařízení, splňující všechny ostatní parametry, ale s 32 GB RAM. Máme zato, že zadavatelem uvedená hodnota by mohla směřovat na konkrétní zařízení jednoho výrobce.

Odpověď zadavatele:

Ano, může být nabídnuto řešení s menší pamětí za předpokladu, že všechny požadované funkcionality budou nasazeny. Zároveň zadavatel upravuje parametr Počet současných L4 spojení na 20M.

Dotaz č. 24:

K webovému aplikačnímu firewallu musí být možné aktivovat následující funkce na jedné HW platformě: L4-7 loadbalancing, ICSA certifikovaný Web aplikační firewall, ICSA certifikovaný síťový firewall, Autorizace a autentizace aplikací, SSL VPN, DNS služby a DNS firewall. Které z těchto funkcí musí být součástí dodávky? Mezi kolik backend serverů bude provoz maximálně rozvažován? Ptáme se z důvodu použití vhodné licence pro loadbalancing a ostatní služby.

Odpověď zadavatele:

Požadovány jsou všechny vyjmenované funkcionality. Požadované je řešení bez limitace backend serverů.

Dotaz č. 25:

Předpokládáme, že součástí dodávky webového aplikačního firewallu musí být funkce autentizační gateway a řízení uživatelských přístupů. Pro kolik současně připojených uživatelů máme řešení licencovat?

Odpověď zadavatele:

Pokud je nutné ve Vašem technickém řešení jakékoliv autentizační služby licencovat na uživatele, tak k dnešnímu dni registrujeme 12500 uživatelských účtů a odhadujeme, že při běžném pracovním dni máme 4500 souběžné připojených uživatelů. Tento počet se při velikosti provozu FN Brno neustále navyšuje, hlavně z pohledu dodavatelů a studentů LF. Proto je nutné zabezpečit provoz pro min. 5000 souběžné připojených uživatelů.

Dotaz č. 26:

K dokumentu „02 FNB KB - PZK - čistopis z 2_4_2019.pdf kapitola 6.1.2

Zadavatel požaduje prokázání technické kvalifikace v následujícím rozsahu, cit.:

„Minimální úroveň pro splnění tohoto kritéria technické kvalifikace prokáže dodavatel referencemi realizovaných významných dodávek nebo významných služeb obdobného charakteru jako je předmět této veřejné zakázky. Minimální úroveň pro splnění tohoto kritéria technické kvalifikace stanovuje zadavatel níže uvedenými kritérii typů významných dodávek nebo významných služeb obdobného charakteru jako je předmět

této veřejné zakázky, řádně poskytnutých příjemci služby (objednateli) za posledních 3 roky před zahájením tohoto zadávacího řízení takto:

- *Typ A - minimálně tři významné zakázky typu „A“ na dodávku a implementaci perimetrového nebo interního NG Firewallu a DDoS ochrany v minimálním finančním objemu 5 mil. Kč bez DPH pro každou jednotlivou významnou zakázku typu „A “. Celková smluvní cena zakázek typu „A“ musí činit alespoň 20 mil. Kč bez DPH.*
- *Typ B - minimálně tři významné zakázky typu „B“ na dodávku a implementaci nástroje pro sběr a korelaci událostí a logů v minimálním finančním objemu 5 mil. Kč bez DPH pro každou jednotlivou významnou zakázku typu „B“. Celková smluvní cena zakázek typu „B“ musí činit alespoň 20 mil. Kč bez DPH.*
- *Typ C - minimálně tři významné zakázky typu „C“ na dodávku a implementaci nástroje pro management zranitelností a hardeningových politik v minimálním finančním objemu 1,5 mil. Kč bez DPH pro každou jednotlivou významnou zakázku typu „C“. Celková smluvní cena zakázek typu „C“ musí činit alespoň 6 mil. Kč bez DPH.*
- *Typ D - alespoň jedna významná zakázka typu „D“ na dodávku a implementaci nástroje Web aplikační firewall v minimálním finančním objemu 2 mil. Kč bez DPH.*
- *Typ E - alespoň jedna významná zakázka typu „E“ na dodávku a implementaci nástroje pro ochranu koncových stanic v minimálním finančním objemu 2 mil. Kč bez DPH.*
- *Typ F - alespoň jedna významná zakázka typu „F“ na dodávku a implementaci systému pro analýzu a správu rizik v minimálním finančním objemu 4 mil. Kč bez DPH.*
- *Typ G - minimálně tři významné zakázky typu „G“ na dodávku analytických prací v oblasti bezpečnosti (analýza rizik, analýza hrozeb a příprava na certifikaci ISO/IEC 27001) v minimálním celkovém finančním objemu 1 mil. Kč bez DPH.*
- *Typ H - alespoň jedna významná zakázka typu „H“ na dodávku procesů podpory a servicedesk dle standardu ITIL v minimálním finančním objemu 700 tis. Kč bez DPH.*
- *Typ I - minimálně tři významné zakázky typu „1“ na dodávku SLA podpory dodavatele v minimálním finančním objemu 1 mil. Kč bez DPH pro každou jednotlivou významnou zakázku typu „I“. Celková smluvní cena zakázek typu „1“ musí činit alespoň 4 mil. Kč bez DPH.*
- *Typ J - minimálně jedna významná zakázka typu „J“ na dodávku LAN nebo WiFi infrastruktury v minimálním finančním objemu 10 mil. Kč bez DPH a minimálně dvě významné zakázky typu „J“ na dodávku LAN nebo WiFi infrastruktury v minimálním finančním objemu 4 mil. Kč bez DPH pro každou jednotlivou významnou zakázku typu „J“, Celková smluvní cena zakázek typu „J“ musí činit alespoň 18 mil. Kč bez DPH.*

b) Realizované zakázky, kterými dodavatel prokazuje splnění technických požadavků, musí být v době prokázání řádně dokončeny a předány objednateli. Výjimkou jsou významné zakázky „Typu I“ kde může dodavatel doložit probíhající plnění dle platné a účinné smlouvy, u kterého se pro účely prokázání technické kvalifikace bude považovat za rozhodný rozsah významné zakázky realizovaný v době podání žádosti o účast.“

Jednotlivé požadavky na reference, resp. jejich výše nijak nereflektuje předpokládaný objem činností v rámci dané veřejné zakázky, tedy např. reference typu A musí dosahovat v součtu nejméně 20 mil. Kč DPH, zatímco reference typu I postačuje v součtu ve výši 4 mil. Kč bez DPH. Vzájemná hodnota poměru služeb v rámci veřejné

zakázky mezi službami typu A a službami typu I však nepředstavuje pětinásobný rozdíl. Dodavatel proto žádá zadavatele o vysvětlení, z jakého důvodu jsou referenční služby v tak významném vzájemném nepoměru (nejen mezi typem A a I, ale i ostatní) a vznáší dotaz, zda zadavatel připustí celkové snížení požadovaných objemů referencí tak, aby byly přiměřené hodnotě jednotlivých oblastí veřejné zakázky. Takto zadavatelem nastavená technická kvalifikace může v důsledku v této veřejné zakázce zvýhodňovat určitý typ dodavatele, aniž by to bylo odůvodněno předmětem veřejné zakázky či potřebami zadavatele.

Odpověď zadavatele:

U služeb typu C snižuje Zadavatel požadavky na významné realizované referenční zakázky za uplynulé tři roky takto:

„Minimálně tři významné zakázky v minimálním finančním objemu 1,3 mil. Kč bez DPH pro každou jednotlivou významnou zakázku typu „C“. Celková smluvní cena zakázek typu „C“ musí činit alespoň 4 mil. Kč bez DPH.“

U ostatních typů služeb Zadavatel potvrzuje oprávněnost požadavku na výši referenčních zakázek

Dotaz č. 27:

K dokumentu „02 FNB KB - PZK - čistopis z 2_4_2019.pdf" kapitola 6.3.2. písm. c)

Zadavatel požaduje prokázání technické kvalifikace v následujícím rozsahu, cit.:

- *„Senior síťový specialista na switching a routing*
- *zaměstnanec účastníka (v návaznosti na zákaz poddodávek)*
- *minimální úroveň vzdělání: VŠ magisterského stupně;*
- *certifikace: CCNA, CCNP;*
- *délka odborné praxe alespoň 5 let v oboru IT;*
- *reference alespoň 5 projektů v oblasti IT bezpečnosti, se zaměřením na switching a routing, na kterých působil ve funkci Senior síťový specialista“*

Certifikace CCNA a CCNP představuje certifikaci konkrétního výrobce (Cisco Systems). Dodavatel vznáší dotazy:

1. zda zadavatel požaduje u daného specialisty vždy certifikaci CCNA a CCNP (tj. ve smyslu konjunkce, kdy musí mít specialista certifikaci nižší i vyšší), anebo zda dostačuje CCNA (tj. ve smyslu disjunkce, kdy postačuje i nižší certifikace)
2. zda zadavatele akceptuje i jiné certifikace, tedy zda lze chápat tento požadavek tak, že požadavek je naplněn vždy, když daný specialista prokáže expertní certifikaci na dodávané technologie?

Odpověď zadavatele:

CCNA je již obsaženo v CCNP. Za splnění se považuje, když daný specialista prokáže expertní certifikaci na dodávané technologie.

Dotaz č. 28:

K dokumentu „02 FNB KB - PZK - čistopis z 2_4_2019.pdf" kapitola 6.3.2. písm. h)

Zadavatel požaduje prokázání technické kvalifikace v následujícím rozsahu, cit.:

„Bezpečnostní specialista na hardening

zaměstnanec účastníka (v návaznosti na zákaz poddodávek)

minimální úroveň vzdělání: VŠ;

certifikace: Expertní certifikace na VMS technologii;

délka odborné praxe alespoň 3 let v oboru IT;

reference alespoň 5 projektů v oblasti IT bezpečnosti, se zaměřením na poptávané technologii skeneru zranitelnosti a hardening“

Dodavatel tímto žádá zadavatele o vysvětlení, co znamená pojem „Expertní certifikace na VMS technologie" – jaký dokument by měl dodavatel předložit?

Odpověď zadavatele:

Za splnění bude zadavatelem považováno, když daný specialista prokáže expertní certifikaci na dodávané technologie.

Dotaz č. 29:

Dotaz ke kapitole 11 (TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY)

V tabulce Šifrování pevných disků jsou uvedeny požadavky na operační systémy klientů. Figuruje zde i Linux, ačkoli v ostatních tabulkách pro ostatní komponenty ochrany stanic uveden není. Je skutečně požadována podpora OS Linux pro řešení šifrování disků koncových stanic?

Odpověď zadavatele:

Ano, zadavatelem je požadována podpora OS Linux pro řešení šifrování disků koncových stanic.

Dotaz č. 30:

Dotazy ke kapitolám 15 a 16 (TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY)

V kapitole 15. Service desk systémpožaduje zadavatel dodání Service deskového systému bez jakékoliv konfigurace, procesů, dokumentace, zaškolení, integrace, reportingu, lokalizace? Není jasné, zda zadavatel požaduje také návrh nastavení a vlastní nastavení systému. Tabulka v dokumentu pouze zjišťuje, zda produkt danou vlastnost splňuje nebo ne. Podle našich zkušeností znamená dodání servicedeskového systému obvykle samostatný projekt s významným zapojením zadavatele.

Odpověď zadavatele:

Ano, zadavatel požaduje také návrh nastavení a vlastní nastavení systému.

Dotaz č. 31:

Kapitola 16.3. Implementace PKI zadavatele

Zadavatel uvádí: „Všechny vydávající CA budou mít vydán certifikát z kořenové CA, která bude offline a nebude chráněná HW prostředky.44 Požadavek nechránit takto kořenovou CA považujeme za velmi nestandardní, obvykle se doporučuje chránit HW prostředky všechny CA v hierarchii. U vydávajících CA není žádná ochrana HW prostředky zmíněna. Mají být chráněny HW prostředky vydávající CA?

Odpověď zadavatele:

Kořenová CA má být offline a nemá být chráněna HW prostředky. Zadavatelem tedy není požadována ochrana HW prostředky vydávající CA.

Dotaz č. 32:

Kapitola 16.3. Provozní a bezpečnostní koncept PKI zadavatele

Zadavatel požaduje zpracování dokumentu — cílového konceptu PKI. V rámci konceptu mají být navrženy jednotlivé aspekty PKI a jedním z nich je využiti HSM. Není ale jasné, zda je požadována i dodávka HSM. V dokumentu je HSM zmíněno jen v kapitolách 10. Web aplikační firewall a 1 6.3. Implementace PKI zadavatele. V dokumentu nejsou zmíněny žádné požadované parametry pro HSM. Požaduje zadavatel dodávku HSM? Pokud ano, žádáme o upřesnění konkrétních parametrů HSM.

Odpověď zadavatele:

HSM není součástí předmětu zadávané veřejné zakázky. Řešení však musí být pro implementaci HSM připraveno.

Dotaz č. 33:

Kapitola 16.3. Online zálohování dat certifikační autority

Jaký má zadavatel důvod požadovat zálohování dat CA do databáze MS SQL? Zadavatel požaduje vytvořit systém pro zálohování a obnovu CA databáze do MS SQL databáze – neboli kopírovat data z CA databáze do SQL databáze a následně je odsud zálohovat (předpokládáme, že MS SQL databáze bude zálohována). Microsoft má pro zálohování CA svůj nástroj, který CA nativně podporuje. Z tohoto důvodu tento požadavek považuji za zbytečnou komplikaci. Žádáme zadavatele o vysvětlení.

Odpověď zadavatele:

Pro online zálohování certifikační autority bude implementován systém pro obnovu a zálohování. Pomocí systému budou data CA zálohována do MS SQL databáze. Součástí systému je mechanismus pro obnovu chybějících dat z MS SQL do CA. Do stejné DB budou zálohována data obou CA (pro uživatele a pro infrastrukturu). Součástí systému je publikační modul, který podporuje publikaci dat do CA.

Zadavatel požaduje online extra zálohování do MS SQL, s podporou obnovy jen chybějících dat.

Dotaz č. 34:

V dokumentu Technická specifikace je na straně 20 v kapitole „Workspace One“ uveden požadavek: „Bezpečná centrální distribuce aplikací na koncová zařízení bez možnosti uživatelských změn s řízením přístupů k aplikacím. Doplnění stávající licence VMware WSP One o 1200 uživatelů." V zadání chybí jakákoli specifikace požadované záruky/maintenance pro VMware WSP One. Žádáme uvedení přesné specifikace záruky/maintenance, kterou zadavatel požaduje.

Odpověď zadavatele:

Záruka/maintenance je pro všechny součástí, komponenty stejná, tedy 5 let od akceptace projektu.

Dotaz č. 35:

V dokumentu Technická specifikace je na straně 21 v kapitole „Rozšíření Horizon View" uveden požadavek: „Doplnění licencí Academie pro systém, který zvyšuje dostupnost pro obsluhu systémů tím, že zjednodušuje a zkracuje náhradu porouchaného zařízení na pouhou výměnu bez nutnosti konfigurace a instalace nového zařízení. Současně se tímto řeší i provoz z druhého datového centra v případě výpadku. V rámci projektu bude pořízeno 500 licencí."

V zadání chybí specifikace požadovaného druhu licencí a opět jakákoli specifikace požadované záruky/maintenance pro VMware Horizon View. Žádáme uvedení přesné specifikace licencí a záruky/maintenance, kterou zadavatel požaduje.

Odpověď zadavatele:

Viz. odpověď na dotaz číslo 34.

Dotaz č. 36:

V dokumentu Technická specifikace je na straně 21 v kapitola 6. „Virtualizace sítě, mikrosegmentace" je uveden požadavek na systém pro virtualizaci sítě. V zadání chybí jakákoli specifikace požadované záruky/maintenance pro uvedený systém. Žádáme uvedení přesné specifikace záruky/maintenance, kterou zadavatel požaduje.

Odpověď zadavatele:

Viz. odpověď na dotaz číslo 34.

Dotaz č. 37:

V dokumentu Technická specifikace je na straně 22 v kapitole 7. „Nástroj pro zobrazení a vyhodnocení toků na virtualizované síťové infrastruktuře" uveden požadavek na systém pro zobrazení a vyhodnocení toků na virtualizované síťové infrastruktuře. V

zadání opět chybí jakákoli specifikace požadované záruky/maintenance pro uvedený systém. Žádáme uvedení přesné specifikace záruky/maintenance, kterou zadavatel požaduje.

Odpověď zadavatele:

Viz. odpověď na dotaz číslo 34.

Dotaz č. 38:

V rámci veřejné zakázky je požadováno rozšíření provozované báze VMware systémů. Žádáme o přesnou specifikaci provozovaných systémů a také specifikaci maintenance na provozovanou bázi pro vyloučení veškerých pochybností nejlépe formou licenčního výpisu.

Odpověď zadavatele:

Všechny potřebné informace jsou součástí technické specifikace.

Dotaz č. 39:

V dokumentu Technická specifikace je na straně 22 kapitola 8. „Nástroj pro správu IP adresních prostorů" uveden požadavek na systém pro správu IP adresních prostorů. V zadání opět chybí jakákoli specifikace požadované záruky/maintenance pro uvedený systém. Žádáme uvedení přesné specifikace záruky/maintenance, kterou zadavatel požaduje.

Odpověď zadavatele:

Viz. odpověď na dotaz číslo 34.

Dotaz č. 40:

V dokumentu Technická specifikace je na straně 33 kapitola 10. „Web aplikační firewall" uveden požadavek na web aplikační firewall. V zadání chybí jakákoli specifikace požadované záruky/maintenance pro uvedený systém. Žádáme uvedení přesné specifikace záruky/maintenance, kterou zadavatel požaduje.

Odpověď zadavatele:

Viz. odpověď na dotaz číslo 34.

Dotaz č. 41:

V dokumentu Technická specifikace jsou na straně 73 v kapitole 13 „SIEM - Stanovení množství EPS a velikosti logovacích záznamů - pro výběr SIEM řešení" uvedeny požadavky:

„Dodavatel v kooperaci se zadavatelem a na základě předchozích kroků vypočte množství událostí za sekundu (dále jen EPS). Dodavatel na základě předchozích kroků vypočte velikost logovacích záznamů a tento návrh předloží zadavateli. - Dodaným výstupem bude: textový editor ve formátu .doc/.pdf/, ve kterém bude popsán výpočet a hodnota EPS a velikosti logovacích záznamů."

A dále:

„Komparace SIEM řešení pro podmínky zadavatele Dodavatel na základě informací z předchozích kroků vytvoří porovnání SIEM řešení tak, aby splňovali požadavky a potřeby zadavatele. - Dodaným výstupem bude: textový editor ve formátu .doc/.pdf/.pdf, ve kterém budou porovnána SIEM řešení různých výrobců splňující výše uvedená kritéria. - Dodavatel se zavazuje, že SIEM řešení, které vytvořil pro zadavatele je také schopen implementovat.

Tuto skutečnost dodavatel doloží příslušnými certifikacemi na konkrétní SIEM řešení. - Dodavatel se zavazuje, že informace uvedená v porovnání jsou přesná a reálná."

Uchazeč nerozumí výše uvedeným požadavkům, vzhledem k tomu, že v rámci nabídky do VZ je povinen předložit nabídku na konkrétní SIEM řešení s konkrétně uvedenou cenou bez možnosti dalšího navyšování např. na základě výsledku studie - Stanovení množství EPS. Výše uvedené měl podle názoru uchazeče provést zadavatel před

vypsáním veřejné zakázky. Žádáme o vyškrtnutí výše citovaných částí ze zadávací dokumentace.

Odpověď zadavatele:

Zadavatel děkuje za upozornění, jedná se o chybu při kompletaci této části zadávací dokumentace. Zadavatel potvrzuje vyškrtnutí citované části bez náhrady.

Dotaz č. 42:

V části TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY kapitola 3 Rozšíření optických rozvodů je uveden požadavek:

„Výsledkem musí být realizace bezpečného a plně funkčního celku s vysokou dostupností, potvrzeného akceptačním protokolem jako výsledkem jeho testovacího provozu. Související stavební práce a dodávky spojené s realizací optických rozvodů nejsou předmětem této veřejné zakázky."

Uchazeči není jasné, jak je ošetřena odpovědnost za včasné předání díla, pokud je část prací nezbytných pro realizaci plně funkčního celku vyjmuta mimo odpovědnost uchazeče. Jakým způsobem bude ošetřena odpovědnost zadavatele za provedení nezbytných stavebních prací včas a v termínu?

Odpověď zadavatele:

Aby zadavatel mohl zajistit přípravu projektových prací pro realizaci datových i napájecích rozvodů, budou tyto práce a dodávky řešeny samostatně a zadavatel je vypouští z předmětu zadávané veřejné zakázky - viz Informace 6.

Dotaz č. 43:

V dokumentu 04b FNB KB - Servisní smlouva - čistopis z 2_4_2019.pdf zcela chybí příloha č.1. Technická specifikace. Žádáme zadavatele o doplnění této přílohy.

Odpověď zadavatele:

Příloha 1 Servisní Smlouvy – Technická specifikace je záměrně nevyplněna. Vyplní ji Uchazeč podle obsahu jím nabízeného řešení a určí tím seznam servisovaného vybavení a s ním související seznam servisních činností.

Dotaz č. 44:

Dotaz ke kapitole 16

Zadavatel požaduje podporu minimálně těchto certifikačních autorit: Česká pošta, s. p., I.CA a eldentity a. s.

Prosíme o vysvětlení níže uvedeného požadavku na dodání QSCD čipových karet s podporou tří CA s ohledem na neexistenci společné karty, kterou by všichni tři požadovaní poskytovatelé kvalifikovaných služeb podporovali.

V kapitole 16.1. Hybridní karta: contact PKI/contactless EMV dále požaduje dodávku hybridních QSCD čipových karet. Zařízení musí podporovat vytváření kvalifikovaného elektronického podpisu dle nařízení eIDAS a disponuje platnou QSCD certifikací.

Z oficiálního seznamu MV ČR (https://www.mvcr.cz/clanek/seznam-vydavanych-kvalifikovanych-prostredku-pro-vytvareni-elektronickych-podpisu-v-ceske-republice.aspx) vyplývá, že neexistuje jediná společná karta, kterou by všichni tři vyjmenovaní poskytovatelé kvalifikovaných služeb podporovali jako QSCD prostředek.

Odpověď zadavatele:

Postačující jsou autority: Česká pošta, s. p., a eldentity a. s.

Dotaz č. 45:

V zadávací dokumentaci není definována personalizovaná PKI aplikace (její vlastnosti), ani kdo ji má dodat.

Je zajištěn dodavatel personalizované PKI aplikace, nebo Zadavatel požaduje její dodání po Uchazeči?

Má tuto aplikaci dodat Uchazeč? Jestli ANO, jaké má mít vlastnosti?

Odpověď zadavatele:

Ano, PKI aplikace musí mít následující vlastnosti:

Vytváření elektronického podpisu na bázi certifikátů ve formě:

- **kvalifikovaného elektronického podpisu,**
- **zaručeného elektronického podpisu,**
- **uznávaného elektronického podpisu a**
- **jiné formy elektronického podpisu.**

Dvoufaktorovou autentizaci na bázi certifikátů X.509 do PC (prostředí Microsoft AD/Smartcard Logon, webových služeb, VPN, aplikací), možnost uložení certifikátů třetích stran, zabezpečení komunikace na bázi e-mailů (S/MIME, elektronický podpis a šifrování e-mailů), archivaci privátních klíčů v procesech vydávání šifrovacích certifikátů, generování a práce s RSA a ECC klíči v čipu, podpora PUK pro odblokování PIN a QPIN, zablokování PIN a QPIN resp. PUK po opakovaném chybném zadání PIN/QPIN, resp. PUK (konfigurovatelný počet pokusů), podpora změny PIN pomocí standardního logon desktopu MS Windows, od verze Win7.

Čipová karta podporuje získání následného certifikátu prostřednictvím aplikace pro automatizovanou obnovu certifikátů. Tato služba je napojena na akreditovaného poskytovatele kvalifikovaných služeb.

Ověření původu klíče pro kvalifikovaný podpis podporuje karta na bázi principu kryptogramu vygenerovaného kartou a jeho ověření na serveru akceptované více akreditovanými CA v ČR.

Dotaz č. 46:

Zadavatel požaduje dodat 6500 ks multifunkčních identifikačních karet s podporou PKI, EMV Pure a Mifare.

Má se tedy jednat o hybridní čipovou kartu s kontaktním čipem, bezkontaktním čipem Mifare a plnohodnotným platebním EMV Pure appletem ?

Musí být dodavatel karty, nebo provozovatel certifikován pro platební operace ?

Je požadována dodávka typu hybridních QSCD čipových karet s podporou bezkontaktního čipu s aplikací pro elektronické poukázky a kontaktním čipem s personalizovanou PKI aplikací.

Musí bezkontaktní čip obsahovat aplikaci pro elektronickou poukázku na bázi EMV ?

Odpověď zadavatele:

Ano, jedná se o hybridní kartu. EMV čip bude v budoucnu sloužit pro benefitní systém. Ano, dodavatel nebo příslušný subdodavatel musí být certifikovaný pro personalizaci zabezpečených čipových karet.

Dotaz č. 47:

Prosíme o vysvětlení níže uvedeného požadavku na možnost odblokování QPINu pomocí PUKu, která je v rozporu regulací elDAS, zákonem 297/201 6 Sb. a nařízením Evropského parlamentu a rady (EU) č. 910/2014.

Zadavatel požaduje, že karta musí podporovat dvě oblasti pro uložení kvalifikovaných a nekvalifikovaných certifikátů, přičemž každá oblast má svůj PIN s ohledem na rozlišení pinové politiky.

Dále jsou pod tímto požadavkem uvedeny politiky, které jsou v rozporu s provozováním QSCD prostředku: Karta musí mít dvě oblasti, přičemž každá má svůj PIN a každá musí mít i svůj odblokovací PUK. Z pohledu regulace elDAS i prováděcího zákona 297/2016 Sb. musí být kvalifikovaný prostředek (QSCD) pod výhradní kontrolou uživatele. Splnění zadání by znamenalo, že by správce nebo Help Desk byl schopen PUKem uloženým v

managementu odblokovat QPIN a poté s jeho znalostí neoprávněně podepsat cizím kvalifikovaným podpisem. V managementu může být uložen PUK, musí však ale existovat QPUK, který bude znát pouze uživatel a bude jím v případě potřeby moci odblokovat QPIN.

Trvá zadavatel na těchto požadavcích i s ohledem na daní bezpečnostní rizika ?

Odpověď zadavatele:

Dle zadávací dokumentace: Zařízení podporuje vytváření kvalifikovaného elektronického podpisu dle nařízení eIDAS a disponuje platnou QSCD certifikací. Současně dovoluje v kontaktním čipu hostovat certifikáty z jiných certifikačních autorit než akreditovaných, zejména jde o podporu uložení doménových certifikátů.

Dodavatel tedy dodá certifikované zařízení dle regulace eIDAS.

Dotaz č. 48:

Požaduje se zpracování dokumentu - cílového konceptu PKI. V rámci konceptu mají být navrženy jednotlivé aspekty PKI. Jedním z nich je využiti HSM.

Není ale jasné, zda je požadována i dodávka HSM. V dokumentu je HSM zmíněno jen v kapitolách 10. Web aplikační firewall a 16.3. Implementace PKI zadavatele. V dokumentu nejsou zmíněny žádné parametry požadované pro HSM

Je požadována dodávka HSM? Má být card management napojen na HSM?

Odpověď zadavatele:

HSM není součástí dodávky. Řešení však musí být pro implementaci HSM připraveno.

Dotaz č. 49:

Pro správu karet Zadavatel požaduje dodání aplikace (subsystému), která (mimo jiné): Podporuje dotisk osobních údajů na karty, jako součást procesu přidělení karty držiteli.

Má Zadavatel již nějaké řešení pro potisk a dotisk karet a chce ho rozšířit, nebo ho nemá a požaduje nabídnout takové řešení jako nové? Jestli požaduje, prosíme o dodání formátu potisku.

Odpověď zadavatele:

Zadavatel nedisponuje žádným zmiňovaným řešením.

Dotaz č. 50:

Kořenová CA má být offline a nemá být chráněna HW prostředky. U vydávajících CA není žádná ochrana HW prostředky zmíněna. Obvykle se doporučuje chránit HW prostředky všechny CA v hierarchii. Požadavek nechránit takto kořenovou CA je velmi neobvyklý.

Mají být vydávající CA chráněny HW prostředky?

Odpověď zadavatele:

Kořenová CA má být offline a nemá být chráněna HW prostředky.

Dotaz č. 51:

Zadavatel požaduje vytvořit systém pro zálohování a obnovu CA databáze do MS SQL databáze - neboli kopírovat data z CA databáze do SQL databáze a následně je odsud zálohovat (předpokládáme, že MS SQL databáze bude zálohována).

Jaký je důvod pro zálohování dat CA do databáze MS SQL?

MS má pro zálohování CA svůj nástroj, který CA nativně podporuje. Z tohoto důvod tento požadavek považujeme za nadbytečný.

Odpověď zadavatele:

Pro online zálohování certifikační autority bude implementován systém pro

obnovu a zálohování. Pomocí systému budou data CA zálohována do MS SQL databáze. Součástí systému je mechanismus pro obnovu chybějících dat z MS SQL do CA. Do stejné DB budou zálohována data obou CA (pro uživatele a pro infrastrukturu). Součástí systému je publikační modul, který podporuje publikaci dat do CA.

Zadavatel požaduje online extra zálohování do MS SQL, s podporou obnovy jen chybějících dat.

Dotaz č. 52:

Dotaz ke kapitole 18

V zadávací dokumentaci rozděluje zadavatel kategorie provozních incidentů na Kritický, Vysoký, Střední a Nízký a určuje pro ně požadované doby odezvy a vyřešení. V návrhu servisní smlouvy, Příloze 3 Specifikace SLA klasifikuje zadavatel priority pro dobu odezvy a dobu vyřešení incidentu podle závažnosti chyby, která k incidentu vedla, a to na Kritickou, Závažnou, Běžnou a Ostatní chybu. Požadovaná garance časů odezvy a vyřešení se liší od garance definované v zadávací dokumentaci. Která skupina kategorií s definovanými dobami odezvy a vyřešení bude po dodavateli požadována?

Odpověď zadavatele:

Závazné jsou kategorie incidentů ve smlouvě.

Dotaz č. 53:

Pro kritický provozní incident požaduje zadavatel přijmout incident na řešení do 30 minut a zároveň 30 minut dojezd. Myslí tím zadavatel onsite přítomnost v místě závady do 30 minut od nahlášení závady, přestože v servisní smlouvě, v příloze 3 zadavatel uvádí garanci dojezdového času do 30 minut pouze u kritického bezpečnostního incidentu a pouze pro Incident response tým?

Odpověď zadavatele:

Definice v Příloze 3 Servisní smlouvy upřesňujeme takto:

Provozní incident – výpadek, chyba, omezení funkčnosti hardwarové nebo softwarové infrastruktury Objednatele

Bezpečnostní incident – je narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb, a nebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.

Garance časů odezvy a vyřešení provozního incidentu

Typ chyby	Doba odezvy	Doba vyřešení
Kritická	Do 1 h	Do 4 h
Závažná	Do 4 h	Do 12 h
Běžná	Do 4 h	Do 36 h
Ostatní	Do 8 h	Best effort

Garance časů odezvy a vyřešení bezpečnostního incidentu

Typ chyby	Doba odezvy	Doba dojezdu
Kritická	Do 30 min	Do 30 min
Závažná	Do 1 h	
Běžná	Do 24 h	

Dotaz č. 54:

Je možné reklasifikovat incident do nižší kategorie v případě snížení jeho kritičnosti nalezením náhradního, případně dočasného řešení (workaroundu)?

Odpověď zadavatele:

Ano, reklasifikovat incident do nižší kategorie ve výše uvedeném případě je možné.

Dotaz č. 55:

Možnou příčinou havárie může být nefunkčnost systému v důsledku softwarové chyby, kterou je nutné eskalovat na výrobce systému a do doby nalezení a otestování řešení (workaround, hotfix...) příslušný ticket pozastavit a o odpovídající dobu prodloužit lhůtu k úspěšnému ukončení podpory. Dodavatel není výrobcem SW a je tedy velmi problematické garantovat odstranění chyby nebo poruchy produktu třetích stran, zejména v situacích, kdy je chyba nebo porucha způsobena chybou odstranitelnou pouze výrobcem příslušného softwaru. Veškeré zásahy doporučujeme provádět vrácením systému do poslední známé konfigurace. Je tento postup pro Zadavatele akceptovatelný?

Odpověď zadavatele:

Když dodavatel dodá náhradní řešení dle založeného incidentů, zastaví se čas SLA. Zároveň se vytvoří nový incident nižší kategorie, který bude v stavu „čeká se na subdovatele“, čas se v tomto stavu nepočítá.

Dotaz č. 56:

Dotaz ke kapitole 19

V kapitole 19. Bezpečnostní operační centrum SoC v odstavci "Security Awareness" požaduje po dodavateli závazek na "...realizaci vzdělávání/zvyšování povědomí". Tento pojem je v této kapitole užíván konzistentně, kromě požadavku na rozsah poskytování: "Dodavatel se zavazuje realizovat školení v minimálním rozsahu 1 školení kvartálně".

Je pojem "školení" shodný s pojmem "vzdělávání/zvyšování povědomí" v kontextu této kapitoly?
Požaduje zadavatel poskytovat "vzdělávání/zvyšování povědomí" v minimálním rozsahu 1x kvartálně?

Odpověď zadavatele:

Ano, pojem "školení" je shodný s pojmem "vzdělávání/zvyšování povědomí" v kontextu uvedené kapitoly a zadavatel v rámci plnění předmětu veřejné zakázky požaduje vzdělávání/zvyšování povědomí" v minimálním rozsahu 1x kvartálně.

Dotaz č. 57:

K dokumentu “04a FNB KB - Kupni smlouva - čistopis z 2_4_2019“ kapitola IX bod 1 Zadavatel v kapitole IX bodu 1 uvádí, cit.:

Objednatel nabývá dnem podpisu Protokolu o předání a převzetí dodaného systému včetně veškerých jeho součástí a příslušenství (tedy včetně software) oprávnění systém, resp. jeho příslušnou část ve smyslu AutZ (zákon 121/2000 Sb., autorský zákon), užít všemi způsoby uvedenými v § 12 AutZ. Toto oprávnění Dodavatel Objednateli poskytuje trvale, tzn. bez časového omezení. Objednatel je oprávněn kopírovat, zveřejnit, upravovat, zpracovávat, překládat systém, měnit jeho název, spojit jej s jiným systémem a zařadit jej do systému souborného.

Dodavatel tímto žádá zadavatele o potvrzení, zda-li opravdu zadavatel požaduje mít možnost „kopírovat, zveřejnit, upravovat, zpracovávat, překládat systém, měnit jeho název, spojit jej s jiným systémem a zařadit jej do systému souborného“.

U SW s GPL licencí takováto možnost je, ale u komerčních software toto výrobci nepovolují a použití svého SW omezují jen dle svých licenčních podmínek. Pokud opravdu zadavatel chce software využívat dle kupní smlouvy (kapitola IX, bod 1.), ať uvede konkrétně u jakého software toto požaduje.

Odpověď zadavatele:

Požadavek se vztahuje pouze na systém, software dodaný na míru v rámci tohoto projektu. Když dodavatel naplní zadávací dokumentaci pomocí komerčního softwaru, tento požadavek se vypouští.

Informace č. 6: **Zadavatel v rámci posílení dodržení zásad, stanovených v § 6 Zákona, z předmětu zadávané veřejné zakázky vypouští:**

- **Celou kapitolu 2. s názvem „Rozšíření kamerového systému FNB“ v dokumentu „TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY" (která zůstane neobsazena) včetně přílohy s názvem „Specifikace CCTV – uprava z 29_4_2019.pdf“ z Vysvětlení zadávací dokumentace – Soubor číslo 03.**
- **Celou kapitolu 3. s názvem „Rozšíření optických rozvodů“ v dokumentu „TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY" (která zůstane neobsazena) včetně přílohy 03a Technická SPC předmětu v podobě souboru s názvem „14a - 03a Technická SPC předmětu - příloha optika.xlsx“ z Vysvětlení zadávací dokumentace – Soubor číslo 02.**
- **V kapitole 17. s názvem „LAN a WiFi instrastruktura“ celou část s názvem „WiFi síť“ (str. 149–151) v dokumentu „TECHNICKÁ SPECIFIKACE PŘEDMĚTU VEŘEJNÉ ZAKÁZKY".**

Pro vyloučení všech pochybností tedy zadavatel sděluje, že rozšíření kamerového systému FNB, rozšíření optických rozvodů a WiFi síť NETVOŘÍ PŘEDMĚT TOHOTO ZADÁVACÍHO ŘÍZENÍ.

Informace č. 7: **Zadavatel v souladu s ustanovením § 98 odstavec (4) a v souladu s ustanovením § 99 odstavec (1) a (2) Zákona prodlužuje lhůtu pro podání nabídek, uvedenou v odstavci 7.2. ZADÁVACÍCH PODMÍNEK, takto:**

Zadavatel ruší dále uvedené znění odstavce 7.2. ZADÁVACÍCH PODMÍNEK

„Lhůta pro podání nabídek začíná běžet dnem zahájení zadávacího řízení podle ustanovení § 57 odstavec (1) Zákona. Všechny nabídky budou zadavateli doručeny nejpozději do

17. května 2019 do 14^{00} hodin.“

a nahrazuje jej novým zněním odstavce 7.2. ZADÁVACÍCH PODMÍNEK takto:

„Lhůta pro podání nabídek začíná běžet dnem zahájení zadávacího řízení podle ustanovení § 57 odstavec (1) Zákona. Všechny nabídky budou zadavateli doručeny nejpozději do

26.června 2019 do 14^{00} hodin.“

Informace č. 8: **Zadavatel ruší dále uvedené znění odstavce 9.6. ZADÁVACÍCH PODMÍNEK**

„9.6. Údaj o předpokládané hodnotě veřejné zakázky

Zadavatelem předpokládaná celková hodnota veřejné zakázky v Kč bez DPH činí celkem 297 794 455,- Kč a je členěna takto:

9.6.1. Předpokládaná hodnota nákladů 1. části životního cyklu v rozsahu uvedeném v odstavci 9.7.1. níže je zadavatelem předpokládána ve výši 259 044 455,- Kč bez DPH.

9.6.2. Předpokládaná hodnota nákladů 2. části životního cyklu v rozsahu uvedeném v odstavci 9.7.2. níže je zadavatelem předpokládána ve výši 17 900 000,- Kč bez DPH.

9.6.3. Předpokládaná hodnota nákladů 3. části životního cyklu v rozsahu uvedeném v odstavci 9.7.3. níže je zadavatelem předpokládána ve výši 26 850 000,- Kč bez DPH.“

a nahrazuje jej novým zněním odstavce 9.6. ZADÁVACÍCH PODMÍNEK takto:

„9.6. Údaj o předpokládané hodnotě veřejné zakázky

Zadavatelem předpokládaná celková hodnota veřejné zakázky v Kč bez DPH činí celkem 257 794 455,- Kč a je členěna takto:

9.6.1. Předpokládaná hodnota nákladů 1. části životního cyklu v rozsahu uvedeném v odstavci 9.7.1. níže je zadavatelem předpokládána ve výši 213 044 455,- Kč bez DPH.

9.6.2. Předpokládaná hodnota nákladů 2. části životního cyklu v rozsahu uvedeném v odstavci 9.7.2. níže je zadavatelem předpokládána ve výši 17 900 000,- Kč bez DPH.

9.6.3. Předpokládaná hodnota nákladů 3. části životního cyklu v rozsahu uvedeném v odstavci 9.7.3. níže je zadavatelem předpokládána ve výši 26 850 000,- Kč bez DPH.“

Informace č. 9: **Zadavatel ruší dále uvedené znění odstavce 9.4.1. ZADÁVACÍCH PODMÍNEK**

„9.4.1. Zadavatel předpokládá zahájení plnění veřejné zakázky ihned po nabytí účinnosti SMLOUVY jejím uveřejněním v Registru smluv, které zadavatel předpokládá nejpozději do 5.června 2019.“

a nahrazuje jej novým zněním odstavce 9.4.1. ZADÁVACÍCH PODMÍNEK takto:

„9.4.1. Zadavatel předpokládá zahájení plnění veřejné zakázky ihned po nabytí účinnosti SMLOUVY jejím uveřejněním v Registru smluv, které zadavatel předpokládá nejpozději do 25.července 2019.“

Informace č.10: **Veškeré dopady ze všech výše uvedených skutečností, které mají případný vliv na znění kupní a servisní smlouvy, budou doplněny do čistopisů kupní a servisní smlouvy před jejich podpisem s vybraným dodavatelem.**

V Brně dne 14.5. 2019 ve spolupráci se zadavatelem vypracovala

Mgr. Markéta Šimková
za zastupujícího zadavatele