ZADÁVACÍ DOKUMENTACE
NA NADLIMITNÍ VEŘEJNOU ZAKÁZKU

„ *Služba na zajištění provozu a expertní podpory datové sítě* “

Otevřené řízení podle § 27 zákona č. 137/2006 Sb.,
o veřejných zakázkách, ve znění pozdějších předpisů

Zadavatel veřejné zakázky:

Česká republika – **Č**eská správa sociálního zabezpečení
Křížová 25, 225 08 Praha 5
IČO: 00006963

Obsah

1 INFORMACE O ZADAVATELI

1.1 ZÁKLADNÍ ÚDAJE

Název:	Česká republika - Česká správa sociálního zabezpečení (dále jen „ČSSZ“ nebo „zadavatel“)
Statutární orgán zadavatele:	prof. JUDr. Vilém Kahoun, Ph.D., ústřední ředitel ČSSZ
Sídlo:	Křížová 25, 225 08, Praha 5
IČO:	00006963
DIČ:	neplátce
Bankovní spojení:	ČNB, pobočka Praha, číslo účtu 10006-127001/0710
Osoba oprávněná jednat	Ing. Milan Shrbený, vrchní ředitel úseku informačních a komunikačních technologií

1.2 KONTAKTNÍ OSOBA ZADAVATELE

Kontaktní osoba zadavatele pro styk s uchazeči:

Kontaktní osoba pro styk s účastníky	Mgr. Jan Dubský
Korespondenční adresa:	Křížová 25, 225 08, Praha 5
Telefon:	+420 257 063 615
E-mail:	jan.dubsky@cssz.cz

2 ZÁKLADNÍ CHARAKTERISTIKA ZADAVATELE

Zadavatel je organizační složkou státu a správním orgánem, který zabezpečuje výběr pojistného na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti, dále provádí zejména důchodové pojištění a zajišťuje agendu nemocenského pojištění.

3 OBECNÁ USTANOVENÍ O ZADÁVACÍ DOKUMENTACI

1. Zadavatel zpracoval tuto zadávací dokumentaci v souladu se zákonem č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „zákon"), s cílem zajistit transparentní, nediskriminační a rovné zacházení. Zadávací dokumentace spolu s uveřejněným formulářem oznámení o zakázce obsahuje všechny informace nutné pro vypracování nabídky uchazečem, včetně přesného vymezení rozsahu požadovaného plnění. Dojde-li k rozporu mezi zadávacími podmínkami upravenými ve formuláři oznámení o zakázce a touto zadávací dokumentaci, platí znění zadávacích podmínek obsažených ve formuláři oznámení o zakázce.
2. Zadávací řízení je realizováno dle zákona. Uchazeč je povinen se při zpracování nabídky tímto zákonem řídit, a to zejména v otázkách prokazování splnění kvalifikace a podání nabídky.
3. Případné dotazy k zadávací dokumentaci mohou uchazeči podat výhradně písemně, a to prostřednictvím datové schránky, pokud to povaha doručované písemnosti umožňuje, nebo na korespondenční adresu kontaktní osoby zadavatele uvedenou v části 1. zadávací dokumentace. Písemná žádost musí být zadavateli doručena nejpozději 6 pracovních dnů před uplynutím lhůty pro podání nabídek. Požádal-li uchazeč o dodatečné informace, odešle zadavatel požadované informace nejpozději do 4 pracovních dnů ode dne doručení požadavku. Dotazy zaslané telegraficky nebo elektronickými prostředky musí splňovat požadavky stanovené zákonem č. 89/2012 Sb., občanský zákoník (dále jen „občanský zákoník"), pro písemnou formu. Dotazy zaslané elektronickou poštou (emailem) musí být podepsány elektronickým podpisem v souladu se zákonem č. 227/2000 Sb., o elektronickém podpisu, ve znění pozdějších předpisů.
4. Dodatečné informace, včetně přesného znění požadavku, odešle zadavatel současně všem uchazečům, kteří požádali o poskytnutí zadávací dokumentace, nebo kterým byla zadávací dokumentace poskytnuta. Zadavatel rovněž uveřejní dodatečné informace včetně přesného znění žádosti stejným způsobem, jakým uveřejnil textovou část zadávací dokumentace, tj. na svém profilu zadavatele na adrese https://www.egordion.cz/nabidkaGORDION/profilCSSZ.

4 SPECIFIKACE PŘEDMĚTU ZAKÁZKY

Předmětem zakázky je zajištění hardwarového servisu, softwarového servisu, technické podpory aktivních prvků sítí LAN, WAN a DC. Součástí zakázky je také kompletní zajištění provozu síťové infrastruktury v lokalitách zadavatele na adrese Křížová 6, 25, Praha 5 a Trojská 13, Praha 8 v režimu 24x7 a služby expertní podpory rozvoje a optimalizace síťové infrastruktury včetně souvisejících infrastrukturních služeb.

Veškeré výstupy vzniklé na základě plnění této veřejné zakázky (např. dokumentace, konfigurace, zprávy) jsou výhradně majetkem zadavatele a ten je může v případě své potřeby poskytovat i třetím osobám.

4.1 TECHNICKÁ SPECIFIKACE SLUŽEB A SLA

4.1.1 PROVOZ A SPRÁVA INFRASTRUKTURY SÍTĚ DATOVÝCH CENTER

ROZSAH POŽADOVANÝCH ČINNOSTÍ

1. Provoz aktivních síťových prvků v obou lokalitách:

    a. Profylaktické činnosti:
        i. Při pravidelných odstávkách (2x ročně) – fyzická kontrola, čištění síťových zařízení CISCO a úprava příslušných kabeláží v rámci racku.
        ii. Pravidelné fyzické kontroly s technikem ICT: fyzická kontrola provozního stavu prvků (teplota, hluk zařízení) 1x měsíčně,
    b. Kontrola logů (na denní bázi),
    c. Kontrola výkonnosti a performance monitoring (na měsíční bázi).
    d. Návrh preventivních opatření s cílem předejít možným výpadkům, snížení výkonu v infrastruktuře ČSSZ (minimálně kvartálně nebo dle aktuální situace),
    e. Odborná technická podpora a odstraňování závad v předmětné oblasti – 2nd level support v souladu se SLA,
    f. Provádění pravidelných záloh SW konfigurací (měsíční zálohy + aktualizace záloh po každé změně).

2. Správa aktivních prvků v obou lokalitách

    a. Kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobců (na měsíční bázi),
    b. Analýza vhodnosti a potřebnosti implementace opravného balíku,
    c. Návrh opatření a postupu implementace opravného balíku ke schválení zadavateli.
    d. Instalace a provedení změn (včetně práce) dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna 1x měsíčně, pokud není potřeba jednat rychleji),
    e. Implementace schválených požadavků na změnu konfigurace aktivních prvků (předpokládaný rozsah je až 240 změnových požadavků měsíčně),
    f. Předkládání návrhů na optimalizaci LAN a DC (na kvartální bázi),
    g. Správa a aktualizace privilegovaných hesel ke všem předmětným zařízením (pravidelné aktualizace a předání zadavateli) musí být vedeno v souladu s bezpečnostní politikou zadavatele (SŘ 19/2006 - O bezpečnostní politice a technickoorganizačních opatřeních k ochraně osobních údajů v informačních systémech územních organizačních jednotek ČSSZ a SŘ 11/2006- Bezpečnostní politika informací v ČSSZ).

3. Součinnost v rámci procesů „Projektového řízení“ souvisejících s návrhem změn v infrastruktuře ICT ČSSZ (společně s dodavateli technologií).

4. Provozní podpora ICT v součinnosti s provozovateli služeb, zajišťujících dostupnost služeb dle parametrů definovaných v SLA. Zejména jde o provozovatele služeb v oblastech:
   - ITSM, zajišťující proaktivní dohled a monitoring LAN,
   - zajišťujících správu operačních systémů a databází, fyzickou správu serverů,
   - součinnost se všemi dodavateli při plánovaných víkendových odstávkách (2x ročně),
   - bezprostřední součinnost při mimořádných odstávkách (vlivy vyšší moci a vládou vyhlášený stav nouze případně jiný výjimečný stav).

5. Zprostředkování HW servisu aktivních prvků (u výrobce/dodavatele) včetně případného zajištění náhrady v případě poruchy (v rozsahu smluvně zajištěné maintenance zadavatele).

6. Správa a aktualizace provozní dokumentace k jednotlivým spravovaným zařízením, která jsou uvedena v seznamu zařízení dále v rozsahu:

   a. Postupy pro provoz a správu každého zařízení
   b. Postupy pro obnovu zařízení ze záloh,
   c. Provozní deník pro každé zařízení v minimálním rozsahu datum, osoba, číslo požadavku z ticket systému, popis prováděné činnosti, výsledek činnosti (úspěch/selhání), doba trvání.

7. Správa a aktualizace technické dokumentace v rozsahu:
   a. Aktuální schéma fyzického zapojení LAN (bez koncových stanic),
   b. Aktuální schéma logického zapojení LAN (VLAN, porty, prvky),
   c. Aktuální schéma Logického zapojení LAN L3, L4 (interní směrování, směrování do externích sítí, přehled ACL) v rámci svěřených technologií,
   d. Aktuální přehled verzí OS aktivních prvků,
   e. správa konfigurací předmětných zařízení v konfigurační DB zadavatele (IP, SN).

8. Účast na jednání provozních a pracovních týmů zadavatele (min. 2x měsíčně).

9. Pravidelné zpracování reportů (reporting 1x měsíčně) a zpracování analýzy trendů z reportovaných údajů včetně zpracování doporučení (kvartálně):
   a. Reportování stavu portové konektivity: (minimálně počet volných portů/ obsazených portů.
   b. Reportování vytížení páteřních přepínačů.

10. Zajištění profylaktických prohlídek a opravy kabelážních systémů:

    a. Zajištění profylaktických prohlídek fyzické vrstvy kabeláží za účelem zvýšení bezpečnosti a spolehlivosti, tj. vizuální kontrola metalických i optických kabelážních systémů, odstranění prachu, prověření jejich stavu včetně provedení potřebných měření příslušným kalibrovaným měřicím přístrojem a vystavení měřících protokolů v digitální podobě,
    b. Odstranění nalezených drobných závad vzniklých v průběhu provozování kabelážních systémů z viny uživatele - opravy poškozených rozváděčů a rozvodů, tj. kabelových tras, kabelů, zásuvek, propojovacích panelů, propojovacích kabelů,

c. Odstranění nalezených záručních závad dle záručních podmínek výrobce kabelážního systému instalovaného v dané lokalitě,
d. Zrušení neaktivních spojů - odstranění propojovacích a připojovacích kabelů na linkách neukončených v zařízení, tj. v pracovních stanicích, tiskárnách či telefonních přístrojích,
e. Četnost: 1x ročně v každé lokalitě, s vypracováním písemného protokolu.

11. Zajištění profylaktických prohlídek zdrojů zálohovaného napájení UPS určených pro napájení prvků síťové infrastruktury. Předmětem profylaktické prohlídky UPS je:

    a. kontrola stavu,
    b. odstranění prachu, vizuální kontrola, kontrola činnosti,
    c. prohlídka a samostatný test baterií,
    d. nastavení a kalibrace,
    e. zátěžový test,
    f. kontrola funkčnosti datové sítě a její případné zprovoznění po zapnutí UPS,
    g. Četnost: 1x ročně v každé lokalitě, s vypracováním písemného protokolu o profylaktické prohlídce popisující stav UPS a obsahující požadavek na případnou výměnu opotřebovaných dílů jako jsou baterie, větráky.

POPIS POŽADOVANÉHO SLA

Kategorie A:

Výpadek jednoho nebo více aktivních prvků (karty), který zapříčiní nedostupnost minimálně jednoho nebo více segmentů sítě, případně nedostupnost celé sítě LAN, DC. Segmentem sítě se rozumí celá oblast zahrnující vlastní přístupový aktivní prvek a všechna na tento prvek přímo připojená koncová zařízení. Výpadek nebo závada, která způsobí nedostupnost kteréhokoliv serveru provozovaného v obou lokalitách.

U této kategorie požaduje zadavatel opravu či odstranění závady garantované do 6 hodin od nahlášení závady.

Reaktivní podpora na HW s garantovanou dobou opravy či odstranění závady do 6 hodin od nahlášení závady. Pracovník uchazeče se dostaví na místo opravy do 2 hodin po nahlášení a poskytuje pracovní sílu, náhradní díly a případně další materiál, potřebný k opravě nebo výměně tak, aby HW výrobky byly uvedeny opět do normálního funkčního stavu. Uchazeč identifikuje a opraví špatné funkce a závady výrobku. Vyměněné díly se stanou majetkem uchazeče.
Služba musí být dostupná 24 hodin denně, od pondělí do neděle, včetně veškerých státních svátků a dnů pracovního klidu.

Kategorie B:

Závada nebo výpadek části prvku nebo karty, který způsobí snížení dostupnosti služeb, avšak nezapříčiní výpadek celého segmentu sítě:

a. Výpadek zálohovaných páteřních linek, který nezpůsobí výpadek druhé záložní linky, respektive nedojde k výpadku celého segmentu sítě,

b. závada redundantních zařízení (karet, napájecích zdrojů, modulů a případně dalších), při kterých nedojde k výpadku záložního zařízení, a tím ani k výpadku celého segmentu sítě,
c. Snížená dostupnost služeb, výkonnostní potíže.

U této kategorie požaduje zadavatel reakci do 4 hodin od nahlášení závady a odstranění závady do 8 hodin od nahlášení závady.

Reaktivní podpora na HW se zaručenou dobou odezvy na servisní požadavek do 4 hodin od nahlášení závady a její odstranění závady do 8 hodin od nahlášení závady. Práce na odstranění závady budou zahájeny nejpozději během následujícího pracovního dne po pracovním dni, kdy byla závada oznámena, a budou probíhat v pracovní dny v době od 08:00 do 17:00 hodin. Služba musí být dostupná v pracovní dny, v době od 08:00 do 17:00 hodin.

Kategorie C:

Závada nebo výpadek komunikačního portu, případně bloku portů aktivního prvku, které jsou připojeny pouze ke koncovým zařízením. Závady, které nezpůsobí výpadek ani nesníží dostupnosti služeb v rámci segmentu koncových stanic nebo jednotlivých serverů.

Ostatní závady nespadající do kategorie A nebo B.

U této kategorie zadavatel požaduje odstranění závady do 2 dnů od nahlášení závady.

Po odstranění závady kategorie A, B, C bude informován ohlašovatel závady (pracovník oddělení správy komunikační a datové infrastruktury a podpory HW nebo jiný příslušný pracovník, který závadu nahlásil), který ověří funkčnost a potvrdí ukončení opravy. Potvrzení ukončení opravy bude považováno za okamžik ukončení opravy.

ZPŮSOB KONTROLY

Měření parametrů služby bude prováděno v pravidelných intervalech během zaručené provozní doby služby. Měřící body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Měřeními bude ověřována dostupnost infrastruktury sítě LAN, DC a jejích služeb. Dostupnost služby se bude měřit souborem testů dostupnosti spravovaných aktivních prvků. Provozní činnosti budou kontrolovány zadavatelem (nebo jím stanoveným subjektem) na měsíční bázi. O výsledku kontrol bude sestavován měsíční report. Report vystavuje kontrolující subjekt, schvaluje zadavatele a slouží zadavateli jako podklad pro vyhodnocení služeb.

DALŠÍ PODMÍNKY

V případě obměny zařízení z důvodu náhrady vadného prvku, nebo z důvodu modernizace budou tato nová zařízení považována za ekvivalentní a budou na ně poskytovány stejné služby. Povinnost zpřístupnit technologie pro definici a implementaci monitorovacích agentů/sond. Povinnost poskytnout součinnost zadavateli (nebo jím jmenovaných subjektů) při provádění kontrolní činnosti na dodržování a plnění náplně této služby.

POŽADAVKY NA ODPOVĚĎ

Uchazeč vyplní u každé položky z kapitoly „Rozsah požadovaných činností“, zda jeho návrh poskytování služeb daný požadavek splňuje a jakým způsobem tento požadavek splňuje. Za účelem popisu, jak návrh poskytování služeb daný požadavek splňuje, připojí uchazeč popis splnění požadavků zadavatele, ve kterém uchazeč ke každému požadavku popíše, jak je tento požadavek řešen a (ne)naplněn, aby z tohoto popisu mohl zadavatel ověřit, zda je daný požadavek skutečně (ne)splněn.

Zadavatel uvádí, že požadavky, uvedené v kapitole „Rozsah požadovaných činností“, jsou požadavky, na kterých zadavatel trvá a výslovně prohlašuje, že návrhy jednotlivých uchazečů musí tyto požadavky zcela splňovat. V případě, že uchazeč jakoukoli z těchto položek nesplní, bude taková skutečnost ze strany zadavatele považována za nesplnění zadávacích podmínek s následkem vyloučení uchazeče z účasti v zadávacím řízení.

POPIS SOUČASNÉHO STAVU PROSTŘEDÍ

Centrální síťová infrastruktura tvoří základní komunikační infrastrukturu ČSSZ. Zajišťuje síťové propojení hlavní administrativní lokality zadavatele na adrese Křížová 25, WAN infrastruktury a datových center, zároveň slouží k propojení jednotlivých funkčních bloků – vrstev.

Centrální síťová infrastruktura se rozkládá na lokalitách zadavatele na adrese:

- Křížová 25 (K25), Praha 5
- Křížová 6 (K6), Praha 5
- Trojská 13 (T13), Praha 8

Centrální síťová infrastruktura je budovaná jako plně redundantní z pohledu zařízení, linek a napájení. Základem centrální síťové infrastruktury je čtveřice L3 přepínačů Cisco Catalyst řady 6500, vzájemně propojených pomocí ethernet linek o rychlosti 1 gigabit provozovaných nad vlastními či pronajatými optickými vlákny. Na lokalitách zadavatele na adrese Křížová 6 a Trojská 13 je centrální infrastruktura z důvodu redundance doplněna L2/3 přepínači Cisco řady 3750.

Součástí centrální síťové infrastruktury jsou také přístupové přepínače pro infrastrukturní systémy. Síťová infrastruktura datových center ČSSZ se rozkládá na lokalitách zadavatele na adrese Křížová 6, Trojská 13 a je rozdělena do dvou funkčních bloků, vrstev. Prvním blokem je aplikační vrstva ČSSZ, dále APV ČSSZ, ve které jsou umístěné veškeré agendové aplikace, včetně aplikačních AAA portálů. Druhým blokem je databázová vrstva ČSSZ, dále DB ČSSZ, ve které jsou umístěné databázové systémy využívané v APV ČSSZ. Síťová infrastruktura DB ČSSZ je budovaná jako plně redundantní z pohledu zařízení, linek a napájení. Z hlediska logického členění jsou oba bloky datových center ČSSZ rozdělené do tří samostatných prostředí:

- Produkční prostředí
- Testovací prostředí
- Integrační prostředí

Základem centrální síťové infrastruktury APV ČSSZ je čtveřice L3 přepínačů Cisco Catalyst řady 6500, vzájemně propojených pomocí ethernet linek o rychlosti 1 gigabit provozovaných nad vlastními či pronajatými optickými vlákny. Přístupová vrstva produkčního a testovací prostředí je tvořena společnou síťovou infrastrukturou, oproti integračnímu prostředí, jehož přístupová vrstva je oddělená. Základem síťové infrastruktury DB ČSSZ je čtveřice L3 přepínačů Cisco Catalyst řady 6500, vzájemně propojených pomocí ethernet linek o rychlosti 10 a 1 Gbps provozovaných nad vlastními či pronajatými optickými vlákny. Oddělení jednotlivých prostředí je zajištěno na síťové infrastruktuře pomocí samostatných VLAN či na aplikační úrovni. Přístupová vrstva pro všechna prostředí je tvořena společnou síťovou infrastrukturou. Součástí síťové infrastruktury datových center ČSSZ jsou také přístupové přepínače. Součástí zajištění provozu centrální síťové infrastruktury je administrace a konfigurace prvků řady Catalyst, Nexus, ACS, ACE modulů, FW modulů, LMS, IDS a WLC řady 5000 a dále asistence dalším subjektům (dalším dodavatelům zadavatele) při diagnostice a řešení problémů u aplikačních a databázových systémů. Uchazeč zajistí sledování nadměrného zatížení linek aplikacemi a diagnostiku zatížení linek při nasazení nové aplikace.

4.1.2 PROVOZ A SPRÁVA INFRASTRUKTURY SÍTĚ WAN

ROZSAH POŽADOVANÝCH ČINNOSTÍ

1. Provoz aktivních síťových prvků ve všech lokalitách:
    a. Profylaktické činnosti:
        i. Při pravidelných odstávkách (1x ročně) – fyzická kontrola, čištění síťových zařízení, případná úprava a optimalizace kabeláží v rámci této činnosti.
        ii. Pravidelné fyzické kontroly s technikem ICT: fyzická kontrola provozního stavu prvků (teplota, hluk zařízení) 1x ročně.
    b. kontrola logů (na denní bázi),
    c. kontrola výkonnosti a performance monitoring (na měsíční bázi),
    d. kontrola výkonnosti a performance WAN akceleračních zařízení,
    e. návrh preventivních opatření s cílem předejít možným výpadkům, snížení výkonu v infrastruktuře ČSSZ (minimálně kvartálně nebo dle aktuální situace),
    f. odborná technická podpora a odstraňování závad v předmětné oblasti – 2nd level support v souladu se SLA,
    g. provádění pravidelných záloh SW konfigurací (měsíční zálohy + aktualizace záloh po každé změně).
2. Správa aktivních prvků ve všech lokalitách:
    a. Kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobců (na měsíční bázi),
    b. analýza vhodnosti a potřebnosti implementace opravného balíku,
    c. návrh opatření a postupu implementace opravného balíku ke schválení zadavateli,
    d. instalace a provedení změn (včetně práce) dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna 1x měsíčně, pokud není potřeba jednat rychleji),
    e. implementace schválených požadavků na změnu konfigurace aktivních prvků (předpokládaný rozsah je až 50 změnových požadavků měsíčně),
    f. předkládání návrhů na optimalizaci WAN sítě (na kvartální bázi),
    g. správa a aktualizace bezpečnostních pravidel zajišťujících filtrování provozu ve WAN,
    h. správa a aktualizace bezpečnostních certifikátů zajišťujících ověřování zařízení ve WAN,

i. správa a aktualizace privilegovaných hesel ke všem předmětným zařízením (pravidelné aktualizace a předání zadavateli) musí být vedeno v souladu s bezpečnostní politikou zadavatele (Směrnice k bezpečnosti informačních a komunikačních technologií.

3. Součinnost v rámci procesů „Projektového řízení“ souvisejících s návrhem změn v infrastruktuře ICT ČSSZ (společně s dodavateli technologií).
4. Provozní podpora ICT v součinnosti s provozovateli služeb, zajišťujících dostupnost služeb dle parametrů definovaných v SLA. Zejména jde o provozovatele služeb v oblastech:
   - ITSM, zajišťující proaktivní dohled a monitoring LAN,
   - součinnost se všemi dodavateli při plánovaných víkendových odstávkách (2x ročně),
   - bezprostřední součinnost při mimořádných odstávkách (vlivy vyšší moci a vládou vyhlášený stav nouze případně jiný výjimečný stav).
5. Zprostředkování HW servisu aktivních prvků (u výrobce/dodavatele) včetně případného zajištění náhrady v případě poruchy (v rozsahu smluvně zajištěné maintenance zadavatele).
6. Správa a aktualizace provozní dokumentace v rozsahu:
   a. Postupy pro provoz a správu každého zařízení,
   b. postupy pro obnovu zařízení ze záloh,
   c. provozní deník pro každé zařízení v minimálním rozsahu datum, osoba, číslo požadavku z ticket systému, popis prováděné činnosti, výsledek činnosti (úspěch/selhání), doba trvání.
7. Správa a aktualizace technické dokumentace v rozsahu:
   a. Aktuální schéma fyzického zapojení centrální WAN infrastruktry (VLAN, porty, prvky),
   b. aktuální schéma logického zapojení centrální WAN infrastruktry,
   c. aktuální schéma logického zapojení WAN infrastruktry L3, L4 (interní směrování, směrování do externích sítí, přehled ACL) v rámci svěřených technologií,
   d. aktuální schéma fyzického a logického připojení poskytovatelů WAN linek,
   e. aktuální přehled verzí OS aktivních prvků,
   f. správa konfigurací předmětných zařízení v konfigurační DB zadavatele (IP, SN).
8. Účast na jednání provozních a pracovních týmů zadavatele (2x měsíčně).
9. Pravidelné zpracování reportů (reporting 1x měsíčně) a zpracování analýzy trendů z reportovaných údajů včetně zpracování doporučení (kvartálně):
   a. Reportování stavu portové konektivity: (minimálně počet volných portů/ obsazených portů,
   b. reportování vytížení centrální WAN infrastruktry,
   c. reportování stavu vytížení a optimalizace provozu WAN akceleračních zařízení,
   d. SLA report dostupnosti zařízení a služeb WAN sítě,
   e. přehled provedených změn v konfiguraci WAN sítě.

10. Zajištění profylaktických prohlídek a opravy kabelážních systémů
    a. Zajištění profylaktických prohlídek fyzické vrstvy kabeláží za účelem zvýšení bezpečnosti a spolehlivosti, tj. vizuální kontrola metalických i optických kabelážních systémů, odstranění prachu, prověření jejich stavu včetně provedení potřebných měření příslušným kalibrovaným měřicím přístrojem a vystavení měřících protokolů v digitální podobě,
    b. Odstranění nalezených drobných závad vzniklých v průběhu provozování kabelážních systémů z viny uživatele - opravy poškozených rozváděčů a rozvodů, tj. kabelových tras, kabelů, zásuvek, propojovacích panelů, propojovacích kabelů,
    c. Odstranění nalezených záručních závad dle záručních podmínek výrobce kabelážního systému instalovaného v dané lokalitě,
    d. Zrušení neaktivních spojů - odstranění propojovacích a připojovacích kabelů na linkách neukončených v zařízení, tj. v pracovních stanicích, tiskárnách či telefonních přístrojích,
    e. Četnost: 1x ročně v každé lokalitě, s vypracováním písemného protokolu. Průměrný počet přípojných míst na lokalitu - 300.

POPIS POŽADOVANÉHO SLA

Kategorie A:
Výpadek jednoho nebo více aktivních prvků (karty), který zapříčiní nedostupnost minimálně jednoho nebo více segmentů sítě, případně nedostupnost celé sítě WAN. Segmentem sítě se rozumí celá oblast zahrnující vlastní přístupový aktivní prvek a všechna na tento prvek přímo připojená koncová zařízení. Výpadek nebo závada, která způsobí nedostupnost kteréhokoliv serveru provozovaného ve vzdálených lokalitách.

U této kategorie požaduje zadavatel opravu či odstranění závady garantované do 6 hodin od nahlášení závady.

Reaktivní podpora na HW s garantovanou dobou opravy či odstranění závady do 6 hodin od nahlášení závady. Pracovník uchazeče se dostaví na místo opravy do 2 hodin po nahlášení a poskytuje pracovní sílu, náhradní díly a případně další materiál, potřebný k opravě nebo výměně tak, aby HW výrobky byly uvedeny opět do normálního funkčního stavu. Uchazeč identifikuje a opraví špatné funkce a závady výrobku. Vyměněné díly se stanou majetkem uchazeče.

Služba musí být dostupná 24 hodin denně, od pondělí do neděle, včetně veškerých státních svátků a dnů pracovního klidu.

Kategorie B:

Závada nebo výpadek části prvku nebo karty, který způsobí snížení dostupnosti služeb, avšak nezapříčiní výpadek celého segmentu sítě:

a. Výpadek zálohovaných páteřních linek, který nezpůsobí výpadek druhé záložní linky, respektive nedojde k výpadku celého segmentu sítě,
b. závada redundantních zařízení (karet, napájecích zdrojů, modulů a případně dalších), při kterých nedojde k výpadku záložního zařízení, a tím ani k výpadku celého segmentu sítě.

Snížená dostupnost služeb, výkonnostní potíže.

U této kategorie požaduje zadavatel reakci do 4 hodin od nahlášení závady a odstranění závady do 8 hodin od nahlášení závady.

Reaktivní podpora na HW se zaručenou dobou odezvy na servisní požadavek do 4 hodin od nahlášení závady a odstranění závady do 8 hodin. Práce na odstranění závady budou zahájeny nejpozději během následujícího pracovního dne po pracovním dni, kdy byla závada oznámena, a budou probíhat v pracovní dny v době od 08:00 do 17:00 hodin. Služba musí být dostupná v pracovní dny, v době od 08:00 do 17:00 hodin.

Kategorie C:

Závada nebo výpadek komunikačního portu, případně bloku portů aktivního prvku, které jsou připojeny pouze ke koncovým zařízením. Závady, které nezpůsobí výpadek ani nesníží dostupnosti služeb v rámci segmentu koncových stanic nebo jednotlivých serverů.
Ostatní závady nespadající do kategorie A nebo B.

U této kategorie zadavatel požaduje odstranění do 2 dnů od nahlášení závady.

Po odstranění závady kategorie A, B, C bude informován ohlašovatel závady (pracovník oddělení správy komunikační a datové infrastruktury a podpory HW nebo jiný příslušný pracovník, který závadu nahlásil), který ověří funkčnost a potvrdí ukončení opravy. Potvrzení ukončení opravy bude považováno za okamžik ukončení opravy.

ZPŮSOB KONTROLY

Měření parametrů služby bude prováděno v pravidelných intervalech během zaručené provozní doby služby. Měřící body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Měřeními bude ověřována dostupnost infrastruktury sítě WAN a sítí LAN jednotlivých vzdálených lokalit. Dostupnost služby se bude měřit souborem testů dostupnosti spravovaných aktivních prvků. Provozní činnosti budou kontrolovány zadavatelem (nebo jím stanoveným subjektem) na měsíční bázi. O výsledku kontrol bude sestavován měsíční report. Report vystavuje kontrolující subjekt, schvaluje zadavatele a slouží zadavateli jako podklad pro vyhodnocení služeb.

DALŠÍ PODMÍNKY

V případě obměny zařízení z důvodu náhrady vadného prvku, nebo z důvodu modernizace budou tato nová zařízení považována za ekvivalentní a budou na ně poskytovány stejné služby.
Povinnost zpřístupnit technologie pro definici a implementaci monitorovacích agentů/sond.
Povinnost poskytnout součinnost zadavateli (nebo jím jmenovaných subjektů) při provádění kontrolní činnosti na dodržování a plnění náplně této služby.

POŽADAVKY NA ODPOVĚĎ

Uchazeč vyplní u každé položky z kapitoly „Rozsah požadovaných činností“, zda jeho návrh poskytování služeb daný požadavek splňuje a jakým způsobem tento požadavek splňuje. Za účelem popisu, jak návrh poskytování služeb daný požadavek splňuje, připojí uchazeč popis splnění požadavků zadavatele, ve kterém uchazeč ke každému požadavku popíše, jak je tento požadavek řešen a (ne)naplněn, aby z tohoto popisu mohl zadavatel ověřit, zda je daný požadavek skutečně (ne)splněn.

Zadavatel uvádí, že požadavky, uvedené v kapitole „Rozsah požadovaných činností“, jsou požadavky, na kterých zadavatel trvá a výslovně prohlašuje, že návrhy jednotlivých uchazečů musí tyto požadavky zcela splňovat. V případě, že uchazeč jakoukoli z těchto položek nesplní, bude taková skutečnost ze strany zadavatele považována za nesplnění zadávacích podmínek s následkem vyloučení uchazeče z účasti v zadávacím řízení.

POPIS SOUČASNÉHO STAVU PROSTŘEDÍ

Centrální infrastruktura sítě WAN je tvořena dvojicí centrálních směrovačů Cisco 7206VXR. Cisco 7206VXR je modulární, výkonný směrovač určený pro široké použití v rozsáhlých podnikových sítích či v sítích poskytovatelů služeb, kde muže plnit funkci WAN agregačního směrovače nebo broadband agragačního směrovače, MPLS P/PE směrovače či IPSec VPN koncentrátoru. Cisco 7206VXR umožňuje využití širokého spektra rozhraní od synchronního či asynchronního sériového, přes E1/T1, E3/T3, ATM, POS, až po ethernet rozhraní o rychlosti 10/100/1000Mbit/s. Směrovače Cisco 7206VXR jsou osazené výkonným procesorovým modulem NPE-G1 s celkovou propustností 1 milión rámců za sekundu. Procesorový modul NPE-G1 zároveň poskytuje základní rozhraní pro připojení směrovače v podobě třech Gigabit ethernet metalických či optických portů. Směrovače Cisco 7206VXR jsou doplněné o vysoce výkonné VPN akcelerační moduly s celkovou propustností až 280Mbit/s pro provoz šifrovaný algoritmem DES/3DES/AES. Cisco VPN akcelerační moduly podporují HW akceleraci IPSec/IKE v módu tunel, šifrovaný GRE tunel, šifrovaný L2TP tunel nebo IPPCP. Cisco VPN akcelerační moduly podporují škálovatelnost IPSec tunelů až do celkového počtu 5000 tunelů.

Centrální směrovače Cisco 7206VXR jsou z hlediska vysoké dostupnosti nainstalované na lokalitách zadavatele na adrese Křížová 25 a Trojská 13. Centrální směrovače Cisco 7206VXR ukončují centrální linky poskytovatelů služeb zajišťující pronajaté IP VPN služby pro připojení vzdálených lokalit. Centrální směrovače Cisco 7206VXR jsou následně připojené na centrální přepínače ČSSZ tak aby bylo možné zajistit optimální směrování WAN provozu na infrastrukturní servery, Internetové proxy či služby poskytované v rámci APV ČSSZ. Centrální směrovače Cisco 7206VXR slouží jako konvergovaná platforma pro virtuální privátní síť a nabízí jednoduchou správu bezpečnosti a šifrování. Směrovač využívá řešení DMVPN (Cisco Dynamic Multipoint Virtual Private Networking), které umožňuje kromě hub-spoke topologie také výměnu dat mezi dvěma vzdálenými místy bez nutnosti jejich posílání přes centrálu. Snižuje tak zátěž sítě i objem datových přenosů na centrálních agregačních linkách.

Součástí centrální infrastruktury WAN jsou také centrální WAN akcelerační zařízení Cisco WAE-7371 umístěné na lokalitách zadavatele na adrese Křížová 25 a Trojská 13. Cisco WAE-7371 jsou Wide Area Application Engine nabízí nejvyšší výkon a úroveň dostupnosti v rámci produktové řady WAE a je navrženo k nasazení jako základní prvek optimalizace a akcelerace aplikací ve WAN pro velká podniková datová střediska. Centrální WAN akcelerační zařízení jsou připojená na centrální přepínače ČSSZ, které zajišťují přepínání akcelerovaného provozu na centrální WAN akcelerační zařízení Cisco

WAE-7371 pomocí protokolu WCCP. WCCP verze 2 (Web Cache Coordination Protocol verze 2) je funkce Cisco IOS implementovaná v Layer 3 přepínačích a směrovačích Cisco, která přináší transparentní zachytávání a přesměrování paketů, clustering pro vysokou dostupnost a rozložení zatížení (load-sharing).

Síťová infrastruktura na vzdálených lokalitách je tvořena pobočkovým směrovačem, WAN akcelerační apliance, L3 a L2 přepínači. WAN linka je připojená do pobočkového směrovače, na kterém jsou ukončené šifrované IPSec tunely z centrálních směrovačů. Kromě šifrování a filtrování provozu zajišťuje směrovač také odklánění provozu na WAN akcelerační zařízení z důvodu optimalizace datového provozu. Pobočkový směrovač je redundantně připojen na dvojici L3 přepínačů zajišťující směrování datového provozu v rámci vzdálené lokality. Kromě směrování L3 přepínače zajišťují také filtrování nežádoucího WAN provozu. Na centrální L3 přepínače vzdálené lokality jsou následně připojené L2 přístupové přepínače.

LOKALITA

Celá Česká Republika

4.1.3 PROVOZ A SPRÁVA INFRASTRUKTURY SÍTĚ DMZ/IKR A B2B ROZHRANÍ

ROZSAH POŽADOVANÝCH ČINNOSTÍ

1. Provoz aktivních síťových prvků v obou lokalitách:
    a. Profylaktické činnosti:
        i. Při pravidelných odstávkách (2x ročně) – fyzická kontrola, čištění síťových zařízení, úprava kabeláži,
        ii. Pravidelné fyzické kontroly s technikem ICT: fyzická kontrola provozního stavu prvků (teplota, hluk zařízení) 1x měsíčně,
    b. kontrola logů (na denní bázi),
    c. kontrola výkonnosti a performance monitoring (na měsíční bázi),
    d. návrh preventivních opatření s cílem předejít možným výpadkům, snížení výkonu v infrastruktuře ČSSZ (minimálně kvartálně nebo dle aktuální situace),
    e. odborná technická podpora a odstraňování závad v předmětné oblasti – 2nd level support v souladu se SLA,
    f. provádění pravidelných záloh SW konfigurací (měsíční zálohy + aktualizace záloh po každé změně).
2. Správa aktivních prvků v obou lokalitách:
    a. Kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobců (na měsíční bázi),
    b. analýza vhodnosti a potřebnosti implementace opravného balíku,
    c. návrh opatření a postupu implementace opravného balíku ke schválení zadavateli,
    d. instalace a provedení změn (včetně práce) dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna 1x měsíčně, pokud není potřeba jednat rychleji),
    e. implementace schválených požadavků na změnu konfigurace aktivních prvků (předpokládaný rozsah je až 240 změnových požadavků měsíčně),
    f. předkládání návrhů na optimalizaci DMZ/IKR sítě (na kvartální bázi),
    g. správa a aktualizace bezpečnostních pravidel zajišťujících filtrování provozu v DMZ/IKR infrastruktuře,

h. správa připojení do externích sítí Internet, Govbone, Govnet a MPSV,
i. správa a aktualizace privilegovaných hesel ke všem předmětným zařízením (pravidelné aktualizace a předání zadavateli) musí být vedeno v souladu s bezpečnostní politikou zadavatele.
j.

3. Správa B2B rozhraní v obou lokalitách:
    a. Kontrola dostupnosti patchů a dalších opravných balíků (na měsíční bázi),
    b. analýza vhodnosti a potřebnosti implementace opravného balíku,
    c. návrh opatření a postupu implementace opravného balíku ke schválení zadavateli,
    d. instalace a provedení změn (včetně práce) dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna 1x měsíčně, pokud není potřeba jednat rychleji),
    e. implementace schválených požadavků na zavedení, změnu a zrušení služby B2B rozhraní (předpokládaný rozsah je až 10 změnových požadavků měsíčně),
    f. správa a aktualizace serverových a klientských certifikátů v B2B rozhraní,
    g. předkládání návrhů na optimalizaci B2B rozhraní (na kvartální bázi),
    h. provádění pravidelných záloh konfigurací B2B rozhraní (měsíční zálohy + aktualizace záloh po každé změně),
    i. správa a aktualizace privilegovaných hesel ke všem předmětným zařízením (pravidelné aktualizace a předání zadavateli) musí být vedeno v souladu s bezpečnostní politikou zadavatele (Směrnice k bezpečnosti informačních a komunikačních technologií,
4. Součinnost v rámci procesů „Projektového řízení“ souvisejících s návrhem změn v infrastruktuře ICT ČSSZ (společně s dodavateli technologií).
5. Provozní podpora ICT v součinnosti s provozovateli služeb, zajišťujících dostupnost služeb dle parametrů definovaných v SLA. Zejména jde o provozovatele služeb v oblastech:
    - ITSM, zajišťující proaktivní dohled a monitoring LAN,
    - zajišťujících správu operačních systémů a databází, fyzickou správu serverů,
    - součinnost se všemi dodavateli při plánovaných víkendových odstávkách (2x ročně),
    - bezprostřední součinnost při mimořádných odstávkách (vlivy vyšší moci a vládou vyhlášený stav nouze případně jiný výjimečný stav).
6. Zprostředkování HW servisu aktivních prvků (u výrobce/dodavatele) včetně případného zajištění náhrady v případě poruchy (v rozsahu smluvně zajištěné maintenance zadavatele).
7. Správa a aktualizace provozní dokumentace v rozsahu:
    a. Postupy pro provoz a správu každého zařízení,
    b. postupy pro obnovu zařízení ze záloh,
    c. provozní deník pro každé zařízení v minimálním rozsahu datum, osoba, číslo požadavku z ticket systému, popis prováděné činnosti, výsledek činnosti (úspěch/selhání), doba trvání.
8. Správa a aktualizace technické dokumentace v rozsahu:
    a. Aktuální schéma fyzického zapojení DMZ/IKR infrastruktry (VLAN, porty, prvky),
    b. aktuální schéma logického zapojení DMZ/IKR infrastruktry,
    c. aktuální schéma logického zapojení DMZ/IKR infrastruktry L3, L4 (interní směrování, směrování do externích sítí, přehled ACL) v rámci svěřených technologií,
    d. aktuální schéma fyzického a logického připojení poskytovatelů linek do externích sítí,
    e. aktuální přehled verzí OS aktivních prvků,
    f. správa konfigurací předmětných zařízení v konfigurační DB zadavatele (IP, SN).
9. Účast na jednání provozních a pracovních týmů zadavatele (2xměsíčně).

10. Pravidelné zpracování reportů (reporting 1x měsíčně) a zpracování analýzy trendů z reportovaných údajů včetně zpracování doporučení (kvartálně):
    a. Reportování stavu portové konektivity: (minimálně počet volných portů/ obsazených portů,
    b. reportování vytížení DMZ/IKR infrastruktry,
    c. reportování vytížení a statistik jednotlivých služeb B2B rozhraní,
    d. SLA report dostupnosti zařízení a služeb DMZ/IKR sítě a B2B služeb,
    e. přehled provedených změn v konfiguraci DMZ/IKR sítě a B2B služeb.

POPIS POŽADOVANÉHO SLA

Popis požadovaného SLA pro DMZ/IKR infrastrukturu

Kategorie A:

Výpadek jednoho nebo více aktivních prvků (karty), který zapříčiní nedostupnost minimálně jedno nebo více segmentů sítě, případně nedostupnost celé DMZ/IKR infrastruktury. Segmentem sítě se rozumí celá oblast zahrnující vlastní přístupový aktivní prvek a všechna na tento prvek přímo připojená koncová zařízení. Výpadek nebo závada, která způsobí nedostupnost kteréhokoliv serveru provozovaného v DMZ/IKR infrastruktuře.

U této kategorie požaduje zadavatel opravu či odstranění závady garantované do 4 hodin od nahlášení závady.

Reaktivní podpora na HW s garantovanou dobou opravy či odstranění závady do 4 hodin od nahlášení závady. Pracovník uchazeče se dostaví na místo opravy do 2 hodin po nahlášení a poskytuje pracovní sílu, náhradní díly a případně další materiál, potřebný k opravě nebo výměně tak, aby HW výrobky a poskytované služby byly uvedeny opět do normálního funkčního stavu. Uchazeč identifikuje a opraví špatné funkce a závady výrobku. Vyměněné díly se stanou majetkem uchazeče.

Služba musí být dostupná 24 hodin denně, od pondělí do neděle, včetně veškerých státních svátků a dnů pracovního klidu.

Kategorie B:

Závada nebo výpadek části prvku nebo karty, který způsobí snížení dostupnosti služeb, avšak nezapříčiní výpadek celého segmentu sítě:

a. Výpadek zálohovaných páteřních linek, který nezpůsobí výpadek druhé záložní linky, respektive nedojde k výpadku celého segmentu sítě,
b. závada redundantních zařízení (karet, napájecích zdrojů, modulů a případně dalších), při kterých nedojde k výpadku záložního zařízení, a tím ani k výpadku celého segmentu sítě.

Snížená dostupnost služeb, výkonnostní potíže.

U této kategorie požaduje zadavatel reakci do 4 hodin od nahlášení závady a odstranění závady do 8 hodin od nahlášení závady.

Reaktivní podpora na HW se zaručenou dobou odezvy na servisní požadavek do 4 hodin od nahlášení závady a její odstranění do 8 hodin od nahlášení. Práce na odstranění závady budou zahájeny nejpozději během následujícího pracovního dne po pracovním dni, kdy byla závada oznámena, a budou probíhat v pracovní dny v době od 08:00 do 17:00 hodin. Služba musí být dostupná v pracovní dny, v době od 08:00 do 17:00 hodin.

Kategorie C:

Ostatní závady nespadající do kategorie A nebo B.

U této kategorie zadavatel požaduje odstranění do 2 dnů od nahlášení závady.

Po odstranění závady kategorie A, B, C bude informován ohlašovatel závady (pracovník oddělení správy komunikační a datové infrastruktury a podpory HW nebo jiný příslušný pracovník, který závadu nahlásil), který ověří funkčnost a potvrdí ukončení opravy. Potvrzení ukončení opravy bude považováno za okamžik ukončení opravy.

Popis požadovaného SLA pro B2B rozhraní

Kategorie A:

Výpadek nebo závada, která způsobí nedostupnost B2B rozhraní. Nedostupností B2B rozhraní se rozumí chybový stav, kdy primární ani záložní server B2B rozhraní v daném datovém centru neodpovídají na klientské dotazy v požadovaném čase.

U této kategorie požaduje zadavatel reakci do 2 hodin od nahlášení závady odstranění závady do 4 hodin od nahlášení závady.

Reaktivní podpora se zaručenou dobou odezvy na servisní požadavek do 2 hodin od nahlášení závady a její odstranění do 4 hodin. Pracovník uchazeče zahájí práce na odstranění závady do 2 hodin od nahlášení. V případě závady na systémech zadavatele či třetích stran bude pracovník uchazeče součástí řešitelského týmu do doby, kdy poskytované služby budou uvedeny opět do normálního funkčního stavu.

Služba musí být dostupná 24 hodin denně, od pondělí do neděle, včetně veškerých státních svátků, dnů pracovního klidu.

Kategorie B:
Výpadek nebo závada části infrastruktury B2B rozhraní, která způsobí snížení dostupnosti poskytovaných služeb, avšak nezapříčiní nedostupnost B2B rozhraní. Nedostupností B2B rozhraní se rozumí chybový stav, kdy primární ani záložní server B2B rozhraní v daném datovém centru neodpovídají na klientské dotazy v požadovaném čase.
Snížená dostupnost služeb, výkonnostní potíže.

U této kategorie požaduje zadavatel reakci do 4 hodin od nahlášení závady a odstranění závady do 8 hodin od nahlášení závady.

Reaktivní podpora se zaručenou dobou odezvy na servisní požadavek do 4 hodin od nahlášení závady a její odstranění do 8 hodin. Práce na odstranění závady budou zahájeny nejpozději během následujícího pracovního dne po pracovním dni, kdy byla závada oznámena, a budou probíhat v pracovní dny v době od 08:00 do 17:00 hodin. V případě závady na systémech zadavatele či třetích stran bude pracovník uchazeče součástí řešitelského týmu do doby, kdy poskytované služby budou uvedeny opět do normálního funkčního stavu. Služba musí být dostupná v pracovní dny, v době od 08:00 do 17:00 hodin.

Kategorie C:

Ostatní závady nespadající do kategorie A nebo B.

U této kategorie zadavatel požaduje odstranění do 2 dnů od nahlášení závady.

Po odstranění závady kategorie A, B, C bude informován ohlašovatel závady (pracovník oddělení správy komunikační a datové infrastruktury a podpory HW nebo jiný příslušný pracovník, který závadu nahlásil), který ověří funkčnost a potvrdí ukončení opravy. Potvrzení ukončení opravy bude považováno za okamžik ukončení opravy.

ZPŮSOB KONTROLY

Měření parametrů služby bude prováděno v pravidelných intervalech během zaručené provozní doby služby. Měřící body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Měřeními bude ověřována dostupnost infrastruktury sítě DMZ/IKR a poskytovaných služeb B2B rozhraní. Dostupnost služby se bude měřit souborem testů dostupnosti spravovaných aktivních prvků. Provozní činnosti budou kontrolovány zadavatelem (nebo jím stanoveným subjektem) na měsíční bázi. O výsledku kontrol bude sestavován měsíční report. Report vystavuje kontrolující subjekt, schvaluje zadavatele a slouží zadavateli jako podklad pro vyhodnocení služeb.

DALŠÍ PODMÍNKY

V případě obměny zařízení z důvodu náhrady vadného prvku, nebo z důvodu modernizace budou tato nová zařízení považována za ekvivalentní a budou na ně poskytovány stejné služby. Povinnost zpřístupnit technologie pro definici a implementaci monitorovacích agentů/sond. Povinnost poskytnout součinnost zadavateli (nebo jím jmenovaných subjektů) při provádění kontrolní činnosti na dodržování a plnění náplně této služby.

POŽADAVKY NA ODPOVĚĎ

Uchazeč vyplní u každé položky z kapitoly „Rozsah požadovaných činností“, zda jeho návrh poskytování služeb daný požadavek splňuje a jakým způsobem tento požadavek splňuje. Za účelem popisu, jak návrh poskytování služeb daný požadavek splňuje, připojí uchazeč popis splnění požadavků zadavatele, ve kterém uchazeč ke každému požadavku popíše, jak je tento požadavek řešen a (ne)naplněn, aby z tohoto popisu mohl zadavatel ověřit, zda je daný požadavek skutečně (ne)splněn.

Zadavatel uvádí, že požadavky, uvedené v kapitole „Rozsah požadovaných činností“, jsou požadavky, na kterých zadavatel trvá a výslovně prohlašuje, že návrhy jednotlivých uchazečů musí tyto požadavky zcela splňovat. V případě, že uchazeč jakoukoli z těchto položek nesplní, bude taková skutečnost ze strany zadavatele považována za nesplnění zadávacích podmínek s následkem vyloučení uchazeče z účasti v zadávacím řízení.

POPIS SOUČASNÉHO STAVU PROSTŘEDÍ

Infrastruktura DMZ/IKR vytváří bezpečné, standardní a unifikované komunikační rozhraní pro komunikaci s klienty ČSSZ (fyzickými i právnickými osobami) a pro výměnu dat s orgány státní moci. Infrastruktura DMZ/IKR ČSSZ se rozkládá na lokalitách zadavatele na adrese Křížová 6 a Trojská 13. Z hlediska instalovaného HW a síťové topologie DMZ/IKR jsou obě lokality totožné. Základem síťové infrastruktury DMZ/IKR ČSSZ je čtveřice L3 přepínačů Cisco Catalyst 6506E, po dvou na každé lokalitě.

Dvojce fyzických šasi v rámci jedné lokality jsou spojené do jednoho virtuálního zařízení pomocí technologie Cisco Virtual Switching Systém - VSS. Centrální přepínače DMZ/IKR jsou osazené moduly Cisco ACE zajišťující rozklad zátěže mezi jednotlivé servery DMZ/IKR infrastruktury. Celé řešení je doplněné dvojicí externích a interních firewall Cisco ASA zapojených v režimu vysoké dostupnosti Active/Active, směrovačem Cisco ASR1002 zajišťujícím propojení do externích sítí a zařízením Cisco GSS. Z pohledu fyzického propojení komponent je využita topologie hvězda, kdy centrálními prvky, které propojují všechny komponenty dohromady, jsou dva logicky seskupené centrální přepínače.

Infrastruktura DMZ/IKR zajišťuje propojení jednotlivých komunikačních rozhraní a publikaci jednotlivých služeb do sítí Internet, Govbone, Govnet (CMS, Testa), přímého propojení v rámci rezortu MPSV a datových center ČSSZ.

Infrastruktura B2B rozhraní doplňuje funkcionalitu datových center ČSSZ o komunikační kanál na externí systémy umístěné jak v Extranetu prostřednictvím VPN, CMS, ZR, GovNet či GovBone tak i v Internetu a byla navržena pro zajištění odchozí a příchozí komunikace založené na HTTP/HTTPS protokolu. Infrastruktura B2B rozhraní centralizuje bezpečnostní standardy pro komunikaci s externími subjekty a zajišťuje plné oddělení aplikační vrstvy ČSSZ. B2B rozhraní zajišťuje publikování interní VIP pro jednotlivé externí zdroje, filtrování provozu na http proxy serveru a navazování zabezpečeného SSL spojení ověřovaného pomocí klientských certifikátů. B2B rozhraní je provozováno jako čtveřice virtuálních serverů s OS Linux běžících na virtualizační platformě VMWare ESX serveru. V každé lokalitě ČSSZ je nainstalovaná dvojce virtuálních serverů. Z hlediska požadavku zajištění vysoké dostupnosti B2B rozhraní jsou servery v jednom datovém centru provozované na různých fyzických blade serverech, umístěných do různých fyzických blade šasi.

LOKALITA

Křížová 6 (K6), Praha 5

Trojská 13 (T13), Praha 8

4.1.4 PROVOZ A SPRÁVA INFRASTRUKTURY DNS A ADRESNÍHO PROSTORU

Rozsah požadovaných činností

Jedná se o zajištění provozu vyjmenovaných serverů DNS umístěných na fyzických a virtuálních serverech zadavatele. Dále se jedná o zajištění provozu systému správy adresního prostoru (IPAM) a jeho integraci do systému IMS (Infrastructure Management System) podle kapitoly 4.1.6.

Požadovány jsou zejména následující činnosti:

- Provoz služby DNS
    - profylaktické činnosti, kontrola systému DNS
    - kontrola logů (na týdenní bázi)
    - kontrola monitoringu služby DNS (na měsíční bázi)
    - návrh preventivních opatření vyplývající z monitoringu a profylaktických činností s cílem předejít možným výpadkům a omezením služby DNS
    - odborná technická podpora a odstraňování závad v předmětné oblasti – 2nd level support (na denní bázi)
    - provádění pravidelných záloh DNS. Uchazeč navrhne a popíše potřebný rozsah zálohování

- vedení provozního deníku služby DNS

- Správa služby DNS:
  - Kontrola dostupnosti patchů, hotfix-ů, service pack-ů a dalších opravných balíků výrobce (na měsíční bázi)
  - údržba služby DNS - údržba databáze (Hostname, C-Name, přenosy zón)
  - analýza vhodnosti a potřebnosti implementace opravného balíku
  - návrh opatření a postupu implementace opravného balíku ke schválení zadavateli
  - instalace a provedení změn dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna 1x měsíčně),
  - implementace schválených požadavků na změnu konfigurace služby DNS
  - předkládání návrhů na optimalizaci DNS systému (na kvartální bázi).
- Provoz služby IPAM
  - profylaktické činnosti, kontrola systému IPAM
  - kontrola logů (na týdenní bázi),
  - kontrola monitoringu služby IPAM (na měsíční bázi),
  - návrh preventivních opatření vyplývající z monitoringu a profylaktických činností s cílem předejít možným výpadkům a omezením služby IPAM
  - odborná technická podpora a odstraňování závad v předmětné oblasti – 2nd level support (na denní bázi)
  - provádění pravidelných záloh IPAM systému. Uchazeč navrhne a popíše potřebný rozsah zálohování.
  - vedení provozního deníku služby IPAM
- Správa služby IPAM:
  - Kontrola dostupnosti patchů, hotfix-ů, service pack-ů a dalších opravných balíků výrobce (na měsíční bázi)
  - údržba služby IPAM - údržba databáze (Zavádění/rušení adresních rozsahů, změny záznamů o využívaných IP adresách)
  - analýza vhodnosti a potřebnosti implementace opravného balíku
  - návrh opatření a postupu implementace opravného balíku ke schválení zadavateli
  - instalace a provedení změn dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna 1x měsíčně)
  - předkládání návrhů na optimalizaci IPAM systému (na kvartální bázi)
- Integrace služby IPAM do systému IMS (Infrastructure Management System) – viz kapitola 4.1.6.
- Součinnost v rámci procesů „Projektového řízení“ souvisejících s návrhem změn v infrastruktuře ICT zadavatele.
- Účast na jednání provozních a pracovních týmů zadavatele (2x měsíčně).

- Pravidelné zpracování reportů (reporting 1x měsíčně) a zpracování analýzy trendů z reportovaných údajů včetně zpracování doporučení (kvartálně):
    - SLA report dostupnosti jednotlivých DNS serverů a DNS služeb,
    - SLA report dostupnosti zařízení a služeb IPAM,
    - přehled provedených změn v konfiguraci DNS služeb.

POPIS POŽADOVANÉHO SLA

Kategorie A:

Výpadek jednoho nebo více DNS serverů, který zapříčiní nedostupnost DNS služby pro minimálně jednu nebo více hostovaných DNS domén, případně nedostupnost celé DNS služby. Nedostupností DNS služby se rozumí chybový stav, kdy primární ani záložní DNS server neodpovídají na klientské DNS dotazy hostovaných DNS domén v požadovaném čase.

U této kategorie požaduje zadavatel reakci do 2 hodin od nahlášení závady a její odstranění do 4 hodin od nahlášení závady.

Reaktivní podpora se zaručenou dobou odezvy na servisní požadavek do 2 hodin od nahlášení závady a její odstranění do 4 hodin. Pracovník uchazeče zahájí práce na odstranění závady do 2 hodin od nahlášení. V případě závady na systémech zadavatele či třetích stran bude pracovník uchazeče součástí řešitelského týmu do doby, kdy poskytované služby budou uvedeny opět do normálního funkčního stavu.
Služba musí být dostupná 24 hodin denně, od pondělí do neděle, včetně veškerých státních svátků, dnů pracovního klidu.

Kategorie B:

Závada nebo výpadek jednoho nebo více DNS serverů, který způsobí snížení dostupnosti DNS služeb, avšak nezapříčiní nedostupnost DNS služby v jednotlivých logických blocích.

Snížená dostupnost služeb, výkonnostní potíže.

U této kategorie požaduje zadavatel reakci do 4 hodin od nahlášení závady a její odstranění do 8 hodin od nahlášení závady.

Reaktivní podpora se zaručenou dobou odezvy na servisní požadavek do 4 hodin od nahlášení závady a její odstranění do 8 hodin. Práce na odstranění závady budou zahájeny nejpozději během následujícího pracovního dne po pracovním dni, kdy byla závada oznámena, a budou probíhat v pracovní dny v době od 08:00 do 17:00 hodin. V případě závady na systémech zadavatele či třetích stran bude pracovník poskytovatele součástí řešitelského týmu do doby, kdy poskytované služby budou uvedeny opět do normálního funkčního stavu. Služba musí být dostupná v pracovní dny, v době od 08:00 do 17:00 hodin.

Kategorie C:
Ostatní závady nespadající do kategorie A nebo B.

U této kategorie zadavatel požaduje odstranění do 2 dnů od nahlášení závady.

Po odstranění závady kategorie A, B, C bude informován ohlašovatel závady (pracovník oddělení správy komunikační a datové infrastruktury a podpory HW nebo jiný příslušný pracovník, který závadu nahlásil), který ověří funkčnost a potvrdí ukončení opravy. Potvrzení ukončení opravy bude považováno za okamžik ukončení opravy.

ZPŮSOB KONTROLY

Měření parametrů služby bude prováděno v pravidelných intervalech během zaručené provozní doby služby. Měřící body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Měřeními bude ověřována dostupnost jednotlivých DNS serverů a dostupnost DNS služby. Dostupnost služby se bude měřit souborem testů dostupnosti DNS služby v jednotlivých logických celcích a vybraných bodech sítě. Provozní činnosti budou kontrolovány zadavatelem (nebo jím stanoveným subjektem) na měsíční bázi. O výsledku kontrol bude sestavován měsíční report. Report vystavuje kontrolující subjekt, schvaluje zadavatele a slouží zadavateli jako podklad pro vyhodnocení služeb.

DALŠÍ PODMÍNKY

V případě obměny zařízení z důvodu náhrady vadného prvku, nebo z důvodu modernizace budou tato nová zařízení považována za ekvivalentní a budou na ně poskytovány stejné služby.

Povinnost zpřístupnit technologie pro definici a implementaci monitorovacích agentů/sond.

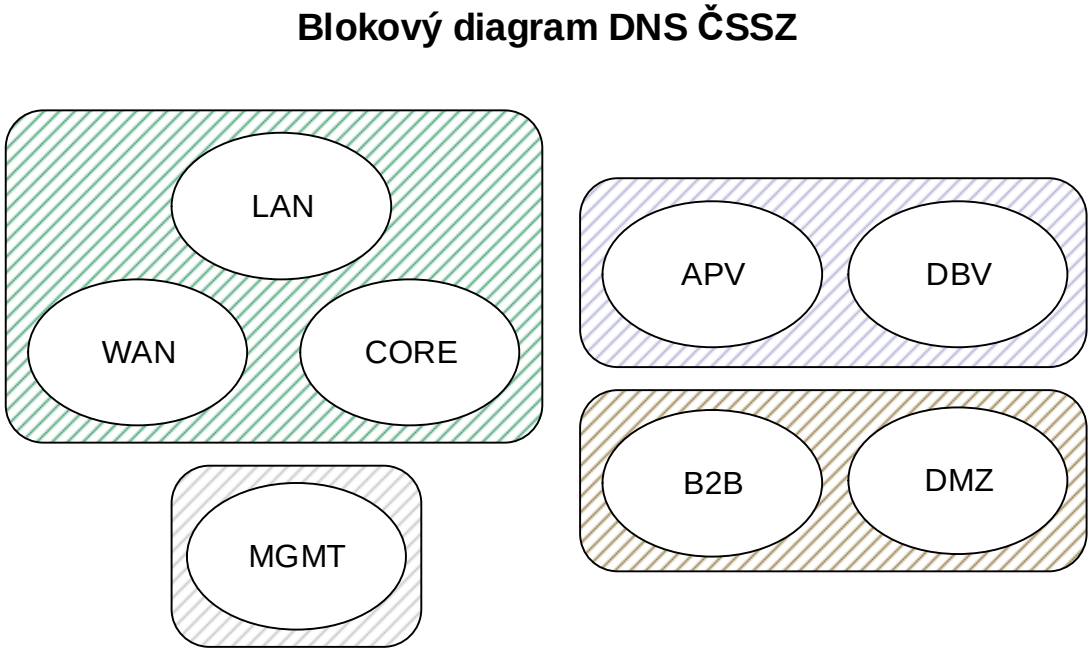
Povinnost poskytnout součinnost zadavateli (nebo jím jmenovaných subjektů) při provádění kontrolní činnosti na dodržování a plnění náplně této služby.

POŽADAVKY NA ODPOVĚĎ

Uchazeč vyplní u každé položky z kapitoly „Rozsah požadovaných činností“, zda jeho návrh poskytování služeb daný požadavek splňuje a jakým způsobem tento požadavek splňuje. Za účelem popisu, jak návrh poskytování služeb daný požadavek splňuje, připojí uchazeč popis splnění požadavků zadavatele, ve kterém uchazeč ke každému požadavku popíše, jak je tento požadavek řešen a (ne)naplněn, aby z tohoto popisu mohl zadavatel ověřit, zda je daný požadavek skutečně (ne)splněn.

Zadavatel uvádí, že požadavky, uvedené v kapitole „Rozsah požadovaných činností“, jsou požadavky, na kterých zadavatel trvá a výslovně prohlašuje, že návrhy jednotlivých uchazečů musí tyto požadavky zcela splňovat. V případě, že uchazeč jakoukoli z těchto položek nesplní, bude taková skutečnost ze strany zadavatele považována za nesplnění zadávacích podmínek s následkem vyloučení uchazeče z účasti v zadávacím řízení

Síť ČSSZ je logický rozdělená do několika bloků podle následujícího diagramu. Podle tohoto rozdělení je i principiálně koncipován systém DNS. V dalších kapitolách je popsáno řešení systému DNS v jednotlivých celcích.



Obrázek 1: Blokový diagram DNS ČSSZ

DMZ

ČSSZ v současnosti zajišťuje DNS službu pro externí a interní domény. Externí domény jsou provozované na Linuxových serverech dns.cssz.cz a dns2.cssz.cz v primární a v záložní lokalitě. Další záložní DNS server je umístěn u Internetového providera. Linuxové DNS servery (DNS platforma BIND) jsou zároveň NTP servery pro ČSSZ síť.

ČSSZ na zmíněných serverech provozuje řádově 30 DNS domén.

Core, LAN, WAN

DNS v části Core+LAN+WAN je provozována na Microsoft doménových kontrolérech v primární a záložní lokalitě. Podobně jako u externích DNS serverů, interní DNS servery jsou také NTP servery. Interní LAN klienti používají současně jeden DNS server z primární lokality a jeden ze sekundární lokality. Na DNS serverech v Core síti je provozováno řádově 20 DNS domén.

Pobočky ČSSZ mají vlastní DNS server. Tento server je využíván pobočkovým serverem s operačním systémem Solaris a také jako sekundární DNS server pro pracovní stanice uživatelů. Pracovní stanice uživatelů na pobočkách používají primární DNS server z primárního datového centra.

MGMT

V management zóně se nacházejí dva DNS servery spravující doménu net.cssz.cz. DNS servery jsou vybudovány nad operačním systémem Linux na DNS platformě BIND.

V rámci reverzní zóny 10.in-addr.arpa zajišťují DNS servery kompletní překlad jmen pomocí automaticky generované konfigurace – zajišťuje systém IMS popsaný v kapitole 4.1.6. IP adresy, které jsou definovány přímo v doméně net.cssz.cz jsou pomocí hostových NS záznamů směrovány na záložní DNS server a ostatní reverzní záznamy se posílají na MS AD servery držící doménu cssz.cz.

APV

Síť APV se dělí na 3 prostředí:

- produkční
- testovací a akceptační
- integrační

Prostředí jsou distribuována přes dvě lokality. Produkční a testovací prostředí používají společné DNS servery, jeden v primární a druhý v sekundární lokalitě. Integrační prostředí využívá oddělených DNS serverů.

Servery prostředí APV jsou provozovány na platformě Microsoft Windows.

DNS služba v rámci B2B prostředí

Směrování provozu ze serverů v APV vrstvě datového centra ČSSZ na B2B kanál je zajištěno pomocí modifikace DNS odpovědí pro cílové servery. DNS servery APV vrstvy datového centra ČSSZ mají nastavený B2B kanál jako DNS forward servery, na které přeposílají DNS dotazy pro záznamy nepatřící do domény cssz.cz. DNS služba běžící na B2B serverech vrací v odpovědích na DNS dotazy virtuální IP adresu B2B kanálu publikovanou v APV vrstvě datového centra ČSSZ.

V rámci B2B služby jsou provozovány 4 DNS servery (v každé lokalitě 2) založené na operačním systému Linux, DNS platforma BIND. Zde je definováno řádově 20 DNS domén.

DBV

V síti DBV je umístěn DNS server založený na platformě IBM AIX. Tento server poskytuje zóny:

- db.cssz.cz
- i-db.cssz.cz
- t-db.cssz.cz

Systém IPAM – správa IP adresního prostoru

Pro účely správy IP adresního prostoru provozuje ČSSZ systém IPAM založený na řešení InfoBlox appliance. Systém IPAM je nasazen jako evidenční nástroj přidělených podsítí včetně identifikace využití dané podsítě. Nástroj slouží správcům MPSV a ČSSZ pro usnadnění správy adresního prostoru v současnosti pro IPv4 a do budoucna i adresní prostor IPv6.

Nástroj IPAM v prostředí ČSSZ se skládá z následujících komponent:

Zařízení Infoblox Trinzic 1420 sloužící jako GRID Master pro ČSSZ

Zařízení Infoblox Trinzic 1420 sloužící jako Multi-GRID Manager (MGM) nadřazený jednotlivým GRID Masterům

MGMT je použit na centrální rozdělení adresních rozsahů pro jednotlivé organizace a zajišťuje tak konzistenci IP adresních rozsahů mezi jednotlivými organizacemi.

LOKALITA

Křížová 6, 25 (K6, K25), Praha 5

Trojská 13 (T13), Praha 8

SEZNAM ZAŘÍZENÍ

1. DNS servery B2B – 4x Linux + BIND
2. DNS servery DMZ – 2x Linux + BIND
3. DNS servery MGMT – 2x Linux + BIND
4. Systém IPAM Infoblox – 2x appliance Infoblox Trinzic 1420, jednou Multi-GRID Manager a jednou GRID Master

4.1.5 PROVOZ A SPRÁVA INFRASTRUKTURY NTP

Jedná se o zajištění provozu vyjmenovaných komponent NTP služby umístěných na zařízeních zadavatele. Požadovány jsou zejména následující činnosti:

- Provoz služby NTP
    - profylaktické činnosti, kontrola systému NTP
    - kontrola logů (na týdenní bázi)
    - kontrola monitoringu služby NTP (na měsíční bázi)
    - návrh preventivních opatření vyplývající z monitoringu a profylaktických činností s cílem předejít možným výpadkům a omezením služby NTP
    - odborná technická podpora a odstraňování závad v předmětné oblasti – 2nd level support (na denní bázi)
    - provádění pravidelných záloh konfigurací služby NTP. Uchazeč navrhne a popíše potřebný rozsah zálohování
    - vedení provozního deníku služby NTP
- Správa služby NTP:
    - Kontrola dostupnosti patchů, hotfix-ů, service pack-ů a dalších opravných balíků výrobce/vydavatele (na měsíční bázi)
    - údržba služby NTP - údržba konfigurace (změny v nastavení povolených přístupů, nadřazených NTP serverů)
    - analýza vhodnosti a potřebnosti implementace opravného balíku
    - návrh opatření a postupu implementace opravného balíku ke schválení zadavateli
    - instalace a provedení změn dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna 1x měsíčně),
    - implementace schválených požadavků na změnu konfigurace služby NTP
    - předkládání návrhů na optimalizaci NTP služeb (na kvartální bázi).
- Součinnost v rámci procesů „Projektového řízení“ souvisejících s návrhem změn v infrastruktuře ICT zadavatele.
- Pravidelné zpracování reportů (reporting 1x měsíčně) a zpracování analýzy trendů z reportovaných údajů včetně zpracování doporučení (kvartálně):
    - SLA report dostupnosti jednotlivých NTP serverů a NTP služby,

- SLA report dostupnosti NTP služby na síťových přepínačích,
- přehled provedených změn v konfiguraci NTP služby.

- Účast na jednání provozních a pracovních týmů zadavatele (2x měsíčně).

POPIS POŽADOVANÉHO SLA

Kategorie A:

Výpadek jednoho nebo více NTP serverů, který zapříčiní nedostupnost celé NTP služby. Nedostupností NTP služby se rozumí chybový stav, kdy primární ani záložní NTP server neodpovídají na dotazy NTP klientům v požadovaném čase, nebo čas poskytovaný službou NTP je s přesností menší než 1/100 sekundy

.

U této kategorie požaduje zadavatel reakci do 2 hodin od nahlášení závady a její odstranění do 4 hodin od nahlášení závady.

Reaktivní podpora se zaručenou dobou odezvy na servisní požadavek do 2 hodin od nahlášení závady a její odstranění do 4 hodin. Pracovník uchazeče zahájí práce na odstranění závady do 2 hodin od nahlášení. V případě závady na systémech zadavatele či třetích stran bude pracovník uchazeče součástí řešitelského týmu do doby, kdy poskytované služby budou uvedeny opět do normálního funkčního stavu.

Služba musí být dostupná 24 hodin denně, od pondělí do neděle, včetně veškerých státních svátků a dnů pracovního klidu.

Kategorie B:

Závada nebo výpadek jednoho nebo více NTP serverů, který způsobí snížení dostupnosti NTP služby, avšak nezapříčiní nedostupnost NTP služby.

Snížená dostupnost služeb, výkonnostní potíže.

U této kategorie požaduje zadavatel reakci do 4 hodin od nahlášení závady a její odstranění do 8 hodin od nahlášení závady.

Reaktivní podpora se zaručenou dobou odezvy na servisní požadavek do 4 hodin od nahlášení závady a její odstranění do 8 hodin. Práce na odstranění závady budou zahájeny nejpozději během následujícího pracovního dne po pracovním dni, kdy byla závada oznámena, a budou probíhat v pracovní dny v době od 08:00 do 17:00 hodin. V případě závady na systémech zadavatele či třetích stran bude pracovník uchazeče součástí řešitelského týmu do doby, kdy poskytované služby budou uvedeny opět do normálního funkčního stavu. Služba musí být dostupná v pracovní dny, v době od 08:00 do 17:00 hodin.

Kategorie C:

Ostatní závady nespadající do kategorie A nebo B.

U této kategorie zadavatel požaduje odstranění závady do 2 dnů od nahlášení závady.

Po odstranění závady kategorie A, B, C bude informován ohlašovatel závady (pracovník oddělení správy komunikační a datové infrastruktury a podpory HW nebo jiný příslušný

pracovník, který závadu nahlásil), který ověří funkčnost a potvrdí ukončení opravy. Potvrzení ukončení opravy bude považováno za okamžik ukončení opravy.

Způsob kontroly

Měření parametrů služby bude prováděno v pravidelných intervalech během zaručené provozní doby služby. Měřící body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Měřeními bude ověřována dostupnost jednotlivých NTP serverů a dostupnost NTP služby. Dostupnost služby se bude měřit souborem testů dostupnosti NTP služby v jednotlivých logických celcích a vybraných bodech sítě. Provozní činnosti budou kontrolovány zadavatelem (nebo jím stanoveným subjektem) na měsíční bázi. O výsledku kontrol bude sestavován měsíční report. Report vystavuje kontrolující subjekt, schvaluje zadavatel a slouží zadavateli jako podklad pro vyhodnocení služeb.

Další podmínky

V případě obměny zařízení z důvodu náhrady vadného prvku, nebo z důvodu modernizace budou tato nová zařízení považována za ekvivalentní a budou na ně poskytovány stejné služby. Povinnost zpřístupnit technologie pro definici a implementaci monitorovacích agentů/sond. Povinnost poskytnout součinnost zadavateli (nebo jím jmenovaných subjektů) při provádění kontrolní činnosti na dodržování a plnění náplně této služby

POŽADAVKY NA ODPOVĚĎ

Uchazeč vyplní u každé položky z kapitoly „Rozsah požadovaných činností“, zda jeho návrh poskytování služeb daný požadavek splňuje a jakým způsobem tento požadavek splňuje. Za účelem popisu, jak návrh poskytování služeb daný požadavek splňuje, připojí uchazeč popis splnění požadavků zadavatele, ve kterém uchazeč ke každému požadavku popíše, jak je tento požadavek řešen a (ne)naplněn, aby z tohoto popisu mohl zadavatel ověřit, zda je daný požadavek skutečně (ne)splněn.

Zadavatel uvádí, že požadavky, uvedené v kapitole „Rozsah požadovaných činností“, jsou požadavky, na kterých zadavatel trvá a výslovně prohlašuje, že návrhy jednotlivých uchazečů musí tyto požadavky zcela splňovat. V případě, že uchazeč jakoukoli z těchto položek nesplní, bude taková skutečnost ze strany zadavatele považována za nesplnění zadávacích podmínek s následkem vyloučení uchazeče z účasti v zadávacím řízení.

POPIS SOUČASNÉHO STAVU PROSTŘEDÍ

Časová synchronizace v ČSSZ je realizovaná pomocí dvou NTP serverů umístěných v DMZ, jeden v primární a jeden v sekundární lokalitě. Jedná se o NTP servery s operačním systémem Linux, které získávají čas z Internetu. Tyto základní NTP servery jsou označovány jako NTP1.

Podle serveru NTP1 se synchronizují AD doménové kontroléry, které pak udržují přesný čas v Microsoft AD doméně. S doménovým časem se synchronizují všichni členové domény, tedy i počítače na pobočkách.

Síťové prvky se synchronizují přes centrální přepínače na lokalitách zadavatele na adrese Křížová 6, Křížová 25 a Trojská 13. Centrální přepínače získávají čas z NTP serverů NTP1.

LOKALITA

Křížová 6, 25 (K6, K25), Praha 5

Trojská 13 (T13), Praha 8

SEZNAM ZAŘÍZENÍ

1. NTP servery DMZ – 2x Linux
2. Všechny aktivní síťové prvky zadavatele

4.1.6 PROVOZ A SPRÁVA SYSTÉMU IMS

Součástí služeb požadovaných od uchazeče je zajištění a provoz integrovaného informačního systému správy síťové infrastruktury IMS (Infrastructure Management System). Jedná se o službu kompletního zajištění IMS systému. Uchazeč naimplementuje a zaintegruje požadovaný systém na HW platformu zadavatele ve formě virtuálního serveru. Tento systém bude k dispozici jednak uchazeči a umožní mu zajistit požadovanou funkcionalitu, datové zdroje a výstupy. Dále bude tento systém v definované formě přístupný i omezené skupině zaměstnanců zadavatele. Systém bude fyzicky implementován v datovém centru zadavatele, nicméně bude dodáván jako služba a jeho dostupnost bude omezena platností smlouvy na provoz síťové infrastruktury zadavatele definované v kapitolách 4.1.1 až 4.1.10 této zadávací dokumentace. Uchazeč bude také zodpovědný za dostatečnou kapacitu a výkonnost tohoto systému s ohledem na rozsáhlost spravované infrastruktury zadavatele. Řádově se bude jednat o 2000 síťových prvků a 2000 serverů.

FUNKČNÍ POŽADAVKY NA SYSTÉM IMS

Jednou z hlavních funkcí IMS systému je evidence spravovaných síťových prvků. Systém musí poskytovat kompletní seznam prvků s detailními parametry a vlastnostmi ke každé položce minimálně v rozsahu dle následujícího seznamu:

- Typ zařízení
- Status (musí být dokumentován celý životní cyklus - planned/active/historic)
- Funkce, role, služby
- Adresy, DNS záznamy
- Umístění (lokalita, místnost, skříň)
- Zapojení jednotlivých síťových rozhraní
- Zapojení rozhraní pro správu (konzolové, MGMT porty)
- Přístupové informace (povolené zdroje, protokoly, SNMP konfigurace)
- Software (operační systém, licence, add-on moduly)
- Seznam HW komponent vč. sériových čísel
- Servisní informace a záznamy

Veškeré datové zdroje budou plnohodnotně přístupné pro čtení, vytvoření, změnu a smazání pomocí externího SOAP/REST API.

IMS systém bude poskytovat konfigurovatelné reporty z evidence síťových prvků ve formátu Office Open XML, OpenDocument a/nebo PDF.

Veškeré informace v evidenci síťových prvků budou automaticky synchronizovány s aktuálním stavem sítě na principu zpětné vazby. Tato synchronizace se bude týkat minimálně hardwarových změn a provozního stavu jednotlivých prvků.

Systém IMS poskytne pro všechny evidované prvky statické URL obsahující definovanou informaci.

IMS systém bude poskytovat i funkci skenování a rozpoznání sítě a prvků v síti. K dispozici budou následující funkce a metody:

Flexibilní profily a pravidla discovery

- profily: metody (ICMP/SNMP) a parametry (community, timeout)
- aplikace a prioritizace profilu podle síťových rozsahů
- aplikace relevantních mechanismů (ARP/CDP/...) dle typu zařízení

ICMP ping scan

SNMP scan

analýza ARP záznamu prvků

analýza CDP tabulek

analýza LLDP tabulek

analýza routovacích tabulek

analýza sousedství prvků (OSPF, BGP, EIGRP)

ruční kontrola a potvrzení objevených parametrů

Network Discovery funkce bude dostupná na systému IMS i externě pomocí SOAP/REST API.

IMS systém bude poskytovat uživatelům archiv konfigurací jednotlivých síťových prvků.

Automatické zálohování konfigurací síťových prvků bude dostupné minimálně pro následující typy prvků:

- Cisco ACE
- Cisco CSS
- Cisco FWSM, ASA, PIX
- Cisco IDSM
- Cisco IOS
- Cisco NX-OS
- HP Comware
- HP ProCurve
- HP Virtual Connect
- možnost přidání a definice dalších typů (pomocí protokolů SNMP, SSH, Telnet, HTTPS, uživatelsky definované skritpty)

Archiv konfigurací síťových prvků v systému IMS bude poskytovat také následující funkce:

- Prohlížení archivu konfigurací pomocí Web rozhraní.
- Možnost porovnání jednotlivých verzi.
- Vyhledávání verzí, ve které přibyl nebo byl odstraněn určitý přikaz.
- Dostupnost archivu konfigurací externě pomocí SOAP/REST API.

Mimo evidenci síťových prvků bude systém IMS poskytovat i informace a evidenci jednotlivých sítí (IP, IPv6) a síťových segmentů použitých v infrastruktuře zadavatele.

Pro uživatele IMS systému budou k dispozici minimálně následující informace a funkcionality:

- Adresace (vč. podpory více rozsahů ve stejném segmentu).
- Vazba na aktivní prvky (seznam zařízení, kde se daný síťový segment vyskytuje).
- Nazvy a čísla VLAN na jednotlivých prvcích (podporováno bude i mapování VLAN).
- Role jednotlivých prvků (router, root atp.).
- Další relevantní parametry (STP, HSRP).
- K čemu je daný segment použit.
- Vyhledání dle lokality, prostředí, aplikace a dalších parametrů.
- Podpora překryvných adresních prostorů (VRF).

Systém IMS umožní obousměrnou synchronizaci dat se systémem IPAM od firmy Infoblox, který má zadavatel implementován ve stávající infrastruktuře.

Systém IMS bude také poskytovat informace a evidenci fyzických a virtuálních serverů. Tyto data jsou důležitá pro kvalitní zajištění správy sítí LAN, WAN a DC a také pro automatizaci přípravy konfigurací síťových prvků. Poskytují komplexní obrázek o návaznosti síťové infrastruktury na obecnou IT infrastrukturu.

Pro servery obecně budou v IMS systému k dispozici následující informace:

- Adresace a umístění do VLAN jednotlivých síťových rozhraní
- Operační systém
- Role (aplikace, služby)

Pro fyzické servery budou v IMS systému k dispozici následující informace:

- Umístění (lokalita, místnost, skříň)
- Zapojení jednotlivých síťových rozhraní do portu switchů
- Adresace speciálních rozhraní (iLO)
- HW parametry

Pro virtuální servery budou k dispozici následující informace:

- Alokované zdroje
- Role (aplikace, služby)

Systém IMS bude také poskytovat informace a evidenci aplikací a VIP virtuálních adres. Tyto data jsou důležitá pro kvalitní zajištění správy sítí LAN, WAN a DC. Poskytují komplexní obrázek o návaznosti síťové infrastruktury na aplikační vrstvu. Pro aplikace a VIP adresy budou v IMS systému k dispozici následující informace:

- Popis, kontakty za vlastníky nebo zodpovědné osoby.
- Role serverů.
- Přiřazené VIP adresy, DNS záznamy.
- Mechanismy rozložení zátěže.
- Přiřazené servery včetně rolí.
- Povolená příchozí komunikace (uživatele, jiné aplikace, třetí strany, atp.)
- Povolená odchozí komunikace.

Přístupy a role jednotlivých uživatelů a operátorů systému IMS budou řízeny centralizovaně pomocí standardních nástrojů dostupných ve stávající IT architektuře zadavatele. Systém IMS bude podporovat možnosti následující integrace:

- Autentizace operátorů pomocí Cisco ACS.
- Autorizace pomocí interní databáze systému IMS.
- Řízení práv uživatelů přes Web UI.
- Role-based access control.
- Možnost napojení na AAA vrstvu dle standardu zadavatele (popis WebSeal/AAAAPI je k dispozici v příloze Zadávací Dokumentace).
- SOAP/REST API pro řízení práv uživatelů.

Systém IMS bude poskytovat rozhraní pro pověřené pracovníky zadavatele umožňující zadávání jednotlivých funkčních požadavků:

- Změnové požadavky na rekonfiguraci LAN/WAN/DC zařízení
  - Zavedení/Změna/Zrušení L2 Vlan
  - Konfigurace L2 rozhraní
  - Konfigurace L3 rozhraní
  - Zavedení/Změna/Zrušení VIP adresy na ACE
  - Zavedení/Změna/Zrušení Access-list
- Požadavky na DNS záznam (zřízení/změna/zrušení)
- Zavedení/změna/zrušení služby B2B rozhraní

Zavedení/Změna/Zrušení uživatele/systému na centrálních ACS serverech

Zavedení/Změna/Zrušení Aplikace

Zavedení/Změna/Zrušení Serveru

Rozhraní IMS systému musí být přístupné přes:

- Web UI
- SOAP/REST API

Systém IMS bude umožňovat vytvoření schémat provádění jednotlivých činností, sledování jejich průběhu a vyhodnocování výsledků.

- Autorizace změn včetně přidělování potřebných zdrojů
- Automatická distribuce požadovaných konfiguračních změn
- Automatizované vedení provozního deníku
- Audit změn
- Vyhodnocení výsledku nasazení nových konfigurací
- Trasování konfiguračních změn s možností návratu k poslední funkční konfiguraci

Systém IMS bude umožňovat automatizované provedení změn v konfiguracích vitalizačního prostředí VMware vSphere, minimálně v následujícím rozsahu:

- Zavedení/Změna/Zrušení virtuálních sítí
- Správa síťových rozhraní jednotlivých VM
- Nastavení port mirroring

Dále systém IMS bude podporovat načtení aktuálního stavu konfigurací vSphere včetně informací o sítích a virtuálních serverech.

Systém IMS bude umožňovat automatizované provedení změn v konfiguracích HP Virtual Connect modulů, minimálně v následujících parametrech:

- Network, network-range
- Server profile
- Server port map
- Uplink port, uplink set
- Port monitor

Systém IMS bude umožňovat automatizované provedení změn v konfiguracích Cisco ACE modulů včetně podpory virtuálních kontextů jednotlivých provozních prostředí a vrstev, minimálně v následujících parametrech:

- interface
- policy-map
- class-map
- sticky
- serverfarm
- probe

- rserver
- Access-list
- Parameter-map
- NAT

Systém IMS bude umožňovat automatizované provedení změn v konfiguracích Cisco FWSM modulů, ASA a PIX zařízení včetně podpory virtuálních kontextů jednotlivých provozních prostředí a vrstev, minimálně v následujících parametrech:

- Interface
- Object-group
- Access-list
- Global NAT
- Static

Systém IMS bude umožňovat automatizované provedení změn v konfiguracích Cisco IOS zařízení včetně podpory virtuálních směrovacích instancí jednotlivých provozních prostředí a vrstev, minimálně v následujících parametrech:

- Vlan
- Interface (nastavení L2/3 parametrů, změna provozního stavu)
- Access-list
- Route-map
- Policy routing
- Parametry STP
- Nastavení SPAN, RSPAN

Systém IMS bude umožňovat automatizované provedení změn v konfiguracích Cisco Nexus zařízení včetně podpory jednotlivých provozních prostředí a vrstev, minimálně v následujících parametrech:

- Vlan
- Interface (nastavení L2/3 parametrů, změna provozního stavu)
- Access-list
- Route-map
- Policy routing
- Parametry STP
- Nastavení SPAN, RSPAN

Systém IMS bude umožňovat automatizované provedení změn v konfiguracích HP přepínačů, minimálně v následujících parametrech:

- Vlan
- Interface (nastavení L2/3 parametrů, změna provozního stavu)
- Access-list
- Parametry STP
- Nastavení SPAN, RSPAN

ZPŮSOB KONTROLY

Měření parametrů služby bude prováděno v pravidelných intervalech během zaručené provozní doby služby. Měřící body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Měřeními bude ověřována dostupnost jednotlivých IMS serverů a dostupnost IMS služby. Dostupnost služby se bude měřit souborem testů dostupnosti IMS služby v jednotlivých logických celcích a vybraných bodech sítě. Provozní činnosti budou kontrolovány zadavatelem (nebo jím stanoveným subjektem) na měsíční bázi. O výsledku kontrol bude sestavován měsíční report. Report vystavuje kontrolující subjekt, schvaluje zadavatele a slouží zadavateli jako podklad pro vyhodnocení služeb.

DALŠÍ PODMÍNKY

V případě obměny zařízení z důvodu náhrady vadného prvku, nebo z důvodu modernizace budou tato nová zařízení považována za ekvivalentní a budou na ně poskytovány stejné služby systémem IMS.

Povinnost zpřístupnit technologie pro definici a implementaci monitorovacích agentů/sond. Povinnost poskytnout součinnost zadavateli (nebo jím jmenovaných subjektů) při provádění kontrolní činnosti na dodržování a plnění náplně této služby

POŽADAVKY NA ODPOVĚĎ

Uchazeč vyplní u každé položky z kapitoly „Rozsah požadovaných činností“, zda jeho návrh poskytování služeb daný požadavek splňuje a jakým způsobem tento požadavek splňuje. Za účelem popisu, jak návrh poskytování služeb daný požadavek splňuje, připojí uchazeč popis splnění požadavků zadavatele, ve kterém uchazeč ke každému požadavku popíše, jak je tento požadavek řešen a (ne)naplněn, aby z tohoto popisu mohl zadavatel ověřit, zda je daný požadavek skutečně (ne)splněn.

Součástí odpovědi uchazeče bude popis nabízeného systému, minimálně v následujícím rozsahu:

- Popis celkové architektury systému
- Popis použitých a dostupných modulů
- Popis bezpečnostního modelu (RBAC)
- Popis uživatelského rozhraní
- Popis poskytovaného programového rozhraní API
- Popis mechanizmu interakce se spravovanými zařízeními v rozsahu zajištění funkčních požadavků na systém IMS
- CLI rozhraní, pokud je podporované

Uchazeč popíše zvolenou metodiku pro nasazení systému IMS, minimálně v následujícím rozsahu:

- Harmonogram implementace a dostupnosti systému pro plné využití
- Popis požadavků na součinnost zadavatele při nasazení systému
- Doba potřebná pro přidání/změnu nového typu požadavků
- Doba potřebná pro integraci s novým typem zařízení

Zadavatel uvádí, že požadavky, uvedené v kapitole „Rozsah požadovaných činností“, jsou požadavky, na kterých zadavatel trvá a výslovně prohlašuje, že návrhy jednotlivých uchazečů musí tyto požadavky zcela splňovat. V případě, že uchazeč jakoukoli z těchto položek nesplní, bude taková skutečnost ze

strany zadavatele považována za nesplnění zadávacích podmínek s následkem vyloučení uchazeče z účasti v zadávacím řízení.

POPIS SOUČASNÉHO STAVU PROSTŘEDÍ

Stávající služba systému IMS (Infrastructure Management System) je poskytována současným dodavatelem. Předmětem této poptávky je poskytnutí IMS systému jako služby v rozsahu výše popsaných požadavků.

LOKALITA

Křížová 6, 25 (K6, K25), Praha 5

Trojská 13 (T13), Praha 8

4.1.7 SPRÁVA A DOHLED PŘÍSTUPU K SÍŤOVÝM PRVKŮM

ROZSAH POŽADOVANÝCH ČINNOSTÍ

1. Provoz aktivních síťových prvků v obou lokalitách:
    a. Profylaktické činnosti:
        i. Při pravidelných odstávkách (1x ročně) – fyzická kontrola, čištění síťových zařízení, úprava kabeláži,
        ii. Pravidelné fyzické kontroly s technikem ICT: fyzická kontrola provozního stavu prvků (teplota, hluk zařízení) 1x ročně,
    b. kontrola logů (na denní bázi),
    c. kontrola výkonnosti a performance monitoring (na měsíční bázi),
    d. návrh preventivních opatření s cílem předejít možným výpadkům (minimálně kvartálně nebo dle aktuální situace),
    e. odborná technická podpora a odstraňování závad v předmětné oblasti – 2nd level support v souladu se SLA,
    f. provádění pravidelných záloh SW konfigurací (měsíční zálohy + aktualizace záloh po každé změně).
2. Správa aktivních prvků v obou lokalitách
    a. Kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobců (na měsíční bázi),
    b. analýza vhodnosti a potřebnosti implementace opravného balíku,
    c. návrh opatření a postupu implementace opravného balíku ke schválení zadavateli,
    d. instalace a provedení změn (včetně práce) dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna 1x měsíčně, pokud není potřeba jednat rychleji),
    e. implementace schválených požadavků na přídání, změnu či zrušení seznamu oprávněných zařízení (předpokládaný rozsah je až 10 změnových požadavků měsíčně),
    f. implementace schválených požadavků na zavedení, změnu a zrušení lokálních uživatelů (předpokládaný rozsah je až 10 změnových požadavků měsíčně),
    g. implementace schválených požadavků na zavedení, změnu a zrušení AAA politik (předpokládaný rozsah je až 2 změnových požadavků měsíčně),
    h. správa a aktualizace serverových a certifikátů CA ČSSZ,

i. správa a aktualizace privilegovaných hesel ke všem předmětným zařízením (pravidelné aktualizace a předání zadavateli) musí být vedeno v souladu s bezpečnostní politikou zadavatele.

3. Zprostředkování HW/SW servisu aktivních prvků (u výrobce/dodavatele) včetně případného zajištění náhrady v případě poruchy (v rozsahu smluvně zajištěné maintenance zadavatele).
4. Správa a aktualizace provozní dokumentace v rozsahu:
    a. Postupy pro provoz a správu každého zařízení,
    b. postupy pro obnovu zařízení ze záloh,
    c. provozní deník pro každé zařízení v minimálním rozsahu datum, osoba, číslo požadavku z ticket systému, popis prováděné činnosti, výsledek činnosti (úspěch/selhání), doba trvání.
5. Správa a aktualizace technické dokumentace v rozsahu:
    a. Aktuální schéma fyzického zapojení ACS serverů,
    b. aktuální schéma logického zapojení ACS serverů (VLAN, porty, prvky),
    c. aktuální přehled verzí OS aktivních prvků,
    d. správa konfigurací předmětných zařízení v konfigurační DB zadavatele (IP, SN).
6. Účast na jednání provozních a pracovních týmů zadavatele (2xměsíčně).
7. Pravidelné zpracování reportů (reporting 1x měsíčně):
    a. SLA report dostupnosti infrastruktury ACS serverů
    b. Přehled provedených změn v konfiguraci infrastruktury ACS serverů

POPIS POŽADOVANÉHO SLA

Kategorie A:

Výpadek jednoho nebo více ACS serverů, který zapříčiní nedostupnost celé infrastruktury ACS serverů. Nedostupností infrastruktury ACS serverů se rozumí nemožnost přístupu na management rozhraní síťových zařízení pomocí centrálně spravovaných uživatelských účtů nebo nemožnost přístupu k bezdrátovému připojení WiFi ČSSZ.

U této kategorie požaduje zadavatel opravu či odstranění závady garantované do 6 hodin od nahlášení závady.

Reaktivní podpora na HW s garantovanou dobou opravy či odstranění závady do 6 hodin od nahlášení závady. Pracovník uchazeče se dostaví na místo opravy do 2 hodin po nahlášení a poskytuje pracovní sílu, náhradní díly a případně další materiál, potřebný k opravě nebo výměně tak, aby HW výrobky byly uvedeny opět do normálního funkčního stavu. Uchazeč identifikuje a opraví špatné funkce a závady výrobku. Vyměněné díly se stanou majetkem uchazeče.

Služba musí být dostupná 24 hodin denně, od pondělí do neděle, včetně veškerých státních svátků a dnů pracovního klidu.

Kategorie B:

Závada nebo výpadek části prvku, který způsobí snížení dostupnosti služeb, avšak nezapříčiní výpadek celé infrastruktury ACS serverů:

a. Závada redundantních zařízení (karet, napájecích zdrojů, modulů a případně dalších), při kterých nedojde k výpadku záložního zařízení,

b. výpadek jednoho ACS serveru, který nezpůsobí výpadek respektive nedostupnost celé infrastruktury ACS serverů.

Snížená dostupnost služeb, výkonnostní potíže.

U této kategorie požaduje zadavatel reakci do 4 hodin od nahlášení závady a její odstranění do 8 hodin od nahlášení závady.

Reaktivní podpora na HW se zaručenou dobou odezvy na servisní požadavek do 4 hodin od nahlášení závady a její odstranění do 8 hodin. Práce na odstranění závady budou zahájeny nejpozději během následujícího pracovního dne po pracovním dni, kdy byla závada oznámena, a budou probíhat v pracovní dny v době od 08:00 do 17:00 hodin. Služba musí být dostupná v pracovní dny, v době od 08:00 do 17:00 hodin.

Kategorie C:

Závady, které nezpůsobí výpadek ani nesníží dostupnosti služeb v rámci infrastruktury ACS serverů. Ostatní závady nespadající do kategorie A nebo B.

U této kategorie zadavatel požaduje odstranění do 2 dnů od nahlášení závady.

Po odstranění závady kategorie A, B, C bude informován ohlašovatel závady (pracovník oddělení správy komunikační a datové infrastruktury a podpory HW nebo jiný příslušný pracovník, který závadu nahlásil), který ověří funkčnost a potvrdí ukončení opravy. Potvrzení ukončení opravy bude považováno za okamžik ukončení opravy.

Způsob kontroly

Měření parametrů služby bude prováděno v pravidelných intervalech během zaručené provozní doby služby. Měřící body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Měřeními bude ověřována dostupnost infrastruktury WiFi sítě a jejích služeb. Dostupnost služby se bude měřit souborem testů dostupnosti spravovaných aktivních prvků. Provozní činnosti budou kontrolovány zadavatelem (nebo jím stanoveným subjektem) na měsíční bázi. O výsledku kontrol bude sestavován měsíční report. Report vystavuje kontrolující subjekt, schvaluje zadavatel a slouží zadavateli jako podklad pro vyhodnocení služeb.

Další podmínky

V případě obměny zařízení z důvodu náhrady vadného prvku, nebo z důvodu modernizace budou tato nová zařízení považována za ekvivalentní a budou na ně poskytovány stejné služby.

Povinnost zpřístupnit technologie pro definici a implementaci monitorovacích agentů/sond.

Povinnost poskytnout součinnost zadavateli (nebo jím jmenovaných subjektů) při provádění kontrolní činnosti na dodržování a plnění náplně této služby.

POŽADAVKY NA ODPOVĚĎ

Uchazeč vyplní u každé položky z kapitoly „Rozsah požadovaných činností“, zda jeho návrh poskytování služeb daný požadavek splňuje a jakým způsobem tento požadavek splňuje. Za účelem popisu, jak návrh poskytování služeb daný požadavek splňuje, připojí uchazeč popis splnění požadavků zadavatele, ve kterém uchazeč ke každému požadavku popíše, jak je tento požadavek

řešen a (ne)naplněn, aby z tohoto popisu mohl zadavatel ověřit, zda je daný požadavek skutečně (ne)splněn.

Zadavatel uvádí, že požadavky, uvedené v kapitole „Rozsah požadovaných činností“, jsou požadavky, na kterých zadavatel trvá a výslovně prohlašuje, že návrhy jednotlivých uchazečů musí tyto požadavky zcela splňovat. V případě, že uchazeč jakoukoli z těchto položek nesplní, bude taková skutečnost ze strany zadavatele považována za nesplnění zadávacích podmínek s následkem vyloučení uchazeče z účasti v zadávacím řízení.

POPIS SOUČASNÉHO STAVU PROSTŘEDÍ

Centralizovanou správu bezpečnostních oprávnění pro správu síťové infrastruktury ČSSZ zajišťuje dvojce AAA serverů Cisco model CSACS-1121-K9 (ACS), nainstalovaných na lokalitě zadavatele na adrese Křížová 25 a Trojská 13. Oba ACS servery jsou nakonfigurované pod společnou správu kde ACS server na lokalitě Křížová 25 je primární nod a ACS server na lokalitě zadavatele na adrese Trojská 13 je sekundární nod. Veškeré konfigurační změny se provádí na primární ACS nodu, který zároveň plní i funkci log serveru. Z pohledu ověřování uživatelských přístupů pracují oba ACS servery v módu Active/Active s podporou protokolů TACACS+ a RADIUS.

Z hlediska logického začlenění do síťové infrastruktury ČSSZ jsou ACS servery součástí centrální infrastruktury ČSSZ.

ACS servery používají dvě databáze uživatelských účtů:

- Lokální databáze
- MS Active Directory

LOKÁLNÍ DATABÁZE

Lokální databáze ACS serverů slouží pro ověřování následujících přístupů:

- Ověřování administrátorů sítě LAN/WAN při přístupu na management rozhraní síťových zařízení,
- ověřování přístupu do systému IMS,
- ověřování přístupu do systému IPAM.

Každý uživatel je přiřazen do příslušné skupiny dle požadované úrovně oprávnění a členění uživatelských skupin je zvoleno s ohledem na efektivní správu přístupových politik

MS ACTIVE DIRECTORY

MS Active Directory slouží pro ověřování identity uživatele a autorizaci oprávnění uživatele přistupovat do bezdrátové sítě ČSSZ. Přístup k bezdrátové síti je ověřován pomocí klientského certifikátu uloženého na čipové kartě. Klientský certifikát je validován oproti seznamu akceptovaných certifikačních autorit na ACS serverech. Kromě ověření identity uživatele pomocí klientského certifikátu je přístup autorizován oproti Microsoft Active Directory, kde uživatelský účet musí být členem skupiny s oprávněním přístupu k bezdrátové síti ČSSZ.

LOKALITA

Křížová 6, 25 (K6, K25), Praha 5

Trojská 13 (T13), Praha 8

4.1.8 APLIKAČNÍ PODPORA V OBLASTI INFRASTRUKTURY, TESTOVÁNÍ A HLEDÁNÍ PROBLÉMŮ

ROZSAH POŽADOVANÝCH ČINNOSTÍ

Nad rámec první a druhé úrovně technické podpory a správy jednotlivých zařízení a podporovaných systémů požaduje zadavatel aplikační podporu pro ostatní oblasti IT infrastruktury ČSSZ, jedná se zejména o:

- Aplikační podpora
    - Konzultační služby při návrhu koncepce virtualizace serverů na bázi platformy VMware vSphere
    - Konzultační služby při návrhu koncepce nových služeb a jejich modulů s ohledem na architekturu sítě ČSSZ a datových center
    - Analýza komunikace na externí systémy založené na protokolu HTTP a HTTPS
    - Analýza komunikace systémů v rámci datových center
    - Kapacitní plánování při nasazení nové služby
- Zátěžové testování systémů a služeb
    - Propustnosti MAN/WAN linek
    - Propustnosti síťových a bezpečnostních zařízení
    - Výkonostní testy aplikací, např. WebSEAL, proxy servery
- Hledání problémů
    - Zachytávání datového provozu na síťové infrastruktuře ČSSZ
    - Analýza datových toků a komunikačních matic
    - Pomoc při řešení komunikačních problémů pro systémy třetích stran

Přepokládaný rozsah prací souvisejících s dodáním požadovaných činností činí 80 člověkodní ročně.

POPIS POŽADOVANÉHO SLA

Zadavatel požaduje realizaci požadavku následující pracovní den (NBD) po nahlášení požadavku.

POŽADAVKY NA ODPOVĚĎ

Uchazeč vyplní u každé položky z kapitoly „Rozsah požadovaných činností“, zda jeho návrh poskytování služeb daný požadavek splňuje a jakým způsobem tento požadavek splňuje. Za účelem popisu, jak návrh poskytování služeb daný požadavek splňuje, připojí uchazeč popis splnění požadavků zadavatele, ve kterém uchazeč ke každému požadavku popíše, jak je tento požadavek

řešen a (ne)naplněn, aby z tohoto popisu mohl zadavatel ověřit, zda je daný požadavek skutečně (ne)splněn.

Zadavatel uvádí, že požadavky, uvedené v kapitole „Rozsah požadovaných činností“, jsou požadavky, na kterých zadavatel trvá a výslovně prohlašuje, že návrhy jednotlivých uchazečů musí tyto požadavky zcela splňovat. V případě, že uchazeč jakoukoli z těchto položek nesplní, bude taková skutečnost ze strany zadavatele považována za nesplnění zadávacích podmínek s následkem vyloučení uchazeče z účasti v zadávacím řízení.

LOKALITA

Všechny lokality ČSSZ, celá Česká republika

4.1.9 SLUŽBY PODPORY ROZVOJE A OPTIMALIZACE SÍŤOVÉ INFRASTRUKTURY

Zhodnocení instalované báze z hlediska životního cyklu (IBLM) a upozornění na kritické problémy zaznamenané v databázi výrobce (FieldNotice).

Strategie řízení programového vybavení, která bude zpracována na základě 3-letého výhledu potřeb organizace a bude obsahovat rozdílovou analýzu stávajícího a optimálního cílového stavu, zhodnocení provozní praxe, návrhy migračních strategií, testování, zavedení SW a doporučení výrobce. Specifikace cílového stavu programového vybavení bude vycházet z doporučení a výhledu vývoje SW výrobce.

Návrh rozvoje síťové architektury. Zpracování metodologie plánování rozvoje a vlastní návrh architektury v souladu se střednědobým výhledem cílů a potřeb zadavatele.

Zhodnocení úrovně síťové bezpečnosti. Vyhodnocení schopnosti síťové infrastruktury zabránit v přístupu ke strategickým informačním systémům a aplikacím zadavatele, identifikace rizik a doporučení k jejich odstranění. Jako součást analýzy síťové bezpečnosti zadavatel požaduje průběžnou zprávu o úrovni síťové bezpečnosti komunikačních prvků, která obsahuje:

- výchozí analýzu bezpečnostního nastavení komunikačních prvků, včetně seznamu zjištěných nedostatků
- dokumentované vyjádření výrobce k provozní praxi z pohledu síťové bezpečnosti,
- dokumentovaná konfigurační doporučení výrobce na základě jemu známých bezpečnostních rizik (báze dat bezpečnostních rizik výrobce, metodologická doporučení).

4.1.10 PROVOZ A SPRÁVA INFRASTRUKTURY WIFI

ROZSAH POŽADOVANÝCH ČINNOSTÍ

1. Provoz aktivních síťových prvků v obou lokalitách:
    a. Profylaktické činnosti:
        i. Při pravidelných odstávkách (1x ročně) – fyzická kontrola, čištění síťových zařízení, úprava kabeláži,
        ii. Pravidelné fyzické kontroly s technikem ICT: fyzická kontrola provozního stavu prvků (teplota, hluk zařízení) 1x ročně.
    b. kontrola logů (na denní bázi),
    c. kontrola výkonnosti a performance monitoring (na měsíční bázi),
    d. návrh preventivních opatření s cílem předejít možným výpadkům, snížení výkonu ve WiFi infrastruktuře ČSSZ (minimálně kvartálně nebo dle aktuální situace),

e. odborná technická podpora a odstraňování závad v předmětné oblasti – 2nd level support v souladu se SLA,
f. provádění pravidelných záloh SW konfigurací (měsíční zálohy + aktualizace záloh po každé změně).

2. Správa aktivních prvků v obou lokalitách
    a. Kontrola dostupnosti patchů, hotfixů, service packů a dalších opravných balíků výrobců (na měsíční bázi),
    b. analýza vhodnosti a potřebnosti implementace opravného balíku,
    c. návrh opatření a postupu implementace opravného balíku ke schválení zadavateli,
    d. instalace a provedení změn (včetně práce) dle schválených návrhů opatření (implementace i více opatření bude souhrnně prováděna 1x měsíčně, pokud není potřeba jednat rychleji),
    e. implementace schválených požadavků na změnu konfigurace aktivních prvků (předpokládaný rozsah je až 10 změnových požadavků měsíčně),
    f. předkládání návrhů na optimalizaci infrastruktury WiFi (na kvartální bázi),
    g. správa a aktualizace privilegovaných hesel ke všem předmětným zařízením (pravidelné aktualizace a předání zadavateli) musí být vedeno v souladu s bezpečnostní politikou zadavatele (Směrnice k bezpečnosti informačních a komunikačních technologií),
3. Zprostředkování HW servisu aktivních prvků (u výrobce/dodavatele) včetně případného zajištění náhrady v případě poruchy (v rozsahu smluvně zajištěné maintenance zadavatele).
4. Správa a aktualizace provozní dokumentace v rozsahu:
    a. Postupy pro provoz a správu každého zařízení,
    b. postupy pro obnovu zařízení ze záloh,
    c. provozní deník pro každé zařízení v minimálním rozsahu datum, osoba, číslo požadavku z ticket systému, popis prováděné činnosti, výsledek činnosti (úspěch/selhání), doba trvání.
5. Správa a aktualizace technické dokumentace v rozsahu:
    a. Aktuální schéma fyzického zapojení infrastruktury WiFi,
    b. aktuální schéma logického zapojení infrastruktury WiFi (VLAN, porty, prvky),
    c. aktuální schéma Logického zapojení infrastruktury WiFi L3, L4 (směrování, přehled ACL) v rámci svěřených technologií,
    d. aktuální přehled verzí OS aktivních prvků,
    e. správa konfigurací předmětných zařízení v konfigurační DB zadavatele (IP, SN).
6. Účast na jednání provozních a pracovních týmů zadavatele (2xměsíčně).
7. Pravidelné zpracování reportů (reporting 1x měsíčně) a zpracování analýzy trendů z reportovaných údajů včetně zpracování doporučení (kvartálně):
    a. Reportování vytížení infrastruktury WiFi,
    b. SLA report dostupnosti bezdrátové sítě ČSSZ,
    c. přehled provedených změn v konfiguraci infrastruktury WiFi

POPIS POŽADOVANÉHO SLA

Kategorie A:

Výpadek jednoho nebo více aktivních prvků (karty), který zapříčiní nedostupnost celé infrastruktury WiFi sítě. Nedostupností infrastruktury WiFi sítě se rozumí nedostupnost bezdrátového připojení v celé oblasti pokrytí signálem WiFi, respektive nedostupnost všech přístupových bodů infrastruktury WiFi sítě v obou lokalitách.

U této kategorie požaduje zadavatel opravu či odstranění závady garantované do 6 hodin od nahlášení závady.

Reaktivní podpora na HW s garantovanou dobou opravy či odstranění do 6 hodin od nahlášení závady. Pracovník uchazeče se dostaví na místo opravy do 2 hodin po nahlášení a poskytuje pracovní sílu, náhradní díly a případně další materiál, potřebný k opravě nebo výměně tak, aby HW výrobky byly uvedeny opět do normálního funkčního stavu. Uchazeč identifikuje a opraví špatné funkce a závady výrobku. Vyměněné díly se stanou majetkem uchazeče.

Služba musí být dostupná 24 hodin denně, od pondělí do neděle, včetně veškerých státních svátků a dnů pracovního klidu.

Kategorie B:

Závada nebo výpadek části prvku nebo karty, který způsobí snížení dostupnosti služeb, avšak nezapříčiní výpadek celé infrastruktury WiFi sítě:

a. Výpadek zálohovaných páteřních linek, který nezpůsobí výpadek druhé záložní linky, respektive nedojde k výpadku celé infrastruktury WiFi sítě,
b. závada redundantních zařízení (karet, napájecích zdrojů, modulů a případně dalších), při kterých nedojde k výpadku záložního zařízení,
c. výpadek jednoho bezdrátového přístupového bodu, který nezpůsobí výpadek respektive nedostupnost celé infrastruktury WiFi sítě.

Snížená dostupnost služeb, výkonnostní potíže.

U této kategorie požaduje zadavatel reakci do 4 hodin od nahlášení závady a její odstranění do 8 hodin od nahlášení.

Reaktivní podpora na HW se zaručenou dobou odezvy na servisní požadavek do 4 hodin od nahlášení a její odstranění do 8 hodin. Práce na odstranění závady budou zahájeny nejpozději během následujícího pracovního dne po pracovním dni, kdy byla závada oznámena, a budou probíhat v pracovní dny v době od 08:00 do 17:00 hodin. Služba musí být dostupná v pracovní dny, v době od 08:00 do 17:00 hodin.

Kategorie C:

Závady, které nezpůsobí výpadek ani nesníží dostupnosti služeb v rámci infrastruktury WiFi sítě.

Ostatní závady nespadající do kategorie A nebo B.

U této kategorie zadavatel požaduje odstranění do 2 dnů od nahlášení závady.

Po odstranění závady kategorie A, B, C bude informován ohlašovatel závady (pracovník oddělení správy komunikační a datové infrastruktury a podpory HW nebo jiný příslušný pracovník, který závadu nahlásil), který ověří funkčnost a potvrdí ukončení opravy. Potvrzení ukončení opravy bude považováno za okamžik ukončení opravy.

ZPŮSOB KONTROLY

Měření parametrů služby bude prováděno v pravidelných intervalech během zaručené provozní doby služby. Měřící body (sondy) a počet měření budou zvoleny tak, aby výsledky byly dostatečné pro vyhodnocení stanovených parametrů SLA služby. Měřeními bude ověřována dostupnost infrastruktury WiFi sítě a jejích služeb. Dostupnost služby se bude měřit souborem testů dostupnosti spravovaných aktivních prvků. Provozní činnosti budou kontrolovány zadavatelem (nebo jím stanoveným subjektem) na měsíční bázi. O výsledku kontrol bude sestavován měsíční report. Report vystavuje kontrolující subjekt, schvaluje zadavatele a slouží zadavateli jako podklad pro vyhodnocení služeb.

DALŠÍ PODMÍNKY

V případě obměny zařízení z důvodu náhrady vadného prvku, nebo z důvodu modernizace budou tato nová zařízení považována za ekvivalentní a budou na ně poskytovány stejné služby.

Povinnost zpřístupnit technologie pro definici a implementaci monitorovacích agentů/sond.

Povinnost poskytnout součinnost zadavateli (nebo jím jmenovaných subjektů) při provádění kontrolní činnosti na dodržování a plnění náplně této služby.

POŽADAVKY NA ODPOVĚĎ

Uchazeč vyplní u každé položky z kapitoly „Rozsah požadovaných činností“, zda jeho návrh poskytování služeb daný požadavek splňuje a jakým způsobem tento požadavek splňuje. Za účelem popisu, jak návrh poskytování služeb daný požadavek splňuje, připojí uchazeč popis splnění požadavků zadavatele, ve kterém uchazeč ke každému požadavku popíše, jak je tento požadavek řešen a (ne)naplněn, aby z tohoto popisu mohl zadavatel ověřit, zda je daný požadavek skutečně (ne)splněn.

Zadavatel uvádí, že požadavky, uvedené v kapitole „Rozsah požadovaných činností“, jsou požadavky, na kterých zadavatel trvá a výslovně prohlašuje, že návrhy jednotlivých uchazečů musí tyto požadavky zcela splňovat. V případě, že uchazeč jakoukoli z těchto položek nesplní, bude taková skutečnost ze strany zadavatele považována za nesplnění zadávacích podmínek s následkem vyloučení uchazeče z účasti v zadávacím řízení.

Popis současného stavu prostředí

WiFi infrastruktura ČSSZ zajišťuje bezdrátové připojení pro interní zaměstnance a externí spolupracovníky ČSSZ. WiFi infrastruktura ČSSZ pokrývá signálem hlavní administrativní budovu na adrese Křížová 25 a školicí středisko Křešice. Základem WiFi infrastruktury ČSSZ je řídící modul bezdrátové sítě Cisco Wireless Controller řady 5500 nainstalovaný na lokalitě zadavatele na adrese Křížová 25. Cisco WLC5508 umožňuje v instalované konfiguraci správu až 50 bezdrátových přístupových bodů. Cisco wireless controller je připojen pomocí dvojce GigabitEthernet linek na centrální infrastrukturu LAN ČSSZ. Linky wireless LAN controlleru jsou sloučené do jednoho ethernetového kanálu a nakonfigurované v módu trunk.

Připojení bezdrátových přístupových bodů v lokalitě zadavatele na adrese Křížová 25 je realizováno pomocí infrastruktury LAN sítě. Přístupové body jsou umístěné do dedikované VLAN sítě, ve které dostávají informaci o umístění centrálního wireless LAN controlleru prostřednictvím DHCP atributů. Veškerá klientská data jsou tunelovaná z přístupových bodů na centrální wireless LAN controller.

Připojení bezdrátového přístupového bodu v lokalitě Křešice je realizováno pomocí WAN sítě a dedikované VLAN v místní LAN infrastruktuře. Přístupový bod v dedikované VLAN dostává informaci o umístění centrálního wireless LAN controlleru prostřednictvím DHCP atributů. Veškerá klientská data jsou tunelovaná z přístupového bodu na centrální LAN wireless controller.

Bezdrátová infrastruktura ČSSZ poskytuje dva přístupové profily:

- CSSZ (Určen pro interní zaměstnance ČSSZ)
- CSSZ-e (Určen pro externí spolupracovníky ČSSZ)

Přístupový profil CSSZ

Profil CSSZ umožnuje plný přístup k interním sdíleným zdrojům pro zaměstnance ČSSZ. Přístup k tomuto profilu je ověřován pomocí klientského certifikátu uloženého na čipové kartě. Kromě ověření identity uživatele pomocí klientského certifikátu je přístup autorizován oproti Microsoft Active Directory, kde uživatelský účet musí být členem skupiny s oprávněním přístupu k internímu profilu bezdrátové infrastruktury ČSSZ. Autentizaci a autorizaci uživatelů bezdrátové sítě ČSSZ zajišťují AAA servery Cisco ACS, viz kapitola 4.7.

Přístupový profil CSSZ-e

Profil CSSZ-e umožnuje omezený přístup k Internetu pro externí spolupracovníky ČSSZ. Přístup k tomuto profilu je ověřován pomocí klientského certifikátu uloženého na čipové kartě. Kromě ověření identity uživatele pomocí klientského certifikátu je přístup autorizován oproti Microsoft Active Directory, kde uživatelský účet musí být členem skupiny s oprávněním přístupu k externímu profilu bezdrátové infrastruktury ČSSZ. Autentizaci a autorizaci uživatelů bezdrátové sítě ČSSZ zajišťují AAA servery Cisco ACS, viz kapitola 4.7. Datový provoz WiFi klientů tohoto profilu je filtrován na FWSM modulu a je povolen pouze na interní Microsoft AD řadiče a Internetový proxy server ČSSZ.

LOKALITA

KŘÍŽOVÁ 6, 25 (K6, K25), PRAHA 5
Trojská 13 (T13), Praha 8

4.1.11 OPRAVY KABELÁŽNÍCH SYSTÉMŮ

V případě HW problémů na síti způsobených kabelovými rozvody zadavatel požaduje řešení i tohoto problému, tj. provádění potřebných měření, detekce vadných spojů či konektorů a zajištění oprav. Odhadovaný rozsah plnění v této části je 72 hodin ročně. Předmětem této veřejné zakázky není výstavba počítačových sítí.

Na kabeláže instalované ve většině lokalit se vztahují záruky garantované výrobcem (Molex) kabelážních systémů (tzv. systémové záruky v délce 20 až 25 let) a výrobce v případě neautorizovaného zásahu do kabeláží odmítá dle záručních podmínek plnit svoje závazky. Proto v rámci zachování systémových záruk zadavatel požaduje, aby uchazeč předložil osvědčení vydané a potvrzené výrobcem kabelážního systému opravňující uchazeče k zásahu do instalovaných kabelážních systémů.

4.1.12 Migrace služeb správy, provozu, dohledu, podpory a rozvoje infrastruktury zadavatele a IMS

Uchazeč popíše zvolenou metodiku pro migraci požadovaných služeb, minimálně v následujícím rozsahu:

- Organizace projektu migrace služeb,
- popis jakým způsobem bude provedena analýza současného stavu a požadavky na zadavatele v rámci této analýzy,
- etapizace, uchazeč navrhne věcné a realistické rozdělení migrace do etap,
- harmonogram migrace služeb, který bude obsahovat důležité milníky, zejména připravenost jednotlivých stran, proces migrace služeb, plná dostupnost jednotlivých modulů služeb,
- metodologie projektového řízení, jakou metodologii uchazeč použije a jakým způsobem ji aplikuje v tomto konkrétním případě,
- jednotlivé položky harmonogramu musejí být popsané co nejdetailněji, včetně dílčích výstupů, návazností a časových odhadů,
- požadavky na součinnost zadavatele,
- požadavky na dokumentační a datové podklady,
- popis řízení rizik pro migraci služeb.

Uchazeč popíše zvolenou metodiku pro nasazení systému IMS, minimálně v následujícím rozsahu:

- Harmonogram implementace a dostupnosti systému pro plné využití,
- popis migrace datových zdrojů ze stávajícího řešení,
- popis požadavků na součinnost Zadavetele při nasazení systému,
- popis požadavků na součinnost třetích stran (výrobců spravovaných systémů, dalších poskytovatelů služeb atp.) při nasazení systému,
- testovací a akceptační kritéria jednotlivých požadovaných služeb systému IMS,
- doba potřebná pro přidání/změnu nového typu požadavku,
- doba potřebná pro integraci s novým typem zařízení,
- doba potřebná pro implementaci nového modulu/funkcionality dle specifikace zadavatele.

5 PROKAZOVÁNÍ SPLNĚNÍ KVALIFIKAČNÍCH PŘEDPOKLADŮ

Uchazeč je povinen v souladu s § 50 zákona prokázat, že je kvalifikovaným pro plnění veřejné zakázky. Všechny doklady požadované k prokázání splnění kvalifikace musejí být součástí nabídky a budou předloženy v kopiích, nestanoví-li zadavatel v této zadávací dokumentaci jinak. Veškeré doklady prokazující splnění kvalifikace musejí být doloženy v českém jazyce, případně v původním jazyce s připojením jejich úředně ověřeného překladu do českého jazyka. Je-li zákonem připuštěno či zadavatelem vyžadováno čestné prohlášení, musí být podepsáno osobou oprávněnou jednat jménem uchazeče, který je fyzickou osobou či za uchazeče, který je právnickou osobou (statutárním orgánem nebo osobou k tomu statutárním orgánem zmocněnou v souladu se způsobem jednání za uchazeče). V případě podpisu jinou osobou musí být jako součást dokladů, kterými uchazeč prokazuje splnění kvalifikace, přiložena kopie zmocnění této osoby k danému úkonu. Nesplnění těchto podmínek posoudí zadavatel jako nesplnění kvalifikace s následným vyloučením uchazeče ze zadávacího řízení.

Uchazeč je oprávněn v souladu s § 127 zákona využít k prokázání splnění kvalifikace výpis ze seznamu kvalifikovaných dodavatelů. Tento výpis nahrazuje prokázání splnění základních kvalifikačních předpokladů podle § 53 odst. 1 zákona a profesních kvalifikačních předpokladů podle § 54 písm. a) až d) zákona v tom rozsahu, v jakém doklady prokazující splnění těchto profesních kvalifikačních předpokladů pokrývají požadavky zadavatele na prokázání splnění profesních kvalifikačních předpokladů pro plnění veřejné zakázky.

Všechny doklady musí být kvalitním způsobem vytištěny tak, aby byly dobře čitelné. Žádný doklad nesmí obsahovat opravy a přepisy, které by zadavatele mohly uvést v omyl.

Doklady prokazující splnění základních kvalifikačních předpokladů a výpis z obchodního rejstříku nesmějí být starší 90 dnů ke dni podání nabídky.

Zadavatel stanoví, že kvalifikovaným pro plnění veřejné zakázky je uchazeč, který splní níže uvedené kvalifikační předpoklady v požadovaném rozsahu.

5.1 PROKAZOVÁNÍ SPLNĚNÍ ZÁKLADNÍCH A PROFESNÍCH KVALIFIKAČNÍCH PŘEDPOKLADŮ

1. Splnění základních kvalifikačních předpokladů podle § 53 odst. 1 zákona prokáže uchazeč předložením následujících dokladů:
   a) výpisu z evidence Rejstříku trestů – viz § 53 odst. 1 písm. a) a b) zákona,
   b) potvrzení příslušného finančního úřadu a ve vztahu ke spotřební dani čestného prohlášení – viz § 53 odst. 1 písm. f) zákona,
   c) potvrzení příslušného orgánu či instituce – viz § 53 odst. 1 písm. h) zákona,
   d) čestného prohlášení ohledně dalších požadovaných skutečností – viz § 53 odst. 1 písm. c) až e) a g), i) až k) zákona.
2. Splnění profesních kvalifikačních předpokladů prokáže uchazeč podle § 54 písm. a) a b) zákona předložením následujících dokladů:
   a) výpisem z obchodního rejstříku, pokud je v něm zapsán či výpisem z jiné obdobné evidence, pokud je v ní zapsán,
   b) dokladem o oprávnění k podnikání podle zvláštních právních předpisů v rozsahu odpovídajícím předmětu této veřejné zakázky, zejména doklad prokazující příslušné živnostenské oprávnění či licenci.

5.2 ČESTNÉ PROHLÁŠENÍ O EKONOMICKÉ A FINANČNÍ ZPŮSOBILOSTI SPLNIT VEŘEJNOU ZAKÁZKU

Uchazeč předloží v souladu s § 50 odst. 1 písm. c) zákona čestné prohlášení o své ekonomické a finanční způsobilosti splnit veřejnou zakázku.

5.3 PROKÁZÁNÍ SPLNĚNÍ TECHNICKÝCH KVALIFIKAČNÍCH PŘEDPOKLADŮ

Zadavatel požaduje v souladu s § 56 zákona k prokázání splnění technických kvalifikačních předpokladů uchazeče pro plnění veřejné zakázky:

a) Předložení seznamu významných služeb realizovaných uchazečem v posledních 3 letech s uvedením jejich rozsahu a doby plnění dle § 56 odst. 2 písm. a) zákona. Toto prokáže tím, že ve své nabídce předloží seznam těch služeb, které jsou požadovány v oblasti předmětu této veřejné zakázky, z nichž alespoň 2 služby jsou službami spočívající v zajištění provozní a expertní podpory datové sítě s celostátním rozsahem (minimálně 50 lokalit) a minimálním počtem 1 500 uživatelů, kteří jsou těmito systémy obsluhováni. Minimálně pro tyto 2 služby pak uchazeč předloží osvědčení dle § 56 odst. 2 písm. a) bod 1 a 2 zákona nebo smlouvu s jinou osobou a doklad o uskutečněném plnění dle § 56 odst. 2 písm. a) bod 3 zákona.

V seznamu významných služeb musí být uvedeny následující údaje:

- identifikace objednatele (jméno, adresa, IČO, kontaktní osoba objednatele, u které je možné uvedené údaje ověřit, telefonní číslo a email této kontaktní osoby objednatele)
- identifikace dodavatele (jméno, adresa, IČO)
- rozsah plnění (počet lokalit, počet uživatelů)
- finanční objem dodávky
- období poskytování služeb
- prohlášení o úplnosti a pravdivosti uvedených údajů
- jméno a podpis osoby oprávněné jednat jménem objednatele, který je fyzickou osobou či objednatelem, který je právnickou osobou (statutárním orgánem nebo osobou k tomu statutárním orgánem zmocněnou v souladu se způsobem jednání za objednatele)

Osvědčení vyhotovené objednatelem musí obsahovat veškeré údaje nutné k posouzení toho, zda je naplněna uvedená definice významné služby.

b) Předložením seznamu členů realizačního týmu uchazeče, osvědčení o jejich vzdělání a odborné kvalifikaci dle § 56 odst. 2 písm. b) a e) zákona. Osoby v tomto seznamu uvedené se budou podílet na plnění této veřejné zakázky, bez ohledu na to, zda se jedná o zaměstnance uchazeče nebo osoby v jiném vztahu k uchazeči. Z tohoto seznamu bude vyplývat, že uchazeč má k dispozici tým odborníků sestávající z:

1) minimálně jedné osoby (projektový manažer) splňujících následující požadavky:

- minimálně 5 let praxe v pozici projektového manažera v oblasti poskytování služeb informačních technologií;
- zkušenost s vedením alespoň 1 projektu splňujícího shora uvedenou definici významné služby na pozici projektového manažera;
- certifikace v oblasti projektového řízení IPMA , PRINCE2, nebo obdobné;
- dokončené vysokoškolské vzdělání v magisterském nebo doktorském studijním programu;
- znalost českého či slovenského jazyka.

2) minimálně tří osob (síťový specialista) splňujících následující požadavky:

- minimálně 5 let praxe v pozici síťový specialista v oblasti poskytování služeb informačních technologií;
- zkušenost s účastí na pozici síťový specialista alespoň na 1 projektu spočívajícím v poskytování služeb návrhu, implementace, provozu a úprav síťové infrastruktury, přičemž služby byly objednateli poskytovány kontinuálně po dobu nejméně 1 kalendářního roku a jejich finanční objem činil alespoň 10 mil. Kč bez DPH;
- certifikaci Cisco Certified Internetwork Expert (CCIE)
- u minimálně jednoho z těchto specialistů HP ASE nebo HP MASE certifikace;
- u minimálně jednoho z těchto specialistů IPv6 Forum Certified Network Engineer certifikace nebo obdobné;
- dokončené středoškolské vzdělání;
- znalost českého či slovenského jazyka.

3) minimálně dvou osob (bezpečnostní specialista) splňujících následující požadavky:

- minimálně 5 let praxe v pozici bezpečnostní specialista v oblasti poskytování služeb informačních technologií;
- zkušenost s účastí na pozici bezpečnostní specialista alespoň na 1 projektu spočívajícím v poskytování služeb návrhu, implementace, provozu a úprav bezpečnostní architektury, přičemž služby byly objednateli poskytovány kontinuálně po dobu nejméně 1 kalendářního roku a jejich finanční objem činil alespoň 10 mil. Kč bez DPH;
- alespoň u jednoho z těchto specialistů certifikace v oblasti bezpečnosti jako je CISM nebo obdobné úrovně;
- u minimálně jednoho z těchto specialistů dokončené vysokoškolské vzdělání v magisterském nebo doktorském studijním programu;
- znalost českého či slovenského jazyka.

4) minimálně dvou osob (WAN specialista) splňujících následující požadavky:

- minimálně 5 let praxe v pozici WAN specialista v oblasti poskytování služeb informačních technologií;
- zkušenost s účastí na pozici WAN specialista alespoň na 1 projektu spočívajícím v poskytování služeb návrhu, implementace, provozu a úprav WAN a WAN akcelerační architektury, přičemž služby byly objednateli poskytovány kontinuálně po dobu nejméně 1 kalendářního roku a jejich finanční objem činil alespoň 10 mil. Kč bez DPH;
- dokončené středoškolské vzdělání;
- znalost českého či slovenského jazyka.

5) minimálně dvou osob (Application Delivery Controller specialista) splňujících následující požadavky:

- minimálně 5 let praxe v pozici Application Delivery Controller specialista v oblasti poskytování služeb informačních technologií;
- zkušenost s účastí na pozici Application Delivery Controller specialista alespoň na 1 projektu spočívajícím v poskytování služeb návrhu, implementace, provozu a úprav LB architektury, přičemž služby byly objednateli poskytovány kontinuálně po dobu nejméně 1 kalendářního roku a jejich finanční objem činil alespoň 8 mil. Kč bez DPH;
- certifikace v oblasti LB pro technologie Cisco nebo F5;
- dokončené vysokoškolské nebo středoškolské vzdělání;
- znalost českého či slovenského jazyka.

6) minimálně jedné osoby (Systémový administrátor - nástroje pro virtualizaci serverů, např. VMware) splňujících následující požadavky:

- minimálně 3 roky praxe v pozici Systémový administrátor - nástroje pro virtualizaci serverů (5 let v případě středoškolského vzdělání);
- dokončené vysokoškolské vzdělání nebo středoškolské vzdělání (ukončené maturitní zkouškou) technického zaměření;
- zkušenost s účastí na pozici Systémový administrátor - nástroje pro virtualizaci alespoň na 1 projektu spočívajícím v poskytování služeb návrhu, implementace, provozu a úprav virtualizace serverů, přičemž služby byly objednateli poskytovány kontinuálně po dobu nejméně 1 kalendářního roku a jejich finanční objem činil alespoň 8 mil. Kč bez DPH;
- znalost produktů pro virtualizaci serverů (např. VMware vSphere), jejichž správa bude předmětem činnosti pracovníka v roli systémového administrátora doložená platným certifikátu VMware Certified Professional;
- znalost českého či slovenského jazyka

Definované role jsou výjimečné a nesmějí se překrývat či kumulovat v jedné osobě.

Přílohou seznamu techniků budou příslušná osvědčení/certifikáty, doklady o vysokoškolském nebo středoškolském vzdělání (diplomy).

Přílohou seznamu techniků budou také profesní životopisy každého technika – člena týmu, přičemž zadavatel požaduje, aby profesní životopisy obsahovaly minimálně následující údaje: jméno a příjmení člena týmu, podrobný popis funkce člena týmu na plnění veřejné zakázky, údaj o zaměstnavateli, popř. IČO člena týmu, čestné prohlášení o odborné zkušenosti s přehledem profesní praxe nebo odborné kvalifikace vztahující se k předmětu plnění veřejné zakázky, další údaje prokazující splnění požadavků zadavatele.

Ze seznamu či profesních životopisů musí vyplývat, že uvedené osoby mají požadované zkušenosti a kde tyto zkušenosti nabyly. U každého člena týmu budou uvedeny kontaktní údaje osoby, u níž lze uváděné zkušenosti ověřit.

6 POŽADAVKY NA ZPŮSOB ZPRACOVÁNÍ NABÍDKOVÉ CENY

Uchazeč v nabídce zpracuje nabídkovou cenu následujícím způsobem:

Název	Cena za měsíc v Kč bez DPH	Cena za měsíc v Kč včetně DPH	Cena za 48 měsíců v Kč bez DPH	Cena za 48 měsíců v Kč včetně DPH
Zajištění provozní a expertní podpory sítě LAN/WAN				
Celkem				

Nabídková cena je celková cena včetně DPH za plnění popsané v části 4 této zadávací dokumentace. Úhrada za plnění bude prováděna zpětně v měsíčních intervalech a bude zaplacena nejdříve 30 dní poté, co bude zadavateli doručena faktura. Faktura bude vystavována měsíčně zpětně.

- Cena bude uvedena v českých korunách, jako cena za 48 měsíců poskytování služeb v rozsahu dle této zadávací dokumentace, částka bude uvedena v členění bez DPH a vč. DPH.
- Nabídková cena bude obsahovat veškeré náklady na splnění veřejné zakázky. Nabídkovou cenu bude možné překročit pouze v souvislosti se změnou daňových předpisů majících vliv na cenu předmětu plnění, a to pouze o výši, která těmto změnám bude odpovídat.

7 OBCHODNÍ A PLATEBNÍ PODMÍNKY

Uchazeč je povinen do návrhu smlouvy zapracovat následující obchodní podmínky a nesmí ve smlouvě pozměnit smysl těchto obchodních podmínek nebo je jakkoliv změkčovat nebo obcházet:

1. Smlouva bude uzavřena v souladu s příslušnými ustanoveními zákona č. 89/2012 Sb., občanský zákoník (dále jen „občanský zákoník“).

2. Závazek uchazeče, že bude pravidelně tvořit, doplňovat a aktualizovat provozní síťovou dokumentaci, kterou předá v aktualizované podobě vždy při předávání měsíčního plnění.

3. Závazek uchazeče přiložit ke smlouvě (formou přílohy) kopii osvědčení vydaného a potvrzeného výrobcem kabelážního systému MOLEX PN opravňující uchazeče k zásahu do instalovaných kabelážních systémů zadavatele. Při podpisu smlouvy předloží vybraný uchazeč originál či úředně ověřenou kopii tohoto osvědčení. Vybraný uchazeč je povinen prokázat tuto skutečnost kdykoli po dobu trvání smlouvy na základě písemné výzvy zadavatele tím, že doručí zadavateli osvědčení (originál či úředně ověřenou kopii) do 7 dnů od doručení výzvy. Nesplní-li uchazeč tuto svou povinnost, je zadavatel oprávněn účtovat uchazeči smluvní pokutu ve výši 250 000,- Kč (slovy: dvěstěpadesáttisíc korun českých). Nesplní-li uchazeč tuto povinnost ani v dodatečné přiměřené lhůtě stanovené zadavatelem, je zadavatel oprávněn odstoupit od smlouvy.

4. Ujednání o ceně za celý předmět smlouvy v souladu s požadavky části 6 této zadávací dokumentace.

5. Ujednání o záruce za jakost poskytovaného plnění v délce alespoň 6 měsíců od poskytnutého plnění.

6. Úhrada ceny plnění bude prováděna měsíčně bezhotovostním převodem po podepsání akceptačního protokolu, a to na základě daňového dokladu (faktury). Splatnost faktury bude činit 30 (třicet) kalendářních dnů od jejího doručení zadavateli. Faktura bude zaslána na adresu zadavatele a kromě náležitostí daňového dokladu v souladu se zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, bude dále obsahovat číslo smlouvy, název zadavatele a číslo účtu uchazeče. Zadavatel bude oprávněn před uplynutím splatnosti fakturu vrátit, bude-li obsahovat nesprávné nebo neúplné cenové údaje nebo nebude-li obsahovat zákonné nebo dohodnuté náležitosti. Nová lhůta splatnosti počíná v takovém případě běžet ode dne doručení opravené faktury zadavateli. Za okamžik uhrazení faktury je považován okamžik odepsání příslušné částky z účtu zadavatele. Přílohou faktury bude podepsaný měsíční akceptační protokol o poskytnutí služeb.

7. Měsíční plnění bude uchazečem reportováno formou akceptačního protokolu, který bude obsahovat seznam jednotlivých požadavků na poskytování provozní a expertní podpory s uvedením časové specifikace přijetí a vyřešení požadavku, lokality řešení, zodpovědné osoby zadavatele a uchazeč a popisem daného řešení. Součástí akceptace je i aktualizace provozní dokumentace.

8. Převzetí předmětu plnění bude prováděno měsíčně zpětně na základě měsíčního akceptačního protokolu podepsaného vedoucím oddělení správy komunikační a datové infrastruktury a podpory HW zadavatele.

9. Ujednání, že uchazeč není oprávněn jakýmkoli způsobem vstupovat do informačních systémů zadavatele, ani se o to pokoušet. Poruší-li uchazeč tento závazek, bude zadavatel oprávněn požadovat zaplacení smluvní pokuty ve výši 1 000 000,- Kč za každé takové prokázané porušení. Nesplní-li uchazeč tuto povinnost ani v dodatečné přiměřené lhůtě stanovené zadavatelem, je zadavatel oprávněn odstoupit od smlouvy.

10. Závazek uchazeče, že přizpůsobí svůj helpdesk stavu helpdesku zadavatele a zajistí takové propojení, které zaručí bezproblémovou komunikaci helpdesků navzájem. Poruší-li uchazeč tento závazek, bude zadavatel oprávněn požadovat zaplacení smluvní pokuty ve výši 100 000,- Kč.

11. Ujednání, že smlouva může být ukončena pouze:

a. písemnou a podepsanou dohodou obou smluvních stran, která musí obsahovat jejich vzájemné vypořádání všech závazků,

b. odstoupením zadavatele od smlouvy z důvodů uvedených v těchto obchodních podmínkách a z důvodu podstatného porušení smluvních povinností v souladu s § 2001 a násl. občanského zákoníku,

c. výpovědí zadavatele kdykoliv i bez udání důvodu s výpovědní lhůtou tři (3) kalendářní měsíce, počínající běžet od prvního dne kalendářního měsíce následujícího po měsíci, v němž došlo k doručení výpovědi uchazeči.

12. Ujednání o kvalitě plnění a odpovědnosti za vady v souladu s ust. § 2615 a násl. občanského zákoníku.

13. Uchazeč se zavazuje mít po celou dobu trvání smluvního vztahu sjednáno pojištění odpovědnosti za škodu způsobenou při výkonu podnikatelské činnosti třetí osobě s limitem pojistného plnění nejméně 25 mil. Kč se spoluúčastí nejvýše 5 % tohoto limitu. Vybraný uchazeč je povinen prokázat tuto skutečnost kdykoli po dobu trvání smlouvy na základě písemné výzvy zadavatele tím, že doručí zadavateli pojistnou smlouvu (originál či úředně ověřenou kopii) nebo jiný obdobný doklad do 7 dnů od doručení výzvy. Nesplní-li uchazeč tuto svou povinnost, je zadavatel oprávněn účtovat uchazeči smluvní pokutu ve výši 250 000,- Kč (slovy: dvěstěpadesáttisíc korun českých). Nesplní-li uchazeč tuto povinnost ani v dodatečné přiměřené lhůtě stanovené zadavatelem, je zadavatel oprávněn odstoupit od smlouvy.

14. Ujednání, že v případě prodlení s úhradou oprávněně vystavené faktury k dílčí platbě uhradí zadavatel uchazeči z nezaplacené částky úroky z prodlení určené nařízením vlády č. 351/2013 Sb., kterým se určuje výše úroků z prodlení a nákladů spojených s uplatněním pohledávky, určuje odměna likvidátora, likvidačního správce a člena orgánu právnické osoby jmenovaného soudem a upravují některé otázky Obchodního věstníku a veřejných rejstříků právnických a fyzických osob. Uchazeč však není oprávněn požadovat po zadavateli smluvní pokutu pro případ tohoto prodlení.

15. Ujednání, že je-li překročena lhůta doby odezvy na straně uchazeče, má zadavatel právo požadovat po uchazeči úhradu smluvní pokuty ve výši 0,5% z měsíční platby včetně DPH za každou i započatou hodinu prodlení. Tím není dotčen ani omezen nárok na náhradu vzniklé nemajetkové újmy či škody. Jakékoliv omezení výše smluvní pokuty není přípustné.

16. Ujednání, že je-li překročena lhůta pro odstranění závady nebo požadavku na straně uchazeče, má zadavatel právo požadovat po uchazeči úhradu smluvní pokuty ve výši 0,5% z měsíční platby včetně DPH za každou i započatou hodinu prodlení. Tím není dotčen ani omezen nárok na náhradu vzniklé nemajetkové újmy či škody. Jakékoliv omezení výše smluvní pokuty není přípustné.

17. Uchazeč se zavazuje během plnění smlouvy i po jejím ukončení zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví od zadavatele v souvislosti s plněním smlouvy. Pokud uchazeč poruší tento závazek, je povinen zaplatit zadavateli smluvní pokutu ve výši 100 000,- Kč (slovy: jednostotisíc korun českých) za každé takové porušení povinnosti, a to do patnácti (15) dnů ode dne doručení vyúčtování smluvní pokuty zadavatelem. Tím není dotčen ani omezen nárok na náhradu vzniklé nemajetkové újmy či škody.

18. Uchazeč se zavazuje nahradit veškerou nemajetkovou újmu či škodu způsobenou zadavateli porušením povinností uchazeče vyplývajících z této zadávací dokumentace nebo z platných a účinných právních předpisů. Škoda se hradí v penězích nebo, je-li to možné a obvyklé, uvedením v předešlý stav, a to dle volby zadavatele v konkrétním případě. Jakékoliv omezení výše či druhu náhrady škody není přípustné.

19. Uchazeč zapracuje do návrhu smlouvy ustanovení o tom, že je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou služeb z veřejných výdajů.

20. Uchazeč v návrhu smlouvy uvede následující text: „Smluvní strany souhlasí s tím, aby byla tato smlouva zveřejněna na profilu zadavatele České správy sociálního zabezpečení. Souhlas se zveřejněním podle předchozí věty se nevztahuje na údaje, které jsou obchodním tajemstvím ve smyslu ustanovení § 504 občanského zákoníku na údaje, jejichž zveřejnění brání zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů, jakož i na údaje,

které jsou chráněny před zveřejněním podle jiných právních předpisů. Uchazeč ve své nabídce uvede, jaká konkrétní ustanovení smlouvy (včetně příloh) a z jakého právního důvodu si nepřeje zveřejnit. Pokud uchazeč žádné ustanovení smlouvy postupem podle předchozí věty neoznačí, bude zadavatel za předpokladu dodržení obecně závazných předpisů oprávněn zveřejnit smlouvu jako celek včetně všech příloh.

21. Veškeré spory mezi smluvními stranami budou řešeny pokud možno smírně. Spory, které se nepodaří vyřešit smírně, budou řešeny před věcně a místně příslušným soudem České republiky. Rozhodčí řízení je vyloučeno.

22. Závazek uchazeče spočívající v převzetí nebezpečí změny okolností ve smyslu ustanovení § 1765 odst. 2 občanského zákoníku.

23. Ve věcech smlouvou neupravených se tato smlouva bude řídit příslušnými ustanoveními občanského zákoníku.

8 DOBA A MÍSTO PLNĚNÍ VEŘEJNÉ ZAKÁZKY

8.1 DOBA PLNĚNÍ

Doba plnění začíná od podpisu smlouvy oběma smluvními stranami. Smlouva se uzavírá na dobu 48 měsíců od podpisu smlouvy.

8.2 MÍSTO PLNĚNÍ

Systémy, pro které bude poskytováno plnění dle této veřejné zakázky, jsou umístěny na pracovištích ČSSZ uvedených v tabulce v příloze č.2 seznam_lokalit.doc této zadávací dokumentace. Uchazeč bere na vědomí, že během zadávacího řízení nebo po dobu platnosti následně uzavřené smlouvy může dojít ke změně sídla uvedených pracovišť, které může být spojeno s jejich případným stěhováním. Tyto skutečnosti nejsou důvodem pro zvýšení ceny za poskytované plnění.

9 ZPŮSOB HODNOCENÍ NABÍDEK PODLE HODNOTÍCÍCH KRITÉRIÍ

Základním hodnotícím kritériem pro zadání veřejné zakázky je ekonomická výhodnost nabídky. Hodnocení v rámci tohoto kritéria proběhne v souladu s § 79 zákona podle níže uvedených dílčích hodnotících kritérií, a to následujícím způsobem:

Dílčí hodnotící kritérium	Váha
Nabídková cena (V souladu se zákonem bude hodnocena výše ceny plnění uvedené v řádku „Celkem“ sloupce „Cena za 48 měsíců včetně DPH“ tabulky v části 6 této zadávací dokumentace)	60%
Kvalita nabízených služeb	40%

Pro hodnocení nabídek použije hodnotící komise bodovací stupnici v rozsahu 0 až 100. Jednotlivým nabídkám je dle dílčího kritéria přidělena bodová hodnota, která odráží úspěšnost předmětné nabídky v rámci dílčího kritéria. V každém dílčím kritériu bude nejvhodnější nabídce přiděleno 100 bodů. Další nabídce bude přidělen počet bodů, který je výsledkem matematického výpočtu:

- pro kritérium „Nabídková cena“, pro které má nejvhodnější nabídka minimální hodnotu kritéria, získá hodnocená nabídka bodovou hodnotu, která vznikne násobkem 100 a poměru hodnoty nejvhodnější nabídky k hodnocené nabídce

$$body = \frac{Nejvhodnější\ nabídka}{Hodnocená\ nabídka} \times 100 = \frac{Nejvýhodnější\ cena}{Hodnocená\ cena} \times 100$$

- pro kritérium „Kvalita nabízených služeb“, pro které má nejvhodnější nabídka minimální hodnotu kritéria, získá hodnocená nabídka bodovou hodnotu, která vznikne násobkem 100 a poměru hodnoty nejvhodnější nabídky k hodnocené nabídce.

$$body\ = \frac{Nejvhodnější\ nabídka}{Honocená\ nabídka} \times 100 = \frac{Nejkratší\ doba\ odstranění\ závady}{Hodnocená\ doba\ odstranění\ závady} \times 100$$

Takto přidělený počet bodů bude následně přepočítán dle váhy kritéria. Na základě součtu výsledných hodnot u jednotlivých nabídek hodnotící komise stanoví pořadí úspěšnosti jednotlivých nabídek tak, že jako nejúspěšnější je stanovena nabídka, která dosáhla nejvyšší hodnoty.

Zadavatel stanovil jako dílčí hodnotící kritérium „Kvalita nabízených služeb“. Toto dílčí hodnotící vychází z potřeby ČSSZ zajistit odstranění závad v co nejkratším čase, tak aby nebylo ohroženo poskytování služeb klientům.

Dílčí hodnotící kritérium „Kvalita nabízených služeb“ bude hodnoceno na základě následujících subkritérií:

Subkritérium pro dílčí hodnotící kritérium „Kvalita nabízeného plnění“	Váha
Doba odstranění závady kategorie A dle kapitoly 4.1.1	50%
Doba odstranění závady kategorie A dle kapitoly 4.1.3	25%
Doba odstranění závady kategorie A dle kapitoly 4.1.2	25%

V předmětu zakázky je u každé jednotlivé kapitoly (4.1.1, 4.1.3, 4.1.2) uvedena požadovaná doba odstranění závady typu A. Uchazeč uvede do nabídky níže přiloženou tabulku, ve které vyplní sloupec „Nabízená doba odstranění závady kategorie A“. Za každých 30 minut zkrácení doby odstranění závady kategorie A bude přidělen 1bod. Maximálně tedy může uchazeč získat 8 bodů za kapitolu 4.1.1., 6 bodů za kapitolu 4.1.3 a 8 bodů za kapitolu 4.1.2.

Předmět plnění	Požadovaná maximální doba odstranění závady (kategorie A) [hodiny]	Minimální doba na odstranění závady (kategorie A) [hodiny]	Nabízená doba odstranění závady (kategorie A) [hodiny]
Kapitola 4.1.1	6	2	vyplní uchazeč
Kapitola 4.1.3	4	1	vyplní uchazeč
Kapitola 4.1.2	6	2	vyplní uchazeč

Výsledné bodové hodnoty všech tří subkritérií budou sečteny a vynásobeny vahou dílčího hodnotícího kritéria.

10 PODMÍNKY A POŽADAVKY NA ZPRACOVÁNÍ NABÍDKY

1) Nabídka bude zpracována písemně, výlučně v českém jazyce (vyjma certifikátů, které mohou být v anglickém jazyce, a diplomů, které mohou být v latině) a podepsána uchazečem či osobou oprávněnou zastupovat uchazeče.

2) Nabídka bude předložena v jednom originále v písemné formě a dále rovněž v elektronické formě na vhodném médiu (CD) ve formátu *.doc. Za účelem efektivní kontroly nabídek při otevírání obálek s nabídkami a následně při posouzení a hodnocení nabídek je vhodné, aby uchazeč předložil nabídku v 6 vyhotoveních (tj. 1 originál a 5 kopií). Za účelem odlišení originálu nabídky s originály úředních listin je nutné originál nabídky označit jako „Originál" a další výtisky jako „Kopie".

3) Uchazeč doručí v uzavřené obálce označené názvem veřejné zakázky a nápisem „NEOTEVÍRAT" na adresu sídla zadavatele uvedenou v bodě I. 1) formuláře oznámení o zakázce. Lhůta pro podání nabídky je uvedena ve formuláři oznámení o zakázce.

4) Na nabídku podanou po uplynutí lhůty pro podání nabídek se pohlíží, jako by nebyla podána. Takovou nabídku zadavatel v souladu s § 71 odst. 5 zákona neotevírá a bezodkladně vyrozumí uchazeče o tom, že jeho nabídka byla podána po uplynutí lhůty pro podání nabídek. Uchazeč na obálce čitelně adresa, na niž je možné uchazeče podle ustanovení § 71 odst. 5 zákona bezodkladně vyrozumět o tom, že jeho nabídka byla podána po uplynutí lhůty pro podání nabídek. Takto pozdě doručená nabídka se uchazeči v souladu s § 155 odst. 1 zákona nevrací.

5) Každý uchazeč může podat pouze jedinou nabídku. Nabídka včetně všech požadovaných dokladů musí být zpracována v českém jazyce (vyjma certifikátů a diplomů, které mohou být v anglickém jazyce nebo v latině). V případě dokladů, které jsou v jiném jazyce než českém (vyjma certifikátů, které mohou být v anglickém jazyce, a diplomů, které mohou být v latině), musí být k těmto dokumentům přiložen úředně ověřený překlad do českého jazyka.

6) Součástí nabídky musejí být doklady prokazující splnění kvalifikace – bližší viz část 5 této zadávací dokumentace. Nabídka a doklady k prokázání splnění kvalifikace musí být, včetně veškerých požadovaných dokladů a příloh, svázány do jednoho svazku. Jednotlivé listy nabídky uchazeč zabezpečí tak, aby je nebylo možno z nabídky vyjmout.

7) Součástí nabídky musí být podle § 68 odst. 3 zákona rovněž:

   a) seznam statutárních orgánů nebo členů statutárních orgánů, kteří v posledních 3 letech od konce lhůty pro podání nabídek byli v pracovněprávním, funkčním či obdobném poměru u zadavatele,

   b) má-li uchazeč formu akciové společnosti, seznam vlastníků akcií, jejichž souhrnná jmenovitá hodnota přesahuje 10 % základního kapitálu, vyhotovený ve lhůtě pro podání nabídek,

   c) prohlášení uchazeče o tom, že neuzavřel a neuzavře zakázanou dohodu podle zvláštního právního předpisu v souvislosti se zadávanou veřejnou zakázkou.

8) Veškeré doklady či prohlášení, u nichž je vyžadován podpis uchazeče, musí být podepsány uchazečem či osobou oprávněnou zastupovat uchazeče; v případě podpisu jinou osobou musí být originál nebo úředně ověřená kopie jejího zmocnění doložen v nabídce.

9) Veškeré doklady musí být kvalitním způsobem vytištěny tak, aby byly dobře čitelné. Žádný doklad nesmí obsahovat opravy a přepisy, které by zadavatele mohly uvést v omyl.

10) Všechny listy každého ze svazků musí být očíslovány průběžnou číselnou řadou počínající číslem 1. Výjimka z povinnosti číslovat listy se vztahuje na úřední doklady resp. jejich úředně ověřené kopie, které nemusí být očíslovány. Vkládá-li uchazeč do svazku jako jeho součást či přílohu některý samostatný celek, který má již listy očíslovány vlastní číselnou řadou, není nutné, aby tyto listy čísloval znovu průběžnou číselnou řadou; to však platí pouze tehdy, je-li číslování listů samostatného celku a průběžné číslování listů svazku zřetelně odlišeno.

11) Zadavatel nepřipouští varianty nabídek. Nabídky podávají uchazeči způsobem uvedeným v § 69 zákona. Zadavatel stanoví, že nedisponuje elektronickými prostředky, které by umožnily elektronické podání nabídky, ty tak mohou být podány pouze v písemné formě.

12) Dokumenty v nabídce budou řazeny následujícím způsobem:

Krycí list nabídky, na kterém uchazeč uvede:

- identifikační údaje dle § 17 písmeno d) zákona, a to obchodní firmu nebo název, sídlo, právní formu, identifikační číslo, bylo-li přiděleno pokud jde o právnickou osobu, a obchodní firmu nebo jméno a příjmení, místo podnikání, popřípadě místo trvalého pobytu, identifikační číslo, bylo-li přiděleno, pokud jde o fyzickou osobu. Podnikatelé zapsaní v obchodním rejstříku také údaj o tomto zápisu, včetně spisové značky, podnikatelé zapsaní v jiné evidenci údaj o tomto zápisu,
- závaznou adresu pro písemný styk s uchazečem (pokud je odchylná od sídla uchazeče),
- nabídkovou cenu za předmět zakázky zpracovanou podle části 6 této zadávací dokumentace,
- zástupce uchazeče pověřeného pro styk se zadavatelem, jeho telefon, fax, e-mail,
- podpis uchazeče nebo osoby oprávněné zastupovat uchazeče,
- podává-li nabídku více uchazečů společně, bude za krycím listem v nabídce vložen originál nebo úředně ověřená kopie listiny obsahující zmocnění pro uchazeče, který je oprávněn za skupinu uchazečů jednat v tomto zadávacím řízení, a z níž vyplývá, že všichni tito uchazeči budou vůči zadavateli a jakýmkoliv třetím osobám z jakýchkoliv závazků vzniklých v souvislosti s plněním předmětu veřejné zakázky či vzniklých v důsledku prodlení či jiného porušení smluvních nebo jiných povinností v souvislosti s plněním předmětu veřejné zakázky zavázáni společně a nerozdílně.

Dále budou následovat:

1) Obsah s členěním dle kapitol a odkazy na první stránky jednotlivých kapitol.
2) Doklady prokazující splnění základních, profesních a technických kvalifikačních předpokladů dle části 5 této zadávací dokumentace.
3) Doklady v souladu s ustanovením § 68 odst. 3 zákona.
4) Specifikace nabídkové ceny dle části 6 této zadávací dokumentace.
5) Detailní popis nabízeného plnění včetně splnění požadavků z části 4 této zadávací dokumentace.
6) Návod k nabízenému produktu v českém jazyce.
7) Popis řešení technické podpory a HelpDeskového systému uchazeče včetně nabízeného SLA a ostatních požadavků dle části 4 této zadávací dokumentace.
8) Návrh smlouvy ve smyslu části 7 této zadávací dokumentace podepsaný uchazečem nebo osobou oprávněnou zastupovat uchazeče.

11 ZÁVĚR

1) Zadavatel nepožaduje složení jistoty.

2) Zadavatel nehradí náklady uchazečů na účast v tomto zadávacím řízení, předložené nabídky zadavatel v souladu s § 155 zákona nevrací.

3) Termín otvírání obálek s nabídkami je stanoven v oznámení zadávacího řízení. Otevírání obálek s nabídkami se může zúčastnit zástupce uchazeče, který podal nabídku do konce lhůty pro podání nabídek. Zástupce uchazeče se prokáže plnou mocí účastnit se jednání podepsanou osobou oprávněnou za uchazeče jednat, pokud sám není touto osobou.

4) Všichni uchazeči jsou svojí nabídkou vázáni do data uvedeného v uveřejněném oznámení zadávacího řízení ve Věstníku veřejných zakázek.

5) Zadavatel si vyhrazuje právo doplnit či změnit zadávací podmínky v průběhu lhůty pro podání nabídek v souladu se zákonem.

Technický gestor

Ing. Pavel Šmejkal

vedoucí oddělení správy komunikační a datové infrastruktury a podpory HW

Ředitel odboru provozu IKT

Ing. Jan Mošna

Seznam příloh:

příloha_č.1_seznam_hardware.xlsx

příloha_č.2_seznam_lokalit.doc

Ing. Milan Shrbený

vrchní ředitel úseku informačních a komunikačních technologií ČSSZ