# Obchodní nabídka pro ČEPRO a.s.

| | |
|---|---|
| datum vypracování | 08.02.2016 |
| název zakázky | **Dodávka systémů síťového monitoringu včetně Log Managementu** |
| předmět | Dodávka a implementace Nástroje pro ochranu integrity komunikačních sítí dle § 17 vyhlášky 316/2014 Sb. o opatřeních a Nástroje pro zaznamenávání činností kritické informační infrastruktury a významných informačních systémů, jejich uživatelů a administrátorů dle § 21 vyhlášky 316/2014 Sb. o opatřeních. |
| zákazník | **ČEPRO, a.s.**<br>IČ: 60193531<br>DIČ: CZ 601 93 531<br>Dělnická 213/12, Holešovice, 170 00 Praha 7 |
| Kontaktní osoba | Milan Trnka<br>Tel.: +420 221 968 254<br>e-mail: milan.trnka@ceproas.cz |
| vypracoval | Josef Appel<br>mobil: +420 728 257 453<br>josef.appel@visitech.cz |
| kontroloval | Dr. Ivo Vašíček, obchodní ředitel |
| datum předání | 08.02.2016 |
| číslo verze | 3 |
| platnost nabídky | 30 dnů |

# OBSAH

# 1. Krycí list

## Krycí list nabídky uchazeče

pro veřejnou zakázku:

## 355/15/OCN
## „Dodávka systémů síťového monitoringu včetně Log Managementu"

**Údaje o zadavateli:**

| | |
|---|---|
| zadavatel (obchodní jméno) | ČEPRO, a.s. |
| sídlo (celá adresa včetně PSČ) | Dělnická 213/12 , 17004 Praha 7 |
| právní forma | akciová společnost |
| IČ | 60193531 |
| DIČ | CZ601 93 531 |
| osoba oprávněná jednat za zadavatele nebo jménem zadavatele | Mgr. Jan Duspěva, předseda předst.<br>Ing. Ladislav Staněk, člen představenstva |
| tel/fax | 221 968 254, Milan Trnka |
| email | milan.trnka@ceproas.cz |

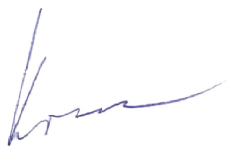
**Údaje o uchazeči:**

| | |
|---|---|
| uchazeč (obchodní jméno) | VISITECH a.s. |
| sídlo (celá adresa včetně PSČ) | Brno Košinova 655/59, Královo Pole, PSČ 612 00 |
| právní forma | Akciová společnost |
| IČ | 25543415 |
| DIČ | CZ25543415 |
| osoba oprávněná jednat za uchazeče nebo jménem uchazeče | Pavel Kocour, předseda představenstva |
| tel/fax | 728 257 453, Josef Appel |
| email | josef.appel@visitech.cz |

**Údaje o nabídce:**

| | |
|---|---|
| celková nabídková cena v Kč bez DPH | 1.799.000,-Kč |

V Brně dne 08.02.2016



.....
Pavel Kocour, předseda představenstva

VISITECH a.s.
Košinova 59, 612 00 Brno
DIČ: CZ25543415

# 2. Profesní kvalifikační předpoklady

Profesní kvalifikační předpoklady jsou splněny formou níže uvedeného čestného prohlášení a předložením výpisu ze seznamu kvalifikovaných dodavatelů.

## 2.1. Čestné prohlášení – Profesní kvalifikační předpoklady

Název zakázky: **Dodávka systémů síťového monitoringu včetně Log Managementu**

Uchazeč

Název: VISITECH a.s.
Sídlo: Košinova 655/59, Královo Pole, 612 00 Brno, ČR

Profesní kvalifikační předpoklady splňuje uchazeč:

a) výpisem z obchodního rejstříku, pokud je v něm zapsán, či výpis z jiné obdobné evidence, pokud je v ní zapsán, ne starší než 90 dnů k datu podání nabídky,

b) dokladem o oprávnění k podnikání podle zvláštních právních předpisů v rozsahu odpovídajícím předmětu veřejné zakázky, zejména doklad prokazující příslušné živnostenské oprávnění či licenci,

Prohlašuji tímto čestně, že uchazeč VISITECH a.s. splňuje profesní kvalifikační předpoklady ve všech bodech tak, jak je zadavatel vymezil ve výzvě.

V Brně, dne 08.02.2016

.....
Pavel Kocour
předseda představenstva

VISITECH a.s.
Košinova 59, 612 00 Brno
DIČ: CZ25543415

# 2.2. Výpis ze seznamu kvalifikovaných dodavatelů



Výpis ze seznamu kvalifikovaných dodavatelů vygenerovaný informačním systémem o veřejných zakázkách

## Výpis ze seznamu kvalifikovaných dodavatelů

vedeného podle § 125 a násled. zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů

**Údaje o dodavateli zapsané v seznamu k 14.12.2015**

### 1. Identifikační údaje o dodavateli

**1.1. Obchodní firma/Název**
VISITECH a.s.

**1.2. Právní forma**
Akciová společnost

**1.3. Sídlo**
Košinova 655/59
61200 Brno Královo Pole
Česká republika

**1.4. IČO**
25543415

**1.5. Statutární orgán**

| Jméno a příjmení statutárního orgánu nebo jeho členů | Funkce ve statutárním orgánu |
|---|---|
| Pavel Kocour | předseda představenstva |
| Ladislav Baloun | místopředseda představenstva |
| Milan Hradil | člen představenstva |

**Způsob a rozsah jednání**

### 2. Základní kvalifikační předpoklady, jejichž splnění dodavatel prokázal

Dodavatel prokázal ministerstvu pro místní rozvoj v souladu s ustanovením § 53 odst. 3 zákona, že:

- § 53 odst. 1 písm. a)
  nebyl pravomocně odsouzen pro trestný čin spáchaný ve prospěch organizované zločinecké skupiny, trestný čin účasti na organizované zločinecké skupině, legalizace výnosů z trestné činnosti, podílnictví, přijetí úplatku, podplacení, nepřímého úplatkářství, podvodu, úvěrového podvodu, včetně případů, kdy jde o přípravu nebo pokus nebo účastenství na takovém trestném činu, nebo došlo k zahlazení odsouzení za spáchání takového trestného činu; jde-li o právnickou osobu, musí tento předpoklad splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu a je-li statutárním orgánem dodavatele či členem statutárního orgánu dodavatele právnická osoba, musí tento předpoklad splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu této právnické osoby; podává-li nabídku či žádost o účast zahraniční právnická osoba prostřednictvím své organizační složky, musí předpoklad podle tohoto písmene splňovat vedle uvedených osob rovněž vedoucí této organizační složky; tento základní kvalifikační předpoklad musí dodavatel splňovat jak ve vztahu k území České republiky, tak k zemi svého sídla, místa podnikání či bydliště,
- § 53 odst. 1 písm. b)
  nebyl pravomocně odsouzen pro trestný čin, jehož skutková podstata souvisí s předmětem podnikání dodavatele podle zvláštních právních předpisů nebo došlo k zahlazení odsouzení za spáchání takového trestného činu; jde-li o právnickou osobu, musí tuto podmínku splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu a je-li statutárním orgánem dodavatele či členem statutárního orgánu dodavatele právnická osoba, musí tento

předpoklad splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu této právnické osoby; podává-li nabídku či žádost o účast zahraniční právnická osoba prostřednictvím své organizační složky, musí předpoklad podle tohoto písmene splňovat vedle uvedených osob rovněž vedoucí této organizační složky; tento základní kvalifikační předpoklad musí dodavatel splňovat jak ve vztahu k území České republiky, tak k zemi svého sídla, místa podnikání či bydliště,

- § 53 odst. 1 písm. c)
  v posledních třech letech nenaplnil skutkovou podstatu jednání nekalé soutěže formou podplácení podle zvláštního právního předpisu,
- § 53 odst. 1 písm. d)
  vůči jehož majetku neprobíhá nebo v posledních třech letech neproběhlo insolvenční řízení, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh nebyl zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení, nebo nebyl konkurs zrušen proto, že majetek byl zcela nepostačující nebo zavedena nucená správa podle zvláštních právních předpisů,
- § 53 odst. 1 písm. e)
  není v likvidaci,
- § 53 odst. 1 písm. f)
  nemá v evidenci daní zachyceny daňové nedoplatky, a to jak v České republice, tak v zemi sídla, místa podnikání či bydliště dodavatele,
- § 53 odst. 1 písm. g)
  nemá nedoplatek na pojistném a na penále na veřejné zdravotní pojištění, a to jak v České republice, tak v zemi sídla, místa podnikání či bydliště dodavatele,
- § 53 odst. 1 písm. h)
  nemá nedoplatek na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti, a to jak v České republice, tak v zemi sídla, místa podnikání či bydliště dodavatele,
- § 53 odst. 1 písm. i)
  nebyl v posledních 3 letech pravomocně disciplinárně potrestán či mu nebylo pravomocně uloženo kárné opatření podle zvláštních právních předpisů, je-li podle § 54 písm. d) požadováno prokázání odborné způsobilosti podle zvláštních právních předpisů; pokud dodavatel vykonává tuto činnost prostřednictvím odpovědného zástupce nebo jiné osoby odpovídající za činnost dodavatele, vztahuje se tento předpoklad na tyto osoby,
- § 53 odst. 1 písm. j)
  není veden v rejstříku osob se zákazem plnění veřejných zakázek.
- § 53 odst. 1 písm. k)
  nebyla mu v posledních 3 letech pravomocně uložena pokuta za umožnění výkonu nelegální práce podle zvláštního právního předpisu.
- § 53 odst. 2 písm. b)
  nebyl pravomocně odsouzen pro trestný čin teroristického útoku, trestný čin krádeže spáchaný v úmyslu umožnit nebo usnadnit spáchání trestného činu teroristického útoku, trestný čin vydírání spáchaný v úmyslu umožnit nebo usnadnit spáchání trestného činu teroristického útoku, trestný čin padělání a pozměnění veřejné listiny spáchaný v úmyslu umožnit nebo usnadnit spáchání trestného činu teroristického útoku, včetně případů, kdy jde o přípravu nebo pokus nebo účastenství na takovém trestném činu, nebo došlo k zahlazení odsouzení za spáchání takového trestného činu; jde-li o právnickou osobu, musí tento předpoklad splňovat statutární orgán nebo každý člen statutárního orgánu, a je-li statutárním orgánem dodavatele či členem statutárního orgánu dodavatele právnická osoba, musí tento předpoklad splňovat statutární orgán nebo každý člen statutárního orgánu této právnické osoby; podává-li nabídku nebo žádost o účast zahraniční právnická osoba prostřednictvím své organizační složky, musí předpoklad podle tohoto písmene splňovat vedle uvedených osob rovněž vedoucí této organizační složky; tento základní kvalifikační předpoklad musí dodavatel splňovat jak ve vztahu k území České republiky, tak k zemi svého sídla, místa podnikání nebo bydliště.

## 3. Profesní kvalifikační předpoklady, jejichž splnění dodavatel prokázal

### 3.1 Profesní kvalifikační předpoklady dle ustanovení § 54 písm. a) dodavatel prokázal:

Výpisem z obchodního rejstříku

### 3.2 Oprávnění k podnikání dle ustanovení § 54 písm. b) dodavatel prokázal:

| Název dokladu | Vystavil | Předmět podnikání | Obory činnosti | Datum vystavení | Datum platnosti |
|---|---|---|---|---|---|
| Výpis z veřejné části Živnostenského rejstříku | Česká pošta, s.p. | Viz poznámka 1 za tabulkou | | 07.05.2014 | |
| Výpis z veřejné části Živnostenského rejstříku | Česká pošta, s.p. | Výroba, obchod a služby neuvedené v přílohách 1 až 3 živnostenského zákona | Viz. poznámka 2 za tabulkou | 07.05.2014 | |

Pozn. 1
Výroba, instalace, opravy elektrických strojů a přístrojů, elektronických a telekomunikačních zařízení
Pozn. 2
Přípravné a dokončovací stavební práce, specializované stavební činnosti
Zprostředkování obchodu a služeb
Velkoobchod a maloobchod
Údržba motorových vozidel a jejich příslušenství
Poskytování software, poradenství v oblasti informačních technologií, zpracování dat, hostingové a související činnosti a webové portály
Pronájem a půjčování věcí movitých

## 4. Datum podání žádosti o zápis do seznamu a jiné důležité informace

Dodavatel podal žádost o zápis do seznamu dne 12.05.2014. Rozhodnutí o zápisu dodavatele do seznamu nabylo právní moci dne 09.06.2014.
Poslední aktualizace zápisu v seznamu byla provedena dne 12.02.2015.

---

Správnost tohoto výpisu se potvrzuje

Česká republika - Ministerstvo pro místní rozvoj

Datum: 14.12.2015

Evidenční číslo: W15120000256

Elektronicky podepsáno dne 14.12.2015 Česká republika, Ministerstvo pro místní rozvoj [IČ 66002222]

# 3. Cenová nabídka, předmět dodání

Zhotovitel nabízí splnění předmětu zakázky specifikovaného ve výzvě k podání nabídky na veřejnou zakázku za nabídkovou cenu ve výši specifikované níže, dle požadované struktury.

Uchazeč prohlašuje, že uvedená nabídková cena je cenou nejvýše přípustnou a nepřekročitelnou, a to s výjimkou změny zákonných sazeb DPH a že obsahuje veškeré náklady nezbytné k realizaci předmětu zakázky.
V rámci projektu bude dodána technická dokumentace a funkční schéma, který je součástí ceny.

Splatnost daňového dokladu – faktury je 30 dnů ode dne jejího prokazatelného doručení zadavateli.
Přílohou daňového dokladu – faktury bude předávací protokol (Protokol o předání a převzetí)

Záruka na předmět díla je 24 měsíců.

## 3.1. Předmět dodání

### 3.1.1. Monitoring sítí

| Počet Ks | Popis produktu |
|---|---|
| 1 | INVEA, FlowMon, Probe, IFP-4000-CU |
| 1 | INVEA, FlowMon, Collector, IFC-500-VA |
| 1 | INVEA, FlowMon, ADS, ADS Business (2 uživatelé, 2 zdroje dat, 1500 fps) |
| 1 | INVEA, FlowMon GOLD support 1 rok, Probe, IFP-4000-CU |
| 1 | INVEA, FlowMon GOLD support 1 rok, Collector, IFC-500-VA |
| 1 | INVEA, FlowMon GOLD support 1 rok, ADS, Business |
| | Implementace HW a SW |
| | Zapojení, instalace a základní konfigurace |
| | Zaškolení 2 administrátorů na straně Zadavatele (1 x školení) |

### 3.1.2. Log management

| Popis produktu |
|---|
| SSB T4 HW Appliance (4TB HDD) - 250 LSH |
| Implementace SSB a agentů |
| Zaškolení 2 administrátorů na straně Zadavatele (1 x školení) |
| Maintenance (Extended Support) aplikace a servisní podpora pro 250 IP adres za 1. rok |

| |
|---|
| HW pro Syslog-ng RELAY HA (8x CORE, 16GB RAM, 300GB HDD (RAID1), 2x PSU) |
| Implementace Syslog-ng RELAY HA |
| Maintenance HW / 1 rok |

## 3.2. Cenová nabídka

### 3.2.1. Celková cena za předmět zakázky

| Předmět zakázky | Cena celkem |
|---|---|
| Celková cena za dílo dle bodu 1.1 ZD | 1.799.000,-Kč |
| Celková cena v Kč bez DPH | 1.799.000,-Kč |

Pro výpočet cen licencí byl použit kurz 1 EUR= 27,02 Kč, a 1 USD = 24,62 Kč. Ceny uvedené v cizích měnách budou přepočteny na Kč ke dni uskutečnění zdanitelného plnění dle kurzovního lístku ČNB.

### 3.2.2. Cena za servis 24 měsíců

| Popis | Celková cena bez DPH | Výše DPH | Celková cena s DPH |
|---|---|---|---|
| Monitoring sítí – servis 24 měsíců | 288.000,-Kč | 21% | 348.480,-Kč |
| Log Management – servis 24 měsíců | 336.000,-Kč | 21% | 406.560,-Kč |
| **Celková předpokládaná cena za servis 24 měsíců** | **624.000,-Kč** | **21%** | **755.040,-Kč** |

Společnost VISITECH uvádí jako předpokládanou cenu za servis a podporu díla po dobu 24 měsíců od předání díla 624.000 Kč bez DPH.

**Software Servis**
V ceně servisních služeb a pozáručního servisu jsou zahrnuty níže uvedené činnosti, které budou pro Zadavatele realizovány na základě Smlouvy o poskytování servisní podpory, a to včetně požadovaných parametrů SLA:

- servisní zásahy
- upgrade nových verzí
- kontrola stavu
- úprava reportingu
- pokročilé customizované nastavení
- Rozsah paušální podpory: min. 24 MD za rok; nevyčerpané paušální MD jsou převoditelné bez omezení do následujících měsíců. Převod nevyčerpaných paušálních MD je ohraničen kalendářním rokem, pak nevyčerpané paušální hodiny propadají. MD – 8 pracovních hodin. Cena za MD = 12.000 Kč bez DPH.

# 4. Návrh technického řešení, technologický postup

Společnost VISITECH a.s. je schopna splnit požadavky uvedené v zadávací dokumentaci a v případě vyzvání ze strany objednatele je schopna doložit reference v dané oblasti.

Název zakázky: **Dodávka systémů síťového monitoringu včetně Log Managementu**

Uchazeč

Název: VISITECH a.s.
Sídlo: Košinova 655/59, Královo Pole, 612 00 Brno, ČR

Prohlašuji tímto čestně, že uchazeč VISITECH a.s. splňuje veškeré technické požadavky na řešení uvedené ve všech bodech tak, jak je zadavatel vymezil v zadávací dokumentaci. Návrh řešení obsahuje potřebný HW, SW a služby s nimi spojené.

V Brně, dne 08.02.2016

.....
Pavel Kocour
předseda představenstva

VISITECH a.s.
Košinova 59, 612 00 Brno
DIČ: CZ25543415

## 4.1. Monitorovací systém

V oblasti monitoringu sítí bude navržené řešení, které je uvedeno v předmětu dodání, splňovat níže uvedené.

Monitorovací systém bude umožňovat dlouhodobé detailní monitorování dění na počítačové síti. Získané informace o dění na síti a chování uživatelů bude umožňovat v reálném čase sledovat a vyhodnocovat bezpečnostní hrozby v síti. Monitorovací systém bude nezávislý na použité síťové infrastruktuře a svou funkcí nebude ovlivňovat sledovanou síť. Ze strany monitorované sítě není zařízení detekovatelné. Vytváření síťových statistik bude prováděno pomocí nezávislých a k tomuto účelu určených zařízení.

Uložení a zpracování statistik bude redundantní na k tomu určených zařízeních – kolektorech. Ty budou vybaveny SW či HW RAIDem. Kolektory poskytují analytické nástroje pro práci se statistikami a jsou schopny zaznamenat každou komunikaci po dobu několika měsíců bez jakékoliv ztrátové agregace a budou poskytovat upozornění a rozhraní pro práci bezpečnostního technika.

Systém bude pracovat s technologií NetFlow ve verzi 5 a 9. Tato technologie je v současné době nejpřesnějším a nejmodernějším prostředkem pro monitorování sítě a oproti konkurenčním technologiím nabízí výhody zpracování všech paketů bez vzorkování, imunitu vůči šifrovanému provozu, škálovatelnost i pro vysokorychlostní a zatížené sítě a průmyslovou standardizaci. Díky standardizaci je možné jeden zdroj statistik využít i v dalších systémech, jako je tiketovací nástroj, systém pro log managemet, či SIEM.

**Vlastnosti:**

- ucelené škálovatelné řešení umožňující dlouhodobé monitorování sítě na bázi technologie NetFlow (nutná podpora NetFlow v5 a NetFlow v9),
- podpora standardů NEL, NSEL a NBAR2,
- sledování bezpečnostních incidentů v několika lokalitách s centrální správou,
- nezávislost na stávající síťové infrastruktuře (optické či metalické datové rozvody) a použitých aktivních prvcích, nesmí docházet k ovlivňování chování sítě,

- specializovaná dedikovaná zařízení (sondy) pro vytváření detailních statistik IP toků o dění na síti, standardizovaný protokol pro výměnu dat o IP tocích (NetFlow v5, v9),
- bezeztrátový sběr dat na kolektorech z několika datových zdrojů, podpora standardizovaných protokolů pro výměnu dat o IP tocích (NetFlow v5, v9 - RFC3954),
- dlouhodobé ukládání statistik IP toků a jejich centrální sledování a vyhodnocování bezpečnostních hrozeb v síti, prokazování bezpečnostních incidentů,
- plná zákaznická podpora v českém jazyce,
- systém ověřený instalacemi na páteřních linkách (10GE) minimálně u 5 poskytovatelů internetu nejméně ve třech zemích světa,
- podpora IPv4, IPv6, VLAN, MPLS, Ethernet 10Mb/s až 10Gb/s, otevřené rozhraní s možností integrace nástrojů i třetích stran.

**Zdroje dat NetFlow**

Zdroje dat NetFlow jsou nezávislé na použité síťové infrastruktuře a svou funkcí nijak neovlivňují sledovanou síť. Ze strany monitorovacích rozhraní připojených do sledované sítě není zařízení detekovatelné. Vytváření síťových statistik je prováděno autonomními, nezávislými a k tomuto účelu navrženými zařízeními.

**Technické, programové vybavení sondy:**

- 100% přesný nezávislý autonomní zdroj NetFlow statistik s podporou IPv4, IPv6, VLAN, MPLS, GRE, NetFlow v5/v9,
- detekce aplikací dle standardu NBAR2, monitorování a analýza HTTP provozu a VoIP statistik,
- snadná instalace do stávající síťové infrastruktury,
- rack mount zařízení,
- pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAP, případně v kombinaci se SPAN porty),
- jeden administrativní port 10/100/1000Mb/s (UTP kabeláž) pro zabezpečenou vzdálenou správu a přenos NetFlow dat,
- zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS,
- správa uživatelů a přístupových práv na zařízení,
- možnost nastavení rychlosti monitorované linky 10/100/1000Mb/s na metalických rozhraních,
- vestavěný kolektor pro dočasné ukládání NetFlow statistik (zajištění redundance), který zahrnuje uživatelsky definovaný dashboard, automatickou tvorbu reportů, detekci aktivních zařízení a detailní analytické možnosti,
- časová synchronizace zařízení proti centrálnímu zdroji času na síti,
- minimální výkon 1,48 milionů paketů za sekundu na každém portu,
- jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky,
- možnost přístupu a konfigurace zařízení prostřednictvím sériové linky (RS-232),
- použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména,
- podpora autentizace vůči LDAP (Active Directory).

**Vlastnosti navržené sondy z pohledu generování NetFlow dat:**

- pasivní odposlech dat ze sítě pomocí specializovaných zařízení (TAPů) či SPAN portů,
- podpora protokolů pro výměnu dat – programové vybavení sondy musí umožnit vytváření NetFlow dat ve formátech verzi 5 a 9,
- zpracování datového provozu IPv4 a IPv6, VLAN, MPLS, GRE a jejich reportování na kolektor,
- uživatelsky definovatelné šablony pro protokoly NetFlow v9 a případně IPFIX,
- podpora monitorování MAC adres,
- detekce aplikací dle standardu NBAR2,
- monitorování a analýza HTTP provozu - včetně položek typu URL, hostname,
- monitorování VoIP statistik - položky typu jitter, latence, ztrátovost paketů,
- hloubkový monitoring DNS provozu, včetně identifikátorů, značek a response kódů
- dlouhodobé a stabilní zpracování na všech měřících rozhraních,
- minimální kapacita paměti současných toků na sondě 500 tisíc toků,
- podpora pro nastavení časů u aktivní a neaktivní expirace toků,
- podpora vzorkování na úrovni paketů,
- podpora vzorkování na úrovni toků,
- podpora simultánního exportu NetFlow statistik na libovolný počet cílů (redundantní kolektory v různých lokalitách, lokální uložení dat na sondě),

- podpora filtrování dat na sondě na základě IP prefixů a VLAN (pro různé cíle exportu různé statistiky),
- podpora vyplňování AS na základě vestavěného či dodaného seznamu,
- podpora filtrování a export datových toků na základě AS.

**Vlastnosti zdrojů NetFlow dat (sondy):**

- počty a rychlosti/typy rozhraní – 1x – 4x 1GbE, metalika – RJ-45,
- podpora 1 Gigabit Ethernetu,
- 1U či 2U velikost,
- minimální výkon 1,48 milionu paketů za sekundu na každém 1GbE portu,
- minimální kapacita paměti současných toků na sondě 4 miliony toků – 1Gb/s modely
- současné měření síťového provozu na minimálně čtyřech gigabitových rozhraních současně pomocí jednoho zařízení,
- připojení na měřenou síť pomocí metalických či optických konektorů či SFP transceiverů – umožňuje ad hoc změnu typu monitorované linky (metalická/optické single mód či optická multi mód) nebo kombinaci více typů linek na jedné sondě.

**Vlastnosti kolektorů**

Kolektory jsou zařízení (datová úložiště) s vysokou diskovou kapacitou určená pro uložení, vizualizaci a vyhodnocení síťových statistik exportovaných NetFlow dat. Zobrazení uložených NetFlow dat a jejich analýzy (vyhledávání, agregace, výpisy aj.) probíhají na kolektoru a jsou zpřístupněna operátorovi prostřednictvím zabezpečeného rozhraní.

**Programové a technické vybavení kolektoru:**

- zabezpečené kolektory NetFlow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce,
- možnost dohledání každé komunikace, průběžné grafy, podpora upozornění, rozšiřitelnost o pluginy na míru,
- snadná instalace do stávající síťové infrastruktury
- jedno administrativní rozhraní pro zabezpečenou vzdálenou správu a přenos NetFlow dat,
- zabezpečená vzdálená správa, dohled a konfigurace – SSH, HTTPS,
- víceuživatelský přístup - včetně možnosti definovat k jakým datům má jednotlivý uživatel přístup,
- podpora autentizace vůči LDAP (Active Directory),
- integrace dohledového systému pro kontrolu dostupnosti (SNMP),
- časová synchronizace zařízení proti centrálnímu zdroji času na síti,
- jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky,
- použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména.

**Kolektory z pohledu sběru dat:**

- podpora verze NetFlow protokolu – programové vybavení kolektoru umožňuje sběr a vyhodnocení NetFlow dat ve verzi 5 a 9,
- podpora pro sběr a analýzu sFlow a NetStream dat,
- podpora standardů NEL a NSEL, monitorování MAC adres,
- podpora pro příjem a analýzu informací o detekovaných aplikacích dle NBAR2 standardu,
- podpora pro příjem a analýzu HTTP provozu - včetně položek typu URL, hostname,
- podpora pro příjem a analýzu VoIP statistik (jitter, latence, ztrátovost),
- podpora sběru a analýzy dat z autentizačních systémů,
- kapacita datového úložiště – systém je schopen sbírat a ukládat dlouhodobě data z desítek NetFlow zdrojů. Disková kapacita datového úložiště musí umožnit záznamy statistik bez jakékoliv redukce v horizontu minimálně tří měsíců.
- možnost přeposílání přijímaných NetFlow statistik ke zpracování na další kolektory včetně možnosti filtrace na úrovni NetFlow paketů.

**Kolektory z pohledu vyhodnocení dat:**

- ucelené řešení pro sledování síťové komunikace, jak v reálném čase, tak dlouhodobě,
- uživatelsky definovatelný dashboard (konfigurace per uživatel),

- vytváření dlouhodobých grafů a přehledů s různými typy pohledů rozdělených do kategorií podle objemu (počet přenesených bytů, toků, paketů), IP provozu (TCP, UDP, ICMP, ostatní) nebo protokolu (HTTP, IMAP, SSH),
- generování statistik a podrobných výpisů nad volitelnými časovými intervaly,
- reporty v podobě průběhových i koláčových grafů,
- online reporty včetně možnosti exportu do PDF a CSV formátu,
- automatické zasílání reportů emailem (reporty v českém a anglickém jazyce),
- řízení uživatelského přístupu k jednotlivým typům reportů (uživatel je oprávněn zobrazovat pouze statistiky, ke kterým mu bylo nastaveno oprávnění administrátorem),
- výpis tzv. top N statistiky podle různých kritérií (počet přenesených bytů, paketů, toků atd.) umožňující vypsat nejaktivnější či anomální počítače podílející se na síťovém provozu,
- upozornění administrátorům v případě vzniku uživatelem definované situace (např. nadměrný přenos dat, výskyt nebezpečné anomálie, použití zakázané aplikace atd.) prostřednictví emailu, SNMP trapu a syslogu,
- vytváření profilů pro ukládání dat vyhovující nadefinovaným filtrům (např. HTTP, FTP, SMTP, SSH provoz),
- podrobné textové výpisy jednotlivých toků s možnostmi filtrování a agregace,
- drill-down – možnost dohledat každý jednotlivý tok zaznamenaný sondami,
- detekce aktivních zařízení na sítí - pro podporu konceptu BYOD,
- podpora korelace dat z autentizačních systémů se síťovými statistikami pro tzv. Identity awereness,
- podpora geolokace na základě IP adresy,
- otevřené rozhraní s možnostmi skriptování a zpracování dávkových úloh.

**Vlastnosti zdrojů kolektorů dat**

- ukládání síťových statistik na multigigabitových linkách bez jakékoliv redukce minimálně po dobu 3 měsíců,
- kapacita 500GB,
- podpora nasazení do virtuálního prostředí VMware
- výkon 75 000 toků za vteřinu.

**Vlastnosti automatického vyhodnocování NetFlow dat**

V rámci řešení je počítáno s automatickým vyhodnocováním měřených dat s cílem identifikovat provozní a bezpečnostní incidenty a tyto reportovat/alertovat jako události. Systém je založen na pokročilých metodách tzv. behaviorální analýzy a umožňuje tak odhalovat hrozby a incidenty, pro které dosud není dostupná signatura.

Funkce poskytované řešením automatické analýzy NetFlow dat:

- Deduplikace a podpora korelace dat před/za PROXY
- Výkon 2500 toků/s, podpora pro samplování na úrovni toků
- Předdefinovaná sada pravidel a algoritmů pro odhalování nežádoucích vzorů chování o Útoky (skenování portů, slovníkové útoky, denial of service, protokol telnet)
    - Anomálie datového provozu (DNS, DHCP, multicast, nestandardní komunikace) o Nežádoucí aplikaci (P2P sítě, instant messaging, anonymizační služby)
    - Interní bezpečnostní problémy (viry, spyware, botnety) o Poštovní provoz (odchozí spam)
    - Vestavěná IP reputační databáze pro detekci útoků a botnetů
    - Provozní problémy (zpoždění, nadměrná zátěž, reverzní DNS záznamy, nefunkční aktualizace)
- Budování dlouhodobých profilů chování zařízení na síti z pohledu služeb, objemů provozu a komunikačních partnerů
    - Objemy datového provozu (přenesená data, počty uskutečněných spojení) o Struktura služeb (využívané a poskytované služby)
    - Komunikační partneři
    - Vyhledávání serverů a klientů v síti
    - Vyhledávání zařízení poskytujících nebo využívajících služby v síti o Celkový pohled na strukturu provozu
    - Detailní profil pro každou IP adresu, sledování trendů

- Předdefinovaná sada pravidel pro odhalování obecných anomálií v síti
  - Predikce chování sítě a detekce odchylek
- Přehledný dashboard s okamžitou indikací problémů a top statistik
- Definice závažnosti události na základě IP adresních rozsahů, typů a míst v síti
- Víceuživatelský přístup - včetně možnosti definovat k jakým datům a událostem má jednotlivý uživatel přístup
- Integrace informací ze služeb DNS, WHOIS, geolokační služby
- Interaktivní vizualizace událostí
- Export statistik o provozu na síti, které událost způsobily ve vhodné formě pro prokazování incidentů
- Export událostí do CSV
- Automatický export událostí ve formátu CEF protokolem Syslog nebo SNMP, pro možnost odesílání dat do systémů třetích stran, jako jsou tiketovací nástroje, log management či SIEM

**Mimofunkční vlastnosti**

- Řešení umožňuje více jazykových mutací, minimálně však češtinu, angličtinu, alespoň v částech řešení, které jsou přístupné pro koncové uživatele
- Řešení také umožňuje úpravy vzhledu rozhraní pro koncové uživatele do korporátního designu

**Omezení a limity**

- Řešení bude implementováno bez přerušení nebo narušení provozu společnosti ČEPRO
- Řešení umožní znovupoužití a využití již pořízených prostředků a služeb na straně zadavatele, a to jak z hlediska již provozované infrastruktury, tak i z hlediska platformy, na níž bude samo vystavěno
- Řešení umožní iterativní nasazení, tedy nasazení po jednotlivých částech
- Řešení nebude zavádět proprietární protokoly nebo formáty tam, kde jsou k dispozici kvalitativně srovnatelné průmyslové standardy, akceptované dalšími výrobci

## 4.2. Log Management

Řešení společnosti VISITECH je postaveno na dodávce a implementaci Log managementu - **Syslog Store Box (SSB) od společnosti BalaBit.**

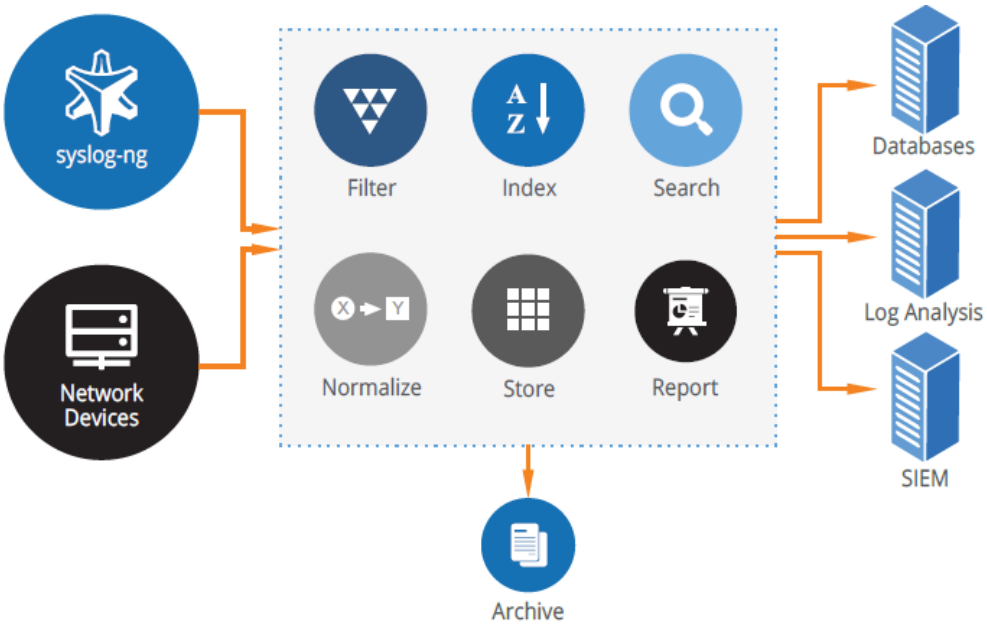
### 4.2.1. Popis produktu

V případě zákazníka ČEPRO, a. s., se jedná o komplexní řešení, které je optimalizováno i pro případné rozšíření o SIEM.
Hlavní komponentou je Syslog Store Box v licenci pro 250 IP adres v provedení hardwarová appliance ve verzi T4 (4x CORE, 8GB RAM, 4TB RAID HDD, 2x PSU).

Součástí nabídky je zároveň dodávka aplikace Syslog-ngNG včetně odpovídajícího HW pro implementaci Syslog-ngNG Relay pro zajištění High Availability na úrovni sběru logů (tedy zajištění „zero drop").

### 4.2.2. Popis řešení

Díky přehlednému webovému rozhraní pro vyhledávání a customizované reporty a statistiky, SSB umožňuje snazší práci s logy při jejich vyhledávání, a to jak za účelem auditu, tak i pro zajištění každodenního provozu.




SSB nabízí konfigurovatelné uživatelské oddělení rolí s využitím silných šifrovacích metod, chrání logy před neoprávněným přístupem k citlivým datům.

Samozřejmostí je automatická archivace a zálohování logů, čímž zároveň SSB naplňuje legislativní požadavky jako např. ISO / IEC / BS, SOX, Basell, HIPAA, COBIT nebo PCI – DSS.

SSB je k dispozici pro zákazníky ve velké škále jak z pohledu výkonu hardware, tak i z pohledu licence (dle počtu připojených IP adres).

HW Appliance SSB T4 bude zapojena v určené lokalitě zákazníka. Jedná se o appliance, a tedy není nutné realizovat instalaci OS a následně aplikace. Vše bude připraveno přímo od výrobce a v prostředí zákazníka bude realizována jenom síťová konfigurace a následně hlavní konfigurace Log Managementu.

Řešení pokryje potřeby zadavatele v rozsahu všech lokalit (cca 25) propojených WAN sítí zadavatele. V rámci každé lokality zajistí řešení sběr událostí z platforem: Windows, CISCO IOS, MSSQL, VMWARE a dále z proprietárních aplikací. V rámci každé lokality řešení aplikuje agent/relay/sběrač/konektor, který je instalován na vybraný Windows server pro zajištění sběru lokálních Windows logů a pro zajištění sběru logů z ostatních komponent dané lokality (jedná se tedy o speciální konfiguraci, kde daný syslog-ng agent slouží nejen jako agent pro Windows logy, ale také jako relay pro ostatní zdroje v dané lokalitě). Sběr událostí tedy nebude prováděn vzdáleně.

Samozřejmostí je využití komprimace na přenosovém syslog kanálu + TLS šifrování pro zajištění důvěrnosti přenášených dat. Pokud bude potřeba snížit nároky na přenosový kanál tak bude realizován „throttling".

Pro zajištění HA bude na dvojici vybraných serverů instalován syslog-ng RELAY server, který bude v režimu failover přijímat logy ze všech lokalit, bude obsahovat výstupní CACHE, pokud by nastala nedostupnost cíle (SSB). Tímto řešením je dosažen HA/"zero drop" sběr logů bez pořizování HA licence pro SSB. Nezanedbatelnou výhodou je také možnost posílat logy do budoucího SIEM bez komplikovaných rekonfigurací a změn (jenom se na úrovni syslog-ng RELAY přidá další destination), taktéž toto řešení poskytuje možnosti instalace SIEM konektorů v HA zapojení přímo na RELAY servery a tím docílit taktéž HA/"zero drop" při implementaci SIEMu bez zakoupení HA licence na úrovni SIEMu.

Z pohledu uložení dat bude využito interní úložiště SSB boxu o velikosti 4TB (v RAID1), kde budou všechny data uložena v šifrované a komprimované podobě s časovým razítkem TSA. Retenční politika bude stanovena dle reálného zaplnění lokálního disku SSB boxu, počítáme, že to bude +- 150 dní.

Součástí dodávky/implementace bude instalace a konfigurace klientů/agentů pro jednotlivé operační systémy a „best practice" doporučení/součinnost při konfiguraci zařízení, které logují přímo protokolem syslog. Pro sběr logů z databází bude využit vstavěný ODBC konektor na úrovni syslog-ng agenta/relay.

**Podpora vstupních protokolů (zdrojů log záznamů) a přenosu dat:**
• SNMP
• syslog:
• UDP (dle RFC 3164)
• TCP
• ETF (RFC 5424) + TLS
• Aktivní sběr logů z databází (přes ODBC jak na úrovni SSB tak pomocí syslog-ng RELAY serverů).
• Agent/Client pro sběr log záznamů jak pro prostředí Windows, tak i pro prostředí Linux/Unix (HP-UX, Solaris, …)/AIX:
• sběr Windows EVT záznamu i z kontejneru Windows Server.
• sběr AIX/Solaris/HP-UX/IRIX auditních OS záznamů.
• sběr textových logů ze souborů.
• sběr logů z databází
• přenos log dat (tj. forward pres syslog) šifrovaným kanálem.
• Podpora RELAY funkce (tj. přeposílací servery, např. pro infrastrukturu v DMZ)
• Podpora BUFFER/CACHE na výstupu jak u Agenta, tak pro RELAY, a také pro Server/Appliance.
• Podpora výstupních protokolů (destinations ~ umístění log záznamu):
• syslog (UDP, TCP, IETF).
• zápis log dat napřímo do databází (ODBC).
• SNMP Trap.
• Možnost konfigurace pokročilého filtrování log záznamů (jakýkoli vstup log dat prochází libovolnou sadou filtrů na libovolný výstup).
• Ukládání log dat:
• Textové uložiště v originálním (RAW) formátu.
• Šifrované uložiště (logspace) s podporou šifrování privátním klíčem/certifikátem a TSA podpisem, pro zajištění právních potřeb forenzního šetření.
• Podpora indexace log dat pro rychlé vyhledávání údajů i v nestrukturovaných v datech (položka message u syslog protokolu).
• Řízení přístupu (AAA):
• Řízení přístupu na úrovni jednotlivých úložišť (logspace).
• podpora GROUP managementu.
• podpora autentizace přes RADIUS.
• lokální /externí databáze uživatelů – LDAP.
• Zálohování, Archivace, Export, Sdílení log dat:
• nezávislé zálohovací politiky jak pro konfiguraci, tak pro jednotlivá úložiště (logspace).
• nezávislé archivační (retention) politiky pro jednotlivá úložiště.
• podpora exportu/sdílení log dat v originálním i ve strukturovaném tvaru.
• Alerting:
• RATE alerting (detekce změn „nestandardního chování zdrojů log záznamů" pro nastavené limitní hladiny datových přenosů v čase).
• Výskyt definovaného slova/znaku v logu (Např. „error", „fail" nebo „alert").

• Artificial Ignorance – funkcionalita, která identifikuje, co je informačně nezajímavé a potlačuje eskalaci. Nebo identifikuje, co informačně systém log managementu ještě nikdy neviděl a eskaluje anomálii.
• Vyhledávání a Reporting:
• Vyhledávání na základě indexace, umožnění vytváření vlastních analytických pohledů.
• Dashboardy/Statistiky log management infrastruktury.
• Uživatelsky konfigurovatelný reporting strukturovaných dat (timestamp, facility, proirity, tag, program, hostname, atd.).

Navrhnuté řešení výkonově pokrývá špičkový krátkodobý vstup a bezztrátové zpracování minimálně 40.000 EPS (v laboratorních podmínkách bylo dosaženo 1 milion EPS).
Licence řešení pokryje sběr událostí z 250 zařízení, v odhadované kapacitě 80GB/den a zajistí dlouhodobě schopnost sběru 5.000 EPS (událostí za vteřinu - průměr za 24hod.). Řešení je škálovatelné tak, aby rychlost i kapacita všech částí mohla být bez ztráty dat navýšena nejméně o 100%.

# 5. Harmonogram

Předpokládaný termín ukončení realizace předmětu díla vychází zcela z požadavku Zadavatele. Avšak dílo bude předáno nejpozději do 60 dnů od data objednání. Přesný harmonogram bude konzultován a potvrzen se Zadavatelem. Návrh harmonogramu viz níže.

| **Termín ve dnech** | **Popis činností** |
|---|---|
| T | Objednávka, Kick off projektu |
| T + 30 | Nákup potřebného HW, SW |
| T + 60 | Základní konfigurace, Zapojení a instalace HW a SW, Zaškolení 2 administrátorů na straně Zadavatele, akceptace díla |
| | Ostrý provoz, případný servis |

# 6. Informace o společnosti VISITECH

## 6.1. Identifikační údaje předkladatele

Obchodní firma: VISITECH a.s.

Sídlo společnosti: Brno Košinova 655/59, Královo Pole, PSČ 612 00

IČ/ DIČ: 25543415 / CZ25543415

Zapsaná v OR vedeného u Krajského soudu v Brně, spisová značka B 6323

Bankovní spojení: Raiffeisenbank a.s. 1017756001/5500

**Hlavní kontaktní osoba**

| | |
|---|---|
| Jméno a příjmení: | Josef Appel |
| Pozice/funkce: | Obchodní manažer |
| Tel.: | +420 728 257 453 |
| Fax: | 274 772 389 |
| E-mail: | josef.appel@visitech.cz |
| Adresa: | Weilova 2e/1450, 102 05 Praha 10 |

**Kontaktní osoba managementu**

| | |
|---|---|
| Jméno a Příjmení: | Ivo Vašíček |
| Pozice/funkce: | Obchodní ředitel |
| Tel: | +420 608 240 742 |
| Fax: | 543 211 754 |
| E-mail: | ivo.vasicek@visitech.cz |
| Adresa: | Košinova 655/59, Královo pole, 612 00 Brno |

### 6.2. Profil společnosti

Naše společnost působí na trhu IT v ČR od roku 1995. Mnoho let se profilujeme na trhu IT/ICT jako specializovaný dodavatel hardware s přidanou hodnotou pro síťová řešení a software pro zajištění bezpečnosti informačních technologií a implementace informačních systémů Microsoft. Jsme certifikovaným partnerem společnosti Microsoft s kompetencí pro Microsoft Dynamics NAV, CRM a SharePoint. Dále jsme partneři společností SOPHOS, Acronis, Dell, HP, Datapolis, Experlogix, České Radiokomunikace.

Navazujícími aktivitami je softwarová podpora dalších podnikových procesů. V týmu projektového řízení za využívání produktů Microsoft Dynamics NAV, Microsoft Dynamics CRM a Microsoft SharePoint pracují certifikovaní odborníci pro oblast Financí, Nákupu, Prodeje, Skladů, Výroby, Servisu, CRM, Finančního managementu a Finanční analýzy, Projektového řízení, Procesního řízení. Součástí týmu jsou odborníci v oblasti programování, vývoje, správy informačního systému a projektového managementu. Všichni členové týmu mají prokazatelné zkušenosti s implementací výše uvedených technologií a to včetně implementací v zahraničí.

**IS a aplikace - Microsoft**

- Microsoft Dynamics CRM -systém pro řízení vztahů se zákazníky
- Microsoft Dynamics NAV - podnikový informační systém ERP (rozšiřující aplikace: NAVmobile - mobilní přístup k NAV)
- MS SharePoint - dokument management systém (rozšiřující aplikace: Workbox - grafický workflow manažer, produktový konfigurátor)
- Servery a nástroje - Windows Server, Exchange server, SQL Server,…

**E – learningové portály** – založené na bázi systému MS SharePoint.
**HW, SW a komponenty datových sítí** – notebooky, servery, PC sestavy, monitory, sítě a kabelážní systémy, aktivní prvky, rozvaděče, …
**Vývoj informačních systémů** – zpracování specifických informačních systémů a agend dle požadavků zákazníka, jejich implementace a následná podpora. S využitím nástrojů Microsoft Visual Studio, technologií Java, C#, ASP.Net a databáze Microsoft SQL Server můžeme připravit SW na míru.
**Bezpečnostní technologie** – Sophos (antiviry a šifrování).
**Kybernetická bezpečnost** – Posudek, Audit, Zavedení systému řízení bezpečnosti informací.
**Úložiště a zálohování** – Acronis (zálohování), Microsoft SC DPM (zálohování), Synology úložiště.
**Sjednocená komunikace** – Microsoft Exchange, Microsoft Lync a hardwarové doplňky (telefony, projektory, videokonferenční zařízení, …).
**DELL** – servery, disková pole, networking, UPS, RACK skříně, PC a NB a Tablety, tiskárny, projektory.
**Síťové prvky** – Sophos UTM, DELL (VPN, FIREWALL, WIFI, bezpečnost, SWITCH), Hewlett-Packard.
**Služby dohledového centra** – monitoring sítí, prvků, serverů a běžících aplikací a následná podpora (Hotline, HelpDesk, Support…).
**Hewlett – Packard** – servery, disková pole, networking, UPS, RACK skříně, PC a NB a Tablety, tiskárny, …
**Virtualizace** – VMware, Microsoft Hyper-V.

Držitel certifikace dle norem ČSN EN ISO 9001:2001 ISO 14001:2005 ISO 27001:2006

# 7. Závěr

V případě požadavku na upřesňující informace k nabídce nás naleznete na níže uvedených telefonních číslech a adresách.

V Praze dne 08.02.2016

Za společnost VISITECH a.s.

VISITECH a.s.
Weilova 2e/1450, 102 05 Praha
DIČ: CZ25543415

Ing. Josef Appel

Obchodní manažer

tel.: +420 274 776 890
mobil: +420 728 257 453
e-mail: josef.appel@visitech.cz