

Smlouva

o dodávce komplexního systému NBA

uzavřená podle § 1746 odst.2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů a zákona č.120/2001 Sb., autorský zákon, ve znění pozdějších předpisů, mezi:

Českou národní bankou

Na Příkopě 28

115 03 Praha 1

zastoupenou: Ing. Vladimírem Mojžíškem, ředitelem sekce informatiky

a

Ing. Zdeňkem Virusem, ředitelem sekce správní

IČO: 48136450

DIČ: CZ48136450

(dále jen „objednatel“ nebo také „ČNB“)

a

Dimension Data Communications Czech s.r.o.

Na Hřebenech II 1718/10

140 00 Praha 4

zastoupenou: Ing. Petrem Hüblem, jednatelem

IČO: 26175738

DIC: CZ26175738

zapsanou v obchodním rejstříku vedeném Městským soudem v Praze oddíl C vložka 77064

(dále jen „poskytovatel“)

Článek I

Předmět smlouvy a místo plnění

1. Poskytovatel se zavazuje dodat, nainstalovat a implementovat v prostředí objednatele technické a programové prostředky (dále též „HW a SW“) Invea FlowMon Collector R5-6000 Pro včetně ADS modulu pro provádění behaviorální analýzy dat a sond FlowMon Probe 4000 (dále jen „NBA systém“ nebo „dílo“). NBA systém musí splňovat požadavky objednatele uvedené v příloze č. 1 prostřednictvím řešení dle specifikace, která tvoří přílohu č.2 smlouvy.
2. Součástí díla je dále dodání dokumentace podle čl. II odst. 1 písm. a) a spoluúčast poskytovatele při akceptačních testech.
3. Poskytovatel se zavazuje nainstalovat v prostředí objednatele nejnovější, stabilní verzi programových prostředků, která bude výrobcem v době plnění uvedena na trh.
5. Předmětem této smlouvy je dále závazek poskytovatele poskytovat objednateli podporu podle článku V, a to ode dne podpisu závěrečného akceptačního protokolu.
6. Místem plnění budou prostory výpočetního střediska v objektu objednatele na adrese: Na Příkopě 28, 115 03 Praha 1 a Strojírenská 175, 155 21 Praha 5.

7. Předmětem této smlouvy je závazek objednatele poskytnout potřebnou součinnost a zaplatit za poskytnutá plnění ceny dle čl. IV.
8. Poskytovatel bere na vědomí, že mu nebude umožněn vzdálený přístup k dodanému zařízení ani k jiným serverům objednatele.

Článek II Průběh, předání a převzetí díla

1. Dílo bude realizováno takto:

a) **IMPLEMENTACE:**

zahrnuje především:

- kompletní dodávku HW a SW, jeho instalaci a konfiguraci v systémovém prostředí ČNB
 - poskytovatel dodá a zajistí montáž a instalaci všech HW komponent do technologických stojanů objednatele
 - poskytovatel zajistí instalaci softwarového vybavení a agentů a dále propojení komponent a konfiguraci NBA systému v prostředí ČNB (zejména napojení na síťové prvky, firewally a systém SIEM)
 - poskytovatel zajistí konfiguraci automatického zálohování systému NBA (konfigurace a dat)
 - poskytovatel zajistí konfiguraci zpracování dat (sesbíraných NetFlow)
 - poskytovatel zajistí v prostředí ČNB konfiguraci ADS modulu provádějícího behaviorální analýzu
 - poskytovatel zajistí konfiguraci zabezpečení celého řešení, včetně nastavení politik přístupů, hesel a pod. pro 10 uživatelů ČNB
- vypracování a předání podrobné technické a provozní dokumentace NBA systému v českém jazyce (předání na médiích CD/DVD/disk ve formátu MS OFFICE 2003 nebo 2010), zahrnující minimálně:
 - funkční schéma řešení včetně jeho popisu
 - schéma zapojení dodaných zařízení včetně jeho popisu
 - popis konfigurace jednotlivých komponent řešení
 - popis bezpečnostních nastavení a jejich konfigurace
 - popis zálohování a archivace
 - postup implementace dodaného systému
 - popis konfigurace FlowMon kolektoru i sond (pro sběr NetFlow dat)
 - popis konfigurace ADS modulu (pro provádění behaviorální analýzy)
 - postupy pravidelné údržby dodaného systému
 - postupy diagnostiky a monitorování provozu dodaného systému
 - postupy řešení havarijních stavů dodaného systému

b) **AKCEPTAČNÍ TESTY:**

- Objednatel provede akceptační testy NBA systému ve lhůtě do deseti pracovních dnů po dokončení implementace. Poskytovatel souhlasí s tím, že akceptační testování bude provádět objednatel.
- provedením funkčních testů NBA systému v prostředí ČNB budou ověřovány:
 - autentizace uživatele do systému NBA

- sběr NetFlow dat z definovaných zdrojů (síťových prvků, sond, případně firewallů)
 - provádění behaviorální analýzy nad sebranými daty
 - odesílání zpracovaných dat do systému SIEM
 - automatické zálohování.
- Objednatel rovněž ověří, zda dodané NBA řešení splňuje veškeré požadavky objednatele uvedené v příloze 1.
 - Akceptační testy jsou ukončeny nahlášením výsledku a předáním seznamu nalezených vad.
 - Po odstranění podstatných vad budou akceptační testy celé opakovány a ověří tak kvalitu předávaného NBA systému nebo jeho části. U ostatních vad se provedou akceptační testy s ohledem na ověření řešení pouze příslušné vady.

Podstatné vady jsou vady, které způsobují tak závažné problémy, že objednatel nemůže produkt nebo jeho klíčovou část používat, ovládat nebo není funkční sběr Net Flow z prvků datové sítě a perimetru uživatele nebo není prováděna (korektně nebo vůbec) behaviorální analýza nebo nejsou zpracovaná data odesílána do systému SIEM.

- Objednatel převezme NBA řešení pouze tehdy, pokud:
 - poskytovatel dodal kompletní NBA systém prostý vad včetně požadované dokumentace,
 - poskytovatel předal v elektronické podobě na sjednaném datovém médiu (např. CD, DVD) veškeré podklady a dokumenty potřebné ke správě a údržbě.
 - Převzetí NBA systému bude uskutečněno podpisem závěrečného akceptačního protokolu. Tím je plnění předáno objednateli k běžnému provoznímu využití.
2. Objednatel umožní poskytovateli vykládku technických prostředků v prostorách objednatele v termínu, o kterém byl poskytovatelem zpraven nejméně tři pracovní dny předem. Objednatel převezme technické prostředky do úschovy a zajistí jejich bezpečné uskladnění do doby zahájení jejich instalace. Při předání a převzetí prostředků do úschovy bude pověřenými osobami obou smluvních stran podepsán dodací list.

Článek III Lhůty plnění

1. Poskytovatel předá objednateli plnění dle článku I odst. 1 a 2 do 2 měsíců od výzvy objednatele k zahájení plnění. Písemná výzva k zahájení plnění bude objednatelem doručena nejpozději do 3 měsíců od podpisu smlouvy na mailovou adresu pověřené osoby poskytovatele.
2. Pověřenými osobami jsou:
 - a) za objednatele:
Petr Puchmeltr, tel. č.: +420 224 412 883, e-mail: petr.puchmeltr@cnb.cz
Luboš Minár, tel. č.: +420 224 412 606, e-mail: lubos.minar@cnb.cz
 - b) za poskytovatele:
Michal Korol, tel. č.: +420 255 770 224, e-mail: michal.korol@dimensiondata.com

3. Smluvní strany se zavazují ohlásit změnu pověřených osob nebo kontaktních údajů podle tohoto článku nejpozději následující pracovní den po provedení změny na e-mailové adresy pověřených osob.

Článek IV

Ceny plnění, množství a platební podmínky

1. Cena za plnění dle článku I odst. 1 a 2 byla stanovena dohodou smluvních stran a činí celkem **989 364 Kč bez DPH**. Bližší specifikace ceny je uvedena v příloze č. 4 (cenová tabulka).
2. Cena za podporu dle čl. V odst. 2 písm. a) až d) je stanovena jako paušální a činí **205 572,40 Kč bez DPH ročně**. V této ceně je zahrnuta podpora dle čl. V odst. 2 písm. d) v rozsahu 2 hodin za měsíc. Nevyčerpané hodiny se převádějí do následujícího měsíce, nejdéle však do posledního měsíce ročního období předplacené podpory.
3. Cena za podporu dle čl. V odst. 2 písm. d) v případě překročení limitu počtu hodin dle odst. 2 tohoto článku bude stanovena jako součin počtu skutečně odpracovaných hodin a hodinové sazby, která činí **1 950 Kč bez DPH**.
4. K cenám uvedeným v odst. 1, 2 a 3 bude účtována DPH v sazbě platné v den uskutečnění zdanitelného plnění. Ceny uvedené v odst. 1, 2 a 3 zahrnují veškeré náklady poskytovatele spojené s plněním podle této smlouvy (včetně nákladů na náhradní díly technických prostředků dodávaných v rámci podpory).
5. Úhrada ceny dle odst. 1 bude provedena na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve v den podpisu závěrečného akceptačního protokolu.
6. Úhrada ceny dle odst. 2 bude prováděna předem na období 12 měsíců, a to na základě dokladu k úhradě, který je poskytovatel oprávněn vystavit nejdříve 14 dnů před začátkem období, na které se platí. Doklad na cenu podpory na první období je poskytovatel oprávněn vystavit nejdříve po podpisu závěrečného akceptačního protokolu.
7. Úhrada ceny dle odst. 3 bude prováděna na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve po poskytnutí podpory (ucelené akce).
8. Doklad k úhradě bude kromě údajů dle § 435 občanského zákoníku obsahovat i evidenční číslo smlouvy objednatele. Daňový doklad bude obsahovat i náležitosti stanovené zákonem o DPH. V případě, že doklad k úhradě bude postrádat některou z těchto náležitostí nebo bude obsahovat chybné údaje, je objednatel oprávněn vrátit vadný doklad poskytovateli. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného daňového dokladu.
9. Doklady bude poskytovatel zasílat elektronicky na adresu faktury@cnb.cz, přičemž doklad musí být vložen jako příloha mailové zprávy ve formátu PDF. V jedné mailové zprávě smí být pouze jeden doklad. Mimo vlastní doklad k úhradě může být přílohou mailové zprávy jedna až tři přílohy k dokladu ve formátech PDF, DOC, DOCX, XLS, XLSX. Nebude-li možné zaslat doklad k úhradě elektronicky, zašle jej poskytovatel na adresu:
Česká národní banka
sekce rozpočtu a účetnictví
odbor centrální účtárna
Na Příkopě 28
115 03 Praha 1

10. Splatnost dokladu je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.
11. Smluvní strany se ve smyslu ustanovení § 1991 občanského zákoníku dohodly, že objednatel je oprávněn započíst jakoukoli svou peněžitou pohledávku za poskytovatelem, ať splatnou či nesplatnou, oproti jakékoli peněžité pohledávce poskytovatele za objednatelem, ať splatné či nesplatné.
12. Ke konci kalendářního roku, nejpozději však do 31.12. je poskytovatel povinen písemně sdělit objednateli, jakou část z uhrazené roční ceny podpory tvoří cena nových verzí představujících technické zhodnocení programových prostředků.

Článek V **Podpora**

1. Poskytovatel ručí za to, že NBA systém bude funkční a schopný použití v prostředí objednatele a bude odpovídat požadavkům objednatele uvedeným v příloze č. 1 a vlastnostem a parametrům deklarovaným v příloze č. 2 a v dokumentaci.
2. Podpora NBA systému (technických a programových prostředků) zahrnuje:
 - a) odstraňování vad technických a programových prostředků na místě,
 - b) poskytování aktualizací programových prostředků (nové verze, opravné verze, bezpečnostní záplaty) a na výzvu objednatele jejich implementace do systému NBA,
 - c) online přístup objednatele k definicím bezpečnostních hrozeb a možnost jejich stažení do zařízení,
 - d) telefonická, e-mailová pomoc (v českém jazyce) a pomoc na místě při identifikaci závad, řešení problémů v oblasti konfigurací, správy a zajištění běžného provozu systému NBA a to jak ze strany poskytovatele, tak v případě potřeby i ze strany výrobce;Veškerá podpora bude prováděna certifikovanými inženýry Flow Mon Technical Specialist.
3. Podpora bude poskytována minimálně v pracovní dny v pracovní době objednatele od 7:45 do 16:15 hod.
4. Odstraňování vad technických prostředků bude poskytovatelem prováděno výměnným způsobem s tím, že náhradní díl nebo zařízení musí být nové a bezvadné, vada musí být odstraněna a celý systém NBA zprovozněn nejpozději do následujícího pracovního dne ode dne ohlášení vady.
5. Aktualizace programových prostředků budou objednateli poskytovány bez zbytečného odkladu, nejpozději však do 14 dnů od uvedení SW výrobcem na trh.
6. Poskytovatel zahájí řešení odstranění vady programových prostředků do následujícího pracovního dne ode dne jejího ohlášení. V případě, že jde o vadu způsobující nefunkčnost systému NBA a nepodaří se systém zprovoznit do následujícího pracovního dne od zahájení řešení, zajistí poskytovatel následující pracovní den dočasné fungování systému například převedením na předchozí funkční verzi operačního systému a aplikačního SW.
7. Potřebu podpory ohlašuje objednatel poskytovateli telefonicky na telefonní číslo poskytovatele 800 100 321 v době od 8 do 17 hodin s následným písemným potvrzením e-mailem na e-mailovou adresu cz_callcenter@dimensiondata.com nebo potřebu podpory

objednatel nahlašuje pouze e-mailem na mailovou adresu poskytovatele uvedenou v tomto odstavci nebo do Incident Management Systému e-Servis na internetové adrese <https://www.e-service-cz.dimensiondata.com> . Oznámení učiněná po uvedené době se považují za oznámená následující pracovní den, v hodině odpovídající začátku uvedené doby.

8. Poskytovatel je povinen potvrdit přijetí oznámení učiněné v pracovní dny v době uvedené v odst.7 do 4 pracovních hodin od doručení. Služby poskytované poskytovatelem musí vyhovovat technickým specifikacím a požadavkům výrobce.

Článek VI

Přechod vlastnictví a nebezpečí škody, licenční ujednání

1. Vlastnické právo k technickým prostředkům dle této smlouvy přechází na objednatele dnem podpisu závěrečného akceptačního protokolu. Programové prostředky poskytnuté podle této smlouvy je objednatel oprávněn užívat od okamžiku instalace/implementace.
2. Poskytovatel poskytuje objednateli nevýhradní, nepřevoditelnou, nedělitelnou, časově a územně neomezenou multilicenci umožňující užívat poskytnuté programové prostředky pouze pro vnitřní potřebu objednatele.
3. Objednatel není povinen licenci využít.
4. Součástí licence je příslušná dokumentace v elektronické podobě.
5. Poskytovatel prohlašuje, že práva, která touto smlouvou poskytuje, mu náleží bez jakéhokoliv omezení, a odpovídá za škodu, která by objednateli vznikla, pokud by toto prohlášení bylo nepravdivé.
6. Licence poskytnuté dle této smlouvy se vztahují i na veškeré poskytnuté aktualizace (tj. update/upgrade/patch/hotfix atd.).

Článek VII

Mlčenlivost, bezpečnostní požadavky objednatele, ochrana osobních údajů

1. Poskytovatel se zavazuje zajistit, že jeho pracovníci, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se u objednatele seznámí, a které nejsou veřejně známy. Povinnost mlčenlivosti není časově omezena.
2. Poskytovatel se zavazuje v plném rozsahu dodržovat bezpečnostní požadavky objednatele, které jsou uvedeny v příloze č. 3 této smlouvy.
3. Dle § 6 zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů (dále jen „ZOOU“), strany sjednaly:
 - 3.1 zpracování veškerých osobních údajů objednatel, který je ve smyslu ZOOU zpracovatelem, probíhá podle ZOOU, zejména je zpracovatel povinen ve smyslu § 7 ZOOU splnit obdobně všechny povinnosti stanovené v § 5 ZOOU pro správce osobních údajů.
 - 3.2 Toto ujednání o zpracování osobních údajů se uzavírá za účelem zajištění evidence osob vstupujících do objektu ČNB a správy přístupového systému ČNB způsobem, v rozsahu a postupem dle smlouvy, jejímž je toto ujednání dle § 6 ZOOU součástí. Rozsah zpracování osobních údajů bude odpovídat účelu zpracování, tedy bude obsahovat identifikační osobní údaje (jméno, příjmení a číslo průkazu totožnosti

zaměstnanců poskytovatele). Zpracování osobních údajů podle tohoto ujednání se sjednává na dobu existence závazkového vztahu vzniklého ze smlouvy, jejíž součástí je toto ujednání, nejpozději do likvidace posledního osobního údaje zpracovatelem ve smyslu povinnosti zlikvidovat osobní údaje podle ZOOU.

3.3 Objednatel poskytuje poskytovateli následující záruky technického a organizačního zabezpečení ochrany osobních údajů:

- veškeré materiály s osobními údaji jsou zajištěny v uzamykatelném nábytku v uzamčených prostorách v sídle objednatele,
- všechny osobní údaje jsou následně zpracovávány na PC, která jsou zabezpečena heslem, a jsou přístupné pouze vybraným zaměstnancům objednatele,
- organizace a povinnosti zaměstnanců objednatele ohledně ochrany osobních údajů, jsou stanoveny ve vnitřním předpisu objednatele.

Článek VIII Uveřejnění smlouvy

1. Poskytovatel si je vědom zákonné povinnosti objednatele uveřejnit na svém profilu tuto smlouvu (celé znění) včetně všech jejích případných změn a dodatků.
2. Profilem objednatele je elektronický nástroj, prostřednictvím kterého objednatel, jako veřejný zadavatel dle zákona č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů (dále jen „ZVZ“) uveřejňuje informace a dokumenty ke svým veřejným zakázkám způsobem, který umožňuje neomezený a přímý dálkový přístup, přičemž profilem objednatele v době uzavření této smlouvy je <https://ezak.cnb.cz/>.
3. Povinnost uveřejnění této smlouvy včetně jejích změn a dodatků je objednateli uložena § 147a ZVZ.
4. Uveřejnění bude provedeno dle ZVZ a příslušného prováděcího předpisu.

Článek IX Smluvní pokuty, úrok z prodlení

1. V případě, že poskytovatel nedodrží závaznou lhůtu pro předání plnění dle čl. III odst. 1, uhradí objednateli smluvní pokutu ve výši 1 000 Kč za každý den prodlení.
2. V případě, že se v průběhu plnění podle článku II prokáže, že nebyl poskytovatelem splněn jakýkoliv požadavek objednatele uvedený v příloze č. 1, má objednatel právo požadovat smluvní pokutu ve výši 1 000 Kč za každý případ nedodržení požadavku.
3. V případě prodlení poskytovatele ve lhůtě podle článku V odst. 4 je objednatel oprávněn požadovat smluvní pokutu ve výši 3 000 Kč za každý pracovní den prodlení.
4. V případě prodlení poskytovatele ve lhůtě pro zajištění dočasného fungování systému dle čl. V odst. 6 je objednatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
5. V případě prodlení poskytovatele ve lhůtě pro potvrzení ohlášení podle čl. V odst. 8 je objednatel oprávněn požadovat smluvní pokutu ve výši 100 Kč za každou pracovní hodinu prodlení.

6. V případě prodlení objednatele s úhradou daňového dokladu má poskytovatel právo požadovat úrok z prodlení podle nařízení vlády č. 351/2013 Sb.
7. Smluvní pokuta a úrok z prodlení jsou splatné do 14 dnů ode dne doručení platebního dokladu povinné smluvní straně. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu oprávněného.
8. Ujednáním o smluvní pokutě není dotčeno právo na náhradu škody ve výši, v jaké převyšuje smluvní pokutu.

Článek X

Doba trvání smlouvy, výpověď, odstoupení od smlouvy

1. Smlouva se v části poskytování podpory uzavírá na dobu neurčitou.
2. Smlouvu lze v části podpory ukončit písemnou výpovědí bez uvedení důvodu, která musí být doručena druhé smluvní straně nejpozději 3 měsíce přede dnem uplynutím předplacené doby podpory. Závazek poskytování podpory zaniká uplynutím posledního dne předplacené doby podpory.
3. Smluvní strany se dohodly, že objednatel je oprávněn kdykoliv v průběhu insolvenčního řízení zahájeného na majetek poskytovatele vypovědět tuto smlouvu v části týkající se poskytování podpory, a to ve 14 denní výpovědní lhůtě, která počíná běžet dnem následujícím po doručení písemné výpovědi poskytovateli.
4. V případě, že účinnost smlouvy skončí před uplynutím předplacené doby podpory, vrátí poskytovatel objednateli alikvotní část předplacené ceny podpory.
5. Poruší-li kterákoliv strana podstatným způsobem závazky vyplývající z této smlouvy, má druhá strana právo odstoupit od smlouvy, a to písemným oznámením o odstoupení. Odstoupení je účinné dnem doručení oznámení o odstoupení druhé smluvní straně. V případě podstatného porušení smlouvy poskytovatelem může objednatel odstoupit od smlouvy do 30 dnů ode dne porušení.
6. Za podstatné porušení smlouvy strany považují zejména tyto případy:
 - a) objednatel neuhradí poskytovateli cenu ve lhůtě 30 dnů po dni její splatnosti ani po písemném oznámení poskytovatele,
 - b) NBA systém, nebo některá jeho komponenta, nebude splňovat veškeré požadavky dle této smlouvy,
 - c) systém není způsobilý pracovat v rámci systémového prostředí ČNB - např. není plně kompatibilní s prvky datové sítě a prvky perimetru uživatele (zejména síťovými prvky a firewally) nebo systémem SIEM nebo jednotlivé komponenty NBA systému nejsou kompatibilní navzájem.
 - d) poskytovatel bude v prodlení s předáním plnění delším než 30 dnů.
7. V případě odstoupení od smlouvy objednatelem se poskytovatel zavazuje zajistit na své náklady odvoz technických a programových prostředků, a to nejpozději do 30 dnů ode dne doručení oznámení o odstoupení od smlouvy.

Článek XI

Ostatní ujednání

1. Poskytovatel je povinen mít po dobu účinnosti této smlouvy uzavřeno pojištění pro případ vzniku odpovědnosti za škodu způsobenou v souvislosti s plněním této smlouvy, a

to s pojistným plněním ve výši nejméně 10 000 000 Kč (slovy: deset milionů korun českých) a jeho spoluúčast nepřevyšuje 5 %.

2. Poskytovatel se zavazuje, že pojištění v uvedené výši a rozsahu zůstane účinné po celou dobu účinnosti této smlouvy, a do 5 pracovních dnů od výzvy objednatele je poskytovatel povinen toto objednateli prokázat.
3. Použije-li poskytovatel při své činnosti subdodavatele, nahradí škodu jím způsobenou, jakoby ji způsobil sám.
4. Poskytovatel je povinen:
 - 4.1 poskytovat plnění v objektech a prostorách vymezených objednatelem, a to pouze pracovníky schválenými objednatelem,
 - 4.2 mít po celou dobu účinnosti této smlouvy platnou autorizaci certifikovaného partnera společnosti Invea-Tech s úrovní certifikace minimálně „Silver Partner“ a disponovat minimálně dvěma, vzájemně zastupitelnými certifikovanými inženýry FlowMon technical specialist, kteří se budou podílet na plnění této smlouvy. Poskytovatel je povinen kdykoliv po dobu účinnosti této smlouvy na požádání objednatele výše uvedené skutečnosti doložit, a to do 5 pracovních dnů ode dne doručení požadavku objednatele.

Objednatel si vyhrazuje právo ověřit si skutečnosti dle odst. 4.2 . Nesplnění kteréhokoliv požadavku objednatele uvedeného odst. 4.2 je považováno za podstatné porušení smlouvy.

Článek XII Závěrečná ustanovení

1. Smlouva nabývá platnosti a účinnosti dnem podpisu oprávněnými zástupci obou smluvních stran.
2. Smlouva může být měněna a doplňována pouze formou písemných vzestupně číslovaných dodatků podepsaných oprávněnými zástupci obou smluvních stran. Za písemnou formu nebude pro účel uvedený v tomto odstavci považována výměna e-mailových či jiných elektronických zpráv. Výjimkami jsou změny pověřených osob nebo jejich kontaktních údajů dle čl.III odst. 3.
3. Práva a povinnosti vzniklé z této smlouvy mohou být postoupena pouze po předchozím písemném souhlasu druhé smluvní strany. Za písemnou formu se nepovažuje e-mail či jiné elektronické zprávy.
4. Odpověď strany této smlouvy podle § 1740 odst.3 občanského zákoníku s dodatkem nebo odchylkou není přijetím nabídky, ani když podstatně nemění podmínky nabídky.
5. Uplatnění domněnky doby dojití dle § 573 občanského zákoníku se vylučuje.
6. Tato smlouva je sepsána v českém jazyce. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém jazyce, nebude-li smluvními stranami v konkrétním případě dohodnuto jinak
7. Smluvní strany se dohodly, že případný spor, který vznikne z této smlouvy nebo v souvislosti s ní bude rozhodován výlučně podle českého práva obecnými soudy v České republice.
8. Smlouva je vyhotovena ve třech vyhotoveních s platností originálu, z nichž objednatel obdrží dvě a poskytovatel jedno vyhotovení.

- Přílohy:** č. 1 – Technické požadavky objednatele
č. 2 - Technická specifikace NBA systému
č. 3 - Bezpečnostní požadavky objednatele
č. 4 - Cenová tabulka

V Praze dne: 14. 9. 2014

V Praze dne: 24. 9. 2014

Za objednatele:

[Redacted signature]

Ing. Vladimír Mojžíšek
ředitel sekce informatiky

[Redacted address]

Ing. Zdeněk Virius
ředitel sekce správní

[Redacted address]

Za poskytovatele:

[Redacted signature]

Ing. Petr Hübl
jednatel

[Redacted address]

ČESKÁ NÁRODNÍ BANKA
Na Příkopě 28, 115 03 Praha 1

TECHNICKÉ POŽADAVKY OBJEDNATELE

Požadavky na sondy:

Je nezbytné, aby zdroje NetFlow dat byly nezávislé na použité síťové infrastruktuře a svou funkcí nijak neovlivňovaly sledovanou síť. Ze strany monitorovacích rozhraní připojených do sledované sítě nesmí být zařízení detekovatelné. Vytváření síťových statistik musí být prováděno autonomními, nezávislými a k tomuto účelu navrženými zařízeními.

Požadavky na technické a programové vybavení sondy

- 100% přesný nezávislý autonomní zdroj NetFlow statistik s podporou IPv4, IPv6, VLAN, MPLS, GRE, NetFlow v9, IPFIX
- detekce aplikací dle standardu NBAR2, monitorování a analýza HTTP provozu a VoIP statistik,
- instalace do stávající síťové infrastruktury ČNB,
- rack mount zařízení,
- pasivní zapojení bez vlivu na monitorovanou síť (zapojení pomocí TAPů, 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 500 tisíc paketů za sekundu na každém portu, možnost upgradu na verzi s wire-speed garancí,
- 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).

Požadavky na sondy z hlediska monitorovacích rozhraní:

- současné měření síťového provozu na minimálně čtyřech gigabitových rozhraních současně pomocí jednoho zařízení,
- celkem požadováno 8 monitorovacích portů 1Gb Ethernet (v každé lokalitě bude umístěno jedno, minimálně čtyřportové zařízení)

Požadavky na Kolektor včetně modulu behaviorální analýzy:

Požadavky na technické a programové vybavení kolektoru

- zabezpečený kolektor NetFlow statistik s databází pro plné uložení síťových statistik na multigigabitových linkách bez jakékoliv redukce,
- dohledání každé komunikace, průběžné grafy, podpora upozornění, rozšiřitelnost o pluginy na míru,
- instalace do stávající síťové infrastruktury – racková montáž (hloubka racku 80cm),
- jeden administrativní port RJ45 Ethernet 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,
- podpora autentizace vůči LDAP (Active Directory),
- HOT SWAP disky, RAID včetně SMART detekce,
- integrace dohledového systému pro kontrolu dostupnosti (SNMP),
- časová synchronizace zařízení proti centrálnímu zdroji času na síti,
- jednoduchá instalace a nastavení zařízení prostřednictvím příkazové řádky,
- přístup a konfigurace zařízení prostřednictvím sériové linky (RS-232),
- použití DNS cache na zařízení pro rychlejší překlad IP adres na doménová jména,
- autentizace administrátorů (uživatelů) při přístupu do systému minimálně jménem a heslem, optimálně prostřednictvím certifikátu.

Požadavky na kolektor z pohledu sběru dat

- podpora verze NetFlow protokolu – programové vybavení kolektoru musí umožnit sběr a vyhodnocení NetFlow dat ve verzi 9, IPFIX,
- podpora standardů NBAR2, monitorování MAC adres, HTTP hostname a URL, VoIP SIP,
- datová bezpečnost - ukládání dat na RAID pole (Redundant Array of Independent Disks – vícenásobné diskové pole nezávislých disků). V případě výpadku jednoho disku je systém stále v praceschopném stavu a nedojde ke ztrátě uložených NetFlow dat. Poškozený disk lze za běhu systému vyměnit,
- kapacita datového úložiště – systém musí být schopen sbírat a ukládat dlouhodobě data z desítek NetFlow zdrojů. Disková kapacita datového úložiště musí umožnit záznamy statistik bez jakékoliv redukce v horizontu minimálně 6 měsíců, což odpovídá cca 8000 Flows/s v9,
- přeposílání přijímaných NetFlow statistik ke zpracování na další kolektory včetně filtrace na úrovni NetFlow paketů.

Požadavky na kolektor 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),
- 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.) prostřednictvím 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 možností filtrování a agregace,
- drill-down – možnost dohledat každý jednotlivý tok zaznamenaný sondami,
- podpora geolokace na základě IP adresy,
- otevřené rozhraní s možnostmi skriptování a zpracování dávkových úloh.

Požadavky na kolektor z pohledu exportu dat do systému SIEM:

- předávání zpracovaných dat prostřednictvím Syslogu do systému SIEM.

Automatické vyhodnocování NetFlow dat

System musí umožňovat automatické vyhodnocování sesbíraných dat s cílem identifikovat provozní a bezpečnostní incidenty a tyto reportovat/alertovat jako události. Musí být založen na pokročilých metodách tzv. behaviorální analýzy a musí tak umožňovat odhalovat hrozby a incidenty, pro které dosud není dostupná signatura.

Definice NBA (Network Behavior Analysis)

Analýza chování sítě (NBA) a detekce nežádoucích vzorů chování na síti slouží k odhalování útoků proti sítím a systémům za použití inteligentní analýzy statistik síťového provozu (např.

Cisco standard NetFlow). Princip detekce incidentů v síti není založen na signaturách, ale na vyhodnocování chování sítě a zařízení do ní připojených. NBA systémy jsou proto schopny detekovat zero-day útoky, polymorfní malware a další pokročilé hrozby, které dokáží obejít běžné bezpečnostní systémy (IDS, IPS, firewall, aplikační proxy) a poté dlouhodobě a nepozorovaně působit v interní síti organizace.

Požadavky funkce poskytované řešením automatické analýzy NetFlow dat

- Výkon nejméně 10000 toků/s, podpora pro samplování na úrovni toků (použité max 1:4), tedy minimálně 2500 Flows/s bez samplování.
- Předdefinovaná sada pravidel a algoritmů pro odhalování nežádoucích vzorů chování, zejména:
 - útoky na síťové služby s cílem získat neoprávněný přístup k zařízení nebo službě,
 - komunikaci s potenciálně nežádoucími IP adresami, mezi které patří stanice šířící malware, botnet comman & control centra, známí útočníci nebo systémy šířící nevyžádanou poštu,
 - anomálie DNS provozu indikující infikované stanice, nežádoucí software nebo chybné konfigurace,
 - anomálie DHCP provozu indikující stanice pokoušející se o odposlech síťové komunikace nebo chybné konfigurace,
 - skenování portů a další projevy infikovaných stanic nebo nežádoucího software,
 - potenciálně nežádoucí síťové aplikace jako jsou P2P síť nebo on-line komunikátory,
 - anonymizační služby jako např. TOR (The Onion Router) s cílem obcházet bezpečnostní opatření a přistupovat na zablokované webové stránky, obcházení PROXY serveru,
 - výpadky síťových služeb a špatné konfigurace síťových služeb, pohyb dat z interní sítě do internetu, tj. potenciální únik dat a využívání služeb pro výměnu dat na internetu (webová úložiště apod.),
 - útoky na internetovou telefonii, ústředny a přístroje připojené do IP sítě,
 - nestandardní poštovní komunikace a šíření nevyžádané pošty, DDoS útoky a zneužívání zranitelné servery a síťové služby pro DDoS útoky.
- 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 událostí na základě IP adresních rozsahů, typů a míst v síti.
- 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.

Požadavky na instalaci:

- Instalace do datové struktury uživatele (ve dvou lokalitách)
- Konfigurace pohledů a reportů na primární NetFlow statistiky na základě s'ových segmentů a klíčových aplikací, zadavatel dodá podklady pro konfiguraci v podobě IP adresního plánu.
- Konfigurace detekce anomálií na základě IP adresního plánu zadavatele, vyloučení planých poplachů (tzv. false positives).
- Konfigurace pravidel pro stanovení priorit událostí na základě zkušeností dodavatele se zohledněním IP adresního plánu zadavatele.
- Konfigurace exportu událostí prostřednictvím syslogu do SIEM systému.
- Provedení zálohy konfigurace a předání této zálohy ve vhodné podobě.

Technická specifikace NBA systému

Řešení FlowMon

FlowMon je kompletní řešení pro monitorování a bezpečnost počítačových sítí na základě IP toků (technologie NetFlow a IPFIX). Řešení poskytuje nástroje pro sledování provozu a zabezpečení sítě, řešení problémů v síti, správu a optimalizaci síťového provozu a další.

Řešení FlowMon zahrnuje výkonné autonomní FlowMon sondy generující statistiky o síťovém provozu, FlowMon kolektory pro uložení, zobrazení a analýzu těchto statistik a systém FlowMon ADS pro automatickou analýzu provozu a identifikaci bezpečnostních a provozních incidentů.

Díky využití průmyslových standardů NetFlow a IPFIX je systém jednoduše rozšiřitelný, dobře škálovatelný a kompatibilní s produkty třetích stran.

FlowMon sonda

FlowMon sonda je výkonné autonomní zařízení, které monitoruje provoz na počítačové síti, vytváří statistiky o tomto provozu v podobě IP toků a zasílá (exportuje) tyto statistiky k uložení a další analýze na FlowMon kolektor.

Sonda FlowMon Probe 4000 CU je 1U zařízení, které obsahuje 4 monitorovací porty (rozhraní 4x 10/100/1000 Ethernet Měď RJ-45, CAT5e) pro monitorování síťového provozu. Výkon na každý monitorovací port je 500tisíc paketů za sekundu. Rozměry zařízení jsou 4,24x43,4x39,4 cm.

IP toky vytvořené FlowMon sondami obsahují informace o tom, kdo komunikoval, s kým, jak dlouho, jakým protokolem, kolik přenesl dat a řadu dalších informací ze záhlaví paketů (TCP příznaky, ToS, AS). FlowMon sonda podporuje export dat ve fixním formátu NetFlow verze 5 či flexibilních formátech NetFlow verze 9 a IPFIX, u kterých je možné přímo zvolit, jaké informace se mají monitorovat a exportovat. FlowMon sondy umožňují monitorovat i položky vyšších vrstev (L5-L7) jako jsou HTTP informace (URL, hostname), VoIP statistiky (latence, jitter, ztráty paketů) či přímo provádět detekci aplikací (podpora NBAR2 standardu).

FlowMon kolektor

FlowMon kolektor je zařízení určené pro dlouhodobé ukládání, zobrazení a analýzu síťových toků ve formátech NetFlow/IPFIX/sFlow a dalších. FlowMon kolektor umožňuje uživatelům přesně, rychle a efektivně řešit problémy v síti, zvýšit její bezpečnost díky detekci vnitřních i vnějších útoků, předcházet incidentům, optimalizovat síť a snížit provozní náklady

Kolektor FlowMon Collector R5-6000 Pro je 1U zařízení s HW RAID5 a kapacitou 6TB (4x SATA Hot Swap HDD) pro ukládání a analýzu přijímaných dat. Zařízení obsahuje redundantní napájení a modul pro vzdálenou správu. Výkon zařízení činí až 150tisíc toků za sekundu. Rozměry kolektoru jsou 4,3x43,4x64,2 cm.

FlowMon kolektor přináší kompletní přehled o dění v síti ve formě dlouhodobých grafů s možností volby perspektivy, Top N statistik o uživatelích, službách a komunikacích, uživatelsky definovatelných profilech, možnosti zobrazení dat až na úrovni jednotlivých komunikací a mnoho dalšího. Poskytuje tak plnou sadu funkcí pro monitorování a reportování o síťovém provozu včetně upozorňování v případě definované události. Funkčnost FlowMon

kolektoru je dále možné rozšířit o systém FlowMon ADS (technologie NBA/NBAD) pro automatickou detekci bezpečnostních a provozních incidentů.

FlowMon ADS

FlowMon ADS je moderní systém detekce anomálií a nežádoucího chování v datové síti, založený na permanentním vyhodnocování statistik o provozu na síti. Cílem řešení je odhalení provozních problémů a zvýšení vnější i vnitřní bezpečnosti datové sítě. Hlavní výhodou proti běžným IDS systémům či SNMP monitoringu je orientace na celkové chování zařízení na síti, což umožňuje reagovat na dosud neznámé nebo specifické hrozby.

Hlavní přínosy

- Získání detailního přehledu o struktuře provozu na datové síti a top uživatelů
- Kontrola dodržování bezpečnostních směrnic a předpisů
- Odhalování vnitřních i vnějších útoků na síť
- Monitoring kvality služeb
- Eliminace nežádoucích aplikací
- Odhalování infikovaných zařízení v síti
- Prevence používání nežádoucího software a sdílení nelegálního obsahu
- Kontrola nad odchozím provozem sítě, ochrana dobrého jména
- Rychlá diagnostika zpoždění sítě, služeb a aplikací
- Odhalování špatných konfigurací sítě a síťových zařízení

Hlavní funkce

- Předdefinovaná sada pravidel pro odhalování nežádoucích vzorů chování
- Předdefinovaná sada pravidel pro odhalování obecných anomálií v síti
- Budování dlouhodobých profilů chování zařízení na síti z pohledu služeb, objemů provozu a komunikačních partnerů
- Přehledný dashboard s okamžitou indikací problémů a top statistik
- Interaktivní vizualizace událostí
- Integrace informací ze služeb DNS, WHOIS, geolokační služby
- Komplexní filtrování a prioritizování událostí s vazbou na reporting a alerty

Zapojení v prostředí ČNB

V prostředí ČNB bude sběr primárních dat prováděn dvěma různými způsoby :

- Netflow z perimetru banky a datová komunikace ve vnitřní síti budou zasílány z centrálních síťových prvků Cisco a firewallů Check Point přímo do FlowMon kolektoru
- Provoz sítě wi-fi bude zrcadlen do FlowMon sond, kde bude primárně vyhodnocen a následně bude generováno Netflow a přeposíláno do FlowMon kolektoru.

Takto shromážděná data budou v FlowMon kolektoru zpracována pomocí technologie Network Behavior Analysis, která vyhodnotí, jestli nedochází k nežádoucí komunikaci v rámci datového toku banky. Takto zpracované informace budou následně předávány do systému SIEM k dalšímu vyhodnocení.

Bezpečnostní požadavky objednatele

1. Poskytovatel odpovídá za to, že do objektů objednatele (dále jen „ČNB“) budou vstupovat nebo vjíždět pouze jeho pracovníci, kteří jsou jmenovitě uvedeni v písemném seznamu, schváleném ČNB (dále jen „seznam“). Tato povinnost se vztahuje i na posádky vozidel poskytovatele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Seznam poskytovatel předloží ČNB nejpozději v den podpisu smlouvy.
2. Seznam bude obsahovat tyto položky: jméno, příjmení a číslo průkazu totožnosti pracovníků poskytovatele. Součástí seznamu je „Prohlášení o získání souhlasu subjektů osobních údajů se zpracováním osobních údajů v ČNB ve smyslu zákona č.101/2000 Sb., o ochraně osobních údajů“. Poskytovatel v něm prohlásí a nese odpovědnost za to, že jeho pracovníci uvedení v seznamu vydali souhlas se zpracováním osobních údajů Českou národní bankou v rozsahu: jméno, příjmení a číslo průkazu totožnosti. Důvodem předání těchto osobních údajů je zajištění evidence osob vstupujících do objektu ČNB a správy přístupového systému ČNB.
3. Požadavky na případné doplňky a změny schváleného seznamu pracovníků poskytovatele je nutno neprodleně oznámit ČNB. Případné doplňky a změny podléhají schválení ČNB. Osoby neschválené ČNB nemohou vstupovat do objektů ČNB, přičemž ČNB si vyhrazuje právo neuvádět důvody jejich neschválení.
4. Při příchodu do objektů ČNB pracovníci poskytovatele sdělí důvod vstupu, prokáží se osobním dokladem a podrobí se bezpečnostní kontrole. Osoby, které nejsou uvedeny na seznamu, nebudou do objektu ČNB vpušteny.
5. Schválení pracovníci poskytovatele musí dbát pokynů bankovních policistů, které se týkají režimu vstupu, pohybu a vjezdu do objektu ČNB. Pracovníci poskytovatele budou do prostorů ČNB vstupovat a v těchto prostorách se pohybovat v režimu návštěv, to znamená vždy pouze v doprovodu zaměstnance ČNB nebo zaměstnance referátu bankovní policie ČNB.
6. V případě mimořádné události se pracovníci poskytovatele musí řídit pokyny bankovních policistů nebo dozorujícím zaměstnancem ČNB a dále instrukcemi vyhlášenými vnitřním rozhlasem.
7. Pracovníci poskytovatele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny apod. O tom co je a není nebezpečný předmět, rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.
8. ČNB si vyhrazuje právo nepustit do objektů ČNB pracovníka poskytovatele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.
9. Bez písemného povolení ČNB je zakázáno fotografování a pořizování videozáznamů z interiéru objektů ČNB.
10. Ve všech prostorech objektů ČNB je přísný zákaz kouření a používání otevřeného ohně. O povolení práce se zvýšeným požárním nebezpečím požádá poskytovatel písemnou formou vždy nejpozději jeden pracovní den před zahájením prací, dozorujícího zaměstnance ČNB. Dále se pracovníci poskytovatele musí zdržet poškozování či zcizení majetku ČNB, a dále zdržet se nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.
11. Pracovníci poskytovatele uvedení na seznamu se musí před započítím výkonu práce v objektech ČNB prokazatelně seznámit, ve smyslu předpisů o požární ochraně, bezpečnosti a hygieně práce, se specifickými danými objekty ČNB (např. způsob vyhlášení požárního poplachu, určení ohlašovny požáru, seznámení s únikovými cestami, poplachovými směrnici, evakuačním plánem, umístěním věcných prostředků požární

ochrany apod.). ČNB je oprávněna kdykoliv podrobit kontrole kterékoli pracovníka poskytovatele uvedeného na seznamu z dodržování těchto předpisů a ustanovení.

CENOVÁ TABULKA			
Dodávka NBA systému FlowMon			
Komponenta	Název komponenty	Počet ks	Jednotková cena v Kč bez DPH
Dodávka technických a programových prostředků NBA			
IFP-4000-CU	Invea FlowMon Probe 4000	2	126 891,00
IFC-R5-6000PRO	Invea FlowMon Collector R5-6000 Pro	1	269 991,00
Dodávka programových prostředků NBA			
FPC-ADS-B	Invea FlowMon ADS Business	1	449 991,00
Instalace a Implementace NBA v prostředí ČNB		1	15 600,00
			Cena v Kč za 1 rok bez DPH
Podpora NBA			205 572,40
			Cena za 1 hodinu v Kč bez DPH
Přímá pomoc a konzultace na místě v sídle objednatele			1 950,00
			0,00