Smlouva
o dodávce komplexního zabezpečení systému elektronické pošty proti malware včetně poskytování podpory

uzavřená podle § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, mezi:

Českou národní bankou
Na Příkopě 28
115 03 Praha 1
zastoupenou: Ing. Vladimírem Mojžíškem, ředitelem sekce informatiky
a
Ing. Zdeňkem Viriusem, ředitelem sekce správní
IČO: 48136450
DIČ: CZ48136450

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

a

AutoCont CZ a.s.
zapsanou v obchodním rejstříku vedeném u Krajského soudu v Ostravě, oddíl B, vložka 814
Hornopolní 3322/34
Moravská Ostrava
702 00 Ostrava
zastoupenou: Ing. Petrem Suntychem, členem představenstva
IČO: 47676795
DIČ: CZ47676795

(dále jen „poskytovatel")

Článek I
Předmět smlouvy a místo plnění

1. Poskytovatel se zavazuje dodat, nainstalovat a implementovat produkt, kterým je výhradně softwarové řešení pro zajištění komplexního zabezpečení systému elektronické pošty proti malware, včetně rozhraní pro jeho správu v prostředí ČNB, jehož bližší technická specifikace je uvedena v příloze č. 1 této smlouvy (dále jen" SW řešení"). SW řešení a příslušné aktualizace musí splňovat veškeré požadavky objednatele uvedené v příloze č. 2 této smlouvy.
2. Součástí plnění je dále zaškolení zaměstnanců objednatele, poskytnutí spoluúčasti poskytovatele při akceptačních testech a dodání dokumentace podle čl. II odst. 1 písm. b) této smlouvy.
3. Poskytovatel se zavazuje odinstalovat stávající program MS Forefront ze serverů Exchange, a to bez ztráty uložených dat.
4. Poskytovatel se zavazuje v rámci plnění podle této smlouvy nainstalovat takovou produkční verzi programových prostředků, která bude jejich výrobcem v době plnění podporována.

[redacted]

5. Předmětem této smlouvy je dále závazek poskytovatele poskytovat na žádost objednatele po dobu účinnosti této smlouvy pomoc při odstraňování malware ze systému elektronické pošty, jehož specifikace je uvedena v preambuli přílohy č. 2 této smlouvy.

6. Dále se poskytovatel zavazuje k podpoře provozu spočívající v odstraňování vad a poskytování aktualizací SW a pravidelné aktualizaci definic malwaru. Aktualizací SW je míněna jakákoliv aktualizace vyvolaná aktualizací SW prostředí (aplikační server, DB atd.), nebo vlastním rozvojem dodávaného systému.

7. Místem plnění budou prostory výpočetního střediska v objektu objednatele na adrese: Na Příkopě 28, 115 03 Praha 1.

Článek II
Průběh plnění

1. Plnění podle čl. I odst. 1, 2 a 3 této smlouvy bude realizováno ve třech etapách takto:

   a) První etapa – **ANALÝZA a vypracování implementačního postupu**:

   - poskytovatel se zavazuje na základě jím zpracované analýzy systémového prostředí ČNB vypracovat implementační postup,
   - **implementační postup** bude obsahovat:
     - popis nasazení SW řešení do prostředí objednatele včetně jeho konfigurace a popisu případných změn stávajících komponent systémového prostředí objednatele,
     - harmonogram implementace SW řešení,
     - nároky na součinnost objednatele.

   b) Druhá etapa – **IMPLEMENTACE** zahrnuje především:

   - odinstalaci původního řešení MS Forefront,
   - kompletní dodávku, instalaci a nastavení SW řešení v systémovém prostředí ČNB,
   - provedení funkčních testů SW řešení v prostředí ČNB,
   - vypracování a předání dokumentace SW řešení v českém jazyce:
     - administrátorská dokumentace (skutečný stav zapojení, nastavení systému, postupy při provozu, nastavení omezení přístupu),
     - instalační dokumentace (podrobný instalační postup),
     - havarijní plán (postupy v případě závady, umístění nezbytných záznamů a konfiguračních souborů a jejich analýza).
   - zajištění zaškolení v rozsahu stanoveném objednatelem spočívajícího zejména v:
     - používání a konfigurování managementu,
     - ovládání a nastavování vlastního produktu,
     - monitorování a logování,
     - aplikaci upgradů a updatů.
   - předání médií (CD, DVD, flash-disk), na kterých je uložena instalace SW řešení a veškerá dokumentace v jednom z formátů MS Office 2010 a vyšší, PDF.

   c) Třetí etapa – **AKCEPTAČNÍ TESTY**:

- objednatel provede akceptační testy SW řešení jako celku ve lhůtě nejpozději do tří týdnů od dokončení druhé etapy. Poskytovatel souhlasí s tím, že akceptační testy provede objednatel,
- objednavatel rovněž ověří, zda dodané SW řešení splňuje požadavky uvedené v příloze 2,
- součástí akceptačních testů je i otestování detekce malware prostřednictvím testovacího řetězec EICAR,
- 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 SW řešení nebo jeho části. U ostatních vad se provedou akceptační testy s ohledem na ověření řešení pouze příslušné vady.

Článek III
Lhůty plnění

1. Poskytovatel předá plnění dle článku I odst. 1, 2 a 3 této smlouvy nejpozději **do 15 týdnů** po podpisu smlouvy.
2. Poskytovatel se zavazuje dokončit a uzavřít jednotlivé etapy v následujících lhůtách:
   1. etapu – nejpozději do 5 týdnů po podpisu smlouvy,
   2. etapu – nejpozději do 10 týdnů po podpisu smlouvy,
   3. etapu – nejpozději do 15 týdnů po podpisu smlouvy.
3. Lhůty uvedené v odstavci 2 tohoto článku mohou být na základě dohody objednatele a poskytovatele prodlouženy formou dodatku k této smlouvě. V dodatku bude rovněž uvedeno, zda a o jakou dobu se prodloužením lhůty pro danou etapu prodlužuje lhůta pro celé plnění stanovená v odst. 1 tohoto článku. Lhůta pro celé plnění ale může být prodloužena pouze tak, aby bylo předáno nejpozději 31. 12. 2015.
4. Pověřenými osobami jsou:

   a) za objednatele:

   p. Martin Podstata, tel.: 224 412 628, e-mail: martin.podstata@cnb.cz,

   p. Petr Schlegr, tel.: 224 413 698, e-mail: petr.schlegr@cnb.cz,

   b) za poskytovatele:

   p. Lenka Kadeřábková, tel..: 724 100 930, e-mail: lenka.kaderabkova@autocont.cz,

   p. Michal Suchý, tel.: 606 733 729, e-mail: michal.suchy@autocont.cz.
5. Smluvní strany se zavazují ohlástit změnu pověřených osob nebo kontaktních údajů podle tohoto článku nebo podle článku VI odst. 5 této smlouvy nejpozději následující pracovní den po provedení změny na e-mailové adresy pověřených osob.

Článek IV
Převzetí plnění

1. Po ukončení první a druhé etapy předloží poskytovatel výsledek jím provedených prací k posouzení objednateli v akceptačním řízení. O výsledku akceptačního řízení bude sepsán

akceptační protokol zhotovený objednatelem, který podepíše vždy alespoň jedna pověřená osoba za objednatele a poskytovatele.

2. Každá etapa bude považována za ukončenou pouze tehdy, pokud bude plnění prosté vad, nerozhodne-li se objednatel přijmout plnění s výhradami. V takovém případě budou jednotlivé výhrady zaznamenány v akceptačním protokolu a zhotovitel je oprávněn pokračovat v navazující etapě. Pokud objednatel přijme plnění s výhradami, musí být vady odstraněny ve lhůtách uvedených v akceptačním protokolu.
3. Akceptaci s výhradami nelze provést, pokud se vystytne alespoň 1 podstatná vada. Podstatné vady jsou vady, které způsobují nemožnost objednatele produkt nebo jeho klíčovou část používat, ovládat, konfigurovat nebo není zajištěna ochrana proti malware v systému elektronické pošty v souladu s dokumentací. Podstatnou vadou v případě implementačního postupu a dokumentace jsou chybějící textové části dokumentace nebo případ, kdy textová část neodpovídá skutečnosti, případně není splněn kterýkoliv z povinných požadavků uvedených v příloze č. 2 této smlouvy.
4. K akceptačnímu protokolu vyhotovenému objednatelem vyjádří poskytovatel své stanovisko vždy nejpozději do 5 pracovních dnů po jeho jeho převzetí. Pokud se poskytovatel k akceptačnímu protokolu nevyjádří, má se za to, že s uvedeným závěrem souhlasí.
5. Objednatel převezme plnění jako celek pouze tehdy, pokud:
   - byly akceptovány všechny dílčí etapy a případné vady byly odstraněny,
   - poskytovatel dodal kompletní SW řešení prosté vad včetně požadované dokumentace,
   - poskytovatel poskytl veškeré potřebné licence pro provoz SW řešení,
   - poskytovatel předal v elektronické podobě na sjednaném datovém médiu (např. CD, DVD) veškeré podklady a dokumenty potřebné ke správě, údržbě.
6. Převzetí celého plnění za účelem běžného provozního využití bude uskutečněno podpisem závěrečného akceptačního protokolu.

Článek V
Ceny plnění a platební podmínky

1. Cena za plnění dle článku I odst. 1, 2 a 3 této smlouvy, která zahrnuje i poskytnutí licence SW pro 1500 uživatelských mailboxů na první rok, a za poskytování podpory provozu dle čl. I odst. 6 této smlouvy včetně akutalizací SW a pravidelné aktualizace definic malwaru v prvním roce, byla stanovena dohodou smluvních stran a činí celkem **164 949,50 Kč bez DPH**.
2. Cena za poskytnutí licence SW pro 1500 uživatelských mailboxů na druhý a další roky poskytování licence SW a poskytování podpory provozu dle čl. I odst. 6 této smlouvy včetně akutalizací SW a pravidelné aktualizace definic malwaru činí ročně **95 659,20 kč bez DPH.**
3. Cena za podporu dle čl. I odst. 5 (podpora na místě) této smlouvy bude stanovena jako součin počtu hodin skutečně poskytnuté služby a hodinové sazby, která činí **1 200,- Kč bez DPH**. K ceně prací je zhotovitel oprávněn účtovat kilometrovné ve výši 8 Kč/km, maximálně 25 km v rámci jednoho výjezdu.

4. K uvedeným cenám bude účtována DPH v sazbě platné v den uskutečnění zdanitelného plnění. Ceny zahrnují veškeré náklady poskytovatele spojené s plněním podle této smlouvy.
5. Úhrada ceny dle odst. 1 tohoto článku bude provedena na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve v den podpisu závěrečného akceptačního protokolu.
6. Úhrada ceny dle odst. 2 tohoto článku bude prováděna vždy ročně předem, a to na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve 30 dnů před začátkem období, na které se platí.
7. Úhrada ceny dle odst. 3, tj. za podporu dle čl. I odst. 5 této smlouvy, bude prováděna na základě daňového dokladu, který je poskytovatel oprávněn vystavit nejdříve poslední den kalendářního měsíce, ve kterém bylo plněno.
8. Daňový doklad bude vedle náležitostí stanovených zákonem o DPH a § 435 občanského zákoníku obsahovat i evidenční číslo smlouvy. Objednatel je oprávněn vrátit daňový doklad poskytovateli, nebude-li obsahovat stanovené náležitosti nebo bude-li obsahovat chybné údaje. Nová lhůta splatnosti začíná běžet dnem doručení bezvadného daňového dokladu.
9. Daňový doklad bude posílán elektronicky na adresu faktury@cnb.cz, přičemž daňový doklad musí být vložen jako příloha mailové zprávy ve formátu PDF. V jedné mailové zprávě smí být pouze jedna faktura (další faktury je třeba posílat jako další mailovou zprávu). Mimo vlastní fakturu může být přílohou mailu jedna až tři přílohy k faktuře ve formátech PDF, DOC, DOCX, XLS, XLSX. Nebude-li možné faktury zasílat elektronicky, zašle poskytovatel fakturu v analogové formě na adresu objednatele:

   Česká národní banka
   sekce rozpočtu a účetnictví
   odbor účetnictví
   Na Příkopě 28
   115 03 Praha 1.

10. Splatnost daňového dokladu je 14 dnů od doručení objednateli. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu objednatele ve prospěch účtu poskytovatele.

Článek VI
Podpora

1. Poskytovatel ručí za to, že SW řešení bude funkční a schopné použití v prostředí objednatele a bude odpovídat jak technickým požadavkům objednatele uvedeným v příloze č. 2 této smlouvy, tak vlastnostem a parametrům deklarovaným v příloze č. 1 této smlouvy a v dokumentaci SW řešení.
2. Poskytovatel bude odstraňovat nahlášené vady nebo malware ze systému elektronické pošty pouze v pracovní dny v době od 7:45 hod. do 16:15 hod.
3. Poskytovatel zahájí odstraňování vady nebo malware ze systému elektronické pošty nejpozději do konce pracovního dne následujícího po dni, ve kterém byla vada nahlášena objednatelem, nedohodnou-li se pověřené osoby smluvních stran v konkrétním případě jinak.

4. V odstraňování vady nebo malware ze systému elektronické pošty bude poskytovatel pokračovat bez neodůvodněného přerušení až do jejího úplného odstranění. Poskytovatel je povinen odstranit podstatnou vadu vymezenou v čl. IV odst. 3 nejpozději do 2 pracovních dnů po jejím nahlášení. Ostatní vady poskytovatel odstraní do 30 kalendářních dnů, nedohodnou-li se pověřené osoby smluvních stran v konkrétním případě jinak.
5. Objednatel nahlásí vadu nebo malware v systému elektronické pošty poskytovateli na tel: 910 973 510, a to v době od 8:30 do 17:00 hod. s následným písemným potvrzením e-mailem na e-mailovou adresu dispecink.praha@autocont.cz nebo vadu či malware systému elektronické pošty nahlásí e-mailem na mailovou adresu poskytovatele: dispecink.praha@autocont.cz.
6. Poskytovatel je povinen potvrdit e-mailem přijetí oznámení nejpozději do 4 hodin po doručení. Oznámení učiněná po 16:15 hod. se považují za oznámené v 8:00 hod. následujícího pracovního dne.
7. Poskytovatel poskytne objednateli aktualizace SW řešení a definic malwaru bez zbytečného odkladu, nejpozději však do 30 dnů poté, co je výrobce uvede na trh.
8. Poskytovatel je srozuměn s tím, že veškerá komunikace při plnění této smlouvy bude mezi objednatelem a pracovníky poskytovatele probíhat v českém jazyce.

Článek VII
Licenční ujednání

1. Pro SW řešení podle čl. I odst. 1 je poskytována nevýhradní, časově a územně neomezená multilicence, tj. právo užití pro 1500 uživatelských mailboxů objednatele. Právo užívání SW dle této smlouvy přechází na objednatele dnem podpisu závěrečného akceptačního protokolu.
2. Objednatel není povinen licenci využít.
3. Součástí licence je příslušná dokumentace v elektronické podobě.
4. 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.
5. Licence poskytnuté dle této smlouvy se vztahují i na veškeré poskytnuté aktualizace (tj. update/upgrade/patch/hotfix atd.).

Článek VIII
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:

a) Zpracování veškerých osobních údajů objednatelem, 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.

b) 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.

c) 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 IX
Smluvní pokuty, úrok z prodlení

1. V případě prodlení poskytovatele v kterékoliv lhůtě uvedené v článku III odst. 1 a 2 této smlouvy, popř. lhůtě prodloužené v souladu s článkem III odst. 3 této smlouvy, je objednatel oprávněn požadovat smluvní pokutu ve výši 2 000 Kč za každý den prodlení. To neplatí, pokud k prodlení poskytovatele došlo z důvodů na straně objednatele.
2. V případě, že se v průběhu plnění prokáže, že nebyl poskytovatelem splněn jakýkoliv z povinných technických požadavků objednatele uvedených v článku 1, 2 a 3 v příloze č. 2 této smlouvy, je objednatel oprávněn požadovat smluvní pokutu ve výši 35 000 Kč za každý takový případ. Tím není dotčeno právo objednatele odstoupit od smlouvy ani požadovat náhradu vzniklé škody.
3. V případě prodlení poskytovatele ve lhůtě pro zahájení odstranění vady podle článku VI odst. 3 této smlouvy je objednatel oprávněn požadovat smluvní pokutu ve výši 500 Kč za každý pracovní den prodlení.
4. V případě prodlení poskytovatele ve kterékoli lhůtě podle článku VI odst. 4 této smlouvy, je objednatel oprávněn požadovat smluvní pokutu ve výši 1 000 Kč za každý pracovní den prodlení.
5. V případě prodlení objednatele s úhradou daňového dokladu je poskytovatel oprávněn požadovat úrok z prodlení podle nařízení vlády č. 351/2013 Sb.
6. Smluvní pokuta a úrok z prodlení jsou splatné do 14 dnů od doručení platebního dokladu povinné smluvní straně. Povinnost zaplatit je splněna odepsáním příslušné částky z účtu povinného ve prospěch účtu oprávněného.
7. Smluvní pokutou není dotčeno právo na náhradu škody.

Článek X
Doba trvání smlouvy, výpověď, odstoupení od smlouvy

1. Smlouva se v části upravující poskytování podpory uzavírá na dobu neurčitou.
2. Smlouvu lze v části upravující poskytování podpory ukončit písemnou výpovědí, která musí být doručena druhé smluvní straně nejpozději 3 měsíce přede dnem uplynutím předplacené doby podpory s tím, že závazky týkající se poskytování podpory zanikají 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. V případě, že účinnost smlouvy skončí před koncem účtovacího období, vrátí poskytovatel objednateli alikvotní část předplacené ceny plnění.
4. Smluvní strany se dále dohodly, že objednatel je oprávněn zrušit tuto smlouvu zaplacením odstupného ve výši 20 000 Kč na účet poskytovatele, a to kdykoli do podpisu akceptačního protokolu první etapy. Zrušení smlouvy je účinné připsáním sjednaného odstupného na bankovní účet poskytovatele. Zaplacením odstupného zanikají všechna práva a povinnosti obou smluvních stran vyplývající ze zrušené smlouvy s výjimkou závazku mlčenlivosti poskytovatele.
5. Poruší-li kterákoliv strana podstatným způsobem závazky vyplývající z této smlouvy, má druhá strana právo odstoupit od smlouvy, a to prostřednictvím písemného odstoupení. Takové odstoupení bude platné a nabude účinnosti dnem jeho doručení druhé smluvní straně.
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) dodané SW řešení, 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 operačními systémy (jejich verzemi), databázemi (jejich verzemi) a aplikacemi (jejich verzemi),
   d) poskytovatel bude v prodlení v kterékoliv lhůtě uvedené v článku III odst. 2 této smlouvy delším než 30 dnů.

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 5 000 000 Kč (slovy: pět 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.

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, není-li ve smlouvě stanoveno jinak.
3. Tato smlouva je sepsána v českém jazyce. Veškerá komunikace mezi smluvními stranami vztahující se k této smlouvě bude probíhat v českém nebo slovenském jazyce, nebude-li smluvními stranami v konkrétním případě dohodnuto jinak.
4. Smluvní strany se dohodly, že tato smlouva a právní vztahy s ní související se řídí zákonem č. 89/2012 Sb., občanský zákoník a ostatními souvisejícími platnými právními předpisy.
5. 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.
6. Smlouva je vyhotovena ve třech vyhotoveních s platností originálu, z nichž objednatel obdrží dvě a poskytovatel jedno vyhotovení.

Přílohy: č. 1 - Technická specifikace SW řešení
č. 2 - Technické požadavky objednatele
č. 3 - Bezpečnostní požadavky objednatele
č. 4 – Cenová tabulka

V Praze dne: 9. 9. 2015

Za objednatele:

[redacted]

Ing. Vladimír Majzlšek
ředitel sekce informatiky

[redacted]

Ing. Zdeněk Viriis
ředitel sekce správní

[redacted]

V Praze dne: 14. 09. 2015

[redacted]

Ing. Petr Suntych
člen představenstva

AUTOCONT 1
AutoCont CZ a.s., Praha
Líbalova 1/2348, 149 00 Praha 4
Tel.: 910 972 111, fax: 910 970 102
DIČ: CZ47676795

Příloha č. 1

Technická specifikace SW řešení

Popis řešení a technické vlastnosti produktu ESET Mail Security for Microsoft Exchange server:

Na každý virtuální server v roli Exchange HUB bude instalován nabízený software ESET Mail Security, který bude kontrolovat průchozí emailovou komunikaci na přítomnost škodlivého kódu, jako je např. vir, spyware, trojan, worm, keylogger apod. Toto řešení umožní kontrolovat příchozí a odchozí komunikaci typu POP3, SMTP, IMAP pomocí VSAPI rozhraní. Správa řešení ESET Mail Securtity bude probíhat skrze jednu konzoli ESET Remote Administrator, veškerá nastavení budou replikovány na všechny instalovány ESET Mail Security servery.

Vlastnosti nabízeného řešení ESET Mail Security:

- je kompatibilní a intregovatelný se stávající vertí Exchange 2010 SP3 RU8v2
- disponuje centrálním managementem (administrátorským rozhraním pro správu)
- nepřeposílá mailovou komunikaci určenou k oskenování mimo servery, kde je zpracovávána v rámci stávajícího systému elektronické pošty
- výrobce řešení je uveden na seznamu podporovaných partnerů společnosti Microsoft.
- výrobce řešení odstraňuje zranitelnosti SW prostřednictvím aktualizovaných verzí nebo fixů.
- využívá nativní rozhraní VSAPI pro antimalwarovou kontrolu na mailboxech a veřejných složkách.
- poskytuje agenta pro antimalwarovou kontrolu na Hub Transport serveru.
- poskytuje ochranu před malware (viry, spyware, trojan, worm, keylogger) s pravidelnými (minimálně denními) aktualizacemi definic, bez nutnosti zvláštního oprávnění k jejich instalaci.
- zpracovává online zprávy, které jsou MS Exchange přijaty, a provádí jejich kontrolu na výskyt malware, včetně zpráv zasílaných mezi uživateli v rámci i jednoho mailboxu.
- provádí dodatečnou on-demand offline kontrolu zpráv již uložených ve složkách/schránkách v MS Exchange s možností definice této periody.
- v případě falešné detekce je k dispozici karanténa, ze které je možné zprávy obnovit. Ke karanténě mají přístup pouze definovaní uživatelé (správci).
- obsahuje mechanismus ochrany proti útokům a hrozbám, které se v systému elektronické pošty snaží využít zranitelnosti používaného software a pro které neexistuje obrana (0 day).
- umožňuje nastavení politik pro povolování, zakazování a omezování přípojek podle jejich názvu a koncovky.
- je „krabicové“ bez nutnosti programátorských úprav nebo zásahů do současné konfigurace Exchange serveru. Instalace/odinstalace je možná prostřednictvím služby MS Installer
- nevyžaduje žádný dodatečný HW a instaluje se pouze do stávajícího systému elektronické pošty.
- je dostupný v českém jazyce.
- všechny definovatelné události na mailboxu související s instalovaným agentem jsou logovány včetně nálezu malware.
- uživatel nemá možnost vynutit spuštění scanu.

- je funkční na virtuálních serverech.
- běží i na větším počtu mailboxů, než je počet zakoupených resp. instalovaných licencí. V tomto případě je do managementu systému publikováno varovné hlášení, ale funkčnost při překročení do 50 licencí není nijak omezena.
- Nabízený sw neodesílá ani žádným jiným způsobem nepředává žádnou část mailové komunikace mimo prostředí objednatele.
- řešení nevyužívá definice malwaru shodné s již na ČNB používanou ochranou pracovních stanic a virtualních stanic od firmy Symantec.
- řešení má minimálně srovnatelné nebo nižší požadavky na zdroje ve srovnání se stávajícím produktem MS Forefront.
- ESET Mail Security je možo snadno vypnout nebo odinstalovat, aniž by bylo potřeba rušit celý Exchange
- V případě potřeby, je možno uřídit výjimky z kontroly pro vybrané soubory adresářů Microsoft Exchange

Management ESET Remote Administrator splňuje následující požadavky:

- Pro všechny komponenty správy je skrze management nástroje ESET Remote Administrator vyřešena dostupnost zajišťující provoz ve dvou lokalitách. Komponenty správy jsou spustitelné na MS Windows Serveru 2008 R2. Pro ukládání konfiguračních položek, politiky a auditních záznamů bude použit systém SQL server 2008 R2 Standard Edition.
- Všechny požadované funkce lze spravovat přes řídící konzoli ESET Remote Administrator , která bude nainstalovaná na MS Windows Serveru 2008 R2 a přístupná přes webové rozhraní. Konzole umožňuje správu, monitoring a vyhodnocování událostí týkající se provozu systému. Události je možné sledovat v reálném čase i zpětně.
- k administraci se využívají doménové účty s využitím SSO včetně doménového přihlášení pomocí čipové karty ČNB.
- management umožnuje zasílání emailů s upozorněním (notifikací) v případě, že nastane událost dle definovaných parametrů.
- ESET Remote Administrator řeší rovněž problém falešného poplachu (nastavení výjimky, vypnutí jádra, obnovu z karantény).
- ESET Remote Administrator je možné nainstalovat nejen na Windows, ale rovněž i formou Virtual Appliance

Příloha č. 2

Technické požadavky objednatele

Preambule

Zadavatel požaduje dodávku komplexního zabezpečení systému elektronické pošty ve standardním systémovém prostředí ČNB. Prostředí ČNB se skládá z fyzických serverů platformy x86 a virtuálních serverů na platformě VMware vSphere 5.1 nebo novějších, a z fyzických pracovních stanic IBM-PC kompatibilních a virtuálních pracovních stanic provozovaných na platformě Citrix.

Systémem elektronické pošty se rozumí:

- MS Exchange 2010 SP3 RU8v2 běžící na serveru s OS MS Windows Server 2008 R2 SP1 provozovaný na fyzickém HW nebo ve virtuálním prostředí takto:
- V každé ze dvou geograficky oddělených lokalitách se nachází 1x virtuální server pro CAS a HUB v konfiguraci 4x CPU 2,8GHz Intel Xeon, 8GB RAM, 64GB systémový disk, 12 GB pagefile a 50GB datový disk. Dále 2x fyzický server s Mailboxy v konfiguraci 2x CPU/6 jader 2,66 GHz Intel Xeon, 24 GB RAM, 64GB systémový disk, 16GB Pagefile, 56GB datový disk + pole disků pro DB (22x146GB).
- Servery mezi lokalitami pracují v případě CAS a HUB pod jedním jménem prostřednictvím MS NLB. Servery pro mailboxy vytvářejí cluster prostřednictvím DAG.
- Klientem je MS Outlook 2010 s využitím mezipaměti (cache mod) na PC s Windows 7 a bez využití mezipaměti na virtuálním desktopu. Pro vzdálený přístup je kilentem MS OWA Exchange 2010.

Malware se rozumí:

Škodlivý počítačový kód nebo program určený ke vniknutí nebo poškození počítačového systému. Zahrnuje vir, spyware, trojan, worm, keylogger atd.

1. SW řešení pro zabezpečení systému elektronické pošty musí splňovat následující požadavky:

1.1 Je kompatibilní a integrovatelné se systémem elektronické pošty objednatele.
1.2 Disponuje managementem (administrátorským rozhraním pro správu).
1.3 Nepřeposílá mailovou komunikaci určenou k oskenování mimo servery, kde je zpracovávána v rámci stávajícího systému elektronické pošty
1.4 Výrobce řešení je uveden na seznamu podporovaných partnerů společnosti Microsoft.
1.5 Výrobce řešení odstraňuje zranitelnosti SW prostřednictvím aktualizovaných verzí nebo fixů.
1.6 Využívá nativní rozhraní VSAPI pro antimalwarovou kontrolu na mailboxech a veřejných složkách.
1.7 Poskytuje agenta pro antimalwarovou kontrolu na Hub Transport serveru.
1.8 Poskytuje ochranu před malware (viry, spyware, trojan, worm, keylogger) s pravidelnými (minimálně denními) aktualizacemi definic, bez nutnosti zvláštního oprávnění k jejich instalaci.

1.9 Zpracovává online zprávy, které jsou MS Exchange přijaty, a provádí jejich kontrolu na výskyt malware, včetně zpráv zasílaných mezi uživateli v rámci i jednoho mailboxu.

1.10 Provádí dodatečnou on-demand offline kontrolu zpráv již uložených ve složkách/schránkách v MS Exchange s možností definice této periody.

1.11 V případě falešné detekce je k dispozici karanténa, ze které je možné zprávy obnovit. Ke karanténě mají přístup pouze definovaní uživatelé (správci).

1.12 Obsahuje mechanismus ochrany proti útokům a hrozbám, které se v systému elektronické pošty snaží využít zranitelnosti používaného software a pro které neexistuje obrana (0 day).

1.13 Umožňuje nastavení politik pro povolování, zakazování a omezování přípojek podle jejich názvu a koncovky.

1.14 Je „krabicové" bez nutnosti programátorských úprav nebo zásahů do současné konfigurace Exchange serveru. Instalace/odinstalace prostřednictvím služby MS Installer.

1.15 Nevyžaduje žádný dodatečný HW a instaluje se pouze do stávajícího systému elektronické pošty.

1.16 Je dostupný v českém jazyce.

1.17 Všechny definovatelné události na mailboxu související s instalovaným agentem jsou logovány včetně nálezu malware.

1.18 Uživatel nemá možnost vynutit spuštění scanu.

1.19 Je funkční na virtuálních serverech.

1.20 Běží i na větším počtu mailboxů, než je zakoupeno. V tomto případě je do managementu systému publikováno varovné hlášení, ale funkčnost při překročení do 50 licencí není nijak omezena.

1.21 Neodesílá ani žádným jiným způsobem nepředává žádnou část mailové komunikace mimo prostředí objednatele.

2. Management musí splňovat následující požadavky:

2.1 Pro všechny komponenty správy je vyřešena dostupnost zajišťující provoz ve dvou lokalitách. Komponenty správy jsou spustitelné na MS Windows Serveru 2008 R2. Pro ukládání konfiguračních položek, politiky a auditních záznamů je použit buď souborový systém, nebo interní databáze (v ceně licence) nebo MS SQL server 2008 R2 Standard Edition.

2.2 Všechny požadované funkce se spravují přes řídící konzoli, která je nainstalovaná na MS Windows Serveru 2008 R2 a přístupná přes webové rozhraní. Konzole umožňuje správu, monitoring a vyhodnocování událostí týkající se provozu systému. Události je možné sledovat v reálném čase i zpětně.

2.3 K administraci se využívají doménové účty s využitím SSO včetně doménového přihlášení pomocí čipové karty ČNB.

2.4 Zasílá emaily s upozorněním (notifikací) v případě, že nastane událost dle definovaných parametrů.

2.5 Řeší problém falešného poplachu (nastavení výjimky, vypnutí jádra, obnovu z karantény).

3. Obecně musí být splněny následující požadavky:

3.1 Řešení nevyužívá pouze definice malwaru shodné s již nasazenou ochranou pracovních stanic a virtualních stanic od firmy Symantec. Důvodem je snížení rizika,

kdy stejné definice znemožní detekci zachycení infikované zprávy nebo naopak omezí výskyt falešného polachu.

3.2 Řešení musí mít srovnatelné nebo nižší požadavky na zdroje ve srovnání se stávajícím produktem MS Forefront.

3.3 SW musí být snadno vypnutelný nebo odinstalovatelný, aniž by bylo potřeba rušit celý Exchange (např. z důvodu nedostatků vzniklých při/po update tohoto SW).

Příloha č. 3

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 na seznamu pracovníků schváleném ČNB (dále jen „seznam"). Tato povinnost se vztahuje i na posádky vozidel poskytovatele vjíždějících do garáží ČNB za účelem složení a naložení nákladu. Poskytovatel předloží seznam ČNB nejpozději v den podpisu smlouvy.

2. Seznam bude obsahovat tyto položky: název poskytovatele, adresu sídla poskytovatele, telefonní a emailový kontakt na poskytovatele, tituly, jména a příjmení pracovníků poskytovatele, čísla průkazů totožnosti pracovníků poskytovatele a pro vozidla bude uveden typ vozidla a registrační značka. 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: titul, 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. Pracovníci neschválení ze strany ČNB nemohou vstupovat do objektů ČNB, přičemž ČNB si vyhrazuje právo neuvádět důvody jejich neschválení.

4. Poskytovatel uvede pracovníky, pro které požaduje vystavení vstupních karet ke vstupu do objektu objednatele. Vystavení vstupních karet podléhá schválení objednatele. První vstupní karty budou vystaveny na náklady objednatele. Každé další vystavení vstupní karty bude zpoplatněno částkou 240,- Kč (vč. DPH) s tím, že tato částka bude poskytovateli vyfakturována. Vstupní karta se nebude platit v případech, kdy:

   - přestane fungovat bez viditelného mechanického poškození,
   - dojde-li ke změně příjmení,
   - byla-li karta odcizena a událost je doložitelná protokolem od Policie ČR.

5. Poskytovatel bude při zahájení činnosti vybaven základním počtem vstupních karet pro jednotlivé pracovníky podle schváleného seznamu. Vstupní karta umožní pracovníkovi poskytovatele samostatný vstup do vyhrazených prostor objektu objednatele a samostatný pohyb v nich. Vstupní karta bude nepřenosná a bude vydávána odborem bankovní bezpečnosti a krizového řízení.

6. Vstupní karty budou vydávány objednatelem každému pracovníkovi poskytovatele jednotlivě proti podpisu, po předložení výpisu z rejstříku trestů, který nebude starší než tři měsíce. Výpis z rejstříku trestů bude vrácen pracovníkovi poskytovatele. Při převzetí vstupní karty bude pracovník poskytovatele poučen o způsobu používání vstupní karty a o režimu vstupu osob a vjezdu vozidel do objektu objednatele a o pohybu v něm.

7. Pracovník poskytovatele, kterému byla vydána vstupní karta, je povinen okamžitě po zjištění ztráty, odcizení, zneužití, zničení nebo poškození vstupní karty, které brání jejímu řádnému užívání, toto oznámit odboru bankovní bezpečnosti a krizového řízení.

8. Při ukončení pracovního poměru pracovníka poskytovatele uvedeného v seznamu nebo při ukončení plnění podle smlouvy je poskytovatel povinen neprodleně vrátit vstupní karty odboru bankovní bezpečnosti a krizového řízení.
9. Objednatel si vyhrazuje právo nevydat vstupní kartu pracovníkům poskytovatele bez udání důvodu.
10. Objednatel si vyhrazuje právo vstupní kartu pracovníku poskytovatele odebrat z důvodu porušení režimu vstupu osob a vjezdu vozidel do objektu objednatele nebo porušení režimu pohybu v něm.
11. Objednatel si vyhrazuje právo odvolat schválené pracovníky poskytovatele ze seznamu bez udání důvodů. Schválení pracovníci musí dodržovat směrnice ČNB a pokyny ostrahy pro vstup do vyhrazených prostor a pro pobyt v nich.
12. Pracovníci poskytovatele jsou povinni podrobit se při každém vstupu do objektu ČNB bezpečnostní kontrole prováděné bankovními policisty.
13. Objednatel si vyhrazuje právo nevpustit do objektů ČNB pracovníka poskytovatele, který je zjevně pod vlivem alkoholu, drog nebo jiné omamné látky.
14. Vstup do objektů ČNB se zvířaty je zakázán.
15. Vstup soukromých návštěv do vnitřních prostor objektů ČNB je zakázán. Pro tyto účely je možné využít určené návštěvní místnosti.
16. Poskytovatel a jeho pracovníci budou věnovat při plnění díla v oblasti požární ochrany zvýšenou pozornost:
    - dodržování právních předpisů o požární ochraně,
    - předpisům objednatele při provádění požárně nebezpečných prací se zvýšeným požárním nebezpečím (svařování, řezání plamenem, pájení, broušení, rozbrušování apod.),
    - průrazům a průchodům u rozvodů instalací a technologií hranicemi požárních úseků, včetně zachování, obnovení nebo nového vyhotovení jejich protipožárních ucpávek.
17. Poskytovatel se zavazuje zajistit, že jeho pracovníci, jakož i pracovníci případných jeho subdodavatelů, kteří se budou na plnění podle této smlouvy podílet, zachovají mlčenlivost o všech skutečnostech, se kterými se v průběhu plnění seznámí a které nejsou veřejně známy.
18. Povinnost mlčenlivosti není časově omezena.
19. V případě mimořádné události se pracovníci poskytovatele musí řídit pokyny bankovních policistů nebo dozorujícího zaměstnance ČNB a dále instrukcemi vyhlašovanými vnitřním rozhlasem.
20. Pracovníci poskytovatele nesmí vnášet do prostor ČNB nebezpečné předměty, jako jsou střelné zbraně, výbušniny, hořlavé kapaliny, tlakové lahve apod. O tom, co je a není nebezpečný předmět, rozhodují bankovní policisté v souladu s vnitřními předpisy ČNB.
21. Fotografování a pořizování videozáznamů je ve všech prostorech objektů ČNB zakázáno. Výjimku tvoří pořizování dokumentace technických havárií a poruch. Konkrétní případ musí předem písemně povolit ředitel odboru bankovní bezpečnosti a krizového řízení nebo ředitel příslušné pobočky ČNB.
22. Ve všech prostorech objektů ČNB je přísný zákaz kouření a používání otevřeného ohně. O povolení k provedení požárně nebezpečné práce se zvýšeným požárním nebezpečím

požádá poskytovatel písemnou formou dozorujícího zaměstnance ČNB, a to vždy nejpozději jeden pracovní den před zahájením prací.

23. Pracovníci poskytovatele se musí zdržet poškozování či zcizení majetku ČNB, a dále nevhodného chování vůči zaměstnancům a návštěvníkům ČNB.

24. Pracovníci poskytovatele uvedení na seznamu se musí před započetím výkonu práce v objektech objednatele prokazatelně seznámit s „Pravidly pro smluvní partnery ČNB k zajištění bezpečnosti a ochrany zdraví při práci, požární ochrany a ochrany životního prostředí v ČNB" (dále jen „pravidla"). Pravidla budou v listinné formě předána zástupci poskytovatele požárním a bezpečnostním technikem ČNB. Zástupce poskytovatele s pravidly seznámí všechny dotčené pracovníky poskytovatele.

25. Objednatel je oprávněn v objektu ČNB kdykoliv podrobit kontrole kteréhokoliv pracovníka poskytovatele uvedeného na seznamu z dodržování požární ochrany, bezpečnosti práce a výše uvedených ustanovení.

Příloha č. 4 smlouvy-cenová tabulka

Antivirová ochrana pro MS Exchange II		
1		**Cena v Kč bez DPH**
a	Licence SW pro 1500 uživatelských mailboxů a podpora provozu, aktualizace SW a pravidelná aktualizace definic malwaru dle čl. I odst. 6 smlouvy na 1. rok[1]	**133 699,50**

2		**Ceny v Kč bez DPH**
a	Analýza a vypracování implementačního postupu	6 250,00
b	Odinstalace stávajícího programu MS Forefront ze serverů Exchange	6 250,00
c	Implementace SW včetně otestování a zaškolení	12 500,00
d	Administrátorská, instalační a havarijní dokumentace	6 250,00
	Analýza a implementace celkem (2a + 2b +2c + 2d)	**31 250,00**
	Dodávka celkem	**164 949,50**

3		**Cena v Kč bez DPH**
a	Licence SW pro 1500 uživatelských mailboxů a podpora provozu, aktualizace SW a pravidelná aktualizace definic malwaru dle čl. I odst. 6 smlouvy na 2. a každý další rok[1]	**95 659,20**
b	Podpora (dle čl. I odst. 5 smlouvy)	**Cena za hodinu v Kč bez DPH** **1 200,00**
c	Doprava (dle čl. I odst. 5 smlouvy, maximální počet km jednoho výjezdu do sídla objednatele je 25)	**Kilometrovné v Kč/km bez DPH** **8,00**

1 S ohledem na to, že není možné cenu licence SW a podpory provozu vč. aktualizací SW a pravidelné aktualizace definic malwaru oddělit, ceny uvedené v řádcích **1a** a **3a** zahrnují jak cenu licence, tak cenu podpory vč. aktualizací SW a pravidelné aktualizace definic malwaru za jednotlivé roky.