SMLOUVA O POSKYTOVÁNÍ ANALYTICKÝCH A KONZULTAČNÍCH SLUŽEB PRO OBLAST KYBERNETICKÉ BEZPEČNOSTI

Hlavní město Praha
se sídlem: Mariánské náměstí 2/2,110 01, Praha 1
IČO: 00064581
DIČ: CZ00064581
bank. spojení: PPF banka, a. s., Evropská 2690/17,160 41, Praha 6, č. účtu: 27-5157998/6000
zastoupeno: JUDr. Markétou Štalmachovou, ředitelkou odboru bezpečnosti Magistrátu hl. m. Prahy
číslo smlouvy Objednatele: INO/39/01/001167/2023
na straně jedné (dále jen „**Objednatel**")

a

Corpus Solutions a.s.
se sídlem: Štětkova 1638/18, 140 00 Praha 4
IČO: 257 64 616, DIČ: CZ257 64 616
společnost zapsaná v obchodním rejstříku vedeném u Městského soudu v Praze, oddíl B, vložka 5936
bank. spojení: Raiffeisenbank a.s., číslo účtu: 69 47 4001/5500
zastoupená: Ing. Tomáš Přibyl, předseda představenstva
na straně druhé (dále jen „**Poskytovatel**")

Objednatel a Poskytovatel jsou společně v textu smlouvy uváděni též jako „**Smluvní strany**" nebo „**Strany**" a každý jednotlivě jako „**Strana**" nebo „**Smluvní strana**".

Smluvní strany níže uvedeného dne, měsíce a roku v souladu s ustanovením § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**") uzavřely tuto Smlouvu o poskytování analytických a konzultačních služeb pro oblast kybernetické bezpečnosti (dále jen „**Smlouva**").

Článek 1

Úvodní ustanovení

1. Objednatel dne 2. 6. 2023 oznámil odesláním oznámení o zahájení zadávacího řízení veřejné zakázky s názvem „*Zajištění analytických a konzultačních služeb pro oblast kybernetické bezpečnosti*" (dále

jen „**Veřejná zakázka**“) zadávané v rámci otevřeného řízení dle zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „**ZZVZ**“). Na základě výsledků výběru dodavatele byl Poskytovatel vyzván k uzavření této Smlouvy na plnění předmětu Veřejné zakázky.

2. Objednatel prohlašuje, že je územně samosprávným celkem vzniklým na základě zákona a že splňuje veškeré požadavky v této Smlouvě sjednané a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

3. Poskytovatel prohlašuje, že je právnickou osobou (obchodní korporací) řádně založenou a zapsanou dle právního řádu České republiky v obchodním rejstříku s předmětem podnikání v oboru činnosti podle předmětu této Smlouvy a že splňuje veškeré podmínky a požadavky v této Smlouvě sjednané a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

4. Poskytovatel dále prohlašuje, že členové realizačního týmu, kteří se budou podílet na plnění předmětu této Smlouvy, bez ohledu na to, zda jde o zaměstnance Poskytovatele nebo osoby v jiném vztahu k Poskytovateli, disponují následujícími certifikáty: CSSLP – Certified Secure Software Lifecycle Professional, CISSP – Certified Information Systems Security Professional, PECB – Certified ISO/IEC 27001 Lead Auditor, Check Point Certifed Security Master, CCSMElite – Check Point Certifed Security Master Elite, F5 – CTS, LTM (F5 Certified Technology Specialist, BIG-IP Local Traffice Manager Certificate), Fedelis Elevate Endpoint-Admin Training, Fedelis Elevate Network-Admin Training, Rapid7 (InsightAppSec Certified, InsightVM Technical Certified), BVS Certifikát. Současně musí být splněny podmínky uvedené v článku 2 odst. 5 této Smlouvy.

5. Smluvní strany shodně prohlašují, že identifikační údaje uvedené ve Smlouvě jsou plně v souladu s právní skutečností v době uzavření Smlouvy, zejména že adresa každé Smluvní strany uvedená v záhlaví této Smlouvy je adresou doručovací. Smluvní strany se zavazují, že změny dotčených údajů oznámí bez prodlení druhé Smluvní straně, zejména pak změnu doručovací adresy, bankovního spojení apod. Smluvní strany dále prohlašují, že osoby podepisující tuto Smlouvu jsou k tomuto právnímu jednání oprávněny.

6. Smluvní strany prohlašují, že si při jednání o uzavření Smlouvy sdělily navzájem všechny skutkové a právní okolnosti, o nichž vědí nebo vědět musí tak, aby se každá ze stran mohla přesvědčit o možnosti uzavřít platnou Smlouvu a aby byl každé ze stran zřejmý její zájem Smlouvu uzavřít.

Článek 2

Předmět plnění, účel Smlouvy

1. Účelem Smlouvy je zajištění poskytování analytických a konzultačních služeb pro oblast kybernetické bezpečnosti s cílem zvýšení odolnosti Objednatele vůči kybernetickým hrozbám. Účelem Smlouvy je realizace Veřejné zakázky dle zadávacích podmínek Veřejné zakázky (dále jen „**Zadávací dokumentace**“) v souladu s požadavky Objednatele definovanými touto Smlouvou a Zadávací dokumentací.

2. Poskytovatel se zavazuje v souladu se Smlouvou provést na své náklady a nebezpečí předmět plnění v rozsahu podle odstavců 3 a 4 tohoto článku Smlouvy. Objednatel se zavazuje v souladu se Smlouvou předmět plnění převzít a zaplatit Poskytovateli dohodnutou cenu uvedenou v článku 3. odst. 1 Smlouvy ve prospěch bankovního účtu Poskytovatele uvedeného v záhlaví Smlouvy.

3. **Předmětem plnění** je poskytnutí odborných analytických a konzultačních služeb pro oblast kybernetické bezpečnosti a bezpečnosti informačních systémů a výkon role architekta kybernetické bezpečnosti v souladu s požadavky vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále „**VKB**“) a dalších relevantních právních předpisů. Předmět plnění je specifikován níže v odstavci 4 tohoto článku a dále v příloze č. 1 této Smlouvy – Specifikace předmětu plnění.

4. **Specifikace analytických a konzultačních služeb**

   a) Podpora na analytické a konzultační práce související s provozem bezpečnostních technologií

   b) Zajištění pravidelné revize bezpečnostních politik

   c) Zajištění vstupů pro plánování posilování kybernetické bezpečnosti organizace

   d) Konzultační práce k připravovaným projektům s cílem poskytnout odborné stanovisko k dané problematice

   e) Tvorba bezpečnostních případů užití

   f) Zajištění správy bezpečnostních výjimek vůči schválenému designu organizace

   g) Revize účinnosti detekce kybernetických hrozeb

   h) Provedení penetračního testování odolnosti bezpečnostních mechanismů informačních systémů zadavatele

   i) Provedení auditu bezpečnosti informačních systémů, či procesů nebo stavu informační bezpečnosti

   j) Zajištění výkonu role architekta kybernetické bezpečnosti v souladu s požadavky VKB

   k) Další konzultační a analytické služby dle požadavků Objednatele

5. Poskytovatel se zavazuje poskytovat Služby sám nebo s využitím poddodavatelů. Objednatel v souladu s § 105 odst. 2 ZZVZ určuje významné činnosti, jejichž plnění musí být zajištěno přímo Poskytovatelem, a to následovně:

   Významnými činnostmi jsou veškeré činnosti, které mají být prováděny osobou disponující certifikátem:

   a) F5 Certified Technology Specialist, BIG-IP Local Traffice Manager Certificate,

   b) Fidelis Elevate Endpoint-Admin Training,

c) Fidelis Elevate Network-Admin Training,

d) Check Point Certifed Security Master,

e) Rapid 7 InsightAppSec Certified, InsightVM Technical Certified),

f) BVS Certifikát.

Tyto významné činnosti není Poskytovatel oprávněn plnit prostřednictvím poddodavatelů či jiných osob. Části technické kvalifikace, které se vztahují k významným činnostem, není Poskytovatel oprávněn prokazovat prostřednictvím jiných osob.

6. Služby jsou Poskytovatelem poskytovány v rozsahu a dle aktuálních potřeb Objednatele. Objednatel v rámci Zadávací dokumentace, konkrétně v příloze č. 6 k Zadávací dokumentaci, stanovil předpokládaný rozsah jednotlivých poskytovaných služeb a tomu odpovídající časovou náročnost v přepočtu na člověkoden (dále jen „**ČD**“). Tento rozsah je pouze předpokládaný a orientační, Poskytovatel není oprávněn si v této příloze uvedený počet ČD nárokovat.

Článek 3

Cena, platební podmínky a fakturace

1. Cena za jeden ČD činí **16 000,00** Kč bez DPH (slovy: **šestnáct tisíc korun českých**). K ceně bude připočtena DPH v zákonné výši **21 %**, která činí **3 360,00** Kč. Celková cena za jeden ČD spolu s DPH činí **19 360,00 Kč** (slovy: **devatenáct tisíc tři sta šedesát korun českých**).
2. Jedním ČD se rozumí čas odpovídající práci jednoho člena realizačního týmu po dobu jednoho pracovního dne, tj. 8 hodin. ČD zahrnuje i všechny související náklady jako náklady na dopravu, stravování, ubytování apod.
3. Objednatel vyzve Poskytovatele k plnění na základě Smlouvy, přičemž ten je povinen bez zbytečného odkladu započít kroky směřující k poskytnutí plnění.
4. Poskytovatel se zavazuje doručit výkaz činnosti, ve kterém podrobně specifikuje provedené činnosti a příslušný počet ČD za každou činnost. Na základě odsouhlaseného výkazu činnosti je Poskytovatel oprávněn doručit svou fakturu.
5. Výkaz, jakož i fakturu doručuje Poskytovatel zpravidla jednou měsíčně. Poskytovatel se od tohoto pravidla může odchýlit a fakturu doručit za více měsíců souhrnně, pokud je to např. administrativně vhodnější.
6. V celkové ceně dle předchozího odstavce jsou zahrnuty veškeré náklady Poskytovatele. Finanční plnění bude uskutečněno platbou na základě faktury. Zálohové platby se nesjednávají.
7. Faktura musí obsahovat veškeré náležitosti daňového dokladu ve smyslu zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, včetně čísla bankovního účtu Poskytovatele, uvedeného v záhlaví této Smlouvy. Číslo účtu Poskytovatele uvedeného na faktuře musí být shodné

se zveřejněným účtem Poskytovatele správcem daně pro účely DPH dle § 98 písm. d) zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.

8. V souladu s nařízením Evropského parlamentu a Rady EU 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR) a taktéž v souladu s příslušným nařízením ředitele Magistrátu hl. m. Prahy k zajištění povinnosti uveřejňovat smlouvy prostřednictvím registru smluv nesmí faktura v rozsahu a předmětu plnění obsahovat osobní údaje fyzických osob jako například jméno a příjmení fyzické osoby, datum narození, číslo jejího bankovního účtu a její kontaktní údaje (telefon, e-mail), DIČ fyzické osoby podnikající.

9. Splatnost faktury činí 30 dnů od jejího doručení Objednateli. Platbou se rozumí prokazatelné odepsání příslušné částky z účtu Objednatele nejpozději v den splatnosti ve prospěch bankovního účtu Poskytovatele.

10. V případě, že faktura bude obsahovat nesprávné cenové nebo právními předpisy vyžadované údaje, je Objednatel oprávněn fakturu vrátit Poskytovateli k opravě. Nová lhůta v původní délce splatnosti počíná běžet znovu ode dne doručení opravené nebo nově vystavené faktury.

Článek 4

Doba (termíny) plnění a místo plnění

1. **Termíny plnění:**

   Smlouva se uzavírá na dobu určitou, a to na 56 měsíců ode dne uzavření Smlouvy nebo do vyčerpání částky 10 000 000,00 Kč bez DPH.

2. **Místo plnění:**

   Místem plnění je zejména sídlo Objednatele a dále též jiné prostory dle potřeby a výslovného pokynu Objednatele.

Článek 5

Centrální evidence smluv

1. Poskytovatel výslovně souhlasí s tím, aby Smlouva vztahující se k této veřejné zakázce byla uvedena v Centrální evidenci smluv (CES), vedené hlavním městem Prahou, která je veřejně přístupná, a která obsahuje údaje o Smluvních stranách, číselné označení této Smlouvy, datum jejího podpisu a text této Smlouvy. Poskytovatel prohlašuje, že skutečnosti uvedené v této Smlouvě nepovažuje za obchodní tajemství ve smyslu § 504 Občanského zákoníku a uděluje svolení k jejich užití a zveřejnění bez stanovení jakýchkoli dalších podmínek.

Článek 6

Smluvní pokuty, úrok z prodlení, odpovědnost za újmu (škodu), odpovědnost za vady

1. V případě prodlení Objednatele s úhradou řádně vyúčtované ceny za plnění, jakož i v případě prodlení s plněním jakéhokoliv jiného peněžitého závazku, k němuž je zavázán Objednatel touto Smlouvou, se sjednává smluvní pokuta ve výši 0,05 % z dlužné částky s DPH za každý den prodlení, splatná do 14 kalendářních dnů ode dne doručení jeho vyúčtování Objednateli. Vedle smluvní pokuty náleží Poskytovateli úrok z prodlení v zákonné výši. Sjednaná smluvní pokuta konzumuje nárok na náhradu škody ve smyslu ustanovení § 2050 Občanského zákoníku.
2. V případě, že Poskytovatel nedodrží stanovenou lhůtu pro předání výstupů z plnění dle čl. 2 této Smlouvy v požadovaném termínu či požadovaném rozsahu, je povinen uhradit Objednateli smluvní pokutu ve výši 2 000 Kč (slovy: dva tisíce korun českých), a to za každý den prodlení, splatné do 14 kalendářních dnů ode dne doručení jejího vyúčtování Poskytovateli. Sjednaná smluvní pokuta konzumuje nárok na náhradu škody ve smyslu ustanovení § 2050 Občanského zákoníku.
3. V otázkách náhrady majetkové újmy (škody) a jiné újmy a odpovědnosti Poskytovatele či Objednatele za újmu (deliktní odpovědnost) Smluvní strany plně odkazují na úpravu Občanského zákoníku.

Článek 7

Další práva a povinnosti Poskytovatele a Objednatele

1. **Práva a povinnosti (závazky) Poskytovatele:**

   a) při plnění závazků ze Smlouvy postupovat s odbornou péčí (best practice) a dodržovat tuto Smlouvu, obecně závazné právní předpisy a technické normy vztahující se k předmětu plnění a v plném rozsahu hájit zájmy Objednatele;

   b) dodat předmět plnění v množství, vysoké jakosti, provedení a době, jež určuje tato Smlouva;

   c) respektovat pokyny Objednatele a upozornit Objednatele na případnou nevhodnost těchto pokynů;

   d) odpovídá Objednateli za dodržování vnitřních pokynů a směrnic Objednatele, které stanoví provozně technické a bezpečnostní podmínky pohybu osob v prostorách a pracovištích Objednatele (v místě plnění), se kterými byl Poskytovatel prokazatelně seznámen;

   e) je-li nutná součinnost Objednatele, určí mu Poskytovatel přiměřenou lhůtu k jejímu poskytnutí. Uplyne-li lhůta marně, má Poskytovatel právo podle své volby si buď zajistit náhradní plnění na účet Objednatele, anebo, upozornil-li na to Objednatele, odstoupit od Smlouvy (§ 2591 Občanského zákoníku) a Objednatel je povinen Poskytovateli uhradit dosud v souvislosti s plněním Smlouvy vzniklé náklady, a to vše, nebude-li Smluvními stranami dohodnuto jinak;

   f) je oprávněn nahlížet do dokladů a dokumentace Objednatele, souvisejících s plněním této Smlouvy;

g) Poskytovatel si je vědom, že bude pracovat v real-time provozu a zavazuje se tomu přizpůsobit metody testování a provádět penetrační testy takovým způsobem, aby nad míru přiměřenou poměrům nenarušoval běžný rutinní provoz Objednatele, a oznámit v dostatečném předstihu písemně Objednateli záměr provádět v konkrétní době penetrační testování k realizaci této Smlouvy;

h) po ukončení plnění Smlouvy zničit na všech svých počítačových systémech záznamy o odhalených bezpečnostních slabinách Objednatele;

i) při realizaci této Smlouvy respektovat v nejvyšší možné míře povinnosti, které určuje zaměstnavateli ustanovení § 316 odst. 2 zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, zejména tedy Poskytovatel nebude zaměstnance Objednatele podrobovat otevřenému či skrytému sledování, odposlechu a záznamu jejich telefonických hovorů, kontrole elektronické pošty nebo kontrole listovních zásilek adresovaných zaměstnanci. Bude-li při plnění této Smlouvy Objednatel požadovat od Poskytovatele postup v rozporu s nadepsaným textem tohoto odstavce, musí tak učinit písemně a Objednatel se výslovně vzdává práva na náhradu škody vůči Poskytovateli, pokud mu taková škoda z tohoto důvodu vznikne. Poskytovatel je oprávněn takový pokyn Objednatele odmítnout.

2. **Práva a povinnosti (závazky) Objednatele:**

a) poskytnout Poskytovateli Poskytovatelem vyžádanou součinnost, zejména mu poskytnout informace o skutečnostech, které potřebuje k plnění Smlouvy;

b) zajistit seznámení pracovníků Poskytovatele s předpisy, které stanoví provozně technické a bezpečnostní podmínky pohybu osob v prostorách a pracovištích objednatele (v místě plnění);

c) umožnit pracovníkům Poskytovatele přístup do prostor místa plnění po dobu plnění Smlouvy.

Článek 8

Ukončení Smlouvy

1. Smlouva se uzavírá na dobu určitou, a to na 56 měsíců ode dne uzavření Smlouvy nebo do vyčerpání částky 10 000 000,00 Kč bez DPH.

2. Smluvní vztah založený touto Smlouvou lze ukončit před uplynutím doby uvedené v předchozím odstavci tohoto článku písemnou dohodou Smluvních stran či jinými způsoby stanovenými českým právním řádem.

3. Aniž by bylo dotčeno právo Objednatele odstoupit od této Smlouvy ze zákonných důvodů, je Objednatel oprávněn odstoupit od této Smlouvy v případě, že:

a) bylo rozhodnuto o likvidaci Poskytovatele,

b) probíhá insolvenční řízení proti majetku Poskytovatele, v němž bylo vydáno pravomocné rozhodnutí o úpadku či insolvenční návrh byl zamítnut, protože majetek Poskytovatele nepostačuje k úhradě nákladů insolvenčního řízení, nebo byl konkurs zrušen, protože majetek Poskytovatele byl zcela nepostačující nebo bylo vydáno jiné rozhodnutí s obdobnými účinky ve vztahu k Poskytovateli,

c) bylo pravomocně rozhodnuto o exekuci na majetek Poskytovatele, nebo bude vydáno jiné rozhodnutí s obdobnými účinky ve vztahu k Poskytovateli,

d) zjistí, že Poskytovatel porušuje svou povinnost ze Smlouvy a Poskytovatel ani v přiměřené době dle ustanovení § 2593 Občanského zákoníku neučiní nápravu, pokud by postup Poskytovatele nepochybně vedl k podstatnému porušení této Smlouvy,

e) prodlení Poskytovatele se zahájením plnění je delší než 10 (deset) kalendářních dnů po sjednané době, jde-li o prodlení z důvodů na straně Poskytovatele,

f) Poskytovatel při provádění plnění nedodržuje obecně závazné právní předpisy či vnitřní předpisy Objednatele, zejména předpisy upravující bezpečnost a ochranu zdraví při práci, požární bezpečnost atd.

4. Aniž by bylo dotčeno právo Poskytovatele odstoupit od této Smlouvy ze zákonných důvodů, je Poskytovatel oprávněn odstoupit od této Smlouvy v případě, že:

   a) prodlení Objednatele s plněním závazku zaplatit Poskytovateli oprávněně vyúčtovanou cenu za plnění Smlouvy je delší než 30 (třicet) kalendářních dnů po splatnosti ceny.

5. Odstupující projev každé Smluvní strany musí být proveden v písemné formě a musí v něm být uveden odkaz na ustanovení této Smlouvy či právních předpisů, které zakládá oprávnění od Smlouvy odstoupit. Odstoupení je účinné dnem jeho doručení druhé Smluvní straně.

6. Plnila-li Smluvní strana (dlužník) zčásti, může druhá Strana (věřitel) od Smlouvy odstoupit jen ohledně nesplněného zbytku plnění. Nemá-li však částečné plnění pro věřitele význam, může věřitel od Smlouvy odstoupit ohledně celého plnění.

7. Uplynutím doby trvání této Smlouvy, odstoupením od ní či jiným oprávněným ukončením smluvního vztahu založeného touto Smlouvou nejsou dotčena práva na zaplacení smluvní pokuty nebo úroku z prodlení, pokud již dospěl, práva na náhradu škody vzniklé z porušení smluvní povinnosti, na jejíž porušení se nevztahuje ujednání o smluvní pokutě, ujednání o ochraně informací a mlčenlivosti a ani ujednání, která mají vzhledem ke své povaze zavazovat Smluvní strany i po odstoupení od Smlouvy, zejména ujednání o způsobu řešení sporů.

8. V ostatním ohledně odstoupení Strany odkazují na ustanovení Občanského zákoníku, není-li v této Smlouvě platně upraveno jinak.

Článek 9

Ochrana informací a povinnost mlčenlivosti

1. Obě Smluvní strany se zavazují chránit svá práva a povinnosti vyplývající ze Smlouvy před třetími osobami a zdržet se jednání, která by jakýmkoli způsobem poškozovala zájmy druhé Smluvní strany. Smluvní strany berou na vědomí a prohlašují, že obchodní, ekonomické, technické a personální informace, které si vzájemně poskytnou v rámci plnění Smlouvy, jsou ve smyslu Občanského zákoníku důvěrné a mohou být použity pouze v souladu se Smlouvou a toliko za účelem jejího plnění.

2. Veškeré důvěrné informace zůstávají výhradním vlastnictvím Objednatele a Poskytovatel vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o jeho vlastní důvěrné informace. S výjimkou rozsahu, který je nezbytný pro plnění této Smlouvy, se obě Smluvní strany zavazují neduplikovat žádným způsobem důvěrné informace druhé Smluvní strany, nepředat je třetí straně ani svým vlastním zaměstnancům a zástupcům s výjimkou těch, kteří s nimi potřebují být seznámeni, aby mohli plnit tuto Smlouvu. Obě Smluvní strany se zároveň zavazují nepoužít důvěrné informace druhé Smluvní strany jinak než za účelem plnění této Smlouvy.

3. Obě Smluvní strany se zavazují udržovat v tajnosti a nezpřístupnit třetím osobám důvěrné informace druhé Smluvní strany bez jejího souhlasu, a že podniknou všechny nutné kroky k zabezpečení těchto informací proti jejich zneužití; za tím účelem (1) Objednatel zejména zajistí:

   a) aby jeho zaměstnanci (a ostatní spolupracující osoby) byli řádně poučeni o povinnosti mlčenlivosti a možných následcích pro případ porušení této povinnosti,

   b) aby písemnosti a jiné hmotné nosiče důvěrných informací Poskytovatele, nutné při plnění této Smlouvy a nutné pro její plnění, byly uchovávány jen v zamykatelných prostorách a v zamykatelných bezpečných skříních nebo trezorech,

   c) zajistí, aby elektronické datové soubory Poskytovatele, obsahující důvěrné informace, nutné při plnění této Smlouvy a nutné pro její plnění, byly ponechány v paměti počítače Objednatele pouze tehdy, je-li přístup k takovým souborům a k užití počítače chráněn vhodnými bezpečnostními opatřeními, nejméně heslem.

   Stejně tak (2) Poskytovatel zejména zajistí:

   a) aby jeho zaměstnanci (a ostatní spolupracující osoby) byli řádně poučeni o povinnosti mlčenlivosti a možných následcích pro případ porušení této povinnosti,

   b) aby písemnosti a jiné hmotné nosiče důvěrných informací Objednatele, nutné při plnění této Smlouvy a nutné pro její plnění, byly uchovávány jen v zamykatelných prostorách a v zamykatelných bezpečných skříních nebo trezorech,

   c) aby elektronické datové soubory Objednatele, obsahující důvěrné informace, nutné při plnění této Smlouvy a nutné pro její plnění, byly ponechány v paměti počítače poskytovatele pouze tehdy,

je-li přístup k takovým souborům a k užití počítače chráněn vhodnými bezpečnostními opatřeními, nejméně heslem.

4. Za důvěrné se považují zejména následující informace:

   a) informace poskytnuté Objednatelem Poskytovateli v souvislosti s touto Smlouvou,

   b) veškeré skutečnosti obchodní, ekonomické, technické a personální povahy, související se Smluvními stranami, které nejsou běžně dostupné v obchodních nebo technických kruzích a se kterými se Smluvní strany seznámí při plnění předmětu této Smlouvy nebo v souvislosti s ní,

   c) informace, na které se vztahuje zákonem uložená povinnost mlčenlivosti Objednatele, na niž objednatel upozornil Poskytovatele,

   d) veškeré další informace, které budou Objednatelem či Poskytovatelem označeny jako důvěrné.

5. Povinnost zachovávat mlčenlivost, uvedená v tomto článku Smlouvy, se nevztahuje na informace:

   a) které mohou být zveřejněny bez porušení této Smlouvy,

   b) které byly předchozím písemným souhlasem obou Stran uvolněny ke zveřejnění,

   c) které jsou nebo se stanou všeobecně a veřejně přístupnými jinak, než porušením právních povinností ze strany Poskytovatele nebo Objednatele,

   d) u nichž je Poskytovatel schopen prokázat, že mu byly známy ještě před přijetím těchto informací od Objednatele, to však za podmínky, že se na tyto informace nevztahuje povinnost mlčenlivosti z jiných důvodů,

   e) které jsou vyžádány soudem, státním zastupitelstvím či příslušným správním orgánem na základě zákona,

   f) které Smluvní strana sdělí osobě vázané zákonnou povinností mlčenlivosti (např. advokátovi nebo daňovému poradci) za účelem uplatnění svých práv,

   g) jejichž sdělení se vyžaduje ze zákona.

6. Jako s důvěrnými musí být nakládáno i s informacemi, které splňují podmínky odstavce 4 shora, i když byly získány náhodně nebo bez vědomí Objednatele, není-li v této Smlouvě stanoveno jinak, a dále veškeré informace získané od třetí osoby, pokud se týkají Objednatele či plnění této Smlouvy, není-li v této Smlouvě stanoveno jinak.

7. Je-li pro účely kontroly vlastností plnění, odstranění vady nezbytné poskytnout Poskytovateli kopii databází, souborů nebo nosičů dat, obsahujících jakékoliv údaje z činnosti Objednatele nebo jím určených osob, je Poskytovatel povinen s takovými údaji nakládat jako s důvěrnými informacemi a zajistit, aby nedošlo k jejich úniku nebo zneužití.

8. Povinnost ochrany důvěrných informací a mlčenlivosti trvá bez ohledu na ukončení této Smlouvy. Závazky plynoucí z tohoto článku není Poskytovatel oprávněn vypovědět, ani jiným způsobem jednostranně ukončit a tyto trvají i po případném odstoupení od této Smlouvy nebo jiném jejím zániku.
9. Při porušení nadepsaných povinností ochrany informací a mlčenlivosti jsou Smluvní strany povinny nahradit si způsobenou škodu v plné výši.
10. Poruší-li Poskytovatel povinnosti vyplývající z této Smlouvy ohledně ochrany důvěrných informací, je povinen zaplatit Objednateli smluvní pokutu ve výši 100 000,- Kč za každé takové porušení povinnosti.

Článek 10

Ostatní a závěrečná ujednání

1. Případné spory obou Stran se budou řešit přednostně dohodou. Nedojde-li k dohodě, rozhodne věcně a místně příslušný soud České republiky dle českého práva. Je sjednána místní příslušnost věcně příslušného soudu České republiky, a to dle místa sídla Objednatele.
2. Obě Smluvní strany, při znalosti svých hospodářských a právních poměrů prohlašují, že nejsou slabší smluvní stranou ve smyslu Občanského zákoníku a jsou podnikateli ve smyslu platné právní úpravy.
3. Obě Smluvní strany prohlašují, že se měly možnost seznámit se všemi doložkami a přílohami odkazujícími mimo vlastní text Smlouvy a s jejich významem.
4. Smluvní strany vylučují možnost postoupení práv a povinností z této Smlouvy na třetí osobu bez předchozího písemného souhlasu druhé Smluvní strany (§ 1895 Občanského zákoníku).
5. Smluvní strany si sjednávají, že jakoukoli vzájemnou pohledávku Smluvních stran, která jim vyplývá z této Smlouvy, lze postoupit na třetí osobu, nebo ji jinak právně zatížit, pouze s předchozím písemným souhlasem Strany, vůči níž pohledávka směřuje a za předpokladu, že postoupení nebo právnímu zatížení nebrání zákon. Nedostatek předchozího písemného souhlasu k postoupení pohledávky považují Smluvní strany za vyloučení možnosti postoupit pohledávku (§ 1881 odst. 1 Občanského zákoníku).
6. Vyskytnou-li se události, které jednomu nebo oběma Stranám částečně nebo úplně znemožní plnění jejich povinností podle Smlouvy, jsou povinni se o tom bez zbytečného prodlení informovat a společně podniknout kroky k jejich překonání.
7. Tato Smlouva může být měněna a doplňována pouze písemně, formou písemných číslovaných dodatků podepsaných oběma Smluvními stranami. Tím je vyloučena možnost měnit obsah této Smlouvy v jiné formě (§ 564 Občanského zákoníku). K písemným návrhům na změnu této Smlouvy se Strany zavazují vyjádřit písemně ve lhůtě 15 dnů od doručení návrhu na změnu (návrhu dodatku) Smlouvy druhé Straně. Po tuto dobu je tímto návrhem vázána Strana, která návrh dodatku doručila. Novou přílohu Smlouvy lze vložit pouze formou písemného číslovaného dodatku Smlouvy, kterým se zruší dosavadní platná příloha a vloží se příloha nová.

8. Doručování: právní jednání v písemné formě působí vůči nepřítomné osobě (nastávají účinky doručení ve smyslu této Smlouvy) od okamžiku, kdy jí projev vůle Smluvní strany dojde, tedy jakmile *se dostane do sféry jeho dispozice, tzn. v okamžiku, kdy adresát nabude objektivní možnost seznámit se s obsahem projevu vůle druhé Smluvní strany.* Doručeno je i v případě, zmaří-li vědomě druhá Strana dojití; v takovém případě došel projev vůle řádně. Vědomým zmařením doručení ve smyslu ustanovení § 570 Občanského zákoníku se rozumí i porušení notifikační povinnosti Smluvní strany oznámit druhé Smluvní straně změnu své doručovací adresy.

9. Pokud oddělitelné ustanovení této Smlouvy je nebo se stane neplatným či nevynutitelným, nemá to vliv na platnost zbývajících ustanovení této Smlouvy. V takovém případě se Strany této Smlouvy zavazují uzavřít do 10 (deseti) pracovních dnů od výzvy druhé ze Stran této Smlouvy dodatek k této Smlouvě nahrazující oddělitelné ustanovení této Smlouvy, které je neplatné či nevynutitelné, platným a vynutitelným ustanovením odpovídajícím hospodářskému účelu takto nahrazovaného ustanovení.

10. Vše, co bylo dohodnuto před uzavřením Smlouvy, je právně irelevantní a mezi stranami platí jen to, co je dohodnuto ve Smlouvě.

11. Smluvní strany výslovně vylučují dispozitivní úpravu Občanského zákoníku tam, kde je v této Smlouvě sjednáno oproti úpravě Občanského zákoníku jinak. Práva a povinnosti výslovně touto Smlouvou neupravené se řídí příslušnými ustanoveními Občanského zákoníku. Smluvní strany se dohodly, že pro závazkový vztah z této Smlouvy vylučují použití těchto ustanovení Občanského zákoníku: § 558 odst. 2, § 1978 odst. 2, § 2609, § 2610 odst. 2 a § 2611.

12. Odpověď Strany této Smlouvy ve smyslu ustanovení § 1740 odst. 3 Občanského zákoníku s dodatkem nebo odchylkou, která podstatně nemění podmínky nabídky, není přijetím nabídky nebo na uzavření této Smlouvy nebo její akceptací. Smluvní strany tímto ve smyslu § 1740 odst. 3 Občanského zákoníku předem vylučují pro účely této Smlouvy přijetí nabídky na uzavření Smlouvy (akceptaci nabídky) s dodatkem či odchylkou.

13. Tato Smlouva nabývá platnosti dnem jejího podpisu oběma Smluvními stranami a účinnosti dnem jejího zveřejnění v registru smluv ve smyslu zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů. Smluvní strany výslovně souhlasí s tím, aby tato Smlouva byla zveřejněna v registru smluv za podmínek citovaného zákona, přičemž zveřejnění zajistí Objednatel. Smluvní strany souhlasí se zveřejněním svých osobních údajů ve Smlouvě, která bude zveřejněna v registru smluv podle věty první.

14. Objednatel je na základě ustanovení § 2 písm. e) zákona č. 320/2001 Sb. o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly. Poskytovatel je v tomto případě povinen vykonat veškerou součinnost s finanční kontrolou.

15. Kontaktní osoby za Poskytovatele:

    a) Ing. Tomáš Přibyl, předseda představenstva, +420 603 527 283, tomas.pribyl@corpus.cz

    b) Mgr. Pavel Cvešpr, ředitel realizace, +420 603 868 819, pavel.cvespr@corpus.cz

16. Kontaktní osoby za Objednatele:

    a) ve věcech podpisu Smlouvy a předání výstupů: JUDr. Markéta Štalmachová, ředitelka odboru bezpečnosti, +420 778 707 560, marketa.stalmachova@praha.eu

    b) ve věcech technických: Ing. Jan Haleňák, vedoucí oddělení kybernetické bezpečnosti, +420 236 002 548, jan.halenak@praha.eu

17. Oprávnění zástupci Smluvních stran si tuto Smlouvu přečetli, prohlašují, že Smlouvě rozumí, že byla sepsána podle jejich pravé a svobodné vůle a na důkaz toho připojují své podpisy, a to i jako deklaraci svých platných jednatelských oprávnění.

Příloha č. 1 – Specifikace předmětu plnění

V Praze dne dle data el. podpisu

Poskytovatel:

Corpus Solutions a.s.
Ing. Tomáš Přibyl
předseda představenstva

V Praze dne dle data el. podpisu

Objednatel:

HLAVNÍ MĚSTO PRAHA
JUDr. Markéta Štalmachová
ředitelka odboru bezpečnosti Magistrátu hlavního města Prahy

Příloha č. 1 - Specifikace předmětu plnění

Analytické a konzultační služby zahrnují:

a) Podpora na analytické a konzultační práce související s provozem bezpečnostních technologií
b) Zajištění pravidelné revize bezpečnostních politik
c) Zajištění vstupů pro plánování posilování kybernetické bezpečnosti organizace
d) Konzultační práce k připravovaným projektům s cílem poskytnout odborné stanovisko k dané problematice
e) Tvorba bezpečnostních případů užití
f) Zajištění správy bezpečnostních výjimek vůči schválenému designu organizace
g) Revize účinnosti detekce kybernetických hrozeb
h) Provedení penetračního testování odolnosti bezpečnostních mechanismů informačních systémů zadavatele
i) Provedení auditu bezpečnosti informačních systémů, či procesů nebo stavu informační bezpečnosti
j) Zajištění výkonu role architekta kybernetické bezpečnosti v souladu s požadavky vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti
k) Další konzultační a analytické služby dle požadavků zadavatele

Detailní popis jednotlivých služeb

a) Podpora na analytické a konzultační práce související s provozem bezpečnostních technologií

Služba zahrnuje:

- Analytické a konzultační práce pro oblast firewallů externího perimetru
- Analytické a konzultační práce pro oblast firewallů interního perimetru
- Analytické a konzultační práce pro oblast multidoménového managementu firewallů
- Analytické a konzultační práce pro oblast centrálního managementu pro ochranu koncových stanic
- Analytické a konzultační práce pro oblast boxů pro ochranu proti pokročilým kybernetickým hrozbám.
- Analytické a konzultační práce pro oblast perimetru aplikačních balancerů
- Analytické a konzultační práce pro oblast perimetru aplikačních firewallů
- Analytické a konzultační práce pro oblast technologie pro zajištění DNS ochrany
- Analytické a konzultační práce pro oblast technologie pro zajištění DDoS ochrany
- Analytické a konzultační práce pro oblast vyhodnocování dopadů zranitelnsotí
- Analytické a konzultační práce pro oblast aktiv v síti, jejich komunikací a vizualizace především se zaměřením na významné informační systémy
- Analytické a konzultační práce pro ADR a EDR

Služba bude poskytována nad technologiemi výrobců:

- Check Point
- F5
- Fidelis
- Rapid 7
- BVS

Plnění služby předpokládá expertní znalost využívaných technologií. Je nutná certifikace:

- Check Point na úrovni CCSM (Check Point Certified Sesurity Master)
- F5-CTS, LTM (F5 Certified Technology Specialist, BIG-IP Local Traffice Manager Certificate
- Fidelis Elevate Network-Admin Training
- Fidelis Elevate Endpoint- Admin Training
- Rapid7 (InsightAppSec Certified, InsightVM Technical Certified)
- BVS Certifikát
- CSSLP – Certified Secure Software Lifecycle Professional
- CISSP – Certified Information Systems Security Professional

b) <u>Zajištění pravidelné revize bezpečnostních politik</u>

Služba zahrnuje minimálně 1x ročně:

- Aktualizace stávajících technických bezpečnostních politik s ohledem na platné bezpečnostní politiky v prostředí Magistrátu hlavního města Prahy
- Aktualizace stávajících technických bezpečnostních politik s ohledem na aktuální stav bezpečnostních technologií v prostředí Magistrátu hlavního města Prah
- Aktualizace stávajících technických bezpečnostních politik s ohledem na požadavky Zákona o kybernetické bezpečnosti a prováděcích vyhlášek

Plnění služby předpokládá expertní znalost využívaných technologií. Je nutná certifikace:

- CISSP – Certified Infromation Systems Security Professional
- PECB Certified ISO/IEC 27001 Lead Auditor
- OSCP – Offfenstive security Certified Professional

c) <u>Zajištění vstupů pro plánování posilování kybernetické bezpečnosti organizace</u>

Služba zahrnuje sběr podkladů vztahujících se k provozovaným bezpečnostním technologiím s cílem poskytnutí odborných informací důležitých pro plánování rozvoje kybernetické bezpečnosti. Jedná se především o:

- Rozpracování problematiky aplikační bezpečnosti
- Rozpracování problematiky zabezpečení cloudu
- Sledování informací od výrobců bezpečnostních technologií
- Konzultace k životnosti technologií
- Konzultace vztahující se k podpoře ze strany výrobců apod.

d) <u>Konzultační práce k připravovaným projektům s cílem poskytnout odborné stanovisko k dané problematice</u>

Služba zahrnuje analytické a konzultační práce zaměřené na identifikaci a přípravu nových projektů pro kybernetickou bezpečnost, posouzení konceptů a strategií, zejména s ohledem na zvyšování úrovně informační bezpečnosti zadavatele a obecně platnou právní úpravu, kterou je zadavatel se povinen řídit.

Obsahem služby je:

- Analýza vstupů
- Analýza trhu
- Srovnávací analýza možných řešení
- Realizace PoC
- Tvorba doporučení
- Tvorba vstupů pro zadání a poptávku služby

e) <u>Tvorba bezpečnostních příkladů užití</u>

Provedení analýzy prostředí zákazníka a identifikaci konkrétní sady klíčových aktiv a procesů, kterou je potřeba cíleně a efektivně chránit bezpečnostním monitoringem. Služba má identifikovat business rizika, potenciální kybernetické hrozby a vymezit doporučené bezpečnostní scénáře pro tým SOC (na základě mapování hrozeb na MITRE Att&ck techniky). Dodavatel bude vycházet z existujících dokumentů analýzy rizik a business impact analýzy.

Požadovaným rozsahem služby je:

- Specifikace primárních procesů, primárních i podpůrných aktiv na základě dostupných materiálů zákazníka (business impact analýza a analýza rizik). Specifikace vymezené sady aktiv, které mají pro zákazníka největší hodnotu, je předpokladem pro efektivní zacílení kybernetické obrany
- Identifikace relevantních kybernetických hrozeb ohrožujících primární aktiva, jejichž nedostupnost, narušení důvěrnosti nebo integrity může znamenat naplnění business rizika
- Určení vektorů útoku mířících na zranitelnosti aktiv (vektor, který může zneužít zranitelnosti aktiva)
- Odvození bezpečnostních scénářů tzv. USE-CASES. Tyto scénáře reagují na identifikovanou potřebu chránit vybraná aktiva proti určeným hrozbám a vektorům útoku

f) Zajištění správy bezpečnostních výjimek vůči schválenému designu organizace

Cílem konzultačních prací je především:

- Posuzování vhodnosti uplatnění výjimky
- Vypracování odborných doporučení
- Tvorba odborných stanovisek

g) Revize účinnosti detekce kybernetických hrozeb

Technické prověření schopnosti detekovat vybrané útočné techniky, díky simulaci jejich skutečných projevů v infrastruktuře. Díky simulaci budou v síti, nebo na určených koncových bodech vygenerovány takové příznaky kybernetického ohrožení, které jsou popsány ve frameworku MITRE ATT&CK. Pro každou simulovanou útočnou techniku se po jejím provedení zkontroluje, zda došlo k její detekci. Pokud nebude simulovaná technika přímo detekována, je prověřeno, zda jsou pro detekci alespoň zaznamenaná data (telemetrie), která je následně možné použít pro sestavení detekčních pravidel, nebo využít pro podporu vyšetřování.

Charakteristické vlastnosti:

› Neinvazivní simulace kybernetického ohrožení v prostředí zákazníka
› Vždy jsou využívány jen bezpečné vzorky kódu, které neobsahují nákazu
› Při simulaci jsou jednotlivé útočné techniky řazeny do fází, jako by se prostředím šířil reálný útok
› Jednotlivé fáze mohou být časovány/zpomaleny, aby byla více navozena reálnost simulace
› Nejedná se o techniky penetračního testování, tudíž není cílem jakýkoli průnik
› Simulace zanechává v prostředí jasně zdokumentované artefakty, které je možné snadno odstranit, nebo zanechat pro případné cvičné vyšetřování

h) Provedení penetračního testování odolnosti bezpečnostních mechanismů informačních systémů zadavatele

Předmětem je provádění penetračních testů, jehož výsledkem je výstup v podobě písemné zprávy „Vyhodnocení penetračních testů“. Testy jsou prováděny se záměrem zjistit stav zabezpečení jednotlivých IS dle definovaných bezpečnostních mechanismů zadavatele. Rozsah a obsah testů bude vždy předmětem písemné dohody mezi zadavatelem a dodavatelem.

i) Provedení auditu bezpečnosti informačních systémů, či procesů nebo stavu informační bezpečnosti

Předmětem je audit prováděný k ověření plnění Technických bezpečnostních politik a vzhledem ke standardům platným pro oblast informační bezpečnosti či ochranu osobních údajů. Výstupem auditu bude podrobná písemná auditní zpráva.

Plnění služby předpokládá expertní znalost využívaných technologií. Je nutná certifikace:

- CISSP – Certified Infromation Systems Security Professional
- PECB – Certified ISO/IEC 27001 Lead Auditor
- OSCP – Offfenstive security Certified Professional

j) <u>Zajištění výkonu role architekta kybernetické bezpečnosti v souladu s požadavky vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti</u>

Zajištění činností vyplývajících z role architekta kybernetické bezpečnosti dle vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti, a dalších právních předpisů. Role architekta kybernetické bezpečnosti je bezpečnostní role odpovědná za zajištění návrhu implementace bezpečnostních opatření tak, aby byla zajištěna bezpečná architektura informačního a komunikačního systému. Plnění služby předpokládá expertní znalost využívaných technologií. Certifikace následujícího charakteru:

- Certified Secure Software Lifecycle Professional (CSSLP)
- Certified Information Systems Security Professional (CISSP)
- CompTIA Security +
- Certified Information Security Manager (CISM)
- Certified in Risk and Information Systems Control (CRISC)
- Manažer BI (akreditační schéma ČIA).

k) <u>Další konzultační a analytické služby dle požadavků zadavatele</u>

Předmětem služby je zajištění jiných výše nepopsaných služeb dle možností dodavatele vztahujícím se ke kybernetické bezpečnosti. Zejména poskytnutí odborného poradenství a konzultační činnosti, v oblasti informační bezpečnosti, včetně technických bezpečnostních aspektů konkrétních IT produktů a řešení, jejich implementací, prověření jejich funkčnosti a úrovně bezpečnosti s cílem zvyšování úrovně informační bezpečnosti zadavatele. Tyto služby nemusí být čerpány.