Stejnopis č.: 1.

MHMPP09M144R

SMLOUVA O DÍLO

Smluvní strany:

Hlavní město Praha

se sídlem: Praha – Staré Město, Mariánské náměstí 2/2, PSČ 11000

IČO: 00064581

DIČ: CZ00064581

bank. spojení: PPF banka, a.s.,

č. účtu: 27-0005157998/6000

zastoupené: Mgr. Jiří Károly, ředitelem Odboru informatických činností (OIC) MHMP

číslo Smlouvy Objednatele: DIL/40/03/003639/2022

(dále jen „**Objednatel**")

a

APPSEC s.r.o.

se sídlem: Thámova 166/18, Karlín, 186 00 Praha 8

IČO: 055 42 812 DIČ: CZ05542812

společnost zapsaná v obchodním rejstříku vedeném Městským soudem v Praze

oddíl C vložka 265478

bank. spojení: Raiffeisenbank, a. s., č. účtu: 1596002/5500

zastoupená: Adamem Pacltem, jednatelem

číslo Smlouvy Poskytovatele: **20022**

(dále jen „**Poskytovatel**")

(dále též společně jen „**Smluvní strany**")

dnešního dne uzavřely tuto smlouvu v souladu s § 1746 odst. 2 a § 2586 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**Občanský zákoník**")

(dále jen „**Smlouva**")

Smluvní strany, vědomy si svých závazků v této Smlouvě obsažených a s úmyslem být touto Smlouvou vázány, dohodly se na následujícím znění Smlouvy:

PREAMBULE

(A) Objednatel se rozhodl provést preventivní test zabezpečení své IT infrastruktury – bezpečnostní audit (dále jen „**Projekt**"), a to v souladu s podmínkami uvedenými v této Smlouvě.

(B) Objednatel se rozhodl realizovat Projekt prostřednictvím Poskytovatele a Poskytovatel je ochoten se na realizaci podílet v souladu s podmínkami stanovenými v této Smlouvě.

(C) Poskytovatel je odborníkem v oboru informačních technologií a je proto připraven plnit své povinnosti vyplývající ze Smlouvy řádně a včas a realizovat předmět Projektu v souladu s principy „*best practice*" dle svého nejlepšího vědomí, ve prospěch Objednatele a s ohledem na hospodárné nakládání s finančními prostředky Objednatele.

(D) Smluvní strany uzavírají tuto Smlouvu za účelem plnění Projektu.

1. ÚVODNÍ USTANOVENÍ

1.1 Objednatel prohlašuje, že:

1.1.1 je veřejnoprávní korporací; a

1.1.2 splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené.

1.2 Poskytovatel prohlašuje, že:

1.2.1 je právnickou osobou řádně založenou a existující podle právního řádu České republiky;

1.2.2 splňuje veškeré podmínky a požadavky v této Smlouvě stanovené a je oprávněn tuto Smlouvu uzavřít a řádně plnit závazky v ní obsažené;

1.2.3 disponuje veškerými profesními znalostmi, dovednostmi a kapacitou k řádnému splnění předmětu Projektu, a že všechny osoby, které použije k plnění této Smlouvy, mají potřebné vzdělání, zkušenosti či jinou profesní způsobilost k plnění, které má Poskytovatel dle této Smlouvy poskytovat. Poskytovatel se zavazuje Objednatele bezodkladně informovat o všech skutečnostech, které by vedly ke změně výše uvedeného prohlášení, stejně jako o dalších změnách v jeho kvalifikaci;

1.2.4 má zájem Projekt pro Objednatele řádně a včas plnit a splnit za úplatu sjednanou v této Smlouvě. Dále Poskytovatel prohlašuje, že se detailně seznámil s rozsahem a povahou předmětu Projektu, zejména že jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k jeho realizaci, těmto podmínkám rozumí a je schopný je dodržet; a

1.2.5 ke dni uzavření této Smlouvy vůči němu není vedeno řízení dle zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů a dle nejlepšího vědomí Poskytovatele ani takové řízení nehrozí, a zároveň se zavazuje Objednatele o všech skutečnostech o hrozícím úpadku bezodkladně informovat.

2. ÚČEL SMLOUVY

2.1 Účelem této Smlouvy je zajištění realizace předmětu Projektu, tj. zejména provést pro Objednatele bezpečnostní audit jeho IT infrastruktury za podmínek stanovených v této Smlouvě.

2.2 Poskytovatel touto Smlouvou garantuje a zavazuje se Objednateli ke splnění zadání Projektu. Tato garance je nadřazena ostatním podmínkám a garancím uvedeným v této Smlouvě. Pro vyloučení jakýchkoliv pochybností to znamená, že v případě jakékoliv nejistoty ohledně výkladu ustanovení této Smlouvy budou tato ustanovení vykládána tak, aby v co nejširší míře zohledňovala účel Projektu vyjádřený v nabídce Poskytovatele s názvem: *Nabídka na externí Blackhat analýzu pro HLAVNÍ MĚSTO PRAHA – Magistrát hlavního města Prahy* ze dne 14. 12. 2021, která je **Přílohou č. 1** této Smlouvy (dále jen „**Nabídka**").

3. PŘEDMĚT SMLOUVY

3.1 Předmětem této Smlouvy je povinnost Poskytovatele poskytovat Objednateli řádně a včas plnění sestávající zejména z:

3.1.1 provedení externího bezpečnostního auditu IT infrastruktury Objednatele podle metodiky Cyber Kill Chain doplněný o další testy z metodiky APPSEC (neboli Blackhat testování) za podmínek ve Smlouvě a Nabídce (dále jen „**Audit**");

3.1.2 provedení výstupní analýzy na základě Auditu, ve které bude detailně popsán celý průběh testování, včetně všech metodik, testovaných zranitelností a seznamu nálezů, včetně prezentace všech výsledků (dále jen „**Analýza**");

(Audit a Analýza společně jako „**Plnění**")

a tomu odpovídající povinnost Objednatele platit za řádně a včas poskytnuté Plnění dohodnutou cenu.

4. ZPŮSOB POSKYTOVÁNÍ PLNĚNÍ

4.1 Poskytovatel se zavazuje poskytovat Plnění vždy v souladu se Smlouvou a pokyny Objednatele.

4.2 Poskytovatel se zavazuje poskytovat Plnění tak, aby provedení jednotlivých výstupů Plnění této Smlouvy bylo dokončeno nejpozději do čtyřiceti pěti (45) dnů ode dne uzavření Smlouvy (tzn. ode dne podepsání Smlouvy oběma Smluvními stranami).

4.3 Poskytovatel je oprávněn Plnění provést a předat i v dřívějším termínu.

4.4 Objednatel se touto Smlouvou zavazuje poskytnout Poskytovateli nezbytnou součinnost při poskytování Plnění Poskytovatelem v rozsahu, který je vymezen v této Smlouvě.

4.5 Objednatel se zavazuje zaplatit Poskytovateli dohodnutou cenu za řádně a včas poskytnuté Plnění, to vše za podmínek dále stanovených touto Smlouvou.

4.6 Poskytovatel se zavazuje plnit Smlouvu prostřednictvím osob definovaných v **Příloze č. 2**, jež splňují minimální technické předpoklady kladené na příslušnou vykonávanou pozici (dále jen „**Realizační tým**"). Každý člen Realizačního týmu bude při plnění Smlouvy osobně vykonávat činnosti dle jejich odbornosti (kvalifikace) a v rozsahu, který takové pozici běžně odpovídá.

4.7 Činnosti, pro jejichž realizaci není nezbytná odbornost příslušných členů Realizačního týmu, je Poskytovatel oprávněn zabezpečit prostřednictvím dalších osob.

4.8 Každý člen Realizačního týmu se bude na plnění Smlouvy podílet po celou dobu trvání Smlouvy a v rozsahu dle své pozice uvedené v této Smlouvě.

4.9 Nebude-li se člen Realizačního týmu řádně podílet na poskytování Plnění v rozsahu stanoveném Smlouvou, např. v důsledku ukončení spolupráce s Poskytovatelem nebo její dlouhodobé absence (zejména dlouhodobá nemoc pravděpodobně překračující délku jednoho (1) měsíce), je Poskytovatel povinen neprodleně namísto člena Realizačního týmu zahájit poskytování Plnění náhradním členem Realizačního týmu, a nejpozději do tří (3) pracovních dnů ode dne, kdy taková situace nastala, informovat Objednatele o této skutečnosti.

4.10 Poskytovatel se zavazuje poskytovat Plnění dle této Smlouvy sám, nebo s využitím poddodavatelů uvedených v **Příloze č. 4** této Smlouvy. Jakákoliv dodatečná změna osoby poddodavatele nebo rozsahu Plnění svěřeného poddodavateli musí být předem písemně schválena Objednatelem, ledaže by Plnění původně svěřené poddodavateli realizoval Poskytovatel sám. Smluvní strany výslovně uvádějí, že při poskytování Plnění dle této Smlouvy prostřednictvím jakékoliv třetí osoby dle tohoto článku má Poskytovatel odpovědnost, jako by Plnění dle této Smlouvy poskytoval sám. Poskytovatel je rovněž povinen seznámit poddodavatele s právy a povinnostmi dle Smlouvy, zejména ve smyslu úpravy kybernetické bezpečnosti, které se týkají Poskytovatel je povinen do tří (3) dnů od doručení písemné výzvy Objednateli potvrdit a doložit, že kterákoliv konkrétní osoba podílející se na Plnění má

kvalifikaci a odbornost nezbytnou k tomu, aby se na poskytování příslušného Plnění podílela, a aby bylo Plnění poskytováno s řádnou a odbornou péčí.

4.11 Audit je prováděn za užití technického nástroje pro provádění standardizovaných penetračních testů dle metodik OWASP, PTES a OSSTMM zvané "JARVIS" (dále jen " **JARVIS**"). Mezi specifické činnosti JARVIS patří:

4.11.1 automatizované získávání informací o použitém softwaru, autorovi softwaru a provozovateli aplikace.

4.11.2 indexace zdrojových kódů.

4.11.3 predikce chyb konkrétních autorů softwaru ve zdrojových kódech na základě indexovaných zdrojových kódů starších verzí aplikace.

4.11.4 pokusy o automatizovanou exploitaci a průnik na úrovni aplikace, vnitřní infrastruktury a pracovních stanic.

4.11.5 audit hesel s automatickým porovnáním jejich podobnosti nebo shody ze známých a veřejných průniků.

4.11.6 vytěžování a strojová analýza dat pro potřebu následného reportu a průniku v rámci zadaného auditu.

4.12 JARVIS je poskytován jako služba (SaaS), kdy JARVIS je provozován na specializované neveřejné infrastruktuře lokalizované v České republice a zajišťované subdodavatelem Poskytovatele.

4.13 Objednatel prohlašuje, že je vlastníkem testovaného informačního systému či prvku infrastruktury a souhlasí s užitím JARVIS pro provedení jejich penetračních testů.

4.14 Objednatel je povinen specifikovat rozsahy IP adres, software a prvků infrastruktury Objednatele, které mají být předmětem testování a jejichž rozsah bude písemně schválen oprávněnou osobou Objednatele, kdy součástí takového schválení bude také prohlášení oprávněné osoby Objednatele o vlastnictví cílových IP adres, software a prvků infrastruktury, přičemž JARVIS bude použit pouze ve vztahu k těmto IP adresám, software a prvkům infrastruktury Objednatele. V případě jakýchkoli nedostatků žádosti či výskytu okolností nasvědčujících tomu, že užití JARVIS nebylo ze strany Objednatele schváleno či že Objednatel není vlastníkem testovaných IP adres, software nebo prvků infrastruktury, je Poskytovatel oprávněn kontaktovat Objednatele a až do získání jeho písemného souhlasu či prokázání vlastnictví k testovaným IP adresám, software a prvkům infrastruktury není povinen provádět Audit. Při neposkytnutí součinnosti Objednatele dle tohoto odstavce se prodlužuje lhůta pro poskytování Plnění, a to bez ohledu na ostatní ustanovení této Smlouvy.

4.15 Bez ohledu na ostatní ustanovení této Smlouvy na jejím základě nedochází k poskytnutí licence k software, který je užíván pro chod JARVIS jakožto platformy. Poskytovatel si vyhrazuje veškerá práva k JARVIS a software užívanému pro chod JARVIS, která nebyla udělena Objednateli podle této Smlouvy. Žádné ustanovení Smlouvy ani žádného jiného dokumentu nebude vykládáno jako udělení, postoupení nebo převedení na Objednatele jakýchkoli práv duševního vlastnictví k JARVIS a jeho výstupům, software užitému pro chod JARVIS, know-how, obchodnímu tajemství, dokumentům, technologickým postupům, patentům nebo odborným posudkům, které jsou ve vlastnictví Poskytovatele nebo které Poskytovatel využívá při poskytování Plnění dle této Smlouvy.

4.16 Objednatel není oprávněn kopírovat či analyzovat vnitřní nastavení, komponenty nebo skripty JARVIS, zkoumat či studovat vnitřní fungování JARVIS, pokoušet se získat přístup ke zdrojovému či strojovému kódu software, který je užíván pro chod JARVIS, přímo či prostřednictvím zpětné analýzy, ani se pokusit vytvořit na základě jakýchkoli informací o JARVIS podobné softwarové nástroje.

5. DOBA A MÍSTO PLNĚNÍ

5.1 Tato Smlouva se uzavírá se na dobu určitou, a to ode dne její účinnosti do řádného provedení Plnění, nejdéle však do 30. 6. 2022. Podrobnější harmonogram Plnění bude stanoven bez zbytečného odkladu dohodou Smluvních stran.

5.2 Hlavním místem plnění Smlouvy je území hlavního města Prahy. Konkrétním místem plnění bude lokalita, kde se nachází aktuální IT prostředí Objednatele vč. datových center Objednatele, dále sídlo Poskytovatele nebo jakékoliv jiné místo v České republice, k němuž se vztahuje či by se mohlo vztahovat poskytování Plnění dle této Smlouvy. Smluvní strany se dále dohodly, že místa plnění mohou být po dobu trvání této Smlouvy měněna také v souvislosti s novým IT prostředím Objednatele, přemístěním aktuálních prostor datových center či jejich částí apod. Pokud to povaha plnění této Smlouvy umožňuje a Objednatel vůči tomu nemá výhrady, je Poskytovatel oprávněn poskytovat Plnění dle této Smlouvy také vzdáleným přístupem.

6. PROVEDENÍ AUDITU

6.1 Poskytovatel je povinen na svůj náklad a nebezpečí provést pro Objednatele Audit, který musí mít vlastnosti v souladu s požadavky uvedenými v této Smlouvě a Nabídce.

6.2 Poskytovatel je povinen provést Audit se znalostí a péčí, která může být očekávána od Poskytovatele, který má veškeré dostupné požadované znalosti a nejnovější relevantní zkušenosti v oblasti ICT technologií a kyberbezpečnosti požadovaných pro provedení Plnění.

7. PROVEDENÍ ANALÝZY

7.1 Poskytovatel je povinen na svůj náklad a nebezpečí vytvořit, dodat a provést pro Objednatele Analýzu.

7.2 Analýza musí vycházet z Nabídky a představovat zejména úplný, jednoznačný a určitý podklad, který může být bez dalšího použit jako detailní popis průběhu testování, včetně všech metodik, testovaných zranitelností a seznamu nálezů, včetně prezentace všech výsledků Auditu, který bude dostatečně detailní, okomentovaný a srozumitelný pro jakoukoliv třetí osobu s odpovídající odbornou způsobilostí.

7.3 Výstupem provádění Analýzy je dokument nebo více dokumentů v českém jazyce v editovatelném elektronickém formátu a v needitovatelné elektronické kopii.

8. AKCEPTACE

8.1 Každý výstup poskytování Plnění bude Objednatelem akceptován na základě akceptační procedury; Plnění se považuje za akceptované po akceptaci všech jeho dílčích částí. Akceptační procedura zahrnuje ověření, zda je Plnění (jeho výstup) výsledkem, ke kterému se Poskytovatel zavázal, a to porovnáním skutečných vlastností Plnění s jejich závaznou specifikací uvedenou ve Smlouvě či jiném dohodnutém závazném dokumentu za využití akceptačních kritérií tam stanovených nebo později pro tento účel dohodnutých Smluvními stranami. Nebyla-li stanovena akceptační kritéria, platí, že se Smluvní strany dohodly na tom, že akceptačními kritérii budou jakékoliv podmínky a kritéria, která musí Plnění splňovat, aby Plnění mohlo plně sloužit svému účelu.

8.2 Objednatel je povinen vznést své výhrady nebo připomínky k Plnění do deseti (10) pracovních dnů ode dne jejich provedení. Vznese-li Objednatel výhrady nebo připomínky k Plnění, zavazuje se Poskytovatel do pěti (5) pracovních dnů provést veškeré potřebné úpravy Plnění dle výhrad a připomínek Objednatele a takto upravené Plnění předat Objednateli k akceptaci. Pokud výhrady a připomínky Objednatele přetrvávají nebo Objednatel identifikuje výhrady a připomínky nové, je Objednatel oprávněn postupovat podle tohoto čl. 8.2 Smlouvy i opakovaně.

8.3 V případě, že Objednatel nemá k Plnění (další) připomínky ani výhrady, zavazuje se ve lhůtě deseti (10) pracovních dnů od provedení Plnění akceptovat a potvrdit písemným akceptačním protokolem.

8.4 Bude-li trvání akceptační procedury ovlivněné vznesením výhrad nebo připomínek Objednatele k Plnění a potřebou jejich vyřešení, bude případné prodlení ve vztahu k dohodnutým termínům přičteno k tíži Poskytovatele.

9. DALŠÍ POVINNOSTI POSKYTOVATELE

9.1 Poskytovatel se dále zavazuje:

9.1.1 poskytovat Plnění podle této Smlouvy vlastním jménem, na vlastní odpovědnost a v souladu s pokyny Objednatele řádně a včas, zejména se zohledněním délky trvání akceptační procedury;

9.1.2 poskytovat Plnění podle této Smlouvy s péčí řádného hospodáře odpovídající podmínkám sjednaným v této Smlouvě; dostane-li se Poskytovatel do prodlení se svým Plněním bez toho, aby to způsobil Objednatel či překážky vylučující povinnost k náhradě újmy po dobu delší než třicet (30) dnů, je Objednatel oprávněn zabezpečit náhradní plnění po dobu prodlení Poskytovatele jinou osobou; v takovém případě se Poskytovatel zavazuje nahradit v plném rozsahu náklady spojené s náhradním plněním;

9.1.3 provést plnění, které není v této Smlouvě výslovně uvedeno, ale Poskytovatel jako odborník v oboru ví anebo by měl vědět, že je nezbytné anebo vhodné je provést;

9.1.4 upozorňovat Objednatele včas na všechny hrozící vady či výpadky svého Plnění, jakož i poskytovat Objednateli veškeré informace, které jsou pro plnění Smlouvy nezbytné;

9.1.5 neprodleně oznámit písemnou formou Objednateli překážky, které mu brání v plnění předmětu Smlouvy;

9.1.6 upozornit Objednatele na potenciální rizika vzniku újmy a včas a řádně dle svých možností provést taková opatření, která riziko vzniku újmy zcela vyloučí nebo sníží;

9.1.7 i bez pokynů Objednatele provést nutné úkony, které, ač nejsou předmětem této Smlouvy, budou s ohledem na nepředvídané okolnosti pro plnění Smlouvy nezbytné nebo jsou nezbytné pro zamezení vzniku újmy; jde-li o zamezení vzniku újmy nezapříčiněné Poskytovatelem, má Poskytovatel právo na úhradu nezbytných a účelně vynaložených nákladů;

9.1.8 postupovat při poskytování Plnění podle této Smlouvy s odbornou péčí a aplikovat procesy *„best practice"* vč. provedení Plnění, které není v této Smlouvě výslovně uvedeno, ale Poskytovatel jako odborník v oboru ví anebo by měl vědět, že je nezbytné anebo vhodné je provést;

9.1.9 v případě potřeby průběžně komunikovat s Objednatelem a třetími osobami, vyžaduje-li to řádné poskytování Plnění, přičemž veškerá taková komunikace bude probíhat v českém jazyce (případně slovenském, nebo za využití překladatele do českého jazyka hrazeného Poskytovatelem);

9.1.10 informovat Objednatele o plnění svých povinností podle této Smlouvy a o důležitých skutečnostech, které mohou mít vliv na výkon práv a plnění povinností Smluvních stran;

9.1.11 zabezpečit, aby všechny osoby podílející se na plnění jeho závazků z této Smlouvy, které se budou zdržovat v prostorách nebo na pracovištích Objednatele, dodržovaly účinné právní předpisy o bezpečnosti a ochraně zdraví při práci a veškeré interní předpisy Objednatele, s nimiž Objednatel Poskytovatele obeznámil;

9.1.12 chránit osobní údaje, data a duševní vlastnictví Objednatele a třetích osob;

9.1.13 upozorňovat Objednatele v odůvodněných případech na případnou nevhodnost pokynů Objednatele;

9.1.14 dodržovat obecně závazné právní předpisy; a

9.1.15 dodržovat ICT standardy Objednatele, jejichž seznam tvoří **Přílohu č. 5** této Smlouvy vč. jejich případných aktualizací a další dokumentace nahrazující ICT standardy Objednatele uvedené v **Příloze č. 5** této Smlouvy.

9.2 Poskytovatel je dále povinen:

9.2.1 poskytnout součinnost při realizaci auditu Poskytovatele Objednatelem dle relevantních právních předpisů o kybernetické bezpečnosti, zejména dle 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 jen „**VKB**");

9.2.2 informovat Objednatele o výskytu bezpečnostních incidentů dle VKB;

9.2.3 informovat Objednatele o rizicích Plnění a jejich řízení ze strany Poskytovatele; a

9.2.4 informovat Objednatele o významné změně ovládání Poskytovatele nebo změně vlastnictví zásadních aktiv, popřípadě změně oprávnění nakládat s těmito aktivy (dále jen „**Změna kontroly Poskytovatele**"). Ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních společnostech a družstvech (zákon o obchodních korporacích), či ekvivalentní postavení, dle VKB. Poskytovatel je povinen nechat si předem schválit Změnu kontroly poskytovatele Objednatelem. Porušení této povinnosti se považuje za podstatné porušení Smlouvy.

9.3 Všechna data a (případně i jejich hmotné nosiče) předaná Objednatelem Poskytovateli jsou výlučným vlastnictvím Objednatele. Nejpozději do patnácti (15) pracovních dnů od doručení žádosti Objednatele nebo od ukončení této Smlouvy je Poskytovatel povinen tato data a jejich nosiče Objednateli předat. Poskytovatel není oprávněn použít podklady, data a hmotné nosiče předané mu Objednatelem dle této Smlouvy pro jiné účely, než je poskytování Plnění podle této Smlouvy.

9.4 Poskytovatel se dále zavazuje udržovat v platnosti a účinnosti po celou dobu účinnosti Smlouvy pojistnou smlouvu, jejímž předmětem je pojištění odpovědnosti za újmu způsobenou Poskytovatelem třetí osobě (zejména Objednateli), a to tak, že limit pojistného plnění vyplývající z pojistné smlouvy, nesmí být nižší než 5.000.000,- Kč za rok. Pojistnou smlouvu dle tohoto článku, pojistku potvrzující uzavření takové smlouvy nebo pojistný certifikát potvrzující uzavření takové smlouvy je Poskytovatel povinen předložit Objednateli nejpozději do deseti (10) pracovních dnů po uzavření této Smlouvy a dále kdykoliv bezodkladně po písemném vyžádání Objednatele. Nepředložením pojistné smlouvy, pojistky nebo pojistného certifikátu do (10) pracovních dnů po uzavření Smlouvy nebo do jednoho (1) měsíce po vyžádání ze strany Objednatele vzniká Objednateli právo na odstoupení od Smlouvy.

9.5 Poskytovatel se zavazuje po celou dobu trvání smluvního poměru založeného touto Smlouvou zabezpečit dodržování veškerých právních předpisů, zejména pak pracovněprávních (odměňování, pracovní doba, doba odpočinku mezi směnami, placené přesčasy), dále předpisů týkajících se oblasti zaměstnanosti a bezpečnosti a ochrany zdraví při práci, tj. zejména zákona č. 435/2004 Sb., o zaměstnanosti, ve znění pozdějších předpisů, a zákona č. 262/2006 Sb., zákoník práce, ve znění pozdějších předpisů, a to vůči všem osobám, které se na Plnění podílejí (a bez ohledu na to, zda budou činnosti prováděny Poskytovatelem či jeho poddodavateli). Poskytovatel se také zavazuje zabezpečit, že všechny osoby, které se na plnění Veřejné zakázky podílejí (a bez ohledu na to, zda budou činnosti prováděny Poskytovatelem či jeho poddodavateli), jsou vedeny v příslušných registrech, jako například v registru pojištěnců ČSSZ, a mají příslušná povolení k pobytu v ČR.

10. CENA A PLATEBNÍ PODMÍNKY

10.1 Cena za provedení Plnění je dohodou Smluvních stran stanovena ve výši **400 000, - Kč bez DPH** (slovy: čtyři sta tisíc korun českých). K ceně za provedení Plnění bude Poskytovatelem připočtena daň z přidané hodnoty (dále jen „**DPH**") v zákonné výši ke dni uskutečnění zdanitelného plnění. Tato cena je pevná a úplná a nejvýše přípustná, tj. zahrnuje veškerá Plnění dle Smlouvy, odměnu za poskytnutí, zprostředkování nebo postoupení oprávnění dle čl. 11

Smlouvy, jakož i výdaje a náklady, které Poskytovateli v souvislosti s poskytováním Plnění vzniknou či mohou vzniknout.

10.2 Cena za Plnění bude Objednatelem uhrazena na základě faktury vystavené Poskytovatelem a doručené Objednateli do pěti (5) dnů ode dne akceptace Plnění jako celku (všech jeho výstupů) dle čl. 8 Smlouvy. Přílohou faktury musí být kopie akceptačních protokolů.

10.3 Doba splatnosti jednotlivých plateb dle této Smlouvy je stanovena na třicet (30) dní od doručení faktury Objednateli. Připadne-li termín splatnosti na den, který není pracovním dnem, posouvá se termín splatnosti na nejbližší následující pracovní den. Ke splnění dluhu Objednatele dojde odepsáním částky z účtu Objednatele ve prospěch účtu Poskytovatele uvedeného na faktuře. Za datum uskutečnění zdanitelného plnění (DUZP) se považuje datum podepsání akceptačního protokolu.

10.4 Všechny faktury musí splňovat všechny náležitosti daňového dokladu požadované zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „**Zákon o DPH**") a Občanským zákoníkem, avšak výslovně vždy musí obsahovat následující údaje: označení Smluvních stran a jejich adresy, jejich IČO a DIČ, údaj o tom, že vystavovatel faktury je zapsán v obchodním rejstříku včetně spisové značky, označení této Smlouvy, označení poskytnutého Plnění, číslo faktury, den vystavení a doba splatnosti faktury, označení peněžního ústavu a číslo účtu, na který se má platit, fakturovanou částku, razítko a podpis oprávněné osoby.

10.5 Nebude-li faktura obsahovat stanovené náležitosti či přílohy, nebo v ní nebo jejích přílohách nebudou správně uvedené údaje dle této Smlouvy, je Objednatel oprávněn ji vrátit v době splatnosti faktury Poskytovateli, a to i opakovaně. V takovém případě se přeruší běh doby splatnosti a nová doba splatnosti počne běžet doručením opravené faktury s opravenými přílohami.

10.6 Platby se provádí bankovním převodem na účet druhé Smluvní strany uvedený ve faktuře.

10.7 Objednatel bude hradit přijaté faktury pouze na bankovní účty Poskytovatele zveřejněné správcem daně způsobem umožňujícím dálkový přístup ve smyslu § 96 odst. 2 Zákona o DPH.

10.8 Poskytovatel prohlašuje, že správce daně před uzavřením této Smlouvy nerozhodl, že Poskytovatel je nespolehlivým plátcem ve smyslu § 106a Zákona o DPH (dále jen „**Nespolehlivý plátce**"). V případě, že správce daně rozhodne o tom, že Poskytovatel je Nespolehlivým plátcem, zavazuje se Poskytovatel o tomto informovat Objednatele do dvou (2) pracovních dní.

10.9 Získá-li Poskytovatel v průběhu trvání závazkového vztahu založeného touto Smlouvou rozhodnutím správce daně status Nespolehlivého plátce anebo se Objednatel dozví o jiných skutečnostech rozhodných pro zákonné ručení Objednatele za odvod daně z přidané hodnoty ve smyslu § 109 Zákona o DPH, je Objednatel oprávněn uhradit daň z přidané hodnoty z provedeného plnění ve smyslu § 109a Zákona o DPH přímo příslušnému správci daně namísto Poskytovatele a následně je Objednatel oprávněn uhradit Poskytovateli cenu poníženou o takto zaplacenou daň, přičemž úhrada daně z přidané hodnoty se bude považovat za úhradu příslušné části ceny Poskytovateli. Poskytovatel je povinen na faktuře uvést účet zveřejněný správcem daně způsobem umožňujícím dálkový přístup ve smyslu § 109 odst. 2 písm. c) Zákona o DPH. Je-li na faktuře vystavené Poskytovatelem uveden jiný účet, než je účet stanovený v předchozí větě, je Objednatel oprávněn zaslat fakturu zpět Poskytovateli k opravě, kdy čl. 10.5 Smlouvy se užije obdobně. Poskytovatel prohlašuje, že je majitelem a beneficientem účtu uvedeného Objednateli dle tohoto čl. 10.9 Smlouvy, a to na základě smlouvy uzavřené s bankou se sídlem v České republice, jejíž je Poskytovatel účastníkem jako majitel účtu.

11. VLASTNICKÉ PRÁVO A UŽÍVACÍ PRÁVA

11.1 K výstupům poskytování Plnění, které jsou movitými věcmi a mají se stát vlastnictvím Objednatele (s výjimkou věcí uvedených v čl. 11.2 této Smlouvy), nabývá Objednatel vlastnické právo k těmto věcem dnem předání takového výstupu Plnění Objednateli.

11.2 Vzhledem k tomu, že Plnění může naplňovat znaky předmětů duševního vlastnictví chráněných zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů (dále jen „**Autorský zákon**"), je k těmto součástem Plnění poskytována licence za podmínek sjednaných dále v tomto článku Smlouvy.

11.3 Objednatel je oprávněn veškeré součásti výstupy Plnění Poskytovatele považované za předměty duševního vlastnictví ve smyslu Autorského zákona (dále jen „**Duševní vlastnictví**") užívat dle níže uvedených podmínek.

11.3.1 Objednatel je oprávněn od okamžiku účinnosti poskytnutí licence k autorskému dílu dle čl. 11.3.2 této Smlouvy užívat toto Duševní vlastnictví v rozsahu, v jakém uzná za nezbytné, vhodné či přiměřené. Pro vyloučení pochybností to znamená, že Objednatel je oprávněn užívat Duševní vlastnictví v původní podobě, v územním rozsahu pro Českou republiku, a v časovém rozsahu po dobu trvání majetkových práv příslušného předmětu Duševního vlastnictví (zejména práv autorských), a to všemi v úvahu přicházejícími způsoby a k jakémukoliv účelu (dále jen „**Licence**"). Licence je poskytována jako neomezená nevýhradní a Objednatel není povinen Licenci využít, a to ani zčásti.

11.3.2 Poskytovatel touto Smlouvou poskytuje Objednateli Licenci, přičemž účinnost této Licence nastává nejpozději okamžikem akceptace výsledku Plnění, který příslušné Duševní vlastnictví obsahuje; do té doby je Objednatel oprávněn Duševní vlastnictví užít v rozsahu a způsobem nezbytným k provedení akceptace příslušného výsledku Plnění.

11.3.3 Licence zahrnuje nevýhradní oprávnění Objednatele a osob oprávněných Objednatelem sdělovat Duševní vlastnictví veřejnosti pod jménem Poskytovatele, s čímž Poskytovatel výslovně souhlasí.

11.3.4 Udělení Licence nelze ze strany Poskytovatele vypovědět a její účinnost trvá i po skončení účinnosti této Smlouvy.

11.3.5 Poskytovatel výslovně souhlasí s postoupením (zcela anebo z části) Licence nebo poskytnutí oprávnění tvořících součást této Licence (podlicenci) zcela nebo zčásti jakékoliv třetí osobě podle volby Objednatele.

11.3.6 Poskytovatel je povinen postupovat tak, aby udělení Licence dle této Smlouvy včetně oprávnění udělit podlicenci a souvisejících oprávnění zabezpečil, a to bez újmy na právech třetích osob.

11.4 Práva získaná v rámci plnění této Smlouvy přechází i na případného právního nástupce Objednatele. Případná změna v osobě Poskytovatele (např. právní nástupnictví) nebude mít vliv na oprávnění udělená v rámci této Smlouvy Poskytovatelem Objednateli.

11.5 Odměna za poskytnutí, zprostředkování nebo postoupení oprávnění dle tohoto čl. 11 Smlouvy je zahrnuta v ceně dle čl. 10 Smlouvy. Bude-li z jakéhokoliv důvodu nezbytné nebo účelné určit výši odměny za poskytnutí oprávnění dle tohoto čl. 11 Smlouvy, pak se Smluvní strany zavazují vyčíslit výši této odměny bez zbytečného odkladu po doručení požadavku na toto vyčíslení druhé Smluvní straně a poskytnout si v tomto ohledu vzájemně veškerou potřebnou součinnost.

11.6 Licence dle této Smlouvy se použije v maximální možné míře přípustné českým právem nejen na Duševní vlastnictví, ale také na veškeré součásti poskytovaného Plnění, které jsou předmětem právní ochrany nehmotných statků, zejména na know-how, které Poskytovatel vytvoří v rámci nebo v souvislosti s plněním Smlouvy. Poskytovatel tak tímto uděluje Licenci rovněž k takovým předmětům práv k nehmotným statkům.

12. ZÁRUKA

12.1 Poskytovatel poskytuje záruku, že každá část výsledku Plnění dle této Smlouvy má ke dni její akceptace funkční vlastnosti stanovené touto Smlouvou, zejména Nabídkou, a je způsobilá k použití pro účely stanovené v této Smlouvě nebo v souladu s touto Smlouvou.

12.2 Poskytovatel poskytuje záruku za jakost každé jednotlivé části výsledku Plnění dle této Smlouvy od okamžiku její akceptace po dobu trvání této Smlouvy, nejméně však dvaceti čtyř (24) měsíců od akceptace výsledku Plnění dle této Smlouvy jako celku.

12.3 Objednatel je oprávněn závady výsledku Plnění nahlásit Poskytovateli kdykoli v průběhu záruční doby bez ohledu na to, kdy je zjistil, aniž by tím byla jeho práva ze záruky či práva z vad jakkoli dotčena.

12.4 Doba od zjištění závady do jejího odstranění se do trvání záruční doby nezapočítává.

12.5 Poskytovatel prohlašuje, že veškeré jeho Plnění poskytnuté/dodané podle této Smlouvy bude prosté právních vad a zavazuje se odškodnit v plné výši Objednatele v případě, že třetí osoba úspěšně uplatní autorskoprávní anebo jiný nárok plynoucí z právní vady poskytnutého Plnění. V případě, že by nárok třetí osoby vzniklý v souvislosti s Plněním Poskytovatele podle této Smlouvy, bez ohledu na jeho oprávněnost, vedl k dočasnému či trvalému soudnímu zákazu či omezení užívání Plnění či jeho části, zavazuje se Poskytovatel zabezpečit náhradní řešení a minimalizovat dopady takovéto situace, a to bez nároku na úplatu nad rámec ceny podle této Smlouvy, přičemž současně nebudou dotčeny ani nároky Objednatele na náhradu újmy.

12.6 Poskytovatel prohlašuje, že je oprávněn vykonávat svým jménem a na svůj účet majetková práva k Duševnímu vlastnictví, které bude součástí Plnění podle této Smlouvy, resp. že má souhlas všech relevantních osob k poskytnutí oprávnění podle čl. 11 této Smlouvy, případně je povinen tyto souhlasy zabezpečit; toto prohlášení zahrnuje i taková práva, která by vytvořením Duševního vlastnictví teprve vznikla.

13. OPRÁVNĚNÉ OSOBY

13.1 Každá ze Smluvních stran jmenuje oprávněnou osobu, popř. zástupce oprávněné osoby. Oprávněné osoby budou zastupovat Smluvní stranu ve smluvních, obchodních a technických záležitostech souvisejících s plněním této Smlouvy. Jména oprávněných osob jsou uvedena v **Příloze č. 3** této Smlouvy.

13.2 Smluvní strany jsou oprávněny změnit oprávněné osoby i bez nutnosti uzavřít dodatek k této Smlouvě, jsou však povinny na takovou změnu druhou Smluvní stranu písemně upozornit. Zmocnění zástupce oprávněné osoby musí být písemné s uvedením rozsahu zmocnění.

14. OCHRANA OSOBNÍCH ÚDAJŮ

14.1 S ohledem na předmět této Smlouvy Smluvní strany nepředpokládají, že bude Poskytovatel zpracovávat osobní údaje nebo zvláštní kategorie osobních údajů Objednatele. Smluvní strany budou při plnění této Smlouvy dodržovat veškeré platné právní předpisy v oblasti ochrany osobních údajů, zejména Nařízení GDPR. Pokud nastane taková zákonná povinnost, Smluvní strany se zavazují uzavřít příslušnou zpracovatelskou smlouvu.

15. OCHRANA DŮVĚRNÝCH INFORMACÍ

15.1 Smluvní strany jsou si vědomy toho, že v rámci plnění závazků z této Smlouvy:

15.1.1 si mohou vzájemně vědomě nebo opominutím poskytnout informace, které budou považovány za důvěrné (dále jen „**Důvěrné informace**"),

15.1.2 mohou jejich zaměstnanci a osoby v obdobném postavení získat vědomou činností druhé Smluvní strany nebo i jejím opominutím přístup k Důvěrným informacím druhé Smluvní strany.

15.2 Smluvní strany se zavazují, že žádná z nich nezpřístupní třetí osobě Důvěrné informace, které při plnění této Smlouvy získala od druhé Smluvní strany.

15.3 Za třetí osoby podle čl. 15.2 této Smlouvy se nepovažují:

15.3.1 zaměstnanci Smluvních stran a osoby v obdobném postavení,

15.3.2 orgány Smluvních stran a jejich členové,

15.3.3 ve vztahu k Důvěrným informacím Objednatele poddodavatelé Poskytovatele,

15.3.4 ve vztahu k Důvěrným informacím Poskytovatele externí dodavatelé Objednatele, a to i potenciální,

za předpokladu, že se podílejí na plnění této Smlouvy nebo na plnění spojeném s plněním dle této Smlouvy, Důvěrné informace jsou jim zpřístupněny výhradně za tímto účelem a zpřístupnění Důvěrných informací je v rozsahu nezbytně nutném pro naplnění jeho účelu a za stejných podmínek, jaké jsou stanoveny Smluvním stranám v této Smlouvě.

15.1 Veškeré informace poskytnuté Objednatelem Poskytovateli se považují za Důvěrné informace, není-li stanoveno jinak. Veškeré informace poskytnuté Poskytovatelem Objednateli se považují za Důvěrné informace, pouze pokud na jejich důvěrnost Poskytovatel Objednatele předem písemně upozornil a Objednatel Poskytovateli písemně potvrdil svůj závazek důvěrnost těchto informací zachovávat. Pokud jsou Důvěrné informace Poskytovatele poskytovány v písemné podobě anebo ve formě textových souborů na elektronických nosičích dat (médiích), je Poskytovatel povinen upozornit Objednatele na důvěrnost takového materiálu též jejím vyznačením alespoň na titulní stránce nebo přední straně média.

15.2 Smluvní strany se zavazují v plném rozsahu zachovávat povinnost mlčenlivosti a povinnost chránit Důvěrné informace vyplývající z této Smlouvy a též z příslušných právních předpisů, zejména povinnosti vyplývající z nařízení 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 (obecné nařízení o ochraně osobních údajů)(dále jen „**Nařízení GDPR**") a ze zákona č. 110/2019 Sb., o zpracování osobních údajů. Smluvní strany se v této souvislosti zavazují poučit veškeré osoby, které se na jejich straně budou podílet na plnění této Smlouvy, o výše uvedených povinnostech mlčenlivosti a ochrany Důvěrných informací a dále se zavazují vhodným způsobem zabezpečit dodržování těchto povinností všemi osobami podílejícími se na plnění této Smlouvy.

15.3 Veškeré Důvěrné informace zůstávají výhradním vlastnictvím předávající Smluvní strany a přijímající Smluvní strana vyvine pro zachování jejich důvěrnosti a pro jejich ochranu stejné úsilí, jako by se jednalo o její 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.

15.4 Bez ohledu na výše uvedená ustanovení se veškeré informace vztahující se k předmětu této Smlouvy a příslušné Dokumentaci považují výlučně za Důvěrné informace Objednatele a Poskytovatel je povinen tyto informace chránit v souladu s touto Smlouvou. Poskytovatel při tom bere na vědomí, že povinnost ochrany těchto informací podle tohoto článku se vztahuje pouze na Poskytovatele.

15.5 Za Důvěrné informace Objednatele se dále bezpodmínečně považují veškerá data, které IT infrastruktura Objednatele či její část obsahuje, i data, která z ní byla získána.

15.6 Bez ohledu na výše uvedená ustanovení se za důvěrné nepovažují informace, které:

15.6.1 se staly veřejně známými, aniž by jejich zveřejněním došlo k porušení závazků přijímající Smluvní strany či právních předpisů;

15.6.2 měla přijímající Smluvní strana prokazatelně legálně k dispozici před uzavřením této Smlouvy, pokud takové informace nebyly předmětem jiné, dříve mezi Smluvními stranami uzavřené smlouvy o ochraně informací;

15.6.3 jsou výsledkem postupu, při kterém k nim přijímající Smluvní strana dospěje nezávisle a je to schopna doložit svými záznamy nebo důvěrnými informacemi třetí strany;

15.6.4 po podpisu této Smlouvy poskytne přijímající Smluvní straně třetí osoba, jež není omezena v takovém nakládání s informacemi; a

15.6.5 je-li zpřístupnění informace vyžadováno zákonem či jiným právním předpisem včetně práva EU nebo závazným rozhodnutím oprávněného orgánu veřejné moci.

15.7 Za Důvěrné informace se ve smyslu čl. 15.6 Smlouvy zejména nepovažují:

15.7.1 ustanovení této Smlouvy včetně jejích příloh; a

15.7.2 výše ceny uhrazené za plnění dle této Smlouvy.

15.8 Za porušení povinnosti mlčenlivosti Smluvní stranou se považují též případy, kdy tuto povinnost poruší kterákoliv z osob uvedených v čl. 15.3 Smlouvy, které daná Smluvní strana poskytla Důvěrné informace druhé Smluvní strany.

15.9 Objednatel je dále výslovně oprávněn zpřístupnit jakékoliv výstupy poskytování Plnění (zejména Duševní vlastnictví a Dokumentaci) uživatelům či třetím osobám v rozsahu a způsoby vhodnými pro využití oprávnění dle čl. 11 Smlouvy. Takové zpřístupnění ze strany Objednatele není považováno za porušení jakýchkoli povinností Objednatele týkajících se Důvěrných informací či porušení obchodního tajemství Poskytovatele.

15.10 Ukončení účinnosti této Smlouvy z jakéhokoliv důvodu se nedotkne ustanovení tohoto článku Smlouvy a jejich účinnost včetně ustanovení o sankcích přetrvá bez omezení i po ukončení účinnosti této Smlouvy.

15.11 Poskytovatel neprodleně na žádost Objednatele, a vždy v případě zániku Smlouvy, vrátí Objednateli všechny písemné dokumenty obsahující Důvěrné informace a jakékoliv další materiály obsahující anebo odvozující jakékoliv Důvěrné informace a dále informace neveřejného charakteru; Poskytovatel rovněž zabezpečí, že totéž učiní všechny další osoby, kterým byly Důvěrné informace Poskytovatelem zpřístupněny. Poskytovatel se zavazuje, že si v takovém případě neponechá žádné kopie, výpisy anebo jiné celkové nebo částečné reprodukce či záznamy Důvěrných informací. Všechny dokumenty, memoranda, poznámky a ostatní písemnosti vyhotovené Poskytovatelem anebo jinými osobami na základě Důvěrných informací je Poskytovatel povinen bez zbytečného odkladu zničit. Poskytovatel se výslovně zavazuje zničit materiály uložené v počítačích, textových editorech anebo jiných zařízeních obsahujících Důvěrné informace. Toto zničení a odstranění materiálů bude Objednateli písemně potvrzeno vedoucím zaměstnancem Poskytovatele, který byl zničením a odstraněním materiálů pověřen.

16. KYBERNETICKÁ BEZPEČNOST

16.1 Není-li v této Smlouvě nebo v souladu s touto Smlouvou stanoveno jinak, Poskytovatel tímto bere na vědomí, že

16.1.1 Objednatel je správcem informačních systémů kritické informační infrastruktury dle § 3 písm. c) ZKB, správcem komunikačního systému kritické informační infrastruktury dle § 3 písm. d) ZKB a správcem významných informačních systémů dle § 3 písm. e) ZKB. Poskytovatel dále tímto bere na vědomí, že poskytnutí Plnění může být prováděno na podpůrných aktivech systémů kritické informační infrastruktury a aktivech významných informačních systému.

16.1.2 Objednatel chápe Poskytovatele jako významného dodavatele ve smyslu § 2 písm. n) a § 8 odst. 1 písm. f) a odst. 2 VKB.

16.2 Smluvní strany potvrzují, že rozsah zapojení Poskytovatele na zajištění bezpečnosti podpůrných aktiv informačních a komunikačních systémů kritické informační infrastruktury a podpůrných aktiv významných informačních systému je určen předmětem této Smlouvy.

16.3 Poskytovatel je povinen v rozsahu plnění této Smlouvy naplnit všechny bezpečnostní požadavky uvedené v **Příloze č. 6** této Smlouvy (dále jen „**Kybernetické požadavky**"), a to nejpozději od účinnosti Smlouvy.

16.4 Poskytovatel je povinen umožnit Objednateli alespoň jednou (1) ročně po dobu účinnosti této Smlouvy a následně také jeden (1) rok po ukončení trvání této Smlouvy provedení zákaznického auditu (kontroly):

16.4.1 jehož rozsah bude ohraničen využíváním ICT prostředků Poskytovatele pro potřeby plnění této Smlouvy a uloženými či zpracovávanými daty a informacemi Objednatele v ICT prostředí Poskytovatele; a

16.4.2 jehož předmětem bude naplnění Kybernetických požadavků a vyhodnocení rizik dle čl. 3 **Přílohy č. 6** této Smlouvy.

16.5 Objednatel je oprávněn při kontrole Kybernetických požadavků využít třetí stranu. V případě využití třetí strany bude Objednatel odpovídat za třetí stranu, jako by kontrolu prováděl sám, včetně odpovědnosti za způsobenou újmu.

16.6 Poskytovatel umožní Objednateli kontrolu Kybernetických požadavků provedenou prostředky Objednatele nebo třetí strany, a to v lokalitě Poskytovatele i vzdáleně, pokud to technické prostředky Poskytovatele umožňují.

16.7 Dále se Poskytovatel zavazuje nedostatky zjištěné:

a) na základě provedení hodnocení rizik dle čl. 3 **Přílohy č. 6** této Smlouvy; nebo

b) v rámci zákaznického auditu dle čl. 16.4 této Smlouvy,

odstranit ve lhůtě určené v písemném oznámení Objednatele. Nestanoví-li Objednatel lhůtu v písemném oznámení, zavazují se Smluvní strany dohodnout na lhůtě pro odstranění nedostatku, která nepřevýší devadesát (90) kalendářních dnů.

16.8 Článek 16.4 této Smlouvy se nepoužijí, pokud je Poskytovatel pro poskytování předmětu plnění orgánem nebo osobou uvedenou v § 3 písm. a) až g) ZKB.

16.9 Poskytovatel se nad rámec čl. 9 této Smlouvy také zavazuje:

16.9.1 poskytnout na vyžádání Objednateli dokumenty a obdobné vstupy, které budou prokazovat naplnění Kybernetických požadavků;

16.9.2 na požádání s Objednatelem konzultovat kdykoli v průběhu poskytování Plnění dle této Smlouvy detailní nastavení bezpečnostních opatření k naplnění Kybernetických požadavků a pro takovéto konzultace zabezpečit účast kvalifikovaných pracovníků;

16.9.3 neprodleně informovat Objednatele o všech významných změnách v naplnění Kybernetických požadavků, které nastanou kdykoli v průběhu trvání této Smlouvy;

16.9.4 bezodkladně a s vyvinutím nejlepšího úsilí zabezpečit náhradní způsob naplnění Kybernetických požadavků, pokud stávající řešení přestalo být funkční a efektivní;

16.9.5 bezodkladně informovat Objednatele o bezpečnostních incidentech, které mohou ovlivnit poskytování Plnění dle této Smlouvy; a

16.9.6 při výkonu své činnosti včas a prokazatelně upozornit Objednatele na zřejmou nevhodnost jeho příkazů či doporučení vztahující se ke Kybernetickým požadavkům a jejichž následkem může vzniknout újma nebo nesoulad se zákony nebo jinými obecně závaznými právními předpisy.

17. SOUČINNOST A VZÁJEMNÁ KOMUNIKACE

17.1 Smluvní strany se zavazují vzájemně spolupracovat a předávat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou Smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy.

17.2 Smluvní strany jsou povinny plnit své závazky vyplývající z této Smlouvy tak, aby nedocházelo k prodlení s plněním jednotlivých termínů a s prodlením splatnosti jednotlivých peněžních závazků.

17.3 Veškerá komunikace mezi Smluvními stranami bude probíhat prostřednictvím oprávněných osob dle čl. 13 této Smlouvy, statutárních orgánů Smluvních stran, popř. jimi písemně pověřených pracovníků.

17.4 Všechna oznámení mezi Smluvními stranami, která se vztahují k této Smlouvě, nebo která mají být učiněna na základě této Smlouvy, musí být učiněna v písemné podobě a druhé Smluvní straně doručena buď osobně nebo prostřednictvím datové schránky jinou formou registrovaného poštovního styku na adresu uvedenou na titulní stránce této Smlouvy, není-li stanoveno nebo mezi Smluvními stranami dohodnuto jinak. Nemá-li komunikace dle předchozí věty mít vliv na platnost a účinnost Smlouvy, připouští se též doručení prostřednictvím e-mailu na adresy uvedené v **Příloze č. 3** této Smlouvy.

17.5 Poskytovatel je oprávněn komunikovat s Objednatelem prostřednictvím informačního systému datových schránek. Poskytovatel bere na vědomí, že dle zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, je Objednatel povinen v zásadě doručovat veškerou korespondenci právnické osobě, která má zpřístupněnu svou datovou schránku, prostřednictvím datové schránky.

17.6 Ukládá-li Smlouva doručit některý dokument v písemné podobě, může být doručen buď v tištěné podobě nebo v elektronické (digitální) podobě v dohodnutém formátu, např. jako dokument aplikace MS Word verze 2003 nebo vyšší, MS Excel 2003 nebo vyšší či PDF na dohodnutém médiu apod.

17.7 Smluvní strany se zavazují, že v případě změny své poštovní adresy, nebo e-mailové adresy budou o této změně druhou Smluvní stranu informovat nejpozději do pěti (5) pracovních dnů.

17.8 Poskytovatel se zavazuje poskytnout Objednateli potřebnou součinnost při výkonu finanční kontroly dle zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, a to i po zániku této Smlouvy, bez nároku na jakoukoliv odměnu či náhradu nad rámec ceny dle Smlouvy. Toto spolupůsobení je povinen zabezpečit i u svých případných poddodavatelů.

18. NÁHRADA ÚJMY

18.1 Pojem „újma" znamená vždy újmu na jmění (škodu) ve smyslu § 2894 odst. 1 Občanského zákoníku a dále vždy i nemajetkovou újmu ve smyslu § 2894 odst. 2 Občanského zákoníku. Toto ustanovení je výslovným ujednáním o povinnosti Smluvních stran odčinit nemajetkovou újmu v případech porušení povinností dle této Smlouvy.

18.2 Každá ze Smluvních stran je povinna nahradit způsobenou újmu v rámci platných právních předpisů a této Smlouvy. Obě Smluvní strany se zavazují k vyvinutí maximálního úsilí k předcházení újmy a k minimalizaci vzniklých škod či újmy.

18.3 Poskytovatel je povinen nahradit Objednateli veškerou újmu, způsobenou porušením této Smlouvy či povinností uložených Poskytovateli dle Nařízení GDPR. Poskytovatel se zároveň zavazuje Objednatele odškodnit za jakoukoliv újmu, která mu v důsledku porušení povinností Poskytovatele vznikne na základě pravomocného rozhodnutí soudu či jiného orgánu veřejné moci.

18.4 Žádná ze Smluvních stran není povinna nahradit újmu, která vznikla v důsledku věcně nesprávného nebo jinak chybného zadání, které obdržela od druhé Smluvní strany. V případě, že Objednatel poskytl Poskytovateli chybné zadání a Poskytovatel s ohledem na svou povinnost poskytovat Plnění dle této Smlouvy s odbornou péčí mohl a měl chybnost takového zadání zjistit, smí se ustanovení předchozí věty dovolávat pouze v případě, že na chybné zadání Objednatele písemně upozornil a Objednatel trval na původním zadání.

18.5 Žádná ze Smluvních stran nemá povinnost nahradit újmu způsobenou porušením svých povinností vyplývajících z této Smlouvy, bránila-li jí v jejich splnění některá z překážek vylučujících povinnost k náhradě újmy ve smyslu § 2913 odst. 2 Občanského zákoníku.

18.6 Smluvní strany se zavazují upozornit druhou Smluvní stranu bez zbytečného odkladu na vzniklé překážky vylučující povinnost k náhradě újmy bránící řádnému plnění této Smlouvy. Smluvní strany se zavazují k vyvinutí maximálního úsilí k odvrácení a překonání překážek vylučujících povinnost k náhradě újmy.

18.7 Každá ze Smluvních stran je oprávněna požadovat náhradu újmy i v případě, že se jedná o porušení povinnosti, na kterou se vztahuje smluvní pokuta, a to v celém rozsahu.

19. SANKCE

19.1 Smluvní strany se dohodly, že:

19.1.1 v případě prodlení Objednatele s úhradou daňového dokladu (faktury), vzniká Poskytovateli právo na úrok z prodlení v zákonné výši;

19.1.2 v případě prodlení Poskytovatele řádně provést Plnění v délce přesahující 45 (slovy: čtyřicet pět) dní vzniká Objednateli nárok na smluvní pokutu ve výši 0,5 % z celkové ceny Plnění za každý započatý den prodlení;

19.1.3 v případě porušení povinnosti Poskytovatele poskytovat plnění dle této Smlouvy s využitím poddodavatelů uvedených v **Příloze č. 4** této Smlouvy a provádět jejich změny pouze se souhlasem Objednatele dle čl. 4.10 Smlouvy, vzniká Objednateli nárok na smluvní pokutu ve výši 5.000,- Kč za každé jednotlivé porušení takovéto povinnosti;

19.1.4 v případě porušení povinnosti Poskytovatele mít sjednáno pojištění za podmínek dle čl. 9.4 této Smlouvy vzniká Objednateli nárok na smluvní pokutu ve výši 5.000,- Kč za každý i započatý den prodlení.

19.1.5 v případě porušení jakékoliv povinnosti Poskytovatele dle čl. 11 Smlouvy vzniká Objednateli nárok na zaplacení smluvní pokuty ve výši 200.000,- Kč za každý jednotlivý případ porušení;

19.1.6 v případě porušení jakékoliv povinnosti Poskytovatele vyplývající z této Smlouvy ohledně ochrany Důvěrných informací dle čl. 15 Smlouvy vzniká Objednateli nárok na smluvní pokutu ve výši 1.000.000,- Kč za každý jednotlivý případ porušení takovéto povinnosti;

19.1.7 v případě porušení jakékoliv povinnosti Poskytovatele dle čl. 16 této Smlouvy nebo Kybernetických požadavků uvedených v **Příloze č. 6** této Smlouvy vzniká Objednateli nárok na smluvní pokutu ve výši 100.000,- Kč za každý jednotlivý případ porušení takovéto povinnosti.

19.2 Smluvní pokuty anebo úroky z prodlení jsou splatné 30. den ode dne doručení písemné výzvy oprávněné Smluvní strany k jejich úhradě povinné Smluvní straně, není-li ve výzvě uvedena lhůta delší.

19.3 Není-li dále stanoveno jinak, zaplacení jakékoliv sjednané smluvní pokuty nezbavuje povinnou Smluvní stranu povinnosti splnit své závazky.

19.4 Zaplacením smluvní pokuty není dotčeno právo Objednatele na náhradu újmy v celém rozsahu.

20. PLATNOST A ÚČINNOST SMLOUVY

20.1 Tato Smlouva je platná dnem připojení podpisu poslední ze Smluvních stran.

20.2 Tato Smlouva nabývá účinnosti uveřejněním v registru smluv dle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů (dále jen „**ZRS**"). Smluvní strany výslovně sjednávají, že uveřejnění této Smlouvy v registru smluv zajistí Objednatel.

20.3 Smlouva neobsahuje obchodní tajemství žádné ze Smluvních stran ani jiné informace vyloučené z povinnosti uveřejnění (s výjimkou uvedenou dále) a je včetně jejích příloh způsobilá k uveřejnění v registru smluv ve smyslu ZRS a Smluvní strany s uveřejněním Smlouvy, včetně jejích příloh, souhlasí; výjimkou jsou Osobní údaje v podobě jmen a kontaktních údajů osob uvedených v **Příloze č. 3** a **Příloze č. 4**, které budou znečitelněny.

20.4 Objednatel je oprávněn bez jakýchkoliv sankcí písemně odstoupit od této Smlouvy v případě jejího podstatného porušení ze strany Poskytovatele, zejména, nikoliv však výlučně, v případě:

20.4.1 že Plnění nebude splňovat kritéria uvedené v této Smlouvě;

20.4.2 prodlení Poskytovatele s provedením Plnění, pokud Poskytovatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Objednatel poskytne v písemné výzvě ke splnění povinnosti,

20.4.3 porušení povinnosti ochrany Důvěrných informací či Osobních údajů dle této Smlouvy ze strany Poskytovatele;

20.4.4 že Poskytovatel porušil povinnost si nechat předem schválit Změnu kontroly poskytovatele Objednatelem dle čl. 9.2.4 Smlouvy.

20.5 Objednatel je dále oprávněn bez jakýchkoliv sankcí písemně odstoupit od této Smlouvy, pokud:

20.5.1 bylo příslušným orgánem vydáno pravomocné rozhodnutí zakazující plnění této Smlouvy;

20.5.2 na majetek Poskytovatele je prohlášen úpadek nebo Poskytovatel sám podá dlužnický návrh na zahájení insolvenčního řízení;

20.5.3 Poskytovatel vstoupí do likvidace; nebo

20.5.4 proti Poskytovateli je zahájeno trestní stíhání pro trestný čin podle zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob, ve znění pozdějších předpisů.

20.6 Poskytovatel je oprávněn odstoupit od této Smlouvy v případě prodlení Objednatele se zaplacením jakékoliv splatné částky dle této Smlouvy po dobu delší než čtyřicet pět (45) dnů, pokud Objednatel nezjedná nápravu ani v dodatečné přiměřené lhůtě, kterou mu k tomu Poskytovatel poskytne v písemné výzvě ke splnění povinnosti, přičemž tato lhůta nesmí být kratší než patnáct (15) pracovních dnů od doručení takovéto výzvy.

20.7 Účinky odstoupení od Smlouvy nastávají dnem doručení písemného oznámení o odstoupení druhé Smluvní straně, není-li v odstoupení stanoveno pozdější datum.

20.8 V případě zániku Smlouvy z důvodu odstoupení Objednatele má Objednatel právo (i) vrátit veškeré či pouze některé dodané části Plnění, které nejsou pro Objednatele objektivně technicky a ekonomicky využitelné; nebo (ii) ponechat si veškeré či pouze některé dodané části Plnění. V případě, že si Objednatel ponechá již dodané, akceptované a provedené části Plnění a je povinen zaplatit za ně příslušnou cenu či její část.

20.9 Smluvní strany se dohodly na vyloučení použití § 1978 odst. 2 Občanského zákoníku, který stanoví, že marné uplynutí dodatečné lhůty stanovené k plnění má za následek odstoupení od smlouvy bez dalšího.

20.10 Poskytovatel nemá právo odstoupit od této Smlouvy v případě nevhodných příkazů Objednatele či poskytnutí nevhodné věci Objednatelem dle § 2595 Občanského zákoníku.

20.11 Zánikem této Smlouvy nejsou dotčena zejména následující ustanovení Smlouvy: čl. 11 (Vlastnické právo a užívací práva), čl. 12 (Záruka), čl. 14 (Ochrana Osobních údajů), čl. 15 (Ochrana Důvěrných informací), čl. 16 (Kybernetická bezpečnost), čl. 17 (Součinnost a vzájemná komunikace), čl. 18 (Náhrada újmy), čl. 19 (Sankce, čl. 21 (Rozhodné právo a řešení sporů), čl. 22 (Závěrečná ustanovení), související ustanovení příloh, tento čl. 20.11 Smlouvy, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku této Smlouvy.

21. ROZHODNÉ PRÁVO A ŘEŠENÍ SPORŮ

21.1 Práva a povinnosti Smluvních stran touto Smlouvou výslovně neupravené se řídí právním řádem České republiky a příslušnými obecně závaznými právními předpisy, zejména Občanským zákoníkem.

21.2 Smluvní strany se zavazují vyvinout maximální úsilí k odstranění vzájemných sporů vzniklých na základě této Smlouvy nebo v souvislosti s touto Smlouvou, včetně sporů o její výklad

či platnost a usilovat o jejich vyřešení nejprve smírně prostřednictvím jednání pověřených osob nebo pověřených zástupců. Nebude-li sporná záležitost vyřešena do třiceti (30) dnů od započetí řešení dle čl. 21.2 Smlouvy, Smluvní strany mají možnost obrátit se se svými nároky na příslušný obecný soud České republiky.

22. ZÁVĚREČNÁ USTANOVENÍ

22.1 Tuto Smlouvu je možné měnit pouze písemnou dohodou Smluvních stran ve formě číslovaných dodatků této Smlouvy, podepsaných za každou Smluvní stranu osobou nebo osobami oprávněnými jednat jménem Smluvních stran.

22.2 Smluvní strany vylučují možnost uzavření smlouvy nebo dodatku bez ujednání o veškerých náležitostech dle § 1726 Občanského zákoníku. Smluvní strany rovněž vylučují použití ustanovení § 1740 odst. 3 a ustanovení § 1757 odst. 2 Občanského zákoníku.

22.3 Poskytovatel na sebe v souladu s ustanovením § 1765 odst. 2 Občanského zákoníku přebírá nebezpečí změny okolností.

22.4 Poskytovatel výslovně souhlasí s tím, aby tato Smlouva, včetně všech jejích změn a dodatků, s výjimkou dle čl. 20.3 této Smlouvy, byla vedena v Centrální evidenci smluv vedené Objednatelem, která je veřejně přístupná. Poskytovatel dále výslovně souhlasí s tím, aby tato Smlouva, včetně všech jejích změn a dodatků, a údajů o výši skutečně uhrazené ceny za Plnění byly v plném rozsahu zveřejněny Objednatelem. Smluvní strany prohlašují, že skutečnosti uvedené v této Smlouvě nepovažují za obchodní tajemství dle § 504 Občanského zákoníku a udělují svolení k jejich užití a zveřejnění bez stanovení jakýchkoliv dalších podmínek.

22.5 Pokud by se kterékoliv ustanovení této Smlouvy ukázalo být neplatným nebo nevynutitelným nebo se jím stalo po uzavření této Smlouvy, pak tato skutečnost nepůsobí neplatnost ani nevynutitelnost ostatních ustanovení této Smlouvy, nevyplývá-li z donucujících ustanovení právních předpisů jinak. Smluvní strany se zavazují takové neplatné či nevynutitelné ustanovení nahradit platným a vynutitelným ustanovením, které je svým obsahem nejbližší účelu neplatného či nevynutitelného ustanovení.

22.6 Veškerá práva a povinnosti vyplývající z této Smlouvy přecházejí, pokud to povaha těchto práv a povinností nevylučuje, na právní nástupce Smluvních stran.

22.7 Poskytovatel není oprávněn postoupit jakékoliv své pohledávky ze Smlouvy vůči Objednateli na třetí osobu bez předchozího písemného souhlasu Objednatele, a to ani částečně.

22.8 Tato Smlouva je vyhotovena ve čtyřech (4) stejnopisech s platností originálu, z nichž Objednatel obdrží tři (3) stejnopisy a Poskytovatel obdrží jeden (1) stejnopis.

22.9 Nedílnou součást Smlouvy tvoří tyto přílohy:

Příloha č. 1:	Nabídka
Příloha č. 2:	Klíčové pozice v Realizačním týmu
Příloha č. 3:	Oprávněné osoby
Příloha č. 4	Seznam poddodavatelů
Příloha č. 5:	ICT standardy Objednatele
Příloha č. 6:	Požadavky na zajištění kybernetické bezpečnosti

Na důkaz svého souhlasu s obsahem této Smlouvy k ní Smluvní strany připojují níže své podpisy.

Objednatel

V Praze dne - 5 -04- 2022

[redacted]

ěsto Praha
ří Károly

ředitel Odb **atických činností (OIC)**
HMP

HLAVNÍ MĚSTO PRAHA
-11-

Poskytovatel

V Praze dne - 5 -04- 2022

[redacted]

APPSEC s.r.o.

Adam Pacit
jednatel

Příloha č. 1

Nabídka na externí Blackhat analýzu pro HLAVNÍ MĚSTO PRAHA – Magistrát hlavního města Prahy

Příloha č. 2

Pozice v Realizačním týmu

Pozice (role)	**Identifikační a kontaktní údaje osoby**	**Poskytovatel / člen společnosti dodavatelů / poddodavatel, k němuž osoba patří**
Projektový manažer	**Adam Paclt**	**Appsec s.r.o.**
Technický specialista	**Jan Mitrovský**	**Appsec s.r.o.**

Příloha č. 3

Oprávněné osoby

Za Objednatele:

v záležitostech smluvních:

Jméno a příjmení	Mgr. Jiří Károly
E-mail	[redacted]
Telefon	

v záležitostech obchodních:

Jméno a příjmení	Mgr. Jiří Károly
E-mail	[redacted]
Telefon	

v záležitostech technických:

Jméno a příjmení	Bc. Ladislav Tobiáš
E-mail	[redacted]
Telefon	

Za Poskytovatele:

Jméno a příjmení	Adam Paclt
E-mail	[redacted]
Telefon	

Příloha č. 4

Seznam poddodavatelů

Pokud Poskytovatel poskytuje Plnění či jeho část prostřednictvím poddodavatelů, uvede tabulku tolikrát, kolika poddodavateli bude poskytovat Plnění. Poskytovatel musí uvést všechny poddodavatele, kteří se budou podílet na poskytování Plnění.

Poskytovatel nebude Plnění dle této Smlouvy poskytovat s využitím poddodavatelů.

Příloha č. 5

ICT standardy Objednatele

Smluvní strany prohlašují, že Poskytovateli budou ICT standardy Objednatele poskytnuty na jeho vyžádání, obvykle nejpozději do deseti (10) pracovních dní ode dne nabytí účinnosti této Smlouvy.

ID	Název standardu
1	SA01 Správa koncových zařízení
2	SB04 Služby datového centra – virtualizace
3	SB05 Pronájem optických vláken a DWDM
4	SB06 Správa Firewall
5	SB07 Správa LAN
6	SB08 SLA Container
7	SB09 Antivir
8	SB10 Správa WAN
9	SB11 Poskytování diskového prostoru
10	SB12 Poskytování výpočetního výkonu (HW)
11	SB13 Identity and access management (IAM)
12	SB14 Správa e-mailových služeb
13	SB15 Internet access
14	SB16 VPN gateway
15	SB17 Poskytování služby ServiceDesk
16	SB18 Poskytování monitoringu infrastruktury a služeb
17	SB19 Poskytování služby Licence management
18	SB20 DNS, DHCP a AD
19	SB21 Správa certifikátu a CA
20	SC01 Generická aplikace
21	MC01 Provoz programového vybavení Celopražského významu
22	MC02 Poskytnutí datového prostoru
23	MC03 Bezpečné úložiště
24	MC04 Poskytování výpočetního výkonu v datovém centru
25	MC05 Poskytování podpůrného programového vybavení

Příloha č. 6

Požadavky na zajištění kybernetické bezpečnosti (Kybernetické požadavky)

Za účelem povinností stanovených Objednateli jakožto povinné osobě dle VKB, je Poskytovatel povinen nad rámec povinností stanovených v těle Smlouvy plnit níže uvedené povinnosti zejm. součinnostního a bezpečnostního charakteru dle této **Přílohy č. 5** Smlouvy.

Poskytovatel je povinen plnit relevantní povinnosti v rozsahu a způsobem tak, aby byl naplněn účel právní úpravy v oblasti bezpečnostních opatření, kybernetických bezpečnostních incidentů, reaktivních opatření, náležitostí podání v oblasti kybernetické bezpečnosti a likvidaci dat ve vztahu k povinnostem, které tato právní úprava stanovuje Objednateli jakožto povinné osobě dle předpisů z oblasti kybernetické bezpečnosti, a to vždy i v případě změny příslušné právní úpravy. V takovém případě je Objednatel oprávněn požadovat od Poskytovatele přiměřenou součinnost i nad rámec povinností stanovených v této **Příloze č. 5** Smlouvy, avšak vždy pouze za účelem zajištění plnění povinnosti Poskytovatele z oblasti kybernetické bezpečnosti ve smyslu shora uvedeného.

Čl. 1 Systém řízení bezpečnosti informací

1. Poskytovatel se bude v rozsahu poskytování Plnění aktivně podílet na splnění povinností uvedených v § 3 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu poskytování Plnění na své straně:
    a. Prosadit bezpečnostní zásady a procesy, které budou pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování Plnění dle Smlouvy.
    b. Na základě bezpečnostních potřeb a výsledků hodnocení rizik zavést příslušná bezpečnostní opatření v rozsahu poskytovaného Plnění dle Smlouvy, monitorovat je, vyhodnocovat jejich účinnost.
    c. Vést záznamy o vytváření a zpracování dat a informací v rozsahu poskytovaného Plnění dle Smlouvy, zaznamenávat veškeré podstatné okolnosti související se zajištěním bezpečnosti těchto dat a informací a na vyžádání tyto záznamy Objednateli zpřístupnit.
    d. Stanovit a udržovat aktuální bezpečnostní politiku, která bude pokrývat zabezpečení dat a informací, jež mohou být vytvářeny a zpracovávány na straně Poskytovatele při poskytování Plnění dle Smlouvy. Bezpečnostní politika musí obsahovat hlavní zásady, cíle, bezpečnostní potřeby, práva a povinnosti ve vztahu k řízení bezpečnosti informací.
    e. Stanovit a udržovat aktuální opatření bezpečnosti ve formě procesů a technologií, které zajišťují naplnění bezpečnostní politiky.
    f. Poskytovatel je dále povinen dodržovat bezpečnostní politiku Objednatele, byl-li s ní seznámen.

Čl. 2 Řízení aktiv

2. Poskytovatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 4 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu Plnění na své straně:
    a. Stanovit a udržovat rozsah a seznam aktiv využívaných pro plnění této Smlouvy (aktivy se rozumí např. data a informace k předmětu Plnění dle této Smlouvy, systémy ICT, moduly, hardware prvky - infrastruktura hlasové a datové komunikace, aplikace, databáze, servery, úložiště, koncová zařízení – pracovní stanice typu osobní počítač nebo notebook, mobilní koncová zařízení – přenosná zařízení typu telefon, tablet, notebook, netbook, PDA, apod.), a tato aktiva strukturovaně popsat a Objednateli předložit do třiceti (30) dnů od nabytí účinnosti této Smlouvy a následně na vyžádání, a to po celou dobu trvání Smlouvy a po dobu dvou (2) let po jejím ukončení.

Čl. 3 Řízení rizik

1. Poskytovatel se bude v rozsahu poskytování Plnění dle této Smlouvy aktivně podílet na splnění povinností uvedených v § 5 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu poskytovaného Plnění na své straně:
    a. Řídit vlastní rizika, která mohou ovlivnit poskytování Plnění dle Smlouvy.
    b. V minimálním intervalu 1x ročně vytvořit a předložit Objednateli zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:
        i. Vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok
        ii. Identifikaci a hodnocení rizik s vazbou na předmět Plnění
        iii. Realizovaná bezpečnostní opatření
        iv. Nepokrytá bezpečnostní rizika a návrh opatření
        v. Vyhodnocení bezpečnostních událostí a incidentů
        vi. Aktuální stav souladu Poskytovatele s těmito Kybernetickými požadavky.

Čl. 4 Organizační bezpečnost

1. Poskytovatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 6 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu předmětu Plnění na své straně:
    a. Jmenovat nejpozději do pěti (5) dnů po uzavření této Smlouvy odpovědnou kontaktní osobu pro potřeby zajištění plnění těchto Kybernetických požadavků a související komunikaci mezi Smluvními stranami (dále také jen „**Kontaktní osoba**"). Kontaktní osobu sdělí Poskytovatel písemně Objednateli v téže lhůtě. Objednatel stanovuje, že určení Kontaktní osoby pro bezpečnost na straně Poskytovatele nemá dopad na ustanovení čl. 13.1a 13.2 Smlouvy týkající se odpovědných osob ve věcech smluvních a technických.
    b. Využívat pro poskytování předmětu Plnění pouze oprávněných osob, které byly řádně seznámeny s příslušnými ustanoveními interních řídících aktů Objednatele a mají ověřenou kvalifikaci, znalosti a zkušenosti k řádnému poskytování předmětu Plnění.

Čl. 5 Řízení dodavatelů

1. Poskytovatel se bude v rozsahu poskytovaného Plnění dle této Smlouvy aktivně podílet na splnění povinností uvedených v § 8 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu poskytovaného Plnění na své straně:
    a. Využívá-li při poskytování Plnění poddodavatele, zabezpečit adekvátní dodržování Kybernetických požadavků rovněž ve smluvních vztazích se svými poddodavateli, přičemž tuto skutečnost se Poskytovatel zavazuje doložit Objednateli do deseti (10) dnů od počátku poskytování Plnění, písemným prohlášením o dodržování Kybernetických požadavků u svých poddodavatelů.
    b. Pokud při poskytování předmětu Plnění dochází ke zpracování Osobních údajů, zabezpečit nad rámec čl. 14 uzavření samostatných smluv (tj. smluv se svými poddodavateli, zaměstnanci a případnými dalšími osobami podílejícími se na poskytování plnění z této Smlouvy) ve smyslu příslušných ustanovení Nařízení GDPR.

Čl. 6 Bezpečnost lidských zdrojů

1. Poskytovatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 9 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu poskytovaného Plnění na své straně:
    a. Zabezpečit, aby Kontaktní osoba nejpozději do třiceti (30) dnů od uzavření Smlouvy potvrdila písemně Objednateli, že všechny osoby podílející se na poskytování Plnění za stranu Poskytovatele byly prokazatelně seznámeny s těmito Kybernetickými požadavky a příslušnými ustanoveními interních řídících aktů Objednatele.
    b. Dodržovat příslušná ustanovení interních řídících aktů Objednatele v rozsahu, v jakém byl s těmito akty seznámen. Za prokazatelné seznámení se považuje školení pracovníků Poskytovatele zajištěné Objednatelem, protokolární či elektronické předání příslušné dokumentace nebo Objednatelem zajištěný přístup na sdílené úložiště obsahující příslušné interní akty řízení.
    c. V případě, že je součástí předmětu Plnění služba dohledu nad předmětem Plnění, definovat a naplnit role a odpovědnosti pro monitoring sítě a zařízení v rozsahu předmětu Plnění.
    d. Zabezpečit, aby osoby podílející se na poskytování Plnění Objednateli v prostředí nebo s prostředky Objednatele, a to i tehdy, pokud jsou prostředky Objednatele používány mimo jeho prostředí:
        i. Pro uložení a sdíleni dat a informací Objednatele využívaly pouze k tomu schválené prostředky (aktiva) a schválené způsoby komunikace;
        ii. Neukládaly ani nesdílely data i informace eticky nevhodného obsahu, odporující dobrým mravům nebo poškozující jméno Objednatele;
        iii. Nestahovaly, nesdílely, neukládaly, nearchivovaly ani neinstalovaly datové a spustitelné soubory v rozporu s licenčními podmínkami nebo předpisy upravující ochranu duševního vlastnictví;
        iv. Nenavštěvovaly internetové stránky s eticky nevhodným obsahem;
        v. Nerealizovaly pokusy o neautorizovaný přístup ke zdrojům Objednatele ani ke zdrojům jiných subjektů;
        vi. Nerealizovaly pokusy o neoprávněnou modifikaci ani jiné neoprávněné zásahy do prostředků Objednatele, a to ani v případě, kdy jim byl prostředek Objednatele svěřen do správy;
        vii. Nepodílely se s prostředky Objednatele na šíření spamu ani škodlivého softwaru;
        viii. Dodržovali obecně závazné právní předpisy.
2. Poskytovatel si je vědom, že součástí podmínek pro získání přístupu ke zdrojům a aktivům Objednatele je na straně Objednatele zpracování Osobních údajů pracovníků Poskytovatele, kteří se podílejí na zajištění předmětu Plnění. Pokud nebude Objednateli umožněno Osobní údaje dotčených pracovníků Poskytovatele v rámci plnění Smlouvy zpracovat, nebude těmto pracovníkům umožněn žádný přístup ke zdrojům Objednatele.

Čl. 7 Řízení provozu a komunikací

1. Poskytovatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 10 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu poskytování Plnění na své straně:
    a. Zabezpečit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování Plnění.
    b. Na vyžádání poskytnout Objednateli přehled, report, či jinou adekvátní informaci o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře.

c. Zabezpečit, že pro poskytování Plnění budou využívány pouze aplikace a technologie, které jsou v souladu s platnou českou a evropskou legislativou, především s ohledem na licenční podmínky a předpisy upravující ochranu duševního vlastnictví.

Čl. 8 Řízení změn

1. Poskytovatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 11 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu poskytování Plnění na své straně:
    a. Přiměřeně reagovat na změny na straně Objednatele a upravit na své straně technická a organizační opatření tak, aby odpovídala novému stavu po provedení změny.
    b. Aktivně spolupracovat při testování významné změny.

Čl. 9 Řízení přístupu

1. Poskytovatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 12 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu poskytování Plnění na své straně:
    a. Přidělovat oprávnění svým jednotlivým pracovníkům ve smyslu oprávnění k výkonu činností tak, aby byla minimalizována rizika nežádoucího přístupu k aktivům Objednatele.
    b. Zabezpečit, aby udělený přístup nebyl sdílen více osobami za stranu Poskytovatele, pokud sdílený přístup nevyžaduje využívaná technologie. V takovém případě musí Poskytovatel vést evidenci využívání sdílených přístupů a tuto na vyžádání předložit Objednateli kdykoli v průběhu trvání této Smlouvy a dva (2) roky po jejím ukončení.
    c. Stanovit v požadavku na přístup rozsah dat/informací, služby, účelu, pro které je přístup k systému ICT Objednatele požadován a časový údaj o délce platnosti přístupu (např.: na dobu neurčitou / 1 rok / 1 měsíc / 1 den).
    d. Zabezpečit, aby osoby podílející se na poskytování Plnění a mající přístup k informačním aktivům Objednatele chránily autentizační prostředky a údaje a nikdy neposkytovaly neautorizovaný přístup dalším osobám.
    e. Průběžně kontrolovat a vyhodnocovat oprávněnost a potřebu přístupu, jak fyzického, tak i logického, u všech osob na straně Poskytovatele, které přistupují do prostředí Objednatele.
2. Poskytovatel bere na vědomí, že přístup k systému ICT je možné povolit pouze fyzické identitě zaměstnance Poskytovatele / poddodavatele Poskytovatele, a to na základě požadavku Poskytovatele na přístup.
3. Poskytovatel bere na vědomí, že přidělení oprávnění přístupu musí být řízeno principem nezbytného minima a není nárokové.
4. Poskytovatel bere na vědomí, že v případě neúspěšných pokusů o autentizaci uživatele (osoby za stranu Poskytovatele) může být příslušný účet zablokován a řešen jako bezpečnostní incident a mohou být uplatněny příslušné postupy zvládání bezpečnostního incidentu (např. okamžité zrušení přístupu k informačním aktivům Objednatele).

Čl. 10 Akvizice, vývoj a údržba

Poskytovatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 13 VKB, které musí splnit Objednatel. **Čl. 11 Zvládání kybernetických bezpečnostních událostí a incidentů**

1. Poskytovatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 14 VKB, které musí splnit Objednatel.

2. Poskytovatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení Kybernetických požadavků, jehož příčina je na straně Poskytovatele, nebude posuzován jako okolnost vylučující povinnost k náhradě újmy Poskytovatele za prodlení s řádným a včasným plněním předmětu Smlouvy a nebude důvodem k jakékoli náhradě případné újmy Poskytovateli či jiné osobě ze strany Objednatele. Ostatní ustanovení ohledně odpovědnosti Poskytovatele za prodlení obsažená ve Smlouvě nejsou tímto ustanovením dotčena.

Čl. 12 Řízení kontinuity činností

1. Poskytovatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 15 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu poskytování Plnění na své straně:
    a. Zabezpečit adekvátní kontinuitu svých aktiv, které jsou potřebné k poskytování Plnění.
    b. Pravidelně kontrolovat a testovat, že je schopen kontinuitu aktiv zabezpečit dle sjednané úrovně poskytovaného Plnění.

Čl. 13 Kontrola a audit

1. Poskytovatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 8 a § 16 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu poskytování Plnění poskytnout adekvátní součinnost při výkonu kontroly Objednatele ze strany Národního úřadu pro kybernetickou bezpečnost dle § 23 ZKB.

Čl. 14 Fyzická bezpečnost

1. Poskytovatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 17 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu poskytování Plnění na své straně:
    a. Dodržovat provozní řády budov (režimová opatření) a využívaných prostor, zejména pak v oblasti fyzické ochrany bezpečnostních zón, kde jsou umístěny aktiva systémů ICT, anebo datové nosiče.
    b. V rozsahu poskytování Plnění zabezpečit fyzické zabezpečení, zejména označení, uchování a likvidaci instalačních, záložních nebo archivních médií a dokumentace v souladu s klasifikací aktiv Objednatele, pokud s ní byl Poskytovatel seznámen.

Čl. 15 Bezpečnostní nástroje

1. Poskytovatel se bude v rozsahu poskytování Plnění dle Smlouvy aktivně podílet na splnění povinností uvedených v § 18 až § 27 VKB, které musí splnit Objednatel. Minimálně se Poskytovatel zavazuje v rozsahu poskytování Plnění na své straně:
    a. Realizovat bezpečnostní opatření pro odstranění nebo blokování síťového spojení/síťových spojení, které/která neodpovídají požadavkům na ochranu integrity komunikační sítě.
    b. Realizovat přístup z mobilního zařízení do prostředí Objednatele pouze prostřednictvím zabezpečeného připojení virtuální privátní sítě (VPN) nebo zvolit adekvátní technické opatření.
    c. Připojovat do prostředí Objednatele pouze ta síťová zařízení (switch, přístupový bod wifi, router, hub apod.), která prošla schvalovacím procesem a jejich připojení bylo schváleno oprávněnou osobou ve věcech technických na straně Objednatele určenou v této Smlouvě.
    d. Bez zbytečného odkladu deaktivovat všechna nevyužívaná zakončení sítě anebo nepoužívané porty aktivního síťového prvku, který je v rozsahu předmětu Plnění a je ve správě Poskytovatele.

e. Na aktiva Objednatele neinstalovat a nepoužívat v prostředí Objednatele tyto typy nástrojů, pokud nejsou součástí předmětu Plnění Smlouvy:

   i. Keylogger – software nebo hardware, který neautorizovaně zaznamenává stisky kláves s cílem narušit důvěrnost zadávaných dat a informací.

   ii. Sniffer – software nebo hardware umožňující odposlouchávání síťového provozu.

   iii. Analyzátor zranitelností (scanner zranitelností) – softwarový nebo hardwarový nástroj umožňující vyhledávání zranitelností systémů ICT, detekování dostupných síťových služeb a portů, běžících procesů, běžících aplikací a jejich verzí apod.

   iv. Backdoor – skrytý softwarový nebo hardwarový nástroj, který umožňuje obejití schválených autentizačních procedur, instalovaný s cílem budoucího snadnějšího a neautorizovaného přístupu do systému ICT.

   v. Malware a jiný škodlivý software, který narušuje, obchází či jinak omezuje bezpečnostní opatření v prostředí Objednatele.

f. Připojovat do prostředí Objednatele pouze zařízení ICT, která jsou chráněna proti malware a jinému škodlivému softwaru, pokud to jejich technologie umožňuje.

g. Průběžně zaznamenávat a uchovávat data o provozu zařízení ICT (provozní a lokalizační údaje) v rozsahu předmětu Plnění a v souladu s požadavky platné a účinné české a evropské legislativy.

h. Na vyžádání poskytnout Objednateli report obsahující výsledky monitorování veškerých uživatelských a administrátorských aktivit a jiných událostí v rozsahu poskytování Plnění dle Smlouvy, a to po celou dobu trvání Smlouvy a po dobu dvou (2) let po jejím ukončení.

i. Zabezpečit sběr informací o provozních a bezpečnostních činnostech v rozsahu poskytování Plnění dle Smlouvy a ochranu získaných informací před jejich neoprávněným čtením nebo změnou.

j. Pro on-line transakce realizované prostřednictvím webových technologií implementovat TLS/SSL certifikáty s cílem zabezpečit jejich důvěrnost, integritu a identitu komunikujících protistran.

k. Veškeré neveřejné informace poskytnuté Objednatelem chránit vhodným šifrováním a proti neautorizovanému přístupu, a to zejména na mobilních zařízeních.

2. Poskytovatel bere na vědomí, že v případě, kdy technické spojení Objednatele s Poskytovatelem narušuje chod služeb Objednatele, může být toto spojení ihned ukončeno bez předchozího upozornění, pokud tato Smlouva nestanoví jinak.

3. Poskytovatel bere na vědomí, že veškeré aktivity Poskytovatele a jeho plnění realizované v prostředí Objednatele jsou monitorovány a vyhodnocovány v rozsahu poskytování Plnění a v souladu s interními dokumenty Objednatele, se kterými byl Poskytovatel seznámen.

appsec

APPSEC, s. r. o
Thámova 18, Praha 8
Česká republika

[redacted]

IČO: 05542812
DIČ: CZ05542812

Nabídka na externí Blackhat analýzu

pro

HLAVNÍ MĚSTO PRAHA

–

Magistrát hlavního města Prahy

Datum vystavení nabídky: 14.12.2021

Platnost nabídky: 30 dní od jejího obdržení

Head Of Sales, APPSEC s.r.o. Filip Motejl

1. Úvod

Název projektu:	Blackhat analýza - externí
Zadavatel:	HLAVNÍ MĚSTO PRAHA – Magistrát hlavního města Prahy
Kontaktni osoba:	Jiří Károly
Použité zkratky	MD – Manday = 1 člověkoden = 8 hodin OWASP - Open Web Application Security Project PTES - Penetration Testing Executing Standard OSSTMM - Open Source Security Testing Methodology Manual GDPR – General Data Protection Regulation - Obecné nařízení o ochraně osobních údajů OSINT – Open-source Intelligence
Zpracovatel	APPSEC s.r.o. Thámova 166/18 Praha – Karlín, PSČ 186 00 IČO: 05542812 DIČ: CZ05542812 [redacted]

2. Základní informace

Na základě komunikace s panem Károlym byla připravena tato nabídka.

HLAVNÍ MĚSTO PRAHA má zájem na zjištění existence bezpečnostních rizik, případných zranitelností v její organizace a jejich nápravě. Cílem je zmapovat stav organizace z pohledu informační bezpečnosti jak po organizační, tak po technické stránce. Přínos testování spočívá především v identifikaci těch nejslabších míst, což napomůže v prioritizaci řešení jednotlivých rizik a k jejich efektivní, včasné a ekonomické nápravě.

V rozsahu této nabídky samotná náprava již zahrnuta není, záleží pak na domluvě, zda si bude HLAVNÍ MĚSTO PRAHA přát i asistenci při realizaci náprav, tým společnosti APPSEC je tuto asistenci schopný v plné míře zajistit.

3. Motivace

- Díky bezpečnostnímu testování můžete efektivně investovat peníze do bezpečnosti tam, kde je to opravdu důležité.
- Bezpečnostní testy vám umožní získat přehled o závažnosti rizik a oddělí kritické zranitelnosti od těch, které nevyžadují akutní nápravu.
- Bezpečnostní incidenty mohou vést ke snížení reputace nebo finančním ztrátám společnosti.
- Zvýšené nároky legislativy na bezpečnost dat zákazníků, zejména GDPR a plynoucí rizika likvidačních pokut nebo trestní zodpovědnosti.
- Rostoucí konkurenční prostředí se zaměřením na zabezpečenou komunikaci.
- Zájem o zodpovědné poskytování kvalitních a zejména bezpečných služeb a produktů zákazníkům.
- Jakékoliv potenciální bezpečnostní incidenty, které by ohrozili důvěrnost, integritu a dostupnost ekosystému organizace, mohou způsobit škody na dobrém jméně společnosti, ztrátu zákazníků nebo finanční škodu.
- Možné sankce:
  - Za porušení zákona č. 418/2011 Sb., o trestní odpovědnosti právnických osob - až 1,46 miliardy Kč
  - Za porušení zákona č. 101/2000 Sb., o ochraně osobních údajů – až 10.000.000 Kč
  - Za porušení evropského nařízení GDPR (General Data Protection Regulation) od května 2018 – až 20.000.000 EUR nebo 4% z celosvětového obratu
  - Smluvní pokuty vyplývající z dohod o mlčenlivosti, které má společnost uzavřené se svými zákazníky

4. Návrh řešení – Blackhat analýza

Tato unikátní služba obsahuje prvky časově omezeného cíleného útoku z perspektivy skutečného útočníka. Umožní nám lépe zmapovat situaci organizace a identifikovat slabá místa a příležitosti ke zlepšení. Slouží zároveň jako referenční test, který je možné realizovat opakovaně a dlouhodobě vyhodnocovat a měřit míru rizikovosti organizace z pohledu cílených útoků.

V kontextu projektu pro HLAVNÍ MĚSTO PRAHA kdy před námi stojí cíl zlepšení celkového zabezpečení organizace, nám pomůže identifikovat místa na které je potřeba se zaměřit. Dále nám umožní se vyhnout zbytečným investicím tam, kde by to nemělo vzhledem k souvisejícím rizikům smysl.

Zároveň nám tento test umožní lépe pochopit organizaci a princip jejího fungování tak, abychom mohli v dalších krocích navrhnout efektivní a smysluplná opatření.

Co dostanete?

- Vyhodnocení obranyschopnosti a identifikace nejkritičtějších míst
- Popis scénáře útoku, vulnerability sken, protokol z útoku a dokumentaci nálezů
- Ukázku toho, jak Vaši organizaci vidí reálný útočník, který mapuje situaci
- Přehled informací, které se o Vás dají nalézt, včetně dat z černého trhu, která by mohla sloužit útočníkovi k zacílení na Vaší organizaci

5. Rozsah Blackhat analýzy

- Organizace z prostředí internetu

6. Průběh Blackhat analýzy

Blackhat analýza je naše jedinečná služba, která Vám umožňuje zjištění bezpečnosti Vašich systémů a Vaší společnosti a jde nad rámec klasického penetračního testu. Dle domluvy nebyl pro Blackhat analýzu pevně stanovený rozsah testování. Při testování používáme APPSEC metodiku, která vychází z metodiky Cyber Kill Chain.

V následujících kapitolách je popsán scénář útoku.

Reconnaissance - zjišťování informací o cíli

Začátkem každého úspěšného i neúspěšného útoku je zjišťování co největšího počtu informací o společnosti, která se stala cílem útoku. K tomuto hacker používá různé dostupné informace, například z webové stránky společnosti, z webových vyhledávačů, z dalších veřejně dostupných zdrojů informací, například různé sociální sítě, darknet, webové stránky pro sdílení uživatelských dat jako pastebin, sdílení různých obrázků, dokumentů a další. Často používanou technikou pro zjištění informací o firmě je vydávání se za potenciálního partnera firmy a informace zjistit například na obchodní schůzce či na pohovoru na relevantní pracovní pozici. Součástí reconnaissance fáze je i vulnerability scan nalezených systémů. Systémy, které jsou službou nějaké třetí strany, jsou z

vulnerability scanů vynechané z právních důvodů. Pro reconnaissance fázi vycházíme z OSINT frameworku dostupného na adrese http://osintframework.com/.

Z hlediska zjišťováni informací o cíli jsou pro útočníka zajímavé především tyto 3 oblasti:

- domény / servery

Doménová jména a IP adresy jsou pravděpodobně prvním z informací, které útočník ve vztahu ke společnosti, kterou se chystá napadnout, zjišťuje.

- E-mailové adresy

E-mailové adresy slouží primárně k zaměření útoku využívajících sociálního inženýrství a to nejen jako příjemce například připraveného malware, ale mohou sloužit i pro podvržený odesílatele e-mailu a tím e-mailu dodat určitou věrohodnost v očích uživatele či klienta právě využitím existující e-mailové adresy.

- další skutečnosti, které mohou pomoci se zacílením útoku

Veškeré další skutečnosti, které mohou útočníkovi pomoci v zacílení útoku na vybranou společnost. Často se jedná například o typ používaného software, hardware, jeho verze, používané služby třetích stran, sídlo společnosti, umístění kanceláří, míra fyzického zabezpečení kanceláří a podobně. V neposlední řadě se v této části objeví případné indikátory toho, že testovaná společnost byla napadena (například se mohou vyskytovat nějaká data společnosti na black marketech či na různých serverech pro sdílení dat, například typu pastebin). V případě naší Blackhat analýzy se v této kategorii věnujeme pouze skutečnostem, které mají nějakou relevanci k technické stránce zabezpečení společnosti.

Weaponization - vytvoření a návrh útoku v případě zjištění použitelných skutečností

V případě, že útočník nalezne v první fázi takové nedostatky, které by bylo možné zneužít k přímému útoku na danou společnost a na daná aktiva, připraví útočník v této fázi samotný útok. Například v situaci, kdy útočník nalezne bezpečnostní chybu ve webové aplikaci společnosti, si připraví takový payload, který mu umožní dostat se k takovým informacím, které si dal za cíl získat. Například v případě útoku za pomoci sociálního inženýrství si v této fázi útočník připraví postup útoku, informace, které by v případě útoku mohl použít atd.

Delivery - snaha o doručení payloadu pro provedení útoku

V této fázi se útočník pokouší o "doručení útoku". V případě útoku na některou z webových či síťových aplikací společnosti jsou většinou využívány klasické vstupní kanály dané aplikace. V případě sociálního inženýrství jsou to pak různé možnosti, například využití e-mailu, doručení útoku přes USB flashdisk poslaný v rámci "marketingové kampaně" a další.

Exploitation - samotné spuštění kódu / payloadu

Ve chvíli, kdy je útok připraven a byl doručen na cílový systém či cílovému uživateli (v případě některých útoku sociálního inženýrství), je na čase, aby byl případný payload spuštěn. K tomu ve většině případů dochází automaticky po doručení payloadu. Může k tomu však v případě některých útoků docházet jako reakce na nějakou událost, například při přihlášení administrátora do systému či otevření neznámé přílohy uživatelem.

Následující body patří k post-exploitation fázi, kterou v rámci Blackhat analýzy neprovádíme, nicméně je zde v krátkosti uvádíme pro celkovou představu

Installation

V této fázi dochází k instalaci zadních vrátek či malware v systému. Útočník si vždy připravuje půdu pro svůj návrat, aby se k úspěšně napadeným systémům mohl dostat i v případě opravení původně zneužité bezpečnostní díry.

Command & control

Vytvoření a použití zadních vrátek či jiného komunikačního kanálu pro přístup k napadenému systému.

Actions on objectives

Nyní již útočník má přístup k systému a dochází k "práci" na původním stanoveném úkolu, ať již se jedná o špionáž, sabotáž či jiné. Tento bod je finálním bodem klasického kybernetického útoku.

Závěrečné upřesnění

Oproti reálnému útoku v žádné fázi nepoužíváme social engineering z časových důvodů a snahy o co nejmenší narušení chodu firmy.

7. Výstup

Výstupem Blackhat analýzy bude report, ve kterém bude celý průběh testování detailně popsán, včetně všech metodik, testovaných zranitelností a nálezů.

Samozřejmostí je také prezentace výsledků (osobní/on-line).

appsec

APPSEC, s. r. o
Thámova 18, Praha 8
Česká republika

[redacted]

IČO: 05542812
DIČ: CZ05542812

8. Cena řešení

Název	Cena v Kč
Externí Blackhat analýza	400 000 Kč

- Ceny zahrnují veškeré práce zmíněné v návrhu řešení a veškeré režijní náklady
- Veškeré ceny jsou uvedeny bez DPH