Smlouva o zprostředkování studie proveditelnosti

číslo smlouvy objednatele: 289/2022

uzavřená podle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., **občanský zákoník**, a zákona 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 **„smlouva"**)

Článek 1: Smluvní strany

Objednatel: **Česká republika - Ministerstvo vnitra**
se sídlem: Nad Štolou 936/3, 170 34 Praha 7
IČO: 00007064
zastoupená: Ministerstvem vnitra – generálním ředitelstvím Hasičského záchranného sboru České republiky
právně jednající: plk. Ing. Jan Brothánek, ředitel Odboru komunikačních a informačních systémů
doručovací adresa: MV-GŘ HZS ČR, Kloknerova 26, 148 01 Praha 414
bankovní spojení: ČNB Praha 1
číslo účtu: 8908881/0710
ID datové schránky: 84taiur

*(dále jen jako **„objednatel"**)*

Dodavatel: **DATASENSE s.r.o.**
se sídlem: Sokolovská 270/201, Praha 9 Vysočany 190 00
doručovací adresa: Sokolovská 270/201, Praha 9 Vysočany 190 00
IČO: 24664812
DIČ: CZ24664812
Bankovní spojení:
číslo účtu:
právně jednající: jednatel společnosti
zapsán v rejstříku: v obchodním rejstříku vedeném rejstříkovým soudem u Městského soudu v Praze, oddíl C, vložka 164474

*(dále jen jako **„dodavatel"**)*

(objednatel a dodavatel společně též jako **„smluvní strany"**)

Podkladem pro uzavření této smlouvy je nabídka dodavatele ze dne ....., která byla pro účely zadání veřejné zakázky, označené jako Studie proveditelnosti", zadávané ve zjednodušeném podlimitním řízení dle § 3 písm. a) zákona č. 134/2016 Sb., o zadávání veřejných zakázek, zveřejněna pod systémovým číslem N006/22/V00027421 prostřednictvím národního elektronického nástroje, a která byla vybrána jako nejvýhodnější (dále jen „**veřejná zakázka**").

Článek 2: Předmět smlouvy

Předmětem smlouvy je:

a) závazek dodavatele poskytnout objednateli služby (včetně provedení děl), jejichž specifikace je uvedena v příloze č. 1 smlouvy (dále jen „**služby**“) a převést, postoupit případně poskytnout mu k nim i veškerá práva, zejména v rozsahu práv vlastnických a práv duševního vlastnictví (dále jen „**právo**“ nebo „**práva**“);

b) závazek objednatele zaplatit dodavateli za služby a práva dohodnutou cenu.

Článek 3: Místo a doba plnění

1. Místem plnění je Česká republika.
2. Doba plnění je uvedena v příloze č. 1 smlouvy. Není-li u konkrétní služby doba plnění uvedena, je objednatel povinen takovou službu dodavateli poskytnout v době přiměřené povaze dané služby, nedohodnou-li se smluvní strany písemně jinak.
3. Smluvní strany se zavazují poskytovat si součinnost; objednatel bude po dobu trvání této smlouvy poskytovat nezbytné spolupůsobení, poskytne zejména technické údaje a doplňující podklady, které si dodavatel vyžádá jako nezbytný předpoklad pro řádné, včasné a úplné splnění svého závazku.

Článek 4: Předání a převzetí plnění

1. Smluvní strany se dohodly, že plnění zachytitelné v hmotné podobě dodavatel objednateli předá v listinné podobě a současně v elektronické podobě na hmotném nosiči dat (elektronická podoba bude ve formátu PDF/A dokumentu podepsaného dodavatelem v souladu s právními předpisy a rovněž ve formátu dokumentu umožňujícího jeho volnou editaci), a to nebude-li objednatelem stanoveno v jednotlivém případě jinak, kontaktní osobě objednatele uvedené v odst. 2. tohoto článku po předchozí telefonické domluvě, na adrese MV-GŘ HZS ČR, Kloknerova 26, 148 01 Praha 4. O předání a převzetí plnění bude mezi smluvními stranami pořízen předávací protokol, jehož součástí bude i prohlášení o všech relevantních právech se ke službám vztahujících (dále jen „**protokol**“). Služby, z jejichž povahy to vyplývá, se předávají samostatně a návazně (bude-li dílo provedeno postupně, vznikají práva a povinnosti smluvních stran, jejichž povaha to připouští, zejména licence, práva z vadného plnění, na smluvní sankci či odstoupení od smlouvy, k jednotlivým stupňům díla samostatně).

2. **Kontaktní osoba objednatele** ve věcech technických a osobou odpovědnou převzít plnění je [redacted]

3. **Oprávněná osoba objednatele** ve věcech smluvních je [redacted]

4. **Kontaktní a oprávněná osoba dodavatele** ve věcech technických a osobou odpovědnou předat předmět smlouvy je [redacted]

Článek 5: Práva

1. Vlastnictví k hmotným nosičům a ostatním hmotným věcem a nebezpečí škody na věci přechází na objednatele okamžikem předání. Cena hmotných nosičů je již zahrnuta v ceně služeb. Zhotovitel pro účely předání služeb poskytuje objednateli právo dílo užít v rozsahu nezbytně nutném.
2. Dodavatel odpovídá objednateli za to, že služby nebudou mít žádné právní vady, že nebudou zatíženy právy třetích osob týkajících se zejména práv duševního vlastnictví, a že dodavatel bude zcela oprávněn disponovat bez jakéhokoli omezení veškerými právy k nim se vztahujícími. Bude-li výsledkem nebo součástí poskytovaného plnění zaměstnanecké či kolektivní dílo ve smyslu autorského zákona, dohodly se smluvní strany, že dodavatel jako zaměstnavatel či osoba, z jejíhož podnětu a pod jejímž vedením je dílo vytvářeno, postupuje ke dni předání takového díla (tzn. dnem předání služeb) právo výkonu majetkových práv k dílu na Objednatele. Bude-li výsledkem nebo součástí poskytovaného plnění dílo, u kterého objektivně nelze ze strany dodavatele na objednatele postoupit právo výkonu majetkových práv, dohodly se smluvní strany, že dodavatel ke dni předání takového díla (tzn. dnem předání služeb) poskytuje objednateli svým rozsahem neomezenou licenci k užití takového díla a to na celou dobu trvání majetkových práv k dílu s tím, že oprávnění tvořící licenci jsou dále postupitelná i poskytnutelná formou podlicence. Pro odstranění všech pochybností smluvní strany výslovně uvádějí, že licence zejména opravňuje nabyvatele takové dílo (díla) užít v původní nebo zpracované či jinak změněné podobě, všemi známými způsoby užití, v neomezeném rozsahu (množstevním i územním), pro veškeré myslitelné účely a ve veškerých možných formách, rozmnožovat jej, spojit jej s jiným dílem nebo jej zařadit do díla souborného. Dodavatel se zavazuje za tímto účelem zajistit řádné a nerušené užívání díla objednatelem, včetně případného zajištění dalších souhlasů a licencí od autorů děl v souladu s autorským zákonem, popř. od vlastníků jiných práv duševního vlastnictví v souladu s právními předpisy. Dodavatel se zavazuje, že objednateli uhradí veškerou újmu, která objednateli vznikne v důsledku toho, že objednatel nebude moci dílo užívat řádně a nerušeně. Objednateli též nejpozději dnem předání díla svědčí práva pořizovatele databáze ve smyslu § 88 a násl. autorského zákona.
3. Objednatel není povinen licenci poskytnutou podle odstavce 2 tohoto článku využít. Zhotovitel je povinen zdržet se výkonu práva dílo jakýmkoliv způsobem užít.

Článek 6: Cena a platební podmínky

1. Cena za služby a práva (dál jen „**celková cena**") byla stanovena dohodou smluvních stran, takto: **750 000,- Kč** (slovy: sedmsetpadesáttisíc korun českých) **bez DPH**, 157 500,- Kč DPH, **celková cena s DPH 907 500,-** Kč (slovy: devětsetsedmtisícpětset korun českých).
2. Cena za jednotlivé fáze:
   - Fáze 1: : **435 000,- Kč** (slovy: čtyřistatřicetpěttisíc korun českých) **bez DPH**, 91 350,- Kč DPH, **celková cena s DPH 526 350,-** Kč (slovy: pětsetdvacetšesttisíctřistapadesát korun českých).
   - Fáze 2: : **315 000,- Kč** (slovy: třistapatnácttisíc korun českých) **bez DPH**, 66 150,- Kč DPH, **celková cena s DPH 381 150,-** Kč (slovy: třistaosmdesátjednatisícstopadesát korun českých).
3. Celková cena je cenou konečnou, nejvýše přípustnou a nepřekročitelnou. Celková cena bude uhrazena objednatelem ve dvou dílčích plněních. První plnění se uskuteční na základě splnění Fáze č. 1 po odsouhlasení dokumentace OHA a druhé plnění po převzetí Fáze č. 2, po ukončení zadávacího řízení (poskytnutí služeb a získání práv), a to na základě faktur vystavených dodavatelem.
4. Daňové doklady (faktury) budou dodavatelem vystaveny v souladu s ustanovením § 28 odst. 3 a 4 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, a dalších dotčených právních předpisů (např. občanského zákoníku, zákona o účetnictví) a objednateli doručen nejpozději do 15 dnů ode dne převzetí dílčí Fáze.
5. Objednatel je povinen dodavatelem oprávněně vystavenou fakturu zaplatit na účet dodavatele do třiceti (30) kalendářních dnů ode dne jejího doručení objednateli. Poskytovatel doručí fakturu do datové schránky objednatele uvedené v článku 1 smlouvy.

   na faktuře bude jako identifikace objednatele uvedeno:

   ČR - Ministerstvo vnitra
   Nad Štolou 936/3
   170 34 Praha 7
   zastoupená:
   MV – GŘ HZS ČR
   Kloknerova 26
   pošt. přih. 69
   148 01 Praha 414
6. Smluvní strany se dohodly, že platba bude provedena v českých korunách (CZK) výhradně na účet dodavatele.
7. Dodavatel je povinen přiložit k faktuře originál protokolu (protokolů).
8. Objednatel je oprávněn před uplynutím lhůty splatnosti faktury vrátit bez zaplacení fakturu, která neobsahuje náležitosti stanovené touto smlouvou či právními předpisy nebo budou-li tyto údaje uvedeny chybně či fakturu, ke které nebude přiložen protokol. Dodavatel je povinen podle povahy nesprávnosti fakturu opravit nebo nově vyhotovit, přičemž vrácením faktury se objednatel nemůže dostat do prodlení se splněním svých závazků. Okamžikem doručení

náležitě doplněné či opravené faktury začne běžet nová lhůta splatnosti faktury v délce třiceti (30) kalendářních dnů.

9. Objednatel nebude poskytovat dodavateli jakékoliv zálohy na úhradu celkové ceny.

Článek 7: Záruka za jakost

1. Dodavatel tímto objednateli poskytuje smluvní záruku za jakost služeb, jejichž povaha to připouští, resp. zaručuje se, že služby (díla) budou svými vlastnostmi odpovídat všem parametrům ve smlouvě sjednaným, i parametrům uvedeným v zadávací dokumentaci veřejné zakázky, a že si tyto vlastnosti zachovají po dobu trvání smlouvy.

Článek 8: Smluvní pokuta a úrok z prodlení

1. V případě nedodržení smlouvou sjednané doby plnění resp. v případě nedodržení termínu sjednaného podle věty druhé čl. 3 odst. 2 smlouvy, je dodavatel povinen uhradit objednateli smluvní pokutu ve výši 0,1 % z celkové ceny za každý i započatý kalendářní den prodlení, a to zvlášť za každou službu nebo právo, s jejichž poskytnutím je v prodlení.
2. Jestliže dodavatel poruší jakoukoliv povinnost podle čl. 9 této smlouvy, zavazuje se dodavatel uhradit objednateli smluvní pokutu ve výši 500.000,- Kč (slovy: pět set tisíc korun českých) za každé jednotlivé porušení smlouvy.
3. Smluvní pokuta je splatná do čtrnácti (14) kalendářních dnů ode dne jejího uplatnění.
4. Zaplacením smluvní pokuty není dotčen nárok na náhradu újmy ani povinnost dodavatele řádně plnit své povinnosti, zejména poskytnout plnění smlouvy.

Článek 9: Zvláštní ujednání

1. Dodavatel prohlašuje, že disponuje veškerými odbornými, materiálními a technickými předpoklady potřebnými pro splnění této smlouvy. Dodavatel též prohlašuje, že ke dni podpisu této smlouvy není v úpadku nebo ve stavu hrozícího úpadku ve smyslu zákona č. 182/2006 Sb., o úpadku a způsobech jeho řešení (insolvenční zákon), ve znění pozdějších předpisů.
2. Dodavatel i objednatel jsou povinni zachovat mlčenlivost o všech skutečnostech, údajích a informacích týkajících se druhé strany, které mají povahu obchodního tajemství v rozsahu a za podmínek § 504 občanského zákoníku, případně které budou druhou smluvní stranou označeny za důvěrné, a o kterých se dozví v souvislosti s plněním této smlouvy, a zavazují se, že tyto skutečnosti nesdělí ani jiným způsobem neposkytnou žádné třetí osobě a zajistí přiměřenou ochranu a utajení těchto skutečností a to zejména technickými a bezpečnostními opatřeními vyplývajících z právních předpisů na úseku kybernetické bezpečnosti a zjištěními z auditů kybernetické bezpečnosti.
3. Dodavatel je povinen zavázat povinností mlčenlivosti podle odstavce 2 tohoto článku všechny osoby, které se budou podílet na plnění této smlouvy z jeho strany (zejména na dodání

studie). Za porušení povinnosti mlčenlivosti těmito osobami odpovídá dodavatel, jako by povinnost porušil sám.

4. Závazky uvedené v čl. 9 odst. 2. platí i po zániku této smlouvy bez časového omezení po dobu, po kterou předmětné informace mají nebo mohou mít povahu obchodního tajemství nebo důvěrných informací.
5. Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím osob oprávněných jednat jménem smluvních stran.
6. Dodavatel je povinen ve smyslu 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.
7. Smluvní strany uzavírají tuto smlouvu v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů, a podle Nařízení Evropského parlamentu a Rady č. 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).
8. Ukončením účinnosti této smlouvy nejsou dotčena ustanovení smlouvy týkající se nároků z odpovědnosti za vady, nároků z odpovědnosti za újmu a nároků ze smluvních pokut, ustanovení o ochraně informací, ani další ustanovení a nároky, z jejichž povahy vyplývá, že mají trvat i po zániku účinnosti této smlouvy.
9. Smlouvu lze ukončit písemnou dohodou smluvních stran, jejíž součástí bude i vypořádání vzájemných závazků a pohledávek.
10. Za podstatné porušení této smlouvy dodavatelem, které zakládá právo objednatele na odstoupení od této smlouvy nebo její vypovězení bez výpovědní doby, se považuje zejména prodlení dodavatele s předáním/poskytnutím plnění o více než sedm (7) kalendářních dnů.
11. Objednatel je dále oprávněn od této smlouvy odstoupit nebo ji vypovědět bez výpovědní doby v případě, že

    a) vůči dodavateli je vedeno insolvenční řízení, v němž bude vydáno rozhodnutí o úpadku,

    b) insolvenční návrh bude zamítnut pro nedostatek majetku pro účely úhrady nákladů insolvenčního řízení,

    c) dodavatel vstoupí do likvidace,

    d) bankovní účet určený k úhradě dodavateli není evidován v registru plátců DPH.

12. Dodavatel je oprávněn od smlouvy odstoupit v případě, že objednatel bude v prodlení s úhradou svých peněžitých závazků vyplývajících z této smlouvy po dobu delší než šedesát (60) kalendářních dní.

Článek 10: Oddělitelnost

Stane-li se kterékoli ustanovení smlouvy neplatným, neúčinným nebo nevykonatelným, zůstává platnost, účinnost a vykonatelnost ostatních ustanovení smlouvy neovlivněna a nedotčena, nevyplývá-li z povahy daného ustanoveni nebo obsahu smlouvy, že toto

ustanovení nelze oddělit od ostatního obsahu smlouvy. Smluvní strany se zavazují nahradit po vzájemné domluvě dotčené ustanovení ustanovením novým, blížícím se svým obsahem nejvíce účelu neplatného, neúčinného či nevykonatelného ustanovení.

Článek 11: Ostatní ujednání

1. Kontaktní osoby smluvních stran jsou oprávněny k poskytování součinnosti podle této smlouvy.
2. Tato smlouva nabývá platnosti dnem podpisu smluvních stran a podle § 6 odst. 1 zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů, účinnosti dnem uveřejnění prostřednictvím registru smluv.
3. V souladu se zákonem o registru smluv, se smluvní strany dohodly, že objednatel zašle tuto smlouvu správci registru smluv k uveřejnění ve lhůtě, stanovené tímto zákonem. Osobní údaje smluvních stran před odesláním budou anonymizovány v souladu se zákonem č. 110/2019 Sb., o zpracování osobních údajů.
4. Smluvní strany nemají zájem, aby nad rámec výslovných ustanovení této smlouvy byla jakákoliv práva a povinnosti dovozovány z dosavadních zvyklostí či budoucí praxe zavedené mezi smluvními stranami či zvyklostí zachovávaných obecně či v odvětví týkajícím se předmětu plnění podle těchto smluv, ledaže je stanoveno jinak. Vedle shora uvedeného si smluvní strany potvrzují, že si nejsou vědomy žádných dosud mezi nimi zavedených obchodních zvyklostí či praxe.
5. Smluvní strany se dohodly, že dodavatel přebírá podle § 1765 občanského zákoníku riziko změny okolností, zejména v souvislosti s cenou za poskytnuté plnění, požadavky na poskytované plnění a licenčními podmínkami výrobce.
6. Smluvní strany vylučují aplikaci ustanovení § 557 občanského zákoníku na tuto smlouvu.
7. Smluvní strany se dohodly, že tato smlouva se bude řídit příslušnými ustanoveními občanského zákoníku, nesjednali-li výslovně jinak.
8. Tuto smlouvu lze měnit, doplňovat či zrušit dohodou smluvních stran, a to písemnými listinnými dodatky číslovanými vzestupnou řadou.
9. Smluvní strany se zavazují, že veškeré spory vzniklé v souvislosti s realizací této smlouvy budou přednostně řešeny smírnou cestou. Nedojde-li k dohodě, budou spory řešeny před příslušnými obecnými soudy.
10. Veškerá korespondence mezi smluvními stranami, včetně jejich prohlášení, je bez vlivu na sjednaný obsah práv a povinností smluvních stran dle této smlouvy, není-li ve smlouvě stanoveno jinak.
11. Tato smlouva je závazná i pro případné právní nástupce obou smluvních stran. Dodavatel není bez písemného souhlasu objednatele oprávněn smlouvu postoupit třetí straně.
12. Tato smlouva je vyhotovena v elektronické podobě. Smluvní strana podepisující tuto smlouvu jako druhá v pořadí je povinna prokazatelně doručit podepsanou smlouvu druhé smluvní straně.

13. Smluvní strany prohlašují, že předem souhlasí, v souladu se zněním zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, s možným zpřístupněním, či zveřejněním všech úkonů a okolností s touto smlouvou souvisejících, včetně těch, ke kterým může kdykoliv v budoucnu dojít.
14. Smluvní strany deklarují autentičnost této smlouvy svým podpisem a zároveň prohlašují, že smlouva nebyla ujednána v tísni ani za jinak jednostranně výhodných podmínek.
15. Příloha č. 1 specifikace služeb.

    Příloha č. 2 čestná prohlášení

V Praze dne viz el. podpis

Za objednatele:

plk. Ing. Jan Brothánek
ředitel Odboru komunikačních a informačních systémů

V Praze dne viz el. podpis

Za dodavatele:

jednatel společnosti

Příloha č. 1 Smlouvy o zprostředkování studie proveditelnosti – specifikace služeb

Předmětem plnění je zajištění poradenských a odborných služeb v rámci přípravy žádostí o dotaci pro financování 3 projektů zvýšení kybernetické bezpečnosti ve struktuře a rozsahu požadovaném ze strany dotačního titulu IROP II pro dotační období 2021-2027.

V rámci každého ze 3 (tří) uvedených projektů (dále také jen „Projekt P1, P2, P3) bude zajištěno následujících pět bodů rozdělených do dvou fází:
Fáze č. 1:
a) Zpracování studie proveditelnosti,
b) Zpracování a předložení dokumentace pro Odbor hlavního architekta,
Fáze č. 2:
c) Zpracování žádosti o dotaci,
d) Komplexní přípravu podkladů pro navazující zadávací řízení,
e) Spolupráci při administraci navazujících zadávacích řízení.

Fáze 1:

a) Zpracování studie proveditelnosti

Vypracování kompletní studie proveditelnosti pro dotační titul IROP II dotačního období 2021-2027 v oblasti kybernetické bezpečnosti. Zpracování studie proveditelnosti se bude skládat ze dvou základních oblastí.

První oblastí studie proveditelnosti je **zpracování návrhové/technické části studie proveditelnosti** obsahující, zejména:
- výchozí stav u zadavatele, analýzu a popis výchozí situace;
- řešení projektu – podrobný popis řešení, přehled navrhovaných technických opatření (definice projektového záměru) – rozsahu, obsahu a výstupů projektu se zohledněním priorit a jejich vzájemných vazeb s cílem zajištění smysluplného a efektivního využití finančních a kapacitních zdrojů. Základní popis požadované HW a SW infrastruktury a souvisejících služeb;
- výčet IS zabezpečovaných v rámci projektu, identifikace nedostatků a potřeb s ohledem na požadavky na zajištění kybernetické bezpečnosti dle vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat;
- navázání navrhovaných opatření na konkrétní technické opatření a konkrétní § zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů;
- přehled výstupů projektu a jejich kvantifikace, návrh monitorovacích indikátorů;
- zdůvodnění potřebnosti realizace projektu.

Druhou oblastí studie proveditelnosti je **zpracování dotační části studie proveditelnosti** obsahující, zejména:
- popis vazby projektu na podmínky IROP II;
- popis cílů a cílových skupin projektu;
- popis indikátorů a výstupů projektu, revize monitorovacích indikátorů projektu;
- popis realizačního týmu projektu;

- popis udržitelnosti projektu;
- realizace a popis průzkumu trhu;
- stanovení rozpočtu projektu, zpracování finanční analýzy a popis majetku projektu;
- úprava Studie proveditelnosti dle konkrétních požadavků.

Součástí těchto služeb musí být také monitorování vývoje všech požadavků na tento dotační titul IROP II.

Výstupem bude:
- zpracovaní studie proveditelnosti pro IROP II.

Výstupní dokumentace:
- studie proveditelnosti ve struktuře odpovídající požadavkům výzvy č. 10 IROP „Kybernetická bezpečnost", která bude upravena podle požadavků nového dotačního titulu IROP II.

b) Zpracování a předložení dokumentace pro Odbor hlavního architekta

Součástí plnění je vypracování dokumentace pro odbor hlavního architekta eGovernmentu Ministerstva vnitra, (dále také jen „OHA") pro schválení ICT (Information and Communication Technologies - Informační a komunikační technologie) projektu. Dále dodavatel zajistí předložení dokumentace na OHA a poskytne veškerou součinnost, a to zejména zpracování doplnění, vyjádření nebo jiných nezbytných činností vedoucích ke schválení dokumentace odborem hlavního architekta.

Zpracování dokumentace pro OHA bude obsahovat, zejména:
- identifikaci motivačních aspektů včetně výkonnostní architektury;
- zpracování byznys architektury;
- návrh aplikační architektury v podobě konceptuálních návrhů dílčích informačních systémů realizovaných projektem;
- návrh řešení technologické architektury v podobě HW a SW infrastruktury;
- návrh řešení komunikační infrastruktury;
- návrh bezpečnostní architektury;
- vypracování kontrolního vyhodnocení shody s Národním architektonickým plánem;
- zhodnocení využívání sdílených služeb veřejné správy;
- zpracování TCO (total cost of ownership – celkové náklady na vlastnictví) projektu;
- zpracování dílčích architektonických schémat.

Výstupem bude:
- kompletní požadované dokumenty pro schválení ICT projektu na OHA;
- administrace dokumentace pro OHA včetně jejich **předložení do 15. 12. 2022** až do jejího konečného schválení OHA.

Výstupní dokumentace:
- kompletní dokumentace pro OHA (technického řešení pro žádost OHA).

Fakturace
- **vystavení faktury bude provedeno po odsouhlasení dokumentace OHA**

Fáze 2:

c) Zpracování žádosti o dotaci

Součástí plnění je zpracování vlastní žádosti v dotačním nástroji IS MS2021+ včetně přípravy a kompletace všech povinných příloh a dokumentů.

Výstupem bude:
- administrace žádosti o dotaci;
- schválení žádosti ze strany Řídicího orgánu k financování vč. vydání právního aktu (tj. Registrace akce a Rozhodnutí o poskytnutí dotace včetně Podmínek)

Výstupní dokumentace:
- dotační dokumentace v nástroji IS MS2021+.

d) Komplexní příprava podkladů pro navazující zadávací řízení

Součástí plnění je komplexní příprava pokladů pro zadávací řízení veřejných zakázek, na základě kterých dojde k pořízení řešení naplňující záměry uvedené ve studii proveditelnosti. Komplexními podklady se rozumí veškeré informace nezbytné pro zadávací podmínky, tedy vč. průzkumu trhu, definování technické specifikace, požadavků na kvalifikaci apod.

Součástí jednotlivých projektů bude následující složení zadávacích řízení:
- **Projekt P1 -** 2 veřejné zakázky v otevřeném nadlimitním řízení
- **Projekt P2 -** 1 veřejné zakázky v otevřeném nadlimitním řízení
- **Projekt P3 -** 1 veřejná zakázka v otevřeném nadlimitním řízení

Připravované podklady budou zapracovávány ze strany dodavatele do vzorových dokumentů objednatele. Tyto dokumenty budou poskytnuty dodavateli.

Výstupem bude:
- příprava podkladů pro navazující zadávací řízení;

Výstupní dokumentace:
- kompletně zpracované zadávací podmínky pro jednotlivá zadávací řízení.

e) Spolupráce při administraci navazujících zadávacích řízení

Součástí plnění je spolupráce dodavatele při administraci navazujících zadávacích řízení, a to především v případě:
- žádostí o vysvětlení zadávací dokumentace
- kontrola splnění zadávacích podmínek (posouzení, zda nabízený předmět plnění odpovídá zadávacím podmínkám)
- námitek proti zadávacím podmínkám či úkonům zadavatele
- řízení před ÚOHS

Samotná administrace procesu zadání navazujících zadávacích řízení bude zajišťována ze strany objednatele a není tedy předmětem této smlouvy.

Výstupem bude:
- ukončení zadávacích řízení.
-

Fakturace
- **vystavení faktury bude provedeno po ukončení zadávacího řízení.**

Dílčí projekty

1. a) Nasazení systému IDM v prostředí HZS ČR

Technické opatření VoKB §19 Nástroj pro ověřování identity uživatelů a §20 Řízení přístupových oprávnění.

Cílem tohoto projektu je především získat nástroj na správu identit, řízení přístupových oprávnění a jejich kontrolu v organizaci, napojení na personální systém (HR) a otestování v ostrém provozu na sadě informačních systémů. Následným krokem je pak postupné zapojování všech aktiv organizace do tohoto systému.

Návrh řešení:

Implementace systému IDM a napojení všech aktiv v organizaci je chápáno jako dlouhodobá koncepce řízení identit, přístupových oprávnění, jejich kontroly a zvýšení zabezpečení přístupů k aktivům organizace. S ohledem na velikost organizace a velkému množství aktiv, nelze pojmout celé spektrum v jednom projektu, protože z pohledu naší organizace systém IDM nemá řídit pouze informační systém spadající do kritické infrastruktury, ale veškerá aktiva, ke kterým je potřeba přístupy řídit. Tato aktiva tak obsahují jednak informační systémy kritické infrastruktury, ostatní informační systémy, systémy pro kontrolu přístupů do zabezpečených lokalit a ostatních prostor organizace.

Primární cíle tohoto projektu lze tak specifikovat takto:

- Analýza interních a externích subjektů, resp. přístupových oprávnění subjektů.
- Analýza životního cyklu identit v organizaci.
- Implementace systémového nástroje pro řízení životního cyklu identit, řízení a kontroly přístupů k jednotlivým aktivům, rekonciliace a reportování.
- Napojení zdroje identit (HR) na systém IDM.
- Definice základních business rolí určujících přístupová práva k vybraným informačním systémům.
- Definice workflow schvalovacích procesů, určující jednoznačnou zodpovědnost za konkrétní přístupová oprávnění.
- Postupné napojení informačních systémů na IDM.
- Řešení musí kromě online řízení oprávnění a identit do připojených aplikací podporovat i tzv. offline řízení oprávnění a identit na základě manuálního potvrzení akce odpovědnou osobou nebo na základě informací získaných z exportu aplikace.

Vazby a závislosti na jiných projektech:

Vazby a závislosti tohoto projektu s ohledem na jeho šíři a složitost jsou rozsáhlé.

Jednou z hlavních podmínek zapojení konkrétních aktiv do systému IDM je zavedení jednotného přihlašování pomocí SSO. Jedná se o jednotný způsob ověřování identity oproti Active Directory. Tento projekt, tzn. úpravy jednotlivých systémů, již v naší organizaci probíhají a postupně jsou systémy upravovány tak, aby splňovaly požadavky na standardní

ověřování – autentizaci. Hlavní podmínkou pro zapojení aktiv je však stav připravenosti a použitých technologií jednotlivých systémů pro napojení do systému IDM.

Jednotlivé systémy lze z pohledu připravenosti a použitých technologií rozdělit do několika kategorií:

- Systémy, které splňují technologické požadavky a jsou po stránce strukturální a technické připraveny k napojení na systém IDM. Bohužel tato skupina systémů je velmi malá a tyto systémy jsou zařazeny do první sady systémů, které budou napojeny v první vlně nasazení systému IDM.
- Systémy, které splňují technologické požadavky a jsou po stránce strukturální připraveny k napojení na systém IDM, ale po stránce technické je nelze připojit. Tyto systému bude nutné nejdříve upravit tak, aby bylo možné systém IDM napojit.
- Systémy, které splňují technologické požadavky a nejsou po stránce strukturální připraveny k napojení na systém IDM a po stránce technické je nelze připojit. Tyto systému bude nutné nejdříve upravit tak, aby jejich struktura vyhovovala standardním bezpečnostním požadavkům a aby je bylo možné na systém IDM napojit.
- Systémy, které nesplňují technologické ani strukturální požadavky a nelze je žádným způsobem napojit na systém IDM. Jedná se o staré systémy, kde jejich stáří v některých případech přesahuje 20 let a u těchto systémů bude muset před napojením do systému IDM předcházet analýza s následným vývojem a přechodem na nejnovější technologie a standardy tak, aby i tyto systémy bylo možné do IDM napojit.

Mezi neméně významné vazby patří analýza a definice business rolí tak, aby tyto business role obsahovaly všechny potřeby a kombinace přístupových oprávnění k jednotlivým aktivům v celé organizaci. Součástí tohoto procesu je i definování jasné zodpovědnosti a schvalovacích procesů za konkrétní přístupová oprávnění k aktivům organizace.

Plánované etapy projektu:

- Etapa 1 - Postupné napojení informačních systémů, ověřovací a následně ostrý provoz.

1. b) Implementace více faktorové autentizace HZS ČR

Technické opatření VoKB §19 Nástroj pro ověřování identity uživatelů, §25 Aplikační bezpečnost a §26 Kryptografické prostředky.

Návrh řešení:

Cílem tohoto projektu je především zavedení prostředků pro ověřování autenticity požadavků oprávněných osob s užitím vícefaktorové autentizace v prostředí informačních systémů a infastruktury HZS ČR, napojení na systém IDM a otestování v ostrém provozu na sadě informačních systémů. Následným krokem je pak postupné zapojování všech aktiv organizace do tohoto systému.

Plánované řešení umožní užívání prostředků pro zajištění práce s kryptografickými prostředky na bázi asymetrické kryptografie a infrastruktury veřejných klíčů, včetně správy kryptografického materiálu, tak také potřeby v oblasti správy a podpory prostředků pro tvorbu a ověřování elektronických pečetí, elektronických podpisů a důvěryhodných časových razítek, a to jak v rozsahu vlastní báze prostředků zajištění důvěry, tak i v rozsahu prostředků pro zajištění důvěry třetích stran.

Požadavky na řešení:

Systém PKI
Konfigurace hierarchie certifikačních autorit pro vydávání certifikátů pro interní uživatele z Active Directory, vydávání certifikátů pro externí subjekty k zabezpečení komunikace, vydávání certifikátů pro servery a zařízení k zabezpečení chráněné komunikace.

- Interní CA.
- Interní CA pro účelové uživatelské certifikáty.
- Interní CA pro účelové certifikáty zařízení (počítače, HW prvky).
- Interní CA pro externí subjekty.
- Soukromé klíče certifikačních autorit musí být bezpečně uloženy v Hardware Security Modulu (HSM).

Řešení musí obsahovat veškerý potřebný hardware, software a licence s podporou na 5 roků, tedy všechny servery, operační systémy a další potřebné moduly.

Kryptografické servery
Hardware Security Modul musí splňovat standard FIPS 140–2 level 3 a level 4 pro fyzickou bezpečnost. Dále musí umožnit následující funkce:

- Vytváření interních přístupových účtů s možným omezením přístupu pouze k určitému klíči nebo skupině klíčů.
- Modulární systém interního firmware.
- Správa klíčů: generování, import / export, backup / restore.
- Zálohování citlivých dat pouze v šifrované podobě pomocí předem definovaného šifrovacího klíče (systém nesmí umožnit exportovat citlivá data v nešifrované podobě nebo pouze chráněné heslem).
- Zařízení musí být schopné vnitřně uchovat více než 25000 RSA klíčů o velikosti 4096 bitů a více než 150000 AES256 klíčů.
- Zabudování do racku.
- Administrativní přístup pouze pomocí čipových karet.
- Rozšiřitelnost o nové šifrovací standardy.
- Podpora časových razítek (timestamp).
- Podpora kryptografických algoritmů: RSA, ECDSA, AES, e-curve.
- Podpora Microsoft Certificate Services.

Pro zajištění provozní stability budou HW a HSM moduly implementovány v režimu High Availibility (clusterové zapojení).

Token Management systém
Obecné vlastnosti:

- Management životního cyklu čipových karet a USB tokenů.
- Podpora vydávání, odvolání.
- Podpora automatického zálohování a obnovy uživatelských oprávnění.
- Podpora evidence ztracených nebo zničených tokenů nebo čipových karet.
- Integrace s Microsoft Active Directory.
- Centrální správa.

Certifikační autority
Obecné vlastnosti:

- Stažení CRL pomocí protokolů LDAP a HTTP / S.

- Software tvořící jádro certifikační autority musí být hodnocen podle CC na úroveň EAL 4+ a vyšší.
- Integrace s Active Directory.
- Možnost definovat a vydávat certifikáty podle šablon certifikátů.
- Úložiště šablony certifikátů v Active Directory.
- Podpora Windows Autoenrollment procesu.
- Podpora čipových karet a USB tokenů.
- Podpora Simple Certificate Enrollment Protocol (SCEP).

OTP autentizační servery
Instalace a konfigurace systému ověřování na základě jednorázových klíčů s podporou event–based, OTP (HOTP definovaný vRFC 4226) a time–based OTP (např. standard TOTP definovaný v RFC 6238).
Aplikační integrace workflow OTP systémů s uživatelskými CA a ActiveDirectory pro zajištění OTP key enrollmentu uživatelům na základě údajů z PKI-CA a registrace klíče v ActiveDirectory.
Self-enrollment portál pro uživatele a aplikace.

Zabezpečení elektronické pošty
Konfigurace certifikační autority pro vydávání certifikátů pro zabezpečení elektronické pošty (šifrování a elektronický podpis). Certifikační autorita bude rovněž uchovávat soukromé klíče těchto certifikátů pro případ obnovy, které bude spravovat správce obnovy klíčů. O uživatelské certifikáty budou počítače uživatelů žádat pomocí automatického procesu vydávání (autoenrollment). Soukromé klíče těchto certifikátů budou uloženy v rámci zabezpečeného úložiště operačního systému.

Obecné vlastnosti:
- Podpora aplikace Microsoft Outlook 2010 a vyšší bez dodatečných SW modulů.
- Podpora AES šifrování.
- Automatické vydávání certifikátů řízené pomocí GPO.
- Centrální úložiště šifrovacích certifikátů v Active Directory.
- Podpora šifrované zálohy soukromého klíče v databázi certifikačního úřadu.

Součástí zabezpečení elektronické pošty je i implementace řešení na uživatelské stanice.

Zabezpečení aplikací PKI-SSO
Konfigurace certifikační autority pro vydávání certifikátů pro zabezpečení úkonů v aplikacích třetích stran s užitím univerzálního PKI-SSO klientu (šifrování a elektronický podpis). Certifikační autorita bude rovněž uchovávat soukromé klíče těchto certifikátů pro případ obnovy, které bude spravovat správce obnovy klíčů. O uživatelské certifikáty budou počítače uživatelů žádat pomocí automatického procesu vydávání (autoenrollment). Soukromé klíče těchto certifikátů budou uloženy v rámci zabezpečeného úložiště operačního systému.

Obecné vlastnosti:
- IN / OUT cut-end vstup a výstup s podporou podepisování kontejneru schránky.
- Podpora AES šifrování.
- Automatické vydávání certifikátů řízené pomocí GPO.
- Centrální úložiště šifrovacích certifikátů v Active Directory.
- Podpora šifrované zálohy soukromého klíče v databázi certifikačního úřadu.

Součástí zabezpečení s užitím PKI-SSO agenta je i implementace řešení na uživatelské stanice.

Zabezpečení aplikačních serverů
Konfigurace certifikační autority pro vydávání certifikátů pro zabezpečení komunikace aplikačních serverů a infrastrukturních celků. Certifikační autorita bude rovněž uchovávat soukromé klíče těchto certifikátů pro případ obnovy, které bude spravovat správce obnovy klíčů. O serverové certifikáty budou zařízení žádat pomocí automatického procesu vydávání (autoenrollment) nebo s asistencí správce zařízení. Soukromé klíče těchto certifikátů budou uloženy v rámci zabezpečeného úložiště operačního systému nebo jiném zabezpečeném úložišti zařízení (např. JAVA úložiště, event. HW / HSM úložiště).

Pro zajištění interakce se servery bude rovněž aplikováno rozhraní pro podporu autentizace bezklíčovým ověřením metodami OTP (One Time Password – jednorázové heslo).

Zabezpečení přihlašování na koncových stanicích
Konfigurace certifikační autority pro vydávání certifikátů pro zajištění. Certifikační autorita bude rovněž uchovávat soukromé klíče těchto certifikátů pro případ obnovy, které bude spravovat správce obnovy klíčů. O serverové certifikáty budou zařízení žádat pomocí automatického procesu vydávání (autoenrollment) nebo s asistencí správce zařízení. Soukromé klíče těchto certifikátů budou uloženy v rámci zabezpečeného úložiště operačního systému nebo jiném zabezpečeném úložišti zařízení (např. JAVA úložiště, event. HW / HSM úložiště).

Součástí zabezpečení je i implementace řešení na uživatelské stanice.

<u>Vazby a závislosti na jiných projektech:</u>

Vazby a závislosti tohoto projektu s ohledem na jeho šíři a složitost jsou rozsáhlé.

Jednou z hlavních podmínek zapojení konkrétních aktiv k užívání vícefaktorové autentizace, jak je předpokládána legislativou, je integrace s prostředky pro ověřování identity v systémech HZS ČR. Jedná se o jednotný způsob ověřování identity oproti AD. Tento projekt, tzn. úpravy jednotlivých systémů, již v naší organizaci probíhá a postupně jsou systémy upravovány tak, aby splňovaly požadavky na standardní ověřování – autentizaci s užitím technických prostředků autentizace prostřednictvím metod pokročilé kryptografie, avšak zatím bez možnosti užití více faktorů autentizace. Rozšiřující podmínkou pro další potřebné způsoby užití vícefaktorové autentizace a užívání prostředků infrastruktury veřejných klíčů je jejich integrace v aplikacích a systémech pro využití v oblasti přihlašování k systémům a aplikacím, tvorby, správy a ověřování elektronických podpisů a pečetí v transakcích a pořizování elektronických časových razítek v důležitých úkonech ukládání informací a konzervace dat. Hlavní podmínkou pro zapojení aktiv je tedy také stav připravenosti a použitých technologií jednotlivých systémů pro její užití.

Jednotlivé systémy a aplikace lze z pohledu připravenosti a použitých technologií rozdělit do několika kategorií:

- Systémy, které splňují technologické požadavky a jsou po stránce strukturální a technické připraveny k užívání vícefaktorové autentizace a úkonů elektronického ověřování a podepisování. Tato skupina systémů je velmi malá a tyto systémy jsou zařazeny do první sady systémů, které budou napojeny v první vlně nasazení systému.
- Systémy, které splňují technologické požadavky a jsou po stránce strukturální připraveny k užívání vícefaktorové autentizace a úkonů elektronického ověřování a podepisování, ale po stránce technické ji nelze bez dalšího aplikovat řízeně v potřebném rozsahu. Tyto systému bude nutné nejdříve upravit tak, aby bylo možné systém napojit k užívání vícefaktorové autentizace a úkonů elektronického ověřování a podepisování.
- Systémy, které splňují technologické požadavky a nejsou po stránce strukturální připraveny k užívání vícefaktorové autentizace a úkonů elektronického ověřování a podepisování a po stránce technické je nelze připojit. Tyto systému bude nutné nejdříve upravit tak, aby jejich struktura vyhovovala standardním bezpečnostním požadavkům a aby je bylo možné upravit k užívání vícefaktorové autentizace a úkonů elektronického ověřování a podepisování.
- Systémy, které nesplňují technologické ani strukturální požadavky a nelze je žádným způsobem zapojit k užívání vícefaktorové autentizace a úkonů elektronického ověřování a podepisování. Jedná se o staré systémy, kde jejich stáří v některých případech přesahuje 20 let a u těchto systémů bude muset před napojením k užívání vícefaktorové autentizace a úkonů elektronického ověřování a podepisování předcházet analýza s následným vývojem a přechodem na nejnovější technologie a standardy tak, aby i tyto systémy bylo možné užívat společně s vícefaktorovou autentizací a úkony elektronického ověřování a podepisování.

Mezi významné vazby patří integrace s autorizačními funkcemi IDM a propojení se systémy řízení rolí a oprávnění.

Plánované etapy projektu:

- Etapa 1 - pořízení a implementace řešení, pasivní napojení pilotní sady systémů.
- Etapa 2 - aktivní napojení pilotní sady systémů a ostrý provoz.

2. Nasazení managementu pro správu privilegovaných účtů pro infrastrukturu v prostředí HZS ČR

Technické opatření VoKB §12 Řízení přístupu a §20 Nástroj pro řízení přístupových oprávnění.

Cílem projektu je správa a zabezpečení přístupů privilegovaných uživatelů k administrovaným systémům. Naprostá většina kybernetických útoků na systémy státní a veřejné správy, ale i na komerční společnosti, byla a je vedena přes privilegované účty. Ať už se jedná o sofistikovaný dlouhotrvající externí útok typu APT, či o zneužití privilegovaného účtu ze strany zaměstnance či zaměstnance dodavatele IT služeb, vždy se jedná o významné ohrožení daného subjektu. Informační prostředí HZS ČR je tvořeno velkým množstvím informačních systémů a rozlehlou síťovou infrastrukturou, na které je chod celé organizace závislý. Každý z prvků tohoto prostředí obsahuje privilegované účty, které jsou využívány pro jejich administraci, běžnou obsluhu, nebo se jedná o servisní účty použité v rámci integrací.

K takovým účtům mají přístup jak zaměstnanci HZS ČR, tak externí dodavatelé, kteří zajišťují provoz a rozvoj IT systémů a služeb HZS ČR.

Návrh řešení:
Implementace privileged account managementu a nasazení na systémy a prvky identifikovány jako aktiva, která podléhají správě privilegovanými účty, se týká celé infrastruktury HZS ČR.

Jedná se o aktiva založená na:
- Systémech Unix / Linux, které se využívají jako operační systémy pro různé aplikace a informační systémy.
- Systémech Windows, které jsou zapojeny do AD domén HZS ČR a jsou též využívány pro aplikace a informační systémy.
- Network (routery, switche, firewall, WCF, IPS, IDS, WIFI, jiné aktivní prvky, atd.).
- VMWare, který je využíván jako virtualizační vrstva.
- Databáze jako datové vrstvy jednotlivých systémů.
- Informační systémy.

Cílem tohoto projektu je zvýšení bezpečnosti a detailní monitorování, protože privilegované účty umožňují takřka neomezený přístup ke zdrojům příslušných systémů včetně manipulace s nimi (např. root, Administrator, sys, sa, atp.), proto jsou významným bezpečnostním rizikem. Oprávnění disponovat takovým účtem mají jak interní zaměstnanci, tak externí dodavatelé a takové oprávnění často není nijak monitorováno, a proto případné zneužití je velice těžko dohledatelné, nebo dokonce není prokazatelné. Toto riziko se vztahuje na všechny systémy, počínaje operačními systémy, databázemi, síťovými prvky až po komplexní informační systémy.

Tento systém lze rozdělit do následujících tří oblastí, které spolu úzce souvisí:
- Password Management - centrální správa privilegovaných účtů se zabezpečeným úložištěm hesel a správou přístupů k těmto účtům.
- Session Recording - zaznamenávání aktivit privilegovaných účtu včetně nahrávek obrazovek a stisků kláves (key-logging).
- Access Control - kontrola přístupu k systému pomocí privilegovaných účtů, zvýšení granularity oprávnění těchto účtů, detekce a ochrana prostředků systému na základě definovaných politik.

Požadavky na řešení:
Řešení musí podporovat možnost vícefaktorové autentizace s možností propojení na adresářové služby typu LDAP i protokol RADIUS. Pro zabránění náhodných nebo nesprávných konfigurací případně dalších chyb lidským faktorem musí řešení umožnit autorizaci "čtyř očí" – Administrátor a Schvalovatel, kde Schvalovatel bude mít možnost sledovat práci Administrátora v reálném čase.
Systém musí umožnit provádět záznamy jednotlivých spojení s možností real-time přehrávání a exportu.

Systém musí dále podporovat integraci s externím ServiceDeskem / HelpDeskem na úrovni evidence požadavků nebo žádostí o připojení na cílový systém k administraci (issue trackingu). Zajištění tohoto procesu může systém ověřit, zda uživatel, správce nebo administrátor má platný důvod pro přístup k systému a popřípadě ukončit spojení, pokud nedojde k autorizaci tohoto spojení.

Plánované etapy projektu:

- Etapa 1 – Postupná integrace systému v celém ICT prostředí.

3. Konsolidace sběru provozních a bezpečnostních logů ze systémů a sítě HZS ČR

Technické opatření VoKB §14 Zvládání kybernetických bezpečnostních událostí a incidentů a §22 Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů.

Jedním z požadavků vyplývajících z VoKB §22 je požadavek na sběr informací provozních a bezpečnostních činnostech a jejich ochranu před neoprávněným přístupem nebo změnou.

V současné době jsou informace o provozních a bezpečnostních událostech (logy) zaznamenávány převážně jen na lokální úrovni, kde není vždy možné zaručit jejich integritu. Projekt zavede kompletní centrální sběr a uchovávání informací o provozních a bezpečnostních událostech (logů) na jednom místě, řešením zaručujícím jejich integritu i všechny další požadavky kladené výše uvedeným zákonem. Toho by mělo být dosaženo nasazením centrálního log management řešení a zapojením všech zdrojů logů ze systémů a sítě HZS ČR do tohoto řešení.

Návrh řešení:

Návrh implementace log management systému do interního prostředí organizace vychází z doporučení oddělení Log management systému a případného budoucího SIEM systému. Pro vlastní log management systém je navrženo využití samostatného / dedikovaného fyzického zařízení pro zpracování všech logovaných informací. Takový systém musí z principu nativně podporovat módy typu High availability (HA), clusterování.

Požadavek na HA funkcionalitu vychází z požadavku zajistit v každém případě uložení a evidenci všech logů i v případě kybernetického útoku nebo jiného selhání. Zajistí se tak možnost zpracování a analýza informací i následně např. i třetí stranou. Správná funkcionalita bude také zajištěna dalšími napojenými technickými prvky, které budou zpracovávat vstupní údaje z monitoringu jak pomocí flow sond, tak přímo napojených monitorovacích nástrojů z ICT prvků pokrývané infrastruktury. Získané informace mohou být využívány rovněž pro potřeby plnění požadavků vyplývajících z GDPR.

Dále log management systém musí umět základní automatizované funkce korelace dat nad zpracovávanými logy a také poskytovat standardizované rozhraní pro integraci na SIEM systémy pro úplné bezpečnostní zpracování a analýzy informací. Nebo/a umožňovat integraci s Security Operation Centry nebo MSSP třetích stran.

Požadavky na řešení:

- Hierarchická struktura implementace log management systému v distribuovaném, agregačním a transportním uspořádání, umožňující sbírat logy i v oddělených segmentech jak v technologických sítích, tak uživatelsko-aplikační datové síti (UAS) HZS ČR.
- Centrální a klíčové prvky systému v módu s vysokou dostupností (HA mód).

- Zajištění příjmu logů v jejich originální formě („RAW"), jejich bezpečné ukládání (šifrovaně, komprimovaně, s použitím TSA certifikačního razítka).
- Přístupy k logům přes uživatelské oddělení rolí s využitím silných šifrovacích metod, za účelem ochrany logů před neoprávněným přístupem.
- Možnost škálování výkonu celého řešení až do řádu cca 2 mil. EPS (pro zajištění potřeb pro cca 35-40 tis. zařízení).
- Oddělený archivační systém, který bude archivovat logy minimálně 6 měsíců a budoucím stavem cca 18 měsíců (požadavek ZoKB pro kritickou informační infrastrukturu, dle §22 vyhlášky č. 82/2018, a to s možností klasifikace a identifikace různých tříd vyřazení a retence dat. Tento archivační systém nebude mít přístupná data online, ale data budou archivována offline a budou přístupná na jednotlivá vyžádání podle potřeby.
- Funkcionalitu WORM logstore – z důvodu jasných auditních záznamů.
- Možnost rozdělení a separace logstores (viz GDPR a právo na zapomenutí).
- Agenty sběru logů, kde je to účelné (především pro technologie MS Windows server).
- Možnost základní korelace logů a vyhledávání včetně nadefinovaných vzorů pro zajištění každodenního provozu a pro účely auditů.
- Příprava na integraci s plnohodnotnými systémy SIEM / SOC / MSSP formou standardizovaných rozhraní a protokolů.
- Naplnění požadavků legislativy a průmyslových standardů, např. ISO / IEC / BS, SOX, Basell, HIPAA, COBIT nebo GDPR.

Plánované etapy projektu:
- Etapa 1 – pořízení a implementace centrálního log management systému.
- Etapa 2 – postupná integrace bezpečnostních technologií.
- Etapa 3 – postupná integrace vybraných systémů v technologických sítích (sítě TECHLAN).
- Etapa 4 – postupná integrace vybraných systémů v uživatelsko-aplikační datové síti (UAS).

Pořizované položky řešení:
- Systém centrálního sběru provozních a bezpečnostních logů ze systémů a sítě HZS ČR.
- Instalace.
- Implementace.

Příloha č. 2

Čestná prohlášení

I.

Ve smyslu § 6 odst. 4 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (odpovědné veřejné zadávání) čestně prohlašuji za společnost **Datasense s. r.o.** že při plnění veřejné zakázky zadávané pod názvem **„Studie proveditelnosti"**:

- nebude docházet k porušování zákonného standardu pracovních podmínek dle zákoníku práce, právních předpisů v oblasti zaměstnanosti a BOZP,
- nebude docházet k porušování mezinárodních úmluv o lidských právech, sociálních či pracovních právech, zejména úmluv Mezinárodní organizace práce (ILO) uvedených v příloze X směrnice č. 2014/24/EU,
- nebude docházet k diskriminaci malých a středních podniků v případě, že se budou na plnění veřejné zakázky podílet poddodavatelé,
- nebude docházet k vytváření problémových podmínek a vztahů v dodavatelském řetězci, zejména pro malé a střední podniky, jako např. opožděná splatnost faktur, nelegální zaměstnávání osob, porušování BOZP, nedodržování právních předpisů o ochraně životního prostředí apod.,
- bude používat dopravní techniku a stavební stroje v souladu s aktuálními ekologickými normami.

II.

Ve smyslu dopadu sankcí proti Rusku a Bělorusku do oblasti veřejných zakázek čestně prohlašuji za společnost **Datasense s. r.o.** že při plnění veřejné zakázky zadávané pod názvem **„Studie proveditelnosti"**, se na plnění, které nabízím, nevztahují mezinárodní sankce. Současně prohlašuji, že si nejsem vědom skutečnosti, že by se mezinárodní sankce vztahovaly na poddodavatele, které budu v průběhu plnění veřejné zakázky využívat.
Dále přikládám čestná prohlášení od svých poddodavatelů, že nepodléhají sankci

Viz elektronický podpis

Za prodávajícího:

.....