Příloha č. 1 Smlouvy o poskytnutí subskripce

# Seznam zkratek

Níže uvedená tabulka obsahuje seznam zkratek a pojmů použitých v rámci této Technické specifikace.

Přehled zkratek a pojmů:

|  |  |
| --- | --- |
| **Zkratka** | **Popis** |
| IT | informační technologie |
| ML | Machine Learning – strojové učení |
| URL | Uniform Resource Locator |
| SSL | Secure Socker Layer |
| TLS | Transport Layer Security |
| IP | Internet Protocol |
| TCP | Transmission Control Protocol |
| IPsec | IP security |
| LDAP | Lightweight Directory Access Protocol |
| NTLM | New Technology LAN Manager |
| RADIUS | Remote Authentication Dial In User Service |
| TACASC | Terminal Access Controller Access-Control System |
| SSO | Single Sign On |
| NAT | Network Address Translation |
| DNS | Domain Name System |
| RSA | Šifra s veřejným klíčem |
| RBAC | Nastavení oprávnění podle rolí |
| RBI | Remote Browser Isolation |
| AV | AntiVirus/AntiMalware systém |
| DLP | Ochrana proti úniku dat |
| SIEM | Security Information and Event Management |
| EDR | Systém pro detekci a řešení bezpečnostních událostí na koncovém zařízení |
| XDR | Systém pro rozšířenou detekci a řešení bezpečnostních událostí na koncovém zařízení |

# Úvod

Tento dokument je přílohou a nedílnou součástí zadávací dokumentace týkající se veřejné zakázky s názvem „Výměna proxy řešení SŽ“ (dále jen „veřejná zakázka“), pro organizaci Správa železnic, státní organizace (dále jen „SŽ“ nebo “Objednatel”). Dokument popisuje technické a jiné požadavky na veřejnou zakázku.

Technická specifikace je závazná a její nedodržení může být důvodem k vyloučení dodavatele ze zadávacího řízení.

## Předmět plnění veřejné zakázky

Předmětem plnění smlouvy je dodávka technologie webového proxy serveru a cloudového osobního firewallu pro ochranu koncových zařízení provozovaných vně i mimo sítě Objednatele, implementace a konfigurace dodané technologie a odborné školení správy a údržby dodané technologie pro vybrané odborné pracovníky Objednatele. Nedílnou součástí plnění je také technická podpora dodaných technologií, pravidelné aktualizace bezpečnostních funkcionalit a post-implementační podpora Objednatele.

Obsahem jsou následující poptávané oblasti:

§Dodávka technologií a subskripcí

§Implementační práce

§Odborné školení správy a údržby dodaných technologií

§Post-implementační a technická podpora

§Konzultační služby na vyžádání.

# Požadavky na plnění

Plnění se musí skládat alespoň z níže uvedených částí:

1. Dodávka subskripcí pro funkcionality cloudové webové proxy
2. Dodávka subskripcí pro funkcionality cloudového firewallu
3. Implementace obou funkcionalit v cloudovém prostředí výrobce/poskytovatele
4. Integrace na interní systémy Objednatele
5. Odborné školení
6. Post-implementační a technická podpora
7. Konzultační služby na vyžádání.

Vyloučení technologií představujících kybernetickou hrozbu

*Dne 17. prosince 2018 vydal Národní úřad pro kybernetickou a informační bezpečnost Varování, č. j. 3012/2018NÚKIB-E/110, kde uvedl, že: „Použití technických nebo*

*programových prostředků následujících společností, včetně jejich dceřiných společností, představuje hrozbu v oblasti kybernetické bezpečnosti:*

*Huawei Technologies Co., Ltd, Šen-čen, Čínská lidová republika*

*ZTE Corporation, Šen-čen, Čínská lidová republika“.*

*Dne 4. ledna 2019 vydal Národní úřad pro kybernetickou a informační bezpečnost Metodiku k varování ze dne 17. prosince 2018 (dále jen „metodika“), kde jsou mj. určeny i postupy pro aktualizaci analýzy rizik. V souladu s vydanou metodikou Objednatel provedl analýzu rizik související s předmětnou veřejnou zakázkou na dodávky, jak je jeho povinností podle § 5 a § 8 vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat, ve znění pozdějších předpisů.*

V návaznosti na to Objednatel identifikoval rizika spojená s výše uvedenými technickými a programovými prostředky jako neakceptovatelná a současně opatření k jejich zvládání, kterým je nepřipuštění použití těchto prostředků v rámci plnění veřejné zakázky.

Objednatel tak na základě varování NÚKIB, navazující metodiky a provedené analýzy rizik, ve spojení s § 4 odst. 4 ZoKB, nepřipouští v rámci plnění veřejné zakázky použití technických nebo programových prostředků společností (výrobců), které jsou uvedené v současné době platném varování NÚKIB jako hrozba v oblasti kybernetické bezpečnosti.

## Dodávka subskripcí pro funkcionality webové proxy

V oblasti dodávky funkcionalit webové proxy definuje Objednatel následující požadavky pro každé z nich:

|  |  |  |
| --- | --- | --- |
| **požadavek na plnění** | **Nabízené řešení splňuje** | **Popis naplnění pro nabízené řešení** |
| Funkce webové proxy pro 11 000 uživatelů respektive 15 000 zařízení. (oba kvantitativní požadavky musí být naplněny) | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Cloudová webová proxy poskytovaná v SLA 99,5% | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Služba bude poskytována z vlastních cloudových center výrobce, nikoli veřejných public cloudů (AWS, Azure atp.) | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Přístup k minimálně 50 datovým centrům po celém světě, z nichž každé musí poskytovat stejnou podporu pro všechny níže uvedené funkce. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platformu je možné omezit na využití cloudových center výrobce striktně jen v EU regionu | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí umožnit definovat lokalizační zónu, aby dotazování vracelo relevantní výsledky pro Českou republiku | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| V každém datovém centru má služba přímý peering s minimálně třemi poskytovateli SaaS – AWS, Google a Microsoft. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Služba, která implementuje popsané funkce, musí zaručit latenci ne vyšší než:   * 10 ms pro nedešifrovaný provoz * 50 ms pro dešifrovaný provoz | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Datová centra, ze kterých bude služba poskytována musí mít následující certifikace:   * ISO 27001 * PCI DSS * SOC 2 Typ II * NIST 800-53/FISMA | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí umožňovat minimálně následující způsoby řízení provozu – instalovaný agent, IPSec, GRE, Cloud Explicit Proxy. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma nesmí shromažďovat a ukládat inspektovaná data, vyjma ukládání metadat, provozních dat (logy/incidenty atp.) | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí být schopna importovat uživatele ze služby Active Directory. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma se musí integrovat s následujícími systémy Objednatele:   * XDR: Fidelis * Microsoft Active Directory | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Přesměrování provozu na službu musí být provedeno pomocí odlehčeného agenta pro následující platformy:   * Windows * MacOS * Linux * Apple iOS * Android | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Musí být možné instalovat agenta pomocí automatizovaných distribučních nástrojů, jako jsou JAMF, SCCM, Microsoft Endpoint Manager (Intune) a Microsoft GPO. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Agent musí detekovat svou přítomnost v místě s přímým přístupem ke zdrojům koncového zařízení (jeho OS). | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Agent by měl směrovat provoz do služby na základě FQDN, subdomén doménových jmen, rozsahu IP adres a jednotlivých IP adres. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Veškerá komunikace se službou musí být prováděna jedním agentem – analýza in-line provozu z hlediska hrozeb, přenos citlivých dat, zajištění plné viditelnosti provozu a přístupu ke zdrojům koncového zařízení (jeho OS). | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Veškerá komunikace mezi agentem a službou musí být šifrována s použitím parametrů ne horších než:   * Šifrovací sada: ECDHE-ECDSA-AES256-GCM-SHA384, * Protokol: TLS v1.2, * Asymetrická výměna klíčů: eliptická křivka Diffie–Hellman (ECDH), * Autentizace: RSA 2048 (vzájemné TLS pomocí certifikátů RSA s délkou klíče 2048 bitů), * Symetrické šifrování: AES-GCM256 (256 bitů), * Integrita: HMAC-SHA384 (384 bitů). | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí umožňovat automatické aktualizace agentů na koncových zařízeních. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí poskytovat možnost vytvářet politiky přístupu, které inspektovaný provoz povolí, zablokují nebo proškolí uživatele. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Politiky přístupu musí být prosazovány alespoň v závislosti na:   * Uživatel * Externí IP adresa * Země * Hodnocení uživatelů * Operační systém * Prohlížeč * Způsoby připojení * Klasifikace zařízení. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Klasifikace zařízení musí být ověřena alespoň na základě:   * Šifrování * Zápisů v registru, * Spuštěných procesů proces, * Členství v doméně * Certifikátu | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí umožňovat vytváření vlastních oznámení pro koncového uživatele pro každou nakonfigurovanou politiku. Oznámení musí umožňovat zobrazení vlastního loga a textu. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí mít rozhraní REST API pro integraci se stávajícími i budoucími systémy Objednatele. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí provádět inline kontrolu provozu a proxy pro HTTP a HTTPS provoz a poskytovat následující funkce:   * Ochrana webového provozu i služeb SaaS a IaaS/PaaS * Schopnost nastavit tunely IPsec a GRE z poboček přímo do služby, aniž by bylo nutné enkryptrovat v jediném místě(centrálním VPN koncentrátoru Objednatele). * Integrace s SSO, MFA a Active Directory * Reverzní proxy pomocí integrace IdP * Nativní kontrola provozu TLS v1.2 a v1.3 * Vytváření podrobné bezpečnostní politiky * Rozpoznávání instancí aplikací a uživatelských akcí * Databáze sdružující hodnocení rizik pro více než 70 tisíc cloudových služeb a aplikací * Open API | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí provádět filtrování webového provozu poskytováním následujících funkcí:   * Filtrování adres URL pro minimálně 130 kategorií * Podpora místních jazyků pro minimálně 190 zemí * Dynamická kategorizace webových stránek pro 70 kategorií * Nástroj pro ověřování kategorií webu * Možnost změny zařazení do jednotlivých kategorií * Povolení, blokování nebo pokračování určitých činností * Definování vlastních upozornění pro uživatele * Vytváření vlastních kategorií včetně seznamů povolených/blokovaných | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí poskytovat ochranu před hrozbami poskytováním následujících funkcí:   * Analýza typu souboru * Antimalwarová inspekce * Napojení na alespoň 40 informačních kanálů s hrozbami (Threat Intel feed) * Schopnost importovat IoC obsahující informace o škodlivých URL a hash hodnot pro soubory * Inline strojové učení přenosných Ano/Ne spustitelných souborů pro detekci a blokování malwaru typu Zero Day Attack * Detekce phishingu s klasifikátorem ML k identifikaci phishingových domén v reálném čase blokováním přístupu na tyto stránky * Standardní sandboxing pro potvrzení všech AV/ML detekcí * Akce karantény pro škodlivé soubory s režimem nasazení API (možnost detailní definice, co s karanténním obsahem dělat) * sdílení informací o hrozbách s EDR/XDR, SIEM | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí být vybavena funkcí Remote Browser Isolation (RBI), která bezpečně zobrazí rizikovou stránku, formou vykreslování pixelů. Takto zobrazená stránka neobsahuje žádné automaticky spouštěné skripty nebo hrozby. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí umožňovat vytváření různých profilů pro RBI, ve kterých bude mít správce systému možnost udělovat akce koncovým uživatelům, alespoň jako: možnost kopírovat obsah do schránky ze stránek zpracovaných v RBI, tisknout stránku a přístup pouze pro čtení. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí analyzovat chování uživatele, aby odhalila následující anomálie:   * Hromadné nahrávání, stahování nebo mazání dat cloudových aplikací * Neúspěšné pokusy o přihlášení * Sdílení přístupových údajů * Neobvyklé události * Rizikové země (jak pro navštěvované stránky, tak pro provoz koncového zařízení) * Exfiltrace dat mezi podnikovými a soukromými instancemi aplikací | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí disponovat funkcí DLPs následujícími možnostmi:   * Analýza dat odeslaných do/z cloudových služeb a aplikací * Minimálně 40 šablon shody s předpisy pro identifikaci citlivých dat v souladu s mnoha mezinárodními předpisy, jako je GDPR, PCI-DSS * Vlastní profily DLP pro citlivá data, která nejsou vázána na konkrétní předpisy. * Vlastní profily musí umět klasifikovat a inspektovat: Osobně identifikovatelné informace (PII), chráněné zdravotní informace (PHI), zdrojový kód, dokumenty chráněné heslem a vulgární výrazy. * Identifikace minimálně 1500 typů souborů z hlediska obsahu citlivých dat * Schopnost definovat vlastní vzory pomocí regulárního výrazu * Schopnost definovat vlastní slovníky * Možnost správy incidentů DLP pro konkrétní administrátorskou roli | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí umožňovat monitorování a pokročilou analýzu rizikových faktorů a poskytovat tyto funkce:   * Uchovávání dat po dobu minimálně 7 dní pro výstrahy, webové události, události aplikací, události přístupu soukromých aplikací, síťové události a transakční události * Dobu uchovávání musí být možné prodloužit o 3, 6 nebo 13 měsíců * Pokročilá vizualizace dat s možností vytvářet vlastní reporty * Knihovna s minimálně 20 předdefinovanými řídicími panely pokrývajícími cloudovou aktivitu, analýzu rizik a zásady dodržování předpisů * Data uchovávaná po dobu 7 dnů v rozsahu nejméně 4 GB pro 100 uživatelů | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí být schopna integrace s řešeními SaaS nebo IaaS pomocí API. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Integrace SaaS musí být možná alespoň s: Box, Cisco Webex Teams, Dropbox, GitHub, Gmail, Disk Google, Microsoft Office 365 (Onedrive, Outlook, SharePoint, Teams), ServiceNow, Slack, Atlassian Confluence, Atlasssian Jira Cloud, Citrix ShareFile, GitHub a Zoom. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Integrace přes API musí poskytovat možnost ověřit zdroje řešení SaaS, alespoň v rozsahu všech souborů na zdroji, souborů porušujících zásady úniku dat (DLP) nebo zjištěných hrozeb. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí poskytovat schopnost automaticky vyjednat s integrovanými aplikacemi zásah v případě, že soubor porušuje pravidla zásady úniku dat (DLP). | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Integrace musí poskytovat možnosti zpětného skenování k identifikaci všech aktiv v integrované aplikaci podle zásad zabezpečení dat (DLP). | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí být auditovatelná podle bezpečnostních standardů, jako jsou NIST, CSF, CIS, PCI, GDPR, ISO 27002, Zákon o kybernetické bezpečnosti. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Audit musí vrátit informace o problému a způsobu řešení problému, aby byl v souladu s normou. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí být spravovatelná z jediné konzole centrální správy přístupné z prohlížeče. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Centrální řídící konzole musí mít vestavěné nástroje pro ověřování správnosti konfigurace, ověřování dostupnosti aplikací a simulaci vytvořených politik. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Musí být možné vytvořit a přiřadit předdefinované role správcům systému pomocí RBAC. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí obsahovat funkcionalitu kontrolující činnost administrátorů. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platforma musí poskytovat protokolování následujících parametrů pro relaci uživatele:   * Datum a čas * Název zásady poskytující soukromý zdroj * Akce – povolit/zablokovat * ID tunelu pro připojení * Čas nastavení tunelu * Uživatelské jméno * Zdrojový port * Operační systém a jeho verze * Název aplikace * Cílový přístav * Počet odeslaných, přijatých bajtů a celková hodnota * Počet odeslaných a přijatých paketů * Čas začátku a konce relace * Délka relace | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Všechny incidenty a výstrahy by měly být dostupné po dobu minimálně 90 dnů. | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Platformu lze jednoduše doplnit o funkcionality ZTNA za použití shodného programového vybavení na straně koncových zařízení | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |
| Výrobce musí poskytovat 24hodinovou technickou podporu, 7 dní v týdnu | Ano/Ne | [DOPLNÍ POSKYTOVATEL] |

## Implementace a integrace

V oblasti implementace a integrace funkcionalit webové proxy a cloudového firewallu jsou definovány následující činnosti, resp. požadavky:

|  |  |
| --- | --- |
| **Oblast** | **Činnost** |
| Vypropagování a základní nastavení cloudového tenantu | Objednatel požaduje zpřístupnění prostředí pro správu řešení a jeho základní nastavení odborníky Dodavatele. |
| Tvorba základních politik | Tvorba a nasazení základních bezpečnostních politik |
| Integrace do systému Objednatele | Integrace na následující systémy:   * XDR: Fidelis * Microsoft Active Directory |
| Implementace pilotního provozu na vybrané skupině uživatelů | Komplexní zajištění distribuce a nasazení agenta na koncové stanice pro vybrané uživatele a otestování funkcionalit. |
| Asistence při nasazení | Konzultace a změnová řízení při nasazení pro celé prostředí Objednatele |

## Odborné školení

V oblasti odborného školení je požadován následující rozsah školení:

|  |  |
| --- | --- |
| **Typ školení** | **Popis** |
| Hands-On školení | Dodavatel provádí implementaci a integraci definovanou v kapitole 3.2 této Technické specifikace ve formě slovního průvodce, kdy veškeré činnosti provádí zástupce Objednatele. Jednotlivé kroky implementace jsou zástupci Objednatele podrobně popsány tak, aby došlo k ideální konfiguraci pro dané prostředí Objednatele. |

## Post-implementační a technická podpora

V oblasti post-implemetační a technické podpory jsou definovány následující požadavky:

|  |  |
| --- | --- |
| **Oblast** | **Požadavky** |
| Oficiální podpora výrobce | Dodavatel zajistí oficiální podporu výrobce po dobu 12 měsíců od dodávky technologií a licencí, která zahrnuje minimálně:   * Režim podpory 24x7x4 (24 hodin denně, reakční doba 4 hodiny). * Podpora dostupná na webovém portálu výrobce, e-mailu a telefonu * Přístup k novým verzím SW (agent)- Aktualizace bezpečnostních definic pro funkcionality definované v kapitole 3.1. |
| Podpora dodavatele | Dodavatel zajistí podporu po dobu 12 měsíců dle parametrů a za podmínek uvedených v Závazném vzoru smlouvy a jejích přílohách (zejména Zvláštní obchodní podmínky pro zakázky v oblasti ICT). |

## Konzultační služby na vyžádání

V oblasti konzultačních služeb jsou definovány následující požadavky:

|  |  |
| --- | --- |
| **Oblast** | **Požadavky** |
| Konfigurační konzultace | Dodavatel zajistí certifikovaného odborníka v oblasti dodané technologie, který Objednateli umožní konzultovat konfigurační parametry dodaného řešení.  Požadovaný počet MD k čerpání: 5 |
| Analytická konzultace | Dodavatel zajistí certifikovaného odborníka v oblasti vyšetřování kybernetických událostí v rámci dodané technologie pro konzultace bezpečnostních nálezů identifikovaných dodaným řešením.  Požadovaný počet MD k čerpání: 5 |

Maximální limit MD k čerpání v součtu pro konfigurační konzultace a analytické konzultace je 10 MD.

# Fáze dodávky a akceptační milníky

Plnění musí být dodáno v níže uvedených fázích. Každá z níže uvedených fází (tj. každý řádek níže uvedené tabulky) musí být Objednatelem separátně akceptována nejpozději v termínu uvedeném v Harmonogramu. Objednatel akceptuje výstupy dané Fáze, jestliže je dodavatel provedl v šíři a kvalitě požadované v zadávací dokumentaci této veřejné zakázky. V opačném případě je dodavatel povinen napravit nedostatky plnění.

|  |  |
| --- | --- |
| **Fáze** | **Popis** |
| F1 | Dodávka funkcionalit webové proxy a cloudového firewallu |
| F2 | Implementační a integrační práce |
| F3 | Školení:- Hands-On školení |
| F4 | Post-implemetační a technická podpora- Oficiální podpora výrobce |
| F4 | Post-implemetační a technická podpora- Podpora dodavatele |
| F5 | Konzultační služby na vyžádání |