SMLOUVA

na dodávku a instalaci webových aplikačních firewallů (WAF)

uzavřená podle ustanovení § 2586 a nasl. zákona č. 89/2012 Sb., občanský zákoník

I. Smluvní strany

Organizace:	**Centrum pro zjišťování výsledků vzdělávání,** státní příspěvková organizace (CZVV)
Sídlo:	Jankovcova 933/63, Holešovice, 170 00 Praha 7
IČO:	72029455
Zastoupené:	RNDr. Michaela Kleňhová, ředitelka
Bankovní spojení:	Česká národní banka
číslo účtu:	1235071/0710

(dále jen „objednatel“)

a

Společnost:	**T-Mobile Czech Republic a.s.**
Sídlo:	Praha 4, Tomíčkova 2144/1, PSČ 148 00
IČO:	649 49 681
DIČ:	CZ64949681
Zast.:	Ing. Jaromírem Červinkou, na základě pověření

zapsaná v obchodním rejstříku vedeném Městským soudem v Praze pod spisovou značkou B, vložka 3787

Bankovní spojení:	Česká spořitelna, a.s., Praha 4
číslo účtu:	994404-242097001/0800

(dále jen „dodavatel“)

II. Předmět a místo plnění

1) Předmětem smlouvy je kompletní dodávka, instalace a konfigurace 2 kusů webových aplikačních firewallů (WAF) dle Technické specifikace, která je přílohou č. 1 smlouvy (dále jen „Technická specfikace“), a to včetně následné 4 leté servisní podpory. Místem plnění je datové centrum v Praze (*na adrese, která bude upřesněna při uzavření smlouvy*). Součástí Technické specifikace je i specifikace plnění plynoucí z nabídky dodavatele předložené v rámci zadávacího řízení vedoucího k uzavření této smlouvy, a to v rozsahu, v jakém neodporuje příloze č. 1.
2) Dodavatel zavazuje dodat objednateli výše uvedenou dodávku, včetně souvisejících činností včas, řádně a bez závad či nedodělků, a objednatel se zavazuje při dodržení podmínek této smlouvy uvedenou dodávku řádně a včas převzít a zaplatit za ni dohodnutou cenu.
3) Jakékoliv nedodržení Technické specifikace je vážným porušením této smlouvy a je důvodem k odstoupení od smlouvy.

4) Dodavatel zaručuje, že je certifikovaným partnerem výrobce předmětného řešení a disponuje dostatečným počtem příslušně certifikovaných pracovníků. V případě, že toto ujištění není pravdivé, je objednatel oprávněn od smlouvy odstoupit.

5) Další podmínky dodávky a instalace zařízení:

   a. Přístup do rozvaděčoven a serveroven bude umožněn pouze za přítomnosti odpovědného pracovníka objednatele po předchozí domluvě mezi zástupci dodavatele a objednatele

   b. Veškerý dodaný SW je v souladu s legislativou, zejména zákona č. 181/2014 Sb. a vyhlášky č. 82/2018 (ZoKB) a zákona č. 110/2019 Sb. (GDPR) a je k němu dodána patřičná dokumentace.

   c. Součástí plnění je i udělení nevýhradního práv užít jakýkoli SW či jakékoli jiné autorské dílo zahrnuté do plnění a předané objednateli, a to v rozsahu odpovídajícím užívání plnění objednatelem v souladu s jeho účelem a touto smlouvou.

III. Doba plnění

1) Doba plnění vlastní dodávky je sjednána nejpozději do 40 dnů od účinnosti této smlouvy. Přesný časový postup plnění dodávky a souvisejících činností dodavatele v rámci uvedené doby plnění je uveden v harmonogramu, který tvoří přílohu č. 2 této smlouvy (*předloží účastník ve své nabídce).*

2) O úspěšné realizaci dodávky dle článku II. smlouvy bude mezi smluvními stranami sepsán Akceptační protokol.

3) Zodpovědným zástupcem objednatele pro převzetí dodávky dle článku II. této smlouvy je Jindřich Mach, [redacted]

4) Prodlení dodavatele s dodávkou delší než 10 pracovních dnů se považuje za podstatné porušení smlouvy a zakládá právo objednatele od smlouvy odstoupit i bez nutnosti jakékoli výzvy.

IV. Cena plnění

1) Cena za celkovou dodávku včetně následné 4 leté servisní podpory v rozsahu dle této smlouvy je oběma smluvními stranami sjednána na základě nabídky dodavatele ve výši:

   1 687 040,- Kč (slovy jeden milion šest set osmdesát sedm tisíc čtyřicet) bez DPH , tedy 2 041 318,4 Kč včetně DPH v sazbě 21 %.

2) Rozpis ceny jednotlivých částí dodávky je uveden v příloze č. 3, která tvoří nedílnou součást této smlouvy (*předloží účastník ve své nabídce).*

3) Sjednaná cena je fixní a nepřekročitelná a zahrnuje všechny náklady dodavatele spojené s předmětem plnění.

4) Smluvní cena bude dodavateli uhrazena až po řádném předání a převzetí dodávky potvrzeném Akceptačním protokolem.

5) Zálohy objednatel neposkytuje.

V. Platební podmínky

1) Dodavatel vystaví fakturu po protokolárním předání a převzetí celé dodávky objednateli, ve které bude samostatně vyúčtována DPH u jednotlivých položek. Přílohou faktury bude kopie dokladu o předání a převzetí – Akceptační protokol.

2) Faktura musí obsahovat náležitosti stanovené zákonem č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákonem č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů

3) Splatnost faktury se sjednává na 30 dnů od obdržení daňového dokladu objednatelem.

4) Objednatel má právo vrátit dodavateli před termínem splatnosti neproplacenou fakturu k doplnění jako neúplnou, pokud tato nebude obsahovat veškeré náležitosti daňového a účetního dokladu a stanovenou přílohu či další náležitosti dle podmínek této smlouvy a souvisejících právních předpisů. Dodavatel je v tomto případě povinen fakturu bez zbytečného prodlení přepracovat resp. doplnit a doručit ji objednateli. V takovém případě začne běžet nová doba splatnosti daňového dokladu.

VI. Zahájení, průběh a ukončení dodávky

1) Dodavatel je povinen elektronicky nebo telefonicky oznámit objednateli nejpozději 2 pracovní dny předem přesné datum a hodinu zahájení prací na dodávce dle této smlouvy.

2) Řízení změn - Dodavatel se zavazuje při plnění smlouvy postupovat dle systému řízení změn Objednatele a v souladu s § 11 VoKB. Dodavatel má v rámci své organizace implementovaný systém řízení změn tak, aby byl schopen doložit veškeré předchozí verze SW či dokumentace, které byly Objednateli předloženy.

3) Dodavatel je povinen Objednatele bez zbytečného odkladu informovat o:
   - identifikovaných kybernetických bezpečnostních incidentech souvisejících s plněním Smlouvy, nejpozději však do 48 hodin od jejich výskytu,
   - způsobu řízení rizik na straně Dodavatele a o zbytkových rizicích souvisejících s plněním Smlouvy,
   - významné změně ovládání Dodavatele, přičemž ovládáním se rozumí vliv, ovládání či řízení dle § 71 a násl. zákona č. 90/2012 Sb., o obchodních korporacích, ve znění pozdějších předpisů, či ekvivalentní postavení, a to do 5 pracovních dnů od uskutečnění této změny,
   - o změně vlastnictví či oprávnění nakládat se zásadními aktivy využívanými Dodavatelem k plnění Smlouvy, a to do 5 pracovních dnů od uskutečnění této změny.

4) Objednatel převezme plnění řádně a včas dokončené v souladu s touto smlouvou poté, co mu budou dodavatelem předvedeny vlastnosti dokončeného plnění a prokázáno, že plnění odpovídá požadavkům a parametrům dle Technické specifikace. Převzetí bude potvrzeno akceptačním protokolem podepsaným zástupcem objednatele, náhradní způsoby potvrzení převzetí se nepřipouští. Dodavatel předá objednateli s dodávkou také veškerou dokumentaci a doklady, které se k dodávce vztahují, a to včetně podrobných podmínek servisní podpory výrobce.

5) Pokud bude mít objednatel k předvedenému plnění výhrady nebo připomínky vyvolané nesouladem dodaného plnění s Technickou specifikací, je oprávněn plnění nepřevzít. V takovém případě je dodavatel povinen výhrady objednatele vypořádat a vyhovující plnění opětovně předložit k převzetí nejpozději do 3 pracovních dnů. Tím není dotčen sjednaný termín plnění.

6) Převezme-li objednatel plnění s výhradou, je dodavatel povinen výhrady objednatele vypořádat ve lhůtě uvedené v akceptačním protokolu, a pokud nebude stanovena, do 30 dnů.

7) Převezme-li objednatel plnění bez výhrad, není tím dotčeno jeho právo ze zjevných vad plnění, a to, ani kdyby objednatel při převzetí výslovně uvedl, že plnění přejímá bez výhrad; ustanovení § 2605 odst. 2 občanského zákoníku se vylučuje.

VII. Záruka za jakost

1) Dodavatel ručí za funkčnost předmětu této smlouvy v rozsahu a parametrech stanovených touto smlouvou. Na dodaná zařízení včetně baterií (akumulátorů) poskytuje záruku v délce 24 měsíců ode dne instalace, resp. 48 měsíců ode dne instalace, pokud jde o plnění pokryté servisní podporou výrobce dle Technické specifikace.

2) V rámci záruky se dodavatel zavazuje nahlášenou závadu odstranit do 30 dnů, to neplatí pro plnění pokryté servisní podporou výrobce dle Technické specifikace, kdy konkrétní podmínky servisní podpory jsou stanoveny v dokumentaci předávané dodavatelem nejpozději v okamžiku dle čl. VI odst. 4).

VIII. Sankce

1) Při prodlení dodavatele s dodávkou je dodavatel povinen zaplatit objednateli za každý den tohoto prodlení smluvní pokutu ve výši 1 000 Kč.
2) V případě prodlení dodavatele s odstraněním záruční vady je dodavatel povinen zaplatit objednateli za každý den tohoto prodlení smluvní pokutu ve výši 500,- Kč.
3) V případě prodlení objednatel s úhradou faktury je dodavatel oprávněn uplatnit vůči objednateli zákonný úrok z prodlení.
4) V případě odstoupení od smlouvy jsou strany povinny vrátit si navzájem veškeré poskytnuté plnění. Tím není dotčen nárok na náhradu škody nebo smluvní pokutu.

IX. Důvěrnost informací

1) Každá ze smluvních stran se zavazuje zachovávat v tajnosti všechny informace důvěrného charakteru, týkající se opačné smluvní strany, které se dozví v průběhu vzájemné spolupráce, a to i po skočení platnosti této smlouvy. Jakékoli tyto informace lze použít jen pro splnění předmětu této smlouvy. Za důvěrné informace se pro účely této smlouvy považují zejména informace obsažené v dokumentaci a materiálech dodaných nebo přijatých v jakékoli formě nebo poskytnuté některou smluvní stranou na základě této smlouvy a další informace týkající se některé smluvní strany, její činnosti či obchodních partnerů apod., které nejsou veřejně známé a dostupné a k jejichž zveřejnění dotčená smluvní strana výslovně neudělila souhlas. Smluvní strany se zavazují, že veškeré důvěrné informace, které jim budou poskytnuty, nesdělí ani jinak nezpřístupní třetím osobám s výjimkou osob zúčastněných na poskytování plnění dle této smlouvy; takové osoby musí být zavázány mlčenlivostí v rozsahu dle této smlouvy. Povinnost zachovávat závazek mlčenlivosti ve vztahu k důvěrným informacím trvá po celou dobu existence smluvního vztahu, tak i po jeho zániku do té doby, nežli se důvěrné informace případně stanou veřejně známými, aniž by smluvní strana porušila své povinnosti podle této smlouvy.
2) Výše uvedená ustanovení a z nich vyplývající závazky se nevztahují na informace:
    a. jejichž poskytnutí nebo sdělení bylo předem písemně schváleno chráněnou smluvní stranou,
    b. které smluvní strana označila výslovně jako veřejné, které se staly veřejně známými, aniž by smluvní strana povinná zachovávat mlčenlivost porušila povinnosti podle této smlouvy nebo ve smyslu této smlouvy,
    c. k jejichž sdělení je smluvní strana povinna podle právního předpisu nebo rozhodnutí soudu, správního či státního orgánu,
    d. údaje uvedené v této smlouvě.
3) Dodavatel je vždy povinen zachovat mlčenlivost o skutečnostech významných pro kybernetickou bezpečnost objednatele.

X.
Závěrečná ustanovení

1) Tato smlouva se řídí právem České republiky, zejména zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

2) Smlouva je uzavřena dnem jejího podepsání oběma smluvními stranami a nabývá účinnosti jejím zveřejněním v registru smluv, jak je níže uvedeno v odstavci 5) tohoto článku smlouvy.

3) Smlouva může být měněna nebo doplňována pouze písemnými, vzestupně číslovanými dodatky.

4) Dodavatel bere na vědomí, že se realizací této veřejné zakázky stane v souladu s ustanovením § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů, ve znění pozdějších předpisů, osobou povinnou spolupůsobit při výkonu finanční kontroly prováděné v souvislosti s úhradou zboží nebo služeb z veřejných výdajů nebo veřejné finanční podpory.

5) Tato smlouva bude zveřejněna v registru smluv podle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv). Objednatel zašle tuto smlouvu správci registru smluv k uveřejnění bez zbytečného odkladu, nejpozději však do 30 dnů od uzavření smlouvy. O zveřejnění smlouvy, které podmiňuje její účinnost, bude objednatel neprodleně informovat dodavatele.

6) Nedílnou součástí smlouvy je

   příloha 1 - Technická specifikace

   příloha 2 - Harmonogram

   příloha 3 - Rozpis ceny.

V Praze dne ……

V Praze dne dle el. podpisu

za objednatele

……

Centrum pro zjišťování výsledků vzdělávání
RNDr. Michaela Kleňhová
ředitelka

za dodavatele

Ing. Jaromír Červinka
Digitálně podepsal Ing. Jaromír Červinka
Datum: 2020.08.27 19:40:25 +02'00'

……

T-Mobile Czech Republic a.s.
Ing. Jaromír Červinka
Senior manažer prodeje státní správě
na základě pověření

Příloha č. 1

Technická specifikace

Obsah

1.1. TECHNICKÁ SPECIFIKACE

Úvod:

[redacted]

CZVV pro zajištění poskytovaných agend, tak interní systémy pro provoz organizace. Vzhledem k tomu, že tato zařízení jsou již morálně zastaraná a výrobce končí v letošním roce s podporou pro tento konkrétní model, rozhodlo se CZVV pro obměnu zařízení, aby mělo zajištěnu podporu pro další roky a mohlo nadále zajistit ochranu svých technologických služeb.

Předmět plnění VZ:

Dodávka a instalace 2 kusů WAF a jejich konfigurace v režimu active/active. Řešení musí obsahovat moduly pro Load Balancing (LB) a Webový aplikační firewall (WAF). V rámci konfigurace bude provedena záloha současných zařízení a nastavení nových zařízení tak, aby plně odpovídala současné konfiguraci. Konfigurace bude přenesena jak pro load balancing, tak samotný aplikační firewall, včetně vytvoření virtuálního hostů, přenosu certifikátů, nastavení reportů, apod. **Součástí dodávky je zajištění provozu a podpory po dobu 4 let**.

[redacted]

Nedílnou součástí plnění musí být:

- Dodávka a zapojení HW řešení do infrastruktury zadavatele v datovém centru v Praze
- Zajištění podpory výrobce na 4 roky (S&M 5x10, RMA NBD)
- Přenesení kompletní konfigurace pro LB a WAF ze současného do nového řešení a zajištění 100% současné funkcionality
- V případě přechodu na jinou než současnou technologii, proškolení obsluhy, napojení na dohledové centrum a zajištění uchování logů po dobu 1 roku.
    - Rozsah: 1 den školení (1 termín pro max. 5 osob)
    - Obsah: základní principy, základy konfigurace, schopnost vyhledávat v lozích pro případný reporting událostí atd.

Technické parametry

Minimální výkonové požadavky na hardware (vztaženo k jednomu nodu):

Parametr	**Hodnota**
Celková propustnost L4 a L7	10 Gbps
Propustnost „Offload" SSL/TLS:	5 Gbps (bulk encryption)
Počet L4 spojení za sekundu	120.000
Počet L4 HTTP požadavků za sekundu	500.000
Počet L7 požadavků za sekundu	350.000
Počet současných spojení	12.000.000
Softwarová podpora komprese	2,5 Gbps
Kapacita integrovaného datového úložiště	1/2 TB (využití jako dočasné uložiště provozních logů)

Specifikace rozhraní hardware (vztaženo k jednomu nodu):

Typ rozhraní	**Počet**
SFP slot podporující 1 Gbps T, SM/MM (SX/LX)	4
SFP+ slot podporující 10 Gbps (SR, LR)	2

Hardware musí být osazen **čtyřmi metalickými porty s kapacitou 1 Gbps** (buď v podobě SFP modulů, nebo jako zabudované porty v zařízení).

Další požadavky na hardware:

- Rack-mount chassis včetně prvků pro osazení o velikosti 1U
- Redundantní zdroj napájení
- Jednotné konfigurační rozhraní pro LB a WAF
- Oddělené fyzické rozhraní pro správu
- Podpora LACP, VLAN tagování (Trunk)

Požadované vlastnosti pro rozložení zátěže směrem k aplikační infrastruktuře (LB) a ochraně aplikací (WAF):

- Balancing aplikačního provozu na základě vrstev L3 – L7
- Reverzní proxy s funkcí NAT44, případně NAT 46, NAT 64
- Klient/Server NAT/PAT
- Podpora různých typů load-balancingu:
    - Kruhová metoda s vážením
    - Podle počtu navázaných spojení

    - Podle URL a cookie
    - Podle vah pro skupiny
- Podpora zajištění konektivity uživatelů k serveru (persistence) na základě IP adresy, HTTP cookie, HTTP Host hlavičky
- Podpora různých typů health monitoringu - ICMP, HTTP, TCP/UDP port…
- Možnost kombinace více metod monitoringu (AND/OR)
- Podpora modifikace provozu:
- Vložení/přepsání cookie
- Modifikace URL
- Možnost vložit zdrojovou IP do L7 hlavičky
- Modifikace HTTP obsahu
- Podpora TCP multiplexingu, multipath TCP (MPTCP)
- Podpora ICAP
- Podpora komprese a cachování HTTP odpovědí od serveru
- Podpora TCP SYN cookie
- Možnost přidávat zákaznické požadavky na základě skriptování
- SSL akcelerace a podpora SSL certifikátů podepsaných SHA-2 metodou
- Podpora TLS 1.2, AES-GCM a ECC pro TLS 1.2
- Podpora šifrování pomocí Suite B, ECDSA, AES-GCM.
- Možnost pracovat až s 4096-bitovými klíči
- Plná podpora IPv6
- Podpora sFlow
- Správa přes GUI, CLI
- Podpora SNMP (1, 2c a 3), SSH a syslogů per aplikace
- Podpora režimu redundance se synchronizací stavových tabulek
- Podpora redundantních clusterů Active-Standby i Active-Active
- Možnost zapojit do redundantniho clusteru různé typy HW
- Dostupnost jak hardwarového tak i virtuálního řešení
- Podpora otevřeného API pro nástroje třetích stran
- Podpora virtualizace – jak kontexty, tak i separace adresního prostoru (aka VRF, route domain)
- Detekce a blokování širokého spektra útoků na aplikační vrstvě, minimálně podle OWASP top10
- Možnost doprogramovat si filtrovací pravidla pro aplikace
- Automatická korelace zranitelností do jednoho bezpečnostního incidentu
- Ochrana AJAX a JSON aplikací
- Ochrana proti L7 DDoS útokům, web scrapingu a útokům pomocí hrubé síly (brute force)
- Podpora Captcha metody pro detekci lidského uživatele
- Automatické odlišení skutečných uživatelů od robotů
- Integrovaný XML firewall
- Podpora maskování/odstranění citlivých informací – čísla kreditních karet, číslo pojištění…
- Automatické nahrávání a aplikování nových signatur
- Podpora pozitivního a negativního bezpečnostního modelu
- Blokování útočníků na základě geolokace (až na úroveň regionů)
- Podpora ICAP pro antivirovou kontrolu – pro SOAP a SMTP
- Ochrana SMTP a FTP na aplikační úrovni
- Podpora různých typů reportů – PCI, geolokační reporty
- Podpora standardů PCI DSS, HIPAA, Basel II a SOX

- Integrované bezpečnostní politiky pro Microsoft Outlook Web Access, Lotus Domino Mail Server, Oracle E-Business Financials a Microsoft SharePoint
- Podpora pro analýzu HTTP provozu (Top URL, Top klienti, nejpoužívanější HTTP metody, návštěvnost stránek podle geogr. Regionu)
- Možnost importu zranitelnosti aplikací z alespoň některých z následujících skenerů:
    - Cenzic Hailstorm
    - WhiteHat Sentinel
    - IBM Rational AppScan
    - QualysGuard Web Application Scanning
- Rozšířená podpora CSHUI – detekce aktivity klávesnice a myši, detekce změn URL od klienta za krátkou dobu
- Ochrana proti Session Highjacking pomocí Browser Fingerprintingu
- Detekce a ochrana před DoS útoky na specifické URL, které mohou zatížit back-end systémy (např. vyhledávácí URL apod.)
- Vynucení přístupu uživatele k chráněné aplikaci přes přihlašovací stránku aplikace
- Podpora nastavení bezpečnostních politik podle IP adresy, doménového jména a URI
- Podpora a filtrování WebSocket provozu
- Blacklistování IP adres, které opakovaně snaží překonat bezpečnostní opatření v politice
- Možnost rozšíření o detekci a ochranu před kampaněmi kybernetických útoků, tedy vlnám kybernetických útoků zaměřených na konkrétní zranitelnost či zranitelnosti technologické nebo aplikační platformy
- Ochrana před útoky typu MitB pomocí obfuskace nebo šifrování formulářových polí v přihlašovacích URL
- Automatická instalace a aktualizace databáze pro detekci útoků, botnetů nebo kampaní kybernetických útoků
- Možnost rozšíření o detekci a ochranu před robotickými klienty pro nativní mobilní aplikace IOS a Android
- Vestavěná ochrana proti HTTP DoS a DDoS útokům založená na behaviorální analýze

Veškerý dodaný SW musí být v souladu s legislativou, zejména ZoKB a GDPR a musí k němu být v tomto smyslu v rámci nabídky dodána odpovídající technická dokumentace.

1.2. INFORMACE K TECHNICKÉMU ŘEŠENÍ

Útočníci a konkurenti neustále hledají způsoby, jak proti vám využít váš vlastní majetek. Většina manažerů informační bezpečnosti se shodne na tom, že ochrana webových aplikací je nutností, avšak integrace takové obranné schopnosti do vývojového životního cyklu může být časově náročná a nákladná. To je částečně způsobeno obtížností kódování obraných mechanismů proti i dobře známým hrozbám. Skutečností však zůstává, že útoky mají mnoho podob, přičemž nejde jen o zneužívání zranitelných míst, ale i o obchodní logiku a náklady spojené s udržováním vysoce dostupné přítomnosti online.

Některé významné hrozby, jako je např. tzv. „credential stuffing“, navíc představují rizika, která zdědíte z narušení bezpečnosti, k nimž došlo v jiných organizacích. Je možné, že jste vynaložili veškerou náležitou péči, abyste ochránili uživatelské účty před útokem, pokud však zabezpečujete účty pomocí hesel, pak jste stale vystavení riziku kvůli tomu, že uživatelé opakovaně používají hesla v rámci různých digitálních prostředí, která navštěvují.

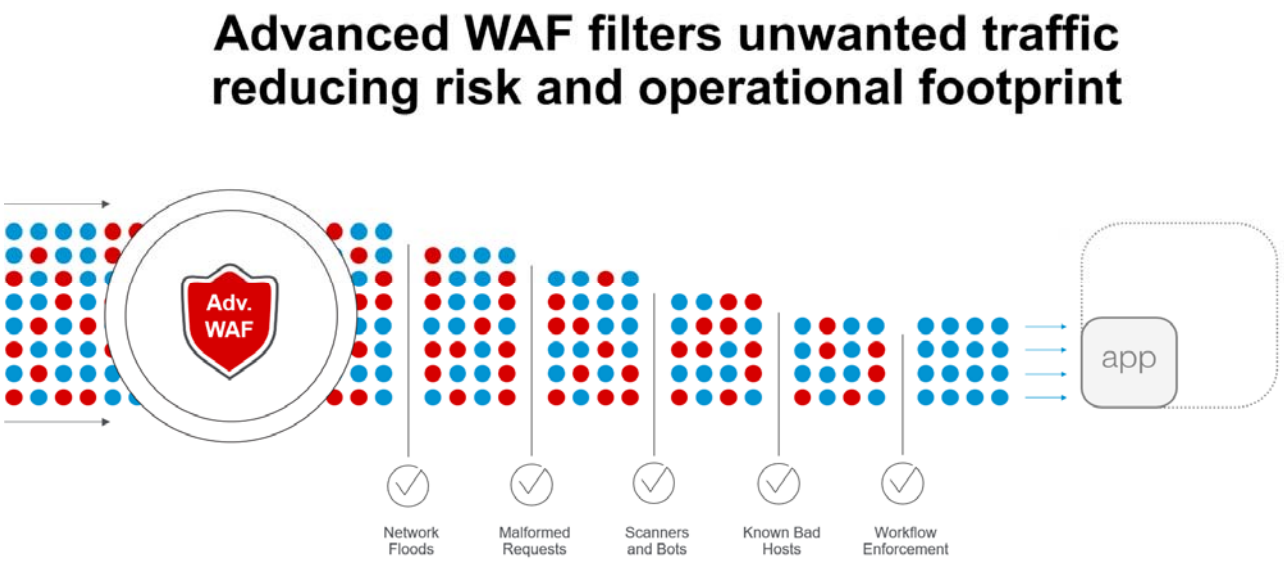
Nástroje jako F5 Advanced WAF mohou také sehrát důležitou roli, pokud jde o cloudové úlohy. Vaše organizace se nepochybně škáluje tak, aby sloužila zákazníkům na základě poptávky a aby těmto zákazíkům nabídla tu nejlepší možnou zkušenost. Nicméně škálování za účelem obsloužení všech návštěvníků s sebou nese související náklady – musíte škálovat tak, abyste obsloužili jak svou zamýšlenou klientelu, tak i veškerý botový provoz a automatizaci (jak chtěnou, tak i nechtěnou). Řešení Advanced WAF vám může pomoci odfiltrovat nechtěnou automatizaci a předejít nutnosti škálovat aplikace nad rámec toho, co vaše cílová klientela vyžaduje. Jedná se o oboustranně výhodný scénář jak z hlediska bezpečnosti, tak i řízení nákladů. Vaše bezpečnostní řešení pak pomáhají snižovat náklady a zároveň zajišťovat odolnost vašich webových aplikací.

1.2.1. PŘEHLED ŘEŠENÍ OD F5

Řešení Advanced WAF od F5 poskytuje vysoce výkonnou, full-proxy ochranu webových aplikací, která umožňuje zmírnění jak již známých, tak i nově vznikajících rizik v oblasti webové bezpečnosti. Nasazení řešení Advanced WAF před vašimi webovými aplikacemi pomůže zastavit útoky dříve, než se mohou dostat do samotných aplikací, což dá vývojovým týmům a vlastníkům aplikací manévrovací prostor a potřebný klid. Řešení Advanced WAF bylo speciálně navrženo tak, aby chránilo webové aplikace a rozhraní API a aby optimalizovalo provoz těchto služeb a zároveň vyžadovalo malou nebo žádnou vývojářskou integraci nebo rozšíření vašich stávajících vývojových postupů.

Kromě toho, pokud pro doručování aplikací a vyrovnávání zátěže používáte funkcionalitu BIG-IP LTM, pak tato obranná schopnost může být využita s minimálními nebo žádnými dodatečnými změnami vaší aplikační architektury. Aplikace podporující SSL/TLS mohou využívat ten nejlepší offloading dešifrování SSL od společnosti F5 a mohou mít rychle a snadno aktivovány politiky a profily řešení Advanced WAF pro zajištění pozitivního bezpečnostního nastavení, které vyžadují pro svůj optimální provoz a výkonnost.

Kromě ochrany zranitelných míst může řešení Advanced WAF poskytovat i funkce, které zvyšují schopnost vaší organizace plnit požadavky na dodržování předpisů a reporting a chrání vaše služby před rostoucím přílivem rizik podporovaných boty. Poskytne i výjimečnou ochranu proti nově vznikajícím hrozbám, jako jsou útoky na samotnou logiku aplikace (angl. business logic), krádež duševního vlastnictví, škrábání obsahu (content scraping), credential stuffing, exfiltrace dat a odepření služby (angl. denial-of-service – DoS) – z nichž všechny obejdou tradiční řešení WAF, poněvadž tyto vektory nepředstavují tradiční webová zranitelná místa, která byste našli v seznamu OWASP Top 10.



Řešení Advanced WAF filtruje nechtěný provoz a zároveň snižuje riziko a provozní stopu

Síťové záplavy | Chybně naformátované žádosti | Skenery a boty | Známí špatní hostitelé | Prosazení pracovního postupu

Obrázek 1: Řešení Advanced WAF od spol. F5

1.2.2. PŘÍPADY POUŽITÍ

Ochrana proti rizikům uvedených v owasp TOP 10	Rozpoznání botů a obrana před nimi	Zpřesnění informací důležitých pro podnikání
Pokud zodpovídáte za vývoj, zabezpečení nebo provoz webové aplikace, pak je znalost dokumentu OWASP Top 10 nutností, a testování bezpečnosti na základě OWASP Top 10 je základním požadavkem mnoha odvětvových a regulačních standardů, jako je např. PCI DSS. Mnohé rizikové oblasti uvedené na seznamu OWASP Top 10 se tam již nacházejí celou řadu let – jedná se o problémy, jejichž řešení je obtížné. Řešení Advanced WAF of spol. F5 obsahuje funkce a ochranné mechanismy, které potřebujete k řešení těchto rizik, a naše přehledy a dashboardy vám umožňují zajistit (a prokázat), že disponujete ochranou, kterou potřebujete.	Vypořádání se s boty je nedílnou součástí podnikání na internetu. Někteří boti jsou neškodní, nebo mohou být dokonce užiteční, jako tomu je v případě digitálních asistentů. Nicméně jako každý užitečný nástroj mohou být boti využiti útočníky k umožnění a škálování škodlivých aktivit. Hrozby související s boty se neustále vyvíjejí, což je způsobeno stále se rozšiřujícím seznamem motivačních faktorů, jako jsou spotřebitelské podvody, krádeže duševního vlastnictví, snaha o dosahování dlouhodobého zisku neetickým způsobem, politické cíle nebo drobné osobní zášti. Rozpoznání botů a škodlivé automatizace je prvním krokem k neutralizaci a zmírnění jejich nepříznivých dopadů.	V době velkých dat a analytik, může blokování zavádějících kliknutí a zároveň zaměření se na kliknutí od vašich zákazníků znamenat rozdíl mezi úspěchem a neúspěchem. Nicméně oddělit legitimní provoz od provozu bezcenného (nebo dokonce škodlivého) může být obtížné, pokud to máte dělat sami. Řešení Advanced WAF od spol. F5 vám může pomoci zvládnout explozi automatizovaného provozu, což vám umožní co nejlépe sloužit svým skutečným zákazníkům, optimalizovat vaše stránky a služby a získat analytické informace, které jsou založeny na datech a které vaše firma potřebuje.

### Zmírnění zranitelností Řešení Advanced WAF od spol. F5 může zmírnit známé pokusy o zneužití cílené na zveřejněná zranitelná místa a pomoci vám znovu získat kontrolu nad vašimi procesy řízení změn a přestat reagovat na nové zranitelnosti s tím, jak jsou zveřejňovány. Řešení Advanced WAF, běžně označované jako tzv. „virtuální záplatování“ (angl. virtual patching), může být integrováno s nástroji skenování zranitelností, aby tak v reálném čase poskytovalo ochranu aplikací, které mohou obsahovat součásti se známými zranitelnými místy, což vám umožní udržovat je online a obsluhovat zákazníky, zatímco jsou vytvářeny a realizovány nápravné plány.	### Prevence webových podvodů Digitální inovace změnily všechno: peníze jsou všude, takže každá firma je potenciálním cílem podvodů. Chcete-li účinně bojovat proti nebezpečí podvodů, potřebujete schopnost rozpoznat a zmařit širokou škálu kreativních, složitých a nenápadných nástrojů a taktických postupů, které zločinci používají k hodnocení a zneužívání zranitelných aplikací a procesů. Řešení Advanced WAF od F5 poskytuje takovou kombinaci ochrany aplikací, síťové bezpečnosti, kontroly přístupu, získávání informací o hrozbách a kontroly koncových bodů, která vám dává nástroje, jež potřebujete k zastavení podvodných aktivit – ještě předtím, než si mohou začít vybírat daň na vaší podnikatelské činnosti.	### Bezpečnost API S tím, jak firmy vytvářejí a vydávají další aplikace, počet rozhraní API – která aplikacím umožňují automaticky komunikovat mezi sebou – exponenciálně vzrostl. V tomto rychle se měnícím prostředí potřebují vývojově provozní týmy (DevOps) rychle vytvářet a spravovat aplikační služby, aniž by se musely obávat slabých míst mezi aplikacemi. Problémem souvisejícím s rostoucím počtem API je skutečnost, že se stávají dalšími cíli hrozeb. Pro zmírnění hrozeb na úrovni API je zásadní mít zabezpečenou autorizaci mezi aplikacemi na základě standardizovaných a otevřených metod napříč webovými, mobilními a desktopovými prostředími.
### Bezpečný přístup k aplikacím Více než polovina případů porušení ochrany údajů se týká slabého, výchozího (defaultního) nebo odcizeného hesla. Řešení Advanced WAF od spol. F5 lze doplnit řešením Access Policy Manager (APM) od spol. F5 pro zajištění bezpečného přístupu kdykoliv a kdekoliv prostřednictvím integrované federace identit založené na standardech, jednotného přihlášení (SSO) a adaptivního vícefaktorového ověřování (MFA).	### Ochrana uživatelských pověření Během posledního desetiletí byly z nejrůznějších služeb odcizeny miliardy uživatelských pověření. Tato uživatelská jména, emailové adresy a hesla jsou zadávány prostřednictvím automatizovaných systémů za účelem převzetí kontroly and účty v rámci celého internetu. A i když jste se dosud nestali obětí některého z případů porušení ochrany údajů, vaši zákazníci jsou stále vystaveni riziku, pokud jinde použili stejné informace o účtu. Proaktivní systémy jako je Advanced WAF od spol. F5 vás nejen ochrání před těmito pokusy, ale především zabrání samotnému zachycení a odcizení těchto uživatelských pověření.	### Dodržování předpisů a reporting Mnoho regulačních norem (např. PCI) předepisuje nástroje jako je Advanced WAF, které pomáhají poskytovat ochranu, již moderní aplikace potřebují k ochraně uživatelských údajů a k zabránění porušení jejich ochrany. Komplexní protokolování a vytváření sestav, včetně dashboardů pro soulad s PCI a pokrytí OWASP vám umožní prokázat auditorům, že jste vynaložili veškerou náležitou péči na ochranu uživatelských údajů a zabránili porušením ochrany údajů, která ohrožují vaše podnikání.

1.2.3. DALŠÍ FUNKCE

Řešení Advanced WAF od společnosti F5 umožňuje bezpečnostnímu týmu zefektivnit obrannou strategii a činnosti týkající se zabezpečení aplikací, a zajistit tak větší svižnost a lepší kontrolu a řízení celé bezpečnosti webových aplikací. Některé důležité vlastnosti a charakteristické rysy řešení Advanced WAF zahrnují (mimo jiné) následující:

Flexibilní nasazení a licencování ▪ Místní hardwarová zařízení a šasi ▪ Privátní cloudové virtuální stroje ▪ Cloudové instance s využitím vlastní licence (Bring-your-own-license) ▪ Cloudové instance s fakturací za služby	**Povědomí o kontextové politice** ▪ Detekce útoků na základě zatížení ▪ Geolokace IP ▪ Inteligentní využívání IP údajů ▪ Identifikační údaje zařízení	**Protokolování a tvorba sestav** ▪ Dashboard pro soulad s OWASP Top 10 ▪ Porušení zásad ▪ Žádosti na bázi botů ▪ Podrobné přihlašovací profily pro každou aplikaci ▪ Plánované sestavy
Správa botů a obrana před nimi ▪ Bezchybné rozpoznání botů ▪ Profily obrany před boty ▪ Mobilní SDK proti botům (Anti-bot Mobile SDK) ▪ Podpisy botů	**Bezpečnostní kanály a předplatné** ▪ Podpisy útoků ▪ Podpisy botů ▪ Kampaně upozorňující na hrozby ▪ Problémy týkající se prohlížečů ▪ Serverové technologie	**Přenositelnost politik** ▪ Exportovatelné politiky, které lze znovu použít ▪ Jednotné politiky v rámci různých režimů nasazení ▪ Jednotné politiky v rámci různých cloudů
Bezpečnost uživatelských pověření ▪ Prevence útoků hrubou silou ▪ Šifrování na úrovni aplikací, formulářů a pověření	**Čištění obsahu** ▪ Čísla sociálního zabezpečení ▪ Čísla kreditních karet ▪ Vlastní vzory	**Kontrola na mikroúrovni** ▪ Politiky pro mikroslužby ▪ Vymáhání na úrovni jednotlivých podpisů ▪ Politiky na bázi jednotlivých URL a stohovatelné politiky pro selektivní vymáhání
Pokročilá programovatelnost a učení provozu ▪ Baselining provozu a behaviorální obrana před DoS na vrstvě L7 ▪ Režim učení a transparentní režim provozu ▪ Pravidla iRules pro odezvu na útok na konkrétní web	**Podpora síťového bezpečnostního modulu Hardware Security Module (HSM)** ▪ Thales (nCipher/Entrust) ▪ SafeNet / Gemalto /Thales ▪ Fortanix (Equinix) ▪ Cavium / Marvell (Liquid Security)	**Doplňky** ▪ Inteligentní využívání IP údajů ▪ Kampaně upozorňující na hrozby ▪ Mobilní SDK proti botům ▪ Řešení WebSafe proti podvodům ▪ Síťový HSM ▪ Správce přístupových zásad: F5 Access Policy Manager (APM)

1.3. SPLNĚNÍ PODMÍNEK ZADÁVACÍ DOKUMENTACE

Veškerý SW dodaný v rámci této dodávky splňuje požadavky vycházející z evropského nařízení (EU) 2016/679 (GDPR) a z něj vycházejícího zákona č.110/2018 a to zejména tím že:

- Zajišťuje sběr pouze nezbytných informací o uživatelích,
- Zajišťuje ochranu těchto dat před neoprávněným přístupem,
- Nepředává data třetím stranám,
- Neuchovává data mimo území EU,
- Nezpracovává informace o aktivitách uživatelů.

Dále splňuje požadavky zákona č. 181/2014 (Zákon o kybernetické bezpečnosti) a vyhlášky č. 82/2018 a to tím že:

- Ověřování identity uživatelů SW odpovídá požadavkům zákona,
- Systém zaznamenává aktivity systému/uživatelů (logy) v souladu s ZoKB,
- Umožňuje zálohování a obnovu dat
- Zajišťuje inventarizaci přístupových účtů

1.4. PŘEDMĚT PLNĚNÍ

Předmět nabídky je připraven na základě požadavků uvedených Zadavatelem v zadávací dokumentaci v její Příloze č. 1 – Technická specifikace. Poskytované plnění zahrnuje **dodávku, instalaci a konfiguraci 2 kusů** [redacted]

Součástí konfigurace je

- Dodávka a zapojení HW řešení v **režimu active/active** do infrastruktury zadavatele v datovém centru v Praze
- Přenesení kompletní konfigurace pro LB a WAF ze současného do nového řešení a **zajištění 100% současné funkcionality**

Vzhledem ke skutečnosti, že dodávaná technologie je shodná se současnou jak z pohledu výrobce, tak z pohledu funkčnosti, nezahrnuje předmět plnění proškolení obsluhy, napojení na dohledové centrum a zajištění uchování logů po dobu 1 roku.

Součástí plnění je zajištění **následné servisní podpory výrobce F5 (S&M 5x10, RMA NBD) po dobu 4 let**.

Příloha č. 2

Harmonogram

Tabulka níže předkládá hrubý implementační harmonogram. Uvedeny jsou nejzazší možné termíny pro dokončení jednotlivých fází realizačního projektu.

Aktivita	Termín
Termín účinnosti smlouvy mezi Zadavatelem a Dodavatelem	T0
Vytvoření konfigurační zálohy Detailní analýza stávající konfigurace Vytvoření základní dokumentace	T0 + 21 dnů
Dodávka HW a instalace do prostředí Zadavatele	T0 + 28 dnů
Konfigurace a nastavení v prostředí Zadavatele, provedení funkčních testů	T0 + 35 dnů
Dodání kompletní dokumentace a nasazení ASM v blokovacím módu	T0 + 40 dnů

Nezbytným předpokladem implementace služby WAF v souladu s výše uvedeným harmonogramem, je dostatečná součinnost ze strany zákazníka, a to zejména:

- včasné poskytnutí potřebných informací a podkladů,
- zajištění a poskytnutí potřebných lidských zdrojů,
- organizační koordinace na straně Zadavatele a jeho dodavatelů,
- organizační koordinace s jednotlivými členy projektového týmu na straně Zadavatele a jeho dodavatelů,
- zajištění konfiguračních oken v souladu s harmonogramem a
- aktivní spolupráce.

Nesplnění výše uvedených požadavků či pozdržení dodání potřebných materiálů může mít negativní vliv na úspěšné a včasné dokončení projektu.

Pro úspěšnou realizaci v průběhu fází předpokládáme zapojení odborných specialistů, zejména pak:

- aplikační architekt/specialista znalý architektury aplikací,
- specialista/analytik bezpečnosti informačních technologií a
- testovací specialista aplikací.

Příloha č. 3

Rozpis ceny

CENA ZA CELKOVOU DODÁVKU

Cena bez DPH (uvedena v Kč)	Sazba DPH	Cena s DPH (uvedena v Kč)
1 687 040,-	21 %	**2 041 318,4**

ROZPIS CENY

Název položky	Popis	Počet jednotek	Jednotková	Celková
			Cena bez DPH (v Kč)	
F5-BIG-AWF-I2600	BIG-IP i2600 Advanced Web Application Firewall (16 GB Memory, Base SSL, Base Compression)	2	369 431,-	738 862,-
F5-SVC-BIG-STD-L1-3	Level 1-3 Standard Service for BIG-IP (5x10)	8	51 356,-	410 848,-
F5-SVC-BIG-RMA-2	Next-Business-Day Hardware Replacement Service (RMA) for BIG-IP	8	8 559,-	68 472,-
F5-UPG-SFPC-R	BIG-IP & VIPRION SFP 1000BASE-T Transceiver (Field Upgrade)	8	7 829,-	62 632,-
F5-UPG-DC-I2XXX	BIG-IP Single DC Power Supply for i2X00 (650 W, Field Upgrade)	2	73 711,-	147 422,-
F5-SBS-BIG-TC-1-3YR	BIG-IP Threat Campaigns License for i4X00/i2X00 Advanced Web Application Firewall (3-Year Subscription)	2	63 051,-	126 102,-
F5-SBS-BIG-TC-1-1YR	BIG-IP Threat Campaigns License for i4X00/i2X00 Advanced Web Application Firewall (1-Year Subscription)	2	26 271,-	52 542,-
Implementační práce T-Mobile	Dodávka a zapojení HW řešení do infrastruktury zadavatele v datovém centru v Praze. Přenesení kompletní konfigurace pro LB a WAF ze současného do nového řešení a zajištění 100% současné funkcionality. Dokumentace a projektové řízení.	1	80 160,-	80 160,-