Kupní smlouva č. SOAP/01-4155/2026-2
JID: SOAP2611928

podle § 2079 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen občanský zákoník)

Článek I.
Smluvní strany

BIT SERVIS spol. s r.o.

Sídlo:	Libušská 144/252, 142 00 Praha 4
Zastoupená:	Ondřejem Koutským, jednatelem
IČ:	45793972
DIČ:	CZ45793972
Bankovní spojení:	1629492/ 0800
ID DS:	5nzruiy
Telefony:	[redacted]
Kontaktní osoby:	[redacted] zároveň kontaktní osoba pro bezpečnost)
Kontaktní e-maily:	[redacted]

Vedená u Městského soudu v Praze, spisová značka C 11262.

(dále jen „prodávající“)

a

Česká republika – Státní oblastní archiv v Plzni

Sídlo:	Sedláčkova 44, 306 12 Plzeň
Zastoupená:	doc. PhDr. Karlem Řeháčkem, Ph.D., ředitelem
IČ:	70979090
DIČ:	CZ70979090, není plátcem DPH
Bankovní spojení:	4245881/0710
ID datové schránky:	b9xaiw4
Telefon:	[redacted]
Kontaktní osoby:	[redacted] informatici
Kontaktní e-mail:	

(dále jen „kupující“)

Článek II.
Předmět plnění

1. Předmětem této smlouvy je dodávka, implementace a uvedení do provozu nástroje pro ochranu veřejně přístupných webových aplikací (Web Application Firewall, dále jen „WAF“) a nástroje pro ochranu elektronické pošty (Secure Email Gateway, dále jen „SEG“) (dále společně jen „zboží“), včetně licencí a technické podpory výrobce po dobu 5 let, implementačních služeb, integrace do bezpečnostní infrastruktury kupujícího, zaškolení administrátorů a dokumentace. Prodávající se zavazuje umožnit kupujícímu nabýt vlastnické právo k dodanému zboží a poskytnout mu příslušná licenční oprávnění.
2. Rozsah a parametry plnění jsou vymezeny v přílohách této smlouvy – Technická specifikace a Soupis položek dodávky. Plnění je nedělitelné; částečné plnění se nepřipouští.
3. Kupující se zavazuje řádně dodané zboží a související služby od prodávajícího odebrat a zaplatit za ně kupní cenu dle této smlouvy.

4. Prodávající prohlašuje, že je oprávněn dodat zboží a poskytovat implementační služby a podporu k němu, a že je držitelem všech oprávnění výrobce, která jsou k tomu nezbytná.
5. Prodávající prohlašuje, že na dodané zboží ani na jeho komponenty nedopadá ke dni uzavření této smlouvy platné varování Národního úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“).

Článek III.
Kupní cena

1. Smluvní strany se dohodly, že cena za zboží je stanovena ve výši:

Cena bez DPH:	826 000,- Kč bez DPH
DPH 21 %:	173 460,- Kč
CELKEM:	**999 460,- Kč s DPH**

2. Cena zahrnuje veškeré náklady spojené s dodáním zboží, jeho instalací a implementací v místě plnění, integrací do infrastruktury kupujícího, testováním, zaškolením, dokumentací a s technickou podporou výrobce po dobu 5 let od převzetí plnění.
3. Cena je stanovena jako nejvýše přípustná, lze ji navýšit pouze v případě změny zákonné sazby daně z přidané hodnoty o takto zvýšenou daň.

Článek IV.
Doba a místo plnění, všeobecné dodací podmínky

1. Prodávající je povinen dodat zboží, provést implementaci a předat celé plnění do 8 týdnů od nabytí účinnosti této smlouvy, nejpozději však **do 30. listopadu 2026**. Dílčí termíny stanoví kapitola 8 přílohy č. 2 – Technická specifikace.
2. Kupující nabývá vlastnické právo ke zboží jeho převzetím od prodávajícího.
3. Převzetí celého plnění bude prokázáno datovaným podpisem akceptačního protokolu podle kapitoly 8 přílohy č. 2 – Technická specifikace, na kterém budou uvedeny identifikátory dodaných licencí.
4. Místo plnění: Státní oblastní archiv v Plzni, Sedláčkova 44, 306 12 Plzeň.
5. Kupující se zavazuje poskytnout prodávajícímu součinnost potřebnou pro řádné plnění závazků z této smlouvy v rozsahu kapitoly 9 přílohy č. 2 – Technická specifikace, zejména zpřístupnit virtualizační platformu, zřídit vzdálený přístup a zajistit součinnost správců dotčených systémů.

Článek V.
Záruka a podpora

1. Součástí dodávky je technická podpora výrobce v délce 5 let od převzetí plnění, včetně nároku na aktualizace programového vybavení (bezpečnostní opravy a nové verze produktu) a na aktualizace detekčních databází v rozsahu přílohy č. 2 – Technická specifikace. Rozsah a podmínky této podpory se řídí podmínkami výrobce a jsou součástí dodávaného plnění.
2. Prodávající poskytuje záruku za jakost v délce 5 let od převzetí plnění, a to na dodané zboží i na konfiguraci, kterou provedl. Podmínky záruky zboží dodaného výrobcem (odlišným od prodávajícího) se řídí podmínkami záruky poskytované výrobcem.
3. Vytkne-li kupující vadu, která brání užívání dodaného plnění, zahájí prodávající její řešení nejpozději do konce následujícího pracovního dne od vytknutí a poskytne bezodkladně náhradní řešení, umožňuje-li to povaha vady. Ostatní vady odstraní bez zbytečného odkladu, nejpozději do 20 pracovních dnů od vytknutí. V případě, že relevantní podmínky záruky výrobce stanoví jinak, použijí se přednostně podmínky výrobce.

4. Předmětem této smlouvy není správa, dohled ani jiné průběžné provozování dodaného řešení. Dodané řešení po převzetí provozuje kupující; provoz a zálohování virtuálních strojů, na nichž je provozováno, zajišťuje kupující.

Článek VI.
Povinnost mlčenlivosti, ochrana osobních údajů

1. Smluvní strany se zavazují zachovávat ve vztahu ke třetím osobám mlčenlivost o informacích, které při plnění této smlouvy vzájemně získají o sobě či o svých zaměstnancích, které nejsou veřejně známé nebo známé třetí straně a které lze s přihlédnutím k okolnostem a obchodním zvyklostem označit za důvěrné, a nesmí je použít v rozporu s účelem této smlouvy ani je poskytnout bez písemného souhlasu druhé smluvní strany žádné třetí osobě (s výjimkou zákonných případů).
2. Smluvní strany jsou povinny zajistit, že nebudou neoprávněně pořizovány kopie důvěrných informací a že nebudou zjišťovány informace, které nejsou nezbytně nutné ke splnění povinností vyplývajících z této smlouvy.
3. Smluvní strany se zavazují pro případ, že se v průběhu plnění této smlouvy dostanou do kontaktu s údaji druhé smluvní strany vyplývající z její provozní činnosti, tyto údaje v žádném případě nezneužít, nezměnit ani nijak nepoškodit, neztratit či neznehodnotit.
4. Smluvní strany se zavazují chránit osobní údaje. Pokud se smluvní strany v rámci plnění této smlouvy dostanou do kontaktu s osobními údaji, jsou povinny je ochraňovat a nakládat s nimi v souladu s příslušnými právními předpisy, a to i po ukončení této smlouvy.
5. Plnění podle této smlouvy není zpracováním osobních údajů pro kupujícího. Získá-li prodávající přístup k osobním údajům zpracovávaným kupujícím, postupují smluvní strany podle odstavce 17.6 přílohy č. 1 – Bezpečnostní opatření.
6. Dostane-li se prodávající při plnění do kontaktu s osobními údaji, nakládá s nimi pouze na základě písemných pokynů kupujícího, nepředává je mimo Českou republiku a zajistí, aby se osoby, které k nim mají přístup, zavázaly k mlčenlivosti.
7. Zjistí-li prodávající porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu kupujícímu.
8. Prodávající nesmí zapojovat do svých činností pro kupujícího kromě svých řádně proškolených zaměstnanců a poddodavatelů uvedených v příloze č. 3 – Soupis položek dodávky žádné další osoby bez předchozího písemného souhlasu kupujícího.
9. Plnění zajišťuje realizační tým uvedený v příloze č. 3. – Soupis položek dodávky. Člena týmu, jehož prostřednictvím prodávající prokázal kvalifikaci, může nahradit jen s předchozím písemným souhlasem kupujícího osobou, která splňuje stejné požadavky na kvalifikaci; souhlas kupujícího nebude bezdůvodně odmítnut.
10. Účinnost ustanovení tohoto článku přetrvá i po ukončení účinnosti této smlouvy z jakéhokoliv důvodu.

Článek VII.
Platební podmínky

1. Prodávající je oprávněn fakturovat kupní cenu až po převzetí celého plnění kupujícím podle článku IV. odst. 3 této smlouvy a fakturu vystaví a doručí kupujícímu do 7 dnů od převzetí plnění.
2. Faktura je splatná do 14 dnů od jejího doručení kupujícímu prostřednictvím informačního systému datových schránek, na e-mail  nebo na adresu sídla kupujícího.

3. Faktura musí mít náležitosti daňového dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a dle § 29 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
4. Faktura se považuje za proplacenou okamžikem odepsání fakturované částky z účtu kupujícího ve prospěch účtu prodávajícího.
5. Kupující není v prodlení s placením fakturovaných částek, jestliže vrátí fakturu prodávajícímu do 7 dnů od jejího doručení proto, že faktura obsahuje nesprávné údaje nebo byla vystavena v rozporu se smlouvou. Konkrétní důvody je kupující povinen uvést zároveň s vrácením faktury. V případě doručení faktury e-mailem je vrácení faktury realizováno oznámením na kontaktní e-mail prodávajícího. U nové nebo opravené faktury běží nová lhůta splatnosti.
6. Zálohu kupující neposkytuje.

Článek VIII.
Smluvní pokuty a sankce

1. Nedodrží-li prodávající smluvený termín dodání nebo termín pro odstranění vad, zaplatí kupujícímu smluvní pokutu ve výši 0,1 % z kupní ceny včetně DPH za každý, byť i započatý, kalendářní den prodlení.
2. Nezaplatí-li kupující kupní cenu včas, je povinen zaplatit prodávajícímu úrok z prodlení ve výši 0,1 % z dlužné částky za každý, byť i započatý, den prodlení.
3. Poruší-li prodávající povinnost mlčenlivosti, povinnosti vztahující se k ochraně osobních údajů vyplývající z této smlouvy nebo povinnosti podle přílohy č. 1 – Bezpečnostní opatření, zejména oznamovací povinnost, zákaz použít data kupujícího k jinému účelu, podmínky zapojení poddodavatelů nebo zákaz použít prostředky, na které dopadá platné varování NÚKIB, je povinen zaplatit kupujícímu smluvní pokutu ve výši 20 000 Kč za každý nikoli nepodstatný případ porušení povinnosti.
4. Zaplacením smluvní pokuty není dotčen nárok kupujícího na náhradu škody v částce převyšující zaplacenou smluvní pokutu.
5. Smluvní pokuty jsou splatné do 15 kalendářních dnů ode dne doručení písemné výzvy oprávněné smluvní strany k jejich úhradě povinnou smluvní stranou, není-li ve výzvě uvedena lhůta delší. Písemná výzva musí být prokazatelně doručena doporučeným dopisem nebo datovou schránkou.
6. Smluvní strany se dohodly, že celková výše smluvních pokut a náhrady škody splatných dle této smlouvy může dosáhnout nejvýše 30 % kupní ceny.
7. Účinnost ustanovení tohoto článku přetrvá i po ukončení účinnosti této smlouvy z jakéhokoliv důvodu.

Článek IX.
Ukončení smlouvy, předání dat a výmaz

1. Od smlouvy lze odstoupit za podmínek stanovených v § 2001-2005 občanského zákoníku a touto smlouvou.
2. Podstatným porušením smluvních povinností se rozumí opakované podstatné neplnění kvantitativních a kvalitativních požadavků kupujícího prodávajícím dle článků II. a III. této smlouvy a opakované nebo závažné porušení povinností podle přílohy č. 1 – Bezpečnostní opatření, pokud taková neplnění nebo porušení nebudou prodávajícím napravena ani v přiměřené dodatečné lhůtě stanovené kupujícím v jeho písemné výzvě k nápravě.

3. Kupující je oprávněn odstoupit od smlouvy, jestliže prodávající vstoupí do likvidace, nebo je prodávající v úpadku nebo prodávající sám podá návrh na zahájení insolvenčního řízení. Prodávající je povinen o této skutečnosti neprodleně písemně informovat kupujícího.
4. Prodávající při předání plnění předá kupujícímu též konfigurace dodaných systémů v exportovatelném a dokumentovaném formátu, provozní a bezpečnostní záznamy vztahující se k plnění a dokumentaci, to vše nejpozději do 10 pracovních dnů. Přechodová součinnost v rozsahu nejvýše 8 hodin je zahrnuta v ceně plnění.
5. Po potvrzení řádného převzetí plnění a uplynutí ochranné lhůty 30 dnů prodávající vymaže data kupujícího ze svých aktivních systémů do 10 pracovních dnů. Data v zálohách, která nelze vymazat jednotlivě, nebudou dále aktivně zpracovávána a budou vymazána při běžné rotaci záloh, nejpozději do 12 měsíců. O dokončení výmazu předá prodávající na žádost kupujícího písemné potvrzení s rámcovým vymezením vymazaných dat, datem dokončení a nejzazším datem výmazu ze záloh. Povinnosti dle tohoto odstavce se nevztahují na povinně uchovávaná data a data potřebná k dalšímu plnění této smlouvy.
6. Odstoupení od smlouvy musí být prokazatelně písemně oznámeno druhé smluvní straně doporučeným dopisem nebo datovou schránkou a je účinné dnem doručení tohoto oznámení. Odstoupením nezaniká právo kupujícího na již poskytnuté licenční oprávnění k plnění, které bylo řádně dodáno a uhrazeno.

Článek X.
Závěrečná ustanovení

1. Tato smlouva nabývá platnosti podpisem obou smluvních stran a účinnosti dnem uveřejnění prostřednictvím registru smluv dle zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv, ve znění pozdějších předpisů. Kupující se zavazuje realizovat zveřejnění této smlouvy v předmětném registru v souladu s uvedeným zákonem.
2. Prodávající je povinen písemně informovat kupujícího o skutečnostech majících vliv na plnění smlouvy, a to neprodleně, nejpozději následující pracovní den poté, kdy příslušná skutečnost nastane nebo prodávající zjistí, že by nastat mohla.
3. Prodávající tímto prohlašuje, že veškeré podmínky a požadavky kupujícího vymezené v zadávací dokumentaci jsou pro něj závazné a jsou součástí této smlouvy.
4. Smlouva může být měněna nebo doplňována jen vzestupně očíslovanými písemnými dodatky, které se stanou nedílnou součástí této smlouvy. Dodatky musí být podepsané oprávněnými zástupci obou smluvních stran.
5. Prodávající nesmí bez předchozího souhlasu kupujícího postoupit svá práva a povinnosti plynoucí z této smlouvy třetí osobě.
6. Z důvodu právní jistoty smluvní strany prohlašují, že jejich závazkový vztah založený touto smlouvou se řídí zákonem č. 89/2012 Sb., občanským zákoníkem, ve znění pozdějších předpisů.
7. Smluvní strany se zavazují, že veškeré spory vzniklé v souvislosti s realizací smlouvy budou řešeny smírnou cestou – dohodou. Nedojde-li k dohodě, budou spory řešeny před příslušnými obecnými soudy České republiky.
8. Vzhledem k veřejnoprávnímu charakteru kupujícího prodávající souhlasí se zveřejněním jakékoli části i plného znění této smlouvy včetně příloh a dodatků dle příslušných právních předpisů, zejména zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů a zákona č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto

smluv a o registru smluv, ve znění pozdějších předpisů. Text této smlouvy, dodatků ani příloh této smlouvy se nepovažuje za obchodní tajemství.

9. Tato smlouva je vyhotovena v elektronické podobě, smlouvu podepsanou oběma smluvními stranami obdrží obě smluvní strany.
10. Obě smluvní strany prohlašují, že tuto smlouvu uzavřely svobodně a vážně, že považují obsah této smlouvy za určitý a srozumitelný a že jsou jim známy veškeré skutečnosti, jež jsou pro uzavření této smlouvy rozhodující, na důkaz čehož připojují k této smlouvě své podpisy.
11. V případě rozporu mezi ustanoveními této smlouvy, jejích příloh a dalších dokumentů, které jsou její součástí, se použijí v tomto pořadí: text této smlouvy, příloha č. 1 – Bezpečnostní opatření, příloha č. 2 – Technická specifikace, ostatní přílohy této smlouvy, zadávací dokumentace, nabídka prodávajícího a obchodní, licenční nebo jiné podmínky prodávajícího či výrobce. Nabídka prodávajícího ani tyto podmínky nesmějí omezit nebo vyloučit bezpečnostní požadavky stanovené touto smlouvou a jejími přílohami.
12. Nedílnou součástí této smlouvy jsou následující přílohy:
    - Příloha č. 1 – Bezpečnostní opatření
    - Příloha č. 2 – Technická specifikace
    - Příloha č. 3 – Soupis položek dodávky
    - Příloha č. 4 – Čestné prohlášení k mezinárodním sankcím

V Praze elektronicky podepsáno
za prodávajícího:



Ondřej Koutský
jednatel

V Plzni elektronicky podepsáno
za kupujícího:



doc. PhDr. Karel Řeháček
ředitel Státního oblastního archivu v Plzni

Příloha č. 1

Bezpečnostní opatření

1. Úvodní ustanovení

1.1 Tato příloha stanoví bezpečnostní požadavky související s plněním prodávajícího a odpovědnost smluvních stran za zavedení, provádění a kontrolu souvisejících bezpečnostních opatření. Prostředím kupujícího se pro účely této přílohy rozumí technické prostředí, ve kterém je předmět plnění provozován nebo do kterého prodávající při plnění přistupuje, včetně prostředí, které kupujícímu poskytuje třetí osoba.

1.2 Kupující je poskytovatelem regulované služby v režimu nižších povinností podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti.

1.3 Předmětem plnění je dodávka a implementace nástroje pro ochranu webových aplikací (WAF) a nástroje pro ochranu elektronické pošty (SEG) a jejich začlenění do bezpečnostní infrastruktury kupujícího. Elektronická pošta a veřejně přístupné webové aplikace kupujícího jsou podpůrnými aktivy, na nichž závisí komunikace kupujícího s veřejností a s orgány veřejné moci a zpřístupňování archiválií. Plnění zasahuje do konfigurace prvků, které tato aktiva chrání, a prodávající při implementaci získává privilegovaný přístup k bezpečnostní infrastruktuře kupujícího a k informacím o jejím uspořádání.

1.4 Bezpečnostní požadavky se uplatní v rozsahu, v němž plnění souvisí s aktivy zahrnutými do stanoveného rozsahu řízení kybernetické bezpečnosti kupujícího. Požadavky zohledňují zejména zákon č. 264/2025 Sb., o kybernetické bezpečnosti, a vyhlášku č. 410/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu nižších povinností.

1.5 Povinnosti podle této přílohy se vztahují na dodání a implementaci předmětu plnění, na odstraňování vad a na povinnosti, které tato příloha výslovně stanoví pro dobu technické podpory výrobce. Běžný provoz, správu, dohled ani zálohování dodaného řešení tato příloha na prodávajícího nepřenáší.

1.6 Odpovědnost kupujícího jako poskytovatele regulované služby za plnění povinností podle právních předpisů není uzavřením smlouvy přenesena na prodávajícího. Tím není dotčena odpovědnost prodávajícího za plnění povinností stanovených smlouvou nebo právními předpisy.

1.7 Smluvní strany se dohodly, že je-li to potřebné ke splnění požadavků právních předpisů v oblasti kybernetické bezpečnosti nebo ochrany osobních údajů, zahájí bez zbytečného odkladu po výzvě kterékoli smluvní strany jednání o uzavření dodatku smlouvy zohledňujícího takové požadavky.

2. Obecné bezpečnostní povinnosti

2.1 Prodávající při plnění dodržuje organizační a technická bezpečnostní opatření přiměřená povaze plnění a bezpečnostním rizikům, která mohou ovlivnit důvěrnost, integritu nebo dostupnost dat, služeb a dalších aktiv kupujícího.

2.2 Kontaktní osoby smluvních stran včetně kontaktní osoby prodávajícího pro bezpečnost jsou uvedeny v článku I smlouvy. Změnu kontaktní osoby nebo jejích kontaktních údajů si smluvní strany oznámí bez zbytečného odkladu; změna nevyžaduje změnu smlouvy.

2.3 Prodávající zajistí, aby osoby podílející se na plnění byly před zahájením činnosti seznámeny s relevantními bezpečnostními požadavky a byly vázány odpovídající povinností mlčenlivosti.

2.4 Prodávající přiděluje osobám podílejícím se na plnění oprávnění podle zásady potřeby vědět, tedy v rozsahu nezbytném pro výkon jejich činnosti.

2.5 Prodávající dodržuje bezpečnostní politiky kupujícího v rozsahu relevantním k plnění, pokud s nimi byl prokazatelně seznámen.

3. Bezpečnost informací a mlčenlivost

3.1 Prodávající chrání důvěrnost, integritu a dostupnost dat a informací kupujícího, které získá v souvislosti s plněním.

3.2 Prodávající používá data kupujícího výhradně za účelem a v rozsahu nezbytném pro plnění smlouvy. Prodávající nesmí data kupujícího využít pro vlastní potřebu, reklamu, profilování, trénování nebo zdokonalování modelů ani k jinému účelu, který není výslovně sjednán ve smlouvě, nebo je zpřístupnit třetí osobě, nestanoví-li právní předpis jinak.

3.3 Informace o uspořádání sítě kupujícího, o konfiguraci bezpečnostních prvků, o bezpečnostních politikách a o zjištěných zranitelnostech jsou důvěrné. Tyto informace ani jiná data kupujícího a jejich kopie nesmí prodávající bez předchozího písemného souhlasu kupujícího ukládat ani zpracovávat mimo prostředí kupujícího. Informace a data uložené se souhlasem kupujícího mimo jeho prostředí prodávající odstraní, jakmile pomine účel jejich uložení, a odstranění na vyžádání doloží.

3.4 Prodávající zachovává mlčenlivost o neveřejných informacích, o nichž se dozví v souvislosti s plněním. Povinnost trvá i po skončení smlouvy po dobu, po kterou informace nejsou oprávněně veřejné nebo nezanikl důvod jejich ochrany.

3.5 Je-li prodávající povinen zpřístupnit data kupujícího orgánu veřejné moci, informuje o tom kupujícího předem, pokud mu to právní předpis nezakazuje. Není-li předchozí informování právně nebo objektivně možné, informuje kupujícího bez zbytečného odkladu poté, co tato překážka pomine. Prodávající omezí zpřístupnění na nezbytný rozsah.

3.6 Předmětem plnění není zpracování osobních údajů pro kupujícího. Získá-li prodávající při implementaci nebo při odstraňování vad přístup k obsahu elektronické pošty nebo k jiným osobním údajům zpracovávaným kupujícím, uzavřou smluvní strany před zahájením takové činnosti ujednání o zpracování osobních údajů podle čl. 28 nařízení Evropského parlamentu a Rady (EU) 2016/679.

4. Řízení přístupů a bezpečnost lidských zdrojů

4.1 Přístup k datům, systémům a prostředkům kupujícího je povolen pouze jednoznačně identifikovaným osobám v nezbytném rozsahu a na nezbytnou dobu. Uživatelské a administrátorské účty jedné osoby musí být odděleny.

4.2 Sdílené osobní účty jsou zakázány. Technické účty musí mít určeného vlastníka, účel a odpovídající omezení.

4.3 Přístupy do prostředí kupujícího přiděluje a odebírá kupující nebo provozovatel prostředí na základě jeho pokynu. Prodávající včas předá identifikaci osob, pro které jsou přístupy požadovány, a bez zbytečného odkladu oznamuje změny, zejména ukončení činnosti osoby na plnění.

4.4 Privilegované a vzdálené přístupy musí používat vícefaktorové ověření. Není-li jeho použití z objektivních technických důvodů možné, prodávající tuto skutečnost předem doloží kupujícímu, navrhne náhradní bezpečnostní opatření odpovídající souvisejícím rizikům a použije je až po odsouhlasení kupujícím.

4.5 Vzdálený přístup do prostředí kupujícího se uskutečňuje výhradně přístupovým kanálem určeným kupujícím, s vícefaktorovým ověřením, jmenovitě pro předem oznámené osoby a po dobu nezbytnou k provedení dohodnuté činnosti.

4.6 Prodávající chrání autentizační prostředky a přístupové údaje proti ztrátě, zpřístupnění a zneužití.

4.7 Prodávající v prostředí kupujícího neinstaluje a nepoužívá nástroje, které nebyly předem písemně odsouhlaseny kupujícím. Prodávající nebude vyvíjet, kompilovat ani šířit programový kód, jehož účelem je neoprávněné ovládnutí, narušení nebo získání dat.

4.8 Prodávající zajistí dostatečnou míru zastupitelnosti pro technické aspekty řešení tak, aby plnění nebylo závislé na dostupnosti jediné osoby.

5. Fyzická bezpečnost

5.1 Prodávající dodržuje v objektech kupujícího režim návštěv a bezpečnostní požadavky na vstup do vymezených prostor.

5.2 Prodávající v objektech kupujícího neponechá volně dostupná datová média ani dokumentaci k předmětu plnění.

6. Řízení poddodavatelů a dodavatelského řetězce

6.1 Prodávající před zahájením plnění sdělí kupujícímu poddodavatele, kteří mohou mít vliv na bezpečnost plnění nebo přístup k datům kupujícího, včetně popisu činností, které budou při plnění zajišťovat.

6.2 Prodávající oznámí kupujícímu zamýšlenou změnu poddodavatele, zapojení dalšího poddodavatele nebo významnou změnu rozsahu činnosti stávajícího poddodavatele alespoň 15 pracovních dnů předem. Změna poddodavatele a zapojení dalšího poddodavatele podléhají předchozímu písemnému souhlasu kupujícího; mlčení kupujícího se nepovažuje za souhlas. Je-li změna nezbytná k bezodkladnému řešení bezpečnostní nebo provozní události, může kupující lhůtu zkrátit. Prodávající zajistí, aby byly příslušné bezpečnostní povinnosti na poddodavatele přeneseny před zahájením jeho činnosti.

6.3 Konfiguraci bezpečnostních politik WAF a SEG a jejich nasazení do produkčního prostředí provádí přímo prodávající; tato výhrada se nevztahuje na dodání licencí, aktualizací a technické podpory výrobce. Další řetězení poddodávek při implementaci není přípustné.

6.4 Prodávající smluvně přenese na poddodavatele bezpečnostní povinnosti podle smlouvy a této přílohy v rozsahu odpovídajícím činnostem poddodavatele.

6.5 Prodávající odpovídá za plnění bezpečnostních povinností poddodavatelů, jako by plnění poskytoval sám.

6.6 Prodávající na vyžádání doloží kupujícímu splnění povinností podle tohoto článku. Prodávající může přiměřeně chránit obchodní tajemství a jiné důvěrné informace, nesmí tím však znemožnit ověření plnění bezpečnostních požadavků.

6.7 Prodávající bez zbytečného odkladu písemně informuje kupujícího o významné změně svého ovládání podle zákona o obchodních korporacích a o změně vlastnictví aktiv zásadních pro plnění.

6.8 Prodávající při plnění nepoužije technické ani programové prostředky, na které dopadá platné varování NÚKIB, a to ani prostřednictvím poddodavatele. Vzdálená správa předmětu plnění ani přístup k datům kupujícího nesmějí být vykonávány z území, na které dopadá platné varování, a na takové území nesmějí být předávána ani na něm ukládána systémová a uživatelská data kupujícího.

6.9 Vydá-li NÚKIB po uzavření smlouvy varování, které dopadá na dodané řešení nebo jeho část, projednají smluvní strany bez zbytečného odkladu způsob jeho zohlednění, včetně výměny dotčené komponenty; výměnu sjednají písemným dodatkem smlouvy.

7. Kontrola a audit

7.1 Kupující je oprávněn přiměřeným způsobem ověřovat plnění bezpečnostních povinností prodávajícího. Prodávající poskytne nezbytnou součinnost a relevantní informace, dokumentaci, záznamy a jiné důkazy.

7.2 Prodávající bez zbytečného odkladu po oznámení zjištěných nedostatků předloží kupujícímu návrh plánu nápravy obsahující opatření, odpovědnosti a termíny jejich provedení. Plán nápravy podléhá odsouhlasení kupujícím. Kritické nedostatky začne prodávající řešit bezodkladně.

8. Změny konfigurace a zranitelnosti

8.1 Změny konfigurace bezpečnostních prvků v produkčním prostředí provádí prodávající po odsouhlasení kupujícím, v dohodnutém časovém okně a s předem připraveným postupem návratu do předchozího stavu. Před změnou pořídí zálohu dotčené konfigurace a provedenou změnu zdokumentuje.

8.2 Před předáním plnění prodávající ověří, že dodané řešení je v aktuální podporované verzi bez známých neopravených zranitelností, a zkontroluje jeho konfiguraci podle bezpečnostních doporučení výrobce. Zjištěné nedostatky odstraní před předáním plnění.

8.3 Po dobu technické podpory výrobce prodávající bez zbytečného odkladu informuje kupujícího o zveřejněných zranitelnostech dodaného řešení a o dostupných opravách a zajišťuje jejich dostupnost v rámci technické podpory výrobce. Nasazení oprav po převzetí plnění zajišťuje kupující.

9. Záznamy o činnosti prodávajícího

9.1 Prodávající vede záznamy o své činnosti v prostředí kupujícího, zejména o přístupech a o provedených změnách konfigurace, a na vyžádání je předá kupujícímu.

9.2 Záznamy nesmějí obsahovat přístupová hesla ani soukromé kryptografické klíče. Prodávající je chrání proti neoprávněnému přístupu, změně a výmazu a uchovává je nejméně 12 měsíců od předání plnění.

10. Zvládání kybernetických bezpečnostních událostí a incidentů

10.1 Prodávající oznámí kupujícímu bez zbytečného odkladu, nejpozději do 24 hodin od zjištění, kybernetickou bezpečnostní událost (dále jen „KBU“), kybernetický bezpečnostní incident (dále jen „KBI“) nebo zranitelnost, která má nebo může mít významný dopad na bezpečnost plnění, data kupujícího, aktiva kupujícího nebo poskytování regulované služby.

10.2 Prvotní oznámení obsahuje alespoň známý čas zjištění, popis události, dotčená aktiva a služby, předběžný dopad, přijatá opatření a kontaktní osobu. Prodávající průběžně předává aktualizace a po zvládnutí incidentu zprávu o příčině, dopadech a nápravných opatřeních.

10.3 Prodávající přijme opatření k omezení dopadů, zachová relevantní důkazy zákonným a forenzně využitelným způsobem a poskytne součinnost při řešení incidentu a plnění oznamovacích povinností kupujícího.

10.4 Oznámení prodávajícího nenahrazuje oznámení, které je kupující povinen učinit příslušnému orgánu.

10.5 Pro oznamování KBU a KBI a pro související komunikaci se použijí kontaktní údaje osob pro bezpečnost uvedené v čl. I smlouvy.

11. Dokumentace a předání

11.1 Součástí plnění je předání konfigurace dodaného řešení v exportovatelné podobě, dokumentace k dodanému řešení a zaškolení v rozsahu, který kupujícímu umožní provozovat dodané řešení vlastními silami nebo prostřednictvím jiného dodavatele bez nedůvodné závislosti na prodávajícím.

11.2 Dokumentace zahrnuje zejména popis architektury a datových toků, dokumentaci bezpečnostních nastavení, postupy nasazení a obnovy a seznam programových komponent a jejich verzí; podrobný rozsah stanoví příloha č. 2 smlouvy.

12. Oprávnění užívat data a licence

12.1 Prodávající je oprávněn nakládat s daty kupujícího pouze v rozsahu nezbytném pro plnění smlouvy a nesmí k nim uplatnit zadržovací právo ani podmínit jejich vydání úhradou sporné pohledávky. Vlastnictví dat zůstává kupujícímu.

12.2 Prodávající zaručuje, že je oprávněn poskytnout licence k dodanému programovému vybavení v rozsahu přílohy č. 2 a 3 smlouvy. Licence a technická podpora výrobce se registrují na kupujícího a jejich užívání není vázáno na trvání smluvního vztahu s prodávajícím ani na využívání jeho služeb.

12.3 Prodávající předem oznámí licenční podmínky komponent třetích stran a otevřeného programového vybavení, které mohou omezit zamýšlené užití nebo bezpečné ukončení služby.

13. Sankce a nápravná opatření

13.1 Porušení povinností podle této přílohy se posuzuje podle jeho závažnosti, dopadu a opakování. Smluvní pokuty a další právní následky stanoví smlouva.

13.2 Prodávající odstraní příčinu porušení, provede nápravná opatření a poskytne kupujícímu důkazy o jejich účinnosti.

Příloha č. 2

Technická specifikace

k veřejné zakázce malého rozsahu na dodávky

1. NÁZEV VEŘEJNÉ ZAKÁZKY

Zvýšení zabezpečení webových aplikací

2. STRUČNÝ POPIS PŘEDMĚTU VEŘEJNÉ ZAKÁZKY

Předmětem plnění je dodávka, implementace a uvedení do provozu dvou nástrojů ochrany na aplikační vrstvě:

- nástroje pro ochranu veřejně přístupných webových aplikací (Web Application Firewall, dále jen „WAF“),
- nástroje pro ochranu elektronické pošty (Secure Email Gateway, dále jen „SEG“),

včetně licencí a technické podpory výrobce po dobu 5 let, implementačních služeb, integrace do stávající bezpečnostní infrastruktury zadavatele, zaškolení administrátorů a předání dokumentace.

Požadavek na integraci se stávajícími prvky zadavatele (kapitola 4.4) je požadavkem na kompatibilitu s prostředím zadavatele, nikoli požadavkem na konkrétní výrobek nabízeného řešení. Customizace, zásahy do zdrojového kódu ani vývoj funkcionality na míru nejsou předmětem plnění.

3. VÝCHOZÍ STAV

Zadavatel provozuje jednotnou bezpečnostní platformu jednoho výrobce: next-generation firewally na perimetru i na pracovištích, centrální správu politik, centrální sběr a korelaci provozních a bezpečnostních záznamů, správu koncových bodů se vzdáleným přístupem a ochranu koncových bodů. Virtualizační platformou je VMware.

Oblast	**Stav**
Ochrana webových aplikací	žádná ochrana na aplikační vrstvě (L7). Veřejně přístupné webové aplikace jsou chráněny pouze prostředky perimetrového firewallu (kontrola šifrovaného provozu, prevence průniku) a službou ochrany proti objemovým útokům na úrovni L3/L4 poskytovanou provozovatelem konektivity.
Provozní zkušenost	veřejně přístupné webové aplikace zadavatele byly v roce 2026 opakovaně přetěžovány automatizovaným provozem z velkého počtu zdrojových adres i z několika málo adres poskytovatelů hostingu a sítí pro doručování obsahu. Dostupné prostředky (blokace podle zemí, omezení provozu na úrovni L3/L4) dopadají stejně na útočníka i na legitimní uživatele a nejsou dlouhodobě použitelné.
Chráněné webové aplikace	portál pro zpřístupňování digitalizovaných archiválií, informační systém pro zveřejňování archiválií a společný server obrazových reprodukcí; dále úložiště pro sdílení souborů a katalog knihovny. Server obrazových reprodukcí generuje odchozí provoz v řádu desítek TB dat a milionů obrazových souborů, zpřístupňovaných po dlaždicích; i jediný automatizovaný klient tak generuje stovky požadavků za sekundu.
Ochrana elektronické pošty	filtrace pošty je zajištěna jako služba v rámci komunikační infrastruktury veřejné správy. Poštovní prostředí zadavatele je hybridní (cloudová poštovní služba Microsoft 365 / Exchange Online a lokální poštovní server).
Rozsah poštovního provozu	přibližně 200 poštovních schránek, přibližně 20 000 zpráv denně.
Umístění řešení	obě komponenty budou provozovány jako virtuální stroje na platformě VMware v prostředí zadavatele.

Podrobné údaje o uspořádání sítě, o konfiguraci bezpečnostních prvků a o bezpečnostních politikách jsou důvěrné a nejsou součástí zadávací dokumentace. Vybraný dodavatel se s nimi seznámí po uzavření smlouvy v rámci implementační analýzy, za podmínek stanovených přílohou Bezpečnostní opatření.

4. ROZSAH PLNĚNÍ

4.1 Ochrana webových aplikací (WAF)

Dodávka licence nástroje WAF ve formě virtuálního zařízení pro platformu VMware, včetně všech funkčních modulů potřebných ke splnění požadavků kapitoly 5.2 a včetně předplatného bezpečnostních aktualizací (signatury, reputační databáze, aktualizace detekčních modelů) a technické podpory výrobce na dobu 5 let od převzetí plnění.

4.2 Ochrana elektronické pošty (SEG)

Dodávka licence nástroje SEG ve formě virtuálního zařízení pro platformu VMware, včetně všech funkčních modulů potřebných ke splnění požadavků kapitoly 5.3 a včetně technické podpory výrobce na dobu 5 let od převzetí plnění, jejíž součástí je nárok na aktualizace programového vybavení. Předplatné detekčních služeb výrobce (antivirových signatur, reputačních a antispamových služeb, analýzy v izolovaném prostředí) zadavatel požaduje jen v rozsahu, v jakém je nabízené řešení potřebuje ke splnění požadavků kapitoly 5.3.

Licenční pokrytí a výkon musí odpovídat nejméně 240 poštovním schránkám a 24 000 zprávám denně, tj. rozsahu podle kapitoly 3 s rezervou 20 %.

4.3 Implementační služby

Implementační služby v rozsahu nejméně 16 člověkodnů zahrnující:

- implementační analýzu a cílový koncept nasazení, odsouhlasený zadavatelem před zahájením konfiguračních prací; koncept obsahuje návrh umístění obou komponent v síti, návrh politik, návrh integrace podle kapitoly 4.4, plán přepnutí provozu a postup návratu do předchozího stavu,
- instalaci a základní konfiguraci obou virtuálních zařízení,
- konfiguraci ochranných politik pro jednotlivé chráněné webové aplikace včetně úvodního učení a ladění tak, aby byl minimalizován počet planých poplachů,
- konfiguraci poštovní cesty a politik ochrany elektronické pošty v obou směrech,
- nastavení poštovní cesty tak, aby zařazení brány nezhoršilo vyhodnocování reputace odesílatele a kontrol SPF, DKIM a DMARC na straně cloudové poštovní služby zadavatele; součástí je konfigurace odpovídající funkce na straně této služby (v prostředí Microsoft 365 rozšířené filtrování pro konektory, tzv. Enhanced Filtering for Connectors) a ověření, že po přepnutí zůstává v hlavičkách zpráv zachován údaj o původním zdroji,
- úpravu politik stávajícího perimetrového firewallu v rozsahu nutném pro začlenění obou komponent,
- integraci podle kapitoly 4.4,
- testování podle kapitoly 4.6 a součinnost při ověřovacím provozu,
- zaškolení podle kapitoly 4.7 a předání dokumentace podle kapitoly 4.8.

Přepnutí produkčního provozu na dodané řešení se provádí v předem dohodnutém časovém okně, s připraveným postupem návratu do předchozího stavu a s účastí dodavatele.

4.4 Integrace do stávající bezpečnostní infrastruktury

Dodané řešení musí být začleněno do stávající bezpečnostní infrastruktury zadavatele. Zadavatel požaduje prokazatelné splnění těchto integračních vlastností:

- odesílání provozních a bezpečnostních záznamů obou komponent do centrálního systému sběru a korelace záznamů, který zadavatel provozuje, ve strukturované podobě, která umožňuje vyhledávání a tvorbu sestav nad jednotlivými poli záznamu (nikoli pouze jako nestrukturovaný text); rozsah odesílaných záznamů navrhne dodavatel v cílovém konceptu tak, aby nepřekročil kapacitu tohoto systému, jejíž rozšíření není předmětem plnění,
- automatizované předávání zdrojových adres, které nástroj WAF vyhodnotí jako škodlivé, stávajícímu perimetrovému firewallu k blokaci na perimetru,
- správu obou komponent prostřednictvím webového rozhraní a dokumentovaného programového rozhraní, které umožňuje zálohu a obnovu konfigurace a řízení změn,

- jednotné hlášení bezpečnostních událostí a možnost sestavit přehled o zablokovaném provozu za zvolené období jako podklad k dokumentaci bezpečnostních incidentů,
- ověřování administrátorů proti adresářové nebo identitní službě zadavatele s možností vícefaktorového ověření.

Stávající prvky zadavatele podle kapitoly 3 jsou produkty výrobce Fortinet: FortiGate, FortiManager, FortiAnalyzer, FortiClient EMS. Splní-li nabízené řešení integrační vlastnosti podle tohoto článku jiným rovnocenným způsobem, zadavatel je připustí; dodavatel v takovém případě v nabídce popíše, jak jsou jednotlivé vlastnosti zajištěny.

4.5 Součinnost při přechodu poštovního provozu

SEG doplňuje ochranu poštovní služby zadavatele místními kontrolami podle kapitoly 5.3. Antivirovou a antispamovou detekci s aktualizacemi zajišťuje u cloudových schránek stávající služba Microsoft 365 / Exchange Online. Dodavatel nastaví konektory tak, aby tato ochrana zůstala účinná; příchod zprávy přes SEG nesmí být důvodem k plošnému vynechání filtrace.

Dodavatel nasadí a ověří SEG v poštovním prostředí zpřístupněném zadavatelem, v cestě příchozích a odchozích zpráv. Řešení musí umožnit spolupráci s předřazenou SMTP filtrační bránou a směrování na určený navazující server. Konkrétní poštovní cestu, ověřování odesílatele a potřebné výjimky pro důvěryhodné mezilehlé servery popíše cílový koncept. Dodavatel nesmí zavést plošné výjimky pro obsahové kontroly celé poštovní cesty pouze kvůli přítomnosti předřazené brány.

Zrušení stávající služby CMS2 není součástí plnění ani podmínkou převzetí. Případné další využití CMS2 po přechodu na Exchange Online ověří zadavatel s jejím provozovatelem; dostupnost tohoto zapojení není podmínkou dokončení zakázky. Přepnutí provozu musí být schváleno zadavatelem a předcházejí mu testy doručování a aktivní antivirové a antispamové filtrace v použité poštovní cestě, se zaznamenáním výsledků a připraveným postupem návratu. Samotné nasazení SEG tyto testy nenahrazuje.

Vlastní migrace schránek ani pořízení či obnova licencí Microsoft 365 nejsou předmětem zakázky. Dodavatel poskytne součinnost při případné migraci nebo rozšíření ochrany Microsoft 365, uskuteční-li se v době implementace.

4.6 Testování a ověřovací provoz

- funkční testy podle testovacího scénáře zpracovaného dodavatelem a odsouhlaseného zadavatelem; scénář pokrývá požadavky kapitol 5.2 a 5.3,
- ověření, že dodané řešení nezpůsobuje planě blokované legitimní požadavky u chráněných webových aplikací a planě zadržené zprávy legitimní pošty; ladění politik podle výsledků,
- ověření, že po zařazení brány do poštovní cesty vyhodnocuje navazující poštovní platforma reputaci odesílatele a kontroly SPF, DKIM a DMARC vůči původnímu odesílateli, nikoli vůči bráně,
- ověření aktivní antivirové a antispamové filtrace v použité poštovní cestě pomocí bezpečných testovacích vzorků; protokol rozliší kontroly provedené SEG a navazující či předřazenou službou, včetně výsledků doručení, zadržení a uvolnění testovací zprávy,
- ověřovací provoz v délce nejméně 10 pracovních dnů, během kterého dodavatel reaguje na zjištění zadavatele a provádí ladění; teprve po jeho úspěšném ukončení se plnění považuje za dokončené.

4.7 Zaškolení

Zaškolení nejméně dvou administrátorů zadavatele v rozsahu nejméně jednoho školicího dne, v prostředí zadavatele a nad dodanou konfigurací. Obsahem je běžná správa, čtení a vyhodnocování záznamů, řešení planých poplachů, úprava politik, záloha a obnova konfigurace a postup při bezpečnostní události. Zadavatel je oprávněn pořídit ze zaškolení audiovizuální záznam pro vlastní vnitřní potřebu.

4.8 Dokumentace

Dodavatel předá v elektronické editovatelné podobě a v českém jazyce:

- provozní dokumentaci dodaného řešení: popis nasazené architektury, umístění komponent, tok provozu, seznam nastavených politik a jejich účel,

- konfigurační přílohu obsahující údaje závislé na prostředí, oddělenou od ostatního textu tak, aby ji zadavatel mohl při změně prostředí aktualizovat samostatně,
- postup zálohy a obnovy konfigurace obou komponent a exportovatelnou zálohu konfigurace k datu předání,
- postup návratu do předchozího stavu (vyřazení komponenty z cesty provozu) pro případ poruchy,
- protokoly z testů podle kapitoly 4.6.

Dokumentace nesmí obsahovat odkazy na dokumenty, které nejsou předány zadavateli, ani být podmíněna přístupem do systémů dodavatele.

5. TECHNICKÉ POŽADAVKY

Není-li uvedeno jinak, jde o požadavky minimální a závazné.

5.1 Společné požadavky

Požadavek	**Minimální úroveň**
Forma dodání	virtuální zařízení pro platformu VMware vSphere provozovanou zadavatelem, obě komponenty samostatně
Výpočetní prostředky	podpora provozu při nejméně 2 virtuálních procesorech na komponentu; dodavatel uvede doporučenou konfiguraci procesorů, paměti a diskového prostoru
Licencování	licence trvalá nebo předplacená nejméně na 5 let; po dobu 5 let od převzetí plnění zahrnuty aktualizace programového vybavení a technická podpora výrobce, u WAF také aktualizace detekčních databází podle kapitoly 4.1, a to bez dalších plateb zadavatele
Podpora výrobce	5 let od převzetí plnění, včetně nároku na aktualizace a nové verze produktu
Vysoká dostupnost	podpora provozu ve dvojici v režimu vysoké dostupnosti (licenční i funkční); zadavatel ji v tomto plnění nepořizuje, řešení ji však nesmí vylučovat
Správa	webové grafické rozhraní v češtině nebo angličtině, oddělené administrátorské role, záznam o úkonech administrátorů
Záznamy	odesílání záznamů protokolem syslog nebo rovnocenným, ve strukturované podobě; místní uchování nejméně 30 dnů
Zálohování konfigurace	export a import úplné konfigurace do souboru, možnost automatizovaného exportu
Časová synchronizace	NTP proti zdroji určenému zadavatelem
Ověření administrátorů	místní účty a současně ověření proti adresářové nebo identitní službě (LDAP, RADIUS nebo SAML) s podporou vícefaktorového ověření

5.2 Ochrana webových aplikací (WAF)

Požadavek	**Minimální úroveň**
Režim nasazení	reverzní proxy (inline) jako primární režim; podpora transparentního režimu
Šifrovaný provoz	ukončení a opětovné navázání TLS (offloading), TLS 1.2 a TLS 1.3, správa certifikátů, podpora více jmen serverů (SNI)
Propustnost	nejméně 100 Mbit/s pro nešifrovaný provoz HTTP a nejméně 50 Mbit/s pro šifrovaný provoz HTTPS (klíč RSA 2048 bitů) podle údajů výrobce. Rozhodující je odolnost vůči objemovým a aplikačním útokům z velkého počtu unikátních zdrojových IP adres, nikoli špičková propustnost
Počet chráněných aplikací	zadavatel předpokládá ochranu 3 až 6 webových aplikací provozovaných na několika serverech. Dodavatel v nabídce uvede, zda a jak je počet chráněných aplikací, serverů, doménových jmen nebo domén chráněných strojovým učením licenčně nebo kapacitně omezen
Ochrana proti útokům na aplikaci	detekce a blokace útoků podle OWASP Top 10 (vkládání SQL, skriptování napříč weby, padělání požadavku, vzdálené spuštění kódu, průchod adresářovou strukturou); pozitivní i negativní bezpečnostní model
Detekce neznámých hrozeb	behaviorální analýza nebo strojové učení pro odhalení dosud neznámých vzorů útoku
Virtuální záplatování	možnost blokovat pokus o zneužití konkrétní zranitelnosti chráněné aplikace bez zásahu do aplikace samotné
Ochrana proti útokům na dostupnost na aplikační vrstvě	detekce a zmírnění útoků typu HTTP flood a pomalých útoků (slowloris a obdobných); ochrana musí být účinná i tehdy, kdy není saturována kapacita linky a útok se projevuje vyčerpáním relací nebo výkonu aplikace

Požadavek	Minimální úroveň
Omezování míry požadavků	omezení počtu požadavků a počtu spojení z jedné zdrojové IP adresy a omezení počtu požadavků na chráněnou adresu URL; možnost nastavit odlišné limity pro vybrané rozsahy zdrojových adres a pro jednotlivé části aplikace
Řízení automatizovaného provozu (bot management)	rozlišení lidského a automatizovaného přístupu, katalog známých vyhledávacích a jiných legitimních robotů s možností jejich povolení, detekce nedeklarovaných a maskovaných robotů, detekce plošného vytěžování obsahu (scraping) u jednotlivého klienta, a to i při rozložení do mnoha relací
Reakce na detekci	stupňovaná reakce: sledování (pouze záznam), ověřovací výzva zajišťovaná samotným řešením (CAPTCHA nebo neviditelná výzva typu JavaScript), blokace a dočasná blokace zdroje na stanovenou dobu
Reputace zdrojů	průběžně aktualizovaná reputační databáze zdrojových adres (zejména botnety, anonymizační proxy, účastníci útoků na dostupnost a škodlivé roboty); blokace nebo omezení podle seznamů adres, rozsahů a podsítí, včetně seznamů pravidelně načítaných z externího zdroje určeného zadavatelem
Ochrana přihlašování	ochrana přihlašovacích formulářů proti útoku hrubou silou, včetně omezení opakovaných pokusů o přihlášení
Ochrana rozhraní API	kontrola konformity protokolů HTTP a HTTPS, ochrana rozhraní REST, kontrola obsahu ve formátech JSON a XML
Funkce doručování aplikací	vyvažování zátěže na aplikační vrstvě, přepisování adres URL, ochrana souborů cookie, sledování relací
Vyloučení planých poplachů	možnost výjimek na úrovni pravidla, adresy URL, parametru a zdroje; režim pouze sledování pro zavádění nových pravidel
Sestavy	přehled zablokovaného provozu podle zdroje, země, chráněné aplikace a typu útoku za zvolené období, s možností exportu

5.3 Ochrana elektronické pošty (SEG)

Požadavek	Minimální úroveň
Režim nasazení	SMTP relay (gateway) v cestě zpráv v obou směrech; podpora nasazení před i za hybridním poštovním prostředím
Zachování údajů o původním odesílateli	při nasazení před cloudovou poštovní službou musí řešení zachovat v hlavičkách zpráv údaje o původním zdroji tak, aby navazující platforma mohla vyhodnotit reputaci odesílatele a kontroly SPF, DKIM a DMARC vůči odesílateli, nikoli vůči bráně
Kapacita	nejméně 240 poštovních schránek a nejméně 24 000 zpráv denně (rozsah podle kapitoly 3 s rezervou 20 %)
Kontrola příloh	blokace nebo zadržení příloh podle typu souboru; kontrola obsahu archivů včetně vnořených, s nastavitelnou nejvyšší hloubkou vnoření; zadržení archivů a dokumentů chráněných heslem a archivů, které nelze rozbalit
Antispamová ochrana	šedý seznam (greylisting), hodnocení reputace odesílajících serverů podle jejich dosavadního chování vůči řešení, statistický filtr učený na poště zadavatele, heuristická a obsahová pravidla (zakázaná slova, slovníky), seznamy blokovaných a povolených odesílatelů na úrovni systému, domény a uživatele; podpora veřejných seznamů DNSBL a SURBL, o jejichž použití rozhodne zadavatel
Ochrana proti podvržení odesílatele	vyhodnocení SPF, DKIM, DMARC včetně politiky DMARC a ARC u příchozí pošty; kontrola nesouladu odesílatele v obálce a v hlavičce zprávy; detekce doménových jmen napodobujících domény zadavatele
Podepisování odchozí pošty	podepisování DKIM; součinnost při nastavení záznamů SPF, DKIM a DMARC v systému doménových jmen zadavatele
Karanténa	centrální karanténa spravovaná administrátorem a současně uživatelská karanténa s pravidelným přehledem zadržených zpráv a s možností uvolnění zprávy uživatelem
Šifrování přenosu	vynucení TLS pro definované protistrany, podpora MTA-STS nebo rovnocenného mechanismu
Ochrana odchozí pošty	uplatnění pravidel pro přílohy a obsah i na odchozí zprávy; omezení míry odesílání podle odesílatele pro odhalení kompromitované schránky
Sestavy a upozornění	přehledy zpracovaných, zadržených a zablokovaných zpráv, sledování jednotlivé zprávy v cestě, upozorňování na definované události
Auditní záznamy	záznam o úkonech administrátorů a o nakládání se zadrženými zprávami

6. BEZPEČNOSTNÍ POŽADAVKY

Zadavatel je poskytovatelem regulované služby v režimu nižších povinností podle zákona č. 264/2025 Sb., o kybernetické bezpečnosti, a vyhlášky č. 410/2025 Sb. Následující požadavky se vztahují k předmětu plnění; povinnosti dodavatele upravuje příloha Bezpečnostní opatření pro smluvní vztahy, která je nedílnou součástí smlouvy.

1. Dodané řešení nesmí obsahovat technické ani programové prostředky, na které dopadá platné varování Národního úřadu pro kybernetickou a informační bezpečnost.

2. Vzdálená správa předmětu plnění ani přístup k datům zadavatele nesmějí být vykonávány z území, na které dopadá platné varování Národního úřadu pro kybernetickou a informační bezpečnost; na takové území nesmějí být předávána ani na něm ukládána data zadavatele.

3. Povinné funkce podle kapitol 5.2 a 5.3 nesmějí být závislé na službě výrobce nebo jiné třetí osoby, které se ke zpracování předává obsah elektronické pošty, obsah požadavků na chráněné webové aplikace nebo záznamy o nich. Tím není dotčeno doručování a filtrování pošty ve stávajících službách zadavatele (Microsoft 365 a CMS2), komunikace dodaného řešení s výrobcem za účelem ověření licence a stahování aktualizací ani dotazy na reputaci adres a doménových jmen. Dodavatel v nabídce uvede externí služby, se kterými dodané řešení komunikuje, jejich účel a předávané údaje. Funkce licenčního balíčku, které by takové předávání vyžadovaly a nejsou potřebné ke splnění požadavků, zůstanou vypnuté; jejich přítomnost v balíčku sama o sobě není důvodem nepřijatelnosti nabídky.

4. Vzdálený přístup dodavatele do prostředí zadavatele se uskutečňuje výhradně přístupovým kanálem určeným zadavatelem, s vícefaktorovým ověřením, jmenovitě pro předem oznámené osoby a po dobu nezbytnou k provedení dohodnuté činnosti. Sdílené účty jsou nepřípustné.

5. Informace o uspořádání sítě zadavatele, o konfiguraci bezpečnostních prvků, o bezpečnostních politikách a o zjištěných zranitelnostech jsou důvěrné; dodavatel je nesmí ukládat ani zpracovávat mimo prostředí zadavatele bez jeho předchozího písemného souhlasu.

6. Změny konfigurace v produkčním prostředí provádí dodavatel po odsouhlasení zadavatelem, v dohodnutém časovém okně a s předem připraveným postupem návratu do předchozího stavu.

7. Dodané řešení musí být po celou dobu podpory udržováno ve verzi, ke které výrobce vydává bezpečnostní aktualizace. Dodavatel informuje zadavatele o zveřejněných zranitelnostech dodaného řešení a o dostupných opravách.

8. Předmětem plnění není zpracování osobních údajů pro zadavatele. Získá-li dodavatel při implementaci nebo při řešení vad přístup k obsahu elektronické pošty, uzavřou strany před zahájením takové činnosti ujednání o zpracování osobních údajů podle článku 28 nařízení (EU) 2016/679.

9. Součástí plnění je předání konfigurace, dokumentace bezpečnostních nastavení a zaškolení v rozsahu, který zadavateli umožní provozovat dodané řešení vlastními silami nebo prostřednictvím jiného dodavatele.

10. Bezpečnostní požadavky se vztahují i na poddodavatele dodavatele.

7. ROZDĚLENÍ BEZPEČNOSTNÍCH ODPOVĚDNOSTÍ

Dodané řešení provozuje po převzetí zadavatel. Rozdělení odpovědností za jednotlivé oblasti je následující:

Oblast	**Zadavatel**	**Dodavatel**
Uživatelské účty a oprávnění v dodaných systémech	zřizuje a spravuje	navrhne rolový model, předá při zaškolení
Privilegované a vzdálené přístupy dodavatele	schvaluje, zřizuje a odebírá	používá jen schválený kanál, jmenovité účty, vícefaktorové ověření
Bezpečnostní konfigurace WAF a SEG	schvaluje, provozuje po předání	provede výchozí konfiguraci a zdokumentuje ji
Kryptografické klíče a certifikáty	vydává a drží	používá podle pokynů, nekopíruje mimo prostředí zadavatele
Zálohování a obnova virtuálních strojů	zajišťuje	předá postup obnovy a exportovatelnou konfiguraci

Oblast	Zadavatel	Dodavatel
Bezpečnostní a provozní záznamy dodaných systémů	sbírá a vyhodnocuje	nastaví jejich odesílání; záznamy o vlastní činnosti uchovává 12 měsíců
Dohled a vyhodnocování záznamů	zajišťuje	poskytuje součinnost při analýze
Řízení zranitelností dodaného řešení	přijímá opatření	sleduje, informuje, dodává aktualizace
Zvládání kybernetických bezpečnostních událostí a incidentů	hlásí příslušnému orgánu	oznamuje do 24 hodin, poskytuje součinnost
Export dat a konfigurací	vyžaduje	zajišťuje

8. TERMÍNY A AKCEPTAČNÍ ŘÍZENÍ

Krok	Termín
Implementační analýza a cílový koncept	do 14 kalendářních dnů od nabytí účinnosti smlouvy
Dodání licencí a instalace obou komponent	do 21 kalendářních dnů od nabytí účinnosti smlouvy
Konfigurace, integrace a testy podle kapitol 4.3, 4.4 a 4.6	do 30 kalendářních dnů od nabytí účinnosti smlouvy
Zahájení ověřovacího provozu	do 30 kalendářních dnů od nabytí účinnosti smlouvy
Zaškolení a předání dokumentace	nejpozději při předání plnění
Dokončení a předání celého plnění	do 8 týdnů od účinnosti smlouvy, nejpozději do 30. 11. 2026

Dílčí termíny jsou nejzazší a nezakládají prodloužení konečného termínu. Dodavatel zahájí ověřovací provoz nejpozději 30 kalendářních dnů od nabytí účinnosti smlouvy. Po nejméně 10 pracovních dnech úspěšného ověřovacího provozu předloží celé plnění k akceptaci. Harmonogram zahrnuje vyjádření zadavatele, odstranění případných vad a opakované předání. Zadavatel se vyjádří do 5 pracovních dnů; převzetí se potvrzuje podpisem akceptačního protokolu, mlčení není převzetím. Vady bránící užívání dodavatel odstraní do 5 pracovních dnů a plnění předá znovu, aniž se tím prodlužuje konečný termín. Převzetí s ostatními výhradami zakládá právo fakturovat.

9. SOUČINNOST ZADAVATELE

- zpřístupnění virtualizační platformu a přidělení výpočetních prostředků podle doporučené konfigurace dodavatele,
- zřízení vzdáleného přístup podle kapitoly 6 bodu 4 (účty pro konkrétní osoby dodavatele),
- poskytnutí údajů o prostředí nezbytné pro implementační analýzu, za podmínek přílohy Bezpečnostní opatření,
- vydání potřebných certifikátů a provedení změn v systému doménových jmen,
- odsouhlasení cílového konceptu, testovacího scénáře a časového okna pro změny provozu.

Příloha č. 3

Soupis položek dodávky

Seznam všech nabízených komponent včetně jejich počtu přesným označením nabízených licencí, předplatných a podpory, včetně názvů a katalogových kódů výrobce.

Výrobce a název komponenty	**Označení od výrobce (Product Number)**	**Počet**
Fortinet - Web Application Firewall - virtual appliance for all supported platforms. Supports up to 2 x vCPU core	FWB-VM02	1
Fortinet Standard Bundle (FortiCare Premium plus AV, FortiWeb Security Service, and IP Reputation)	FC-10-VVM02-936-02-60	1
Fortinet Subscription license for FortiMail-VM (2 CPU) with Base Bundle included.	FC2-10-FEVVS-646-02-60	1

Seznam členů realizačního týmu a jejich role:

- [redacted] NSE4, NSE7 – Solution Architekt
- [redacted] – NSE7 – specialita FortiWEB
- [redacted] NSE4, NSE6 – specialista FortiMail
- [redacted] projektový manažer

Odkazy na technické dokumentace výrobce nebo veřejně přístupný odkaz na technickou specifikaci:

- Web Application Firewall:
  - https://www.fortinet.com/products/web-application-firewall/fortiweb
  - https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiWeb.pdf
- FortiMail:
  - https://www.fortinet.com/products/email-security
  - https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiMail.pdf
- FortiCare Fortine support:
  - https://www.fortinet.com/support
  - https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/sb-forticare-services.pdf

Příloha č. 4

Čestné prohlášení

k veřejné zakázce malého rozsahu s názvem

„Zvýšení zabezpečení webových aplikací“

Identifikační údaje kupujícího	
Název:	Česká republika – Státní oblastní archiv v Plzni
IČO:	70979090
Sídlo:	Sedláčkova 44, 306 12 Plzeň
Jednající:	doc. PhDr. Karel Řeháček, Ph.D., ředitel
Identifikační údaje prodávajícího	
Obchodní firma/název:	BIT SERVIS spol. s r.o.
IČO:	45793972
Sídlo:	Praha 4, Libušská 144/252, PSČ 14200
Osoba oprávněná jednat za prodávajícího:	Ondřej Koutský, jednatel

1) Za prodávajícího **tímto čestně prohlašuji**, že na smlouvě společnosti, kterou zastupuji, není/nebude ruské zapojení do smluv překračujících limity stanovené v článku 5k nařízení Rady (EU) č. 833/2014 ze dne 31. července 2014, o omezujících opatřeních vzhledem k činnostem Ruska destabilizujícím situaci na Ukrajině, ve znění nařízení Rady (EU) č. 2022/576 ze dne 8. dubna 2022, v platném znění.

Zejména prohlašuji, že:

(a) dodavatel, kterého zastupuji (a žádná ze společností, které jsou členy našeho konsorcia), není ruským státním příslušníkem nebo fyzickou nebo právnickou osobou, subjektem nebo orgánem usazeným v Rusku;
(b) dodavatel, kterého zastupuji (a žádná ze společností, které jsou členy našeho konsorcia), není právnickou osobou, subjektem nebo orgánem, jejichž vlastnická práva jsou přímo nebo nepřímo vlastněna z více než 50 % subjektem uvedeným v písmenu a) tohoto odstavce;
c) ani já, ani společnost, kterou zastupuji, nejednáme jménem nebo na pokyn subjektu uvedeného v písmenech a) nebo b) výše, včetně poddodavatelů, dodavatelů nebo subjektů, jejichž způsobilost je využívána ve smyslu směrnic o zadávání veřejných zakázek, pokud představují více než 10 % hodnoty zakázky.

2) Prodávající, jakož i osoba/osoby jednající jeho jménem **tímto čestně prohlašují**, že nejsou sankcionovanou osobou ve smyslu nařízení Rady (EU) č. 269/2014 ze dne 17. března 2014, o omezujících opatřeních vzhledem k činnostem narušujícím nebo ohrožujícím územní celistvost, svrchovanost a nezávislost Ukrajiny, v platném znění, nařízení Rady (EU) č. 208/2014 ze dne 5. března 2014, o omezujících opatřeních vůči některým osobám, subjektům a orgánům vzhledem k situaci na Ukrajině, v platném znění, nařízení Rady (ES) č. 765/2006 ze dne 18. května 2006, o omezujících opatřeních vzhledem k situaci v Bělorusku a k zapojení Běloruska do ruské agrese proti Ukrajině, v platném znění, včetně aktuálních příloh těchto všech nařízení, tj. **nenachází se na tzv. sankčních seznamech**.

Prodávající, jakož i osoba/osoby jednající jeho jménem **tímto čestně prohlašují**, že se zavazuje informovat kupujícího o změnách spočívajících ve skutečnostech uvedených v bodě 1) a 2) výše.