Kupní smlouva

(dále jen „smlouva“)

dle § 2079 a násl. zákona č. 89/2012 Sb., občanského zákoníku,
ve znění pozdějších předpisů (dále jen „**občanský zákoník**“)

1. Smluvní strany

1.1.	**Kupující:**	**Město Krnov**
	se sídlem:	Hlavní náměstí 96/1 Pod Bezručovým vrchem, 794 01 Krnov 1
	zastoupen:	Mgr. Tomášem Hradilem, starostou
	Identifikační číslo:	00296139
	DIČ:	CZ00296139
	(dále jen jako „**kupující**“)	

1.2.	**Prodávající:**	**awin IT, s.r.o.**
	se sídlem:	Nad Šutkou 540/14, 182 00 Praha 8
	zastoupen:	Jindřichem Rosičkou, jednatelem
	zástupce ve věcech technických:	René Kmoch
	IČ:	03173631
	Bankovní spojení:	225668183/0600
	Telefon:	+420 778 058 077
	E-mail:	info@awinit.cz
	(dále jen jako „**prodávající**“)	

Obě smluvní strany po vzájemném projednání a shodě uzavírají tuto smlouvu:

2. Předmět smlouvy

2.1. Účelem této smlouvy je dodávka zařízení včetně jeho implementace a napojení na ostatní infrastrukturu kupujícího (včetně současně budované infrastruktury) a následné předání funkčního kompletu kupujícímu, zaškolení administrátorů, uživatelů, rozvoje a podpory. Zařízení je určené pro kupujícího (Město Krnov) a pro jeho organizace.

2.2. Podkladem pro uzavření této smlouvy je nabídka prodávajícího, podaná v zadávacím řízení nazvaném **„V 00855 – Krnov – ochrana sítě před kybernetickými hrozbami“, část 2** (dále jen „Veřejná zakázka“), zadávaném přiměřeně dle Metodického pokynu pro oblast zadávání zakázek pro programové období 2021 – 2027 vydaného Ministerstvem pro místní rozvoj (dále jen „Pravidla“) a dle § 56 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění.

2.3. Touto smlouvou se prodávající zavazuje dodat za podmínek v ní sjednaných kupujícímu zboží, uvedené v článku 3. této smlouvy a převést na něj vlastnické právo k tomuto zboží.

2.4. Kupující se zavazuje zboží převzít a zaplatit za něj sjednanou kupní cenu způsobem a v termínu stanoveném touto smlouvou.

2.5. Předmět plnění bude spolufinancován z dotačního projektu **„Krnov – ochrana sítě před kybernetickými hrozbami“, reg. č. CZ.31.2.0/0.0/0.0/23_093/0009763**, financovaného z Národního plánu obnovy (dále jen „Projekty“).

3. Předmět koupě

3.1. Předmětem smlouvy je **pořízení a implementace NGFW**, jehož specifikace včetně technických parametrů je uvedena v příloze č. 1 této smlouvy (dále jen „zboží“).

3.2. Součástí předmětu koupě jsou i veškeré doklady požadované právními předpisy k používání předmětu koupě - zboží. Prodávající prohlašuje, že předmět koupě splňuje veškeré podmínky stanovené právními předpisy k jeho používání, a že kupujícímu předá veškeré doklady potřebné k provozování předmětu koupě, za což kupujícímu ručí.

3.3. Předmětem koupě dle této smlouvy je dále:

- doprava do místa plnění,
- implementace, tj. veškeré nezbytné práce jejichž smyslem je zprovoznění včetně zapojení do stávajícího prostředí kupujícího tak, aby je kupující mohl užívat obvyklým způsobem (dále jen „implementace“),
- předání průvodní dokumentace,
- zaškolení kupujícího,
- testovací provoz,
- nezbytná technická podpora po dobu udržitelnosti Projektu, která činí 5 let od data předání do provozu. Technická podpora zahrnuje zejména aktualizace SW, maintenance, legislativní upgrade a update (dále jen „technická podpora“). Podrobné podmínky poskytování technické podpory jsou uvedeny v příloze č. 2 této smlouvy.

4. Kupní cena a platební podmínky

4.1. Celková kupní cena činí:

2 464 206 Kč bez DPH

517 483,26 Kč DPH

2 981 689,26 Kč vč. DPH

4.2. Cena bez DPH podle čl. 4.1. této smlouvy je stanovena dle technické specifikace (Příloha č. 1 této smlouvy) jako cena nejvýše přípustná a konečná a zahrnuje celý předmět plnění dle této smlouvy (s výjimkou ceny za poskytování technické podpory, která je upravena v čl. 4.5. níže).

4.3. Sjednaná cena celkem může být změněna pouze v případě změny zákona č. 235/2004 Sb., o DPH, týkající se sazby DPH a v souvislosti s ustanoveními § 222 zákona č. 134/2016 Sb., o zadávání veřejných zakázek.

4.4. Kupující se zavazuje zaplatit kupní cenu na základě faktur, vystavených prodávajícím a doručených kupujícímu dle níže uvedeného mechanismu:

- Prodávající vystaví zálohovou fakturu na 70 % z kupní ceny dodaného zboží po oboustranném podpisu zápisu o dodání zboží.
- Prodávající vystaví fakturu na 30 % z celkové kupní ceny po oboustranném podpisu předávacího protokolu (tj. po předání a převzetí zboží do plného provozu).

4.5. Cena za technickou podporu po předání zboží do provozu je stanovena dohodnou smluvních strany na:

14 000 Kč bez DPH za 1 měsíc

2 940 Kč DPH

16 940 vč. DPH za 1 měsíc

4.6. Úhrada ceny za technickou podporu bude probíhat na základě měsíčně vystavované faktury. Datum uskutečnitelného zdanitelného plnění je sjednáno na poslední kalendářní den v měsíci.

4.7. Faktury musí splňovat náležitosti daňového dokladu podle § 28 zákona č. 235/2004 Sb., o DPH, bude obsahovat cenový rozpad dle jednotlivých položek dle přílohy č. 1 této smlouvy a bude obsahovat číslo a název dotačního projektu (konkrétně bude uveden text ve znění: *Projekt **„Krnov – ochrana sítě před***

kybernetickými hrozbami", reg. č. CZ.31.2.0/0.0/0.0/23_093/0009763*, je spolufinancován z Národního plánu obnovy*) a bude zaslána prodávajícím na adresu kupujícího. **Splatnost faktury činí 30 kalendářních dní.**

4.8. Kupující bude oprávněn před uplynutím lhůty splatnosti vrátit prodávajícímu bez zaplacení fakturu, která nebude obsahovat některou náležitost uvedenou v této smlouvě, případně bude mít jiné závady v obsahu nebo bude uvedeno bankovní spojení a číslo účtu prodávajícího v rozporu s touto smlouvou anebo tyto náležitosti budou uvedeny chybně. U vrácené faktury musí kupující vyznačit důvod vrácení. Prodávající je povinen podle povahy nesprávnosti fakturu opravit nebo nově vyhotovit. Kupujícímu vrácením faktury přestává běžet původní lhůta splatnosti. Celá lhůta splatnosti běží znovu ode dne doručení opravené nebo nově vyhotovené faktury kupujícímu.

4.9. Platby budou zásadně probíhat bezhotovostní formou na bankovní účet prodávajícího uvedený ve smlouvě. Změnu bankovního spojení a čísla účtu prodávajícího bude možno provést pouze písemným dodatkem k této smlouvě nebo písemným sdělením prokazatelně doručeným kupujícímu, nejpozději spolu s příslušnou fakturou.

4.10. Faktura se považuje za včas uhrazenou, pokud je fakturovaná částka odepsána z účtu kupujícího.

5. Místo a doba plnění a dodací podmínky

5.1. Místem plnění je sídlo zadavatele.

5.2. Prodávající je povinen dodat veškeré zboží **nejpozději do 75 dní od účinnosti této smlouvy**. Kupující umožňuje postupné dodání zboží po částech.

5.3. Dodávka se považuje podle této smlouvy za dodanou, pokud bylo:

- zboží řádně dodáno včetně příslušné dokumentace (k instalaci, nastavení, zabezpečení jednotlivých komponent a včetně návrhu plánu obnovy).
- provedena instalace, implementace (případné podrobné specifické podmínky implementace jsou uvedeny v příloze č. 1 smlouvy) a úspěšně vyzkoušena funkčnost,
  - činnost u níž se nepředpokládá žádný výpadek služeb lze provádět v pracovní době MÚ
  - činnost u které se obě strany shodnou že předpokládaný výpadek bude kratší než 10 min lze provádět mimo úřední hodiny.
  - činnosti s výpadkem delší se mohou provádět pouze mimo pracovní dobu MÚ. Termín odstávky musí být znám alespoň týden předem
  - termín školení uživatelů určený předem.
  - školení OIT může probíhat v průběhu instalace.
- součástí instalace bude následný testovací provoz provedený bez zbytečného odkladu v délce nutné pro ověření funkčnosti dodaného HW a SW. Náplň testovacího provozu bude následující:
  - zahoření a ověření funkčnosti HW zařízení
  - ověření vzájemné spolupráce jednotlivých HW zařízení
  - ověření napojení na LAN síť zadavatele
  - provedení zátěžových testů
  - ověření chování systému při výpadku některého ze zařízení (ověření vysoké dostupnosti)
  - ověření chování systému při výpadku el. energie

5.4. Po dodání zboží v částech **2 a 3 zakázky** proběhne **audit kybernetické bezpečnosti**.

5.5. V rámci auditu kybernetické bezpečnosti dojde k prověření funkčnost technických opatření a celkové bezpečnosti dodávky pomocí jejího otestování. Otestování provede 3. osoba zvolená kupujícím, a to nejpozději do 14 dní od dodání zboží v částech 2 a 3 této veřejné zakázky, přičemž toto otestování bude trvat maximálně 60 dní. V návaznosti na dokončení auditu kybernetické bezpečnosti prodávající napraví nalezené chyby bránící užívání dle účelu smlouvy, a to nejpozději do 14 dní od okamžiku, kdy obdrží výsledek auditu kybernetické bezpečnosti.

5.6. Po splnění dodávky zboží bude vyhotoven **zápis o předání a převzetí zboží**, který bude obsahovat níže uvedené náležitosti:
- název a sídlo prodávajícího a kupujícího,
- označení dodaného zboží včetně výrobního čísla,
- datum dodání,
- číslo a název dotačního projektu (konkrétně bude uveden text ve znění: *Projekt **„Krnov – ochrana sítě před kybernetickými hrozbami“, reg. č. CZ.31.2.0/0.0/0.0/23_093/0009763** je spolufinancován z Národního plánu obnovy*).

5.7. Zápis o předání a převzetí zboží podepíší oprávnění zástupci obou smluvních stran, přičemž podpisem zápisu o předání a převzetí dochází k převzetí a předání zboží a ke splnění předmětu koupě.

6. Odpovědnost za vady, záruka za jakost, servis

6.1. Prodávající nese odpovědnost za to, že zboží dodané a předané podle této smlouvy je ke dni dodání plně funkční a splňuje technické parametry uvedené této smlouvě. Prodávající přejímá níže uvedenou záruku za jakost zboží dodaného podle této smlouvy. Záruční doba počíná běžet dnem oboustranného podpisu zápisu o předání a převzetí zboží. **Záruční doba pro jednotlivé položky v souladu s přílohou č. 1 této smlouvy činí 60 měsíců** ode dne předání a převzetí zboží.

6.2. Záruka se nevztahuje na spotřební materiál a na vady způsobené zaviněným jednáním kupujícího anebo způsobené vyšší mocí.

6.3. Kupující se zavazuje respektovat pokyny prodávajícího v oblasti údržby a používání správných pracovních postupů.

6.4. Technická podpora a servis budou poskytovány minimálně po celou dobu udržitelnosti projektu (tj. min. 60 měsíců ode dne předání do provozu).

6.5. Technická podpora a servis budou realizovány v sídle kupujícího. Výjimku tvoří činnosti realizovatelné vzdáleným připojením.

6.6. V případě nahlášení závady prodávajícímu bude oprava provedena vzdáleně či na místě nejpozději následující pracovní den od jejího nahlášení. V případě nemožnosti opravy následující pracovní den nabídne prodávající kupujícímu alternativu (tj. náhradní řešení) na dobu trvání opravy. V případě záruční opravy (tj. pokud se nejedná o vadu způsobenou zaviněným jednáním kupujícího anebo způsobenou vyšší mocí), není kupující povinen hradit náklady na cestovné servisních techniků ke kupujícímu a zpět, tyto náklady nese prodávající.

6.7. Nahlášení závady bude provedeno prostřednictvím e-mailu zaslaného na e-mailovou adresu it@awinit.cz, telefonicky na tel. číslo +420 778 058 077, prostřednictvím elektronické oznamovací služby (tzv. HelpDesku) nebo prostřednictvím vzdáleného připojení na PC uživatele / server.

6.8. Telefonická, e-mailová podpora a podpora prostřednictvím vzdáleného připojení bude k dispozici minimálně v pracovních dnech od 8 do 16 hod.

6.9. Služba HelpDesk umožní příjem požadavku na servisní zásah v českém jazyce prostřednictvím webového rozhraní v režimu 7x24 hod (s výjimkou předem nahlášených servisních zásahů při správě systému HelpDesk).

6.10. Prodávající se v záruční době zavazuje zajistit dostupnost náhradních dílů a spotřebního materiálu.

6.11. Veškeré záruční a servisní podmínky, uvedené v tomto článku 6. smlouvy, platí pouze tehdy, **pokud není v rámci technické specifikace v příloze č. 1 této smlouvy pro konkrétní produkty uvedeno jinak**. (Resp. odlišná úprava záručních a servisních podmínek v příloze č. 1 této smlouvy má před tímto čl. 6 smlouvy přednost.)

6.12. Podrobné podmínky poskytování technické podpory jsou upraveny v příloze č. 2 této smlouvy.

7. Smluvní pokuta a úrok z prodlení

7.1. Smluvními stranami bylo ujednáno, že pokud bude kupující v prodlení s úhradou ceny plnění ujednané podle této smlouvy, je kupující povinen zaplatit úrok z prodlení ve výši 0,05 % z dlužné částky za každý, byť i započatý kalendářní den prodlení.

7.2. Ocitne-li se prodávající v prodlení s plněním podle této smlouvy dle čl. 5.2, či 5.5., je povinen zaplatit kupujícímu smluvní pokutu ve výši 0,05 % z kupní ceny, a to za každý, byť i započatý kalendářní den prodlení se splněním dodávky.

7.3. Ocitne-li se prodávající v prodlení s plněním dle čl. 6.6. této smlouvy, je povinen zaplatit kupujícímu smluvní pokutu ve výši 500,- Kč za každý započatý den prodlení s dokončením servisní opravy dle čl. 6.6.

7.4. Uplatněním nároku na smluvní pokutu dle této smlouvy není dotčen nárok na náhradu škody.

7.5. Smluvní pokuta je splatná ve lhůtě 30 dnů od doručení jejího vyúčtování povinné smluvní straně z této smluvní pokuty.

8. Doba trvání smlouvy, ukončení smlouvy

8.1. Tato smlouva se uzavírá na dobu určitou, nejdéle do doby splnění závazku dle této smlouvy (tj. do okamžiku ukončení poskytování nezbytné technické podpory, resp. do doby uplynutí 5 let od data předání zboží do provozu).

8.2. Od této smlouvy může smluvní strana dotčená porušením povinnosti jednostranně odstoupit pro podstatné porušení této smlouvy, přičemž za podstatné porušení této smlouvy se zejména považuje:

a) na straně kupujícího – nezaplacení kupní ceny podle této smlouvy ve lhůtě delší 14 dní po dni splatnosti příslušné faktury,

b) na straně prodávajícího – prodlení s dodáním zboží o více než 14 dní po termínu dodání dle čl. 5.2. či dodání nefunkčního zboží, nesplňujícího požadavky čl. 3 této smlouvy, marné uplynutí sjednané lhůty pro vyřízení záruční opravy dle čl. 6.6. či prodlení s opravou chyb bránících užívání zboží dle účelu smlouvy, nalezených v rámci auditu kybernetické bezpečnosti, a to o více než 14 dní po termínu dle čl. 5.5. této smlouvy.

8.3. Smluvní strana porušením povinnosti dotčená je povinna odstoupení od smlouvy písemně oznámit druhé smluvní straně.

9. Ostatní ujednání

9.1. Smluvní strany se dohodly, že vlastnické právo k dodanému předmětu smlouvy nabývá kupující okamžikem převzetí zboží od prodávajícího.

9.2. Nebezpečí škody na zboží přechází z prodávajícího na kupujícího okamžikem převzetí zboží od prodávajícího či okamžikem, kdy kupujícímu bylo umožněno zboží převzít a ten jej nepřevzal.

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

9.4. Smluvními stranami bylo ujednáno, že veškeré informace, jež si navzájem poskytnou, jsou označeny jako důvěrné a žádná ze smluvních stran není oprávněna je poskytnout třetí osobě ani použít v rozporu s jejich účelem pro své potřeby.

9.5. Prodávající nesmí bez předchozího souhlasu kupujícího postoupit svá práva a povinnosti plynoucí ze smlouvy třetí osobě.

9.6. Kupující se zavazuje umožnit přístup určeným pracovníkům prodávajícího do prostoru svého objektu za účelem splnění této smlouvy (předání a převzetí zboží, servis a technická podpora).

9.7. Právní vztahy touto smlouvou neupravené, jakož i právní poměry z ní vznikající a vyplývající, se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanského zákoníku a dalšími právními předpisy České republiky.

9.8. Ujednává se, že případné spory vzniklé z této smlouvy budou účastníci řešit především vzájemnou dohodou. Pro řízení o případných sporných nárocích se ujednává příslušnost soudů. Rozhodným právem je právo České republiky.

9.9. Za písemnou formu výzvy nebo oznámení se pro účely této smlouvy pokládají oznámení učiněná elektronickou poštou na dohodnuté elektronické adresy.

9.10. Prodávající je povinen zajistit, že veškeré vlastnosti předmětu smlouvy, včetně jeho update, legislativních update, upgrade a legislativních upgrade budou po celou dobu účinnosti této smlouvy odpovídat obecně platným právním předpisům ČR.

9.11. Prodávající prohlašuje, že bude mít po celou dobu plnění předmětu smlouvy uzavřenu pojistnou smlouvu krytí odpovědnost za škodu způsobenou provozní činností s limitem pojistného plnění minimální výši kupní ceny zboží dle čl. 4.1., kterou se zavazuje kdykoliv na vyžádání předložit k nahlédnutí kupujícímu.

10. Závěrečná ustanovení

10.1. Prodávající je povinen umožnit všem subjektům oprávněným k výkonu kontroly projektu, z jehož prostředků je dodávka hrazena, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu danou právními předpisy ČR k jejich archivaci (zákon č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů a zákon č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů).

10.2. Prodávající je povinen uchovávat veškerou dokumentaci související s realizací plnění dle Smlouvy včetně účetních dokladů po dobu deseti let od finančního ukončení projektu s názvem **„Krnov – ochrana sítě před kybernetickými hrozbami“, reg. č. CZ.31.2.0/0.0/0.0/23_093/0009763**, minimálně však do konce roku 2037. Pokud je v českých právních předpisech stanovena lhůta delší, musí ji poskytovatel použít.

10.3. Prodávající je povinen uvádět povinné prvky publicity podle podmínek strukturálních fondů EU na všech tištěných dokumentech vytvořených v souvislosti s předmětem koupě (nevztahuje se na interní účetní dokumentaci apod.). Tyto povinné prvky publicity sdělí a poskytne prodávajícímu na vyžádání kupující.

10.4. Prodávající je povinen při kontrole poskytnout na vyžádání kontrolnímu orgánu daňovou evidenci v plném rozsahu. **Prodávající je podle ustanovení § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů (zákon o finanční kontrole), ve znění pozdějších předpisů, osobou povinou spolupůsobit při výkonu finanční kontroly.**

10.5. Prodávající se zavazuje umožnit osobám oprávněným k výkonu kontroly projektu, z něhož je veřejná zakázka hrazena, provést kontrolu dokladů souvisejících s plněním zakázky, a to po dobu nejméně 10 let od ukončení financování díla způsobem, který je v souladu s platnými právními předpisy České republiky a Evropských společenství.

10.6. Prodávající je povinen minimálně do konce roku 2037 poskytovat požadované informace a dokumentaci související s realizací projektu, z něhož je Veřejná zakázka hrazena, zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.

10.7. Prodávající bere na vědomí, že úhrada ceny za předmět plnění bude provedena s využitím dotačních prostředků, získaných kupujícím a podléhajících kontrole z hlediska vykazování účelnosti jejich čerpání. Prodávající se zavazuje, že kupujícímu nahradí veškeré škody a náklady, které mu vzniknou nebo budou muset být vynaloženy, pokud z důvodu porušení této smlouvy prodávajícím vznikne kupujícímu závazek vrátit dotaci nebo její část, poskytnutou na úhradu ceny za předmět plnění, jejímu poskytovateli, a to i včetně penále případně vyměřeného jako důsledek porušení pravidel nakládání s veřejnými prostředky. To platí obdobně, pokud prodávající znemožní řádný výkon kontroly orgánům, oprávněným ke kontrole účelnosti vynaložení dotačních prostředků, resp. nepředloží jimi požadované doklady.

10.8. Prodávající se zavazuje během plnění smlouvy i po jejím ukončení smlouvy zachovávat mlčenlivost o všech skutečnostech, o kterých se dozví od kupujícího v souvislosti s plněním smlouvy

10.9. Tuto smlouvu lze měnit nebo doplnit pouze dohodou smluvních stran, a to formou písemného číslovaného dodatku.

10.10. Smluvní strany prohlašují, že si tuto smlouvu přečetly, a že byla ujednána po vzájemném projednání podle jejich svobodné vůle, určitě, vážně a srozumitelně.

10.11. Prodávající se zavazuje k dodržování mezinárodních sankcí Evropské unie, přijatých v souvislosti s ruskou agresí na území Ukrajiny vůči Rusku a Bělorusku, zejména nařízení Rady EU č. 2022/576, nařízení Rady (EU) č. 269/2014 ve spojení s prováděcím nařízením Rady (EU) č. 2022/581, nařízení Rady (EU) č. 208/2014 a nařízení Rady (ES) č. 765/2006 nebo v jejich prospěch (dále jen „mezinárodní sankce EU“).

10.12. Smlouva je, v souladu s podmínkami zákona č. 134/2016 Sb., podepsána elektronicky.

10.13. Rada města Krnov souhlasila s uzavřením této smlouvy na svém jednání dne 10. 11. 2025 usnesením č. 3398/86/RM/2025.

10.14. Smlouva nabývá platnosti dnem podpisu a účinnosti dnem jejího uveřejnění v registru smluv. Uveřejnění smlouvy v registru smluv provede kupující.

10.15. Nedílnou součástí této smlouvy jsou následující přílohy:

Příloha č. 1 – Technická specifikace

Příloha č. 2 – Podmínky poskytování technické podpory

Prodávající:	Kupující:
V Praze dne dle data el. podpisu	V Krnově dne dle data el. podpisu
Jindřich Rosička Digitálně podepsal Jindřich Rosička Datum: 2025.12.02 09:30:17 +01'00'	
.....	.....
Jindřich Rosička	Mgr. Tomáš Hradil, starosta
Jednatel	Město Krnov

Příloha č. 1 – Technická specifikace

Pořízení a implementace NGFW

Parametr	Minimální požadavek	Splňuje ANO/NE[1]
Výrobce, model, cena	Sophos XGS 3300 Security Appliance 2x Sophos Xstream Protection for XGS 3300 - 60 MOS Sophos XGS 3300 Webserver Protection - 60 MOS Sophos XGS 3300 Email Protection - 60 MOS Sophos XGS 3300 Enhanced to Enhanced Plus Support Upgrade - 60 MOS port 10 GE SFP+ Flexi Port module 2x Trend Micro Deep Discovery Email Inspector 7300 HW(incl.5y warranty): New, Normal, License,60 months Trend Micro Deep Discovery Email Inspector - Gateway Module, SW v5.x: New, Normal, 1-1000 User License, 60 months Cena: 2 464 206 Kč bez DPH	
Provedení	• rackmount provedení, max. 1RU	ANO
Vlastnosti a funkce	• stavový firewall s integrovanou IPS (deep paket inspection) • možnost vytváření vlastních IPS pravidel • podpora dynamických směrovacích protokolů BGP, OSPF • plná podpora kontroly SSL provozu (“man-in-the-middle”) • antivirová kontrola na UTM bráně • podpora detekce zero-day útoků s možností sandboxingu • podpora detekce malware infekce s možností detekce a prevence připojení nakažených stanic k C&C serverům • Web Proxy (transparentní / explicitní) s možností ověřování identity uživatelů v Active directory, protokolem NTLM, nebo autentifikace dedikovaným ověřovacím klientem, či předávání identity uživatele Endpoint bezpečnostním klientem. • podpora autentizace přístupů pomocí: Active Directory, eDirectory, RADIUS, LDAP a TACACS+ • podpora Traffic Shaping, QoS s podporou priroritizace provozu na základě analýzy provozu (aplikačních detektorů) včrtně možností DSCP markup • podpora VPN (site to site a remote access) - IPSec a SSL VPN (obojí bez omezení počtu tunelů, či uživatelů) • neomezený počet SSL VPN klientů zdarma • vestavěné šablony pro aplikační firewall (WAF): Microsoft Exchange, SharePoint a další XML • vestavěné (on-box) statistiky a reporty k dispozici alespoň 6měsíců zpětně • plný MTA agent pro kontrolu a filtrování emailové komunikace • podpora FastPath metody optimalizace odbavení paketů	ANO

[1] Pozn. Účastník ve sloupci vyplní splnění závazných požadavků zadavatele (ANO/NE), případně doplní číselnou hodnotu požadovaného parametru. Účastník doloží závazných požadavků zadavatele rovněž odkazy na stránky výrobce, kde je možné požadovaný parametr ověřit (viz tabulka *„URL k dokumentaci technických parametrů“* níže). Účastník musí splňovat veškeré min. technické požadavky zadavatele.

	• podpora High Availability (HA), 2 zařízení v režimu active-passive / active-active • pasivní zařízení v HA režimu musí fungovat bez dalších poplatků za podporu/výměnu nebo licence • integrovaný WiFi kontroler, • funkce antivirové kontroly provozu pro vybrané protokoly s možností sanitarizace aktivního obsahu kancelářských souborů (odstranění možného škodlivého kódu z dokumentů), podporou detekce Botnet IP/domén, detekce malware pro mobilní platformy, podpora kontroly souborů a odkazů technikou sandboxing (on-prem nebo cloud), všechny databáze udržovány a aktualizovány výrobcem.	
VPN	• Funkce SSL VPN (portálový režim, tunelový režim). • Funkce IPSEC VPN (IKE, PSK, certifikát, gateway to gateway, hub and spoke, internet browsing konfigurace, podpora vice tunelů – redundantní VPN s podporou dynamického routování). • Možnost vzdálené instalace VPN klienta. • Zobrazení aktuálně připojených uživatelů v GUI. • Licenčně neomezený počet VPN tunelů, připojených uživatelů a přenosu dat. • Neomezený počet SSL VPN a IPSEC klientů.	ANO
Ochrana serverů a aplikací	• Reverzní proxy pro ochranu interních webových serverů a aplikací. • Ochrana skenováním antimalware utilitou • Filtrování http a https komunikace • Automatické přesměrování http komunikace na https • Podpora nahrávání vlastních certifikátů pro jednotlivé virtuální servery • Možnost monitorovat nebo blokovat (odmítnout) komunikaci • Přeposílání originální hlavičky (pro zobrazení skutečných zdrojů komunikace na cílovém serveru) • Podpora zabezpečení koncových aplikací vytvářením přihlašovacích formulářů • Ochrana proti útokům na aplikace • Ochrana proti podvržení cookies (podepisování) • Blokování komunikace na základě reputační služby výrobce • Blokování útoků typu SQL injection ANO • Možnost specifikace výjimek • Logování komunikace v reverzní proxy.	ANO

Minimální HW parametry	• podpora pro redundantní zdroj napájení
	• LAN porty min.:
	  ○ 8x RJ45 10/100/1000Mb
	  ○ 2x SFP 1000Mb
	  ○ 4x 10Gb SFP+ porty
	  ○ konzolový port pro management
	  ○ minimálně 120 GB SSD disk s dedikovanou oblastí pro ukládání logů a detailní reporting (onbox)
		ANO

Záruka, servis	• min. 5 LET, max. odezva NBD on-site po nahlášení problému	ANO

	• servis je poskytován servisním partnerem případně přímo výrobcem • jediné kontaktní místo pro nahlášení poruch pro všechny komponenty dodávaného systému • servisní zásahy budou prováděny vždy v místě instalace zařízení ať už pomocí vzdáleného přístupu nebo fyzicky na místě. Nabízené zařízení musí být pokryto oficiální podporou výrobce tak, aby v případě závady, kterou není prodávající schopen odstranit, mohl kupující tuto závadu eskalovat přímo k technické podpoře výrobce zařízení • zadavatel musí mít možnost si sám legálně stahovat bezpečnostní záplaty i nové verze Software/Firmware pro nabízené zařízení přímo ze stránek výrobce zařízení	
Certifikace dodavatele, původ zboží	• Jsou splněny „Požadavky na certifikaci dodavatele HW a původ zboží“	ANO

Obecné požadavky na nabízené řešení

Předmětem je komplexní zabezpečení bezpečnosti dle níže uvedených specifikací.

Zabezpečení vstupu do sítě na perimetru

Základní parametry požadovaného řešení – Next Generation Firewall

Zadavatel poptává řešení Next-generation Firewall typu hardware appliance. Administrace řešení musí být možná přes webové rozhraní s podporou textového rozhraní tzv. „cli“.
Kompletní řešení se musí skládat ze dvou fyzických zařízení (hardware appliance) zajišťující funkcionalitu vysoké dostupnosti (active-passive) a plnohodnotný reporting. Součástí dodávky jsou veškeré licence pro zajištění požadovaných funkcí. Nabízené řešení musí podporovat hardware akceleraci skrze dedikovaný čip (nezávislý na standardním procesoru).

Nabízené řešení musí obsahovat podporu 24/7/365, záruku na hardware a licence na dodané řešení po dobu 5 let.

Vyžadované funkce nabízeného řešení

a) Základní požadavky

Požadavky	
Napojení na Active Directory	ANO
Podpora bezagentového přihlášení uživatelů nezávislé na portu komunikace	ANO
Podpora funkcionality typu SD-WAN (včetně funkce rozkládání zátěže mezi primární a záložní internetovou linku a WAN failover na základě dostupnosti WAN konektivity).	ANO

Možnost automatické zálohy systému a v případě potřeby kompletní obnovy konfigurace nahráním ze zálohy	ANO
Vynucení šifrování záloh	ANO
Logování a rozšířený reporting (vč. statistik uživatelských aktivit)	ANO
Podpora vrácení se na předchozí verzi software (po aktualizaci na novou verzi systému)	ANO
Vlastní API rozhraní pro propojení s dalšími interními nástroji	ANO
Licenční práva minimálně pro 350 uživatelů a 50 domén	ANO

b) Funkční požadavky na logování a reportování

Požadavky	**Splňuje ANO/NE**
Real-time analýza provozu	ANO
Podpora retrospektivního procházení logů za účelem odhalení dříve neznámých hrozeb Možnost tvorby vlastních detailních reportů	ANO
Možnost exportu reportů (HTML, PDF, CSV, XML)	ANO
Možnost vlastní definice monitorovaných událostí	ANO
Možnost nativní integraci s poptávaným NGFW řešením	ANO

c) Proaktivní ochrana perimetru

Požadavky	
Stavové filtrování paketů, NAT	ANO
L2 transparentní režim (dva a více sítových rozhraní)	ANO
L2 interface pair (dvě sítové rozhraní)	ANO
IDS/IPS filtr nastavitelný na konkrétní komunikaci (pravidla firewall)	ANO
Možnost vytvářet vlastní IPS pravidla	ANO
Blokování komunikace C&C a typu Botnet a možnost specifikace výjimek	ANO
Identifikování kompromitovaného systému na základě C&C komunikace	ANO
Aplikační kontrola (blokování konkrétních aplikací z pravidelně aktualizovaného seznamu výrobce).	ANO
Logování a reportování	ANO

d) VPN – vzdálené přístupy

Požadavky	
IPSEC – propojení vzdálených lokalit, včetně podpory IKEv2	ANO
SSL VPN i IPSEC – připojení vzdálených PC	ANO
SSL VPN - Odlišný certifikát / uživatel	ANO
Možnost vzdálené instalace VPN klienta	ANO
Zobrazení aktuálně připojených uživatelů v GUI	ANO
Licenčně neomezený počet VPN tunelů, připojených uživatelů a přenosu dat	ANO
Neomezený počet SSL VPN a IPSEC klientů součástí licence	ANO
Podpora IPSEC route-based VPN	ANO

Logování a reportování	ANO

e) ZTNA

Požadavky	
Plně podporuje princip „trust nothing, verify everything“	ANO
Integrace s AD, Azure AD, Okta	ANO
Oprávnění je možné kontrolovat politikami až na úroveň aplikace	ANO
Podporuje mikrosegmentaci aplikací přístup na jednotlivé aplikace, uživatel není nutně v LAN	ANO
Podpora je realizována agentem pro OS Windows a macOS, připouští se pro webové aplikace „agentless“ přístup	ANO
Podporuje kontrolu „Device health“	ANO
Zajišťuje SSL/TLS inspekci komunikace	ANO
Management je prováděn řízením přes cloud	ANO
ZTNA podporuje spolupráci s XDR řešením	ANO

f) Ochranu přístupů na internet

Požadavky	
Filtrování HTTP, HTTPS a FTP	ANO
SSL / TLS skenování neomezené jen na HTTPS protokol	ANO
Ochrana skenováním antimalware	ANO
URL filtrování (min. 75+ kategorií)	ANO
Blokování datových typů na základě přípony souboru a MIME hlavičky	ANO
Propojení s Active Directory	ANO
Možnost definovat výjimky (minimálně na zdrojové IP, cílové IP a webové stránky)	ANO
Podpora platnosti pravidel pouze ve specifikovaný čas	ANO
Pravidla musí být možno specifikovat na skupinu/uživatele z Active Directory	ANO
Funkce kategorizace webových stránek (web filtering) s podporou minimálně 60 kategorií (pracovní zájmy, osobní zájmy, stránky se škodlivým kódem, nově registrované domény atp.), podpora definice časové kvóty, kterou nesmí daný uživatel na dané kategorii za den překročit, výrobcem aktualizovaná a udržovaná databáze.	ANO
Kontrola souborů pomocí technologií Sandboxing buď on-prem nebo cloud based nástrojem výrobce	ANO
Logování a reportování	ANO

g) Reverzní proxy pro ochranu interních webových serverů a aplikací

Požadavky	
Ochrana antimalware motorem	ANO
Filtrování http a https komunikace	ANO
Automatické přesměrování http komunikace na https	ANO
Podpora nahrávání vlastních certifikátů pro jednotlivé virtuální servery	ANO

Možnost monitorovat nebo blokovat (odmítnout) komunikaci	ANO
Přeposílání originální hlavičky (pro zobrazení skutečných zdrojů komunikace na cílovém serveru)	ANO
Podpora zabezpečení koncových aplikací vytvářením přihlašovacích formulářů navázaných na Active Directory	ANO
Ochrana proti útokům na aplikace	ANO
Ochrana proti podvržení cookies (podepisování)	ANO
Blokování komunikace na základě reputační služby výrobce	ANO
Blokování útoků typu SQL injection	ANO
Možnost specifikace výjimek	ANO
Logování a reportování	ANO

h) Minimální technické požadavky a propustnosti deklarované výrobcem

Požadavek	**Hodnota**	
Hardware akcelerace	S možností aktualizace firmware akceleračního chipu	ANO
Active/passive cluster	2 fyzická zařízení	ANO
Porty	Min. 8x GE RJ45, 1x management port 4x SFP 4X SFP+	ANO
Rozšiřitelné moduly	1	ANO

Propustnost	**Hodnota**	
Firewall	>=50Gbps	ANO
IPSEC VPN	>=30 Gbps	ANO
IPS	>=12 Gbps	ANO
NGFW	>=10 Gbps	ANO
Latence	<=5 µs	ANO
Konkurenční spojení	>7 miliónů	ANO
Nová spojení / sekunda	>250000	ANO

Celé řešení firewall musí podporovat zasílání informací do nabízeného XDR řešení a mít přímou podporu od výrobce přímých změn ve firewallu například v průběhu nákazy malware (zákaz nebezpečné komunikace, vyhodnocování komunikace atd.).

Zabezpečení detašovaných pracovišť

Předmětem je bezpečné připojení detašovaných pracovišť s vlastním přístupem na internet (Městská policie Krnov 'Žižkova 539/20, Krnov', Jednotka sboru dobrovolných hasičů Krnov 'Partyzánů 2333/16 , Krnov') k hlavní počítačové síti ‚Hlavní náměstí 1' tak, aby se staly jeho integritní součástí. Řešení musí mít možnost připojit vzdálené pobočky přes internet pomocí šifrovaného VPN tunelu přes další, dedikované hardware zařízení, ale stále s jednotnou správou (z centrálního firewallu)

1. Technické požadavky

Požadavek	Hodnota	Splňuje ANO/NE
Minimální propustnost IPSec VPN	4 Gbit/sec	ANO
LAN rozhraní	4 x 10/100/1000 Base-TX (1 Gbit E Copper)	ANO
WAN rozhraní	1 x 10/100/1000 Base-TX (připouští se sdílení s SFB rozhraním)	ANO
SFP rozhraní	1x SFP Fiber (připouští se sdílení s WAN rozhraním)	ANO
USB port	1 x USB 3.0	ANO

2. Funkční požadavky

Požadavek	Hodnota	Splňuje ANO/NE
Podpora šifrování IPSec spojení	AES-256 nebo vyšší	ANO
Podpora SSL a TLS protokolů	TLS 1.3	ANO

Ochrana e-mailové komunikace

Funkční a technické požadavky na ochranu emailové komunikace

1) Obecné požadavky na řešení

Žádné z dodávaných částí řešení nesmí být v době podání nabídky v režimu End of Sale / End of Support

Řešení musí být dodané jako HW Appliance ve formě HA dvojice boxů

2) Obecné požadavky na platformu

Dodané prvky musí fungovat jako platforma, tedy funkční celek, na které jsou kladeny následující požadavky. Funkční požadavky u jednotlivých částí dodávky jsou zpřesněním a mohou být duplicitní.

MINIMÁLNÍ POŽADAVKY	Splňuje ANO/NE
Zařízení ve formě HW appliance o velikosti 1RU (VM appliance či aplikace instalovaná do obecného operačního systému nebude akceptována)	ANO
podpora režimu vysoké dostupnosti (A-A, A-P). Pokud je vyžadována licence pro takové režimy fungování, musí být součástí dodávky.	ANO
Podpora diskové kapacity alespoň 1TB a záloha uložiště RAID 0 a vyšší	ANO

požadovaná propustnost řešení je min 100 000 email/h při využití souběžné inspekce pomocí antivirus a antispam profilů. referenční velikost kontrolovaného emailu je 100 kB.	ANO
řešení je schopno konfigurovat pro ochranu až 50 domén	ANO
možnost nasazení v režimu gateway (MTA), server i transparent. Licence pro všechny požadované režimy provozu je součástí dodávky řešení.	ANO
v režimu server je možno vytvořit až 350 schránek. Případná licence pro takový počet schránek je součástí nabízeného řešení. Licenčně je možné počet schránek navýšit alespoň dvojnásobně.	ANO
certifikace řešení alespoň VBSpam nebo VB100	ANO
Bezpečnostní a síťové funkce	
podpora IPv4 i IPv6	ANO
podpora SMTP autentizace min. pomocí protokolů LDAP, RADIUS, POP3 a IMAP	ANO
integrovaná funkce antivirové ochrany emailového provozu s podporou real-time ochrany před outbrake škodlivého kódu. Databáze antivirových signatur musí být udržována výrobcem nabízeného řešení a automaticky aktualizovaná	ANO
integrovaná funkce antispam ochran s možností kategorizace v emailu nalezených URL, IP reputační databáze výrobce, graylisting, reputace odesílatelů, behaviorální analýza, analýza hlaviček mailů, heuristická analýza mailů, podpora systémů třetích stran (blacklisty), kontrola založená na Bayesian přístupu, white a black listing, analýza obrázků s možností detekce a selekce newsletter emailů, podpora funkce tzv. bounce verification, podpora greylistingu. Všechny databáze potřebné pro provoz požadovaných funkcí jsou sprované a aktualizované výrobcem nabízeného řešení.	ANO
podpora nastavení limitů v rámci SMTP relací (počet zpráv od jednoho klienta za určitou dobu, maximální počet spojení od jednoho klienta za určitou dobu, podpora endpoint reputace, napojení na LDAP za účelem verifikace uživatelů; možnost omezení počtu HELO/EHLO v rámci jedné SMTP relace, možnost omezit počet emailových zpráv v rámci SMTP relace, možnost omezit počet příjemců v rámci adresátů emailu, možnost manipulace s hlavičkou mailu (odstratení Received hlavičky)	ANO
schopnost analýzy PDF dokumentů v příloze kontrolované zprávy	ANO
shodné možnosti nastavení a provedení kontroly příchozí i odchozí komunikace	ANO
granulární konfigurace pravidel (pravidla na základě IP adres a/nebo domén příjemce, možnost využití wildcard notace)	ANO
možnost využití zabudované geo databáze IP adres v rámci pravidel. Databáze je udržována udržovaná výrobcem nabízeného řešení.	ANO
podpora karantény s uživatelským přístupem umožnujícím běžné operace pomocí odděleného síťového rozhraní	ANO
podpora systémové karantény	ANO
podpora externího úložiště (šifrovaná komunikace, např. SFTP)	ANO
řešení a jeho dodané licence umožní provozovat TLS šifrování	ANO
řešení a jeho dodané licence umožní nastavit S-MIME	ANO
řešení a jeho dodané licence umožní nastavit DKIM, SPF a DMARC	ANO
řešení a jeho dodané licence umožní nastavit zabezpečení přenosu mailové komunikace pomocí IBE	ANO
funkce ochrany rate limiting, vyhodnocování lokálního skóre odesílatelů (na základě nedávné activity) s možností nastavení chování pro různé úrovně skóre	ANO

funkce zabezpečení dokumentů v příloze se schopností odstranění potencionálně nebezpečných prvků v dokumentu (makra, URL, …) včetně dokumentů MS Office a PDF při zachování původního typu dokumentu	ANO
automatická dekrypce šifrovaných dokumentů za pomoci administrátorem předdefinovaného slovníku hesel, za účelem provedení plné AV a AS kontroly	ANO
reakce na detekovanou hrozbu v podobě alespoň přřidání tagu, přidání nové hlavičky, přeposlání emailu na jiný SMTP server, odmítnutí (reject), zahození (discard), uložení do karantény, přepsání adresy příjemce	ANO
funkce opakované kontroly emailu ve chvíli jeho vyzvednutí z karantény	ANO
ochrana před škodlivými URL (výrobcem udržovaná databáze škodlivých URL). Možnost uživatelské volby nežádoucích webových kategorií (phishing, malware, adult material, ...)	ANO
URL click protection a ochrana proti impersonifikaci	ANO
SandBox funkcionalita v prostředí výrobce řešení pro podporu detekce Zero Day hrozeb	ANO
ochrana před útoky typu BEC	ANO
architektura MTA musí umožnit provést kontrolu emailu ještě před uložením do emailové fronty	ANO
Integrace s poptávaným XDR řešením	ANO
Správa řešení	
plnohodnotná správa pomocí (HTTPs) a CLI (SSH) je součástí nabízeného řešení	ANO
možnost omezení administrátorských práv na definované domény	ANO
Integrované logování systémových událostí a průběhu inspekce provozu s možností zobrazení logů v GUI	ANO
podpora protokolů SNMP (v2c, v3) a syslog pro možnost začlenění do externího monitorovacího systému	ANO
podpora logování na externí log server (syslog)	ANO
podpora archivace (přístup do archive pomocí protokolu IMAP)	ANO
podpora REST API pro možnost integrace management do stávající infrastruktury. Pokud tato funkce vyžaduje licenci, tak tato musí být součástí dodávky.	ANO
oddlění administrátorského a uživatelského přístupu do emailových schránek a karantény pře různá síťová rozhraní	ANO
Požadavky na podporu řešení	
podpora nabízeného produktu v režimu 24/7 a to telefonicky i elektronicky	ANO
nabízené řešení obsahuje všechny potřebné licence pro výše popsané a požadované funkce	ANO
všechny popsané funkce nabízeného řešení musí být možné ověřit ve veřejně dostupné produktové dokumentaci výrobce řešení	ANO

3) Funkční požadavky

Požadavky	**Splňuje ANO/NE**
Řešení umožňuje založit v administrativním rozhraní jmenné účty s alespoň dvěmi úrovněmi oprávnění (např. Administrátor, Operátor).	ANO
Řešení umožňuje definování různých politik pro jednotlivé uživatele (whitelist, blacklist, apod.).	ANO
Řešení musí umožňovat procházení fronty e-mailů v reálném čase a umožnovat v ní vyhledávání minimálně podle IP adresy odesílatele, e-mailové adresy odesílatele, emailové adresy příjemce, předmětu, hash přílohy.	ANO

Řešení poskytuje detailní záznamy o automaticky provedenných činnostech a detekovaných událostech pro potřeby auditu.	ANO
Řešení musí umožňovat zpětné doručení zprávy, která byla dána do karantény.	ANO
Řešení musí mít schopnost přeposílat podezřelé e-maily do vyhrazené e-mailové schránky.	ANO
Řešení umožňuje přidání textu na začátek předmětu podezřelých e-mailů. Přidávaný text musí být možné upravit v nastavení Řešení.	ANO
Řešení umožňuje přidání HTML textu na začátek těla e-mailu s možností přizpůsobení podle kontextu zprávy, například výchozí zpráva pro všechny e-maily a specifické zprávy pro e-maily obsahující přílohy, odkazy nebo podezřelý obsah.	ANO
Řešení umí reportovat denní, týdenní a měsíční statistiky počtu zpracovaných e-mailu a reporty o své činnosti.	ANO
Řešení umožňuje generování reportů zaměřených na sledování efektivity e-mailových politik, jejíž součástí jsou i statistiky o počtu zablokovaných, karanténovaných a propuštěných e-mailů.	ANO
Řešení podporuje logování (Syslog).	ANO
Možnost úpravy reportů a jejich generování v PDF a e-mailem	ANO
Nastavení notifikací pomocí e-mailu a SNMP Trap	ANO
Řešení podporuje integraci se SIEM (např. ArcSight, Splunk, QRadar).	ANO
Řešení musí umožňovat sledování a řízení využití systémových prostředků (CPU, operační paměť, disková kapacita) a upozornit administrátory v případě přetížení nebo blížícího se vyčerpání zdrojů.	ANO
Řešení musí umět vytvořit network dump na síťovém interface pro účely řešení problémů	ANO
Před pokusem o doručení e-mailu musí umět ověřit, jestli na interním Active Directory serveru existuje záznam pro cílovou e-mailovou adresu (jedná se o ověření, zda e-mailová schránka existuje v prostředí zadavatele).	ANO
Požadavky na ochranu emailové komunikace	ANO
Možnost rozšíření o analýzu souborů a URL v sandboxu napojením na onpremise Sandbox	ANO
Možnost rozšíření o analýzu souborů a URL v sandboxu běžícím přímo na dané emailové HW apliance (například nákupem dodatečné licence bez nutnosti výměny HW)	ANO
Možnost napojení na XDR (prostřednictvím sdílením detekčních logů)	ANO
Mapování logů a detekcí na MITRE ATT&CK	ANO
Schopnost skenovat zaheslované soubory na základě hesla uvedeného v e-mailu nebo na základě seznamu předem definovaných hesel	ANO
Možnost zazálohovat soubor před tím, než je proveden sken	ANO
Detekce dosud netestovaných, nekategorizovaných URL	ANO
Možnost blokace zaheslovaných souborů a zaheslovaných Office dokumentů	ANO
Možnost blokace příloh na základě nastavených parametrů (např. název, přípona, velikost)	ANO
Možnost blokování všech příloh	ANO
Musí obsahovat centrální e-mail karanténu	ANO
Možnost nastavení retence dat v karanténě	ANO
Možnost stáhnout si soubor z karantény v zaheslovaném archivu	ANO
Dostupné akce pro karanténu musí být minimálně - obnovit, stáhnout a nebo smazat	ANO
Řešení umožňuje uživatelům přístup k jejich vlastní karanténě e-mailů s možností uvolnění e-mailu v ní. Minimálně jednou denně probíhá automatické zaslaní e-mailového upozornění na uživatele, který má nějaké e-maily v karanténě.	ANO
Řešení musí umět kontrolovat soubory v příloze každého e-mailu na přítomnost malware.	ANO
Řešení musí umět e-mail na základě nastavené politiky zařadit do karantény nebo e-mail rovnou zablokovat a odmítnout ho.	ANO

Řešení musí umět detekovat a filtrovat SPAM, phishing a spear phishing (např. podle obsahu, odesílatele, URL).	ANO
Řešení umožnuje detekci a blokaci BEC (Business E-mail Compromise).	ANO
Řešení podporuje využití machine learning při detekci neznámých vzorků malware.	ANO
Řešení podporuje skenování a analýzu komprimovaných archívů (ZIP, RAR, 7z) v e-mailech, včetně víceúrovňových archívů.	ANO
Nabízené Řešení řešení musí obsahovat databáze signatur, pravidel, reputačních informací (IP adresa, doména), které jsou vyvíjeny a aktualizovány výrobcem tak, aby byly optimalizovány pro minimalizaci falešně pozitivních i falešně negativních detekcí.	ANO
Řešení musí automaticky od výrobce stahovat reputační informace o odesílatelích (IP adresa) a na jejich základě blokovat příjem e-mailu.	ANO
Řešení umožňuje detekci a blokování QR kódů v e-mailech, které odkazují na podezřelé nebo škodlivé webové stránky.	ANO
Řešení umožňuje, který přesměruje uživatele na bezpečnostní bránu, kde je původní odkaz zkontrolován a analyzován na přítomnost hrozeb až při kliknutí uživatele.	ANO
Řešení musí analyzovat odkazy v e-mailech a blokovat e-maily obsahující odkazy na škodlivé stránky.	ANO
Řešení musí umět kontrolovat DKIM, SPF a DMARC a na základě vyhodnocení provádět rozdílné akce (blokace, přesun do karantény, přidání textu do předmětu).	ANO
Ochrana proti bounce útokům	ANO
Možnost nastavení maximálního počtu spojení na SMTP	ANO
Možnost nastavení maximálního počtu příjemců pro jeden e-mail	ANO
Ochrana proti directory harvest útoku	ANO
Možnost přepsat adresu a doménu v rámci e-mailové zprávy	ANO
Řešení musí umět přepsat URL adresy v e-mailu, aby kontrola bezpečnosti cílové URL proběhla v momentě, kdy na URL uživatel přistoupí (s co nejaktuálnější reputační databází)	ANO
	ANO
Požadavky na záruku a podporu	ANO
Součástí dodávky je i SW maintenence výrobce, která umožňuje zadat požadavek přímo na podporu výrobce	ANO
Součástí dodávky jsou i aktualizace a patchování SW a firmware výrobce (Pravidelné aktualizace a bezpečnostní záplaty, které zajišťují, že systém bude chráněn proti nejnovějším hrozbám) po celou dobu platnosti smlouvy, včetně podpory nových verzí Microsoft Exchange.	ANO
Technická podpora musí být poskytovaná odborníky, s garantovanými odezvami na kritické incidenty do 1 hodiny od založení požadavku.	ANO
Možnost založení požadavku minimálně přes webový formulář a telefonicky	ANO

URL k dokumentaci technických parametrů[2]

URL odkazy na dokumentaci výrobce, dokládající technické parametry
https://support.sophos.com/support/s/article/KBA-000007279?language=en_US
https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/Licensing/AdministrationLicensing/index.html#license-bundles
https://support.sophos.com/support/s/article/KBA-000004113?language=en_US
https://www.sophos.com/en-us/products/next-gen-firewall

[2] Účastník zde v jednotlivých řádcích uvede URL odkazy, kterými bude dokumentovat výše uvedené technické parametry jím nabízeného předmětu plnění.

https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/Licensing/AdministrationLicensing/index.html#license-bundles
https://docs.sophos.com/nsg/sophos-firewall/21.5/help/en-us/webhelp/onlinehelp/AdministratorHelp/Authentication/STAS/AuthenticationClientlessSSO/index.html
https://docs.sophos.com/nsg/sophos-firewall/21.5/help/en-us/webhelp/onlinehelp/AdministratorHelp/BackupAndFirmware/BackupAndRestore/BackupAndRestoreCreateRestore/index.html#create-a-backup
https://docs.sophos.com/nsg/sophos-firewall/21.5/help/en-us/webhelp/onlinehelp/AdministratorHelp/BackupAndFirmware/BackupAndRestore/BackupAndRestoreSSMK/index.html
https://docs.sophos.com/nsg/sophos-firewall/21.5/help/en-us/webhelp/onlinehelp/AdministratorHelp/BackupAndFirmware/API/index.html
https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/Licensing/AdministrationLicensing/index.html#license-bundles
https://support.sophos.com/support/s/article/KBA-000007279?language=en_US
https://docs.sophos.com/nsg/sophos-firewall/20.0/Help/en-us/webhelp/onlinehelp/AdministratorHelp/Administration/Licensing/AdministrationLicensing/index.html#license-bundles
https://support.sophos.com/support/s/article/KBA-000007279?language=en_US
https://assets.sophos.com/X24WTUEQ/at/7wf85vbnnqf939bbhtxgfk/sophos-firewall-br.pdf
https://ohc.blob.core.windows.net/o-help/manual/fc91541a-649c-45d4-b190-51b9bd78c1f2/ddei_5.1_idg.pdf
https://www.virusbulletin.com/virusbulletin/2025/06/vbspam-comparative-review
https://grahamcluley.com/vb100-win-sophos-virus-bulletins-largest-comparative-review/
https://docs.trendmicro.com/en-us/documentation/article/deep-discovery-email-inspector-51-online-help-end-user-quarantine
https://docs.trendmicro.com/en-us/documentation/article/deep-discovery-email-inspector-51-online-help-file-passwords
https://docs.trendmicro.com/en-us/documentation/article/deep-discovery-email-inspector-51-online-help-time-of-click-protec
https://docs.trendmicro.com/en-us/documentation/article/deep-discovery-email-inspector-51-online-help-business-email-compr
https://docs.trendmicro.com/en-us/documentation/article/deep-discovery-email-inspector-51-end-user-quarantine-introduction-euq

Příloha č. 2 – Podmínky poskytování technické podpory[3]

Dodavatel musí disponovat vlastním systémem pro monitoring spravovaných zařízení a služeb, který zajistí:

Nepřetržitý dohled

- Systém musí umožnit 24/7 monitoring spravované infrastruktury a okamžité hlášení incidentů.

Proaktivní přístup k řešení problémů

- Systém by měl identifikovat a hlásit anomálie, které mohou vést k výpadkům, ještě před jejich vznikem, a umožnit tak preventivní zásahy.

Přehledné rozhraní a reporting

- Dodavatel je povinen zajistit kupujícímu přístup k přehledným reportům o stavu spravovaných zařízení a služeb.
- Součástí reportů musí být informace o klíčových událostech, výpadcích a jejich řešení, jakož i statistiky využití a výkonu.

Kompatibilita se spravovanými zařízeními a službami

- Systém musí být plně kompatibilní s hardwarem a softwarem, které budou předmětem správy.

Bezpečnost a ochrana dat

- Dodavatel musí garantovat, že monitorovací systém bude splňovat bezpečnostní standardy a že veškerá data budou chráněna v souladu s platnou legislativou.

Kupující bude hlásit požadavky na služby následujícími způsoby:

- Do helpdesk systému dodavatele
- Kupující bude využívat Helpdesk systém poskytnutý dodavatelem pro evidenci a správu požadavků.
- Dodavatel musí zajistit přístup k Helpdesk systému pro autorizované osoby kupujícího.
- Systém musí umožňovat přehlednou evidenci požadavků, jejich aktuální stav a historii řešení.

Hlášení prostřednictvím e-mailu

- Kupující bude mít možnost hlásit požadavky na určenou e-mailovou adresu dodavatele.
- Dodavatel zajistí, aby e-mailové hlášení bylo automaticky zaevidováno v Helpdesk systému a označeno odpovídající prioritou.

Hlášení prostřednictvím telefonu

- V naléhavých případech, zejména u požadavků s vysokou prioritou, může kupující hlásit požadavky telefonicky na kontaktní číslo dodavatele.
- Telefonicky hlášené požadavky musí být následně zaevidovány v Helpdesk systému dodavatele.

Požadavky na Helpdesk systém dodavatele:

- Musí být k dispozici během pracovní doby (8 – 16 hodin)
- Dodavatel zajistí uživatelskou podporu při využívání Helpdesk systému.
- Systém musí umožnit automatické potvrzení přijetí požadavku.
- Evidence požadavků musí být přístupná kupujícímu pro kontrolu a zpětnou vazbu.

KVALITATIVNÍ PARAMETRY TECHNICKÉ PODPORY:

- **Minimalizace výpadků:** Služba bude poskytována tak, aby byly minimalizovány výpadky obchodní a provozní činnosti kupujícího způsobené spravovanou technikou.
- **Prioritní řešení:** Požadavky s přímým dopadem na produkt kupujícího budou řešeny nejpozději do 4 hodin v běžné pracovní době kupujícího.

REAKČNÍ DOBA TECHNIKŮ DODAVATELE V PRACOVNÍ DOBĚ (8:00 – 16:00):

- Priorita vysoká:
  - Situace: Vady zabraňující provozu, produkt není použitelný ve svých základních funkcích nebo se vyskytuje funkční závada znemožňující činnost systému. Tento stav může ohrozit běžný provoz Objednatele a nelze jej dočasně řešit organizačním opatřením.

[3] V rámci této přílohy je prodávající označen rovněž jako „dodavatel“.

    - Reakce: Okamžitá odezva technika, výjezd technika (nebo online zásah) do 8 hodin, řešení problému.
- Priorita střední:
    - Situace: Vady omezující provoz, funkčnost systému je ve svých funkcích degradována tak, že tento stav omezuje běžný provoz Objednatele. Jedná se také o vady způsobující problémy při užívání a provozování produktu nebo jeho části, ale umožňující provoz, jimiž způsobené problémy lze dočasně řešit organizačními opatřeními.
    - Reakce: Odezva technika do 8 hodin, řešení následující pracovní den.
- Priorita nízká:
    - Situace: Vady neomezující provoz, jedná se o drobné vady, které nespadají do kategorií „vysoká“ nebo „střední“.
    - Reakce: Řešení dle dohody při další návštěvě technika nebo do tří pracovních dnů vzdálenou správou.

Sankce za nedodržení kvalitativních požadavků:

- V případě prodlení Prodávajícího s odstraněním vad ve lhůtách stanovených v této příloze výše se Prodávající zavazuje Kupujícímu uhradit smluvní pokutu ve výši 200 Kč za každou hodinu prodlení v případě vad kategorie „priorita vysoká“ a smluvní pokutu ve výši 500 Kč za každý i započatý den prodlení v případě vady kategorie „priorita střední“, a to pro každý případ prodlení, není-li jinými ustanoveními této smlouvy výslovně uvedeno jinak.
- V případě, že Prodávající neumožní Kupujícímu zadat požadavek na servisní zásah z důvodu nedostupnosti služeb Hot-line ani HelpDesk, způsobené výpadkem uvedených služeb na straně Prodávajícího, je Kupující oprávněn po Prodávajícím požadovat smluvní pokutu ve výši 500 Kč za každý jednotlivý případ. To se netýká případu, kdy Prodávající provádí preventivní údržbu a na tuto skutečnost předem upozornil Kupujícího.
- Smluvní pokuty a úrok z prodlení jsou splatné do 30 dnů od doručení jejich vyžádání oprávněnou smluvní stranou straně povinné. Platby budou provedeny bezhotovostním bankovním převodem na účet oprávněné smluvní strany. Ujednání o smluvních pokutách se nedotýkají náhrady škody.
- Za podstatné porušení této smlouvy, pro něž může smluvní strana dotčená porušením povinnosti jednostranně odstoupit, se mimo jiné považuje:
    - neposkytnutí servisní podpory Prodávajícím, po řádném nahlášení požadavku Kupujícím, delší než 30 dní,
    - nedodržení doby odezvy nebo jiných dohodnutých termínů Prodávajícím o více jak 5 dnů,
    - bezdůvodné přerušení prací na servisním případu Kupujícího,
    - opakované nesplnění závazku Kupujícího poskytnout Prodávajícímu součinnost při plnění ustanovení této smlouvy i přes písemné upozornění doručené Kupujícímu.