PŘÍLOHA č. 1

Specifikace Dodávky

Požadavky Kupujícího

Touto veřejnou zakázkou bude zajištěna podpora od výrobce i dodavatele řešení bezpečnostní technologie perimetru sítě MHMP. Součástí dodávky je i funkční upgrade managementu řešení, který je z důvodu zachování investice a vize dalšího rozvoje nutné povýšit na výkonnější. Povýšení managementu bude provedeno metodou „trade-in", kde budou částečně vráceny náklady na již používané řešení. Navrhované zajištění servisní podpory bezpečného perimetru představuje zajištění vysoké úrovně bezpečnosti IS/ICT MHMP pro období tří let a zároveň optimální využití veškeré předchozí investice do bezpečnostních technologií perimetru sítě MHMP a souvisejících služeb po dobu 36 měsíců

Dodávka se skládá z těchto částí:

1. Zajištění 3 leté servisní podpory bezpečného perimetru pro produkty:
- 21000 Appliances
- Smart-1 Appliances
- Threat Emulation Appliance
- Software Products

2. Povýšení managementu řešení metodou trade-in
- Smart-1 5150 Next Generation Security Management Appliance. včetně 3 leté podpory.

3. Bezpečností servisní subskripce:
- Mobile Threat Prevention Blade
- Capsule WorkSpace a Mobile Threat Prevention Blade
- Enterprise Based Protection – NGTX

4. Implementační práce v rozsahu 25 člověkodnů

Popis aktuálního a cílového stavu

Zadavatel dnes využívá pro zabezpečení perimetru sítě a sítě MEPNET bezpečnostní technologie Check Point. Stávají podpora je zajištěna pouze do 30. 6. 2018.

Cílem zakázky je zajištění nezbytně nutné podpory výrobce na období 30. 6. 2018 – 30. 6. 2021. Součástí je i funkční upgrade managementu řešení, který je z důvodu zachování investice a vize dalšího rozvoje nutné povýšit na výkonnější.

Zajištění servisní podpory bezpečného perimetru je požadováno na 3 roky, aby zaručilo vysokou bezpečnost úřadu pro toto období a zároveň optimálně využilo veškeré předchozí investice do bezpečnostních technologií perimetru sítě úřadu.

POŽADOVANÉ DETAILNÍ TECHNICKÉ PARAMETRY

Pravidla pro vyplňování technických parametrů řešení

Uchazeč vyplní v následujících kapitolách pouze všechny žlutě označené části.

Tato příloha slouží **k vymezení minimálních technických požadavků zadavatele na řešení a osvědčení jejich splnění uchazečem.**

V níže uvedených tabulkách jsou uvedeny veškeré povinné minimální parametry kladené na celý systém. Nesplnění těchto požadavků je důvodem k vyřazení nabídky.

Dodavatel v níže uvedených tabulkách vyplní sloupce „Splňuje ANO/NE".

Sloupec vyjádření „Splňuje ANO/NE" může nabývat pouze hodnot ANO nebo NE, bude-li uvedeno něco jiného, je to rovněž důvod k vyřazení nabídky.

Nebude-li popis splnění/řešení požadavku odpovídat popisu požadavku, tato skutečnost může mít za následek i to, že bude konstatováno, že dodavatel nesplnil zadávací podmínky stanovené Zadavatelem.

Výše uvedená pravidla na vyplnění tabulek jsou společné pro všechny kapitoly této přílohy.

1.) ŘEŠENÍ ZAJIŠTĚNÍ 3 LETÉ SERVISNÍ PODPORY BEZPEČNÉHO PERIMETRU

Vlastnost	Požadavek Objednatele	Splňuje ANO/NE
Požadavek na obnovení podpory stávající instalované báze IS MHMP		
Základní SLA požadavek	7 x 24 x 365	ANO
Požadovaný čas reakce	30min pro celkové výpadky systému, 60 minut pro ostatní	ANO
Výměna zařízení po schválení RMA	Následující den	ANO

Požadavky na obnovu bezpečnostních funkcí		
Obnova pokrytí (subscription) bezpečnostních modulů IPS, ABOT, AV, pro instalovanou bázi	ANO	ANO
Obnova pokrytí (subscription) bezpečnostních modulů URLF, APCL pro instalovanou bázi	ANO	ANO

Obnova pokrytí (subscription) bezpečnostních modulů Threat emulation, Threat extraction pro instalovanou bázi	ANO	ANO

2.) POVÝŠENÍ MANAGEMENTU METODOU TRADE-IN

Vlastnost	Požadavek Objednatele	Splňuje ANO/NE
Požadavky na správu (management) řešeni		
HW zařízeni pro umístení do standardního racku (2ks)	ANO	ANO
Jednotný management pro všechny bezpečnostní aplikace s možností definice administrátorských rolí	ANO	ANO
Definice bezpečnostních pravidel na základě identity uživatele nebo jeho uživatelské skupiny z AD	ANO	ANO
Konsolidovaný centrální management: správa politik a analýza logů na jedné platformě	ANO	ANO
Automatická verifikace politiky (např. proti redundanci, překryvu a inkonzistenci pravidel)	ANO	ANO
Zajištění vysoké dostupnosti v režimu HA	ANO	ANO
Podpora vyhledávaní v pravidlech, vyhledávaní textových výrazů/objektů/IP adres nebo prohledávaní všech objektů	ANO	ANO
Podpora administrátorských profilů s možností přidělování práv (read only, red-write, none) pro jednotlivé skupiny administračních funkcí	ANO	ANO
Definice oddělených politik s možností práce více administrátorů najednou	ANO	ANO
Možnost přidělení práv administrátorům jen pro definovanou politiku/část politiky	ANO	ANO
Podporovaný počet řízených bran	Min. 120	ANO
Podporovaný počet řízených domén	Min. 25	ANO
Duální, Hot-Swappable PSU	ANO	ANO
Interní storage, hot-swappable	Min. 20TB	ANO
Podporované typy RAID konfigurace	5, 6, 10, 50	ANO

Počet zpracovaných indexovaných logů za vteřinu	Min 20000	ANO
Využití procedury trade-in	ANO	ANO

Povýšení managementu řešení metodou trade-in včetně 3 leté podpory

Povýšení managementu:

Technologie	Množství	Číslo výrobce	Popis
CheckPoint	2	CPAP-NGSM5150	Smart-1 5150 Next Generation Security Management Appliance for 150 GWs (SmartEvent & Compliance 1 year)
CheckPoint	2	CPSB-DMN-25	25 domains package for Multi-domain Security Management

Tříletá podpora výrobce:

Technologie	Množství	Číslo výrobce	Popis
CheckPoint	3	CPCES-CO-PREMIUM	Collaborative Enterprise Support Premium, 1year, HW

3.) BEZPEČNOSTÍ SERVISNÍ SUBSKRIPCE

Zajištění 3 leté servisní podpory výrobce technologií bezpečného perimetru:

- Mobile Threat Prevention Blade
- Capsule WorkSpace a Mobile Threat Prevention Blade
- Enterprise Based Protection – NGTX

Support a servis boxů musí zahrnovat tyto komponenty výrobce:

Technologie	Množství	Číslo výrobce	Popis
CheckPoint	1	CPCES-CO-PREMIUM	Collaborative Support Premium
CheckPoint	1	CPEBP-NGTX	Enterprise Based Protection - Next Generation Threat Extraction Package kage Including IPS, APCL, URLF, AV, ABOT, ASPM, TX and TE blades
CheckPoint	3	CP-CPSL-WORK-CONTRACT-3Y	Check Point Capsule Workspace and Docs subscription for 1 year
CheckPoint	3	CP-MTP-USR-3Y	Check Point Mobile Threat Prevention per user subscription for 1 year

4.) POŽADAVKY NA IMPLEMENTACI

Dodavatel provede úplnou implementaci v datovém centru Magistrátu hl. m. Prahy. Úplná implementace zahrnuje:

- Dodávku a oživení v prostředí DC;
- Migraci stávajících politik
- Optimalizaci stávajících politik
- Napojení na monitoring
- Zprovoznění zálohování konfigurace

Ověření podmínek upgrade a specifikace potřebných změn před provedením upgrade

Prověření všech skutečností, které mohou blokovat upgrade. Návrh řešení, možnosti vyřešení konkrétních problémů ještě před migrací. Jde např. o:

- IPS package version
- non-Unicode characters
- DHCP relay
- OPSEC produkty

Výběr postupu upgrade

Z možných variant upgrade vybrat způsob, který bude znamenat minimální dopad na produkci a zároveň zajistí integritu prostředí během migrace. Je potřeba brát v úvahu, že jde o management HA prostředí.

Simulace upgrade

Vybraný způsob migrace otestovat v neprodukčním prostředí

Sestavení implementačního plánu

Před migrací bude připraven implementační plán, který přesně popíše:

- „Odpovědnost" – kdo je odpovědný za úspěšnou realizaci daného kroku
- „Podmínky realizace" - podmínky, které musí být splněny, aby bylo možné zahájit práce na daném kroku.
- „Kontrolní body" - popis kontrol, které se ověřují pro určení úspěšnosti prací. Jejich úspěšné splnění umožní postup na další krok prací.
- „Havarijní plán" - popis možných rizik, které z prací, souvisejících s aktuálním krokem, plynou a způsob jejich řešení, případně roll-back plán.

Optimalizace politik pro R80

- Access Politiky
- Threat prevention politiky

Pilotní provoz

Při tomto kroku se nebudou realizovat žádné konkrétní plánované práce. Systém by měl běžet ve zprovozněném stavu po určité, předem dohodnuté, testovacím období (14 dní), po které se bude v provozním režimu zjišťovat, zda vše funguje dle předpokladů a požadavků. Pouze v případě, že se objeví nějaké problémy nebo ze strany zákazníka vyvstanou požadavky na úpravu funkce, se bude realizovat technický zásah.

Konfigurace zálohování a monitoringu nového prostředí

Vytvoření projektové dokumentace

Implementační práce budou provedeny v minimálním rozsahu 25 člověkodnů

SPOLEČNÉ PARAMETRY A POŽADAVKY NA DODANÉ ŘEŠENÍ

Místo plnění

Místem plnění je Datové centrum Magistrátu hl. m. Prahy

Požadavky na záruku za jakost a podporu

Záruka za jakost a s tím spojená podpora je požadována v trvání 36 měsíců, v režimu pokrytí 5 pracovních dnů v týdnu, 8 hodin denně s garancí opravy následující pracovní den (NBD)

Společné

- Zařízení musí být nové, nepoužité a homologované pro provoz na území EU.
- Servisní podpora výrobce musí být poskytována v České republice a v českém jazyce.
- Je požadováno potvrzení od lokálního zastoupení výrobců jednotlivých částí plnění, že nabízené zboží je určeno pro český (EU) trh a bude plně podporováno servisním střediskem v ČR.

Nabízené řešení Prodávajícím

Nabízené řešení splňuje veškeré požadavky zadavatele. Řešení se skládá z těchto částí:

1. Zajištění 3 leté servisní podpory pro
   a. 21000 Appliances
   b. Smart-1 Appliances
   c. Threat Emulation Appliance
   d. Software Products

2. Povýšení managementu řešení metodou trade-in
   a. Smart- 1 5150 Next Generation Security Management Appliance včetně 3 leté podpory

3. Bezpečnostní servisní substrikce:
   a. Mobile Threat Prevention Blade
   b. Capsule WorkSpace a Mobile Threat Prevention Blade
   c. Enterprise Based Protection – NGTX

4. Implementační práce v rozsahu 25 člověkodní

Nabízené řešení splňuje detailní technické požadavky:

1.) Navržené ŘEŠENÍ ZAJIŠTĚNÍ 3 LETÉ SERVISNÍ PODPORY BEZPEČNÉHO PERIMETRU odpovídá ve všech parametrech

2.) Navržené POVÝŠENÍ MANAGEMENTU METODOU TRADE-IN odpovídá ve všech parametrech.

Povýšení managementu řešení metodou trade-in včetně 3 leté podpory

Povýšení managementu:

Technologie	Množství	Číslo výrobce	Popis
CheckPoint	2	CPAP-NGSM5150	Smart-1 5150 Next Generation Security Management Appliance for 150 GWs (SmartEvent & Compliance 1 year)
CheckPoint	2	CPSB-DMN-25	25 domains package for Multi-domain Security Management

Tříletá podpora výrobce:

Technologie	Množství	Číslo výrobce	Popis
CheckPoint	3	CPCES-CO-PREMIUM	Collaborative Enterprise Support Premium, 1year, HW

3.) BEZPEČNOSTÍ SERVISNÍ SUBSKRIPCE odpovídají ve všech parametrech

Zajištění 3 leté servisní podpory výrobce technologií bezpečného perimetru:

- Mobile Threat Prevention Blade
- Capsule WorkSpace a Mobile Threat Prevention Blade

- Enterprise Based Protection – NGTX

Support a servis boxů musí zahrnovat tyto komponenty výrobce:

Technologie	Množství	Číslo výrobce	Popis
CheckPoint	1	CPCES-CO-PREMIUM	Collaborative Support Premium
CheckPoint	1	CPEBP-NGTX	Enterprise Based Protection - Next Generation Threat Extraction Package kage Including IPS, APCL, URLF, AV, ABOT, ASPM, TX and TE blades
CheckPoint	3	CP-CPSL-WORK-CONTRACT-3Y	Check Point Capsule Workspace and Docs subscription for 1 year
CheckPoint	3	CP-MTP-USR-3Y	Check Point Mobile Threat Prevention per user subscription for 1 year

4.) IMPLEMENTACI zahrnuje:

Úplnou implementaci v datovém centru Magistrátu hl. m. Prahy. Úplná implementace zahrnuje:

- Dodávku a oživení v prostředí DC;
- Migraci stávajících politik
- Optimalizaci stávajících politik
- Napojení na monitoring
- Zprovoznění zálohování konfigurace

Ověření podmínek upgrade a specifikace potřebných změn před provedením upgrade

Prověření všech skutečností, které mohou blokovat upgrade. Návrh řešení, možnosti vyřešení konkrétních problémů ještě před migrací. Jde např. o:

- IPS package version
- non-Unicode characters
- DHCP relay
- OPSEC produkty

Výběr postupu upgrade

Z možných variant upgrade vybrat způsob, který bude znamenat minimální dopad na produkci a zároveň zajistí integritu prostředí během migrace. Je potřeba brát v úvahu, že jde o management HA prostředí.

Simulace upgrade

Vybraný způsob migrace otestovat v neprodukčním prostředí

Sestavení implementačního plánu

Před migrací bude připraven implementační plán, který přesně popíše:

- „Odpovědnost“ – kdo je odpovědný za úspěšnou realizaci daného kroku

- „Podmínky realizace“ - podmínky, které musí být splněny, aby bylo možné zahájit práce na daném kroku.
- „Kontrolní body“ - popis kontrol, které se ověřují pro určení úspěšnosti prací. Jejich úspěšné splnění umožní postup na další krok prací.
- „Havarijní plán“ - popis možných rizik, které z prací, souvisejících s aktuálním krokem, plynou a způsob jejich řešení, případně roll-back plán.

Optimalizace politik pro R80

- Access Politiky
- Threat prevention politiky

Pilotní provoz

Při tomto kroku se nebudou realizovat žádné konkrétní plánované práce. Systém by měl běžet ve zprovozněném stavu po určité, předem dohodnuté, testovacím období (14 dní), po které se bude v provozním režimu zjišťovat, zda vše funguje dle předpokladů a požadavků. Pouze v případě, že se objeví nějaké problémy nebo ze strany zákazníka vyvstanou požadavky na úpravu funkce, se bude realizovat technický zásah.

Konfigurace zálohování a monitoringu nového prostředí

Vytvoření projektové dokumentace

Implementační práce budou provedeny v rozsahu 25 člověkodnů