# Hlavní město Praha

# RADA HLAVNÍHO MĚSTA PRAHY

# U S N E S E N Í

Rady hlavního města Prahy

číslo 2962
ze dne 18.12.2023

*k záměru odboru informatických činností MHMP na realizaci veřejné zakázky "Obnova podpory výrobce pro technologie Check Point" a k návrhu na úpravu rozpočtu v kapitole 07 - Bezpečnost a v kapitole 1016 - Pokladní správa v roce 2023*

**Rada hlavního města Prahy**

**I. s c h v a l u j e**

1. záměr realizace veřejné zakázky dle přílohy č. 1 tohoto usnesení
2. úpravu rozpočtu vlastního hl.m. Prahy na rok 2023 dle přílohy č. 2 tohoto usnesení
3. úpravu rozpočtu vlastního hl.m. Prahy na rok 2023 dle přílohy č. 3 tohoto usnesení

**II. r o z h o d u j e**

o zahájení zadávacího řízení po splnění zákonných podmínek

**III. u k l á d á**

1. MHMP - OIC MHMP
   1. realizovat zadávací řízení k veřejné zakázce "Obnova podpory výrobce pro technologie Check Point" dle přílohy č. 1 tohoto usnesení

Kontrolní termín: 31.1.2024

2. radnímu RNDr. Danielovi Mazurovi, Ph.D.
   1. předložit Radě HMP návrh na rozhodnutí o výběru dodavatele

      Kontrolní termín: 29.2.2024
3. MHMP - ROZ MHMP
   1. realizovat rozpočtové opatření dle bodu I.2. a I.3. tohoto usnesení

      Termín: 29.12.2023

doc. MUDr. Bohuslav Svoboda, CSc. v. r.
primátor hl.m. Prahy

MUDr. Zdeněk Hřib v. r.
I. náměstek primátora hl.m. Prahy

Předkladatel: primátor hl.m. Prahy
Tisk: R-49692
Provede: MHMP - OIC MHMP, radní RNDr. Daniel Mazur, Ph.D., MHMP - ROZ MHMP
Na vědomí: odborům MHMP

**Záměr realizovat veřejnou zakázku dle ustanovení *Hlavy I., článek 6 písm. e)* Pravidel pro zadávání veřejných zakázek v podmínkách hlavního města Prahy**

(nad 20 000 000 Kč bez DPH)

**Odbor MHMP: Odbor informatických činností** **Pořadové č. záměru: 75/23/OIC**

| **Název veřejné zakázky** | **Obnova podpory výrobce pro technologie Check Point** |
|---|---|
| **Předmět plnění** | Předmětem veřejné zakázky na služby je obnova podpory výrobce pro stávající zařízení, vč. příslušenství. Tato podpora je vázána ke konkrétním technologickým celkům, které lze rozdělit do následujících oblastí, a to do 30/6/2026 pro technologie dle specifikace a), b), c), f) a g); do 31/3/2025 pro technologie d) a e).<br><br>**a) Check Point SG15600 – 2 ks**<br>o externí firewall MHMP, který odděluje sítě Internet, MepNet a CMS2 od externích DMZ a interconnectu vedoucího k interním sítím,<br>o využívané funkcionality: Firewall, Antibot, AntiVirus, IPS, Application Control, URL filtering, Identity Awareness.<br>**b) CheckPoint SG5400 – 5 ks**<br>o firewelly určené pro lokality MHMP (dosud využity pro PoC na MČ), nově využity v lokalitách MHMP pro segmentaci<br>o lokalita Bohdalec – 2 ks:<br>▪ určen pro interní segmentaci v rámci lokality MHMP,<br>▪ využívané funkcionality – Firewall, Antibot, AntiVirus, IPS, Application Control, URL filtering, Identity Awareness.<br>o KACPU – 2 ks<br>▪ určen pro externí segmentaci v rámci lokality MHMP,<br>▪ využívané funkcionality – Firewall, Antibot, AntiVirus, IPS, Application Control, URL filtering.<br>o Zbraslav – 1 ks<br>▪ hraniční Mepnet firewall pro MMČ Zbraslav,<br>▪ využívané funkcionality – Firewall, Antibot, AntiVirus, IPS, Application Control, URL filtering.<br>**c) Check Point Endpoint**<br>o určeno pro zabezpečení koncových stanic,<br>o zahrnuje:<br>▪ 1 x Endpoint Management Server<br>▪ 2 x Endpoint Policy Server<br>▪ 3 300 x licence na koncová zařízení<br>o využívané funkcionality –Antibot, AntiVirus, IPS, Application Control, URL filtering, Threat Emulation.<br>**d) SandBlast TE1000x – 2 ks** |

| | |
|---|---|
| | o ZeroDay ochrana emailové komunikace a koncových stanic<br>o využívané funkcionality – Threat Emulation<br>**e) SandBlast TE2000x – 2 ks**<br>o ZeroDay ochrana koncových stanic<br>o využívané funkcionality – Threat Emulation<br>**f) Check Point Smart-1**<br>o centrální managementy a log servery pro Check Point bezpečnostní brány,<br>o přes tyto appliance jsou spravovány veškerá Check Point zařízení dle bodu a), b), d) a e) předmětu VZ.<br>**g) Check Point SmartEvent**<br>o centrální korelační nástroj pro Check Point prostředí,<br>o pokročilé řešení na korelaci událostí z bezpečnostních bran,<br>o tento produkt je využíván BEZ pro identifikaci bezpečnostních incidentu. |
| **CPV kód** | 72250000-2 - Systémové a podpůrné služby |
| **Zastoupení zadavatele v řízení** | NE |
| **Zdůvodnění potřeby veřejné zakázky** | Základním bezpečnostním prvkem perimetrické ochrany ICT prostředí MHMP vůči kybernetickým hrozbám a útokům jsou technologie NGTP (New Generation Threat Pervention) plnící funkce NG perimetrického firewallu s technologií sanboxu. Konkrétně MHMP využívá NGPT - dle předmětu VZ a) a b), vendora Check Point, dlouhodobě patřícího mezi leadery v oblasti perimetrických bezpečnostních technologií (Gartner Magic Quandrant).<br>NGPT zajišťují bezpečnostní analýzu datových toků procházejících perimetrem z Internetu a MepNetu a zajišťují i funkci "virtual patching" pro ochranu systémů MHMP na perimetru, u nichž nelze příslušné zranitelnosti řešit na úrovni systému nebo aplikace (zastaralost systému, neexistence oprav výrobce apod.). NGFW jsou integrovány s dalšími bezpečnostními technologiemi (SIEM, sandbox, apod.).<br>V rámci ochrany síťového prostředí MepNet provozuje MHMP na vybraných lokalitách prvky perimetrické ochrany a bezpečnostního dohledu síťového provozu prostředí MepNet s možností ochrany i interního síťového prostředí dané lokality (včetně segmentace sítí) – bod b) předmětu VZ. NGPT firewally zajišťují bezpečnostní analýzu datových toků procházejících rozhraním MepNetu a dané lokality, s možností stejných funkcí i pro vnitřní sítě lokality.<br>MHMP provozuje v souladu s doporučeními NÚKIB funkcionalitu centrálního sandboxu založené na technologii Check Point Sandblast, která je plně integrovaná s NGTP - dle předmětu VZ d) a e). Sandbox je klíčovou bezpečnostní technologií pro automatizovanou analýzu chování škodlivého kódu, resp. podezřelého nebo nedůvěryhodného kódu. Tento kód je technologií sandbox analyzován a popřípadě proveden (detonován) |

| | |
|---|---|
| | v bezpečném kontrolovaném prostředí. Sandbox analyzuje chování nedůvěryhodného kódu a dopady, které by měl běh nedůvěryhodného kódu v produkčním prostředí MHMP. Technologie Sandblast je plně integrována do systémů ochrany perimetru a ochrany koncových stanic a tyto systémy využívají sandbox k ověření chování a bezpečnosti nedůvěryhodných kódů a současně jsou tyto výsledky poskytovány dalším systémům kybernetické bezpečnosti (SIEM).<br><br>Pro zajištění bezpečnosti koncových stanic provozuje MHMP systém Check Point Endpoint který na koncových stanicích zajišťuje funkci preventivní ochrany proti kybernetickým hrozbám a útokům, včetně ochrany proti škodlivému kódu. Tento systém pracuje v kooperaci s EDR systémem Fidelis, přičemž CHKP Endpoint zajišťuje funkce prevence (ochrany, EPP) a Fidelis EDR zajišťuje funkce detekce, mitigace, investigace a remediace. Jedná se tedy o komplexní systém ochrany koncových bodů proti kybernetickým hrozbám. Systém je dále integrován do dalších bezpečnostních systémů (SIEM). V současnosti MHMP disponuje licencemi pro 3 300 koncových bodů.<br><br>Celý systém je centrálně řízen a monitorován managmentem služeb – technologie f) a g) dle této VZ.<br><br>Licence a technická podpora prvků na ochranu perimetru končí 31.12.2023. Pro technologii dle předmětu e) této VZ končí 31.3.2024.<br><br>Zajištění obnovy podpory a licencí je nezbytné pro zachování stávajících funkcionalit infrastruktury MHMP a jejich vypršení by vedlo k degradaci či úplnému výpadku kritických bezpečnostních funkcí.<br><br>Pro tyto prvky infrastruktury je nutné obnovit maintenance výrobce, aby byla zachována funkcionalita řešení, licenční pokrytí potřeb MHMP, zajištěna kontinuální obnova software včetně bezpečnostních patchů a technická podpora provozu pro HW včetně zajištění jeho výměny s garancí SLA.<br><br>Neprodloužení této kategorie podpor a obnovy licencí by tak ve výsledku způsobilo zastarání Threat-intel databází a nefunkčnost systémů vůči novým kybernetickým hrozbám, výpadek bezpečnostní ochrany koncových bodů (vypršení licencí) a znemožnilo garantovat nastavená SLA (jak OIC, tak dodavatelům), která jsou často vázána právě na podporu ze strany výrobce. |
| **Analýza trhu** | Datum vzniku analýzy trhu:<br><br>Nebyla provedena. Jedná se o zajištění podpory stávající technologie, tj. byla poptána indikace pro zajištění obnovy podpory a stávajících licencí od výrobce technologie. |
| **Byla použita předběžná tržní konzultace?** | NE – technické požadavky vyplývají ze stávajícího stavu infrastrukturních prvků, tj. byly jasně definovány prvky určené pro obnovu podpory. |

| | |
|---|---|
| **Cíl veřejné zakázky** | Cílem veřejné zakázky je zajistit podporu výrobce pro komplexní systém zabezpečení perimetru sítě.<br>Podpora pro veškeré prvky budou aktivovány následovně - a to do 30/6/2026 pro technologie dle specifikace a), b), c), f) a g); do 31/3/2025 pro technologie d) a e). |
| **Koncepční materiál nebo rozhodnutí na základě kterého se veřejná zakázka zadává** | ICT Koncepce MHMP na období 2019 – 2023, která byla schválena usnesením Rady HMP č. 75 ze dne 20. 1. 2020.<br>o digitální služby a otevřená městská data,<br>o efektivnější provoz ICT,<br>o vyšší stabilita a bezpečnost ICT.<br>o koncepce eGovernmentu,<br>o související legislativa a normy.<br>Záměr byl doporučen k realizaci komisí RHMP pro ICT na jejím 6. jednání dne 18.10.2023. |
| **Druh veřejné zakázky podle předmětu a předpokládané hodnoty** | Veřejná zakázka na služby;<br>nadlimitní veřejná zakázka. |
| **Předpokládaná hodnota[1] a datum stanovení** | 29 231 487 Kč bez DPH, stanovena dne 31.10.2023 |
| **Způsob stanovení předpokládané hodnoty[2]** | Předpokládaná hodnota byla zadavatelem stanovena na základě údajů z indikativní cenové kalkulace od výrobce technologie - společnost Check Point Software Technologies, s.r.o., dne 26/09/2023, a to následovně:<br>a) Check Point SG15600 – ve výši 5 665 579 Kč bez DPH<br>b) Check Point SG5400 – ve výši 2 934 998 Kč bez DPH<br>c) Check Point Endpoint – ve výši 11 409 774 Kč bez DPH<br>d) SandBlast TE1000x – ve výši 2 231 952 Kč bez DPH<br>e) SandBlast TE2000x – ve výši 2 932 576 Kč bez DPH<br>f) Check Point Smart-1 – ve výši 3 627 136 Kč bez DPH<br>g) Check Point SmartEvent – ve výši 429 472 Kč bez DPH<br>**Výsledná předpokládaná hodnota je 29 231 487 Kč bez DPH.** |
| **Druh zadávacího řízení** | otevřené řízení |
| **Požadavky na prokázání způsobilosti a kvalifikace** | Prokázání veškeré základní způsobilosti stanovené v § 74 ZZVZ a profesní způsobilosti dle § 77 odst. 1 ZZVZ, technickou kvalifikaci dle § 79, odst. 2 písm. b), d) ZZVZ. |
| **Způsob hodnocení** | Ekonomická výhodnost nabídky hodnocená na základě nejnižší nabídkové ceny. |
| **Kritéria hodnocení** | Nejnižší nabídková cena v Kč bez DPH (váha 100%). |

[1] Při stanovení předpokládané hodnoty byla brána v úvahu všechna možná spolu související plnění ve smyslu zejm. ust. § 16 a násl. ZZVZ; PH je stanovena v souladu s ustanovením § 16 a násl. ZZVZ; bližší údaje obsahuje dokumentace VZ.

[2] Zejm. s ohledem na ustanovení § 16 odst. 6 ZZVZ.

| | |
|---|---|
| **Způsob financování** | Financování bude realizováno z rozpočtu odboru OIC MHMP celkem ve výši 35 370 099,27 Kč s DPH následovně:<br>rok 2024:<br>ORJ 0740 ODPA 6171 POL 5168 ORG 0041946 Kč 35 370 099,27 |
| **Předpokládaný termín zahájení řízení k veřejné zakázce** | prosinec 2023 |
| **Předpokládaná doba realizace veřejné zakázky** | Předpokládané datum uzavření smlouvy je leden 2024 s dobou poskytování podpory do 30. 6. 2026. |
| **Informace, zda se připouští varianty nabídky dle § 102 ZZVZ** | Varianty nabídky se nepřipouští. |
| **Odůvodnění nerozdělení nadlimitní veřejné zakázky na části** | Zadavatel samotný předmět plnění na části nerozdělil, přičemž k tomuto kroku přistoupil z důvodu jeho komplexnosti a návaznosti jednotlivých částí předmětu veřejné zakázky. |
| **Odůvodnění použití jiných komunikačních prostředků při podání nabídky namísto elektronických prostředků** | Celé zadávací řízení bude realizováno v souladu se ZZVZ výhradně elektronicky prostřednictvím elektronického nástroje Tender Arena. |
| **Odůvodnění neodeslání předběžného oznámení** | Předběžné oznámení bude odesláno do Věstníku veřejných zakázek a do Úředního věstníku EU. |
| **Odůvodnění nejmenování komisí** | Komise budou jmenovány. |

*Příloha č. 2 k usnesení Rady HMP č. 2962 ze dne 18. 12. 2023*

## Úprava rozpočtu vlastního hlavního města Prahy ve vazbě na vlastní zdroje HMP (včetně OPP)

| II. Úprava rozpočtu výdajů včetně tř. 8 - financování (strana DAL) | | | | | | |
|---|---|---|---|---|---|---|
| **Uprava rozpočtu běžných výdajů** | | | | | | |
| **Odbor/Organizace** | **Číslo akce** | **Účel / Název akce** | **ODPA** | **UZ** | **ORJ** | **Úprava rozpočtu (v tis. Kč)** |
| ROZ HMP | 0091601770000 | Neúčelová rezerva | 6409 | 3 | 1016 | -25 900,00 |
| OIC MHMP | 0041946 | Bezpečnost IS/ICT | 6171 | 0000 | 0740 | 25 900,00 |
| | | **C e l k e m** | | | | **0,00** |

*Příloha č. 3 k usnesení Rady HMP č. 2962 ze dne 18. 12. 2023*

## Úprava rozpočtu vlastního hlavního města Prahy ve vazbě na vlastní zdroje HMP (včetně OPP)

| II. Úprava rozpočtu výdajů včetně tř. 8 - financování (strana DAL) | | | | | | |
|---|---|---|---|---|---|---|
| **Úprava rozpočtu běžných výdajů - mimo pol. 5347** | | | | | | |
| **Odbor/Organizace** | **Číslo akce** | **Název akce** | **ODPA** | **ÚZ** | **ORJ** | **Úprava rozpočtu (v tis. Kč)** |
| OIC MHMP | 0040985 | Projekty rozvoje IS MP HMP | 6171 | 0000 | 0740 | -9 470,10 |
| OIC MHMP | 0041946 | Bezpečnost IS/ICT | 6171 | 0000 | 0740 | 9 470,10 |
| | | **C e l k e m** | | | | **0,00** |

## Důvodová zpráva k tisku č. R-49692

**Návrh na schválení záměru realizace veřejné zakázky „Obnova podpory výrobce pro technologie Check Point“**

Předmětem nadlimitní veřejné zakázky zadávané v otevřeném řízení je obnova podpory výrobce pro stávající zařízení, vč. příslušenství, a to do 30/06/2026, pro položky d) a e) do 31/3/2025. Tato podpora je vázána ke konkrétním technologickým celkům, které lze rozdělit do následujících oblastí:

| | | | |
|---|---|---|---|
| a) | Check Point SG15600 | – | perimetrické NGPT firewally (2ks) |
| b) | Check Point SG5400 | – | NGPT firewally pro interní/externí segmentaci a další bezpečnostní funkce pro lokality MHMP (5ks) |
| c) | Check Point Endpoint | – | bezpečnostní ochrana koncových stanic (EPP) – 3300 licencí pro koncové stanice, Policy Server, Management Server |
| d) | SandBlast TE1000x | – | ochrana emailové komunikace, včetně ochrana proti útokům typu ZeroDay (sandboxy, Threat Emulation) (2ks) |
| e) | SandBlast TE2000x | – | ochrana koncových stanic, včetně ochrana proti útokům typu ZeroDay (sandboxy, Threat Emulation) (2ks) |
| f) | Check Point Smart-1 | – | centrální management pro používané CheckPoint bezpečnostní technologie |
| g) | Check Point SmartEvent | – | pokročilé řešení na korelaci událostí z bezpečnostních bran, řešení je využíváno BEZ při vyhodnocování bezpečnostních incidentů |

Základním bezpečnostním prvkem perimetrické ochrany ICT prostředí MHMP vůči kybernetickým hrozbám a útokům jsou technologie NGTP (New Generation Threat Pervention) plnící funkce NG perimetrického firewallu s technologií sandboxu. Konkrétně MHMP využívá NGPT - dle předmětu VZ a) a b), vendora Check Point, dlouhodobě patřícího mezi leadery v oblasti perimetrických bezpečnostních technologií (Gartner Magic Quandrant).

NGPT zajišťují bezpečnostní analýzu datových toků procházejících perimetrem z Internetu a MepNetu a zajišťují i funkci "virtual patching" pro ochranu systémů MHMP na perimetru, u nichž nelze příslušné zranitelnosti řešit na úrovni systému nebo aplikace (zastaralost systému, neexistence oprav výrobce apod.). NGFW jsou integrovány s dalšími bezpečnostními technologiemi (SIEM, sandbox, apod.).

V rámci ochrany síťového prostředí MepNet provozuje MHMP na vybraných lokalitách prvky perimetrické ochrany a bezpečnostního dohledu síťového provozu prostředí MepNet s možností ochrany i interního síťového prostředí dané lokality (včetně segmentace sítí) – bod b) předmětu VZ. NGPT firewally zajišťují bezpečnostní analýzu datových toků procházejících rozhraním MepNetu a dané lokality, s možností stejných funkcí i pro vnitřní sítě lokality.

MHMP provozuje v souladu s doporučeními NÚKIB funkcionalitu centrálního sandboxu založené na technologii Check Point Sandblast, která je plně integrovaná s NGTP - dle předmětu VZ d) a e). Sandbox je klíčovou bezpečnostní technologií pro automatizovanou analýzu chování škodlivého kódu, resp. podezřelého nebo nedůvěryhodného kódu. Tento kód je technologií sandbox analyzován a popřípadě proveden (detonován) v bezpečném kontrolovaném prostředí. Sandbox analyzuje chování nedůvěryhodného kódu a dopady, které by měl běh nedůvěryhodného kódu

v produkčním prostředí MHMP. Technologie Sandblast je plně integrována do systémů ochrany perimetru, ochrany mailové komunikace a ochrany koncových stanic. Tyto systémy využívají sandbox k ověření chování a bezpečnosti nedůvěryhodných kódů a současně jsou tyto výsledky poskytovány dalším systémům kybernetické bezpečnosti (SIEM).

Pro zajištění bezpečnosti koncových stanic provozuje MHMP systém Check Point Endpoint – dle předmětu VZ c), který na koncových stanicích zajišťuje funkci preventivní ochrany proti kybernetickým hrozbám a útokům, včetně ochrany proti škodlivému kódu. Tento systém pracuje v kooperaci s EDR systémem Fidelis, přičemž CHKP Endpoint zajišťuje funkce prevence (ochrany, EPP) a Fidelis EDR zajišťuje funkce detekce, mitigace, investigace a remediace. Jedná se tedy o komplexní systém ochrany koncových bodů proti kybernetickým hrozbám. Systém je dále integrován do dalších bezpečnostních systémů (SIEM). V současnosti MHMP disponuje licencemi pro 3 300 koncových bodů.

Celý systém je centrálně řízen a monitorován managmentem služeb – technologie f) a g) dle této VZ.

Licence a technická podpora prvků na ochranu perimetru končí 31.12.2023. Pro technologii dle předmětu e) této VZ končí 31.3.2024.

Zajištění obnovy podpory a licencí je nezbytné pro zachování stávajících funkcionalit infrastruktury MHMP a jejich vypršení by vedlo k degradaci či úplnému výpadku některých funkcí.

Pro tyto prvky infrastruktury je nutné obnovit maintenance výrobce, aby byla zachována nepřetržitá funkcionalita řešení (průběžné dodávky Threat feed a aktualizací bezpečnostních engine), bylo zajištěno licenční pokrytí potřeb MHMP, zajištěna kontinuální obnova software včetně bezpečnostních patchů a technická podpora provozu pro HW včetně zajištění jeho výměny s garancí SLA.

Neprodloužení této kategorie podpor a obnovy licencí by tak ve výsledku způsobilo zastarání Threat-intel databází a nefunkčnost systémů vůči novým kybernetickým hrozbám, výpadek bezpečnostní ochrany koncových bodů (vypršení licencí) a znemožnilo garantovat nastavená SLA (jak OIC, tak dodavatelům), která jsou často vázána právě na podporu ze strany výrobce.

Záměr vychází ze schválené ICT koncepce MHMP na období 2019 – 2023, která byla schválena usnesením Rady HMP č. 75 ze dne 20. 1. 2020.
Záměr byl doporučen k realizaci komisí RHMP pro ICT na jejím 6. jednání dne 18. 10. 2023.

**Předpokládaná hodnota veřejné zakázky: 29 231 487 Kč bez DPH**

Financování bude realizováno z rozpočtu odboru OIC MHMP celkem ve výši 35 370 099,27 Kč s DPH následovně:

rok 2024:
ORJ 0740 ODPA 6171 POL 5168 ORG 0041946 Kč 35 370 099,27

Zajištění financování VZ bude realizováno následovně:

- vzhledem ke skutečnosti, že odbor OIC MHMP nedisponuje aktuálně dostatkem finančních prostředků k zajištění financování VZ, bude financování zajištěno převodem finančních prostředků z neúčelové rezervy v kap. 1016 dle přílohy č. 2 tohoto usnesení,

- rozpočtovou úpravou mezi akcemi rozpočtu OIC MHMP v kap. 0740, dle přílohy č. 3 tohoto usnesení.

Vzhledem k časové náročnosti v rámci schvalovacího řízení, bude financování realizováno v roce 2024, částka celkem ve výši 35 370 099,77 Kč, bude předmětem převodu do rozpočtu provozních výdajů odboru OIC MHMP _ kap 0740, v r. 2024.

Přílohy:

1. Záznam o stanovení předpokládané hodnoty
2. Zápis z jednání komise RHMP pro ICT ze dne 18.10.2023