PRA HA PRA GUE PRA GA PRA G	HLAVNÍ MĚSTO PRAHA MAGISTRÁT HLAVNÍHO MĚSTA PRAHY KOMISE RHMP PRO ICT

ZÁPIS
z jednání Komise RHMP pro ICT
č. 18 ze dne 16. 02. 2021

Účastníci:

Přítomni	Ondřej Kallasch (předseda), Jiří Károly, Jan Ladin, Aneta Heidlová, Michal Šorel, Petr Říha, Jan Rambousek, Radomír Nepil, Markéta Horská (tajemnice)
Omluveni	Milan Krch, Jan Žáček
Neomluveni	
Hosté	Jiřina Onderčová, Petr Matuš

Program:

1) Úvod	O. Kallasch
2) Nákup licencí a obnova technologické podpory systému ochrany koncových stanic	J. Károly
3) Obnova technologické podpory systému zabezpečení síťového prostředí	J. Károly
4) Zajištění nezbytné obslužné infrastruktury pro velké lokality MHMP	J. Károly
5) Různé	

Projednáno:

1) Úvod

Jednání zahájil předseda komise O. Kallasch, hlasováním o programu jednání komise a schválení hostů.

Hlasování: 6-0-0 (pro-proti-zdržel se). Program byl schválen.

2) Nákup licencí a obnova technologické podpory systému ochrany koncových stanic

J. Károly uvedl projednávaný bod a rozvedl odpovědi na obdržené dotazy. Předmětem veřejné zakázky je zajištění technologické servisní podpory výrobce pro technologii, která zabezpečuje preventivní ochranu koncových stanic (2 800 stanic). Systém zajišťuje nejen antivirovou ochranu, ale i další pokročilé funkce zabezpečení koncové stanice označované jako Endpoint Detection Systém – tj. zabezpečení síťového prostředí MHMP proti spamu, virům, malware, zneužití a cílenému kybernetickému útoku.
Cílem zakázky je zabezpečit chod na stávajících koncových stanicích (2 800 licencí) a dodávka řešení (500 licencí), které bude chránit koncové uživatele a mail server před spamy, viry, malware a zneužitím dat. Řešení je zvoleno tak, aby bylo kompatibilní se stávajícím zabezpečením koncových stanic. Doplněním těchto licencí bude zajištěno homogenní prostředí ochrany koncových stanic. Zároveň bude sjednoceno období podpory produktu.

Diskuse:

Šorel: Měl bych dotaz, jelikož se obojí týká bezpečnostních technologií pro ochranu KS a DC, jsou ještě nějaké mimo tyto, které využíváme? Nebo je toto opravdu pokrytí veškerého bezpečnostního sw MHMP.

Károly: Toto není kompletní výčet. Využíváme další systémy jako SIEM a Fidelis, požádám paní Onderčovou.

Onderčová: Technologie v záměru se zabývají správou perimetru, tedy na ochranu sítě. Jsou i další technologie komplementární, jako BVS pro zjišťování a další zpracování informací, Fidelis a F5 pro load balancing. Systém technologií je širší, jedná se o 5 doplňujících se bloků.

Šorel: V záměru ohledně FW se jedná o jednu technologii?

Onderčová: Je to souhrn 3 technologií, které se paralelně doplňují. Nastavená pravidla na interním FW, s tím korelují pravidla na externím FW a SandBlast provádí operace nad těmito technologiemi.

Šorel: SandBlast appliance slouží pro ochranu koncových stanic a tohle je součást jiné technologie kooperující s FW. Je i analýza provozu sítě v rámci této technologie, nebo je ještě něco jiného sledující provoz na sítích? Resp. co všechno tato součást SandBlastu dělá?

Onderčová: V prvním záměru se jedná o licence pro KS, zjednodušeně antivir chránící KS standardními způsoby a dále komunikuje o úroveň výš. Druhý záměr se skládá ze 4 prvků: ochrana interního FW (ochrana interní část MHMP), 2 fyzické appliance s navázanými sw, část chránící externí FW od prostředí internetu a management, který vše spravuje. Poté ještě SandBlast chránící emailovou poštu, stahování souborů z internetu, spouštění z flash disků. Vše je v detailu důvodové zprávy, který můžeme dodat.

Károly: Endpointy na KS, při stahování souboru z pošty či rozbalování souboru z webu, se spojí s DC a podívá se co stahujete a může Vás zastavit. V rámci DC jsou zakoupeny dva sandboxy a potřebujeme v rámci druhého záměru dokoupit maintenance. V loňském roce jsme žádali o nákup dalších dvou sandboxů, což bylo schváleno a zakoupeno. Aktuálně byly sandboxy převezeny do ČR a v průběhu 14 dnů budou nasazeny do DC. Chceme navýšit výkonnost pro rychlejší kontrolu vstupů a výstupů na KS. Záměry jdou ruku v ruce a jsou rozděleny, jeden je na KS a druhý se týká sítě a DC.

Usnesení:

„Komise RHMP pro ICT doporučuje záměr s názvem Nákup licencí a obnova technologické podpory systému ochrany koncových stanic, který je přílohou tohoto usnesení ke schválení.“

Hlasování: 6-0-0 (pro-proti-zdržel se). Usnesení bylo přijato.

3) Obnova technologické podpory systému zabezpečení síťového prostředí

J. Károly uvedl projednávaný bod. Předmětem veřejné zakázky je zajištění technologické servisní podpory výrobce pro technologii, která zabezpečuje ochranu síťového prostředí MHMP:

- externí firewall,
- interní firewall,
- multidoménový managment,
- sandblast.

Magistrát hlavního města Prahy využívá pro zabezpečení provozu síťového prostředí komplexní technologii, která je složena z několika dílčích celků, které zabezpečují jednotlivé části síťového prostředí. V roce 2021 bude končit podpora jednotlivých komponent v rozmezí od 31/3/2021 – 16/9/2021. Technologie jsou umístěny v DC4 a v DC5 – celkem 4 fyzické brány appliance next-generation firewall (NGFW) kombinuje tradiční firewallovovu technologie a další funkce efektivní obrany proti kyberhrozbám a 2 fyzické apppliance proti pokročilým hrozbám (ATP).

Cílem této zakázky je sjednotit M&S u jednotlivých technologií tak, aby byla zajištěna kontinuita HW a SW podpory jako celku.

Usnesení:

„Komise RHMP pro ICT doporučuje záměr s názvem Obnova technologické podpory systému zabezpečení síťového prostředí, který je přílohou tohoto usnesení ke schválení“

Hlasování: 6-0-0 (pro-proti-zdržel se). Usnesení bylo přijato.

4) Zajištění nezbytné obslužné infrastruktury pro velké lokality MHMP

14:24 se k jednání Komise RHMP pro ICT připojil pan Rambousek

J. Károly představili projednávaný bod a zdůvodnil záměr pomocí prezentace. Předmětem plnění je dodávka technologické infrastruktury (serverů) do jednotlivých lokalit MHMP, které zvýší komfort a dostupnost služeb koncových uživatelů. Stávající vybavení technologické infrastruktury pro obsluhu koncových stanic(uživatelů) je dnes provozováno na velmi zastaralé infrastruktuře bez jakékoliv podpory a jakýkoliv výpadek má za následek výpadek koncových stanic v dané lokalitě a tím paralyzování chodu úřadu. V tomto kontextu byla navržena technologická infrastruktura obsluhy větších lokalit, která umožní provoz nezbytných služeb v dané lokalitě, sníží závislost na konektivitě dané lokality a tím přinese uživatelům a správcům zvýšení kvality a dostupnosti služeb.

Diskuse:

Rambousek: Mohu to chápat jako upgrade již existující redundance, když DC4 i DC5 je nadimenzováno i na situaci nerealizace této akce? Další upgrady DC budou respektovat současný stav, kdyby virtualizované servery nad 100 uživatelů instalovány nebyly, tak upgrade DC bude probíhat jako nadstavba pro současnou špičku, jak jsou na to všichni zvyklí? Je to nad úroveň současné redundance?

14:32 se k jednání Komise RHMP pro ICT připojil pan Nepil

Matuš: Jsou dva přístupy, kdy můžeme služby centralizovat a zbavit se serverů na lokalitách. Nepřináší nám to náročnost jednotlivých linek, které generují velké náklady. Chceme na lokalitách servery mít a zbavit se závislosti na konektivitě. Vedli jsme diskusi o velikosti lokality, kdy jsme se rozhodli řešit to jen u největších lokalit a zbytek bude závislý na redundanci DC.

Rambousek: Dle Lifecycle managementu DC se přihlédne, že nebude potřeba je škálovat do míry jako teď. Virtualizované servery to částečně pokryjí v lokalitách nad 100 uživatelů a investice se na to přesunou nebo budou investice na všech lokalitách stejné do budoucna?

Matuš: Nebudou, závisí na vytíženosti linky. Nechceme tuto architekturu rozšiřovat do všech lokalit, chceme to jen na velkých lokalitách, kdy početně jsme se shodli na 100 uživatelích.

Rambousek: Dělali jste assessment, co vyjde lépe z dlouhodobé udržitelnosti i do budoucna? Pokud byste zkapacitnili prostupy, které jsou důležité a nedostačují nebo je výhodnější varianta tato předkládaná?

Matuš: Nedělali jsme to, abych Vám řekl matematický výstup. Server nás dnes stojí 260 tisíc korun, kdy nakupujeme support na 5 let. Je zavřená cesta navyšováním konektivity. Shodli jsme se jít cestou mít v lokalitách redundanci.

Kallasch: Za mě osobně to dává smysl dělat to tímto způsobem. Můžeme posílit linky, ale není to nutné je posílit po celou dobu. Nevyužíváme je 24 h v kuse, za sebe tam vidím úsporu v konektivitě. Dívat se na to způsobem, kolik bychom platili poskytovatelům za garantovanou konektivitu, že to linka vydrží. Nebo zda když máme lokalitu, připravíme to v noci a pak to spustíme. V tom vidím hlavní ukazatel záměru.

Rambousek: Nejsem si jistý, zda užívají úředníci NTB, které si odnáší domů (odhlédnu od současné situace). Nemůžete naplánovat aktualizaci na noc a škálovat rozložení zátěže na noc, kdy úředníci nepracují?

Károly: Ohledně NTB, MHMP má 2500 zaměstnanců, je vydáno 1150 NTB a nakoupeno dalších 800 ks. Cílem je pouze jedno KZ na zaměstnance, a to mobilní zařízení. Může to být rok až dva práce tohoto typu pro kompletní výměnu zařízení. Když se dnes díváme na využití, tak 400-500 lidí denně pracuje vzdáleně.

Matuš: Nezaměřujme se jen na aktualizace, ale pokud nebude server, tak se nikdo nepřihlásí do počítače a celou lokalitu odřízneme při závislosti na DC. Pokud bude server, tak se uživatel přihlásí, může tisknout, má funkční vybavení počítače. U velkých lokalit chceme funkčnost.

Rambousek: Nepochopil jsem popis monitorovacích serverů. Mají monitorovat platformu, funkčnost a posílá tikety na HD?

Matuš: Jedná se o celomagistrátní systém monitoringu, kdy monitorujeme kompletní vrstvu. Motivace je zbavit se závislosti na současné infrastruktuře. Pokud tyto systémy vypadnou, nejsme schopni mít funkční monitoring. Vyčleňujeme stávající monitoring na dva servery ve vysoké dostupnosti a povyšujeme jej do úrovně primární síťové vrstvy, abychom výpadek viděli a monitoring jako takový zůstal funkční.

Rambousek: SLA je definováno poměrně vágně. Je zde napsáno 24/7 a 4hodinová odezva. Předpokládám, že se jedná o lepší dostupnost, aby úředníci měli agendy plně funkční. Reakční doba je opravdu stejná po celou dobu?

Matuš: Je to SLA, které aplikujeme na infrastrukturu DC, kdy nám to ekonomicky dává smysl. Do 4 hodin máme opravenou část infrastruktury.

Károly: Je to zřejmě chybně napsáno, nejedná se o nástup, ale vyřešení problému do 4 hodin od nahlášení problému.

Šorel: K SLA, to je hodně dobré SLA. Nevím, jak se pohybují ceny. Jak by to bylo s cenou, kdyby to bylo vyřešeno do začátku následujícího pracovního dne, dá se to vyčíslit?

Matuš: Úvaha, na kterou narážíte, my to SLA máme na infrastrukturu od HP, které je v DC. Tímto záměrem nesměřujeme k nákupu HP. Vezmeme jakoukoliv jinou infrastrukturu. Napadá mne, zda to svazovat s takovýmto SLA, když pak zvýhodníme HP. Vyšli jsme dle toho, co máme na infrastruktuře DC

Károly: Na těch 7 server těch lokalit bych nedával toto SLA všude, jen na ty dvě monitorovací.

Kallasch: To znamená úpravu záměru, ale možnost dát to do usnesení, abychom se k tomu nemuseli vracet. Musíme to vyspecifikovat.

Károly: Podívali bychom se na cenový rozdíl, dáme tam jiné SLA a uvidíme, zda to budeme měnit. Uděláme asi ekonomický rozpad, dáme na stůl nový záměr a schválili bychom jej per rollam.

Nepil: SLA je jedna věc, ale řešení motivuje výše pokuty. Mě by zajímala výše pokuty při nesplnění.

Károly: To už může být v rámci zadávací dokumentace, ale můžeme se k tomu vyjádřit ze standardních smluv s HP, kde jsou uvedeny smluvní pokuty.

Kallasch: Prosím uvést i pokuty v rámci zasílané dokumentace k odsouhlasení per rollam.

Károly: Dohledali jsme cenu SLA, kdy vychází 200 tis. ročně na 7 serverů.

Matuš: Diskuse v kontextu zakázky je o tom, zda ušetříme 100 tis. ročně

Kallasch: Abychom neeliminovali ostatní dodavatele.

Matuš: Motivace je to otevřít a postavíme to tak, aby se tam všichni vešli.

Kallasch: Upravit a zaslat záměr včetně doplnění cenového rozpadu.

Šorel: Šlo by rozvést, jak je na tom nasazení SCCM? Již se používá, pilotní provoz, jak jsme na tom?

Károly: Požádám pana Ladina, který má projekt na starosti.

Ladin: Ohledně SCCM proběhlo pilotní nasazení. V tuto chvíli proběhlo kromě pilotu zkontrolovaného a schváleného společností MS, zda bylo vše dodrženo. Došlo k dohodě nad roll outem do celého prostředí MHMP. První fáze je roll out na MHMP. Dnes proběhla kontrolní schůzka a je aktuálně na 2100 KS, kde je SCCM nainstalováno. Následují další fáze. Můžeme připravit informaci pro členy Komise. Je nainstalován klient a připravují se jednotlivé aplikace a prostředí se zvelebuje.

Šorel: Je termín pro instalace pro SCCM?

Ladin: Od 1.12.2020 probíhají instalace prostřednictvím SCCM. Součástí správy KZ MHMP.

Šorel: Stará se o to oddělení na OICT?

Ladin: Ano, přesně tak. Aplikací na MHMP je v aplikačním katalogu 190 a namapovaných v SCCM je cca 26. 190 aplikací je cílový stav a nevyužívají jej všichni uživatelé. V tuto chvíli je to postupná práce. Je nasazeno a instaluje se v něm. Cílem je centralizovat a narovnávat stav.

Károly: MHMP, respektive můj odbor má smlouvu s OICT na správu KS. Ke konci března/dubna chystáme změnu smlouvy, budeme měnit katalogové listy, tak aby vše bylo v pořádku. Na MHMP je jedna výjimka, INI má dva zaměstnance starající se o VIP klienty a o zbytek se stará OICT se svými lidmi.

Ladin: Změna smlouvy půjde určitě přes komisi ICT.

Usnesení:

I. **Komise RHMP pro ICT požaduje porovnání SLA všech možných dodavatelů a optimalizaci jeho nastavení v záměru. Včetně smluvní pokuty.**

II. **Komise RHMP pro ICT požaduje zaslání upraveného záměru v rámci per rollam hlasování.**

Hlasování: 8-0-0 (pro-proti-zdržel se). Usnesení bylo přijato.

5) Různé

Dynamický nákupní systém

Rambousek: Rád bych se zeptal na přehled dodavatelů?

Kallasch: Je tam 60 – 80 společností, za každý odbor je tam mírně rozdílný počet. Měl představit pan ředitel Krch. Předpokládám, že tento bod projednáme na příští Komisi pro ICT.

Károly: Aktuální DNS je tady tři roky, možná déle. Tento rok má končit a musíme jej přesoutěžit a vyhlásit to celé znovu. Na MHMP existují diskuse, zda pokračovat či nikoliv. Já jsem pro, abychom pokračovali, jen musíme správně nastavit kritéria. Tato cesta je pro MHMP daleko rychlejší oproti OVŘ.

Zajištění podpory GINIS

Nepil: Zajímá mě téma GORDIC respektive GINIS, jelikož by nám měla končit podpora za cca 6-12 měsíců. Byl bych rád, kdyby nám na příští komisi informatika představila, jakou cestou se vydá a naplní usnesení Zastupitelstva, které byly schváleny pro zahájení soutěže na ekonomický systém.

Zasedání se uskutečnilo od 14:00 do 15:01 hod.

Termín příštího řádného jednání byl stanoven na 16. 3. 2021 v 14 hodin.

Ověření zápisu:

	Jméno	**Datum**
Zapsala	Markéta Horská	16.02.2021
Schválil	Ondřej Kallasch	23.02.2021