

PRA PRA PRA PRA	HA GUE GA G	HLAVNÍ MĚSTO PRAHA MAGISTRÁT HLAVNÍHO MĚSTA PRAHY KOMISE RHMP PRO ICT
ZÁPIS z jednání Komise RHMP pro ICT č. 07 ze dne 15. 10. 2019		

Účastníci:

Přítomni	Ondřej Kallasch (předseda), Aneta Heidlová, Michal Šorel, David Vorlíček, Ladislav Tobiáš, Jan Žáček, Radomír Nepil, Petr Říha, Markéta Horská (tajemnice)
Omluveni	Jan Rambousek, Petra Burdová, Zdeněk Zajíček
Neomluveni	
Hosté	Ivo Vašíček, Petr Matuš

Program:

1) Úvod	O.Kallasch
2) ICT koncepce MHMP na období 2019-2022	D.Vorlíček / L.Tobiáš
3) Upgrade a doplnění nezbytné kapacity pro systém sběru logů	L.Tobiáš / P. Matuš
4) Zajištění podpory stávajícího a nově budovaného síťového prostředí jednotlivých lokalit	L.Tobiáš / P. Matuš

Projednáno:

1) Úvod

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

Hlasování: 7-0-0 (pro-proti-zdržel se). Schváleno.

2) ICT koncepce MHMP na období 2019 - 2025

L. Tobiáš uvedl projednávaný bod: důvodem pro vznik tohoto materiálu je potřeba MHMP v zajištění kontinuity rozvoje oblasti ICT, narovnání tematicky problematických oblastí a sjednocení poskytovaných služeb, a to na celoměstské úrovni. Cílem materiálu je dále navázat na aktivity eGovernmentu, předchozí koncepční dokumenty HMP, zvláště pak na Koncepci provozu a rozvoje informatiky MHMP a Celoměstskou koncepci rozvoje informačních systémů pro potřeby hl. m. Prahy a městských částí. ICT koncepce MHMP je tvořena několika tematicky zaměřenými dokumenty, cílem je vždy popsat: Stávající stav, Cílový stav, Návrh projektů vedoucích k cílovému stavu včetně uvedení priority a časového rámce.

V řadě případů se jedná pouze o oblasti, které je nutné řešit, nikoliv konkrétní technické/technologické řešení či formu jak bude řešeno. Předpokládáme, že to bude předmětem přípravy a realizace daných projektů. Dílčí koncepce:

- **Koncepce řízení infrastruktury ICT (datová centra, sítě a koncové stanice)**
- Koncepce rozvoje digitálních služeb
- Koncepce rozvoje webových aplikací, portálů a on-line informačních služeb využívajících datové fondy hl. m. Prahy.
- Koncepce rozvoje systému řízení IS/ICT.

- Koncepce rozvoje řízení kybernetické bezpečnosti IS/ICT.
- Koncepce integrace aplikací včetně napojení na státní registry
- Koncepce technologické aplikační podpory
- Koncepce rozvoje aplikačního portfolia

Byl prezentován celkový rámec ICT architektury MHMP.

Diskuze:

Říha: navrhuji zařadit IP Telefonie pod odbor IT. Zajímali by mě náklady na provoz.

Kallasch: koncepce je možné včetně roadmapy aktualizovat např. jednou ročně.

Vorlíček: na všechny koncepce je možné se domluvit na prezentaci přímo na IT a případně rovnou vypořádat připomínky.

Kallasch: do kdy je termín pro připomínky?

Vašíček: mělo by to projít na ZHMP.

Vorlíček: tady by to hlavně měla schválit RHMP.

Vašíček: i zástupci opozice se k tomu pozitivně vyjádřili, důležité je, aby to bylo dobře zpracováno a předpoklad byl do konce října. V současné době jedeme podle koncepce z roku 2013 a má platnost do 2019, tzn. že tato věc musí vypadnout do konce roku. V prosinci se má na zastupitelstvu hlasovat o rozpočtu a tedy tohle to by mělo proběhnout dříve než se bude schvalovat rozpočet.

Kallasch: vyjádření komise dostanete do 14 dní.

Usnesení:

„Komise RHMP pro ICT bere na vědomí předložené ICT koncepce MHMP.“

Hlasování: 7-0-0 (pro-proti-zdržel se). Usnesení bylo přijato.

3) Upgrade a doplnění nezbytné kapacity pro systém sběru logů

P.Matuš uvedl projednávaný bod, seznámil členy komise se záměrem vypsát nadlimitní veřejnou zakázku prostřednictvím DNS.

Hlavním cílem této veřejné zakázky je zajistit rozšíření stávajícího systému tak, aby byla zajištěna dostatečná kapacita pro sběr a uchovávání sebraných dat. Stávající logování bezpečnostních logů je realizováno SIEM systémem LOGmanager, jako hlavním úložištěm logů. Část logů je na základě výběru dle alertu dále přeposílána na analytický SIEM systém QRadar. Logy ze zdrojových systémů je nutné uchovávat po dobu 2 let, než mohou být smazány. Se stávajícím systémem LOGmanageru L je při průměrné velikosti denního indexu (120 GB) tato doba necelý 1 rok (310 dní), což je z bezpečnostních důvodů, které jsou dány buďto zákonem nebo interními směrnicemi nedostatečné.

Cílem této VZ je i zajištění nezbytně nutné záruky a uživatelské podpory pro nové i stávající technologie. Jedná se o jednu ze základních komponent pro monitoring sítě, která umožňuje bezpečný provoz síťového prostředí. Provozování zmíněných technologií bez této záruky a lokální podpory by bylo rizikové pro včasnou detekci problémů na síti. Zároveň budou efektivněji využity veškeré předchozí investice do monitorovacích technologií sítí.

Diskuze:

Kallasch: kolik už nás to aktuálně stálo?

Matuš: do dvou miliónů

Kallasch: není ideální doba si říct, že použijeme jinou opensource technologii? Navrhuji využití Elastic a Kibana? Je možné během měsíce tyto možnosti prověřit?

Žáček: všechny běžné SIEM balíčky nějakou funkci ukládání logů mají, proč chceme posilovat vendor lock in?

Tobiáš: ano prověříme tuto možnost a porovnáme v rámci všech nákladů.

4) Zajištění podpory stávajícího a nově budovaného síťového prostředí jednotlivých lokalit

P.Matuš uvedl projednávaný bod, seznámil členy komise se záměrem vypsát nadlimitní veřejnou zakázku formou otevřeného řízení.

Správa síťového prostředí jednotlivých lokalit je s ohledem na nezbytnost dostupnosti ICT prostředků jednou z kritických služeb IT. Infrastruktura je rozložena ve 23 lokalitách, kde dosavadními centrálními lokalitami jsou datová centra NUB, DC1, DC4 a DC5. Vnitřní infrastruktura jednotlivých lokalit se typicky liší podle její velikosti. Malé lokality, kterých je většina, jako jsou např. VYS, VAL, STAR, RYT, REZ, OPLET, MKP, CHAR, JAR, BOH jsou vybaveny malým počtem L2 switchů bez zajištěné vysoké dostupnosti (redundance zařízení a fyzických propojů). Centrální lokality a větší lokality JUN, NR, KON jsou kromě přístupových L2 switchů vybaveny redundantními L3 switchi, které zajišťují L3 routing již v rámci své lokality. Na základě analýz jednotlivých konfigurací a prvků proběhla v roce 2018/2019 na sítích ve všech lokalitách MHMP obnova síťových prvků. Pro tyto obnovené síťové prvky nejsou nastaveny služby podpory, profylaxe a rozvoje. U některých lokalit dnes navíc neexistuje redundantní řešení pro zajištění vysoké dostupnosti, síťové prostředí není segmentováno a v případě útoku je tak možný dopad do všech lokalit. Z výše uvedených důvodů je nezbytné zajištění centrální správy síťového prostředí až na úroveň L2 switchů.

Diskuze:

Žáček: vloni proběh upgrade síťových zařízení, co bylo součástí podpory?

Matuš: HW maintenance

Říha: jak došlo ke stanovení PH? Není tam žádný překryv s předchozí zakázkou?

Matuš: od 1.1. nebude žádná podpora na síťové prvky, končí jak smlouva AC tak TS.

Říha: jak je postavená tedy ta stará smlouva?

Matuš: stávající smlouva řeší jen některé lokality a staré prvky, ještě před obměnou.

Šorel: jak se teď nahlašuje událost?

Tobiáš: jde to přes INI, používáme SD dodavatelů.

Kallasch: dává smysl to sjednotit pod jednoho dodavatele.

Žáček: cílově ale říkáme že by to mělo skončit u OICT, proč tedy 3 roky?

Tobiáš: ty KL se dají vždy vypovědět, všechny služby se objednávají na pokyny. Výpovědní doba jsou 3M.

Žáček: Je možné doplnit záměry a důvodovou zprávou o monitoring prostřednictvím centrálního SD?

Vašíček: ve smlouvě by měl být zmíněný OICT, že to převezme.

Vorlíček: tady je řešení že se prostě ten katalogový list neobjedná.

Matuš: záměr je v otevřeném řízení, ale podpora je jen do konce roku. Termínově to již teď nestíháme.

Kallasch: můžeme někoho z komise jmenovat do hodnotící komise k zakázce.

Říha: co se stane, když se dosáhne stanovené částky?

Vorlíček: nebude možné vystavit fakturu.

Usnesení:

„Komise RHMP pro ICT souhlasí se záměrem na Zajištění Podpory stávajícího a nově budovaného síťového prostředí jednotlivých lokalit za podmínek:

- I) bude ve smlouvě počítáno s případným přechodem pod Operátora ICT,**
- II) bude zajištěn centrální servis desk pro logování ticketů.“**

Hlasování: 7-0-0 (pro-proti-zdržel se). Usnesení bylo přijato.

Zasedání se uskutečnilo od 17:00 do 19:20 hod.

Termín příštího řádného jednání byl stanoven na 19.11. 2019 v 17.00 hodin.

Ověření zápisu:

	Jméno	Datum	Podpis
Zapsala	Markéta Horská	15.10.2019	
Schválil	Ondřej Kallasch	.10.2019	