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

ZÁPIS
Z mimořádného jednání Komise RHMP pro ICT
č. 32 ze dne 25. 01. 2022

Účastníci:

Přítomni	Ondřej Kallasch (předseda), Jiří Károly, Jan Žáček, Jan Ladin, Jan Hora, Aneta Heidlová, Markéta Horská, Jan Rambousek, Hana Hermannová (tajemnice)
Omluveni	Michal Šorel, Radomír Nepil
Neomluveni	
Hosté	Vendula Kožíšková, Jiřina Onderčová

Program:

1) Úvod	O. Kallasch
2) Technologická podpora a rozvoj systému pro sběr logů	J. Károly
3) Různé	

Projednáno:

1) Úvod

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

Hlasování: 8-0-0 (pro-proti-zdržel se). Program byl schválen.

2) Technologická podpora a rozvoj systému pro sběr logů

Projednávaný bod uvedla J. Onderčová. Předmětem veřejné zakázky je zajištění provozu a rozvoje systému LOGmanager na období 36 měsíců. Konkrétní rozsah zakázky:

- nezbytné pokrytí instalované technologie LOG manager XL - 2 ks, formou dodávky podpory výrobce, včetně SLA
- rozšíření stávajících kapacit o technologií LOGM XL - 1 ks, formou dodávky HW a podpory výrobce, včetně SLA
- obnova LOGM L - 1 ks, formou dodávky HW a podpory výrobce, včetně SLA
- technologická podpora pro kompletní technologii LOGmanager v rozsahu 36 měsíců
- rozvojové a konfigurační práce v rozsahu 100 MD

Jedná se o jednu ze základních komponent pro monitoring sítě, která umožňuje bezpečný provoz síťového prostředí. Stávající systém je provozován v rozsahu:

- LOG manager XL - 2 ks, LOGM L - 1 ks
- Systém byl v uplynulém období 2 let konfigurován a postupně propojen s ostatními provozně bezpečnostními technologiemi tak, aby byla zajištěna maximální možná efektivita pro vyhodnocení dat
- Na základě rozvoje navazujících systémů / sítě / nárůstu počtu dat, není již dostačující stávající stav a je nutné revidovat architekturu zapojení, konfiguraci a zálohování logů.

- Nově navržená architektura zajistí zejména:
  - zajištění potřebného výkonu pro správu, vyhledávání události, zlepšení uživatelské odezvy
  - operativní přístup k historickým datům za účelem vyšetřování
  - bezpečný přístup třetích stran, tj. separace rolí pro analýzu dat – BEZ, správci DC, atd. (nebude narušena primární cesta toku LM – SIEM)
  - dostatečné kapacity pro sběr a ukládání logů dle aktuálních a budoucích potřeb

Diskuse:

Kallasch: Podobný záměr byl řešen v roce 2019 při implementaci do prostředí. Řešil se výběr technologie, diskutovala se možnost jiné cesty. Výhodou této technologie jsou relativně nízké pořizovací náklady, ale provozní náklady jsou relativně vysoké. Na základě promítnutého návrhu usnesení návrh vytvoření analýzy během roku a v případě vzniku možných úspor nákladů z dlouhodobého hlediska zvážení ukončení stávající Smlouvy. Mít podklad pro možnost zvážení pokračování ve stávající technologii či přejít na jinou. Provozní náklady se budou stále navyšovat s rozšiřováním systému.

Károly: Čas na analýzu je dostatečný, pokud Komise souhlasí s termínem do jednoho roku.

Kallasch: Pokud zvládneme analýzu dřív, bude to lepší, ale nevadí navrhovaný termín. Není čas zabrzdit, když podpora v březnu končí.

Ladin: Nahrazuje stávající, nebo se jedná o doplnění.

Onderčová: Stávající boxy zůstanou a dokoupíme podporu. Nové boxy budou i doplněny.

Žáček: Při dřívější debatě jsme zjistili, že LOGmanager je standardní produkt Elastic u SIEM řešení. Produkt je jen rebrandovaný Elastic dodávaný na vlastním HW. Hlavní přínos pořízení spočívá v tom, že dodavatel nastaví řešení pro správný sběr logů. Po dvou letech provozu říkáme, že není správně nastaveno, a je proto nutnost dalších MD.

Onderčová: MD, které není nutné vyčerpat a jsou alokované pro řešení v průběhu tří let na základě podrobných Katalogových listů oproti paušálním službám. Jedná se o gap pro případné rekonfigurace. Jedná se o nadstandardní věci v případě součinností a nemuseli jsme se správcem technologie řešit dokoupení např. 4 MD při čerpání Smlouvy. Čerpání není podmíněno.

Žáček: Tento požadavek se objevuje v každém tisku, kdy si vytváříme rezervu pro další konfigurace a je vždy vyčerpáno. Minule při schvalování tisku se řešilo prodloužení záruky, ale ve Smlouvě je ta samá položka. Potřebujeme pořídit další dva servery a na každé Komisi máme tisk o pořizování HW. Proč potřebujeme pro generický opensource systém Elastic dodávku HW od jednoho dodavatele? Jedná se o vendor lock-in. Nerozporuji potřebu sledování a vyhodnocování logů včetně expertní podpory dodavatele. Nepotřebujeme další krabice HW, těchto nákupů schvalujeme na Komisi velké množství. Potvrdit nebo vyvrátit, zda Elastic může fungovat i na stávajících HW, které jsou V DC?

Károly: V roce 2019 jsem u projednávaných diskusí nebyl, z jakých podkladů vycházíte?

Žáček: Byl předkládán tisk k rozhodnutí, kde byly uváděny částky v PH, uzavřená Smlouva obsahuje vyšší hodnoty. Zdůvodňujeme nutnost sledování logů, zákonný rámec byl 2 roky, dnes 18 měsíců. Z jakého zákona vycházíme?

Onderčová: Dohledáme a doplníme zákon.

Žáček: Bylo řečeno v zápisu Komise ze dne 26.11.2019, že bude doplněno a nedostali jsme odpověď.

Onderčová: Doplníme.

Károly: Zeptám se pana Ladina, zda doporučení od Národního úřadu pro kybernetickou a informační bezpečnost?

Ladin: Uvedeno ve vyhlášce. Doplnění emailem ze dne 25.1.2022: §22 - Vyhláška č. 82/2018 Sb. Vyhláška o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti)

(3) Povinná osoba uvedená v § 3 písm. c), d) a f) zákona uchovává záznamy událostí zaznamenaných podle odstavce 2 nejméně po dobu 18 měsíců.

(4) Povinná osoba uvedená v § 3 písm. e) zákona uchovává záznamy událostí zaznamenaných podle odstavce 2 nejméně po dobu 12 měsíců.

Povinná osoba z pohledu vyhlášky je statutární zástupce. Ten deleguje tyto činnosti organizačním řádem. V tomto případě odbor BEZ a OIC.

Károly: Aktuálně máme na MHMP 4 měsíce.
Kallasch: Na jaké technologie je LOGmanager postavený a co získáváme navíc? Finální produkt včetně HW.
Onderčová: Nemám podklady pro rozporování, že se jedná o rebrandovaný Elastic. Systém je nativní i přímo na boxech, technicky nejsem schopná rozporovat, jak jsou odlišné a co je výhodnější, Zda boxy, na které budeme instalovat, nebo boxy již nainstalované.
Kallasch: Je požadována analýza v rámci usnesení. Ohledně MD, přijde mi to správně a je potřeba v průběhu něco přenastavit. Poptávat externího dodavatele na 4MD je nadceněno.
Károly: Hodnota 100 MD je 1.2 mio Kč. Máte pravdu, když má dodavatel možnost čerpat MD navíc, snaží se je vyčerpat. Pokud bychom je neměli, museli bychom soutěžit jinou formou, VZMR nad 500 tis. Kč, musím soutěžit OVŘ a mohu dostat jiného dodavatele, než kdo systém spravuje.
Žáček: Pokud v rutinním provozu v běhu, tak 100 MD je vysoká dotace.
Károly: Možnost odsouhlasit schvalování změny na Komisi v případě čerpání 10+ MD.
Kallasch: S tím souhlasím, minimálně pro informaci. Pokud nejdeme cíleně, nevíme, kolik se z RS vyčerpalo.
Onderčová: Nejedná se o systém, který se zapne a běží, nefunguje setrvačností. Díky volnějším kapacitám budeme připojovat další systémy a aplikace, což nemusí být vždy standardní cestou. Je tam myšleno na součinnosti s třetí stranou, proto nedokážeme aktuálně pojmenovat, ale bude nutné to zajistit provozovatelem systému, a ne jiným dodavatelem. Jedná se o cca 30 MD za rok, kdy je potřeba dělat něco navíc. Budget není dle mě neadekvátní.
Žáček: Tento tip kompetence by bylo dobré držet in-house. Dohledávat bezpečnostní incidenty přes externího dodavatele je náročné. Technologie pro SIEM v LOGmanageru je složitá, využívá se Elastic, řekli jsme si, že se jedná o standardní Elastic a pojďme to využívat. Najděme si člověka in-house. Po dvou letech další tisk, který směřuje k 15 mio Kč nákladů a provoz nás stojí přes 5 mio Kč/rok, což je hodně. Abychom nestáli před stejným rozhodnutím za tři roky.
Károly: Byl bych rád, aby tomu tak bylo. Když vidím stav lidí na informatice, tak letos to nevyjde. Je to úkol na odbor bezpečnosti, kde to je také nereálné. Máme OICT, otázka na pana Ladina, zda jsou schopni nám tyto kapacity doplnit? Za mě jediná možnost, jak toho dosáhnout v rámci MHMP.
Onderčová: Došetřování je bezpečnost schopna dělat sama, proto v nové architektuře na to myšleno. Při rozšiřování sítě je nutné navýšit kapacity. Support sítě a DC musí být adekvátní, nejedná se o lineární linku.
Žáček: Při předkladu jsem očekával poskytnutí informace o kontextu vytížení boxu, včetně srovnání finančních investic.
Onderčová: Na začátku jednání jsme se shodli, že analýza není problém.
Žáček: To se týká všech předkládaných tisků. Bavíme se o systému, který běží a můžeme vyčíslit, kolik incidentů bylo dohledáno, kolik nás stál provoz systému. Doplňkové informace klíčové pro záměr.
Onderčová: Informace máme, bez toho bychom nemohli vytvořit návrh nové architektury a požadavků. Technický podklad, proč je nutná tato konfigurace máme. Záleží, jak velký detail Komise požaduje.
Kallasch: Zdůvodnění pro nás, jako členy Komise, je nedostatečné. Pokusím se navrhnout šablonu zdůvodnění, kde jsou otázky, které nás zajímají a podle toho bychom chtěli vytvořit podklad od vás, jako předkládajících.
Károly: Požádám o rozeslání analýzy, kterou jsme vytvářeli na členy Komise.
Onderčová: Máme měsíční reportingy a zašlu. Je technický, ale je tam manažerské shrnutí, díky kterému uvidíte kontinuitu vytížení. Pokud nenajdete, co potřebujeme, poptáme a dopracujeme statistiku.
Žáček: Bylo by lepší to mít předem jako součást materiálu. Zajímala by mě reálná zákonná povinnost, jak dlouhé období pro uložení logů je potřeba.
Ladin: Doplněno výše v rámci zápisu na základě emailu rozeslaného členům Komise.
Kallasch: Má OICT zájem o přebrání tohoto Katalogového listu?
Ladin: Je to zajímavé téma, využíváme pro vlastní potřeby. Otevřeme téma s panem ředitelem a začneme na tom pozvolna pracovat.
Kallasch: Prodloužíme stávající technologii a promyslíme další možnosti, jako je pilot u OICT a prohlubování včetně technologie.
Ladin: Pro začátek spoluúčastni u vytvoření analýzy. Poté můžeme pokračovat i dále.

Rambousek: Jaký problém tímto projektem vyřešíme? Existuje aktuálně zásadní problém, nebyl incident vyřešen před expirací logů? Z jakého důvodu se toto vytváří?
Ladin: §22 říká, jakmile se stane jakákoliv bezpečností událost, kompetentní osoba má na starost prozkoumat logy za celý rok. Tímto eliminujeme riziko, že budou logy k dispozici. Útoky se dějí a do logů se musí u významných systémů. Eliminace rizik.
Károly: Souhlasím s panem Ladinem, jsme na 98% kapacity boxů. Aktuální logy držíme 180 dní, nemůžeme tak napojit další systémy, prodloužit lhůtu 180 dní. Pro bezpečnost by to byl lepší přístup, aktuálně musí do archivních systémů a práce je tak složitější. Držet delší retenci z více zdrojů dává větší smysl a usnadnění práce.
Rambousek: Komponenty obsluhovaného systému má úložiště a logy kopíruje do centrálního systému. Je to forma redundance logů?
Kallasch: Logy nejsou po tak dlouhou dobu, berou prostředky na serverech. Po měsíci se logy zálohují jinde a smažou se. Hledání logů na jednotlivých aplikačních serverech a HW, to si nedokážu představit. Elastic, který využíváme, je nástroj, který nám umožňuje sledovat logy nezávisle na tom, na kolika serverech to běží.
Rambousek: Zajímalo mě, zda se jedná o formu redundance nebo ne. Požádám o komparativní analýzu, pokud to nebude výhodnější mít v cloudu.
Károly: Kolegové z bezpečnosti by data tohoto typu v cloudu rozhodně nepovolili ukládat.
Kallasch: Nástroj nám umožňuje shromažďování logů v jednom HW. Pro ty, kteří s logy pracují se můžou chovat jako v cloudovém úložišti, není nutné vědět, kde přesně leží, ale že je k nim snadný přístup.
Rambousek: Myslel jsem tu první variantu. Úvahu pro porovnání centrální úložiště vs. cloud. Chápu, že může být legislativní problém, ale z hlediska, že nejsou v bezpečí jsem nepomyslel. Požádám o komparativní analýzu a pokud je obava mít data v cloudu, tak o důvodu, proč tam MHMP data nemohou být.
Kallasch: Přidáno jako bod do usnesení.
Ladin: MVČR mají strategii cloudu, debata, jaká data se mohou do cloudu dát a která ne.
Onderčová: Ukládání dat, která jsou brána jako archivována, plánování využití technologií Veritas. Po dohodě s odborem bezpečnosti.
Rambousek: Pokud by z komparativní analýzy vyjde toto řešení nevýhodné oproti jinému? Jaké jsou tam penále, pokud bude po roce Smlouva ukončena? Mohli bychom informaci obdržet?
Onderčová: Nedokážu si to aktuálně představit, otázka je, jak v analýze zohledníme přechod na jinou technologii.
Károly: Pokud budeme chtít skončit, bude to složité. Doporučoval bych až po třech letech po ukončení Smlouvy. Nebudeme dělat žádný rozvoj, nevyčerpal bych 100 MD, ale HW bude v majetku MHMP. Domnívám se, že by se jednalo o finanční ztrátu. Technologie se obhajovala v minulosti a RHMP a Komise souhlasila.
Onderčová: Odbor bezpečnosti na tom participuje a oni souhlasili s pokračováním funkční technologie.
Kallasch: Nevzpomínám si, zda bylo po roce 2019 v Komisi RHMP pro ICT. Analýza nebyla předložena, to vidím jako důvod dnešní diskuse. V rámci usnesení se snažím předejít podobné diskusi do budoucna.
Rambousek: Navrhuji, aby Komise nehlasovala v tomto bodě a brali jej pouze na vědomí. Typický problém vendor lock-in. Pokud nemůžeme aktuálně jinak, schvalme to, ale řešme to příště předčasně.
Kallasch: Já nemám problém pro materiál i přes časovou tíseň hlasovat a navrhuji oddělené hlasování o jednotlivých bodech usnesení.

Usnesení:

I. Komise RHMP pro ICT doporučuje záměr s názvem **Technologická podpora a rozvoj systému pro sběr logů**, který je přílohou tohoto usnesení ke schválení.
II. Komise RHMP pro ICT požaduje, aby byla zpracovaná analýza přechodu na jinou technologii (Elastic, Kibana, Zabix atd.):
    a. Porovnat pořizovací náklady a provozní náklady
    b. Zpracovat dopadovou analýzu, ve smyslu, jaký by byl dopad na ostatní systémy včetně nákladů na změnu technologie

c. Prověřit možnost zajištění ze strany Operátora ICT
d. Prověřit možnost ukládání logů do cloudu
e. Přiložit výslednou analýzu k příštímu záměru na řešení této oblasti

Termín: Kdykoliv v průběhu čerpání stávající technologie, nejpozději však před přípravou prodloužení supportu či upgradu stávajícího systému.

Hlasování:
Usnesení č. I: 7-0-1 (pro-proti-zdržel se). Usnesení bylo schváleno.
Usnesení č. II: 8-0-0 (pro-proti-zdržel se). Usnesení bylo schváleno.

Zasedání se uskutečnilo od 15:00 do 16:17 hod.

Termín příštího řádného jednání byl stanoven na 15.02.2022 od 15:00 hodin.

Ověření zápisu:

	Jméno	**Datum**	**Podpis**
Zapsala	Hana Herrmanová	25.01.2022	
Schválil	Ondřej Kallasch	01.02.2022	