Dohledové centrum eGovernmentu a Vládní dohledové centrum

Ing. Bohuslav Zůbek, CMICT

Manažer kybernetické bezpečnosti resortu MV

Samostatné oddělení kybernetické bezpečnosti

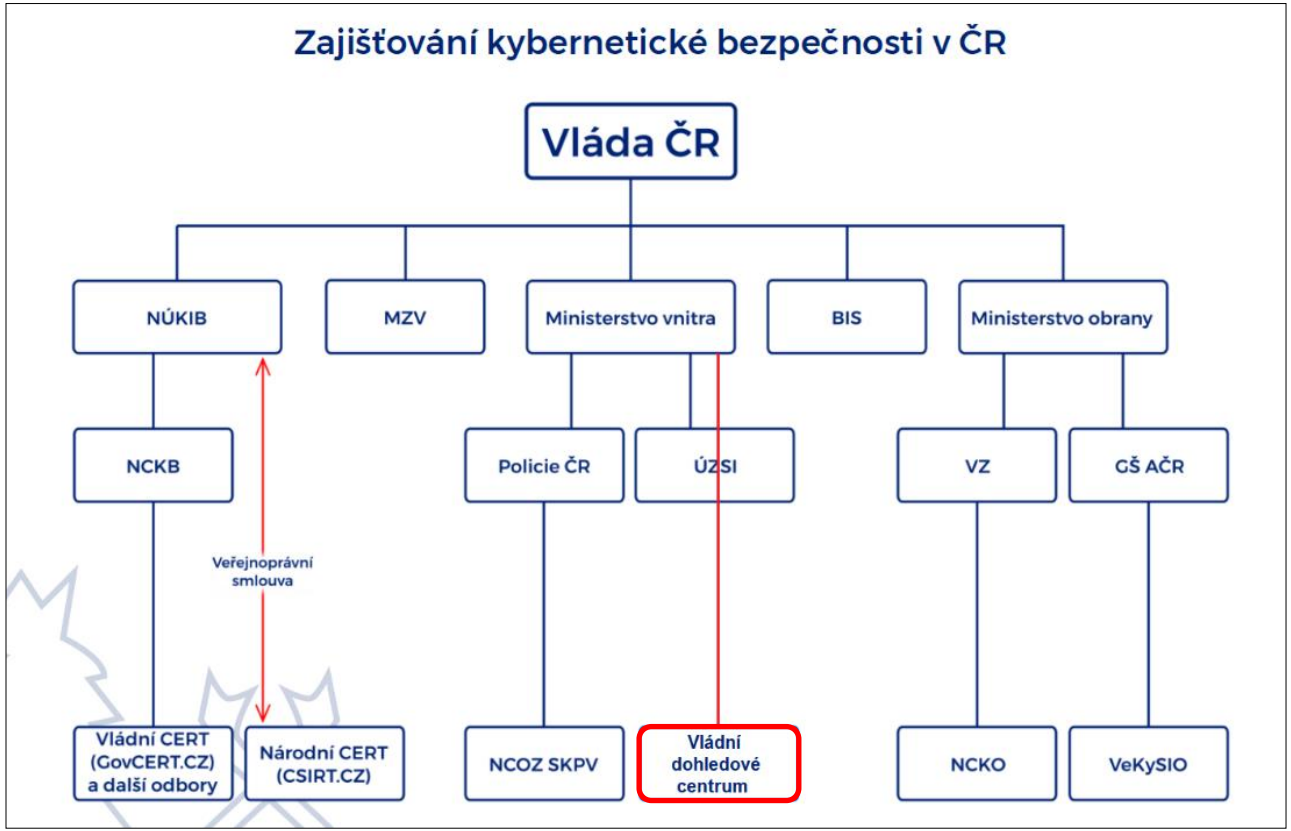
Ministerstvo vnitra

Program

1. Úkol č. 82 uložený Ministerstvu vnitra z Akčního plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025
2. Financování úkolu č. 82 – transformace Dohledového centra eGovernmentu na Vládní dohledové centrum (VDC)

1. Úkol č. 82 uložený MV z Akčního plánu k Národní strategii kybernetické bezpečnosti ČR na období let 2021 až 2025

Informace o Vládním dohledovém centru – role VDC



- MV byl ve spolupráci s MO, MZV, NÚKIB a zpravodajskými službami uložen následující úkol v Akčním plánu k Národní strategii kybernetické bezpečnosti České republiky na období let 2021 až 2025: „***Zajistit rozvoj dohledového centra e-Governmentu s cílem vytvořit jednotné Vládní dohledové centrum, poskytující jednotný monitoring a dohled pro systémy e-Governmentu a další relevantní systémy***“.
- Termín pro splnění úkolu byl stanoven do **Q4 2023.**
- Ve stručnosti je předmětem úkolu **zajistit přestavbu současné DCeGOV na Vládní dohledové centrum** (dále jen „VDC“) jako jednu ze základních součástí vnitřní bezpečnosti státu.
- DCeGOV bylo primárně postaveno **pro zajištění monitoringu systémů resortu MV**, protože vytvářet dohledové nástroje pro každý systém zvlášť by bylo značně **neefektivní a mnohonásobně dražší než jedno centrální dohledové pracoviště**.
- Kvalita poskytovaných služeb DCeGOV zaujala také ostatní organizace státní správy (mimo jiné například MD, ÚOOÚ, …), které projevily zájem jeho služby také využívat. Nicméně z důvodu nastavení zákona o zadávání veřejných zakázek **neexistovala jednoduchá cesta, která by umožňovala ostatním organizacím služby DCeGOV využívat**. Mimo jiné i z tohoto důvodu byl zadán úkol vybudovat VDC, jehož předmětem činnosti má být poskytování služeb monitoringu v rámci veřejné správy (nejenom tedy v rámci resortu MV).

Informace o Vládním dohledovém centru – cíle

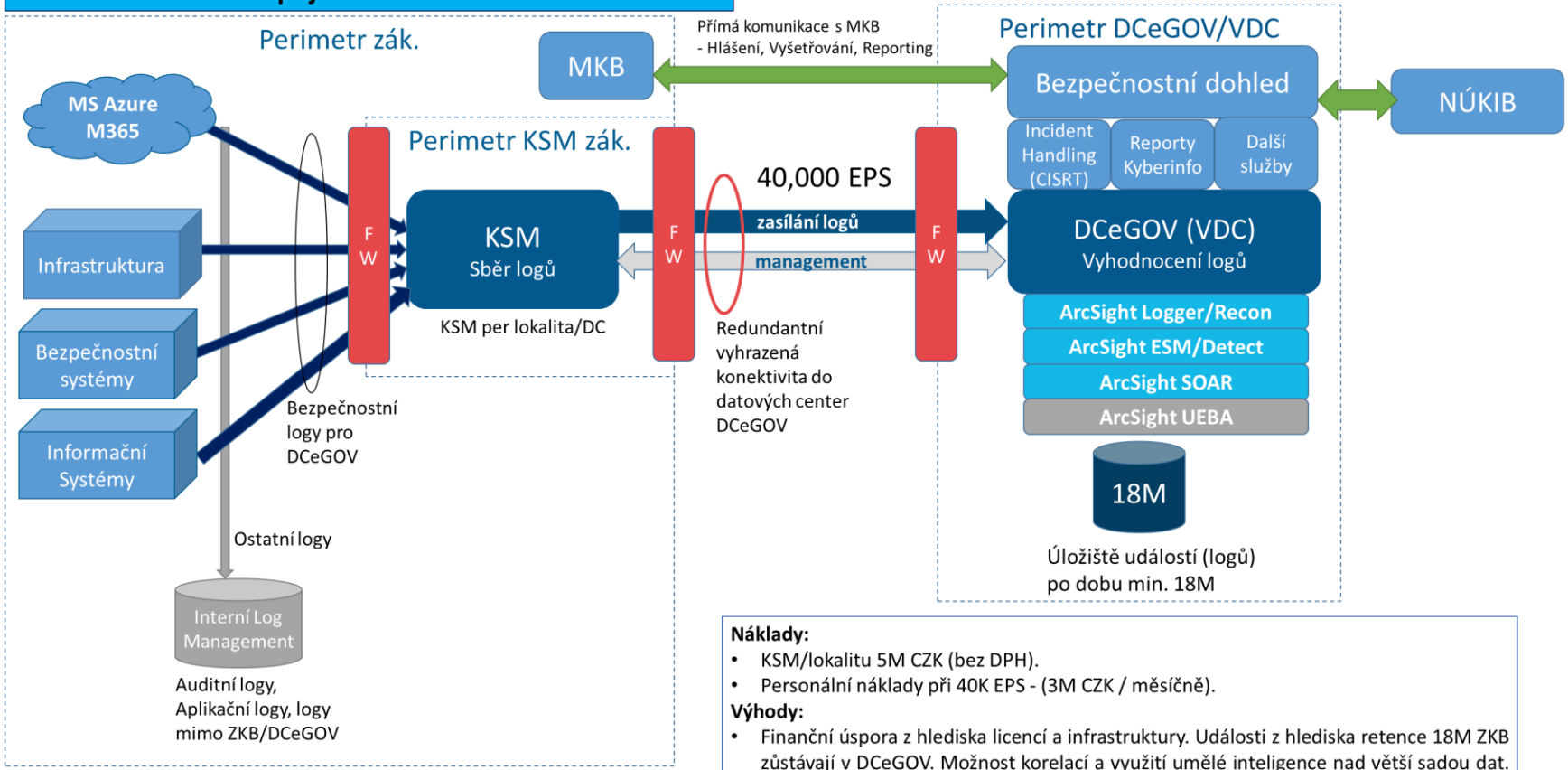
1. Výrazně **posílit kybernetickou bezpečnost** ve veřejné správě.
2. V maximální míře **využít již vynaložené finanční prostředky státu** na vybudování a provoz stávajícího DCeGOV.
3. **Využít všech zkušeností a navázané spolupráce** se státními, komerčními i akademickými institucemi, které má stávající DCeGOV včetně schopnosti být atraktivním pracovištěm pro mladé, kvalitní odborníky.
4. Centralizací bezpečnostních a certifikovaných procesů dosáhnout **maximálního využití odborných znalostí a zkušeností** a optimálně využít finanční náklady na rozvoj a provoz připravovaného pracoviště VDC.
5. Sdílením služeb VDC pro více zákazníků a informačních systémů dosáhnout **efektivního využití investic**, které stát již investoval a investuje do stávajícího DCeGOV a jeho přeměny na VDC a zejména kapacit specialistů – odborníků, kterých je dlouhodobě na trhu práce kritický nedostatek a státní organizace nejsou a nebudou v budoucnu schopny je zaměstnat a adekvátně zaplatit.
6. Díky centrálnímu uložení a zpracování relevantních bezpečnostních logů na VDC bude možné **velmi efektivně tyto logy v případě potřeby i zpětně prohledávat a analyzovat, a to ve kteroukoliv denní či noční dobu** bez nutnosti složitě vyžadovat a koordinovat spolupráci dalších osob a subjektů. Tím dojde k výraznému posílení bezpečnosti monitorovaných systémů i státu.
7. **Poskytovat analytické výstupy pro zákazníky i stát** na základě metadat a logů, které bude shromažďovat pro svou činnost a na základě své činnosti.
8. **Spolupracovat se všemi relevantními partnery v rámci ČR i mezinárodně**.

- **Služba kategorie I – základní služba VDC**:
  1. Příjem, záznam událostí hlášených od uživatelů a předání k řešení.
  2. Dohled a detekce – Triage, Monitoring, identifikace, klasifikace bezpečnostních událostí a incidentů v bezpečnostních nástrojích.
  3. Threat Hunting (hledání neznámých hrozeb) - Sledování, analýza a vyhodnocování informačních zdrojů a SW nástrojů.
  4. Bezpečnostní zpravodajství na základě vlastní činnosti.
  5. Analýza a řešení KBU/KBI - Analytická činnost, návrhy řešení, návrhy opatření (nápravná a preventivní) k mitigaci bezpečnostních událostí a incidentů.
  6. Kontrola a koordinace řešení bezpečnostních událostí a incidentů (CISRT).
  7. Návrhy prevence v bezpečnostních oblastech.
  8. Optimalizace bezpečnostních nástrojů - Aktualizace a optimalizace nastavení bezpečnostních, provozních a systémových pravidel dohledových, bezpečnostních a monitorovacích nástrojů a jejich prostředí, dále pak prostředí Service Desk.
  9. Podpora a konzultace MKB - Konzultační činnost, příprava podkladů.
  10. Pravidelný reporting.
  11. Uchovávání logů v souladu se ZoKB – zajištění plnění zákonné povinnosti; využití logů pro následné zpracovávání pokročilými nástroji – jedna z budoucích klíčových výhod tohoto řešení.

- Tato služba **by měla pokrýt vše pro zákazníka** od příjmu informace / logu, až po aktivní řízení incidentu, vypracování zprávy a návrhu opatření. Zároveň zahrnuje preventivní činnosti a podporu MKB v jeho informování a návrhu opatření. Podpora plnění paragrafu §14, §22, §23, §24 a §31 dle vyhlášky č. 82/2018 Sb. Podrobnosti jsou řešeny studií proveditelnosti napojení na DCeGOV/VDC.

Varianta 2 – Plné napojení na VDC včetně retence 18M

Nezávazný pracovní návrh. Uvedené ceny a odhady jsou na základě ceníkových cen, pracnost je stanovena dle zkušeností v obdobných systémech.



Pro logy zasílané do DCeGOV (VDC) nutné vyžádat stanovisko bezpečnostních sborů. DCeGOV (VDC) smí zaznamenávat události z hlediska činnosti běžných uživatelů pouze na úroveň přihlášení a odhlášení.

Náklady:

- KSM/lokalitu 5M CZK (bez DPH).
- Personální náklady při 40K EPS - (3M CZK / měsíčně).

Výhody:

- Finanční úspora z hlediska licencí a infrastruktury. Události z hlediska retence 18M ZKB zůstávají v DCeGOV. Možnost korelací a využití umělé inteligence nad větší sadou dat. Zabezpečení vypořádání žádostí pro NÚKIB.
- Možnost varování a dle dodávaných IoC a dalších informací pro dobu min 18M = větší efektivita.

- **Služba kategorie II – volitelná služba VDC dle požadavku připojené organizace**:
  1. Provádění bezpečnostních testů dle požadavku zákazníka.
  2. Podpora procesu řízení zranitelností a detekce zranitelností.
  3. Forenzní analytické služby.
  4. Konzultační činnost v oblasti kybernetické bezpečnosti (nad rámec běžné činnosti podpory MKB).
  5. Phishingové kampaně.
  6. … v budoucnosti další služby podle požadavků a strategie rozvoje VDC.

2. Financování úkolu č. 82 – transformace Dohledového centra eGovernmentu na Vládní dohledové centrum (VDC)

Financování úkolu č. 82 – současný stav

- **Financování DCeGOV:** DCeGOV je v současnosti financováno formou služby G6 NHS (pozn. jedná se o měsíční paušální platbu):

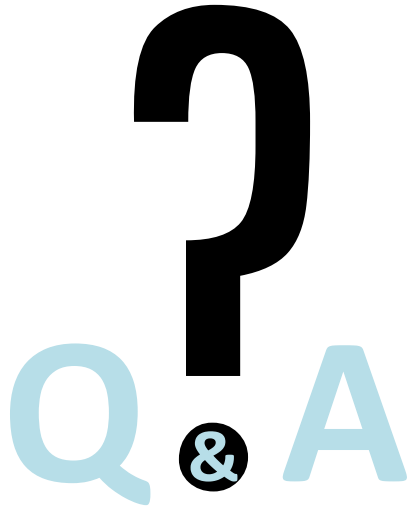
Název služby	Systém	Provozní výkon NAKIT (bez DPH)	Administrativní přirážka (bez DPH)	Přímá výrobní režie (bez DPH)	Cena služby celkem (bez DPH)
G6	DCeGOV	5 316 976 Kč	29 525 Kč	97 529 Kč	**5 444 030 Kč**

- **Financování VDC:** Vzhledem k tomu že v letech 2020-21 nebyly přiděleny dostatečné finanční prostředky na rozvoj DCeGOV, bylo přijato rozhodnutí využít prostředků z NPO pro zajištění splnění úkolu č. 82 cestou tří projektů:
  1. **Dohledové centrum eGovernmentu –** Rozvoj a posílení infrastruktury DCeGOV ve výši **80 mil Kč bez DPH**;
  2. **Navyšování kapacity datových center a datových úložišť –** Posílení úložiště logů ve výši **234 mil Kč bez DPH**;
  3. **Kybernetická bezpečnost, zákon č. 181/2014 Sb. –** implementace opatření pro vybrané systémy pro splnění požadavků zákona o kybernetické bezpečnosti, včetně zajištění připojení systémů na DCeGOV ve výši **350 mil Kč bez DPH**.
- Díky těmto třem projektům bude infrastruktura DCeGOV upravena a rozšířena tak, aby byla snadno škálovatelná a bude tvořit základ pro VDC.

- Do 31. 3. 2023 bylo MV správcem části systémů, u kterých prostřednictvím svého DCeGOV zajišťovalo služby monitoringu.
- **K 1. 4. 2023 došlo k převodu části systémů MV na DIA**.
- Aby byla zajištěna kontinuita služeb a aby systémy převedené na DIA neztratily služby monitoringu, tak byl na základě žádosti DIA zahájen **tzv. testovací režim**, jehož účelem bylo také upřesnit, jaké finanční prostředky stojí monitoring u těchto převedených systémů.
- Do dnešního dne zatím **platí za monitoring** systémů DIA **MV** v rámci NHS – služba G6.

- Model personálních nákladů **je odvozen od stávajícího modelu fungování DCeGOV**, kde se vychází z aktuálního počtu událostí za vteřinu (EPS = Events Per Second) s rozpadem pracnosti na jednotlivé role pro výkon bezpečnostního dohledu (SOC).
- Tento finanční model vychází z v **praxi ověřených postupů**, vytíženosti jednotlivých rolí při denní práci a tím i daného nezbytného počtu osob a rolí na DCeGOV pro zajištění jeho bezvadného fungování a garanci vysoké úrovně dodávané služby a bezpečnosti pro zákazníka.
- Na základě výše uvedeného jsme dali do rovnice **množství dat**, která nám systém zákazníka posílá ke zpracování a dají se objektivně měřit **a průměrnou práci**, kterou je na naší straně nutné vykonat k jejich zpracování až po případné řešení incidentu.
  - **Cena za práci přepočtená na 1 EPS = XXX CZK bez DPH / měsíc.**

- Zákazník bude dobře předvídat, **kolik ho bude služba stát a plánovat si rozpočet**.
- VDC bude moci provádět rozšíření nebo zkvalitnění svých nástrojů a tím bezpečnosti **bez závislosti na rozpočtu zákazníků a diskuze s nimi**.
- VDC bude moci připravovat a budovat **zcela nové služby**, které bude následně zákazníkům nabízet nebo se stanou součástí základní služby a tím se opět **posílí bezpečnost zákazníka i státu**.
- **VDC bude financováno transparentně** jedním kanálem, který bude lehce kontrolovatelný. Zjednoduší se administrativa kolem financování VDC.
- Zákazník bude platit **jen za odebrané služby**, kterým bude rozumět včetně jejich financování.


Q & A

Děkujeme za Vaši pozornost.