



SPCSS

Státní pokladna
Centrum sdílených služeb

**Poskytovatel služeb datových center
a služeb kybernetické bezpečnosti
pro státní správu**

Přímá cesta SPCSS do hybridního cloudu

Ondřej Nekovář

Co Vás dnes čeká

1. Přechod do cloudového řešení ve státní organizaci
2. Bezpečnost cloudu/v cloudu
3. Use-case (příklad užití)
4. Budoucnost



Dvě bezpečná datová centra (TIER III) a přidružené ICT a kyberbezpečnostní služby pro státní správu

DC Vápenka



DC Zeleneč



- Předmětem podnikání SPCSS je **provozování datových center**, zajišťování řádného chodu aplikací primárně z oblasti finančního řízení státu a auditu a poskytování dalších ICT služeb, určených především pro subjekty veřejné správy.
- SPCSS **provozuje kritické informační systémy státu** (např. provoz systému Státní pokladny, daňového informačního systému, základních registrů, Ares gambling...).
- SPCSS je **prvkem kritické infrastruktury státu**.
- SPCSS **provozuje resortní cloud MF** a připravuje **státní část eGovernment cloudu**.

Přechod do cloudového řešení ve státní organizaci

Jiří Bajgar

Jak jsme se dostali k hybridnímu cloudu

- **2015** vznik společnosti a počátek využívání produktů M365
- Provozování virtuální platformy (VMware)
- **2016** první služby implementované v MS Azure
- **2017** PoC Oracle Cloud
- **2018 – 19** PoC MS Azure Stack Hub
- **2019** PoC IBM cloud



Jak jsme se dostali k hybridnímu cloudu

- Inspirace v zahraničí + rozhodnutí o hybridním cloudu
- **2020** – příprava VZ na hyperkonvergovanou infrastrukturu
- **12/2020** – GCP
- **2021** – infrastruktura pro SLDB (hybridní řešení)
- **4/2021** – nákup Azure Stack Hub (privátní Cloud)



Náš přístup hybridnímu cloudu

Realita včerejška (třeba i SLDB)

- **Privátní část**
SPCSS virtualizace
- **Veřejná část**
využití MS Azure

Realita dneška/zítřka

- **Privátní část**
 - Hyperkonvergovaná infrastruktura (SM Azure Stack Hub)
 - SPCSS virtualizace
- **Veřejná část**
 - MS Azure
 - Google Cloud Platform

Realizace nové koncepce hybridního cloudu

- Veřejná zakázka na hyperkonvergovanou infrastrukturu
- **Nákup Azure Stack Hub** – hurá máme vyhráno
- **Implementace** – ještě zdaleka ne
 - Sítě
 - Monitoring
 - Zálohování



Výzvy pro organizaci

- Model poskytování služeb
- Zvýšení agility (ANC/AMPA)
- Billing
- IaaC
- Organizační struktura
- *Obdobná výzva stála i před ÚKB ...*



Bezpečnost cloudu / v cloudu



Ondřej Nekovář

Bezpečnost cloudu / v cloudu

Bezpečnost v cloudu – východiska

- Nové **neznámé prostředí**
- **Závislost** na poskytovateli
- Počáteční **minimální znalost** nástrojů
- **Odlišná architektura** řešení
(On-prem All-in-one vs desítky služeb v cloudu)
- **Nová specializace** pro pracovníky



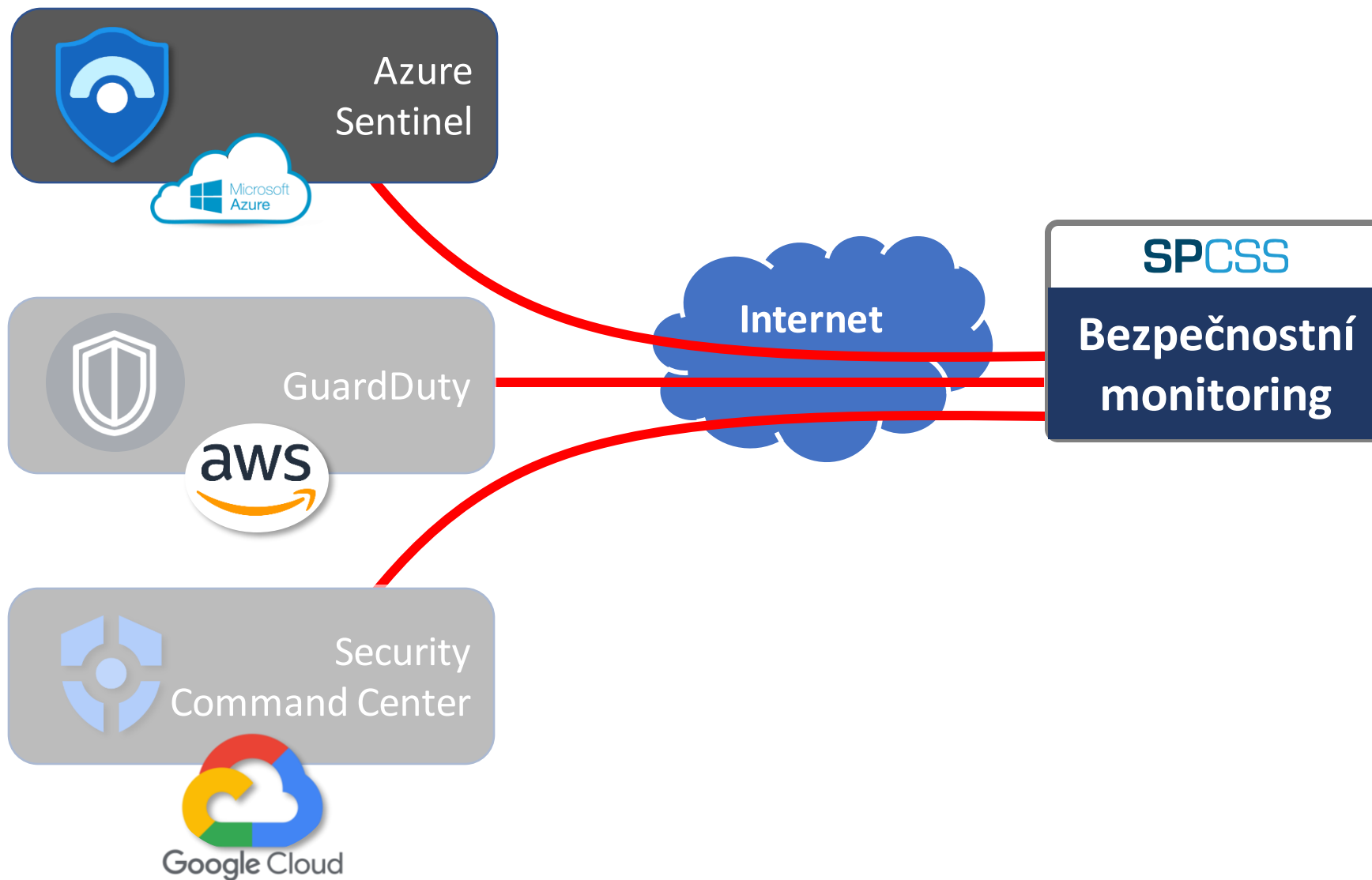
Bezpečnost cloudu / v cloudu

Co děláme (aktuální aktivity)

- Systematické vzdělávání - schéma
- Celopodnikový incident response proces
- Zohlednění cloudových technologií v AR
- Splnění vstupních kritérií do katalogu služeb eGC
- SOC2 ®
- Realizace procesů spojených se zabezpečením kubernetes
- Analýza nákladů při přechodu z on-prem do cloud only
- Centralizované řízení detekčních pravidel (jednou vytvoříš, použiješ všude)



Napojení monitoringu cloudových služeb



Malinko z praxe

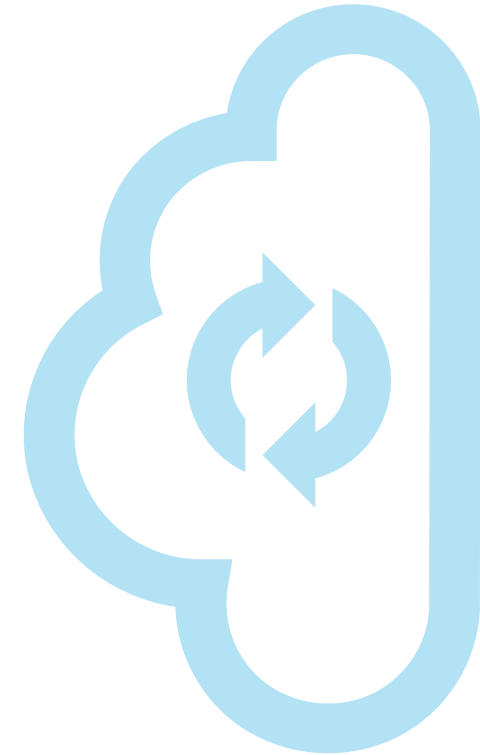


HYBRID
CLOUD

Šimon Beneš; Jan Pohl

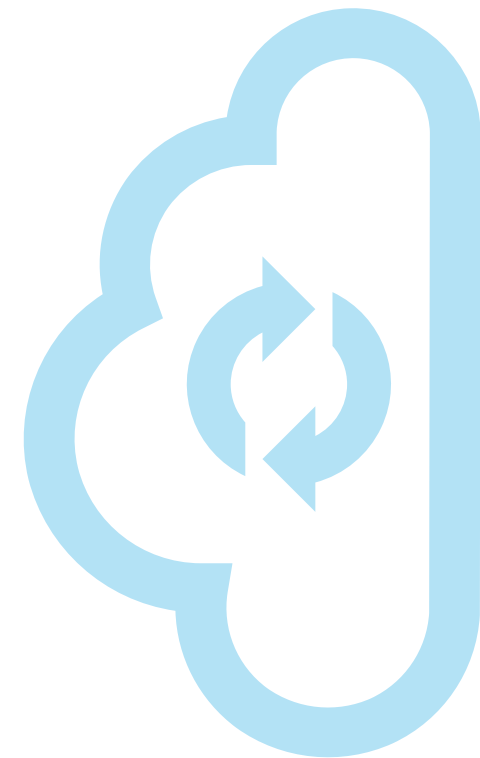
Kubernetes – provoz

- Vanilla je "easy", ale realita je jiná
- Ohled na bezpečnost, uživatelský komfort
- Ohled na funkcionalitu požadovanou zákazníky
- Break point - nepomůže ani dodavatel ani vývojář
- Nutná kooperace se všemi



Kubernetes – bezpečnost

- Out of box detekce funguje jenom na papíře
- SOC nemá možnost ovládat všechny technologie
- Nutná spolupráce pro využití znalostí a zkušeností
- Bezpečnostní řešení fungují jenom v labu
- V reálném prostředí nutné ohýbání



Blízká budoucnost



Ondřej Nekovář



Blízká budoucnost

Cesta za poskytováním služby cloud computingu v rámci katalogu eGovernmentu cloud

- Služba Microsoft Azure
- Služba Microsoft AzureStack



Budoucnost

Provozovatel státní části eGovernment cloudu

- Příprava na provozování státní části eGC
- Assessment pro IS BÚ4 k přechodu do státní části eGC
- Realizace SOC2® - BÚ3 (Azure, AzS), BÚ4



Budoucnost

Spolupráce

- Tvorba Metodiky bezpečnostního standardu **kubernetes**



Děkujeme za pozornost

Nebojte se zeptat
info@spcss.cz