Rok informatiky

Daniel Rokos – vedoucí Odboru informatiky

Středočeský kraj

Středočeský kraj

Rok informatiky - Agenda

1. Technologické centrum kraje
2. Kybernetická bezpečnost PO
3. Elektronizace centrální evidence a správy majetku SK
4. Realizace služebních cest a návštěv - RCN (GINIS)
5. Vzdálené pečetění a podepisování
6. NÚKIB

Technologické centrum kraje (obnova k 31.12.2025)

- **Hyperkonvergovaná infrastruktura** (HCI), stavební bloky (servery) a SAN switche vč. licencí **VMware Virtual Cloud Foundation (VCF) – využití současné HCI – Technologické centrum a HCI – DTM**

Nasazení jiné virtuální platformy??? – Hyper-V, OpenStack, Nutanix – cena VMware (Broadcom), přechod na službu/jiné licencování (optimalizace stavebních bloků – socketů)

- **Cloudové služby** v rozsahu celkového sizingu stanovených informačních systémů a softwarových aplikací (instancí VM), resp. poskytovaných služeb pro příspěvkové organizace kraje
  - **8 měsíců Proof of Concept (revize VM infrastruktury, instancí SW, sizing, datové toky)**
  - **Nastavení optimálního modelu financování (75% mandatorní + 25% plovoucí)**
  - **Reporting a vyhodnocování provozu (5 let) v rozsahu celkového financování – schopnost migrovat VM (cloud/on-premise)**
- **opce na 4 stavební bloky** (servery) nad rámec výše uvedené dodávky HCI
- + další služby

Kybernetická bezpečnost PO

Dodávka technologické a aplikační architektury a s ní související služby pro zajištění komplexní bezpečnosti sdílených služeb poskytovaných z Technologického centra kraje („TCK“) pro příspěvkové organizace Středočeského kraje („PO SčK“), a to v souladu se zákonem o kybernetické bezpečnosti.

- Projekt - spolufinancován z prostředků Evropské unie a státního rozpočtu v rámci (IROP) Integrovaného regionálního operačního programu – Kick-off 2024
- Navazuje na Kybernetickou bezpečnost KÚ

Etapa 1 - Dodávka Firewallů (Perimetrů) pro KÚ a 260 PO

- Cíle:
  - Zajistit bezproblémovou komunikaci mezi KÚ a PO
  - Nastavit bezpečnostní pravidla pro komunikaci (tunel pro core systémy)
  - Minimalizovat výpadky systémů (Blacklist, nastavení emailových služeb, chyby na www stránkách, internetová konektivita) = eliminovat problémy a zejména latence při jakémkoliv výpadku sdílených služeb (KÚ vs. PO)

Pozn.: Sdílené služby = poskytované IS (VIS) – spisová služba e-spis Lite, GINIS, anonymizační nástroj, IDM, Service desk atd…

Kybernetická bezpečnost PO

Etapa 2 – Nasazení jednotného centrálního systému pro komplexní správu uživatelů PO – IDM (Identity management). Řízení uživatelských identit, oprávnění a rolí.

- Cíle:
  - Efektivně řídit identity, oprávnění a role v rámci poskytovaných IS PO = efektivně řídit přístup pracovníků PO do poskytovaných IS z TCK
  - Nastavit workflow (pracovní postupy) – zřízení, změna, zrušení přístupů pracovníků PO = náhrada PDF formuláře pro přístup k IS. Nebyli jsme schopni tuto oblast efektivně a systémově řešit
  - Správa pracovníků PO = každá organizace má přístup na vlastní web stránku se seznamem pracovníků (oprávnění a role do IS poskytovaných z TCK), které si sama spravuje = základní editace přístupů pracovníků PO – není pod komplexní správou Odboru informatiky

Středočeský kraj

Kybernetická bezpečnost PO

Etapa 3 – Dodávka dohledového systému, který primárně zajišťuje dohled nad komunikací mezi KÚ a PO (v rámci dodaných zařízení – etapa 1)

- Cíle:
  - Zajistit dohled nad komunikací mezi KÚ a PO v rámci dodaných firewallu/perimetrů
  - Na straně KÚ vyhodnocovat provoz + zajistit centrální napojení na SOC - Security Operations Center
  - Nastavit automatické zakládání požadavků do Service Desku/Helpdesku KÚ/PO, volání, SMS
  - Nastavit scénáře/pravidla pro bezpečnou komunikaci mezi KÚ a PO (scénáře = nestandardní provoz – např. zvýšení přenosové kapacity linky, výpadky, latence apod.)

Jednotlivé etapy dokončeny – květen 2025, aktuálně v řešení penetrační testování.

Elektronizace centrální evidence a správy majetku SčK

Pořízení jednotného SW nástroje a nasazení modulů (PAS, FM) - Technologické centrum kraje (2020 Proof of Concept – zapojení 6 PO do testování) – Spolupráce Odboru majetku a informatiky

Scope:

- Přehled a vyhodnocení energetické náročnosti objektů SčK.
- Přehledový reporting – sestavy z jednotlivých modulů potřebné k rozhodování o investicích či dalším nakládání s majetkem.
- Pořízení HW nástrojů pro vlastní energetický monitoring objektů (termokamery, IOT měřidla).
- Distribuce přístupů na jednotlivé PO dle míry jejich oprávnění s integrací na centrální správu uživatelů (IDM – identity management), integrace na modul MAJ.

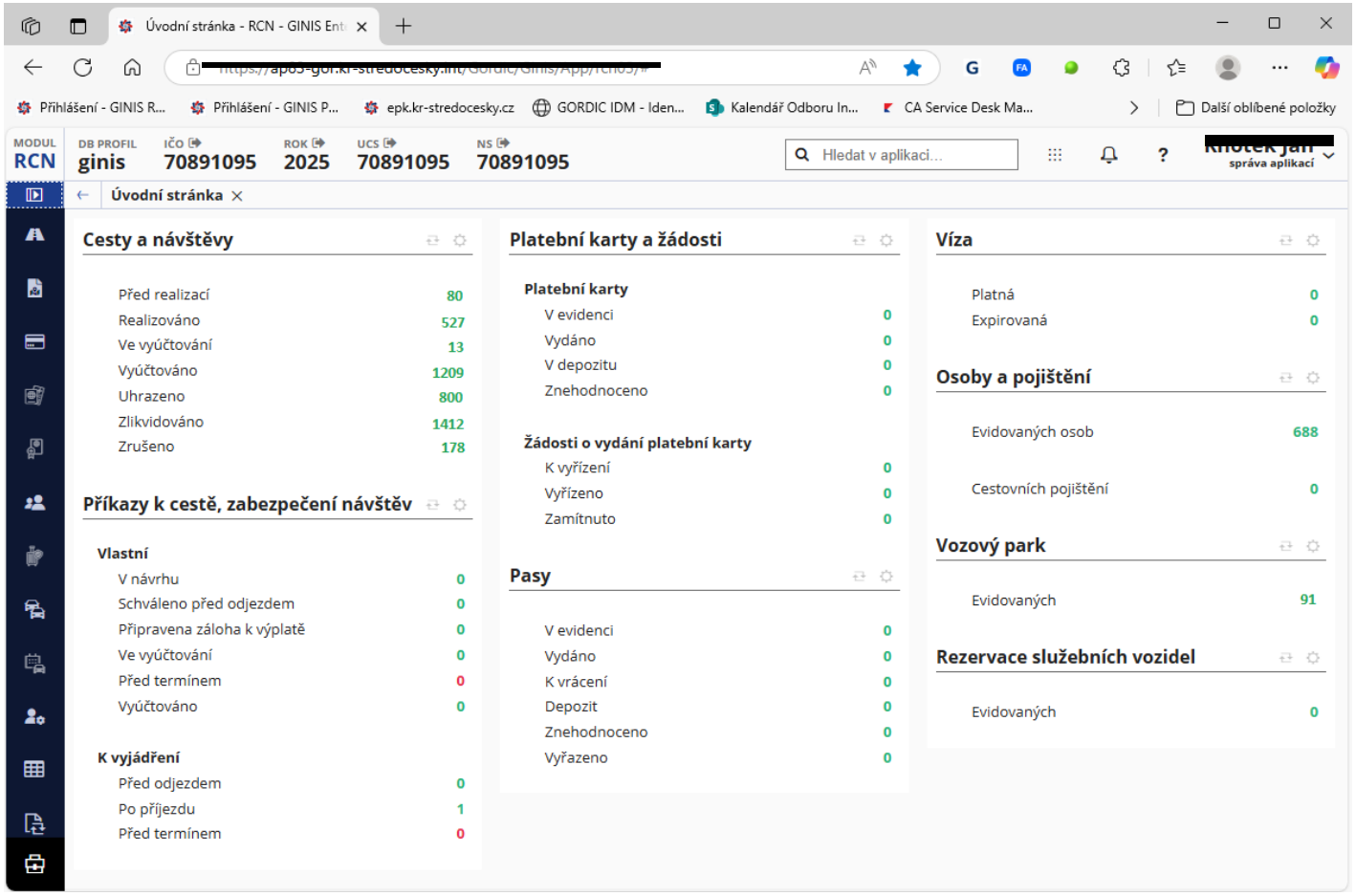
Aktuální stav:

- Příprava cílového konceptu vč. požadavků na infrastrukturu (1 fáze projektu – 4 měsíce). Zpracován formulář OHA – požadavek na dodatečné spolufinancování EU z Integrovaného regionálního operačního programu 2021-2027

Dle katastru nemovitostí má SčK ve svém vlastnictví evidováno více než 1.700 budov a přes 25.000 pozemků. Většina nemovitého majetku je svěřena do hospodaření některé z 260 příspěvkových organizací (PO) Středočeského kraje, které jsou zároveň zodpovědné za jeho správu.

Realizace služebních cest a návštěv - RCN (GINIS)

- Komplexní realizace pracovních cest, kalkulace záloh, jejich vyúčtování a rezervace služebních vozidel – nasazení 2024
- Provázanost s dalšími EKO agendami (alokace finančních prostředků, zakládání dokladů, elektronická podpisová kniha)
- Aktuální stav:
  - Dokončeny tuzemské pracovní cesty
  - Komplexní worfklow (vyúčtování)
- Plán do 12/2025
  - Zahraniční cesty
  - Rezervace služebních vozidel (vozový park)
- Problematika „digitalizace agendy“



Vzdálené pečetění a podepisování

- **Software 602 -** služby pro vzdálené podepisování a pečetění (testování 3 měsíce, aktuálně produkční provoz)
- Náhrada 2 smluv OHS/OINF – Česká pošta - Certifikační autorita PostSignum
- Služby poskytovány pro KÚ a PO (pouze časová razítka) v rozsahu informačních systémů:
  - ICZ e-spis
  - ICZ e-spis Lite
  - GINIS
  - Kissos (Sociální systém) – bude implementováno

NÚKIB

- Kontrola – červenec 2024

4 typy zjištění:

- potenciální rizika (systém řízení bezpečnosti informací, řízení rizik, plán zvládání rizik, bezpečnost lidských zdrojů, řízení kontinuity činností, fyzická bezpečnost)
- neshody (organizační bezpečnost, řízení dodavatelů, bezpečnostní politika a bezpečnostní dokumentace, audit kybernetické bezpečnosti)
- příležitost ke zlepšení (Řízení aktiv)
- pozoruhodné úsilí (Bezpečnost komunikačních sítí)

Odbor bezpečnosti (KO), Odbor informatiky (skoro OK)

Středočeský kraj

Děkuji za pozornost