

Projektový záměr

Projektový záměr vychází z vládou schválené Koncepce ICT (Příloha č. 3) a z připravované strategie ICT 2015+. Přes snahu průběžně modernizovat technologickou infrastrukturu MPSV, se tato infrastruktura dostala do stavu, kdy část technologických prostředků je zastaralá morálně i výkonově, není výrobcí podporována a nachází se v zásadně nevyhovujících datových centrech. MPSV již zahájilo první kroky vedoucí k nápravě a modernizaci infrastruktury, avšak pro dokončení modernizace je potřebné realizovat řadu projektů. Projekty požadované zadavatelem v rámci zakázky na Rozvoj KSI MPSV plně respektují požadavky na tuto obnovu a modernizaci.

Oblast Datových center

V současné době disponuje MPSV dvojicí hlavních datových center a třetím, menším datovým centrem. Třetí datové centrum poskytuje zázemí pro umístění technologické infrastruktury určené pro informační podporu pracoviště MPSV nacházejícího se v lokalitě Podskalská.

První z hlavních datových center je umístěno v suterénu budovy MPSV v Praze v ulici Na Poříčním právu 1 (dále jen DC NPP) a historicky vytvářelo primární lokalitu, kam byla umísťována technologická infrastruktura. V lokalitě Praha, Sokolovská 855 bylo vybudováno druhé, sekundární datové centrum (dále jen DC SOK) původně zamýšlené jako sekundární datové centrum pro zajištění vysoké dostupnosti rozproštěním poskytovaných aplikačních služeb a umístění datových úložišť do dvou lokalit v rámci Prahy (tzv. metro-cluster). V současné době je však situace víceméně obrácená a za primární datové centrum lze považovat DC SOK.

DC NPP je vystaveno v dnes již nevyhovujících historických prostorách. Z hlediska problematického fyzického přístupu, nemožnosti umístění dalších technologií, kapacity rozvodné elektrické sítě, neexistence náhradního nezávislého energetického zdroje, nedostatečného chlazení (klimatizace) a absenci automatizovaného hasicího systému je toto centrum nevyhovující požadavkům na moderní datové centrum.

Situace v DC SOK je lepší zejména díky existenci hasicího systému, dostatečnému příkonu elektrické rozvodné sítě, redundantního připojení do energetické sítě, dostatečné nosnosti podlahových ploch a výkonné klimatizaci. Bohužel i toto datové centrum se začíná potýkat s omezenou možností umístění dalších technologií a je velmi problematicky přístupné, což může fatálně ohrozit centrum zejména v souvislosti s řešením přírodních katastrofických událostí.

Revitalizace datových center či jejich náhrada v lokalitách vlastněných či pronajímaných MPSV je činnost nákladná a z pohledu kompetenční činnosti resortu podpůrná. Budování privátních datových center jednotlivých resortů státní správy je také v rozporu s vládní koncepcí využívání služeb v oblasti ICT napříč resorty.

Do budoucna tak MPSV přesune technologickou infrastrukturu ze svých datových center do datových center státem centrálně poskytovaných resortům (například datové centrum Státní tiskárny cenin) a bude je využívat formou služby se smluvně zajištěnou kvalitou (SLA).

Takovýto přístup sejme z MPSV potřebu kvalifikovaně provozovat datová centra, zajišťovat jejich rozvoj a řešit otázku jejich zabezpečení.

V konkrétní rovině tak MPSV v budoucnu plánuje využívání dvojice - primárního a záložního - datových center, geograficky vzdálených v rámci Prahy. Ty budou doplněny o třetí menší datové centrum (v další lokalitě) za účelem vyhodnocování a řízení přepínání provozu mezi primárním a záložním datovým centrem. Datová centra pak budou doplněna o lokalitu, v rámci které budou ukládána archivační a záložní média.

S ohledem na ochranu investic a z důvodu bezpečnosti přístupu k aplikacím a datům budou v datových centrech umístěny technologie ve vlastnictví MPSV, vytvářející nejnížší vrstvu výpočetní platformy.

Projekt revitalizace datových center si klade za cíl v období 2015 až 2017 vybudovat moderní technologickou platformu flexibilního charakteru, která umožní pružně a rychle reagovat na požadavky jejího využití. Za účelem vytvoření této platformy dojde k realizaci následujících kroků:

- Dokončení modernizace technologií umístěných v datových centrech a ukončení provozu zastaralých a nepodporovaných technologií.
- Realokaci technologické infrastruktury do nových datových center ve společné infrastruktuře státu.
- Využívání bezdrátových komunikačních technologií v lokalitách MPSV a ÚP jako hlavní komunikační technologie, podpořené přechodem na protokol IPv6 a dokončením konvergence hlasových služeb v datové síti.
- Dobudování výpočetní platformy na základě plně virtualizovaného prostředí a vytvoření standardizovaných aplikačních rámců pro potřeby nasazování vyvíjených aplikací a systémů.

Tato oblast je řešena projekty:

- Konsolidace datových center - fáze 2
- Vybudování komunikační infrastruktury pro nové datové centrum
- Upgrade a virtualizace ACS serverů
- Virtualizace serverů v demilitarizované zóně (DMZ)
- Zajištění VPN přístupu servisních organizací do nového datového centra
- Zvýšení odolnosti centrálního DDI (DNS, DHCP, IPAM)
- Optimalizace služby NTP
- Upgrade serverů s Win 2003 na Win 2008 či vyšší verzi
- Obměna nepodporovaného HW v Datových centrech

Oblast komunikační infrastruktury

Již v uplynulém období začala být komunikační infrastruktura MPSV a ÚP budována způsobem, který je v souladu s vizí následujících období.

Prvním z klíčových aspektů je využívání komunikační infrastruktury státu (KIVS – Komunikační infrastruktura veřejné správy) pro propojení resortních organizací a poboček a kontaktních pracovišť ÚP. Tento trend je, v souladu s koncepcí eGovernmentu, nezbytné zachovávat a dále posilovat například v rámci přechodu datových center do infrastruktury státu.

Dalším aspektem je již realizovaný přechod poskytování hlasových služeb na základě datové komunikace¹. Tento přístup přináší možnost vytvoření skutečně jednotné, konvergované komunikační

¹ Tzv. IP telefonie využívající IP protokolu k přenosu digitalizované hlasové komunikace.

základny, ochranu investic v souvislosti s využíváním infrastruktury datové komunikace a možnost dalšího zpracování digitálních hovorů.

Přes výše uvedené však existuje několik oblastí, kterým je z budoucího hlediska potřebné věnovat pozornost a ke kterým v oblasti komunikací směřovat.

První takovou oblastí je zavedení komunikačního protokolu IP verze 6 (dále též jen IPv6), nahrazujícího verzi 4, na jejímž základě je vybudována síť Internet a je téměř výhradně využívána všemi typy organizací pro budování jejich sítí. Zavedení tohoto protokolu uvnitř resortu tak do budoucna zejména zabráni stávajícím problémům v kolizích adres síťových zařízení a přinese zvýšenou úroveň zabezpečení v důsledku jednoznačné a nezaměnitelné identifikace síťových zařízení účastníků se komunikace. Přejít na protokol IPv6 je navíc vyžadován usnesením vlády č. 727 ze dne 8. června 2009 a je tak nezbytnou podmínkou souladu ICT MPSV s legislativou.

Další oblastí, která zaznamenala v uplynulých letech zásadní rozmach, je využívání bezdrátových sítí v rámci organizací. Moderní technologie již poskytují dostatek prostředků v oblasti zabezpečení těchto sítí tak, že tyto mohou být bez obav využívány i pro potřeby privátní komunikace. Navíc používání bezdrátových sítí je nezbytnou premisou pro zavádění využívání mobilních zařízení a na ně orientovaných informačních služeb. Přestože MPSV již v některých oblastech využívá bezdrátových sítí je nezbytné tyto pilotní aktivity nadále rozpracovat, stanovit jednoznačnou koncepci využívání bezdrátových sítí a vybudovat potřebnou infrastrukturu.

Obecně lze říci, že v oblasti komunikační infrastruktury MPSV nastoupilo správný směr, který je nezbytné dále prohlubovat a rozvíjet nejenom s moderními technologickými trendy ale i v souladu s budováním eGovernmentu v České republice.

Tato oblast je řešena projekty:

- Globální analýza měnících se požadavků na KI a návrh efektivního zajištění souladu služeb poskytovaných KI
- Implementace šifrování ve WAN MPSV
- Unifikace IP VPN ve WAN MPSV
- Migrace Ethernet spojnic na IP VPN, nasazení šifrování, redukce počtu směrovačů
- Změna telekomunikačního operátora v rámci KIVS
- Mobilita uživatelů - bezdrátové připojení do KI MPSV
- Implementace MS Lync a integrace s videokonferencí
- Upgrade videokonferencí
- Redesign zálohování ve WAN
- Způsob publikace do internetu pomocí virtuálního prostředí - zabezpečený přístup k aplikacím
- Centrální systém testování odezvy WAN
- Rozvoj zastřešujícího monitoringu
- Ad-hoc testování odezvy WAN

Oblast výpočetní platformy

V uplynulých letech došlo v oblasti výpočetní platformy k jejímu výraznému zastarání. Zastaralá zařízení přináší problémy nejen technického charakteru, ale zejména problémy s postupným ukončováním podpory těchto zařízení ze strany jejich výrobců. Za účelem řešení tohoto problému úřad již zahájil obnovu zastaralých zařízení a jejich náhradu novými.

V souladu s aktuálními požadavky vynucenými nezbytnou modernizací a rozvojem agendových informačních systémů byl zahájen projekt výběrových řízení na nezbytné posílení výpočetní platformy.

Projekty obnovy i posílení infrastruktury probíhají zcela v souladu s moderním trendem virtualizace technologické platformy. Ta umožňuje s využitím konceptu virtuálního výpočetního prostředku poskytovat aplikacím prostředí, kde je možno dynamicky konfigurovat hardwarové parametry a optimalizovat tak přidělování skutečných hardwarových zdrojů. Navíc možnost snadného přenášení virtuálních výpočetních prostředků v rámci technologické infrastruktury (například i mezi datovými centry) přináší nástroje pro zajištění vysoké dostupnosti aplikací.

Virtualizace též umožňuje snadno řešit jeden ze zásadních problémů, s nimiž se obecně potýká podniková ICT – existence a dostupnost testovacích, vývojových a integračních prostředí nezbytných pro vznik nových a realizaci změn stávajících systémů a aplikací. Tato prostředí ať už jsou charakteru dlouhodobého či jsou ad-hoc vytvářena musí svojí strukturou (a ideálně též výkonností) odpovídat prostředím, která budou použita pro cílový provoz. V případě, že není využíváno technologie virtualizace, znamená vytvoření pomocných prostředí další investiční a provozní prostředky v násobcích prostředků potřebných pro realizaci pouze prostředí provozního.

Z hlediska dlouhodobého rozvoje bude pokračováno v již nastoleném trendu virtualizace výpočetní platformy s cílem, že virtualizovány budou všechny výpočetní prostředky poskytované pro provoz aplikací a systémů. Moderní technologie a standardy řízení virtualizovaných prostředí pak umožňují řízení technologie virtualizace různých výrobců, včetně technologií vzniklých na základě volně dostupného software. Ministerstvo se tak nemusí dlouhodobě upínat pouze k jedné technologické platformě a může minimalizovat náklady využitím volně šiřitelného software v oblastech, kde je to možné. Navíc si zachová nezbytnou otevřenost vůči svým dodavatelům, kterou jako orgán veřejné správy musí zachovávat.

V oblasti technologické infrastruktury zálohování a archivace Ministerstvo již disponuje nezbytnými technologiemi. Z hlediska budoucího stavu, je však nezbytné formalizovat interní standardy a procesy tvorby záloh a to včetně procesu ukládání záloh a archivů do lokality mimo datová centra pro případ krizové události likvidačního charakteru.

Dohled a monitoring technologické infrastruktury výpočetní platformy je již zajišťován jak na úrovni vlastní infrastruktury, tak i úrovni virtualizace. Cílem je pak získávané klíčové údaje začlenit do údajů zpracovávaných specializovanými systémy pro řízení kvality a zprostředkovat je i nejvyšší rovině vedoucích pracovníků v oblasti ICT.

Technologie a licence nezbytné k vytvoření výpočetní platformy budou i nadále vlastnictvím MPSV a budou vždy umístěny v technologické infrastruktuře státu ať už ve vlastních či státem poskytovaných datových centrech.

S ohledem na potřebu vysoce odborných znalostí v oblasti moderní výpočetní platformy je nezbytné zajistit návrh její architektury, realizaci i rutinní provoz dodavatelským způsobem. Na úrovni ministerstva pak dále nutné budovat expertní znalost oponentního a kontrolního charakteru pro řízení dodavatelů výpočetní platformy.

Historicky vznikly informační systémy MPSV v době, kdy rozlehlé datové sítě (WAN) byly pomalé, drahé a nestabilní. Z hlediska architektury musely být informační systémy určené pobočkové síti úřadu práce budovány jako distribuované se samostatnými uzly. Takovéto uzly pak spolu komunikovaly a vyměňovaly

si data s centrálním uzlem. Provozované aplikace měly povahu samostatných aplikací instalovaných na počítačích koncových uživatelů. Uvedený přístup pak přinášel a ještě dnes částečně přináší celou řadu problémů spočívajících v synchronizaci dat, aktualizací koncových aplikací a nutnosti správy téměř stovky uzlů – lokálních datových center.

V souvislosti s rozvojem datových komunikačních technologií doplněných o rozvoj technologií používaných ve službě WWW sítě Internet začaly být nové a některé stávající aplikace vytvářeny formou centralizovaných aplikací.

Takováto architektura kromě jiného přináší zjednodušení potřebného aplikačního vybavení koncových zařízení. Z technologického hlediska mohou být aplikace evidenčního a kancelářského typu využívané MPSV realizovány čistě v kontextu moderního prohlížeče WWW stránek. Postupně tak zaniká potřeba využívání plnohodnotného PC jako koncového zařízení uživatele ÚP či MPSV.

Zároveň s výše uvedeným vývojem situace v architektuře aplikací došlo v podnikové sféře k diametrálnímu nárůstu využívání mobilních počítačů – notebooků. Smyslem jejich využívání je jak jejich klesající cena, tak i mobilita (jeli podpořena bezdrátovými komunikačními technologiemi) umožňující efektivitu a dynamiku reorganizace prostor úřadů.

Trendem posledních let je další rozvoj mobilních zařízení reprezentovaných chytrými telefony a tablety. Přestože v současném způsobu práce koncových uživatelů ÚP a MPSV tato mobilní zařízení nemají zcela jasné uplatnění, je naopak oblast řízení resortu místem, kdy tato koncová zařízení mohou být využívána velmi efektivně. Navíc díky jejich rostoucí oblibě nemohou již být tato zařízení opomíjena s ohledem na aplikace určené veřejnosti.

Z hlediska budoucích nákladů a zjednodušení provozní podpory je nezbytné, aby stávající koncová PC byla postupně obměňována za jednodušší zařízení typu tenkého klienta či nenáročných notebooků (netbooků). Zároveň společně s úřadem práce dojde ke zpracování studie vyhodnocující možnost využívání chytrých telefonů a tabletů pro řízení resortu, využívání koncovými uživateli úřadu práce (například při terénní práci) a při komunikaci s veřejností.

Vlastní pořízení či obměna koncových zařízení bude řešena s v soutěži vybraným dodavatelem rámcovým způsobem zaručujícím postupnou obnovu a servis zařízení. Vlastní podpora koncových zařízení na úřadech práce pak může být řešena v případě nefunkčnosti pouhou výměnou normovaného zařízení a jeho předáním dodavateli k servisu.

V oblasti tiskových výstupů je nutné reflektovat trend eGovernmentu minimalizace výměny papírové dokumentace. Na druhou stranu však tiskové výstupy budou potřebné. Současná tisková zařízení jsou však již poměrně autonomní zařízení, která vyžadují pouze doplňování kancelářského materiálu poučeným uživatelem. Vzhledem k velikosti tiskových zařízení je nezbytné smluvně zajistit servis dodavatele zařízení přímo v místě jejich umístění.

Budoucí rozvoj v oblasti tiskových zařízení tak bude evolučně vycházet ze stávající situace a postupně díky inteligenci moderních zařízení bude zjednodušovat svojí infrastrukturu.

Digitalizace listinných dokumentů bude pro nejbližší období dále řešena v rámci jednotlivých úřadů při přijetí dokumentů podatelnou úřadu. Je však nezbytné dopracovat systematický koncept digitalizace a zvážit, zdali stávající model nenahradit modelem využívajícím centrální digitalizaci se svozem dokumentů.

Modernizace koncových zařízení si klade za cíl provést průběžně náhradu stávajících koncových stanic na bázi PC tenkými klienty. Cíle jsou následující:

- Průběžná náhrada PC koncových uživatelů tenkými klienty stacionárními či přenosnými.
- Zavedení využívání mobilních zařízení pro podporu činnosti řídicích pracovníků.

- Zpracování konceptu využívání mobilních zařízení v předmětných činnostech ÚP a MPSV.

Tato oblast je řešena projekty:

- Centrální patch management pro servery
- Konsolidace serverů na ÚP ČR
- Správa koncových stanic MPSV a ÚP ČR
- Virtualizace stanic MPSV/ÚP ČR
- Virtualizace kiosků ÚP ČR

Oblast systémové infrastruktury

Cílem v této oblasti je efektivní řízení a provozování systémových služeb resortu MPSV, tak aby bylo možné těmito službami podporovat provoz aplikací jednotlivých organizací resortu MPSV. Jedná se o služby v následujících oblastech:

- Adresářové služby (Active Directory)
- Elektronická pošta (MS Exchange)
- Identity management (IDM)
- Systém pro evidenci IT majetku (HW, SW)

V oblasti adresářových služeb povede k takové konfiguraci AD, kdy bude každá organizace resortu MPSV (ČSSZ, MPSV + ÚP ČR, SÚIP) pokryta vlastním AD adresářem s jedinou AD doménou. Mezi těmito adresáři bude navázán adresářový vztah důvěry (obousměrný, transitivní).

Služby AD budou zcela centralizovány do datových center na dostatečném počtu kontrolérů zajišťujících služby AD. Služby AD budou rozprostřeny mezi datovými centry tak, aby umožnily plnou geografickou vysokou dostupnost. Datová struktura služby AD bude členěna do organizačních jednotek tak, aby v maximální míře umožnila delegaci správy datového obsahu služby. Součástí služby AD bude též služba DNS, provozovaná na doménových kontrolérech a řízená systémem IPAM (viz strategie v oblasti síťových a hlasových služeb).

Směr v oblasti elektronické pošty je takový, že každá organizace resortu (CSSZ, MPSV + ÚP ČR, SUIP) bude pokryta vlastní Exchange Organizací. Exchange bude integrován v AD adresáři příslušné Organizace. Služby MS Exchange budou zcela centralizovány v datových centrech a budovány s ohledem na možnost rozšiřitelnosti (velikost schránky, počet uživatelů apod.). Služby MS Exchange budou rozprostřeny mezi datová centra tak, aby umožnily plnou geografickou vysokou dostupnost.

Pro příjem pošty z internetu a odeslání do internetu budou organizace resortu využívat systém poštovních bran, který poskytne zároveň první úroveň virové, spamové a malware kontroly.

O životní cyklus uživatelských účtů se bude starat IDM systém, přímo napojený na systémy oddělení správy lidských zdrojů (personálních oddělení). Každá organizace MPSV bude používat vlastní systém, napojený na její AD adresář. IDM systém bude plnit především následující funkce (dle potřeb další):

- Založení uživatelského účtu a vyplnění mandatorních atributů (na základě pracovního zařazení, lokality apod.)

- Zařazení účtu do skupin pro získání přístupů do aplikací příslušející danému pracovnímu zařazení (rolí) metodou single sign on (SSO)
- Spuštění schvalovacího procesu pro získání přístupů do aplikací
- Zařazení účtu do skupin pro získání oprávnění k nakládání s klasifikovanými informacemi způsobem odpovídajícím přiřazené roli
- Vytvoření Emailové schránky s požadovanými parametry (limity apod.)
- Změny v attributech účtu během fáze jeho existence (např. změna jména, lokace, pracovní pozice a členství ve skupinách apod.)
- Zneplatnění účtu při přerušení nebo ukončení pracovněprávního vztahu
- Smazání účtu

Služby IDM budou rozprostřeny mezi datovými centry tak, aby umožnily plnou geografickou vysokou dostupnost.

Pro evidenci IT majetku (HW i SW) bude provozován systém, který bude plnit následující funkční požadavky:

- Evidence vlastnictví majetku a možnosti propojení na modul majetku systému EKIS (SAP, Ginis)
- Evidence vlastnictví software a podpora licenční čistoty (SW Asset Management)

Tato oblast je řešena projekty:

- Migrace aktiv directory (AD), MS Exchange, Certifikační autority (CA) z Cloudu
- Monitorování MS Infrastruktury
- IDM - Náhrada současného řešení ISU (MIIS)
- Evidence IT majetku a správy SW licencí

Oblast zajištění bezpečnosti

IT bezpečnost, jejíž součástí jsou kybernetická a informační bezpečnost, je nedílnou součástí jednotného systému řízení bezpečnosti resortu MPSV. Základním cílem v této oblasti je vytvoření bezpečného IT prostředí, kde veškerá informační aktiva budou odpovídajícím způsobem chráněna proti vnějším i vnitřním hrozbám. Musí být zajištěn soulad s existující i připravovanou legislativou (zákon o kybernetické bezpečnosti). Musí být průběžně vyhodnocovány bezpečnostní trendy a bezpečnostní opatření budou v těchto souvislostech aktualizována. V souladu s navrženým systémem jednotného řízení bezpečnosti resortu MPSV bude vytvořena odpovídající bezpečnostní dokumentace. Uvedených cílů bude dosaženo implementací opatření, navržených po důkladné bezpečnostní analýze celého ICT prostředí resortu MPSV při zahrnutí již existujících analýz a respektující již fungující řešení.

Pro zajištění IT bezpečnosti resortu je nezbytné mít schopnost detekovat a zvládat bezpečnostní incidenty a také mít schopnost o nich informovat. Proto je nutné:

- Vybudovat a udržovat schopnost řešit incidenty kybernetické a informační bezpečnosti zřízením resortního dohledového centra stavu kybernetické a informační bezpečnosti – tzv. resortní CSIRT (Computer Security Incident Response Team)



Projektový záměr

Příloha č. 9

- Zavést a udržovat systém pro průběžné hodnocení a řízení zranitelností a jejich evidenci v systému pro řízení znalostí
- Zavést a udržovat systém pro zvládání bezpečnostních incidentů
- Zavést a udržovat systém pro spolupráci s autoritami v oblasti kybernetické bezpečnosti (NBÚ - Národní Bezpečnostní Úřad, NCKB - Národní Centrum Kybernetické Bezpečnosti)
- Zavést a udržovat systém pro řízení a sdílení znalostí o zranitelnostech a hrozbách v resortu MPSV i na národní úrovni

Tato oblast je řešena projekty:

- Vytvoření systému infrastrukturní autentizace
- Nasazení procesů pro SOC
- Náhrada internetových loadbalancerů
- Bezpečnostní standardy KI - etapa B
- SOC - Q-radar SIEM (IBM) a Flowmon (Invea)
- Systém pro detekci pokročilého malware (antibot, 0.day malware,...)
- Systém pro pokročilou detekci průniků IDS /IPS
- Zabezpečení dat na PC a mobilních zařízeních
- Nasazení systému ochrany důvěrnosti dat (DLP) + Klasifikace dat MPSV
- Upgrade FW soustavy (interní)
- Nasazení Aplikačních FW soustavy
- Filtrování internetového provozu
- Ochrana proti DDOS útokům
- Zabezpečení fyzického přístupu do počítačové sítě
- Nasazení Mobile Device Management(MDM)