Technologické centrum obce s rozšířenou působností

Technology centrum of ORP

Martin Maňásek

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Martin MAŇÁSEK**
Osobní číslo:	**A07256**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Informační a řídicí technologie**
Téma práce:	**Technologické centrum obce s rozšířenou působností**

Zásady pro vypracování:

V rámci strategie rozvoje eGovernmentu ve státní správě a samosprávě spustilo ministerstvo vnitra ambiciózní projekt "Smart Administration", který řeší elektronizaci veřejné správy. Celý projekt začal šířením kontaktních míst CzechPoint v obcích a městech všech úrovní, pokračuje v současnosti spouštěním informačního systému datových schránek a následně bude pokračovat zřízením eGon center, která budou poskytovat administrativní, školicí a technologickou podporu pro obce I. a II. typu. Tato centra budou umístěna na obcích s rozšířenou působností a na krajích.

1. **Vytvořte analýzu současného stavu.**
2. **Zpracujte studii proveditelnosti a samotné realizace tvorby technologického centra. Bude se jednat o výkonné zařízení blade-ového typu (zvlášť aplikační a databázové servery) s diskovým polem, zálohováním, nastavení firewallových politik.**
3. **Zvažte zavedení virtualizace.**
4. **Zaměřte se na popis principů komunikace mezi jednotlivými organizacemi, nabízené služby.**
5. **Zahajte samotnou realizaci tohoto projektu.**

Rozsah bakalářské práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **PUŽMANOVÁ, Rita. TCP/IP v kostce. [s.l.] : Kopp, 2009. 619 s. ISBN 978-80-7232-388-3.**
2. **DOSTÁLEK, Libor a kolektiv. Velký průvodce protokoly TCP/IP: Bezpečnost. [s.l.] : Computer Press, 2003. 592 s. ISBN: 80-7226-849-X.**
3. **Zákon č. 365/2000, Sb., o informačních systémech veřejné správy Zákon č. 300/2008, Sb., o datových schránkách.**
4. **NORTHCUTT, Stephen, et al. Bezpečnost počítačových sítí : Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě. [s.l.] : Computer Press, 2005. 592 s. ISBN: 80-251-0697-7.**
5. **RUEST, Danielle, RUEST, Nelson. Virtualizace : Podrobný průvodce. [s.l.] : Computer Press, 2010. 408 s. ISBN: 978-80-251-2676-9.**

Vedoucí bakalářské práce: **doc. Ing. Martin Sysel, Ph.D.**
Ústav počítačových a komunikačních systémů

Datum zadání bakalářské práce: **5. března 2010**

Termín odevzdání bakalářské práce: **1. června 2010**

Ve Zlíně dne 5. března 2010

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Ing. Ivan Zelinka, Ph.D.
ředitel ústavu

ABSTRAKT

Tato bakalářská práce je zaměřena na popis tvorby Technologického centra města Otrokovice. V Teoretické části jsou popsány vize koncepce vlády České republiky „Efektivní veřejné správy a přátelských veřejných služeb“, význam Technologických center a navazující projekty. V praktické části jsou popsány konkrétní kroky při přípravě Technologického centra. Jedná se zejména o analýzu současného stavu, stanovení hardwarové konfigurace, popisu komunikací a konkrétních postupů při realizaci projektu.

Klíčová slova:

Technologické centrum, Obec s rozšířenou působností, Centrální místo služeb, Komunikační infrastruktura veřejné správy

ABSTRACT

This work is aimed at describing the creation of the Technology Centre of the town Otrokovice. In the theoretical section are described visions of the concept of the Czech Republic Government "Effective public administration and public service friendly, the importance of technology centers and related projects. The practical part describes the specific steps in the preparation of the Technology Centre. These include analysis of current status, determine hardware configuration, describe communication and the specific procedures for project implementation.

Keywords:

Technology Centre, Municipality with Extended Competence, the Central Location of Services, Communication Infrastructure of Public Administration

Chtěl bych touto cestou velmi poděkovat:

doc. Ing. Martin Sysel, Ph.D., Fakulta aplikované informatiky Univerzity Tomáše Bati ve Zlíně, za pomoc při výběru tématu, sestavování obsahu, poskytnutí materiálů a cenných rad při tvorbě bakalářské práce.

Ing. Marie Malíková, tajemník MěÚ Otrokovice, za podporu a schválení vybraného tématu.

Ing. Josef Řihošek, vedoucí odboru provozního, MěÚ Otrokovice, za podporu a cenné rady z praxe.

Ing. Pavel Sedláček, vedoucí systémového oddělení, Vera, spol. s r.o., za metodickou pomoc při implementaci elektronické spisové služby

Josef Vávra, Senior Security Konsultant, Trusted Network Solutions, a.s., za poskytnutí materiálů a metodickou pomoc při implementaci UTM

Roman Hlaváč, Mid Market Solution Manager, IBM Česká republika, spol. s r.o., za poskytnutí materiálů a konzultací při stanovování optimální hardwarové konfigurace

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….…….

podpis diplomanta

OBSAH

ÚVOD

Projekt Technologické centrum města Otrokovice vychází z konceptu realizace rozvoje služeb eGovernmentu v obcích, jak byl popsán v základních dokumentech vydaných Ministerstvem vnitra České republiky. Pro stanovení nejvýhodnějšího řešení byla zpracována analýza současného stavu, která proběhla v obcích I. a II. stupně na území správního obvodu Obce s rozšířenou působností (ORP) a na Městském úřadě v Otrokovicích.

Cílem projektu je vytvoření základního rámce služeb eGovernmentu v regionu ORP s návazností na stanovenou celostátní Strategii realizace Smart Administration v období let 2007–2015. Projekt zohledňuje jak specifika ORP Otrokovice, tak i současný stav informatizace a realizovaných či připravovaných projektů.

I. TEORETICKÁ ČÁST

1 EFEKTIVNÍ VEŘEJNÁ SPRÁVA A PŘÁTELSKÉ VEŘEJNÉ SLUŽBY

Strategický rámec projektu Technologických center vychází ze stanovené strategie efektivní veřejné správy dané dokumentem „Efektivní veřejná správa a přátelské veřejné služby“ – Strategie realizace Smart Administration v období 2007–2015. [23] Tato centrální strategie je doprovázena legislativními změnami (zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů a zákon č. 111/2009 Sb., o základních registrech).

1.1 Strategie realizace Smart Administration v období 2007-2015

Vláda české republiky vytyčila základní směřování ke zkvalitňování veřejné správy ve strategii Efektivní veřejná správa a přátelské veřejné služby (Smart Administration). V projektu Rozvoj služeb eGovernmentu v obcích jsou zásadní tyto stanovené strategické cíle:

- Efektivnější činnost úřadů, snížení provozních finančních nároků a zajištění transparentního výkonu veřejné správy,
- Přiblížení se veřejné služby občanovi a zajištění jejich maximální dostupnost a kvalitu.

Z pohledu koncepce budování Technologických center je zásadní stanovení cíle v oblasti infrastruktury:

- „Vytvoření robustní, bezpečné a efektivní infrastruktury, schopné zprostředkovat přístup k datovým zdrojům s potenciálem dalšího rozvoje“. [23]

1.2 Strategie implementace eGovernmentu do území

Materiál zabývající se implementací eGovernmentu do území byl vytvořen na půdě ministerstva vnitra v roce 2008. Definuje záměry státu při implementaci eGovernmentu do území formou typových projektů, které je důležité realizovat pro naplnění cílů strategie Smart Administration. Projekty jsou koncipovány v souladu s Integrovaným operačním programem a Operačním programem lidské zdroje a zaměstnanost. Tímto odstraňují základní požadavek, a to odstranění územních disparit vývoje informatizace na území ČR.

Strategie implementace eGovernmentu do území zároveň ukazuje, že řada informačních problémů regionu může být efektivně řešena jen ve spolupráci kraje a ORP, obcí II. a I. stupně a dalších součástí veřejné správy regionu a ostatních partnerů. V rámci realizace je nutno vyřešit technické otázky typu vzájemné výměny dat a veřejného poskytování služeb jednotlivých informačních systémů. Současně je klíčové dlouhodobě spravovat a využívat informační toky i samotné informace a znalosti jako jedny ze zásadních zdrojů regionu.

Vymezení a uspořádání cílů

- Strategický cíl
    - Jedním ze strategických cílů ORP je „Efektivní správa věcí veřejných“ [23]
- Globální cíl
    - Zajistit rovnovážný rozvoj eGovernment služeb v území, kde se jedná o součinnost ORP a kraje, a využití regionálních eGON center
    - Efektivní rozvoj eGovernment služeb – jedná se o efektivní využití existujících prostředků ICT, optimalizace provozních nákladů a dosažení vyváženého rozvoje ve všech směrech IT [23]
- Specifické cíle
    - Usnadnění komunikace občanů s úřady, kdy systém služeb napomáhá realizovat a optimalizovat procesy vedoucí k uplatňování občanských práv a povinností fyzických a právnických osob (Czech POINT)
    - Zefektivnit běh agend, kdy systém služeb napomáhá k efektivnímu a rychlému výkonu státní správy a samosprávy
    - Zajistit důvěryhodnou správu elektronických dokumentů. Rozvoj eGovernmentu zrovnoprávňuje elektronické dokumenty s papírovými, a proto je nutno zajistit celý životní cyklus uchovávání elektronických dokumentů.
    - Zajistit dostupnost informací. Cílem je tedy vytvořit služby podporující efektivní správu a rozhodování dostupností kvalitních informací v reálném čase a v rozsahu odpovídajícím potřebám jednotlivých agend. [23]

1.3 Informace o vývoji projektu

Implementace eGovernmentu vyžaduje vytvoření, provoz a údržbu infrastruktury pro zpracování klíčových dat regionu prostřednictvím systémů, jako jsou elektronické spisové služby, datové sklady, digitální mapy veřejné správy atd. K tomu slouží i vybudování Technologických center ORP a krajů. Na úrovni krajů a ORP získá informatika výrazně regionální charakter. Funkcionalita Technologických center bude postupně rozšiřována implementací nových služeb.

Primárním cílem Technologického centra je zajistit s obcemi v území ORP konzistentní technologický systém vytvořením robustního, škálovatelného a rozšiřitelného prostředí pro zpracování potřebných aplikací. Technologické centrum ORP bude schopno přenášet, uchovávat a zpracovávat velké množství dat, které bude možno v reálném čase prezentovat uživatelům systému. Partnery projektu jsou obce v území ORP Otrokovice, jejich organizace a samotné město Otrokovice. Předpokládanými výstupy projektu jsou síťová infrastruktura, serverová infrastruktura, vizualizace, negarantované úložiště a zálohování a obnova včetně implementovaných softwarových produktů.

V Technologickém centru budou provozovány kromě centrálních služeb a aplikací pro potřeby samospráv obcí a centrálních projektů všechny aplikace samotného MěÚ Otrokovice. Stávající vybavení serverové výpočetní techniky bude využito pro vytvoření záložního centra, které by bylo schopno v případě totálního výpadku Technologického centra zajistit náhradní provoz strategických aplikací.

Druhým stěžejním cílem tvorby Technologického centra je pořízení, či upgrade elektronické spisové služby, splňující požadavky dané zákonem 499/2004 Sb., o spisové službě a archivnictví, ve znění pozdějších předpisů. Zajistit její údržbu a provozování jak pro ORP a organizace zřízené ORP, tak i pro obce v našem správním obvodu a jejich zřizované organizace. V současné době platná legislativa zrovnoprávňuje elektronické dokumenty s papírovými a tento fakt je nutno zohlednit ve všech fázích jejich životního cyklu. Proto vytvořením Technologického centra chceme umožnit provoz spisové služby a negarantovaného úložiště na všech výše zmíněných subjektech.

1.3.1 Varianty řešení

Již od počátku byly pro samotné řešení Technologického centra uvažovány dvě varianty řešení. První variantou bylo vybudování nového Technologického centra ORP a druhou variantou bylo začlenění stávajících vhodných kapacit ORP do nově budovaného Technologického centra. Většina stávajících hardwarových kapacit není vzhledem k navrhované architektuře plně vyhovující, přestože byly dosud využívány pro zabezpečení provozu agend MěÚ Otrokovice, a proto bude nutné pořídit nové technologie v souladu s navrženou architekturou Technologického centra ORP. Ze stávajících kapacit ORP budou využity tyto prvky:

- 2 x server rackového typu
- 1 x pásková knihovna
- 1 x bezpečnostní UTM zařízení

1.3.2 Etapy projektu

Celý projekt budování Technologického centra je rozdělen do dvou etap:

1. Etapa vybudování Technologického centra a pořízení spisové služby
2. Etapa integrace vnitřního chodu úřadu

Etapa budování Technologického centra je rozdělena do následujících fází:

1. Předinvestiční fáze – zabývá se přípravou projektu
2. Investiční fáze – zabývá se realizací projektu
3. Poinvestiční fáze – zajištění provozu min. po dobu udržitelnosti projektu (5 let)

1.4 Návaznosti na další projekty

Realizace a veřejná podpora tvorby Technologických center vychází z cílů strategie Smart Administration. Tato strategie nepředpokládá ukončení tohoto projektu samotným vybudováním Technologických center krajů a ORP, ale je mnohem ambicióznější a předpokládá další rozvoj služeb eGovernmentu jak v území, tak i v celé veřejné správě.

1.4.1 Informační systém centrálních registrů

Základním kamenem pro budoucí rozvoj je vybudování **centrálních registrů veřejné správy**.

Současná nejednotnost a roztříštěnost v evidenci klíčových dat potřebných pro všechny informační systémy veřejné správy neumožňuje jejich sdílení mezi kompetentními subjekty. Prostředkem pro nápravu tohoto neutěšeného stavu je úprava legislativy. Jedná se zejména o zákon o vytvoření centrálních registrů veřejné správy a návrhy zákonů na realizaci čtyř základních registrů.

Informační systém základních registrů budou tvořit jednotlivé registry, které budou od sebe datově oddělené a relevantní data budou mezi sebou provázána pomocí identifikátoru. Dosavadní identifikátor v současných systémech je rodné číslo, což je z bezpečnostního hlediska nevyhovující a předpokládaným identifikátorem bude číslo občanského průkazu. Informační systém základních registrů bude sestávat z těchto stěžejních částí:

A. RPP – registr práv a povinností

Referenční údaje o působnosti orgánů veřejné moci:

- o agendách
- o orgánech veřejné moci, které je vykonávají
- o informačních systémech, které pro výkon agend používají, a o rozsahu oprávnění přístupu k referenčním údajům
- v budoucnu návaznost na eSbírku

Referenční údaje o právech a povinnostech osob

- údaje o rozhodnutích, na jejichž základě došlo ke změně referenčních údajů v základních registrech
- údaje o dalších právech a povinnostech osob, pokud tak stanoví jiný právní předpis

B. ROB – registr obyvatel

Aktuální referenční údaje:

- o všech občanech ČR
- o cizincích s povolením k pobytu v ČR

- o občanech jiných států vedených v základních registrech (zahraniční vlastníci nemovitostí)

Jaké údaje registr obsahuje?

- příjmení, jméno
- odkaz do registru územní identifikace na adresu místa pobytu
- datum narození a úmrtí
- odkaz do registru územní identifikace na místo a okres narození a úmrtí
- státní občanství

Registr bude obsahovat i **údaje, které jsou podpůrné pro další informační systémy a projekty realizované v oblasti eGovernmentu**:

- čísla elektronických občanských průkazů
- údaj o tom, zda má daná fyzická osoba datovou schránku
- doručovací adresu

C. ROS – registr osob

Údaje o všech osobách, tedy ekonomických jednotkách či subjektech podnikatelského i nepodnikatelského charakteru:

- právnických osobách
- podnikajících fyzických osobách
- orgánech veřejné moci
- organizačních složkách zahraničních právnických osob

Zdroj dat:

- obchodní rejstřík
- živnostenský rejstřík
- další agendové informační systémy

Základním principem, podle něhož je možné daný subjekt považovat za osobu, která bude k nalezení v tomto registru, je registrace či evidence osoby před tím, než zahájí svoji činnost u některého správního subjektu či jiného úřadu.

D. RUIAN – registr územní identifikace adres a nemovitostí

Údaje o základních územních prvcích:

- území státu, katastr, parcela, nemovitost
- kraje, obce, části obcí, ulice, číslo popisné, číslo orientační
- region soudržnosti
- vyšší územní samosprávní celek, kraj, okres, správní obvod obce s rozšířenou působností a obce s pověřeným obecním úřadem
- území obce
- vojenský újezd
- správní obvod v hlavním městě Praze, městský obvod a městská část ve statutárních městech a v hlavním městě Praze
- základní sídelní jednotka, katastrální území, stavební objekt, adresní místo
- pozemek v podobě parcely [21]

Důležitým prvkem systému bude **převodník identifikátorů fyzických osob – tzv. ORG**, jež bude v gesci Úřadu pro ochranu osobních údajů. Činnost ORG je pro ochranu osobních údajů v celém systému základních registrů zcela klíčová. ORG bude jedinou institucí, která dokáže přepočítávat agendové identifikátory z jednoho registru pro druhý. Už tedy nebude možné díky znalosti rodného čísla získat o tomto obyvateli informace prakticky z každého informačního systému veřejné správy, jako to lze nyní. [20]

Registry ve své cílové podobě vytvoří jednotný a vzájemně provázaný ucelený systém, z něhož bude možno čerpat relevantní data pro všechny subjekty veřejné správy a samosprávy.

1.4.2 Centrální místo služeb / KIVS

Je samozřejmostí, že celá strategie by nebyla životaschopná, kdyby nebyla doprovázena vybudováním kvalitní vysokorychlostní komunikační infrastruktury.

Pro bezpečnou výměnu dat bude využito **komunikační infrastruktury veřejné správy** (KIVS). Tato síť je zabezpečena centrálně, a to na bázi IP. Provozovatelem KIVS je stát a jeho účelem je poskytovat hlasové a datové služby subjektům veřejné správy. V projektu Technologických center hraje klíčovou roli přenosová kapacita spojení mezi

Technologickým centrem ORP a kraje. Dle této přenosové kapacity lze zvolit různá uspořádání Technologických center. Buď jako Stand Alone řešení, či jako součást regionální komunikační infrastruktury s možnostmi vizualizace.

Centrální místo služeb (CMS) je v rámci KIVS jediným místem, kde dochází k výměně dat mezi centrálními informačními systémy. Zároveň je tento bod jediným místem, kde je KIVS připojen do veřejné sítě Internet a k dalším sítím. [14] CMS plní v konceptu eGON center jakousi úlohu centrálního technologického centra, jehož hlavní funkcí je směrem k eGON centrům zabezpečit provoz:

- Generických služeb:
    - Adresářové služby
    - Identity management
    - Jmenné služby DNS
    - Služba přesného času NTP
- Centralizovaných služeb:
    - Poštovní server
    - Antivir
    - Centrální dohledový systém

Některé služby (poštovní server, antivir) bude CMS nabízet pro subjekty v rámci KIVS, které nemají možnost tyto služby provozovat vlastními silami. [22]

1.5 Povinné služby v rámci Technologického centra ORP

Projekt stanovuje základní povinné služby TC ORP:

- Negarantované úložiště nevyřízených a neuzavřených spisů jako výstupů dat ze systému elektronické spisové služby nebo dokument management systému
- Elektronická spisová služba [22]

Vzhledem k předpokládanému rozšiřování těchto povinných služeb budou i pořizované budoucí hardwarové prostředky vyhovovat koncepci TC ORP a budou do něj integrovány

2 POPIS KOMUNIKAČNÍ INFRASTRUKTURY VEŘEJNÉ SPRÁVY

Jedním z klíčových prvků rozvoje eGovernmentu v České republice je komunikační infrastruktura. Páteřní síť tvoří komunikační infrastruktura veřejné správy (KIVS). Jedná se o síť napříč celou republikou sahající do všech bývalých okresních měst. Tato síť je galvanicky oddělena od všech ostatních sítí a je využívána pouze pro účely zajišťování dat a informací pro výkon veřejné správy.

Současný rozvoj eGovernmentu umocňuje nutnost využívat kvalitní a bezpečnou vysokorychlostní komunikační infrastrukturu. Ta slouží k propojení strategických uzlů ve smyslu Technologických center ORP a krajů, které budou poskytovat elektronické služby i ostatním subjektům a obcím. Menší obce by si z vlastních finančních zdrojů nikdy tyto služby nezřídily. Tím se pomohou dorovnávat rozdíly v elektronizaci mezi regiony a jednotlivými obcemi.

Datový provoz a žádosti o informace celé KIVS bude řídit a dohlížet Centrální místo služeb (CMS). To zajistí vzájemné řízené a bezpečné propojení subjektů veřejné a státní správy. Mimoto zajistí i komunikaci subjektů veřejné a státní správy s ostatními i neveřejnými subjekty ve vnějších sítích. Tím mám na mysli síť Internet či komunikační infrastrukturu Evropské unie. CMS vytvoří jediné logické místo pro propojení operátorů telekomunikačních infrastruktur poskytujících služby pro KIVS.

2.1 Nabízené služby ORP pro obce a organizace

Při spuštění projektu TC ORP budou obcím v našem správním obvodu nabídnuty pouze základní služby vyplývající jako povinné z projektu č. 06 z Integrovaného operačního programu, prioritní osa č. 2 Zavádění ICT v územní veřejné správě, oblast podpory: 2.1 Zavádění ICT v územní veřejné správě. Jedná se o zajištění služby negarantovaného úložiště, které bude využíváno jako datový prostor pro neukončené spisy z elektronických spisových služeb a služby hostované elektronické spisové služby. Tato spisová služba bude včetně databáze instalována na TC ORP a přístup k této službě bude zajištěn přes síť Internet. Administrace bude zajištěna pracovníky oddělení informatiky MěÚ Otrokovice.

K těmto povinným službám bude subjektům zapojeným do projektu TC ORP automaticky nabízeno zálohování dat uložených v technologickém centru a zajištění

provozu a dohledu celého řešení jak z pohledu infrastruktury, tak z pohledu lidských zdrojů.

Další rozšiřující nabídka možných služeb vyplývá z analýzy, která byla provedena pomocí dotazníků, a jsou uvedeny v tabulce č. 3. Jedná se zejména o služby:

- centrální spisovny, která by nezávisle na hostově systému evidovala veškeré spisy pořízené pomocí elektronické spisové služby;
- konverze dat do PDF, kdy v současné chvíli si tuto povinnost zajišťuje každá obec samostatně;
- kopie centrálních registrů, v rámci optimalizace procesů by každý den proběhla off-line replikace centrálních registrů a klienti našich služeb by se pro požadované informace nemuseli dotazovat přes CMS, ale tyto informace by jim byly poskytnuty samotným TC ORP;
- poskytování digitální mapy veřejné správy sestavené z tematických vrstev, jako jsou digitální ortofotomapy, digitální katastrální mapy, účelové katastrální mapy a technické mapy vytvořené v rámci činnosti samospráv, a to včetně metadat;
- portál občana – CzechPoint@home.

Dalšími nabízenými službami by mohly být redakční systém, webhosting, elektronické zadávání zakázek, školský systém, finanční systémy, schránky elektronické pošty, provoz domén, základní zabezpečení (antivir, antispam, firewall) atd. Nabídka těchto služeb bude řízena poptávkou ze strany subjektů zapojených do projektu. Všechny subjekty budou nejprve na pravidelných schůzkách seznámeny s vývojem projektu a s možností nabízených služeb.

Mimo výše uvedené plánované služby stojí oblast metodické pomoci a vzdělávání. Již v minulém roce při spouštění ostrého provozu informačního systému datových schránek bylo uspořádáno několik schůzek s dotčenými subjekty. Všichni určení zástupci těchto subjektů byli proškoleni k obsluze datových schránek a byla jim poskytnuta metodická pomoc s aktivací datových schránek a s instalací kvalifikovaných certifikátů, které využívají pro podepisování elektronických dokumentů. Na MěÚ Otrokovice vzniklo eGON centrum, které si klade za cíl právě kvalitní vzdělávání a metodickou pomoc jak samotným úředníkům MěÚ, tak i uživatelům z ostatních subjektů. Pro tyto účely máme vybavenou školicí místnost vzdělávání, kde budou probíhat školení po celou dobu udržitelnosti Technologického centra ORP.

2.2 Služby mezi ORP a Centrálním mítem služeb

Centrální místo služeb bude zabezpečovat komunikaci a datové toky v rámci KIVS. Jelikož se bude jednat o jediné místo, kde spolu mezi sebou komunikují různé systémy, bude CMS plnit v konceptu eGON center úlohu centrálního Technologického centra (TC C). Hlavní funkcí je směrem k eGON centrům, zabezpečit provoz:

Generických služeb:

- adresářové služby,
- Identity management,
- jmenné služby DNS – zajišťují překlad IP adres na jména v prostředí eGON center,
- služba přesného času NTP – zajišťuje synchronizaci přesného času jednotlivých eGON center s CMS.

Dalších centralizovaných služeb:

Poštovní server – poskytuje služby pro ORP, které nemají vlastní poštovní server.

Antivir – odvirovávání dat, která přicházejí do eGON centra prostřednictvím CMS na úrovni protokolu HTTP, FTP, SMTP a provádí detekci virů v jazycích Java a ActiveX.

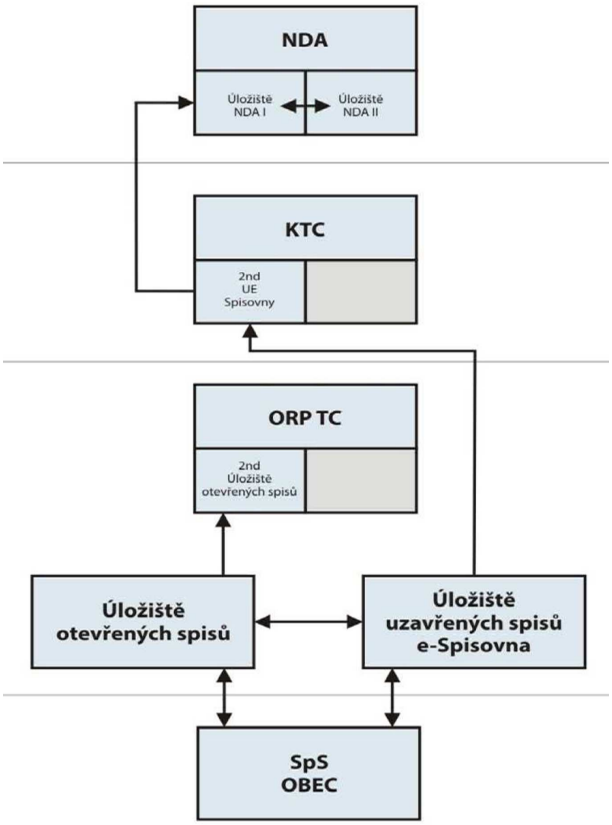
Centrální dohledový systém – zajišťuje kontrolu dostupnosti eGON center a umožňuje jejich správu. [22]

2.3 Komunikace mezi ORP a obcemi a Zlínským krajem

Komunikaci mezi jednotlivými subjekty projektu eGON center a jejich nabízených služeb nejlépe dokladuje následující schéma.

Subjekty využívající elektronickou spisovou službu, pomocí které přijímají, připravují a zpracovávají elektronické dokumenty, ukládají tyto do negarantovaného úložiště TC ORP.

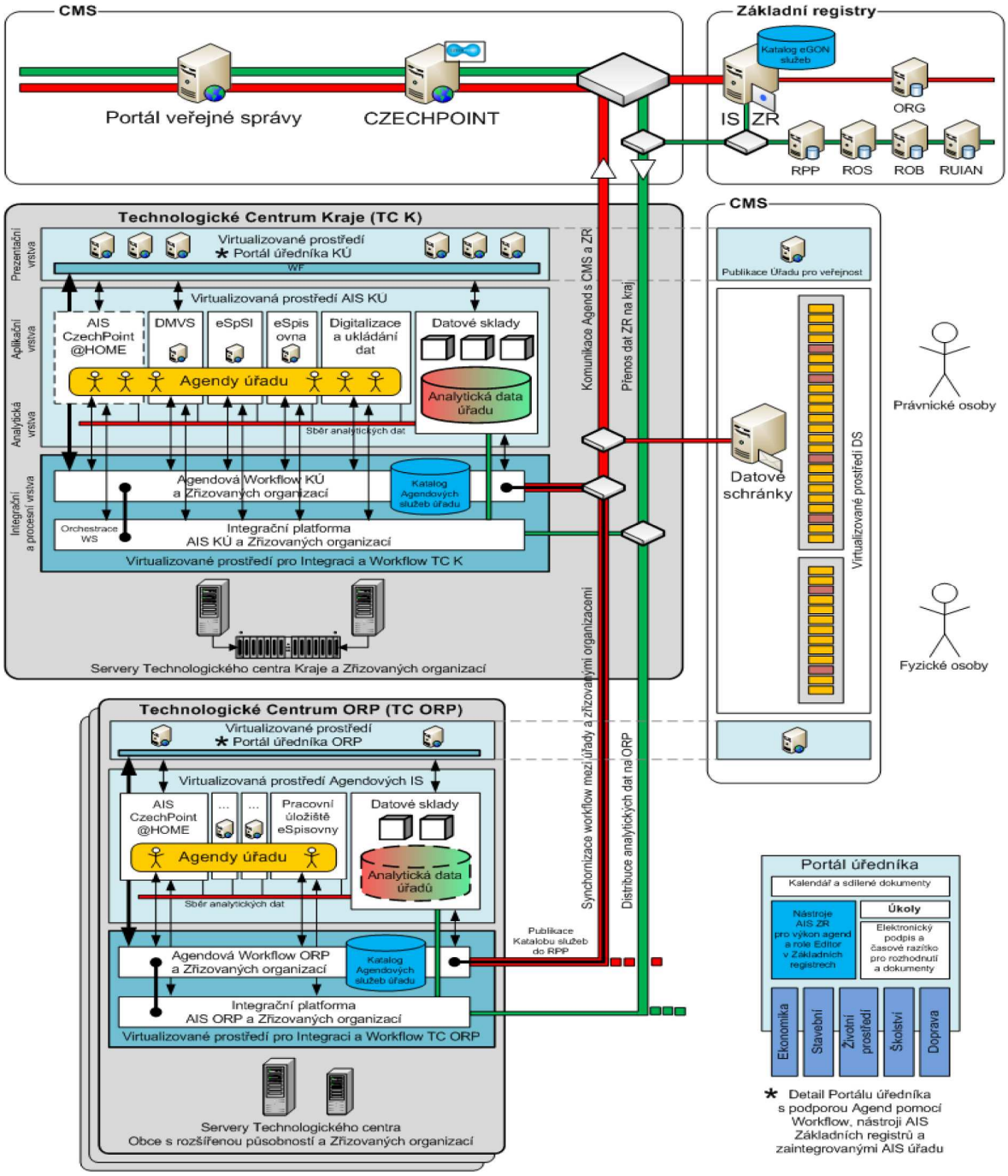
V závěrečné fázi jsou tyto dokumenty uzavřeny. Po uzavření se již dokumenty nesmí měnit. Pokud je spis uživatelem ukončen, bude elektronickou spisovou službou vytvořen datový balíček SIP. Po uzavření spisů budou přesouvány tyto datové balíčky SIP do garantovaného úložiště – krajské digitální spisovny. Odtud budou uzavřené spisy putovat do Národního digitálního archivu. [14]



Obr. 1. Cyklus elektronických spisů [14]

2.4 Komunikace mezi ORP a Centrálním místem služeb

Na blokovém schématu je názorně vidět komunikace mezi eGON centry (TC ORP a TC K), a to jak s informačním systémem datových schránek (ISDS), informačním systémem základních registrů (ISZR), tak i s Centrálním místem služeb (CMS). Žádost o referenční údaje je vyslána daným eGON centrem do CMS, kde bude ověřeno oprávnění uživatele a agendového systému a poté budou poskytnuty žádané informace. Stejný princip komunikace bude probíhat i pokud bude žádáno o informace z Portálu veřejné správy nebo ze systému Czech POINT. Pokud je dotaz o referenční údaje směřován na ISZR, putuje do centrálního místa služeb, kde je směrován na Katalog eGON služeb. Ten zajistí ověření a komunikaci s příslušným registrem a odpoví žadateli. [14] Samotnou součást systému tvoří ISDS, jež komunikuje s uživateli pomocí webového rozhraní přístupného přes internet anebo pomocí rozhraní elektronických spisových služeb.



Obr. 2. Schéma komunikační infrastruktury veřejné správy [22]

Informační systém základních registrů bude s ostatními informačními systémy veřejné správy komunikovat asynchronně pomocí eGON služeb. Jedná se o agendové informační systémy, kdy po ověření přístupových práv agendového systému a uživatele budou z informačního systému základních registrů poskytnuta referenční data. Neexistuje možnost přístupu k referenčním datům přímou cestou, ale pouze přes služby ISZR. Totéž platí i pro agendové IS, které mezi sebou komunikují také pouze pomocí služeb.

Zcela novou funkcionalitou ISZR je možnost občanů získat informace o přístupech k datům, které se váží k jejich osobě. Zároveň, pokud dojde ke změně referenčních údajů, lze pomocí zprávy odeslané do datové schránky informovat komerční subjekty o změně.

II. PRAKTICKÁ ČÁST

3 ANALÝZA SOUČASNÉHO STAVU A POPTÁVKY SLUŽEB

3.1 Úvod analýzy

Analýza současného stavu vybavenosti, připravenosti a požadavků na zajištění služeb eGON centra na ORP Otrokovice proběhla v souladu s požadavky výzvy č. 6 „ROZVOJ SLUŽEB E-GOVERNMENTU V OBCÍCH“. Tato výzva dává možnost čerpat finanční dotaci z integrovaného operačního programu strukturálních fondů EU na zřízení Technologického centra ORP, pořízení elektronické spisové služby pro celý správní obvod ORP a dalších nepovinných služeb, poskytovaných obcím I. a II. typu a vnitřní integrace úřadu.

Analýza současného stavu je zaměřena především na:

- Analýzu obcí I. a II. stupně o možnosti využívání služeb Technologického centra ORP Otrokovice
- Analýzu současného stavu ICT na ORP Otrokovice
- Analýzu požadavků příspěvkových organizací na služby Technologického centra ORP Otrokovice

Základním podkladem pro analýzu aktuálního stavu, jakož i zjištění zájmu obcí o přístupu k elektronické spisové službě, byl zvolen dotazníkový průzkum. Zjednodušeným způsobem byly dotazovány vybrané organizace zřizované ORP Otrokovice a obcemi v našem správním obvodu. Zde byl zjišťován převážně zájem o pořízení a používání spisové služby.

Dotazník pro obce I. a II. stupně obsahoval následující části:

- Oblast připojení k internetu
- Oblast spisová služba
- Oblast služeb Technologického centra
- Oblast digitální mapy veřejné správy

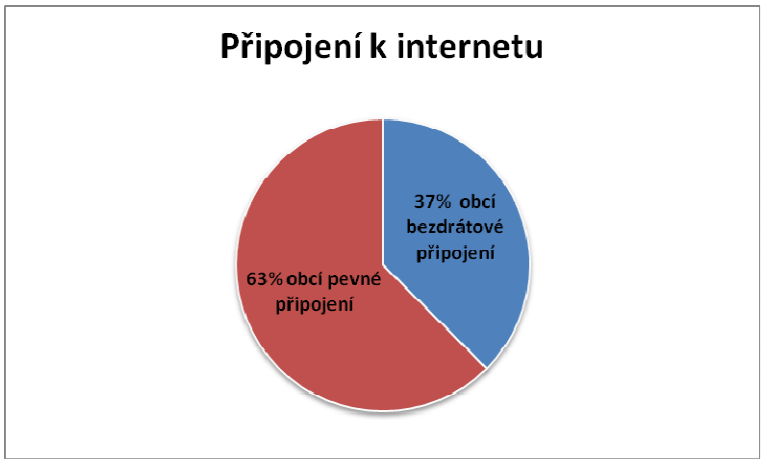
Spolu s dotazníkem byl rozeslán obcím i dokument „Vyjádření zájmu obce“, kde obce deklarovali svůj zájem o provoz elektronické spisové služby v hostovaném režimu na Technologickém centru ORP Otrokovice. Dotazníky byly odeslány všem devíti obcím v našem správním obvodu. Z toho jsme obdrželi 8 vyplněných dotazníků týkajících se

zjišťování aktuálního stavu na obcích, což představuje 90% návratnost. U dotazníku zaměřeného na „Vyjádření zájmu obce“ bylo dosaženo 100% návratnosti.

3.2 Analýza stavu obcí ve správním obvodu ORP Otrokovice

3.2.1 Připojení k internetu

Všechny obce, které vyplnily dotazník, jsou připojeny k internetu. Z toho 3 bezdrátovou technologií a 5 obcí pomocí pevné linky. Mezi poskytovatele internetového připojení obcí patří firmy TC Servis, s. r. o. (3 obce), Telefonica O_2 Czech Republic, a. s. (2 obce), Avonet, s. r. o. (2 obce) a společnost Spdreamnet (1 obec).



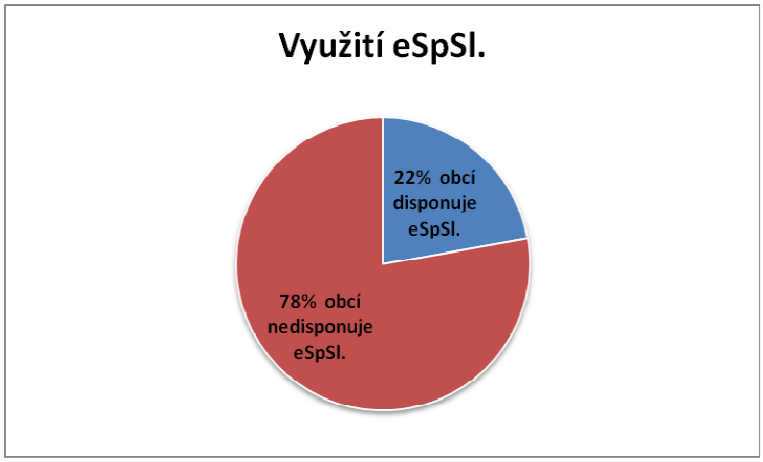
Obr. 3. Typy připojení k internetu obcí v ORP Otrokovice

3.2.2 Spisová služba

Jako podklady pro zpracování analýzy poptávky na hostovanou spisovou službu a na zjištění současného stavu sloužil právě formulář „Vyjádření zájmu obce “. Z uvedených informací vyplynulo, že 2 obce v našem správním obvodě disponují elektronickou spisovou službou a 7 obcí nedisponuje spisovou službou.

Pro tyto obce bude pořízena elektronická spisová služba, která bude provozována v hostovaném režimu na Technologickém centru.

ORP Otrokovice má již zavedenou a několik let úspěšně provozuje elektronickou spisovou službu od společnosti Vera, spol. s r. o.



Obr. 4. Graf využití elektronických spisových služeb

Pořadové číslo	Obec	Obec disponuje vlastní ESS.	Typ obce
1.	Bělov	nedisponuje	obec I. stupně základního typu
2.	Komárov	nedisponuje	obec I. stupně základního typu
3.	Oldřichovice	nedisponuje	obec I. stupně základního typu
4.	Pohořelice	nedisponuje	obec I. stupně základního typu
5.	Spytihněv	nedisponuje	obec I. stupně základního typu
6.	Tlumačov	nedisponuje	obec I. stupně s matrikou
7.	Žlutava	nedisponuje	obec I. stupně základního typu
8.	Halenkovice	disponuje	obec I. stupně s matrikou
9.	Napajedla	disponuje	obec I. stupně s matrikou a stavebním úřadem

Tab. 1. Seznam obcí v ORP Otrokovice disponujících ESS

Příspěvkové organizace ORP Otrokovice, které mají také zájem o využívání hostované spisové služby, byly osloveny dotazníky „Vyjádření zájmu příspěvkové organizace“.

V rámci probíhající analýzy byly příspěvkové organizace kategorizovány do dvou oblastí:

- **příspěvkové organizace zřizované ORP Otrokovice**

Zde všech 6 příspěvkových organizací projevilo zájem o elektronickou spisovou službu v hostovaném režimu provozovanou na TC ORP Otrokovice

- **příspěvkové organizace obcí I. a II. stupně ve správním obvodu ORP Otrokovice**

Formulář „Vyjádření zájmu příspěvkové organizace“ jsme obdrželi vyplněný pouze od 2 příspěvkových organizací zřízených obcemi I. a II. stupně.

P. č.	Příspěvková organizace
1.	Základní škola T. G. Masaryka Otrokovice, příspěvková organizace
2.	Základní škola Trávníky Otrokovice, příspěvková organizace
3.	Základní škola Mánesova Otrokovice, příspěvková organizace
4.	Mateřská škola Otrokovice, Jana Žižky 1356, příspěvková organizace
5.	SENIOR Otrokovice, Školní 1299, příspěvková organizace
6.	Dům dětí a mládeže Sluníčko Otrokovice, příspěvková organizace
7.	Základní škola Napajedla, příspěvková organizace
8.	Základní škola Tlumačov, okres Zlín, příspěvková organizace

Tab. 2. Seznam příspěvkových organizací žádající o ESS

Pořízení nové spisové služby pro školy nebo jiné příspěvkové organizace plánují 3 obce v ORP Otrokovice – Napajedla, Tlumačov a Žlutava.

3.2.3 Služby Technologického centra

V počátku projektu je mimo provozování elektronické spisové služby povinná pouze jedna služba pro Technologické centrum, a to negarantované úložiště nevyřízených a neuzavřených spisů jako výstupů dat ze systému elektronické spisové služby.

Analýzou bylo zjištěno, že o tuto povinnou službu bude mít zájem 8 obcí – Bělov, Halenkovice, Komárov, Oldřichovice, Pohořelice, Spytihněv, Tlumačov, Žlutava. Předpokládáme, že i když obec Napajedla nevyjádřila zájem o tuto povinnou službu, nebude chtít investovat finanční prostředky do své spisové služby a využije negarantované

úložiště v Technologickém centru ORP Otrokovice. To bude zprostředkovávat přenos uzavřených spisů do Technologického centra Zlínského kraje. TC ORP Otrokovice bude na tuto variantu technologicky i kapacitně připraveno.

Pomocí dotazníku bylo naší snahou zjistit zájem i o potenciální možné služby, které by TC ORP mohlo v budoucnu nabízet. U služeb, o které nebude zájem jak ze strany obcí, tak ze strany samotného ORP Otrokovice, nebude uvažováno o jejich uvedení do provozu.

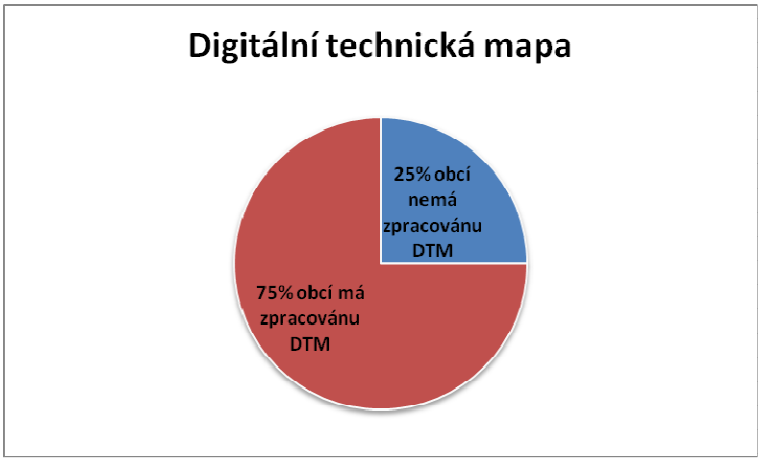
Služba TC ORP	Počet obcí
Zajištění negarantovaného úložiště dokumentů	8
Zálohování dat	7
Provoz spisovny	4
Služba konverze dat do PDF	3
Kopie centrálních registrů	2
Elektronické zadávání zakázek	1
WEBhosting	1
Školský systém	1
Redakční systém pro publikování na internetu	1
Metodická a systémová podpora	8

Tab. 3. Seznam požadovaných služeb obcemi I. a II. stupně na TC ORP

3.2.4 Digitální mapa veřejné správy

Šest obcí uvedlo, že mají zpracovanou digitální technickou mapu svého území, kterou využívají pro výkon státní správy a samosprávy. Dvě obce digitální technickou mapu zpracovanou nemají.

Mezi poskytovatele služeb v oblasti GIS patří Katastrální úřad Zlínského kraje (5 obcí). Obce Bělov, Halenkovice a Spytihněv v dotazníku neuvedly žádné dodavatele služeb v oblasti GIS.



Obr. 5. Digitální technická mapa v obcích ORP Otrokovice

3.3 Analýza stavu obcí ve správním obvodu ORP Otrokovice

3.3.1 Popis serverové části

Místnost s umístěním technologických prvků sítě LAN a samotnými servery je umístěna v budově Městského úřadu v Otrokovicích. Serverovna se nachází v 1. patře budovy. Vstup do budovy je otevřen pro veřejnost od 6:30 h do 18:00 h a poté je budova pro veřejnost uzavřena. Budova, ale i serverovna je napojena na elektronický zabezpečovací systém, který je vyveden na centrální pult Městské policie v Otrokovicích. Součástí zabezpečení technologické místnosti, kde bude TC ORP umístěno a kde se v současnosti nachází stávající servery, je identifikace osob, které do ní chtějí vstoupit. Tato identifikace je prováděna přes docházkovou kartu a vstup je umožněn pouze pracovníkům oddělení informatiky.

Dalším bezpečnostním vybavením serverovny je elektronický protipožární systém, a to včetně zhášecího systému.

Vzhledem k současnému, ale i budoucímu výkonu umístěnému v technologické místnosti je nezbytné provádět neustálé chlazení prostoru. Z těchto objektivních důvodů je místnost vybavena klimatizací, která je napojena na samostatný okruh elektrické energie.

Napájení serverů je řešeno také samostatným elektrickým okruhem. Pro krátkodobé výpadky je serverovna vybavena záložními zdroji elektrické energie APC Smart-UPS XL 3000VA a APC Smart-UPS 1500VA. Tyto náhradní zdroje zabezpečují ochranu serverů a ostatního technologického vybavení před předpětím, podpětím a samozřejmě před

výpadkem elektrické energie. V praxi bylo ověřeno, že zdroje při výpadku elektřiny udrží veškeré technické vybavení místnosti minimálně dalších 15 minut v provozu, což je dostatečně dlouhá doba k překonání krátkodobých výpadků elektrické energie. Záložní zdroj UPS je vybaven dálkovým ovládáním připojených zařízení, a pokud se stav baterií dostane na předem stanovenou kritickou hodnotu, vyšle pomocí protokolu TCP/IP příkaz všem připojeným zařízením k okamžitému vypnutí. Pro dlouhodobé výpadky elektrické energie je město Otrokovice vybaveno dieselovým generátorem Volvo Penta TWD 610G o výkonu 164 kVA, který je schopen svým výkonem zajistit elektřinu pro dvě plně fungující budovy MěÚ Otrokovice. Technologické centrum, jež bude umístěno v serverovně, je těmito prostředky chráněno před dlouhodobými výpadky elektřiny.

Základní seznam a popis současného serverového vybavení ORP Otrokovice.

Označení serveru	Konfigurace	Provozované služby
IBM x3500	• CPU 2,5 GHz XEON • 4 GB RAM • Disková kapacita 700GB	• MS SQL • File server • Systémové aplikace
IBM x3650	• CPU 2,0 GHz XEON • 4 GB RAM • 600 GB RAID 0 • 72 GB RAID 1	• Zálohovací server • Stavebni archiv • Uživatelské aplikace
HP Proliant ML350G5	• CPU 1,8 GHz XEON • 2 GB RAM • 72 GB RAID 1 • Disková kapacita 300 GB	• Domain Controler • File server • Systémové aplikace
HP Proliant ML370G4	• CPU 2x 2,5 GHz XEON • 4 GB RAM • 300 GB RAID 1	• Radnice Vera® • DB Oracle
HP Proliant ML310G3	• CPU P4 3,2 GHz • 1,5 GB RAM • 250 GB RAID 1	• Print server • Uživatelské aplikace
HP Proliant ML370G2	• CPU 2,0 GHz XEON • 2 GB RAM • 146 GB RAID 1	• GIS • T-Mapy
HP Proliant ML370G2	• CPU 2,0 GHz XEON • 2 GB RAM • 72 GB RAID 1	• WWW
HP Proliant ML370G5	• CPU 2,5 GHz XEON • 4 GB RAM • 300 GB RAID 1	• Email • Uživatelské aplikace
HP Proliant DL380G6	• CPU 2,66 GHz XEON • 4 GB RAM • 400 GB RAID 1	• Vera Flexi

Tab. 4. Soupis stávající serverové infrastruktury

3.3.2 Místní síť LAN

Síť LAN, kterou provozujeme, je založena na hvězdicové topologii, kde aktivními prvky jsou switche řady 4200G, 4500G a 5500G od firmy 3COM®. Celá síť je provozována na rychlosti 1 Gbit. Páteřní trasy jsou tvořeny optickými spoji, spojení mezi koncovými stanicemi a aktivními prvky jsou metalickými spoji. Optické spoje jsou provozovány na multividových vláknech.

Město Otrokovice využívá internetovou konektivitu od lokálního providera, a to o rychlosti 30 Mbit – duplexní provoz. Tato konektivita je zajišťována bezdrátovým spojem. Vzhledem ke strategickému významu budovaného Technologického centra je město Otrokovice vybaveno náhradní konektivitou od jiného providera. Budoucí vývoj v této oblasti není opomíjen a spolu se Zlínským krajem a ostatními obcemi s rozšířenou působností v našem kraji připravujeme projekt regionální metropolitní sítě. Zde budou propojeny metropolitní sítě jednotlivých měst s páteřní trasou Zlínského kraje. Stejný projekt byl v minulosti realizován krajem Vysočina – tzv. Rowanet. Výhody, které přinese takováto síťová infrastruktura, budou značné, a to jak v oblasti finančních úspor, v oblasti bezpečnosti a sdílení dat, centrálního krizového řízení a v neposlední řadě také ve sdílení informačních technologií, kdy při totálním výpadku některého Technologického centra bude moci jeho funkci převzít jiné ORP či kraj.

3.3.3 Firewall

V rámci přípravy na tento projekt a projekt TC ORP bylo zakoupeno a implementováno nové bezpečnostní UTM zařízení od společnosti Trusted Network Solutions, a. s.

Je to nový typ bezpečnostního zařízení UTM Kernun Net Access, které zabezpečuje více bezpečnostních služeb v jednom zařízení najednou. Toto zařízení zajišťuje firewall, antivirus, antispam, antispyware, filtrování a blokování obsahu komunikace, popřípadě protokolů, routing, QoS a VPN. V rámci naší organizace zabezpečuje především ochranu naší privátní sítě LAN a přístupy do jednotlivých DMZ.

3.3.4 Datová úložiště a data

Aktuální konfigurace a infrastruktura HW zařízení neumožňuje kvalitní a bezpečnou konsolidaci dat na jedno datové úložiště, a proto jsou aplikační data uložena vždy na konkrétním serveru. Klíčová data jsou uložena na redundantních komponentách v režimu RAID 1, což v kombinaci s hot-swapovými HDD většinou umožňuje výměnu vadného HDD za provozu. Diskový řadič po výměně nového dílu zajistí přenesení bitové kopie na nový HDD.

Databázová data jsou uložena také lokálně, a to dle databázové instance, která je na konkrétním serveru založena. Město Otrokovice provozuje tyto databáze – Oracle® 10g, Microsoft® SQL Server 2000 a Firebird.

3.3.5 Zálohování

V současnosti pro zálohování využíváme zálohovací software Symantec Backup Exec. Pomocí klientů jsou data v nočních hodinách kopírována na páskovou knihovnu IBM TS3100. Tato pásková knihovna je založena na technologii LTO4, kde na jednu pásku lze umístit až 1,8 TB komprimovaných dat. V pravidelných intervalech jsou měsíční pásky uchovávány v jiné budově MěÚ v protipožárním trezoru.

Pro zálohování dat z provozovaných databází využíváme nástroje dodávané s jednotlivými databázovými produkty a exportovaná data jsou kopírována v rámci záloh na pásky.

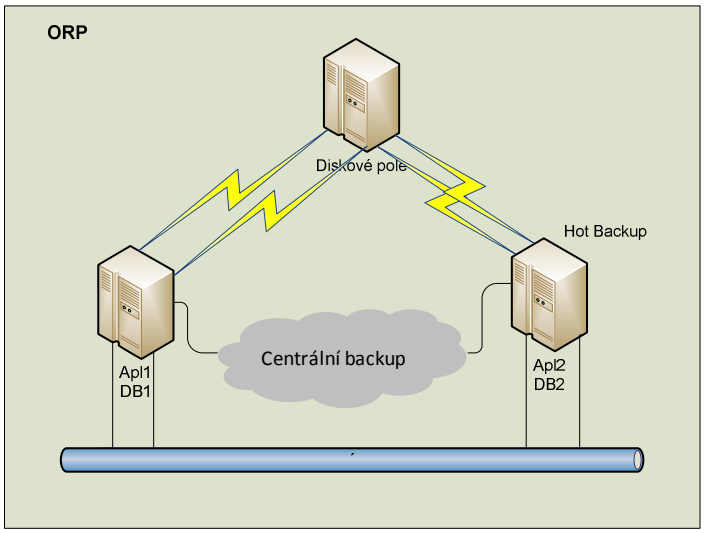
3.3.6 Využívaný software

V současné době ORP Otrokovice využívá 3 operační systémy na svých serverech. Linux RedHat 4.0, Linux CentOS a Windows 2003 Server Standard R2. Jelikož byly operační systémy nakoupeny jako OEM licence s nákupy jednotlivých serverů, nebudou moci být využity pro připravované TC ORP.

4 STUDIE PROVEDITELNOSTI A REALIZACE TVORBY TECHNOLOGICKÉHO CENTRA

Základní požadavky na TC ORP byly stanoveny výzvou č. 06 z IOP – Integrovaného operačního programu, prioritní osa č. 2 Zavádění ICT v územní veřejné správě, oblast podpory: 2.1 Zavádění ICT v územní veřejné správě.

Tyto požadavky jsou rozděleny do několika oblastí:



Obr. 6. Schéma požadované infrastruktury [22]

Popis serverové části dle výzvy č. 06

- musí obsahovat minimálně 2 fyzické servery, které budou poskytovat služby typu aplikačního a databázového serveru
- budou identicky nainstalovány, aby mohly v případě výpadku jednoho z nich převzít v systému úlohu i toho druhého
- oba servery budou připojeny redundantními cestami k diskovému poli
- budou mít identickou konfiguraci
- výkon serverů musí být na takové úrovni, aby byla možnost implementovat vizualizační technologii, a konfigurace serverů musí podporovat nejrozšířenější typy operačních systémů

Minimální doporučená konfigurace pro všechny typy serverů:

- nejméně 1 CPU čtyř jádrový s 64bitovou architekturou, frekvence nejméně 2 GHz;

- nejméně 8 GB RAM s možností rozšíření na nejméně 32 GB;
- záruka po celou dobu udržitelnosti projektu. [22]

Popis úložiště dle výzvy:

- k serverům bude připojeno úložiště k ukládání dat databáze a aplikačního serveru.
- ukládání dat řešit prostřednictvím NAS (Networked Attached Storage), popř. SAN (Storage Area Network), s implementovanou TIER architekturou a HSM (Hierarchical Storage Management) designem. Produkční data ukládat na TIER 0 na rychlé FC disky (nebo rychlejší) diskového úložiště (např. rychlost pro 4 KB bloky alespoň 60 tis. IOPS pro RAID 6, R/W sekvenčně).
- propojení serverů a diskového pole bude redundantní pro zajištění vysoké dostupnosti dat;
- diskové pole musí být dostatečně výkonné a škálovatelné, aby pokrylo předpokládané budoucí nároky aplikací, a musí umožňovat použití jak vysoce výkonných, tak kapacitních disků;
- klíčové komponenty systému pro ukládání dat budou řešeny jako redundantní.

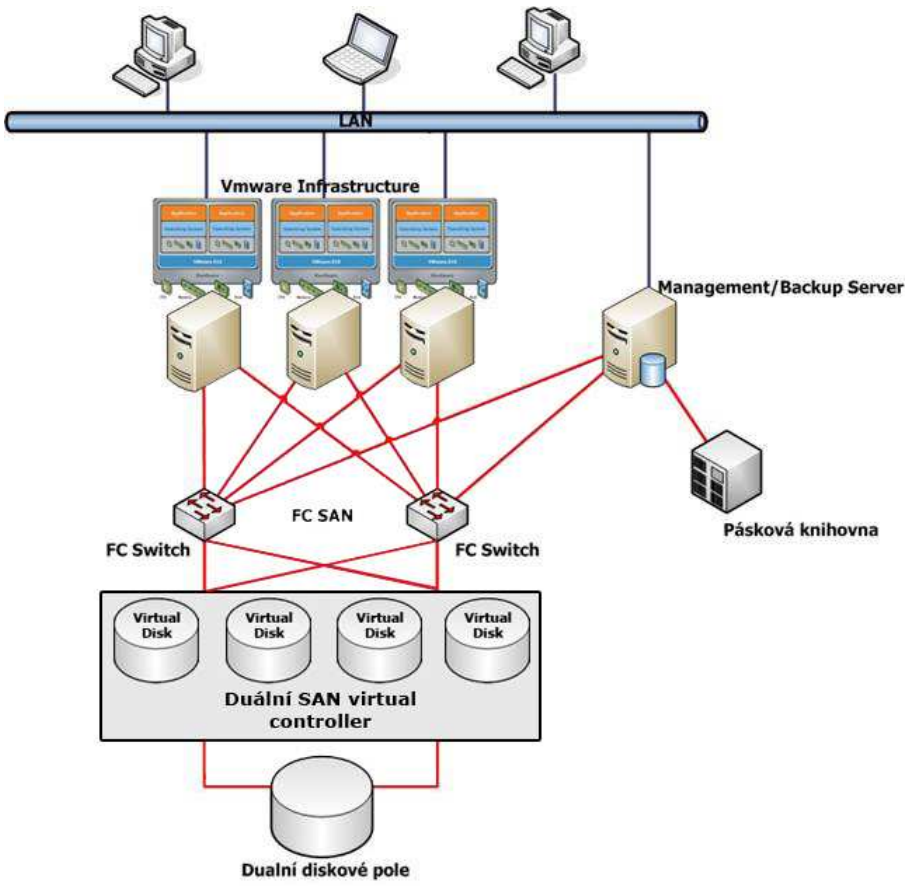
Minimální konfigurace: Čistá využitelná kapacita: 1 TB [22]

Další podmínky plynoucí pro žadatele o dotaci jsou:

- zajištění SLA TC ORP 5 x 12 hodin;
- teplota prostředí – od 18 °C do 24 °C;
- místnost bude vybavena požárními čidly kouře a teploty;
- místnost bude vybavena elektronickou zabezpečovací signalizací
- v místnosti bude rozvod elektrické energie 230/50 V s bezvýpadkovým zálohováním, samostatně jištěný rozvaděč a pro případ dlouhodobého výpadku elektrické energie zajištění diesel agregátu;
- vnější ochrana budovy 7 x 24 hodin;
- prokazatelná evidence vstupujících osob do serverovny;
- serverovna se musí nacházet mimo zátopovou oblast tzv. stoleté vody.

4.1 Návrh a popis architektury TC ORP

Vzhledem k budoucímu rozvoji Technologického centra bylo vybráno řešení, kdy celá infrastruktura bude umístěna do racku 42U.



Obr. 7. Schéma navržené architektury TC ORP

Serverová část architektury TC ORP bude založena na serverovém systému typu „blade“. Prvotní investice bude obsahovat blade chassi, 3 produkční servery, z toho 2 aplikační a 1 databázový a vybavení SAN architekturou včetně dvou diskových polí. Pro management bude využit stávající server v majetku ORP, konkrétně se bude jednat o server IBM x3650. Pro zálohování bude využita stávající pásková knihovna IBM TS 3100. Celý systém je navržen s ohledem na snadný budoucí rozvoj TC ORP.

4.2 Serverová infrastruktura

Při rozhodování o technologické otázce, zda bude TC postaveno na systému „blade“ nebo na klasickém rackovém řešení byly zváženy všechny dostupné aspekty.

Vzhledem k jednoznačným výhodám – úspora místa, řízení spotřeby energie a emise tepla, snížení kabeláže, snadná rozšiřitelnost a maximální redundance, byla vybrána technologie „blade“.

Jedná se o modulární řešení, kdy do bladeového chassi, ve kterém jsou integrovány společné komponenty, jsou instalovány servery. Chassi je vybaveno redundancí napájení, chlazení a i datových cest.

4.2.1 BladeCenter H

Jako nejvhodnější řešení pro TC ORP bylo vybráno chassi od společnosti IBM® – BladeCenter® H.

Obr. 8. IBM BladeCenter H - 1 [16]

Obr. 9. IBM BladeCenter H - 2 [16]

Jedná se o chassi o velikosti 9U, které obsáhne až 14 hot-swap serverů. Konstrukčně je toto chassi řešeno tak, že každý server je k tomuto chassi připojen pomocí duálního midplane dvěma identickými konektory, přičemž každý z konektorů je součástí

galvanicky oddělených datových sběrnic, které jsou propojeny s rozšiřujícími moduly. Redundance všech tras je na maximální úrovni.

Chassi o rozměrech 711 mm x 711 mm lze vybavit až čtyřmi hot-swapovými redundantními elektrickými zdroji 2 900 W AC s funkcí load-balancingu výkonu. To znamená, že tyto zdroje dodávají výkon dle počtu a instalované konfigurace serverů v chassi. Napájecí napětí je v rozmezí 200–240 V. Chassi je energeticky rozděleno tak, že první pár redundantních zdrojů zajišťuje napájení pro prvních 7 blade pozic a druhý pár pro zbytek instalovaných bladeových serverů. V současném návrhu je počítáno s instalací maximálně 6 serverů při zajištění kompletního provozu TC ORP a z tohoto důvodu bude chassi obsahovat pouze dva redundantně zapojené elektrické zdroje. Blade chassi je vybaveno „Media Tray“ panelem, který obsahuje DVD-RW mechaniku, USB rozhraní a panel zobrazující aktuální stav zařízení.

Pro odvod tepla z chassi bude toto vybaveno dvěma redundantními dmychadly, která zajistí optimální chlazení instalovaných serverů.

Obr. 10. IBM chlazení [16]

Otáčky ventilátorů se liší v závislosti na teplotě okolního vzduchu v přední části chassi a teploty vnitřních komponent. Při teplotách do 25 °C dmychadla běží na minimální výkon. Při selhání některého z dmychadel bude zbývající bez ohledu na teplotu okolního vzduchu pracovat na maximální výkon do doby výměny vadného dílu a obnovení redundance.

4.2.2 Advanced Management Module

Součástí standardního vybavení je i modul management konzole. Tento management modul je dodáván v provedení hot-swap a TC ORP bude obsahovat dva tyto moduly pro redundantní zapojení. Sekundární modul je během provozu pasivní nebo v pohotovostním režimu a automaticky začne vykonávat své funkce při selhání primárního

modulu. Využívá se ke konfiguraci a administraci všech instalovaných komponent Blade centra a obsahuje nejenom funkce pro správu systému, ale i rozhraní pro klávesnici, video a myš (KVM). Ovládá sériový port pro dálkové připojení, 10/100 Mbps Ethernet pro vzdálenou správu připojení a KVM zařízení.

Servisní procesor v management modulu komunikuje se servisními procesory v jednotlivých blade serverech. Modul ovšem nekomunikuje pouze s blade servery, ale umožňuje komunikaci se všemi jednotkami Blade centra, odhaluje přítomnost či absenci zařízení, obsluhuje jejich hlášení či zasílá upozornění na chybové stavy v případě potřeby. Monitoring sleduje především event log, hardware a firmware, otáčky ventilátorů, teploty a spotřebu. Konfigurovat lze řízení spotřeby energie, přístupy k I/O modulům, změnu spouštěcí sekvence serverů, vzdálená virtuální média, vlastnictví vyměnitelných médií a USB portů a datum a čas. Pro signalizaci kritických alarmů je využita i světelná signalizace.

Obr. 11. IBM Management Module [16]

4.2.3 BNT Ethernet Switch

Pro připojení TC ORP k místní síti LAN bude vybaveno dvěma moduly BNT Layer 2/3 Cooper Gb Ethernet Switch. Jedná se o přepínač, který správcům umožňuje konsolidovat provoz na druhé a třetí vrstvě OSI. Konsolidace spočívá ve vnitřním vytvoření topologie datového centra a infrastruktury a snížení počtu samostatných zařízení, management konzol a ostatních systémů.

Přepínače jsou vybaveny:

- 14 interními full-duplex gigabitovými porty, kde každý port je přidělen k určitému blade serveru,
- 2 interními full-duplex 10/100 Mbps porty pro připojení k management modulům,
- 6 externích portů 1000BASE-T metalických konektorů RJ-45 s automatickou optimalizací rychlostí jednotlivých portů,
- RS-232 sériový port pro instalaci software a nastavení modulu,
- nastavením až 128 rozhraní IP na přepínač,
- podporou až 1024 VLAN sítí,
- podporou Jumbo frames (max. 9 216 byte),
- Virtual Router Redundancy Protocol (VRRP), redundancí pro třetí vrstvu routování
- IEEE 802.1D Spanning Tree Protocol (STP) pro poskytování Layer 2 propouštění,
- Access Control Listy pro VLAN, MAC adresy i IP adresy,
- 802.1x port-based autentizací Radius/TACACS+,
- Quality of Service (QoS),
- IP forwarding a filtrováním pomocí ACL,
- servisními protokoly (SNMP) a administrátorskými nástroji pro efektivní správu, dohled a monitoring ethernetové komunikace v daném modulu. [16]

Obr. 12. IBM Ethernet Switch [16]

4.2.4 Qlogic 8Gb SAN Switch

Pro připojení k virtuálnímu diskovému řadiči bude Technologické centrum vybaveno dvěma redundantně zapojenými QLogic 20-Port 8Gb SAN Switch moduly.

Obr. 13. IBM QLogic SAN Switch [16]

Jedná se o poslední dostupnou verzi vysokorychlostního Fibre Channel switche vytvářející SAN síť o rychlosti 8 Gbps. V každém modulu budou instalovány tři 8 Gbps SFP + optické moduly. Switch je zpětně kompatibilní i se staršími optickými SFP moduly pracujícími s rychlostmi 1 Gbps, 2 Gbps a 4 Gbps. Fibre channelový switch je vybaven 14 interními FC porty umožňující komunikaci rychlostmi 2 Gbps, 4 Gbps a 8 Gbps, dvěma interními full-duplex 100 Mbps ethernetovými rozhraními a šesti externími autosenzitivními Fibre Channel porty, které primárně fungují na maximální rychlosti. Podporuje propojení až 239 FC switchů, přičemž celková šířka pásma je uváděna 320 Gb/s ve full-duplexním provozu a maximální velikost frame 2 148 byte. Switch disponuje propracovanou detekcí chyb, mezi které patří například cyklická redundantní kontrola, kontrola parity, dlouhého a krátkého rámu, nesoulad D_ID a S_ÏD a 8 byte a 10 byte konverze. Podporuje servisní (SNMP) i bezpečnostní (IPSec) protokoly a webové rozhraní pro konfiguraci, management a dohled zařízení. [16]

4.2.5 Popis serveru HS 22

O samotný výpočetní výkon Technologického centra se budou starat v prvé fázi projektu tři servery IBM HS22. Díky nejnovějším procesorům Intel® Xeon® založených na architektuře Westmere,výrobní technologii 32nm a schopnosti pracovat jak v 32bitovém, tak i v 64bitovém režimu, jsou tyto servery určeny pro široké spektrum náročných úloh, vizualizaci nebo jiných enterprise aplikací. Technologické centrum bude vybaveno servery obsahující dva čtyř jádrové CPU Intel® Xeon® X5640, pracující na frekvencích 2,66 GHz a vybavené 12 MB L3 cache. Procesor X5640 vykazuje maximální energetickou náročnost

80W a disponuje technologií Max Turbo frekvence, která umožňuje procesoru automatické přetaktování až na frekvenci 2,93 GHz.

Obr. 14. IBM server HS 22 [16]

Frekvence sběrnice dosahuje rychlost až 1 066 MHz a systém pracuje s registrovanými operačními paměťmi typu DDR3 ECC o stejné rychlosti. Teoretická datová propustnost komunikačního protokolu QPI mezi severním můstkem a procesorem je v produktových materiálech uváděna až 5,86 Gbps. [12] Jako chipset je integrován Intel® 5520. Server dokáže pracovat až s 96 GB operační paměti RAM. Původní procesorová architektura Intel® Nehalem komunikovala na maximální frekvenci pouze s třemi DIMM paměťmi na CPU. Současná architektura procesorů Westmere umožňuje komunikaci na maximální frekvenci se šesti paměťmi na jeden CPU. Tím současná verze serverů HS22 osazená procesory Intel® umožňuje efektivnější využití větší kapacity operační paměti RAM.

Servery jsou vybaveny redundantními hot-swapovými pevnými disky o velikosti 2,5“. Tyto SAS disky budou disponovat kapacitou 146,8 GB s rychlostí otáček 15 000 za minutu. Server sice umožňuje použití i SSD HDD, ale pro úložiště operačního systému je jejich cena vzhledem k požadovanému výkonu prozatím nevýhodná. Komunikační rozhraní disků technologie SAS umožňuje HDD komunikaci rychlostí až 6 Gbps. HDD budou zapojeny v režimu RAID 1 a budou obsahovat operační systémy provozované na daných serverech. Zrcadlení disků (RAID 1) zabezpečuje řadič ServeRaid-MR10ie.

Zajimavým technickým řešením je interní USB konektor připravený pro FLASH paměť s VMwarem ESXi pro embedded virtualizaci. Samozřejmostí je i standardní výbava jako VGA adaptér, konkrétně Matrox G200eV s 16 MB video paměti a osazení dvěma porty Gigabit Ethernet (Broadcom BCM5709S). Rozměry serveru jsou výška – 245

mm, šířka – 29 mm a hloubka – 446 mm. Při plném osazení váží server 5,44 kg. Server lze dovybavit rozšiřující kartou, a to buď 10 Gb Ethernet, 4X InfiniBand, iSCSI či 8 GB Fibre Channel. V naší konfiguraci budou servery rozšířeny právě o 8 GB Fibre Channelové karty. [16]

4.3 Storage Area Network

Základ SAN bude tvořen dvěma diskovými poly, vizualizačním řadičem a Fibre Channelovou infrastrukturou. Obě disková pole budou založena na Fibre Channel technologii a primární diskové pole v celém systému bude plnit úlohu úložiště produkčních dat. Jedná se o diskové pole IBM Systém Storage DS 5020 Express.

4.3.1 System Storage DS 5020

Toto diskové pole o velikosti 2U je vybaveno jak redundantními řadiči, duálními 8 Gbps porty, 1 Gbps iSCSI rozhraním, tak i redundantním napájením. Je vybaveno 2 GB baterií zálohované cache. Diskové pole DS5020 pojme 16 HDD ovšem s tím, že lze tato disková pole škálovat tak, že může obsahovat až 112 fyzických pevných disků. Zařízení umožňuje kombinovat různé technologie HDD v jedné diskové polici. Tímto je nám umožněno kombinovat disky FC, FDE a SATA, a to o velikostech od 146 GB (15K) až po 1 TB (7.2K). TC ORP počítá s vybavením šesti kusů HDD 450 GB (15K) FC DDM a deseti kusů HDD 1 000 GB (7.2K) SATA DDM.

Obr. 15. IBM System Storage DS5020 [19]

4.3.2 System Storage DS 3400

Jako sekundární diskové pole bude implementováno diskové pole IBM Systém Storage DS3400. Jeho výška je 2U a pojme až 12 fyzických pevných disků s možností

rozšíření až na 48 HDD pomocí tří expanzí EXP3000. Do SAN bude připojeno pomocí 4 Gbps Fibre Channel rozhraní. Diskové pole DS3400 umožňuje také kombinaci různých technologií HDD, jako DS5020, ale na rozdíl od primárního pole umožňuje kombinaci SAS a SATA technologií. DS3400 obsahuje interní paměť 1 GB zálohované cache (512 MB na každý řadič). Z toho vyplývá, že diskové pole bude vybaveno stejně jako primární diskové pole dvěma řadiči i napájením.

Obr. 16. IBM Systém Storage DS3400 [17]

Diskové pole podporuje RAID režimy 0, 1, 3, 5, 6 a 10. Sekundární diskové pole bude vybaveno 12 HDD 1 TB (7.2K) a bude využíváno především jako úložiště neaktivních dat a úložiště snapshotů produkčních dat, takže při totálním výpadku primárního pole bude schopno sekundární převzít v systému jeho funkci.

4.3.3 System Storage TS 3100

K archivaci bude sloužit pásková knihovna IBM System Storage TS3100. Jedná se o zařízení, které je již MěÚ Otrokovice provozováno a bude implementováno do TC ORP.

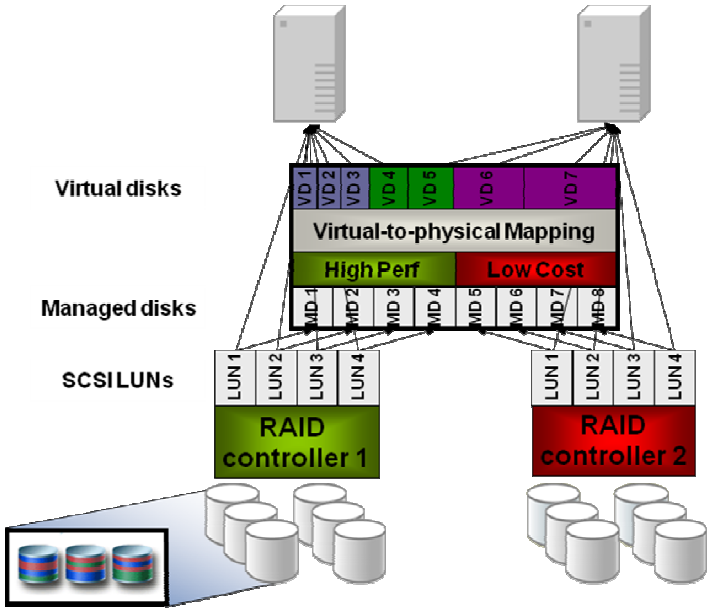
Obr. 17. IBM Systém Storage TS3100 [11]

Pásková knihovna pojme 24 pásek a disponuje jednou zálohovací mechanikou využívající technologii LTO4. Díky této technologii můžeme uložit na jednu magnetickou pásku až 1.8 TB komprimovaných dat. Pásková knihovna bude sloužit nejenom jako součást zálohování, ale zároveň bude součástí hierarchického ukládání dat, kdy

nepoužívaná data budou pásky využívat jako úložiště. Pokud by vznikl dotaz na tato data, budou čtena právě z pásky.

4.3.4 System Storage SAN Volume Controller

Vrcholem SAN architektury je IBM System Storage SAN Volume Controller. Je to zařízení, které umožní sdružit kapacitu několika heterogenních systémů pro ukládání dat do jediné společné paměťové oblasti, kterou lze spravovat z jediného místa a umožní provádět změny fyzických prostředků pro ukládání dat bez vlivu na aplikace v hostitelském režimu. Tento vizualizační engine pro SAN pracuje tak, že fyzická úložiště se neinterpretují serverům, ale SVC. Ten následně interpretuje virtuální diskové oddíly serverům. SVC při vytváření virtuálních disků rozdělí jednotlivé LUN na 4 KB bloky (extenty) a z těch dle svých vlastních vizualizačních pravidel interpretuje virtuální disky. Virtualizační pravidla jsou nastavitelná a záleží pouze na administrátorovi, jaká pravidla využije. Při ukládání dat je možno zvolit dva přístupy k diskům. Jeden způsob je sekvenční zápis, kdy jsou data zapisována na jeden disk postupně za sebou. Druhý způsobem ukládání dat je „striped mode“, kdy jsou extenty rovnoměrně rozloženy do několika LUN. Tím dochází k tomu, že pro zápis stejných dat je k dispozici více disků – více zapisovacích hlaviček, což vede ke zvýšení výkonu diskového pole a postupného zaplňování.



Obr. 18. Princip IBM virtualizace storage [18]

Nespornými výhodami SVC jsou funkce jako vytváření snapshotů mezi dvěma diskovými poli, přičemž tato pole nemusí mít společného výrobce ani technologii HDD.

SVC umožňuje mirroring mezi diskovými poli a opět tato funkce není závislá na výrobci polí. Virtualizace Storage umožňuje migrovat extenty z jednoho LUN na jiný, a to bez výpadku služeb. Server připojený k SVC tuto operaci vůbec nezpozoruje a bude pracovat se svým virtuálním diskem naprosto kontinuálně. Pokud bude pomocí monitoringu vyhodnoceno, že jsou některé disky přetíženy, lze touto metodou virtuální disk přesunout na rychlé disky, a tím zvýšit výkon systému a předejít možné nestabilitě systému. Poslední zmíněnou funkcí je tzv. „thin provisioning“, kdy SVC umožňuje snadnou alokaci prostoru pro servery, a to vždy jen tolik, kolik aktuálně potřebují.

Díky své škálovatelnosti dokáže spravovat i velmi rozsáhlá prostředí pro ukládání dat, a to i od různých výrobců. SAN Volume Controller umožňuje odstínit servery od změn na fyzickém úložišti, což znamená, že blade chassi bude připojeno redundantními cestami ke dvěma SAN Volume Controllerům, které umožní vytvářet v SAN virtuální diskové prostory. Ty jsou fyzicky umístěny na jednotlivých diskových polích a páskové knihovně. Každé z diskových polí bude redundantně připojeno ke každé jednotce SAN Volume Controlleru.

Obr. 19. IBM System Storage SAN Volume Controller [18]

SAN Volume Controller je vybaven zálohovanými cache paměťmi až do velikosti 32 GB, čímž povyšuje i běžná disková pole na vyšší výkonnostní úroveň. Obrovskou výhodou této technologie z hlediska plánovaného budoucího rozvoje je možnost připojit více heterogenních systémů diskových polí od různých výrobců. SAN Volume Controller integruje hardwarové prostředky se softwarovým vybavením, kdy tato zařízení jsou založena na serverové technologii Intel® Xeon®. SVC Controller, konkrétně model „Entry level“, bude pro MěÚ Otrokovice vybaven procesorem Intel® Xeon® E3110 (3 GHz) s 6 MB L2 cache, standardně bude vybaven 8 GB cache a čtyřmi 4 Gbps Fibre channel porty. Pro zajištění vysoké dostupnosti jsou SVC Controllery dodávány vždy v páru a jsou vybaveny vlastními náhradními zdroji elektrické energie UPS. Spolu s SVC je vždy

dodáván „System storage produktivity center“, což je server, pomocí kterého lze provádět konfiguraci a management SVC Controllerů. SVC podporuje připojení diskových polí i pomocí iSCSI. [18]

4.4 Popis firewallu

Následující oddíl bude věnován firewallu implementovanému v prostředí MěÚ Otrokovice a nastavení politik přístupů ke službám. MěÚ Otrokovice na konci minulého roku počítal s vybudování TC ORP, a proto již byly prováděny přípravy k tomuto projektu. Jednou z příprav byla implementace kvalitního firewallu do prostředí výpočetní techniky na MěÚ. V poptávkovém řízení byl jako nejkvalitnější UTM zařízení vybrán produkt společnosti Trusted Network Solutions, a. s.

UTM „Kernun Net Access“ funguje na principu „aplikačních proxy“, které neumožňují přímou komunikaci mezi účastníky komunikace. V tomto případě nelze zaměňovat klasické http-cache proxy s aplikačními, protože slouží pouze jako vyrovnávací paměť a ne jako bezpečnostní opatření. Aplikační proxy fungují jako zprostředkovatel každého spojení, a tím poskytují vyšší úroveň zabezpečení než pouhá stavová kontrola IP datagramů. „Proxy fungují tak, že naslouchají požadavkům o služby od interních klientů a pak je předávají na externí síť, jako kdyby byl klientem – původcem samotný server proxy. Jakmile obdrží proxy od veřejného serveru odpověď, vrátí tuto odpověď původnímu internímu klientskému počítači, jako kdyby byl sám původním veřejným serverem.“ [2]

Pokud proxy komunikačnímu protokolu „nerozumí“ nebo zjistí nesoulad s nastavenými pravidly, tuto komunikaci směrem ke klientovi neuskuteční.

Pro samotné řízení spojení lze využívat i prostředky stavové inspekce, a to především paketový filtr s možností detekce vzdáleného operačního systému, řízení šířky pásma a ochrany proti DoS útokům. Další služby, které Kernun nabízí, jsou například obousměrný překlad adres a logování komunikace. Systém lze vybavit i prevenčním systémem Intrusion Prevention Systém (IPS). „Prevenční systémy IPS od prvního možného okamžiku brání v úspěšném dokončení útoku. Systém IPS spolupracuje s detekčním systémem IDS, přičemž výrobci zpravidla oba mechanizmy kombinují.“ [6]

Během zavádění firewallu do provozu bylo rozhodnuto, že zařízení bude pracovat v modelovém nastavení, kdy všechny služby jsou zakázány a na povolené služby jsou

v systému uděleny výjimky. Jednotlivé služby jsou konfigurovány pro uživatele definované v Access Control List (ACL) a jsou konkretizovány, pro jaký typ komunikace na daném portu má být spojení úspěšné. Pokud komunikační provoz neodpovídá těmto pravidlům, neumožní Kernun spojení.

V projektu TC ORP bude Kernun plnit především obranou funkci před případnými útoky zvenčí a prostředníka pro vytváření bezpečného spojení s organizacemi a obcemi využívajících námi nabízených služeb.

Při spuštění projektu do ostrého provozu je počítáno se spuštěním pouze dvou základních služeb TC ORP. Jedná se o negarantované úložiště, které budou využívat převážně spisové služby jako datový prostor pro neuzavřené spisy. Uzavřené spisy budou průběžně přesouvány na TC kraje. Druhou poskytovanou službou bude hostovaná elektronická spisová služba.

Hostovaná elektronická spisová služba je aplikace třetí strany. Jedná se o aplikaci zabezpečující evidencí písemností v elektronické podobě a vyhovující předpisům stanoveným zákonem č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů a vyhláškou č. 191/2009 Sb., o podrobnostech výkonu spisové služby. Komunikace bude zpřístupněna na lokálním serveru umístěném v demilitarizované zóně (DMZ) místní sítě LAN. Službu zprostředkovává aplikace Tomcat na portu 8080. Externí organizace budou přistupovat do DMZ pomocí tunelu VPN. Pro vytvoření bezpečného komunikačního spojení bude mezi uživateli služeb a TC ORP vytvořen šifrovaný kanál virtuální privátní sítě (VPN). „Nad sítí VPN může každý vzdálený uživatel bezpečně a spolehlivě komunikovat s privátní sítí LAN i přes veřejný internet. U sítě VPN nehraje prostorové rozmístění prakticky žádnou roli.“ [6]

Pro vytváření virtuální privátní sítě bude pro jednotlivé uživatele použit speciální klientský software OpenVPN. Na serverové straně bude vytvořen klientský certifikát, který bude umístěn na bezpečné úložiště – token. Po předání uživatelům, bude provedena osobní návštěva pracovníků oddělení informatiky MěÚ v místě připojované lokality, kde bude provedena instalace a konfigurace klientského software. V rámci tohoto servisního zásahu bude ověřena funkčnost spojení. Pro organizace s vyšším počtem PC nebude sestavována VPN pro každého uživatele zvlášť, ale bude vytvořen VPN tunel pomocí zařízení Kernun Branch Access, které zabezpečí připojení celé vzdálené lokality a její místní sítě LAN.

Pro spojení prostřednictvím VPN je v současné chvíli k dispozici pouze protokol IPv4. UTM zařízení je do budoucna připraveno i pro komunikaci pomocí protokolu IPv6, záleží pouze na konfiguraci. Používání klienta OpenVPN je možné i ze sítě, která využívá NAT. Spojení je realizováno VPN tunelem pomocí UDP protokolu (port 4500). „Protokol UDP je nespojovaná služba (na rozdíl od protokolu TCP), tj. nenavazuje spojení. Odesílatel odešle UDP datagram příjemci a už se nestará o to, zdali se datagram náhodou neztratil (o to se musí postarat aplikační protokol). Pole délka dat obsahuje délku UDP datagramu (délku záhlaví + délku dat). Minimální délka je tedy 8 bajtů.“ [4]

Každý datagram obsahuje záhlaví UDP, jež obsahuje identifikaci zdrojového (source port) a cílového portu (destination port). Spolu s identifikací portů záhlaví obsahuje informace o délce UDP datagramu (UDP lenght) a kontrolním součtu (UDP checksum).

4.5 Analýza zavedení virtualizace na TC ORP

Analýza současného stavu ICT na MěÚ Otrokovice ukazuje, jakým způsobem a jakými mechanizmy je zajišťován oddělením informatiky provoz serverové části výpočetní techniky. Z důvodu rozložení rizik nedostupnosti klíčových aplikací je v provozu několik serverů, které zajišťují hardwarové vybavení pro poskytované služby uživatelům. Vytíženost těchto zařízení se v průměru pohybuje do 15 % využití výpočetního výkonu.

Právě snahou o vyšší dostupnost a efektivnější využití výpočetního výkonu serverů jsme byli vedeni k myšlence využití virtualizačních technologií v našem projektu. V minulé kapitole je popsán návrh serverové architektury, která bude právě pro virtualizaci využita. Spolu s těmito systémovými prostředky bude využita i vhodná stávající technologie, kterou MěÚ Otrokovice disponuje. Všechny hardwarové prostředky využité v nově budovaném TC ORP disponují tzv. „zelenou technologií“, která umožňuje radikální snížení provozních nákladů. Toho je dosaženo variabilním výkonem napěťových zdrojů, které mění svůj výkon dle aktuálního zatížení komponent systému. Cesta, kterou se ubírá vývoj serverových technologií, je snažit se při maximálním využití systémových prostředků minimalizovat spotřebu elektrické energie a produkci zbytkového tepla. Tím je dosaženo i prodloužení životnosti klimatizačních jednotek a snížení jejich spotřeby elektrické energie.

Projekt TC ORP je převážně o poskytování služeb jak samotnému ORP, tak i obcím v jeho správním obvodu. Celý projekt bude úspěšný pouze za předpokladu, že v rutinním

provozu bude celá architektura stabilní a finančně efektivní. Tomu musí předcházet maximálně kvalitní příprava všech fází projektu. To platí i o přípravě virtualizace.

Přechod technologie TC ORP na virtuální prostředí lze definovat v pěti krocích:

- „Analýza – první krok začíná s inventarizací datového centra a určením vhodných kandidátů na virtualizaci.
- Virtualizace – druhý krok je zaměřen na úplné porozumění možnostem, které může virtualizace nabídnout.
- Maximalizace hardwaru – třetí krok se zaměřuje na obnovu hardwaru a na zákonné investice při přidání nového hardwaru nebo nahrazení starších systémů.
- Architektura – čtvrtý krok se týká architektury, kterou musíte připravit pro správné zavedení vizualizačních technologií do procesů vašeho datového centra.
- Správa – poslední krok se zaměřuje na aktualizaci nástrojů správy, které použijete k dodržení úplných virtualizačních scénářů ve vašem novém dynamickém datovém centru.“ [5]

4.5.1 Analýza

Při zpracování analýzy byla na našem úřadě provedena inventarizace současného datového centra a systémových uživatelských prostředků. Pro inventarizaci MěÚ Otrokovice využívá SW produktu od společnosti FairNet spol. s r.o. – MagicEYE. Výsledky inventarizace jsou využívány při lokalizaci jednotlivých zdrojů a pro efektivní správu výpočetní techniky. Výsledky inventarizace serverové techniky jsou uvedeny v tabulce č. 4.

Součástí prováděné analýzy bylo i určení vhodných zařízení, použitelných k virtualizaci. Ze současného vybavení MěÚ bude pro virtualizaci využit pouze jeden server, který bude zajišťovat dohledové a administrační funkce pro TC ORP.

Součástí vyhodnocení analýzy je stanovení kategorií zařízení poskytující služby v rámci TC ORP. Jedná se především o:

- servery součástí síťové infrastruktury – jedná se o zařízení poskytující v celé architektuře základní síťové služby, jako např. DHCP server, DNS server, DMZ zóny, zajištění směrování či umožnění vybudování VPN přenosů;

- servery pro správu identit – tyto servery zajišťují správu identit v místní síti, konkrétně v našem případě jde o Domain Controller (Win2003 R2) s Active Directory;
- aplikační servery – jedná se o zařízení zajišťující provoz centrálních i lokálních aplikací;
- databázové servery – servery poskytující databázové služby aplikačním serverům;
- souborové a tiskové servery – servery poskytující služby síťových úložišť dat a tiskových serverů;
- webové servery – servery umístěné v DMZ určené na provoz webových služeb pro veřejnost a servery zajišťující webové služby pro potřeby MěÚ.

Cílem analýzy je vytvořit synergii, kdy dosáhneme optimalizace HW prostředků a počtu spravovaných serverů.

4.5.2 Virtualizace

Samotný pojem virtualizace je definován jako:

„umělé prostředí, které je prozkoumáváno prostřednictvím smyslových podnětů (jako je dívání se či zvuky) zprostředkovaných počítačem a ve kterém akce subjektu částečně určují, co se v prostředí stane.“ [5]

Virtualizaci můžeme rozdělit do několika vrstev:

- serverová virtualizace – zajistí rozdělení fyzických instancí operačního programu na virtuální instance;
- virtualizace sítě – umožňuje spravovat dostupnou šířku pásma pomocí VLAN;
- virtualizace storage – v případě TC ORP jde o SAN architekturu, kdy virtualizační controller vytváří logické jednotky úložiště o definovaných velikostech (LUN) alokováním diskové kapacity fyzických diskových úložišť v SAN;
- management virtualizace – umožňuje správu a administraci TC ORP;
- virtualizace aplikací – umožní nezávislost provozovaných aplikačních služeb na konkrétních prostředcích výpočetní techniky;
- virtualizace prezenční vrstvy;
- virtualizace desktop.

Samotnou virtualizaci se dělí dle modelů použití, a to:

- hardwarová virtualizace – tento princip virtualizace využívá tzv. Hypervizor, což je programový kód integrovaný přímo do hardware. Hypervizor zprostředkovává a obsluhuje hardware všem virtuálním serverům, které jsou na daném HW instalovány. Nevyžaduje operační systém a dokáže pracovat přímo z firmwaru počítače.
- softwarová virtualizace – vyžaduje a je závislá na operačním systému hostitele, je vhodná spíše pro modelové instalace, než pro nasazení v reálném prostředí.

4.5.3 Maximalizace využití výkonu hardware

Při dimenzování hostitelských serverů jsme se drželi následujících pravidel:

"Mělo by se jednat, pokud možno, o blade servery, neboť jejich implementace je po počáteční konfiguraci skříně rychlejší než implementace jiných typů serverů. Měly by obsahovat více síťových karet, aby byla zajištěna dostatečná propustnost pro více provozovaných virtuálních počítačů. Operační systém by měl být uložen na sdíleném úložišti nebo na hardwaru hostitele, neboť bude zajišťovat provisioning." [5]

Největším problémem pro virtualizovaná zařízení je dostatek operační paměti RAM. Pro využití operační paměti RAM nelze stejnou oblast alokovat pro více virtuálních serverů, a proto musí systém obsahovat dostatek RAM, aby pokryl nároky všech virtuálních serverů. Z těchto objektivních důvodů je doporučená minimální kapacita paměti RAM v hostitelských serverech 32 GB (optimálně 64 GB). Vzhledem k tomu, že běžné 32bitové systémy umí adresovat maximálně 4 GB operační paměti, jsou virtualizované servery postaveny na architektuře procesorů x64. 32bitové systémy většinou alokují 2 GB pro potřeby systému a zbylá kapacita 2 GB může být využita pro provozované služby a aplikace. To může být limitující faktor, způsobující nestabilitu systému. Řešením této problematiky je implementace 64bitovýh operačních systémů. Tyto nám umožňují adresovat v současné době dostatečné kapacity operačních pamětí RAM.

4.5.4 Architektura infrastruktury

Při tvorbě TC ORP je pro nás nejdůležitější parametr vytvoření robustní a hlavně maximálně dostupné infrastruktury, která nebude obsahovat žádný „single point sof failure", tzn. zamezit správnou architekturou vzniku jediných míst selhání. Vybrané prvky byly při rozhodování konfrontovány právě s touto myšlenkou. Proto byl při návrhu vybrán

systém s maximální redundancí jak klíčových komponent, tak i datových cest, konektivity k internetu a clusterování jak výpočetních zdrojů, tak i aktivních prvků sítě LAN. Tím bylo dosaženo rozložení zátěže klíčových komponent a vysoké dostupnosti. V případě výpadku některého zdroje jeho funkci automaticky převezme zdroj spojený v clusteru s původním zdrojem.

Pro přístup k datům ve virtualizovaném prostředí bude využito bezpečnostní politiky CDS (Castle Defense System). Jedná se o systém přístupu k datům přes několik ochranných vrstev, kde každá z těchto vrstev v systému zabezpečuje daný stupeň ochrany. V praxi to znamená, že každý požadavek o informaci bude nejprve prověřen, zda má daný uživatel k požadovaným informacím oprávnění. Pokud je uživatel autorizován, zapojí se do ochranného systému uživatelů operační systém, který pomocí svých bezpečnostních prvků tvoří další bezpečnostní vrstvu. V našem případě se bude jednat o umístění TC ORP v 1. patře budovy, zabezpečené elektronickým zabezpečovacím systémem s identifikací vstupujících osob do serverovny. Řádný přístup bude umožněn pouze pracovníkům oddělení informatiky MěÚ Otrokovice. Jediný přístup k místnosti, ve které bude TC ORP umístěno, bude přes kancelář vedoucího oddělení informatiky a místnost bude vybavena bezpečnostními dveřmi. Technologická místnost bude vybavena kvalitním chladícím klimatizačním systémem, elektronickou protipožární signalizací, zhášecím systémem a nepřerušitelným zdrojem elektrické energie. V případě dlouhodobého výpadku elektrické energie je dodávka elektřiny zajištěna náhradním dieselovým agregátem.

Poslední ochrannou vrstvu tvoří zabezpečení samotné vizualizované aplikace, která nám poskytuje konkrétní data.

4.5.5 Strategie obnovení systému

Pro stanovení vhodné strategie obnovení systému jsou lokalizována a vyhodnocena oddělením informatiky rizika, která ovlivňují nejenom samotné TC ORP, ale všechnu výpočetní techniku na MěÚ. Zpracování analýzy rizik je stanoveno interním dokumentem „Bezpečnostní politika informačního systému veřejné správy“, který byl oddělením informatiky vytvořen a kterým je řízena činnost informačního prostředí a uživatelů. [28]

Nejvýhodnější strategií kvalitní dostupnosti TC ORP bylo maximalizovat redundanci všech klíčových komponent, včetně datových cest. „Redundance systémů je zajištěna implementací metod a prostředků, které zajistí, že v případě selhání určité

součásti její funkci okamžitě převezme jiná součást nebo alespoň bude dobře zdokumentován postup uvedení dané součásti zpět do provozuschopného stavu a systémoví operátoři budou s touto dokumentací dobře obeznámeni.“ [5]

Na logických jednotkách úložišť bude implementován princip koordinované práce s daty RAID 6. Ten pro svou funkci využívá dvou paritních disků, přičemž každý z těchto disků vypočítává paritu jiným způsobem. Jednoznačná výhoda RAID 6 je odolnost proti výpadku až dvou disků najednou.

Jednotka SAN Volume Controlleru, kterým bude TC ORP vybaveno, zajišťuje vytváření tzv. snapshotů. Jedná se o snímky dat, které jsou uloženy mimo produkční oblast dat a ze kterých lze jednoduše obnovit činnost. V našem případě půjde o snímkování na sekundární diskové pole, které v případě totálního výpadku primárního pole převezme jeho funkci a zajistí dostupnost služeb.

Pro katastrofický scénář úplného výpadku celého Technologického centra připravujeme v jiné budově MěÚ (tato je umístěna v jiné lokalitě města) náhradní serverovnu, která bude moci poskytnout základní strategické služby. Data se budou přenášet pomocí replikace a hardwarové prostředky tohoto náhradního datového centra budou optimalizovány na dočasné zabezpečení klíčových aplikací a služeb a ne na výkon.

V rámci připravovaného projektu metropolitní sítě Zlínského kraje bude také možno z bezpečnostních důvodů přesouvat strategická data mezi vzdálenými lokalitami, takže bychom v případě teroristického útoku, který by zničil veškerou infrastrukturu výpočetní techniky u nás, včetně záloh uložených na pásce v trezoru, měli tato data „uschována“ v lokalitách jiných měst. Tato města by poté byla schopna zprostředkovat nezbytné služby.

4.5.6 Správa vizualizovaného prostředí

V Technologickém centru budou implementovány dva modely virtualizace. Jeden model bude spočívat ve virtualizaci zdrojů výpočetního výkonu a tento bude spravován z administračních nástrojů společnosti VMware vCenter.

Druhý použitý model bude virtualizace storage, pro jehož administraci budeme využívat nástrojů zařízení SAN Volume Controller, které poskytuje veškeré nástroje pro konfiguraci a správu diskových úložišť.

4.5.7 Plánování a příprava

Při plánování a přípravě konsolidace zdrojů virtualizace je postup rozdělen do několika fází implementace. V našem případě začneme virtualizovat webové servery, zajišťující intranetové služby uživatelům spolu se souborovými a tiskovými servery. Servery zajišťující klíčové centrální aplikace budou virtualizovány jako poslední. Jelikož jsou současné servery již minimálně dva roky v plném provozu, nebude použita při jejich konsolidaci metoda převodu stávajících instalací do virtuálního prostředí, ale všechny konsolidované servery budou nově instalovány.

Při zvažování zavedení virtualizace v TC ORP bylo rozhodnuto, že bude implementována virtualizace od komerčního výrobce. Toto rozhodnutí nese vyšší finanční nároky, ale z důvodu důležitosti celého projektu jsou finance za vizualizační technologie akceptovatelné.

Hlavní výrobci virtualizačních produktů na trhu jsou společnosti VMware, Microsoft a Citrix. Existují i jiní výrobci se svými řešeními, ta jsou ale optimalizována na konkrétní produkty. Technologické centrum potřebuje vzhledem k různorodosti prostředí stabilní, rychlé a v praxi ověřené řešení pro všechny platformy, které budou implementovány.

Srovnání výrobců v základních parametrech:

Metrika	VMware	Microsoft	Citrix
Režie provozu hypervisoru	Zanedbatelné	Jedno jádro procesoru	Jedno jádro procesoru
Maximální velikost paměti	256 GB	32 GB až 2 TB	128 GB
Paměť RAM pro hypervisor	32 MB+	512 MB+	256 až 512 MB+
Maximální počet soketů procesorů (hostitel)	32 jader	24 jader	Neomezeno
Maximální počet soketů procesorů (host)	4	4	8
Vyžadovaný počet síťových karet pro správu	1	1	1
Maximální počet serverů ve fondu nebo clusteru	32	16	16
Počet virtuálních počítačů na jedno jádro	8 až 11	8	2 až 8

procesoru			
Maximální velikost paměti (host)	64 GB	64 GB	32 GB
Současně aktivních hostů na jednoho hostitele	192	192	Neomezeno
Podpora hostovaných operačních systémů	Microsoft Windows 3.1/3.11/95/98/Me/ NT/2000/2003/2008/XP /Vista platforem x86 nebo x64 MS-DOS 6.x Red Hat Enterprise Linux 2.1/3/4/5 RedHat Linux Advanced Server 2.1 Rad Hat Linux 7.2/7.3/8.0/9.0 SUSE Linux Enterprise Server 8/9/10 SUSE Linux 8.2/9.0/9.1/9.3 FreeBSD 4.9/4.10/4.11/5.0 Turbo Linux 7.0, Enterprise Server/Workstation 8 Novell Linux Desktop 9 Sun Java Desktop Systém 2 Netvare 6.5/6.0/5.1 Solaris 9/10 platformy x86	Microsoft Windows 2000/2003/2008/XP Pro/ platforem x86 a x64 SUSE Enterprise Linux Server 10 SP1	Microsoft Windows 2003 SP2 platformy x64 Microsoft Windows 2000/2003/SBS 2003/2008/XP SP2/Vista platformy x86 Pentos 4.1/4.2/4.3/4.4/4.5/5.0/5.1 platformy x86 a 5.0/5.1 platformy x64 OracleEnterprice Linux 5.0/5.1 platforem x86 a x64 Red Hat Enterprise Linux 3.5/3.6/3.7/4.1/4.2/4.3/ 4.4/5 platformy x86 a 5.0/5.1 platformy x64 SUSE Enterprise Linux Server 9 SP2/9 SP3/10 SP1 32bitový Debian Sarge 3.1/Etch 4.0 32bitový
Podpora 64bitového hosta	Většina operačních systémů platformy x64	64bitové operační systémy Windows	64bitové operační systémy Windows

Tab. 5. Srovnání vlastností virtualizačních prostředí [5]

Porovnáním vlastností jednotlivých řešení bylo rozhodnuto, že pro implementaci bude využito produktů od společnosti VMware, a to především pro jeho kompatibilitu s různými platformami a univerzálnost systému. Mimo to nabízí také nejmodernější funkce, jako např. VMotion, které umožní přesun virtuálního prostředí na jiný hardware bez výpadku aplikace či služby.

5 REALIZACE PROJEKTU

5.1 Popis stávajících prostor

Veškerá stávající infrastruktura, viz Tabulka č. 4, včetně serveru pro příspěvkovou organizaci, telefonní ústředny a centrálního uzlu topologie LAN se nachází v místnosti o velikosti 1,5 m x 2,7 m. Pro svou velikost je místnost nevyhovující z důvodu ztížené manipulace se zařízeními a značného nárůstu teploty během velmi krátkého časového intervalu při výpadku klimatizační jednotky. Místnost je nedostatečně zabezpečena proti násilnému vniknutí a není vybavena ani elektronickou protipožární signalizací. Účast na projektu TC ORP byla jedinečnou příležitostí k organizačním změnám na MěÚ, a tím se podařilo uvolnit sousedící místnost se stávající serverovou a vytvořit podmínky pro přesun serverové techniky do nové technologické místnosti. Ve stávající místnosti zůstane telekomunikační ústředna i rozvody sítě LAN, servery budou přesunuty.

5.2 Nová serverovna a přípravy nových prostor

Při vybavování nové technologické místnosti došlo nejprve na vybavení zabezpečovacími prvky, které ve stávající serverovně chyběly. Nutnost těchto zabezpečovacích prvků je součástí podmínek dotace.

Elektronický zabezpečovací systém byl dodán společností Systém Plus, která implementovala zabezpečovací systém na celém úřadě. Místnost byla vybavena bezkontaktní snímací hlavou, která umožní vstup pouze osobám s magnetickou docházkovou kartou, pro kterou je v systému zadáno oprávnění vstupu. Pomocí snímací hlavy je ovládán elektronický zámek dveří a jsou odesílána data serveru o jednotlivých průchodech.

Nová místnost je vybavena klimatizací, elektronickou protipožární signalizací, bezpečnostními dveřmi, zhášecím systémem.

Vzhledem k faktu, že v současnosti MěÚ nedisponuje rackem, který je vhodný pro osazení servery, byl objednán rack od společnosti APC, konkrétně se jedná o typ NetShelter SX o rozměrech 42U, šířka 600 mm a hloubka 1 070 mm. Novými technologiemi a požadavky na vysokou dostupnost jsou kladeny vyšší nároky na zajištění kvalitního a dostatečně dimenzovaného záložního zdroje. Pro tento projekt bylo vybráno

zařízení APC Smart-UPS RT 6000VA RM 230V, které bude taktéž řešeno jako redundantní.

Při výběru UPS byla spočítána maximální možná spotřeba jednotlivých prvků a dle toho bylo identifikováno vhodné zařízení.

Pro zajištění síťové konektivity bylo využito stávajících metalických kabelů kategorie 6e, jimiž bude bladeové chassi připojeno ke dvěma aktivním prvkům 3COM® 5500G a 3COM® 4500G. Tímto připojením bude zajištěna redundance aktivního prvku sítě LAN pro vysokou dostupnost. Při případném výpadku jednoho ze zařízení druhé automaticky převezme jeho funkci.

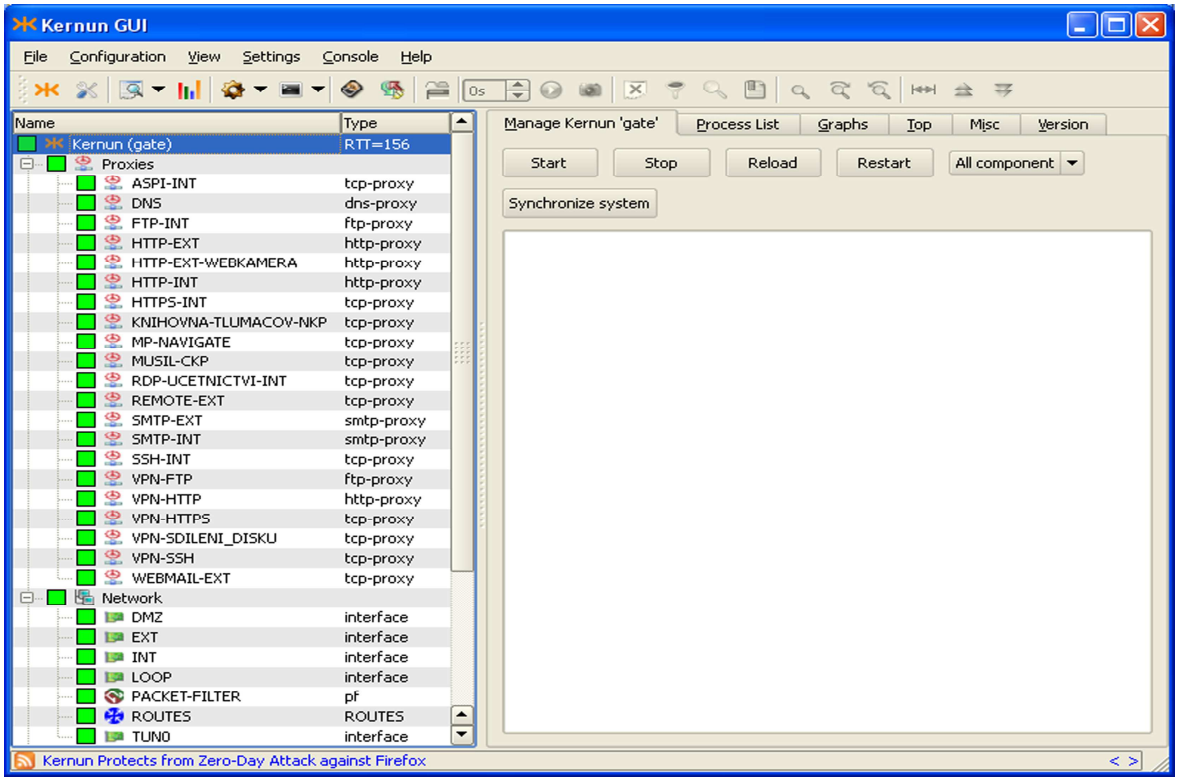
5.3 Implementace firewallu

Mimo průběžných přípravných prací bylo v souvislosti s plánovaným zřízením TC ORP na konci roku 2009 vypsáno poptávkové řízení na UTM zařízení, které bude plnit funkci hlavního bezpečnostního prvku v místní síti a kterým bude zajištěna bezpečná komunikace s externími sítěmi. Firewallem bude zajištěn také vzdálený přístup třetích stran do místní sítě LAN a to pouze k takové množině aktiv, která jsou nezbytně nutná. Úspěšné i neúspěšné autentizace jsou zpracovány dle bezpečnostních pravidel MěÚ a jsou zaznamenány. [28] V poptávkovém řízení byl jako nejvhodnější UTM zařízení vybrán produkt společnosti Trusted Network Solutions, a. s.

Samotné implementaci předcházelo dvoudenní školení na obsluhu a konfiguraci daného zařízení a definice pravidel a postupů pro nastavení bezpečnostní politiky firewallu. Ze dvou směrů bezpečnostních politik byla vybrána restriktivní politika, kdy je zařízení nakonfigurováno tak, že všechny služby jsou zakázané a administrátor povoluje jednotlivé služby. Nevýhodou tohoto zabezpečení je delší časový interval nutný pro implementaci do provozního prostředí a nároky na vysokou preciznost definice bezpečnostních pravidel. Zákazník nemá možnost zásahu do samotného programového jádra UTM zařízení a z tohoto důvodu bylo zařízení dodáno již včetně nainstalovaného softwarového vybavení.

Obr. 20. UTM Kernun Net Access [13]

V podstatě se jedná o jednoprocesorový server DELL s instalovaným CPU Intel® Xeon® E5520, běžícím na frekvenci 2,26 GHz a obsahující 8 MB L3 cache. Server je vybaven 6 GB paměti RAM typu DDR3 pracující na frekvenci 1 066 MHz, dvěma 3,5“ 300GB HDD typu SAS otáčející se 15 000 otáčkami za minutu. Oba pevné disky jsou redundantně zapojeny v RAID 1 pomocí řadiče PERC 6/i s 256 MB cache, která je zálohovaná baterií. [8] Samotné aplikační prostředí tvoří upravený operační software freeBSD. Tento OS je upravován a vyvíjen společností Trusted Network Solutions, a. s., která do něj implementovala svou bezpečnostní aplikaci.



Obr. 21. UTM Kernun Net Access - konfigurace

Pomocí konfiguračního rozhraní UTM byla nejprve nakonfigurována rozhraní síťových karet, jednak externí rozhraní určené jako vstup/výstup z UTM do externích sítí, interní rozhraní jako vstup z interní sítě do UTM zařízení a rozhraní demilitarizované zóny (DMZ). Součástí DMZ je v současné době server, na kterém je spuštěn zkušební provoz hostované elektronické spisové služby. Součástí konfigurace rozhraní byla i definice virtuálního rozhraní zprostředkovávajícího VPN připojení externích klientů.

5.4 Budování VPN

Přípravy vhodného bezpečného připojení organizací a obcí k Technologickému centru proběhly v březnu roku 2010. VPN spojení pro jednotlivé uživatele bylo vytvořeno pomocí klientského programu OpenVPN, jež je volně ke stažení na URL adrese *http://openvpn.net/index.php/open-source/downloads.html*. Klientské certifikáty jsou vytvářeny pomocí software OpenSSL, jež je naimplementováno přímo na UTM Kernun.

5.5 Správa klíčů a certifikátů pro VPN

Vytvoření certifikátu sestává ze dvou kroků:

- vygenerování klíče a certifikační žádosti,
- podepsání regestu klíčem certifikační autority.

Při generování certifikátu klienta je nutno dbát na to, aby si sebou nesl příznak „client“, což je nastaveno v souboru openssl.cnf. Konkrétně se jedná o položku „nsCertType“. Generujeme certifikáty s platností 1470 dnů.

5.5.1 Generování klíče a certifikační žádosti

Veškeré úkony spojené s certifikáty jsou prováděny přímo v UTM Kernun v adresáři, kde je OpenSSL implementován. Prvním příkazem je vytvořena certifikační žádost a nový privátní klíč.

```
# openssl req -config $CATOP/openssl.cnf -new -nodes -keyout
newreq.pem -out newreq.pem -days 1470
```

V proměnné `$CATOP` je zadáno konkrétní umístění konfiguračního souboru v adresářové struktuře Kernunu. Pro spuštění příkazu se na obrazovce objeví dialogové okno, kde je systémem vyžadováno zadání následujících položek:

```
Generating a 2048 bit RSA private key
writing new private key to 'newreq.pem'

Country Name (2 letter code) [CZ]:
State or Province Name (full name) [Czech Republic]:
Locality Name (eg, city) [Otrokovice]:
Organization Name (eg, company) [Mestsky Urad]:
Organizational Unit Name (eg, section) [OVPN-MUO]:
Common Name (eg, YOUR name) []:MartinManasek
Email Address []:manasek@muotrokovice.cz

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

Položky, které nemají předvyplněnou hodnotu (údaj uvedený v hranatých závorkách), je doplněn uživatelsky a po potvrzení prázdného hesla vznikne soubor „newreq.pem“, který obsahuje žádost o certifikát a privátní klíč. Tento request je následně podepsán klíčem certifikační autority.

5.5.2 Podpis žádosti klíčem certifikační Autority

Z příkazového řádku je provedeno

```
#  openssl ca -config $CATOP/openssl.cnf -days 1470 -policy
policy_anything -out newcert.pem -infiles newreq.pem
```

Vznikne nový soubor newcert.pem, který obsahuje nový certifikát.

```
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CZ'
stateOrProvinceName   :PRINTABLE:'Czech Republic'
localityName          :PRINTABLE:'Otrokovice'
organizationName      :PRINTABLE:'Mestsky Urad'
organizationalUnitName:PRINTABLE:'OVPN-MUO'
commonName            :PRINTABLE:'MartinManasek'
emailAddress          :IA5STRING:'manasek@muotrokovice.cz'
Certificate is to be certified until May 23 10:27:33 2014 GMT
(1470 days)
Sign the certificate? [y/n]:y

1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
```

Oba soubory newreq.pem a newcert.pem jsou přejmenovány a uschovány v bezpečném úložišti.

5.5.3 Tvorba PKCS#12

Formát PKCS#12 je binární podoba certifikátu, která může kromě privátního klíče (newreg.pem) obsahovat i certifikát (newcert.pem) a také certifikát Autority. Tento formát je používán především pro import certifikátů do Internet Exploreru, ale umí jej používat také právě software OpenVPN klient. Nově vzniklý soubor formátu PKCS#12 (newcert.p12) je chráněn heslem, které je zadáno v dialogu během vytváření tohoto souboru.

```
# openssl pkcs12 -export -in newcert.pem -inkey newreq.pem -
certfile cacert.pem -out newcert.p12
```

5.5.4 Revokace certifikátu, vytvoření CRL

Revokace certifikátu je prováděna, pokud má být ukončena jeho platnost dříve, než sám exspiruje. Nejprve je nutno zjistit pomocí souboru `index.txt`, o který certifikát z adresáře `newcerts` se jedná. Poté následuje samotná revokace certifikátu.

```
# openssl ca –config $CATOP/openssl.cnf –revoke
$CATOP/newcerts/01.pem
```

V souboru `index.txt` je změněn příznak u daného záznamu certifikátu z písmena „V“ na písmeno „R“. Po revokaci následuje vytvoření nového CRL souboru, jehož obsahem je seznam revokovaných certifikátů.

```
# openssl ca –config $CATOP/openssl.cnf –gencrl –out
$CATOP/crl/crl.pem
```

Od tohoto okamžiku se již uživatel s revokovaným certifikátem nebude moci přihlásit k UTM zařízení a nebude mu umožněno vytvoření VPN spojení.

Pokud vznikne nutnost krátkodobě znemožnit platnému uživateli připojení k naší síti, lze to provést deaktivací virtuálního interface přiřazeného danému uživateli.

Spojení vzniká tak, že je v Kernunu provedena konfigurace virtuálního rozhraní typu TUN, jež se chovají jako klasické virtuální zařízení. Při rozhodování, zda bude použit typ TUN, nebo TAP pro virtuální zařízení, bylo nutno definovat si požadavky na spojení a vlastnosti jednotlivých typů.

TUN – tunel, spojení typu Point-to-Point navržen k IP tunelování. Konfigurací rozhraní v UTM je docíleno přiřazení pevné IP adresy připojovanému klientu. Princip TUN zařízení nedovoluje klientovi si tuto přidělenou IP adresu změnit. Systémy Windows, TUN rozhraní pouze emulují jako TAP zařízení, ale s 30bitovou maskou podsítě. Tzn., že rozsah standardní sítě (255 IP adres) je rozdělen na 64 oddílů po čtyřech IP adresách. Z toho jednou IP je udávána adresa sítě, jednou broadcast a zůstávají pouze dvě IP adresy použitelné pro vytvoření spojení. Pokud by si chtěl útočník změnit IP adresu, dojde k ukončení spojení, protože by musel použít IP z jiné sítě. Zařízení typu TUN umožňuje připojení maximálně 64 klientů.

TAP – jedná se o emulaci ethernetového rozhraní. Síť používá klasickou 24bitovou masku podsítě (255 IP adres). První IP udává adresu sítě a poslední IP z daného rozsahu udává broadcast. Všechny ostatní IP jsou určeny pro klienty. Zařízení typu TAP umožňuje připojení až 253 klientů.

Pro vytváření VPN tunelů byl vybrán typ TUN z důvodu možnosti uplatňování bezpečnostní politiky na základě IP adres. U zařízení typu TAP toto není možné.

Pro připojení externích lokalit k síti LAN MěÚ Otrokovice není použito certifikátů, jako je tomu v případě jednotlivých uživatelů, ale VPN tunel byl vytvořen pomocí hardwarového zařízení Kernun Branch Access. Je to hardwarový VPN klient přímo určený pro vytváření bezpečných tunelů mezi pobočkami a. Veškeré komunikační služby u tohoto bezpečného spoje jsou provozovány v tunelu a jsou řízeny centrální firewallem. Z těchto služeb je vyjmuta pouze služba VoIP, která je směřována přímo na internet, aby zbytečně nezabírala kapacitu linky.

VPN spojení je budováno především k bezpečnému využívání služeb TC ORP, především negarantovaného úložiště a elektronické spisové služby.

5.6 Školení spisové služby

Ke konci minulého roku MěÚ Otrokovice zřídilo vzdělávací eGON centrum, které má za úkol vzdělávat uživatele v centrálních aplikacích eGovernmentu, jako jsou např. Czech POINT a Informační systém datových schránek. Mimo těchto oblastí je plánováno v polovině letošního roku začít se školením uživatelských aplikací, jako jsou MS Word a

MS Excel. Kompletní seznam plánovaných školicích kurzů včetně časových dotací na jednotlivá školení:

- Obecné základy práce s portálem Czech POINT (CzP) – (4 hod.)
- CzP – Katastr nemovitostí (2 hod.), CzP – Živnostenský rejstřík (2 hod.), CzP – Rejstřík trestů (2 hod.), CzP – Obchodní rejstřík (1 hod.), CzP – Seznam kvalifikovaných dodavatelů (1 hod.), CzP – Modul autovraků informačního systému odpadového hospodářství (2 hod.), CzP – Insolvenční rejstřík (1 hod.), CzP – Bodové hodnocení řidiče (2 hod.)
- CzP – Autorizovaná konverze dokumentů (4 hod.)
- CzP – Agendy Informačního systému datových schránek (ISDS) I. (4 hod.)
- CzP – Služby ISDS II. (6 hod.)
- Informační systém datových schránek (8 hod.)
- Zaručený elektronický podpis (8 hod.)
- Word pro začátečníky (24 hod.)
- Excel pro začátečníky (24 hod.)
- Vidimace a legalizace (8 hod.)
- Úvod do elektronických spisových služeb, praktická práce s ESS (8 hod.)

Na školení těchto dovedností byl vypracován tříletý plán, který počítá se 4 lektory zajišťujícími školení. Byla zajištěna vhodná místnost, která je vybavena devíti školicími místy, elektronickými didaktickými pomůckami a projektorem. Představa vybudování eGON center jako technologických a metodických strategických pracovišť, poskytujících tyto zásadní služby obcím a organizacím ve svém správním obvodu, vychází rovněž z vládní iniciativy „Smart Administration“, kde vláda České republiky deklarovala základní směřování ke zkvalitňování veřejné správy ve strategii Efektivní veřejná správa a přátelské veřejné služby. [23]

Pro všechny obce v našem správním obvodu bylo v loňském roce podstatné datum 1. listopad 2009, kdy byla všem orgánům veřejné moci aktivována Datová schránka. Aby k tomuto termínu byly naše obce schopny pracovat s touto převratnou novinkou v doručování písemností, byly ještě před aktivací všechny proškoleny na obsluhu svých

datových schránek, základní principy a práci s elektronickými certifikáty. Spolu s uvedeným školením byly obce proškoleny i na konverzi elektronických dokumentů do papírové podoby a naopak. Jelikož část našich obcí k tomuto termínu otevírala i nová pracoviště CzP na svých úřadech, probíhalo i školení obsluhy a základních funkcionalit CzP.

V loňském roce, konkrétně od 1. června 2009, vstoupila v platnost novela archivního zákona, která stanovuje pravidla nakládání orgánů veřejné moci s elektronickými dokumenty. Tato novela stanovuje i nejzazší závazné termíny přizpůsobení obcí těmto podmínkám. Pro obce (a to je v našem správním obvodu většina), které nedisponovaly k termínu vydání novely žádnou elektronickou službou, ale evidovaly písemnosti písemně, byl stanoven závazný termín 1. červen 2010. K tomuto termínu mají obce začít evidovat své písemnosti v elektronické spisové službě odpovídající aktuální novele zákona č. 499/2004 Sb., o archivnictví a spisové službě a zákonu č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů. [27]

Aby bylo umožněno našim obcím dodržet tento termín bez zbytečných investic do dočasných řešení, bylo rozhodnuto vyhradit naše serverové zařízení pro poskytnutí služby hostované elektronické spisové služby (ESS) do doby, než bude v ostrém provozu TC ORP. Proto byla obcím nabídnuta možnost školení na popis a základní principy práce s elektronickou spisovou službou.

5.7 Instalace hostované elektronické spisové služby Vera Flexi

Pro provoz dočasného řešení hostované ESS bylo vybráno zařízení HP Proliant DL380 G6.

Obr. 22. HP Proliant DL380 G6 [10]

Tento server o výšce 2U je osazen jedním Quad-core CPU Intel® Xeon® X5550 vybaveným 8 MB L3 cache. V systému jsou implementovány 4 GB operační paměti RAM, konkrétně se jedná o paměti typu RDIMM DDR3 PC3-10600R. O konektivitu se starají dva gigabitové ethernetové porty. Pro zajištění vysoké dostupnosti je server vybaven redundantním napájením a chlazením. Redundance dat je zajištěna diskovým řadičem Smart Array P410i/256 MB, BBWC, jehož zapisovací cache (256 MB) je zálohována samostatnou baterií pro případ náhlého přerušení dodávky elektrické energie. Diskovým řadičem jsou obsluhována dvě logická pole v RAID 1 – jedno o velikosti 146 GB a druhé o velikosti 300 GB. Obě pole jsou tvořena SAS externími disky s rychlostí otáčení ploten 15 000 otáček za minutu. První pole je určeno pro instalaci operačního systému a provozních aplikací. Druhé logické pole je určeno jako úložiště dokumentů a dat uložených z datových schránek obcí a organizací. Podstatná data jsou zálohována páskovou knihovnou IBM TS3100 během každého večera.

Na doporučení výrobce ESS společnosti VERA, s. r. o., byl server nainstalován na operační systém (OS) Red Hat Linux 5.0 (RHL). Jedná se o komerční stabilní řešení.

Při instalaci OS byl bootovací pevný disk rozdělen na tři svazky. Svazku „/boot“ byla přidělena velikost 100 MB, rootovskému svazku „/“ 36 GB a poslední svazek „/home“ byl nakonfigurován na velikost 94 GB. Druhý pevný disk nebyl rozdělen a slouží jako úložiště pro dokumenty, přičemž jeho velikost je 270 GB a označení „/home2“. Všechny svazky jsou naformátovány na souborový systém ext3.

Po instalaci operačního systému byla provedena instalace doplňkových služeb a software nutného k provozování aplikace elektronické spisové služby od společnosti Vera, s.r.o. Z těchto důvodů byla nainstalována aplikace Java JRE 6 (Java Runtime Environment) a následně i webový server Tomcat verze 6.0.20. Instalovány byly verze aplikací, které má výrobce spisové služby uvedeny v port listu, který zajišťuje kompatibilitu s jeho produktem a stabilní provoz. Tomcat je nastaven tak, aby své webové služby nabízel uživatelům na portu 8080.

Kvůli správné komunikaci se zálohovacím serverem bylo nutno provést instalaci linuxového klienta zálohovacího systému Backup Exec (RALUS). Ten zajišťuje pravidelnou každodenní zálohu určených dat na páskovou knihovnu IBM TS3100.

Po systémových instalacích bylo započato s instalacemi prostředí aplikace spisové služby.

Žádná moderní aplikace se neobejde bez databázového prostředí pro svá aplikační data. Na MěÚ Otrokovice je provozován centrální radniční systém od společnosti VERA s. r. o. Jeho součástí jsou veškeré finanční agendy, jako např. (příjmy, výdaje, účetnictví, objednávky, pohledávky, splátky a půjčky, evidence psů, výherních automatů a komunální odpad), agendy pro výkon přenesené působnosti státní správy (stavební úřad, sociální odbor, živnostenský úřad atd.) a jiné evidenční systémy. Celkem je provozováno 54 agend. Jako databázové prostředí pro tento radniční systém je používána databáze Oracle. Vzhledem k faktu, že hostovaná spisová služba je od stejného výrobce, byla logická volba integrovat databázový prostor do serveru, na kterém je provozována zmíněná databáze. Pomocí databázové konzole byl vytvořen tabulkový prostor pro databázi, kterou pro svůj provoz využívá elektronická spisová služba. Ta se k tomuto databázovému stroji připojuje pouze pomocí služby přes port 1521.

Dnes již neodmyslitelnou součástí ESS je automatizovaný přístup k informačnímu systému datových schránek. Města a obce jako orgány veřejné moci mají zákonem stanovenou povinnost odesílat, pokud je to možné, svá rozhodnutí do datových schránek adresátů v elektronické podobě. Ti, pokud je to pro ně důležité, si mohou elektronický dokument nechat zkonvertovat do papírové podoby přes pracoviště CzP.

Společností VERA byla pro svoji ESS vyvinuta aplikace, která zajišťuje komunikaci s datovým rozhraním systému Datových schránek. Jedná se o WDS konektor, v našem případě jde o verzi 0.9.29. Jde o webovou službu, jež zprostředkovává webový server Tomcat. Jako taková tedy není instalována, ale pouze nakopírována do pracovního adresáře Tomcatu. Po přihlášení do administračního prostředí je součástí nastavení rozhraní port pro připojení ke konektoru, cesta k certifikátu potřebnému pro ověření ISDS a heslo k němu. Konfigurace je ukončena definicí základních adres webových služeb ISDS, které jsou provozovány Ministerstvem vnitra České republiky (MV ČR) a přes které je prováděna komunikace ESS s ISDS.

Další aplikací, která je pro provoz systému nezbytná, je Jednotná správa uživatelů (JSU). Jedná se o webovou aplikaci vytvořenou v technologii JSP (Java Server Pages). Pro správnou instalaci je výrobcem dodáván instalační skript, pomocí něhož je aplikace

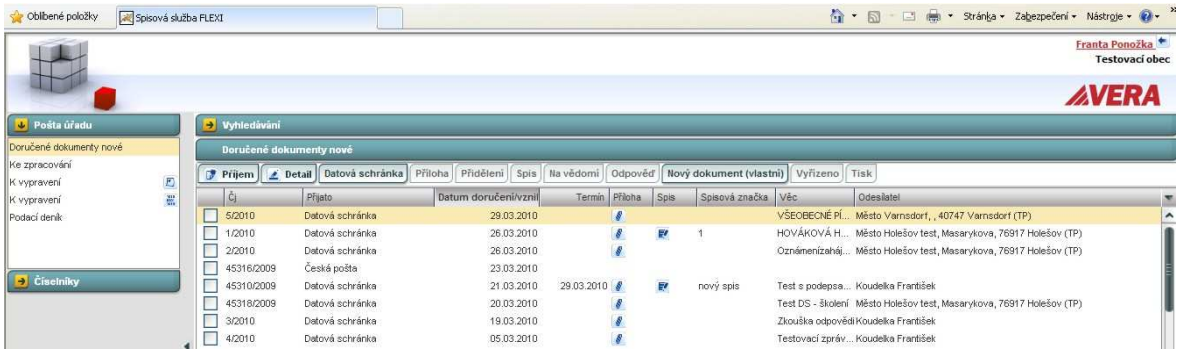
nainstalována. Po instalaci je služba nakonfigurována administrátorem pro rutinní provoz. Nejprve se nakonfigurují organizace a k nim jednotliví uživatelé. V současné době je systém konfigurován pro obec Tlumačov a obec Bělov. Pro testování byla založena organizace testovací obce, kde mají všichni uživatelé oprávnění vstupu. Prostředí testovací obce je napojeno na datovou schránku, která je umístěna v testovacím prostředí ISDS. I přestože budou všichni uživatelé proškoleni na práci s ESS, bude institut testovací obce zachován i v příštím období tak, aby si uživatelé mohli ověřovat správnost pracovních postupů bez rizika poškození ostrých dat.

Obr. 23. Vera - konfigurace uživatelů

Nyní se dostáváme k aplikaci samotné ESS. Elektronická spisová služba FLEXI je také webová aplikace vytvořená v technologii JSP. Pro provoz této aplikace je nutno mít nainstalovaný databázový server. Výrobcem ESS jsou podporovány databáze Informix, Oracle nebo Microsoft SQL Server. Vzhledem k faktu, že je na MěÚ provozována databáze Oracle pro agendový systém Radnice Vera®, byl využit tento databázový server. V databázi byl vytvořen nový oddělený tabulkový prostor, který nemá žádnou vazbu na současná data MěÚ Otrokovice. Při konfiguraci rozhraní na databázi je definován správný databázový ovladač (oracle.jdbc.driver.OracleDriver) a URL adresa, přes kterou bude rozhraní komunikovat. Pro ověřené připojení k databázi je nutno konfigurovat i automatické přihlášení pomocí vloženého loginu a hesla k databázi ESS. Jako poslední byly zadány identifikační údaje k datové schránce organizace, a to jak port na WDS, přes

který bude komunikace probíhat, tak i ID datové schránky pro jednoznačnou identifikaci a číselnou řadu čísel jednacích. Heslo z bezpečnostních důvodů není uvedeno a je zadáváno až samotnými uživateli, pokud potřebují s DS komunikovat.

V ESS Flexi je umožněno pro každou organizaci samostatné nastavení.



Obr. 24. Vera Flexi

Ze strany MěÚ Otrokovice, vystupujícího v roli implementátora eGovernmentu v území, byla obcím ve správním obvodu ORP Otrokovice nabídnuta maximální vstřícnost. Našim přáním je, aby při společném postupu s ostatními obcemi s rozšířenou působností a Zlínským krajem bylo docíleno stabilních a efektivních služeb občanům.

ZÁVĚR

V této bakalářské práci jsem se snažil popsat současný vývoj eGovernmentu ve státní správě a samosprávě. Jako zaměstnanec Městského úřadu v Otrokovicích jsem součástí řešitelského týmu, který se touto oblastí zabývá. Vedení Městského úřadu sdílí myšlenky s vizí vlády České republiky „Efektivní veřejná správa a přátelské veřejné služby“ - Strategie realizace Smart Administration v období 2007–2015 a proto přistoupilo k vytvoření eGON centra v ORP Otrokovice.

V teoretické části jsem se snažil představit projekt Technologického centra ORP Otrokovice z globálního pohledu nabízených služeb státní správy a samosprávy. Bakalářská práce obsahuje informace i o připravovaných projektech, které byly do první poloviny roku 2010 zveřejněny a budou mít přímou návaznost na již realizované projekty. V praktické části jsou uvedeny výsledky analýzy, která byla nutná pro kvalitní přípravu projektu Technologického centra ORP. Spolu s analýzou je uvedena i vybraná technologie, která bude tvořit hardwarovou infrastrukturu a studie proveditelnosti, jež zohledňuje všechny aspekty a jejich dopad na celý projekt. Vzhledem k vybudování nové infrastruktury je zvážena možnost virtulizace a výběr z nabízených řešení na trhu. V závěru bakalářské práce jsem se věnoval popisu implementace zabezpečení a praktické simulace poskytování některých služeb na současném hardware. Všechny odkazy a údaje použité v bakalářské práci byly v době tvorby aktuální a dostupné.

Práce popisuje řešení Technologického centra ORP Otrokovice. Ostatní eGON centra v ČR jsou samosprávné celky a realizují svá Technologická centra dle svých požadavků. Podmínkou je dodržení standardů stanovených Ministerstvem vnitra, které rozvoj eGovernmentu zaštiťuje.

RESUME

In this work I tried to describe the current development of eGovernment in Public Administration. As an employee of the Municipality of Otrokovice I am part of the team that deals with this topic. The management of the municipality share ideas with a vision of the Government of the Czech Republic "Effective public administration and public service friendly" - Smart Administration Strategy for the period 2007-2015 and is joined to a center in the district eGON Otrokovice.

In the theoretical part, I tried to imagine the project Technology Centre district Otrokovice global terms of services offered state and local governments. Bachelor thesis contains information, including upcoming projects, which were in the first half of 2010 published and will be directly related to the already completed projects. The practical part contains the results of analysis, which was necessary for the preparation of quality project Technology Centre of the Otrokovice district. Together with the analysis is presented selected technology, which will form the hardware infrastructure and a feasibility study that takes into account all aspects and their impact on the entire project. Due to the new infrastructure is explored virtulization and selection of available solutions on the market. In the end of the dissertation I worked on the description of the security implementation and practical simulations provide certain services on the current hardware. All references and data used in the thesis were at the time of creation of this bachelor´s work current and accessible.

This work describes a solution of the Technology Centre of Otrokovice district. Other eGON centers in the Czech Republic are local units and they realize their technological centers according to their requirements. The condition is compliance with the standards set by the Interior Ministry, which sponsored the development of eGovernment.

SEZNAM POUŽITÉ LITERATURY

[1.] NORTHCUTT, Stephen, et al. *Bezpečnost počítačových sítí : Kompletní průvodce návrhem, implementací a údržbou zabezpečené sítě*. Brno : Computer press, 2005. 592 s. ISBN 80-251-0697-7.

[2.] STREBE, Matthew; PERKINS, Charles. *Firewally a proxy-servery : Praktický průvodce*. Brno : Computer Press, a.s., 2003. 450 s. ISBN 80-7226-983-6.

[3.] PUŽMANOVÁ, Rita. *TCP/IP : v kostce*. České Budějovice : KOPP nakladatelství, 2009. 619 s. ISBN 978-80-7232-388-3.

[4.] DOSTÁLEK, Libor; KABELOVÁ, Alena. *Velký průvodce protokoly TCP/IP a systémem DNS*. Brno : Computer Press, a.s., 2008. 488 s. ISBN 978-80-251-2236-5.

[5.] RUEST, Danielle; RUEST, Nelson. *Virtualizace : Podrobný průvodce*. Brno : Computer Press, a.s., 2010. 408 s. ISBN 978-80-251-2676-9.

[6.] THOMAS, Thomas M. *Zabezpečení počítačových sítí : bez předchozích znalostí*. Brno : Computer Press, a.s., 2005. 338 s. ISBN 80-251-0417-6.

[7.] Data deduplication : Deduplikace dat - nový přístup k ukládání dat. *Connect*. 2009, 10, s. 10-11.

[8.] *Dell Česká republika* [online]. 2010 [cit. 2010-05-01]. Dostupné z WWW: < http://www.dell.cz/ >.

[9.] *EGONcentrum.cz* [online]. 2010 [cit. 2010-04-16]. Dostupné z WWW: < http://www.egoncentrum.cz/ >.

[10.] *HP - Česká republika* [online]. 2010 [cit. 2010-05-03]. Dostupné z WWW: < http://www8.hp.com/cz/cs/home.html >.

[11.] *IBM - Česká republika* [online]. 2010 [cit. 2010-04-19]. Dostupné z WWW: < http://www.ibm.com/cz/cs/ >.

[12.] *Intel Corporation* [online]. 2010 [cit. 2010-05-05]. Dostupné z WWW: < http:// www.intel.com/ >.

[13.] *Kernun - UTM Kernun Appliance* [online]. 2010 [cit. 2010-03-22]. Dostupné z WWW: < http://www.kernun.cz/ >.

[14.] *Ministerstvi vnitra České republiky* [online]. 2010 [cit. 2010-05-21]. Dostupné z WWW: < http://www.mvcr.cz/ >.

[15.] *VMware Virtualization Software for Desktops, Servers & Virtual Machines for a Private Cloud* [online]. 2010 [cit. 2010-05-10]. Dostupné z WWW: < http://www.vmware.com/ >.

[16.] *IBM Redbooks* [online]. 2009 [cit. 2010-05-02]. IBM BladeCenter Products and Technology. Dostupné z WWW: < http://www.redbooks.ibm.com/abstracts/sg247523.html >.

[17.] *IBM Redbooks* [online]. 2010 [cit. 2010-05-02]. IBM System Storage DS3000: Introduction and Implementation Guide. Dostupné z WWW: < http://www.redbooks.ibm.com/abstracts/sg247065.html?Open >.

[18.] *IBM System Storage* [online]. 2009 [cit. 2010-05-02]. IBM System Storage SAN Volume Controller. Dostupné z WWW: < http://www-03.ibm.com/systems/storage/software/virtualization/svc/index.html >.

[19.] *IBM System Storage* [online]. 2010 [cit. 2010-05-02]. IBM System Storage DS5020 Express. Dostupné z WWW: < http://www-03.ibm.com/systems/storage/disk/ds5020/index.html >.

[20.] *Ministerstvi vnitra České republiky* [online]. 15.04.2010 [cit. 2010-04-17]. Základní registry veřejné správy. Dostupné z WWW: < http://www.mvcr.cz/clanek/zakladni-registry-verejne-spravy.aspx >.

[21.] *Ministerstvi vnitra České republiky* [online]. 2010 [cit. 2010-04-17]. Systém základních registrů. Dostupné z WWW: <http://www.mvcr.cz/clanek/egon-symbol-egovernmentu-dokumenty-seznam-zakladnich-registru.aspx >.

[22.] *Portál odboru strukturálních fondů Ministerstva vnitra ČR* [online]. 4.10.2009, 13.5.2010 [cit. 2010-05-16]. Výzva 06 (výzva otevřena do 31. 5. 2010). Dostupné z WWW: < http://www.osf-mvcr.cz/vyzvy/2-1-zavadeni-ict-v-uzemni-verejne-sprave-rijen-2009 >.

[23.] *Svaz měst a obcí České republiky* [online]. 2007 [cit. 2010-02-12]. Strategie efektivní veřejné správy a přátelské veřejné služby. Dostupné z WWW: < http://www.smocr.cz/cinnost/informatika/strategie-efektivni-verejne-spravy-a-pratelske-verejne-sluzby.aspx >.

[24.] Česká republika. Zákon č. 111/2009 Sb. ze dne 26. března 2009 o základních registrech. In *Sbírka zákonů*. 2009, č. 33/2009, s. 1267.

[25.] Česká republika. Zákon č. 300/2008 Sb. ze dne 17. července 2008 o elektronických úkonech a autorizované konverzi dokumentů. In *Sbírka zákonů, Česká republika*. 2008, č. 98/2008, s. 4491.

[26.] Česká republika. Zákon č. 365/2000 Sb. ze dne 14. září 2000 o informačních systémech veřejné správy a o změně některých dalších zákonů. In *Sbírka zákonů*. 2000, č. 99/2000, s. 4666.

[27.] Česká republika. Zákon č. 499/2004 Sb. ze dne 30. června 2004 o archivnictví a spisové službě a o změně některých zákonů. In *Sbírka zákonů*. 2004, č. 173/2004, s. 9742.

[28.] *Bezpečnostní politika informačního systému veřejné správy*. Otrokovice (Česká republika) : Město Otrokovice, 2008. 32 s.

[29.] *Informační koncepce*. Otrokovice (Česká republika) : Město Otrokovice, 2008. 54 s.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

AC	***Označení střídavého proudu***
ACL	***Access control list***
BBWC	***Battery Backed Write Cache***
CDS	***Castle Defense System***
CMS	***Centrální místo služeb***
CRL	***Certificate revocation list***
CzP	***CzechPoint***
DHCP	***Dynamic Host Configuration Protocol***
DIMM	***Dual In-line Memory Module***
DMZ	***Demilitarizovaná zóna***
DNS	***Domain Name System***
DoS	***Denial-of-service attack***
DS	***Datová schránka***
DTM	***Digitální technická mapa***
ESS	***Elektronická spisová služba***
EU	***Evropská unie***
FC	***Fibre Channel***
FDE	***Full disk encryption***
GIS	***Geografický informační systém***
HSM	***Hierarchical storage management***
ICT	***Informační a komunikační technologie***
IDS	***Intrusion Detection System***
IOP	***Integrovaný operační program***
IOPS	***Input/Output Operations Per Second***

IP	***Internet Protocol***
IPS	***Intelligent Protection System***
IS	***Informační systém***
iSCSI	***Internet Small Computer System Interface***
ISDS	***Informační systém datových schránek***
ISVS	***Informační systém veřejné správy***
ISZR	***Informační systém základních registrů***
JRE	***Java Runtime Environment***
KIVS	***Komunikační infrastruktura veřejné správy***
KVM	***Zkratka pro klávesnici, video, myš***
LAN	***Local area network***
LTO4	***Linear Tape Open verze 4***
LUN	***Logical Unit Number***
MěÚ	***Městský úřad***
MV ČR	***Ministerstvo vnitra České republiky***
NAS	***Network Attached Storage***
NDA	***Národní digitální archiv***
NTP	***Network Time Protocol***
ORP	***Obec s rozšířenou působností***
PDF	***Portable Document Format***
QoS	***Quality of Service***
QPI	***Intel QuickPath Interconnect***
RAID	***Redundant Array of Inexpensive Disks***
ROB	***Registr obyvatel***
ROS	***Registr osob***

RPP	***Registr práv a povinností***
RUIAN	***Registr územní identifikace, adres a nemovitostí***
SAN	***Storage Area Network***
SAS	***Serial Attached SCSI***
SATA	***Serial ATA***
SCSI	***Small Computer System Interface***
SFP	***Small form-factor pluggable***
SIP	***Submision Information Package***
SLA	***Service level agreement***
SNMP	***Simple Network Management Protocol***
SSD	***Solid-state drive***
SSL, SpS	***Spisová služba***
STP	***Spanning Tree Protocol***
SVC	***SAN Volume Controller***
TC	***Technologické centrum***
TC C	***Centrální technologické centrum, část CMS zajišťující společné služby pro TC K a TC ORP***
TC K, KTC	***Technologické centrum na úrovni kraje***
TC ORP	***Technologické centrum na úrovni ORP***
TUN, TAP	***Virtuální síťová rozhraní***
UDP	***User Datagram Protocol***
UPS	***Uninterruptible Power Supply***
UTM	***Unified Threat Management***
VLAN	***Virtuální LAN***
VPN	***Virtual private network***

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

Příloha 1 : DOTAZNÍK

pro analýzu požadavků na zajištění služeb TC ORP Otrokovice v obcích II. a I. stupně

Obecné dotazy		
Obec:		
Pověřená osoba (jméno, kontakt):		
Jste obec jen s matrikou?	☐ ANO ☐ NE	
Jste obec s matrikou a stavebním úřadem?	☐ ANO ☐ NE	
Jste obec základního typu?	☐ ANO ☐ NE	
Otázka	**Odpověď**	**Poznámka**
WAN		
1. Jakým způsobem jste připojeni do internetu?		
2. Jakou rychlostí jste připojeni?		
3. Kdo je poskytovatelem připojení?		
4. Máte vybudováno záložní připojení k internetu? Pokud ANO, jaký typ?	☐ ANO ☐ NE	
5. Používáte firewall? Jaký typ?		
6. Používáte router? Jaký typ?		
7. Máte internetové stránky obce?		
8. U koho stránky hostujete?		
LAN		
9. Máte na Vašem úřadě vybudovanou LAN síť? (vzájemné propojení PC)	☐ ANO ☐ NE	

10. Kolik uživatelů PC máte na Vašem úřadě?		
11. Kolik PC máte na Vašem úřadu?		
12. Kolik PC je připojeno k internetu?		
13. Kolik budov má Váš úřad?		
14. Jsou tyto budovy spolu propojeny? Pokud ANO, tak jakou rychlostí?	☐ ANO ☐ NE	
Email		
15. Máte na Vašem úřadu zprovozněnou službu elektronické pošty?	☐ ANO ☐ NE	
16. Pokud ANO, jaký je celkový počet emailových schránek?		
Spisová služba		
17. Odhadněte počet došlých dokumentů denně		
18. Provozujete elektronickou spisovou službu (eSpSI)?	☐ ANO ☐ NE	
19. Od které firmy v současné době používáte eSpSI?		
20. Počet současných uživatelů eSpSI?		
21. Plánujete pořízení eSpSI v rámci projektu TC ORP s využitím dotace?	☐ ANO ☐ NE	
22. Plánujete pořízení eSpSI samostatně mimo projekt TC ORP?	☐ ANO ☐ NE	
23. Uveďte počet uživatelů eSpSI (včetně plánovaných):		
24. Plánujete pořízení nové elektronické spisové služby pro školy, případně jiné příspěvkové organizace obce?	☐ ANO ☐ NE	
Pokud ANO, uveďte název		

organizace, počet uživatelů eSpSl a rychlost připojení organizace k internetu.		
25. Plánujete rozšíření stávající spisové služby obce pro školy, případně jiné příspěvkové organizace obce?	☐ ANO ☐ NE	
26. Budete mít zájem o metodickou a systémovou podporu pro sebe a tyto organizace?	☐ ANO ☐ NE	
Technologické centrum		
27. Jste informováni o plánovaných službách poskytovaných technologickými centry?	☐ ANO ☐ NE	
28. Máte zájem o službu TC		
a) zajištění negarantovaného úložiště dokumentů a otevřených spisů	☐ ANO ☐ NE	
b) provoz spisovny	☐ ANO ☐ NE	
c) zálohování dat	☐ ANO ☐ NE	
d) služba konverze dat do PDF	☐ ANO ☐ NE	
e) WEBhosting (umístění internetové prezentace obce)	☐ ANO ☐ NE	
f) redakční systém pro publikování na internetu	☐ ANO ☐ NE	
g) školský systém (el.třídní kniha, školská matrika, el. žák.kniha)	☐ ANO ☐ NE	
h) elektronické zadávání zakázek	☐ ANO ☐ NE	
i) kopie centrálních registrů	☐ ANO ☐ NE	
j) Uveďte další požadované služby:		

k) Co očekáváte v rámci elektronizace veřejné správy od TC ORP Otrokovice?		
Digitální mapa veřejné správy		
29. Máte v současné době pro území obce zpracovánu a používáte Digitální technickou mapu?	☐ ANO ☐ NE	
30. Kdo je (jsou) váš(i) hlavní dodavatel(é) služeb v oblasti GIS?		
HW + SW		
31. Jaké je průměrné stáří Vaší výpočetní techniky?		
32. Jaké operační systémy používáte? (Windows, Linux)		
33. Jaké kancelářské systémy používáte? (MS Office, OpenOffice …)		
34. Zálohujete data ? Jakým způsobem?	☐ ANO ☐ NE	
35. Kolik pracovníků využívá kvalifikovaný certifikát?		
36. Kontakty na zodpovědnou osobu za správu IT na Vašem úřadu.		

Příloha 2 : Vyjádření zájmu obce

……

(název obce)

1. Obec **má zájem** o přístup k elektronické spisové službě splňující požadavky dané zákonem č. 499/2004 Sb., o spisové službě a archivnictví, ve znění pozdějších předpisů pro svoji potřebu a potřebu jimi zřízených organizací pořizované v rámci výzvy č. 6 IOP prioritní osa 2.

2. Obec **disponuje – nedisponuje***) vlastní elektronickou spisovou službou.

*) *nehodící se škrtne*

3. Obec **má – nemá***) zájem

a) o elektronickou spisovou službu v hostovaném režimu provozovanou na TC ORP*)

b) o nákup licence plné verze elektronické spisové služby provozované na vlastní technologii obce*)

*) *nehodící se škrtne*

V případě, že obec požaduje nákup licence plné verze elektronické spisové služby provozované na vlastní technologii obce, uvede typ provozovaného informačního systému, se kterým má být elektronická spisová služba provázána a kompatibilní.

Typ provozovaného informačního systému, se kterým má být elektronická spisová služba provázána a kompatibilní:

V …….. ……

Dne Starosta obce

Příloha 3 : Vyjádření zájmu příspěvkové organizace

……..……

(název příspěvkové organizace)

1. Příspěvková organizace **má zájem** o přístup k elektronické spisové službě splňující požadavky dané zákonem č. 499/2004 Sb., o spisové službě a archivnictví, ve znění pozdějších předpisů pro svoji potřebu v rámci výzvy č. 6 IOP prioritní osa 2.

2. Příspěvková organizace **disponuje – nedisponuje***) vlastní elektronickou spisovou službou.

**) nehodící se škrtne*

3. Příspěvková organizace **má - nemá***) zájem

o elektronickou spisovou službu v hostovaném režimu provozovanou na Technologickém centru ORP Otrokovice

**) nehodící se škrtne*

V …….. ……

Dne Ředitel příspěvkové organizace