3 VÝCHOZÍ STAV - ANALÝZA STAVU ICT

Klíčovou částí zpracování Strategie rozvoje a bezpečnosti ICT je analytické šetření a obeznámení se současným stavem informatizace v podmínkách Městského úřadu Králíky a identifikace současných a budoucích potřeb městského úřadu, zainteresovaných osob a subjektů.

Problematiku informačních a komunikačních technologií (ICT) zabezpečuje oddělení informatiky, které je organizačně začleněno do Odboru organizačního a správního. Informatika městského úřadu je orientována především na podporu chodu městského úřadu. Informatika je na MěÚ Králíky průřezovou činností, poskytující podporu většině procesů. Oddělení informatiky nemá vlastní rozpočet, položky jsou rozpočtovány v rámci kapitoly Odboru organizačního a správního.

Z úrovně města jako veřejnoprávní korporace není informatika do území řízena ani koordinována. Všechny subjekty budují a provozují vlastní ICT řešení pro potřeby výkonu agend a chodu organizace. Organizace mají v organizační struktuře začleněny útvary, odpovědné za provoz a rozvoj ICT a částečně nebo plně využívají outsourcing externími dodavateli. Spolupráce a synchronizace napříč organizacemi je minimální.

3.1 HW Infrastruktura MěÚ Králíky

Zhodnocení stavu fyzických serverů a úložišť:

- Servery i primární úložiště jsou již technicky a morálně zastaralé
- Vzhledem ke stáří se s časem zvyšuje pravděpodobnost poruchy
- Nejsou již pod supportem výrobce, tudíž jakákoliv porucha ponese neúměrně vysoké náklady na opravu, případně nebude již oprava možná

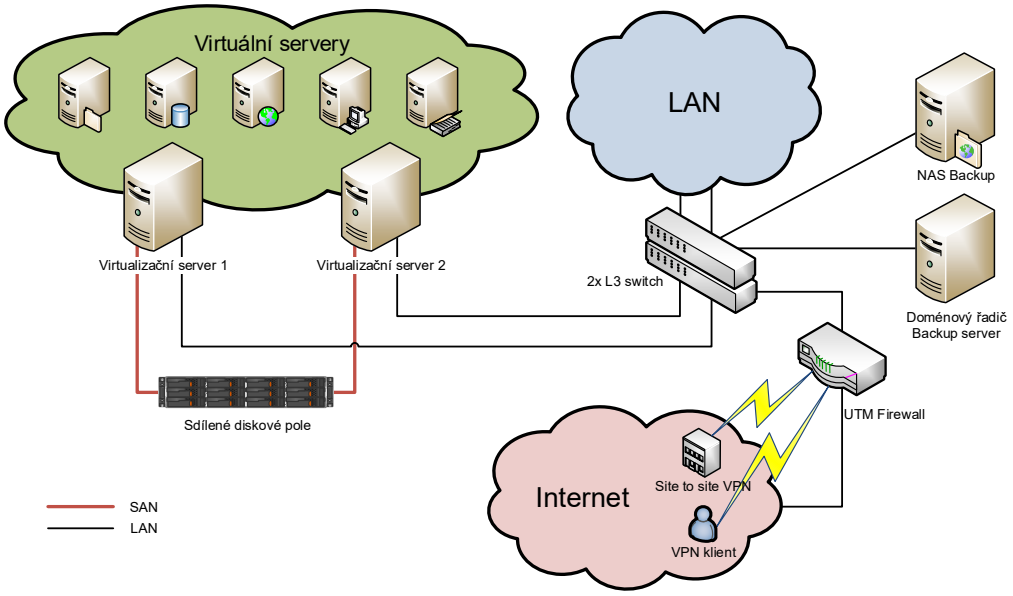
3.1.1 HW zařízení

V současnosti MěÚ Králíky provozuje v racku následující HW zařízení:

- Server Dell PowerEdge R510 (1 x) – role DC + Backup Server
- Server Dell PowerEdge R710 (2 x) – hostitelé virtualizace
- Diskové pole Dell EMC AX4-5f – Primární úložiště pro virtuální servery
- NAS server QNAP TS-809U-RP – primární úložiště pro zálohy
- Synology DS1815+ DiskStation – sekundární úložiště pro zálohy
- Přepínač CISCO Catalyst 2960S-24TS-L (2 x)
- KVM přepínač ATEN CL-1008M
- Fortigate 100D – UTM Firewall
- UPS Dell 5600R HV – UPS Pro zálohování napájení

3.1.2 Fyzická topologie serverů a úložišť

V TC jsou v provozu 3 fyzické servery, které slouží pro běh dalších aplikací. Tyto servery jsou připojeny k úložištím potřebným pro běh virtuálních serverů a zálohování.



3.1.3 Fyzické servery

Doménový řadič a backup server

- Zajišťuje základní síťové služby, ověřování uživatelů apod., zároveň slouží jako server pro zajišťování záloh dat

SRV-DC1 / Dell PowerEdge R510 – doménový řadič a backup Server

- Windows Server 2012R2
- Active Directory Domain Services
- DHCP Server
- DNS Server
- Altaro VM Backup

Hostitelé virtualizace

- Zajišťují chod virtuálních serverů a umožňují tak efektivní využití fyzického HW, při zajištění spolehlivosti a redundance

SRV-HYPERV1 / Dell PowerEdge R710 – virtualizační server

- Windows Server 2012R2 Datacenter Edition
- Hyper-V 2012R2

SRV-HYPERV2 / Dell PowerEdge R710 – virtualizační server

- Windows Server 2012R2 Datacenter Edition
- Hyper-V 2012R2

3.1.4 Virtuální servery

Souborový server

- Zajišťuje základní síťové služby, ověřování uživatelů apod., zároveň slouží jako úložiště dokumentů úřadu

SRV-FILE – file server, print server, doménový řadič

- Windows Server 2008R2
- File Services
- Active Directory Domain Services
- Active Directory Certificate Services
- DHCP Server
- DNS Server
- Internet Information Services
- Print and Document Services

Aplikační server

- Slouží pro zajištění chodu webových aplikací, skenovací linku apod.

SRV-APP1 – aplikační server

- Windows Server 2008R2
- File Services
- Internet Information Services
- Vema
- ASPI
- Helios Fenix
- Portál úředníka (Microsoft Sharepoint Foundation 2010)
- Elisa – Spisová služba
- ABBYY Recognition Server
- Firebird
- FileZilla Sever
- ScanFlow
- další aplikace

Databázový server

- Slouží pro zajištění provozu databází konsolidovaných na jednom serveru pro podporu funkčnosti jednotlivých aplikaci a to jak pro výkon veřejné správy, tak i pro chod IT infrastruktury.

SRV-SQL – databázový server

- Windows Server 2008R2
- MS SQL 2008 R2
- Databáze aplikací běžící v síti úřadu
    - Elisa
    - Portál úředníka
    - Fenix
    - Microsoft Sharepoint
    - System CenterEssentials

- Stavební úřad
- A další.

Poštovní server

- Slouží pro zajištění poštovních služeb.

SRV-EXCH – poštovní server

- Windows Server 2008R2
- Eset Mail Security – Antispamová Ochrana
- MS Exchange 2010 – schránky všech uživatelů úřadu

Management server

- Slouží pro provoz SW určeného pro správu IT infrastruktury.

SRV-MGMT – management server

- Windows Server 2008R2
- MS System Center Essentials 2010
- Internet Information Services
- Network Policy and Access Services
- Windows Server Update Service
- ESET Endpoint Security management console

Terminálový server

- Slouží pro připojení vzdálených uživatelů terminálovými službami.

SRV-TS - terminálový server

- Windows Server 2012R2
- Helios Fenix pro vzdálené uživatele

3.1.5 Úložiště

Primární diskové úložiště

Diskové pole Dell EMC AX4-5f

- Primární úložiště pro virtuální servery
- Připojeno pomocí k virtualizačním serverům pomocí technologii FC 4 Gb/s
- Osazeno 12 ks disků (7x 400 GB SAS, 5x 2 TB SATA)

Úložiště pro primární zálohy

NAS server QNAP TS-809U-RP

- iSCSI diskové pole
- Jsou prováděny zálohy dat pomocí zálohovacího SW
- Připojeno do LAN pomocí metalických propojů 2x 1 Gbit
- Osazeno 8x 4 TB disky

Úložiště pro sekundární (offsite) zálohy

NAS Synology DS1815+ DiskStation (8 bay)

- iSCSI diskové pole
- Jsou prováděny zálohy dat pomocí zálohovacího SW

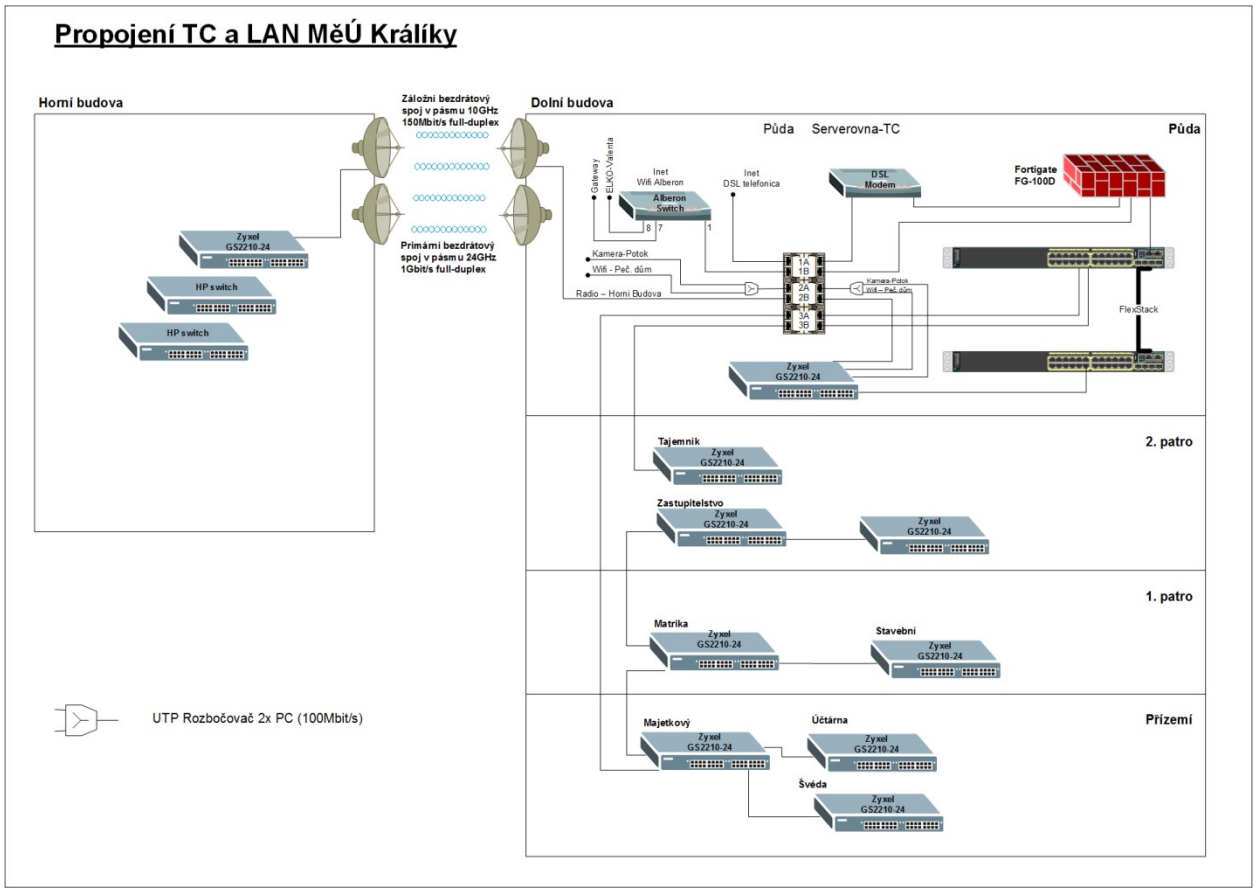
- Připojeno do LAN pomocí metalického připojení 1x 1 Gbit
- Osazeno 8x 2 TB disky

3.1.6 Fyzická topologie LAN

LAN TC se nachází v serverovně umístěné v dolní budově MěÚ Králíky. LAN TC je tvořena Firewallem Fortigate FG-100D s UTM (Unified Thread Management Gateway) funkcionalitami (formou 5-leté subscription) umístěném na perimetru sítě zajišťující směrování provozu do internetu (přepínání provozu mezi primární a záložní linkou), Demilitarizovanou zónu a bezpečnostní funkcionality v podobě Next-generation firewallu a VPN koncentrátoru (pro připojení okolních obcí a outsourcingových firem spravujících informační systémy). Zároveň zde jsou umístěné PE routery obou providerů.

LAN TC tvořena dvojicí switchů Catalyst 2960S-24TS-L propojených do stohu pomocí FlexStack sběrnice do jednoho logického zařízení. Tyto switche zajišťují Inter-Vlan routing provozu mezi jednotlivými serverovými a uživatelskými Vlanami.

Tyto 2 switche primárně zajišťují core vrstvu, distribuční vrstvu a připojení serverových systémů TC, dále pak připojení do vzdálených lokalit skrze Zyxel GS2210-24 switch. (Horní budovy, pečovatelského domu a kamery snímající místa důležitá z pohledu krizového řízení).



3.1.7 LAN CORE + distribution + server access

Z důvodů vysoké dostupnosti je většina systémů TC připojena „multihome" - redundantně na oba serverové switche (pro zajištění konektivity v případě výpadku jednoho ze switchů). Konfigurace většiny portů na switchích je realizována zrcadlově, kdy nastavení portu Gi1/0/1 je totožné s nastavením portu Gi2/0/1 (kdy první číslice udává pozici switche v rámci stacku a poslední číslo určuje port switche). Systémy, které neumožňují multihoming, jsou primárně připojeny na první switch (Gi1/0/x) – v případě poruchy prvního switche pak musejí být administrátorem přepojeny

do zrcadlového portu na druhém switchi - port Gi2/0/x) - jedná se například o router ISR G2.

Systémy, které umožňují ether-channel (trunking) ať již statický popř. dynamicky vyjednávaný pomocí LACP protokolu, jsou připojeny na porty v ether-channel módu a umožňují dynamické rozkládání zátěže mezi síťovými kartami a switchi.

Klíčové serverové systémy jsou připojeny rychlostí 1 Gbit/s a full duplexem (vypnuto autonegotiation), toto nastavení musí být pro správnou funkčnost i na straně serverů. Ostatní porty mají nastavenu rychlost a duplex na automatické vyjednávání.

Cisco FlexStack - stohovací hot-swap technologie. Všechny přepínače ve stohu působí jako jeden switch. Cisco FlexStack poskytuje jednotnou konfiguraci, a jednu IP adresu pro správu celého stohu přepínačů. Výhody stohování jsou nižší celkové náklady na vlastnictví (TCO) díky zjednodušené správě a vyšší dostupnosti. Cisco FlexStack podporuje cross-stack funkcionality včetně EtherChannel, SPAN a FlexLink technologie. FlexStack modul může být přidán do jakéhokoli Cisco Catalyst 2960-S přepínače s LAN Base softwarem.

3.1.8 User access

Přístup pro uživatele zajišťují přístupové L2 přepínače Zyxel GS2210-24. Jedná se 24 portové gigabitové přepínače s podporou managementu a 4x Combo rozhraní RJ45 / SFP.

Aktuálně jsou přepínače propojeny v některých případech (horní budova) do kaskády z důvodu nedostatku páteřních propojů mezi TC a místem instalace přepínačů.

3.1.9 Propojení budov

MěÚ sídlí ve dvou budovách Velké náměstí čp. 5 a Karla Čapka čp. 316). Aktuálně mezi budovami není pevné datové propojení. Propojení budov je realizováno dvojicí bezdrátových spojů.

Primární bezdrátový spoj v pásmu 24 GHz s přenosovou rychlostí 1 Gb/s duplexně.

Záložní bezdrátový spoj v pásmu 10 GHz s přenosovou rychlostí 180 Mbit/s duplexně sloužící jako záloha v případě výpadku primárního spoje.

3.1.10 Segmentace LAN do VLAN

LAN technologického centra je rozdělena do VLAN, pro oddělení provozu a zvýšení bezpečnosti. Směrování provozu mezi L3 Vlanami zajišťuje dvojice switchů s lan-base routing SDM šablonou, která aktivuje základní L3 routing funkcionality (statický routing, směrování mezi Vlanami). Tyto switche jsou propojeny pomocí FlexStack stohovací sběrnice, zajišťující vysokou dostupnost směrovacích a dalších funkcionalit, předáváním MASTER role mezi oběma switchi.

Jednotlivé systémy TC jsou pak připojovány do portů switche náležejících do příslušné VLANy popř. jsou připojovány do TRUNK portů agregujících provoz všech VLAN. Pro oddělení provozu jednotlivých VLAN je použito IEEE802.1Q encapsulace. Nativní VLAN v rámci všech trunků je nastavena na VLAN999 (všechny provozní VLANy v trunku jsou tagované).

3.1.11 Portály, služby přístupné z internetu

Překlad adres NAT/PAT

LAN TC využívá privátní adresace dle RFC1918, pro přístup do sítě internet musí být tyto adresy přeloženy na veřejné směrované v internetové síti, k tomuto překladu adres je využívána technika NAT/PAT (Network Address Translation/Port Address Translation).

Na firewallu jsou definovány subnety, jež mají povolen překlad adres do internetu, subnety které nejsou uvedeny, nemají přístup do internetu. Statické veřejné adresy má TC přiděleno pouze od poskytovatele primární linky.

Primárně je veškerý provoz z těchto sítí překládán pomocí overload NATu na adresu rozhraní do sítě jednotlivých poskytovatelů ISP1 a ISP2. V případě provozu přes primární linku ISP1 se jedná o IP adresu odchozího provozu, v případě provozu přes záložní linku ISP2 je překlad na adresu 10.0.0.1 - zde se jedná opět o privátní adresu dle RFC1918, další překlad je proveden ADSL routeru poskytovatele, jehož veřejná adresa není fixní (poskytována DHCP serverem).

MěÚ provozuje v rámci TC systémy a portály, které musí být přístupné z internetu. Tyto systémy a portály jsou přeloženy pomocí statického NAT/PAT záznamu na veřejnou adresu – Překlad adres a řízení přístupu FW pravidly zajišťuje Firewall Fortigate FG-100D.

3.2 SW infrastruktura

Používané SW prostředky lze rozdělit do tří hlavních kategorií:

- operační systémy a základní podpůrný SW,
- informační systémy a
- kancelářské aplikace a ostatní SW.

3.2.1 Serverové operační systémy

- Provozovány jsou operační systémy Windows Server 2008R2 a 2012R2.
- Z hlediska spolehlivosti a náročnosti na údržbu a řešení problémů je doporučeno sjednocení verzí serverových OS.
- Konec rozšířené podpory pro OS Windows Server 2008 R2 byl stanoven na 14.1.2020, základní podpora již byla ukončena.
- Konec základní podpory pro OS Windows Server 20012 R2 byl stanoven na 9.10.2018, rozšířená podpora pro OS Windows Server 2012 R2 poté končí 10.10.2023.
- V rámci rozšířené podpory jsou vydávány pouze bezpečnostní aktualizace.
- Je doporučena migrace na poslední verzi serverového OS v současné době Windows Server 2016, bude tak zajištěna spolehlivost, bezpečnost provozovaných aplikací a úřad bude připraven na provoz všech moderních aplikací.

3.2.2 Poštovní systém

- Provozován je poštovní systém Exchange Server 2010.
- Provozováno je cca 70 emailových schránek
- Konec rozšířené podpory pro Exchange Server 2010 SP3 byl stanoven na 14.1.2020, základní podpora již byla ukončena.
- V rámci rozšířené podpory jsou vydávány pouze bezpečnostní aktualizace.
- Je doporučena migrace na poslední verzi poštovního systému v současné době je to Exchange Server 2016, bude tak zajištěna jeho spolehlivost a bezpečnost a kompatibilita se stávajícími aplikacemi.

3.2.3 Databázový systém

- Provozován je poštovní systém Microsoft SQL Server 2008 R2.
- Provozováno je přes 30 databází různých informačních systémů.
- Konec rozšířené podpory pro Exchange Server 2008 R2 byl stanoven na 7.9.2019, základní podpora již byla ukončena 8.7.2014.
- Je doporučena migrace na poslední verzi databázového systému, v současné době je to Microsoft SQL Server 2016, bude tak zajištěna jeho spolehlivost a bezpečnost a kompatibilita se stávajícími aplikacemi.

3.2.4 Portál úředníka

- Provozován je na platformě Microsoft SharePoint Foundation 2010 Service Pack 2.
- konec rozšířené podpory pro SharePoint Foundation 2010 byl stanoven na 13/10/2020, základní podpora již byla ukončena 13/10/2015.
- Je doporučena migrace na poslední verzi platformy v současné době je to Microsoft Sharepoint Server 2016, bude tak zajištěna jeho spolehlivost a bezpečnost a kompatibilita se stávajícími aplikacemi úřadu.

3.2.5 Aplikace pro zajištění výkonu veřejné správy

3.2.5.1 Spisová služba ELISA

Na Městském úřadě v Králíkách je provozována aplikace Spisové služby od roku 2003. Dodavatelem je společnost CNS a.s., Mělník.

Program „Spisová služba ELISA" slouží ke sledování oběhu dokumentů v organizaci od jejich příchodu do systému (evidenční karta), přes jejich zpracování (historie dokumentu, lhůty vyřízení, zařazení do spisu) až po jejich archivaci a skartaci.

Program „Spisová služba" (dále SSL) plně respektuje Národní standard pro elektronické systémy spisové služby a platné legislativní. Systém řeší otázky ochrany dat před jejich zneužitím, stejně jako komplexní ochranu informačního systému před poškozením a ztrátou dat.

Díky využití vlastností podporovaných serverových platforem umožňuje SSL poskytnout uživateli rozsáhlé služby na úrovni datových komunikací. Součástí nabídky jsou i SW produkty, které jsou schopny zabezpečit datovou komunikaci mezi uživatelem a dalšími informačními systémy, a to na základě dohodnutých datových rozhraní (např. napojení na Informační systém Datových schránek).

Za základ řešení produktu SSL byla použita architektura tenký nebo webový Klient/Server s uplatněním podpůrných vývojových nástrojů.

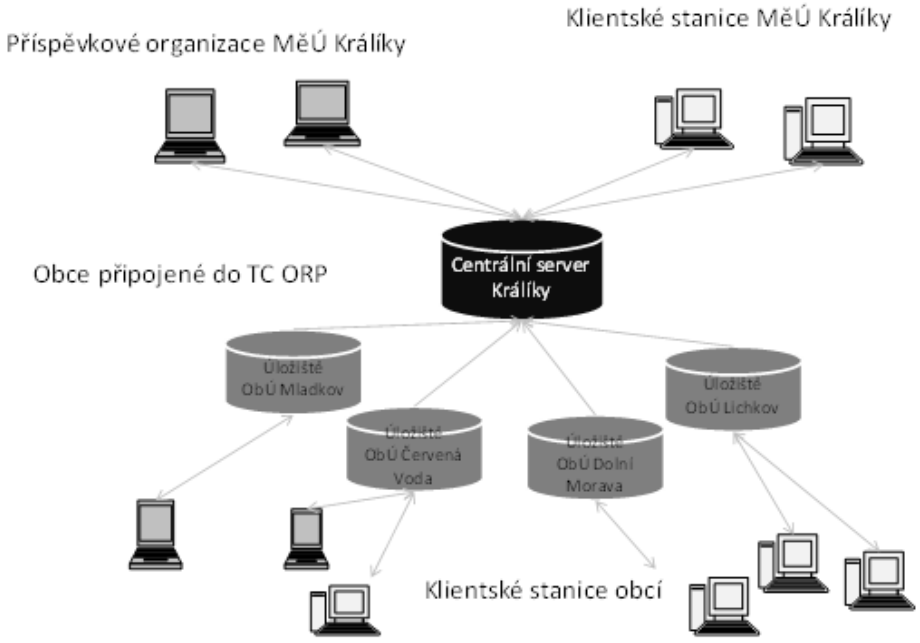
Při návrhu produktu SSL bylo prioritně uplatněno uživatelské hledisko, takže výsledný produkt může sloužit jako nástroj optimalizace, objektivity a kvality veškerých činností vykonávaných jednotlivými složkami zadavatele.

Technologické centrum ORP

Základním principem řešení TC ORP je, že všechny instalace na jednotlivých obcích jsou centralizované a závislé na „on-line" internetové konektivitě k TC ORP. Jedná se tedy o hostovanou spisovou službu provozovanou na TC.

Technologické centrum ORP pro obce/organizace poskytuje technické zázemí (vč. zálohování databází) a metodickou podporu.

Nad všemi databázemi napříč je pak vystavěn modul „Centrální databáze Spisové služby", který zajišťuje funkci negarantovaného úložiště dat.



Centrální úložiště = SQL server obsahuje databáze jednotlivých obcí se systémem zálohování.

Úložiště obecních úřadů = SQL server s databází konkrétní obce, kde se vede vlastní číselná řada čísel jednacích a evidenčních, nastavení aplikace SSL obce, jednotlivé dokumenty, spisy.

Na MěÚ Králíky jsou implementována tato rozhraní:

- Datové schránky
- Základní registry
- Interface na Registr živnostenského podnikání
- Komunikační rozhraní CzechPOINT (Autorizovaná konverze)

3.2.5.2 Aplikace GEOVAP - GIS

Aktuálně se na MěÚ Králíky využívají celkem 4 nástroje pro editaci a prohlížení mapových podkladů

1) Aplikace „KN informace". Tato aplikace slouží pouze pro prohlížení dat Katastru nemovitostí České republiky, který zpracovává rozsáhlé standardizované datové sady popisových i grafických informací v rámci ORP Králíky. Data katastru nemovitostí obsahují údaje o jednotlivých vlastnících včetně rodných čísel nemovitostí a katastrálních území, druhy pozemků, čísla a výměry parcel, údaje o způsobu ochrany a využití nemovitostí a údaje o právních vztazích a dalších právech k nemovitostem. Digitální data katastru nemovitostí se přebírají bezplatně na základě žádosti realizované odborem ÚPaSÚ cca 4x ročně ve zveřejněném výměnném formátu dat. Tato aplikace musí být samostatně nainstalována na každém PC. Data jsou uložena na serveru v technologickém centru MěÚ Králíky (tato data nelze ze zákona zveřejňovat na Internetu).
2) GeoStore® V6 profesionální GIS/CAD software v sobě spojuje nejdůležitější funkce pro tvorbu, aktualizaci a správu geografických dat s pokročilými funkcemi GIS. Může sloužit jako výkonný grafický editor s plnou škálou editačních funkcí obvyklých u CAD nástrojů nebo jako pokročilý desktopový GIS systém. Zakoupené licence jsou pouze ve verzi Viewer, tj. slouží pouze k prohlížení existujících dat.
3) ArcGIS for Desktop profesionální GIS/CAD software v sobě spojuje nejdůležitější funkce pro tvorbu, aktualizaci a správu geografických dat s pokročilými funkcemi GIS, může pracovat

s více než stovkou vektorových, rastrových nebo textových formátů. Lze připojit GIS i CAD data, soubory z přístrojů GPS, tabulky či data z databázových systémů. Lze využívat i data publikovaná na internetu – ve formátech OGC, WMS i jako služby ArcGIS serveru, které nabízí více možností pro zpracování a vizualizaci. Nutný SW pro územní plánování.

4) Veřejně dostupné a bezplatné mapy, služby a geografická data na Internetu. Zveřejněná především na webu Pardubického kraje a ČÚZaK.

3.2.5.3 Aplikace Vema

V současné chvíli **Město Králíky** využívá aplikace Vema:

- Mzdy
- Elektronické odesílání ELDP (ELD)
- Registr nemocenského pojištění (RNP)
- Evidence docházky (DCH)

Mzdy

Aplikace Mzdy nabízí možnost komplexního výpočtu platů s výstupy na zdravotní pojišťovny, na správu sociálního zabezpečení, do peněžních ústavů atd.:

- kompletní zpracování všech druhů mezd, řešení více souběžných pracovněprávních vztahů;
- maximální pružnost při počátečním nastavení;
- varianty odměňování pro veřejné služby a správu až po automatické platové postupy;
- opravy do minulosti s automatickým přepočtem až do hloubky 12 měsíců;
- definice vlastních kalendářů, neomezené množství rozvrhů pracovní doby;
- automatické zpracování dovolené a jejího krácení;
- roční zúčtování daně;
- srážky ze mzdy (v zákonném pořadí);
- hromadné provádění změn (např. zadání celozávodní dovolené, příplatek určité skupině zaměstnanců apod.);
- zadávání pracovních neschopností, vyhodnocení navazujících nemocí, vyhodnocení intervalu s náhradou mzdy, možnost proplacení náhrady i za karenční dobu, příloha k žádosti o dávku;
- komplexní řešení problematiky pracovních úrazů;
- kontrola kolize intervalů zadaných nepřítomností (dovolená, pracovní neschopnost,…);
- zadávání mateřské dovolené a automatický přechod na rodičovskou dovolenou;
- výpočet průměrných výdělků pro pracovněprávní účely podle platných právních předpisů, výpočet odvodů zdravotního a sociálního pojištění;
- ošetření minimální mzdy (automatické doplatky do minimální a zaručené mzdy).

Aplikace Mzdy má nejrůznější druhy vazeb na své okolí (na účetnictví, rozbory, na statistiku, nákladová hlediska, Trexima, převodní příkazy, příspěvky do penzijních fondů, podklady pro kontrolu daní, pojistného ad.). Vytváří také závazné výstupy pro státní správu a jiné „veřejné" organizace (elektronické podání ELDP, přihlášky a odhlášky nemocenského pojištění, komunikace se zdravotními pojišťovnami). Jedná se o samostatné aplikace, které jsou v cenové kalkulaci vyčísleny zvlášť (ELD, RNP a KZP). Aplikace Mzdy má pro Informační systém o platech zapracováno automatické vytváření souboru ve formátu XML pro odesílání předkladateli.

Docházka

Aplikace Docházka primárně slouží ke kontrole a vyhodnocení docházky zaměstnanců, neméně důležité je ale zpracování docházkových dat do formy podkladů pro zpracování mezd, které zásadním způsobem zefektivňuje práci mzdové účtárny:

- zpracování všech forem pevné i pružné pracovní doby, s vlastní definicí rozvrhů;
- paralelní zpracování neomezeného počtu skupin zaměstnanců s různými rozvrhy a parametry výpočtu;
- zaokrouhlení a korekce nasnímaných průchodů a složek pracovní doby dle individuálního požadavku zákazníka;
- evidence nadpracovaných hodin a zadávání přesčasů;
- práci s přestávkami na jídlo a oddech včetně jejich automatického generování;
- zadávání a generování příplatků k odpracované době;
- možnost evidence docházky pomocí intervalů;
- rozdělení odpracované doby, přerušení a příplatků na pracoviště, zakázky, účetní činnosti;
- definici a údržbu seznamů identifikačních karet včetně jejich přiřazení k jednotlivým zaměstnancům a seznamů karet pro návštěvy.

Pohled na docházková data je zprostředkován prostřednictvím webové docházkové karty. Je určena pro práci docházkových vedoucích (tj. vedoucí resp. pracovníci pověření správou a kontrolou docházky dané množiny zaměstnanců), případně pro pohled řadových zaměstnanců.

Mezi její výhody patří jednoduchost zobrazení dat a intuitivní ovládání. Je tvořena několika záložkami se seznamem podřízených, jejich měsíčními a denními výkazy, včetně evidence průchodů.

3.2.5.4 Webové stránky www.kraliky.eu

Popis současného stavu

- Design a struktura: odpovídá době, ve které byly stránky vytvořeny, časem však došlo k přidání dalších prvků, které ne vždy dobře zapadly.
- Technologie: PHP v 5.2, databáze MySQL 5.5.55, Windows-1250.
- Zabezpečení: riziko zranitelnosti pomocí SQL injection, případně phishing nebo jiné ohrožení pomocí vnořených rámců z jiných webů.
- Redakční systém: byl součástí dodávky webových stránek od společnosti SecurityNet.cz s.r.o.

Umožňuje:

- administraci uživatelů (přidělování oprávnění pro jednotlivé sekce);
- přidávání a odebírání sekcí (stránek) a to včetně zařazení do struktury webu);
- úpravu obsahu těchto sekcí, nastavení termínu zobrazení (od-do), obsahuje wysiwyg editor s možností vkládání obvyklých prvků a případně přepnutí do html režimu;
- připojení souborů ke stažení (nebo obrázků) ke každé jednotlivé sekci;
- tvorbu jednoduchých formulářů a anket (bez ukládání dat v databázi).

Plánovaný stav (rozpracovaná verze na www.kraliky.eu/redesign)

3.2.6 Kancelářské aplikace a ostatní SW

Kancelářský SW

- je využíván MS Office a to v mnoha verzích (XP, 2003, 2007, 2013 příp. 2016). Ve specifických případech jsou využívány další aplikace MS Office, konkrétně MS Visio a MS Project.
- Verze XP – 2007 již nejsou kompatibilní s navrhovanými SW technologiemi, proto pro zajištění funkčnosti je třeba zajisti jejich migraci na novější verzi, v současné době je to Microsoft Office

2016.

- Jakákoliv podpora produktů Microsoft Office XP, 2003 již byla ukončena, podpora pro Microsoft Office 2007 SP 3 konči 10.10.2017.

Ostatní SW

Jako další SW jsou využívány:

- Adobe Reader,
- ARCGis,
- Adobe InDesign,
- Corel Draw,
- Wtran32 (slovník).
- Eset Endpoint Antivirus
- 602 Form Filler
- A další …

3.3 Analýza současného stavu nastavení bezpečnosti ICT

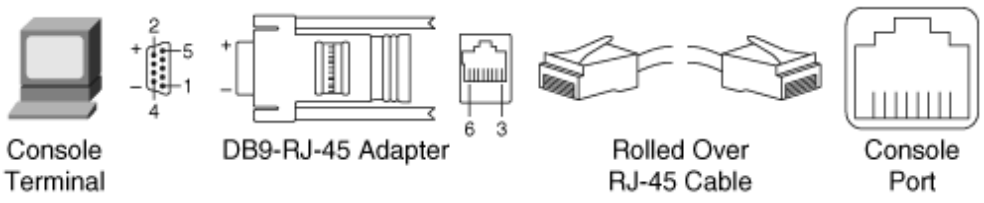
Vzdálená správa síťových zařízení

SSH - Secure Shell - vzdálenou správu síťových zařízení lze provádět pomocí SSH (Secure Shellu) např. pomocí open-source ssh a telnet klienta PUTTY. Alternativně lze použít embeded WWW konfigurátory, které umožňují pouze nejběžnější nastavení, a neposkytují všechny konfigurační možnosti operačního systému IOS. - Z tohoto důvodu jsou WWW konfigurátory deaktivovány.

Console - konzolový port představuje OOB sériové rozhraní pro počáteční konfiguraci zařízení, popř. konfigurační rozhraní v případě problémů s In-band management (konfigurace pomocí rollover kabelu a klientů PUTTY, Hyperterminal).

Nastavení sériového rozhraní PC:

- Speed: 9600 bps
- Data bits: 8
- Parity: none
- Stop bit: 1
- Flow control: none

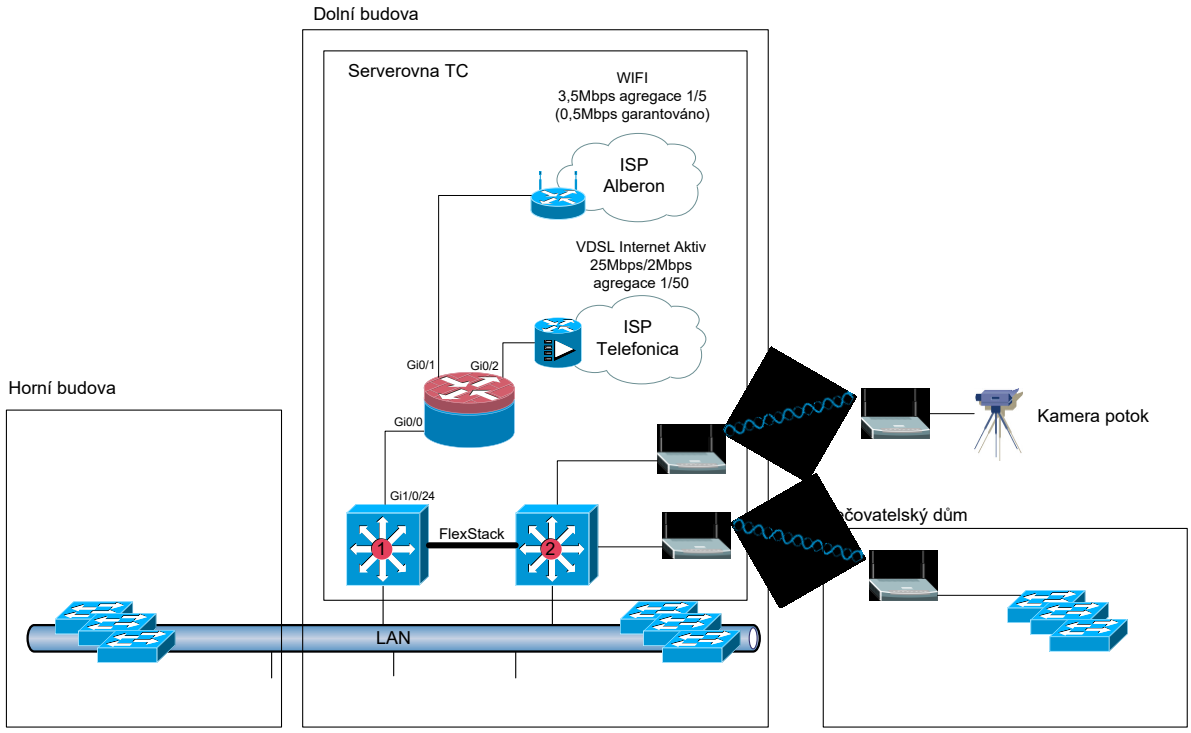


Management port - je dedikované nesměrované IP rozhraní pro OOB management.

IOS - Internetwork Operating System - Operační systém síťových zařízení společnosti Cisco Systems, využívající CLI (Command Line Interface) pro konfiguraci funkcionalit.

3.3.1 Konfigurace LAN TC

MěÚ Králíky - Technologické centrum - Fyzická topologie



LAN Technologického centra se nachází v serverovně umístěné v dolní budově MěÚ Králíky.

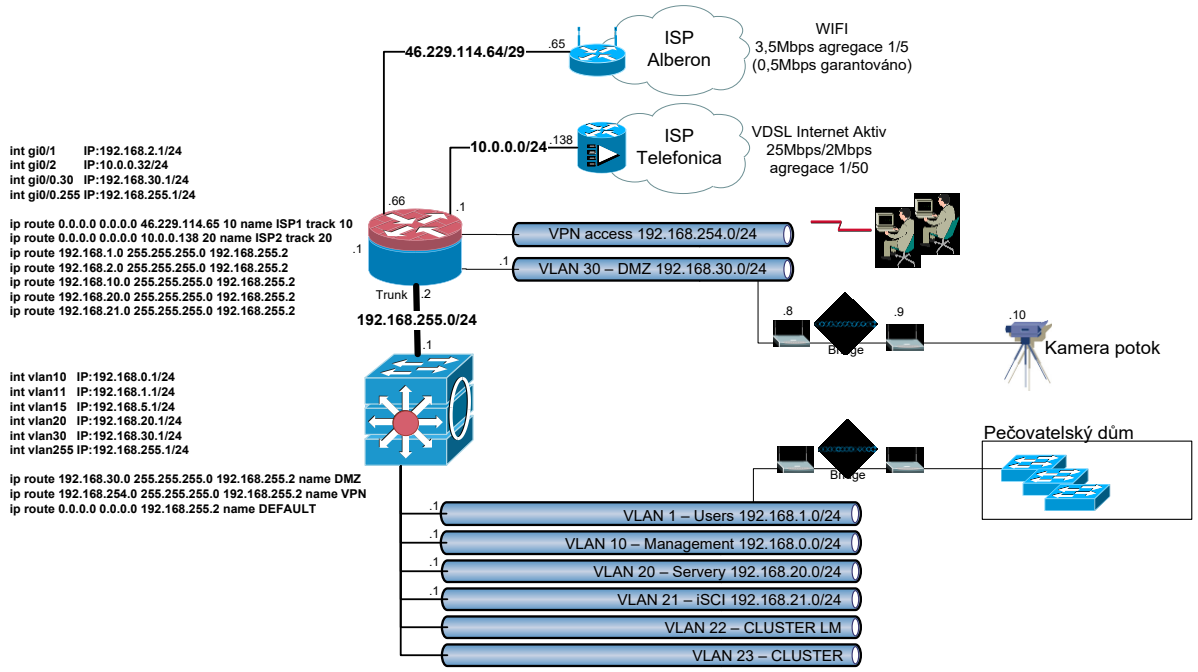
LAN TC zákazníka je tvořena ISR G2 routerem Cisco 2911 na perimetru sítě zajišťující směrování provozu do internetu (přepínání provozu mezi primární a záložní linkou), Demilitarizovanou zónu a bezpečnostní funkcionality v podobě zone-based firewallu a VPN koncentrátoru (pro připojení okolních obcí a outsourcingových firem spravující ch informační systémy).

Zároveň zde jsou umístěné PE routery obou providerů.

V serverovém bloku je pak LAN tvořena dvojicí switchů Catalyst 2960S-24TS-L propojených do stohu pomocí FlexStack sběrnice do jednoho logického zařízení. Aktivací SDM templatu lanbase-routing tyto switche zajišťují Inter-Vlan routing provozu mezi jednotlivými serverovými a uživatelskými Vlanami.

Switche primárně zajišťují připojení serverových systémů TC, dále pak připojení LAN MěÚ k serverovým systémům TC, a vzdálených lokalit (Horní budovy, pečovatelského domu a kamery snímající potok).

MěÚ Králíky - Technologické centrum – L3 topologie



Segmentace LAN do VLAN

LAN technologického centra je rozdělena do VLAN, pro oddělení provozu a zvýšení bezpečnosti. Směrování provozu mezi L3 Vlanami zajišťuje dvojice switchů s lan-base routing SDM šablonou, která aktivuje základní L3 routing funkcionality (statický routing, směrování mezi Vlanami). Tyto switche jsou propojeny pomocí FlexStack stohovací sběrnice, zajišťující vysokou dostupnost směrovacích a dalších funkcionalit, předáváním MASTER role mezi oběma switchi.

VLAN ID	VLAN NAME	IP SUBNET	DESCR.
1	Users	192.168.1.0/24	Vlan pro připojení uživatelů
10	Management	192.168.10.0/24	Vlan pro management zařízení TC
20	Servers	192.168.20.0/24	Vlan pro připojení serverových systémů
21	iSCSI	192.168.21.0/24	Vlan pro iSCSI komunikaci se storage systémy
22	CLUSTER-LM	---	L2 Vlan pro Live Migration komunikaci
23	CLUSTER	---	L2 Vlan pro Cluster komunikaci
30	DMZ	192.168.30.0/24	Vlan Demilitarizované zóny
255	trans-to-rtr	192.168.255.0/24	spojovací síť mezi switchem a routerem

Flexstack

Propojení switchů pomocí FlexStack stohu představuje hot-swap stohovací technologii, kdy všechny přepínače ve stohu působí jako jeden switch. Cisco FlexStack poskytuje jednotnou konfiguraci, a jednu IP adresu pro správu celého stohu přepínačů. Výhody stohování jsou nižší celkové náklady na vlastnictví (TCO) díky zjednodušené správě a vyšší dostupnosti. Cisco FlexStack podporuje cross-stack) funkcionality včetně EtherChannel, SPAN a FlexLink technologie.

Směrování internetového provozu

Směrování provozu do internetu zajišťuje ISR G2 router. Router využívá technologie IP SLA a trackingu ke sledování funkčnosti obou linek. Ke sledování stavu linek je využíván IP SLA DNS probing z obou inet. rozhraní routeru vždy na 4 DNS servery v internetu (primární a sekundární DNS server seznam.cz, primární a sekundární server centrum.cz) s rozdílným nastavením vah.

IP SLA DNS probingu je pak využíváno pro tracking směrování. Směrování do internetu je zajišťováno pomocí trackovaných defaultních směrovacích cest s různou metrikou (primární linka metrika 10, záložní linka metrika20).

V případě výpadku primární linky (detekováno pomocí DNS probingu - DNS servery neodpovídají na DNS dotazy) dojde k odebrání defaultní směrovací cesty přes ISP1 ze směrovací tabulky, čímž se začne směrovat dle defaultní cesty přes ISP2. Po obnovení komunikace na primární lince, dojde k opětovnému převzetí směrování přes primární linku ISP1.

Policy based routing (HTTP/HTTPS offload)

V případě funkčnosti obou internetových linek, je pomocí policy-based routingu směrován HTTP a HTTPS provoz z uživatelské vlany (VLAN1) přes záložní linku ISP2(Telefonika). Primárním cílem je snížení zátěže primární linky webovým provozem uživatelů, optimálním pro přenos přes asymetrické DSL linky.

Překlad adres NAT/PAT

LAN TC využívá privátní adresace dle RFC1918, pro přístup do sítě internet musí být tyto adresy přeloženy na veřejné směrované v internetové síti, k tomuto překladu adres je využívána technika NAT/PAT (Network Address Translation/Port Address Translation).

Na routeru jsou definovány subnety, jež mají povolen překlad adres do internetu, subnety, které nejsou uvedeny, nemají přístup do internetu.

LAN-to-NAT subnety s povoleným překladem adres
192.168.1.0/24
192.168.10.0/24
192.168.20.0/24
192.168.30.0/24

Statické veřejné adresy má TC přiděleno pouze od poskytovatele primární linky - společnosti Alberon Letohrad. Jedná se o subnet 46.229.114.64/29.

subnet 46.229.114.64/29	
.64	Adresa sítě
.65	adresa rozhraní routeru poskytovatele
.66	adresa rozhraní routeru TC
.67	Volně použitelné IP

subnet 46.229.114.64/29	
.68	Volně použitelné IP
.69	Volně použitelné IP
.70	Volně použitelné IP
.71	Broadcast

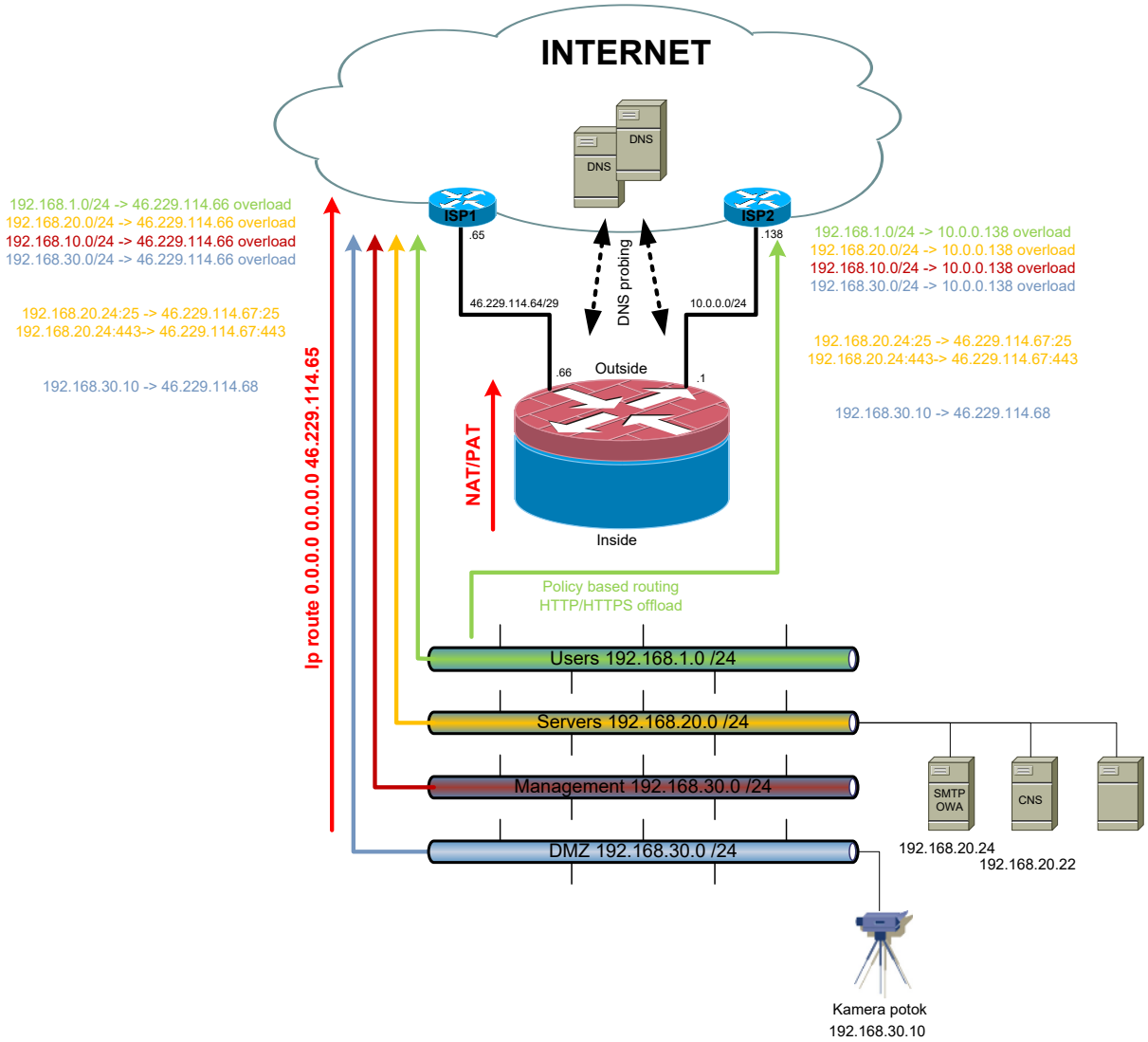
Primárně je veškerý provoz z těchto sítí překládán pomocí overload NATu na adresu rozhraní do sítě jednotlivých poskytovatelů ISP1 a ISP2. V případě provozu přes primární linku ISP1 se jedná o IP adresu odchozího provozu 46.229.112.66, v případě provozu přes záložní linku ISP2 je překlad na adresu 10.0.0.1 - zde se jedná opět o privátní adresu dle RFC1918, další překlad je proveden ADSL routeru poskytovatele, jehož veřejná adresa není fixní (poskytována DHCP serverem).

Portály, služby přístupné z internetu

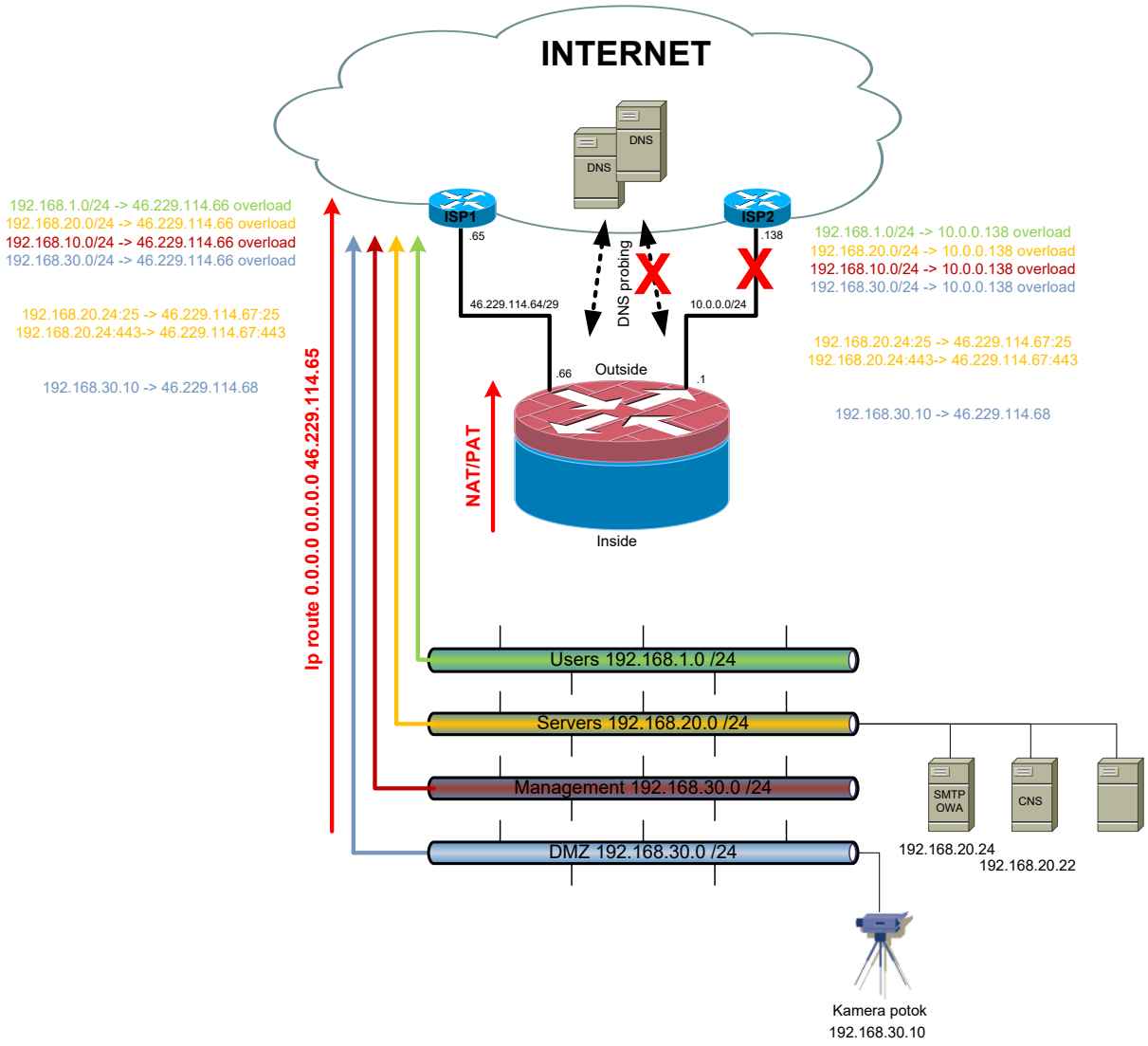
MěÚ provozuje v rámci TC systémy a portály, které musí být přístupné z internetu. Tyto systémy a portály jsou přeloženy pomocí statického NAT/PAT záznamu na veřejnou adresu. Jedná se o následující systémy a portály.

Systém /portál	Privátní LAN adresa	Veřejná INET adresa	Poznámka
Exchange - mail server Exchange - OWA	192.168.20.24:25 192.168.20.24:443	46.229.114.67:25 46.229.114.67:443	SMTP server Outlook Web Access
CNS spisová služba	192.168.20.22:6667 192.168.20.22:6668 192.168.20.22:6669	46.229.114.67:6667 46.229.114.67:6668 46.229.114.67:6669	CNS pro Mladkov CNS pro Lichkov CNS pro Dolní Moravu
Kamera Potok	192.168.30.10	46.229.114.68	Kamera snímající potok

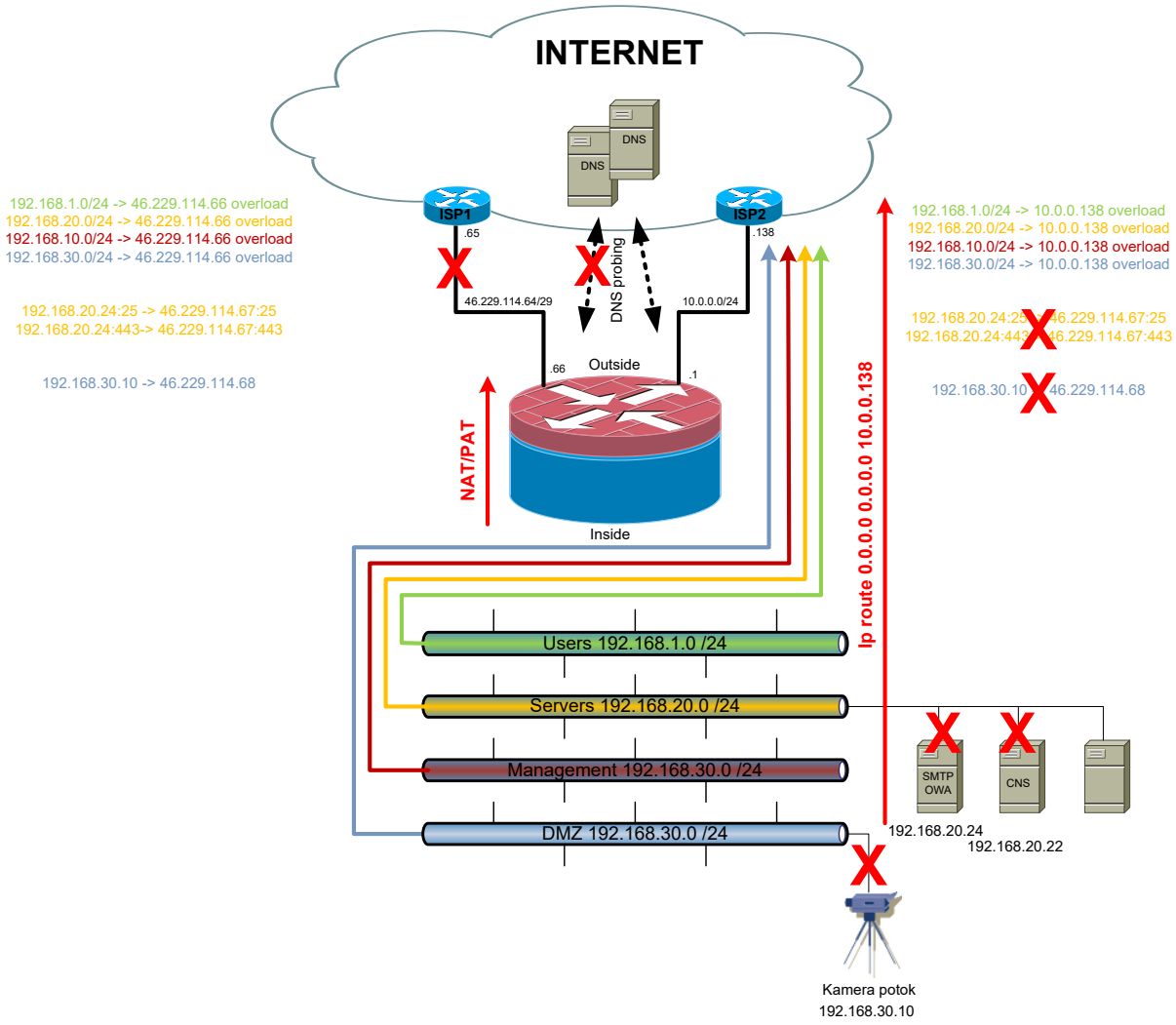
Směrování a překlad adres v případě funkčnosti obou linek



Směrování a překlad adres v případě výpadku záložní linky

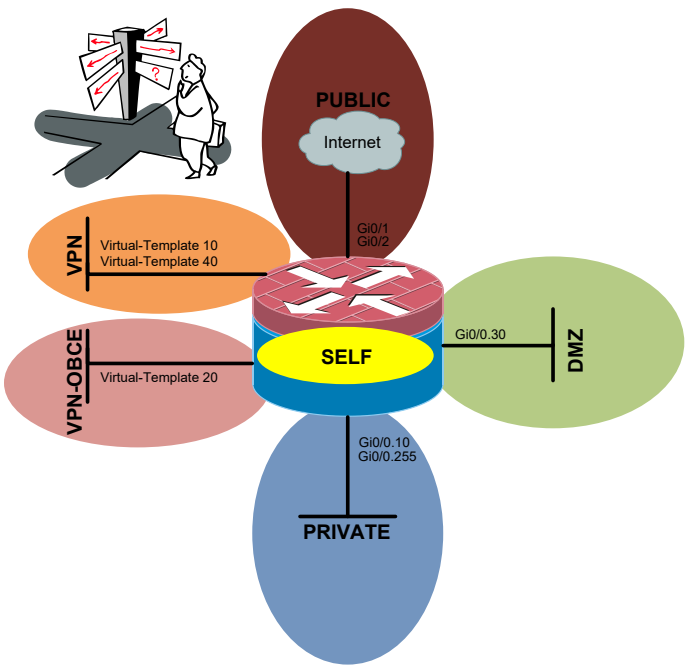


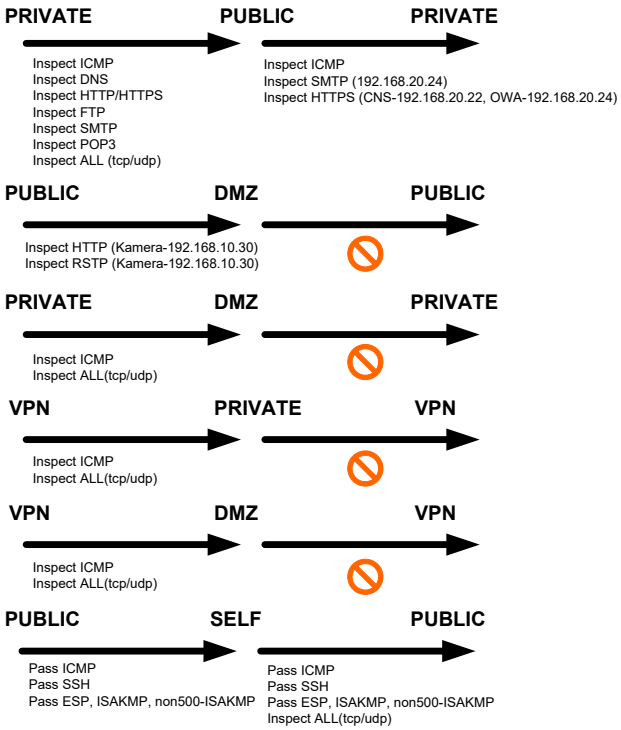
Směrování a překlad adres v případě výpadku primární linky



Zone-Based Firewall

Pro správnou funkci zónového firewallu (inspekční stavový firewall) musí být jednotlivá IP rozhraní směrovače přiřazena do zón, mezi jednotlivými zónami musí být definovány politiky určující pravidla komunikace mezi jednotlivými zónami.(Pokud není definována politika mezi jednotlivými zónami je veškerý provoz blokován, výjimkou je SELF zóna kde je bez politiky veškerý provoz povolen). SELF zóna definuje IP rozhraní routeru, a je určena k definování politiky pro provoz Z a NA rozhraní routeru. Rozdělení rozhraní do zón a jednotlivé politiky mezi zónami zobrazuje následující obrázek.





ICMP provoz je filtrován- umožnuje pouze následující typ zpráv:
(echo, echo-reply,time-exceeded,traceroute,unreachable)

VPN přístup

K VPN klientskému přístupu je využívána IPSEC VPN v tunelovacím režimu s šifrováním provozu pomocí AES algoritmu. Pro správnou funkci funkci musí mít uživatel nainstalovaného Cisco VPN klienta.

VPN přístup je realizován pomocí tzv. VTI rozhraní (Virtual Tunnel Interface), umožňující vysokou škálovatelnost z pohledu síťových funkcionalit.

Pro VPN přístup jsou připraveny 3 VPN profily definované pomocí group autentizace(svázané s Virtual-Template rozhraními), lišící se v přístupových oprávněních do sítě zákazníka. Následně se provádí extended autentizace uživatele oproti lokální DB na routeru a účtu v AD přes radius server.

VPN profil	Group ID	Virt-template	tunelled networks	Poznámka
support	support	virt-template 10	192.168.1.0/24 192.168.10.0/24 192.168.20.0/24 192.168.21.0/24 192.168.30.0/24	Pro potřeby administrátorů TC.
orp-obce	orp-obce	virt-template 20	192.168.20.0/24	Pro potřeby přístupu okolních obcí (zatím nepoužíváno)
vpn-dodavatele	vpn-dodavatele	virt-template 40	192.168.20.0/24	Pro potřeby přístupu dodavatelů systémů a portálů TC.

Extended autentizace VPN uživatelů

Po group autentizaci VPN uživatele následuje extended autentizace samotného uživatele oproti lokální DB na routeru nebo AD pomocí radius serveru - Network Policy Server na platformě Windows server 2008 R2. Lokální účet na routeru je pouze jako emergency VPN přístup v případě problémů v komunikaci s radius serverem. Primárním ověřovatelem je radius server s vazbou na AD. Network Policy Server (radius) je provozován na serveru srv-mgmt (192.168.20.25).

Pro autentizaci VPN uživatelů je v AD zřízena skupina VPN_Users, jejichž členové právo VPN přístupu.

Server blok - Switche

Jak již bylo zmíněno výše - LAN TC je rozsegmentována do virtuálních LAN sítí - VLAN. Jednotlivé systémy TC jsou pak připojovány do portů switche náležejících do příslušné VLANy popř. jsou připojovány do TRUNK portů agregujících provoz všech VLAN. Pro oddělení provozu jednotlivých VLAN je použito IEEE802.1Q encapsulace. Nativní VLAN v rámci všech trunků je nastavena na VLAN999 (všechny provozní vlan v trunku jsou tagované).

Z důvodů vysoké dostupnosti je většina systémů TC připojena „multihome" - redundantně na oba serverové switche (pro zajištění konektivity v případě výpadku jednoho ze switchů. Konfigurace většiny portů na switchích je realizována zrcadlově kdy nastavení portu Gi1/0/1 je totožné s nastavením portu Gi2/0/1 (kdy první číslice udává pozici switche v rámci stacku a poslední číslo určuje port switche). Systémy, které neumožňují multihoming jsou primárně připojeny na první switch (Gi1/0/x) v případě poruchy prvního switche pak musejí být administrátorem přepojeny do zrcadlového portu na druhém switchi - port Gi2/0/x) - jedná se například o router ISR G2.

Systémy, které umožňují ether-channel (trunking) ať již statický popř. dynamicky vyjednávaný pomocí LACP protokolu, jsou připojeny na porty v ether-channel módu a umožňují dynamické rozkládání zátěže mezi síťovými kartami a switchi.

Klíčové serverové systémy jsou připojeny rychlostí 1Gbit/s a full duplexem (vypnuto autonegotiation), toto nastavení musí být pro správnou funkčnost i na straně serverů (viz nastavení portů). Ostatní porty mají nastavenu rychlost a duplex na automatické vyjednávání.

Cisco FlexStack - stohovací hot-swap technologie. Všechny přepínače ve stohu působí jako jeden switch. Cisco FlexStack poskytuje jednotnou konfiguraci, a jednu IP adresu pro správu celého stohu přepínačů. Výhody stohování jsou nižší celkové náklady na vlastnictví (TCO) díky zjednodušené správě a vyšší dostupnosti. Cisco FlexStack podporuje cross-stack) funkcionality včetně EtherChannel, SPAN a FlexLink technologie. FlexStack modul může být přidán do jakéhokoli Cisco Catalyst 2960-S přepínače s LAN Base softwarem.

3.4 Projekty realizované z evropských fondů

Výzva č. 22 - projekt CZ.1.06/2.1.00/22.09380 Konsolidace IT ORP Králíky

Projekt Konsolidace IT ORP Králíky navazoval na projekt regionálních center, tzv. eGON center, která mají složku technologickou, vzdělávací a administrativní. Takto pojatá centra se stala výrazným nositelem a šiřitelem znalostí konceptu eGovernment v regionech.

Realizací eGON center a v rámci nich vytvořených Technologických center ORP byl vytvořen kvalitní základ pro rozvoj služeb elektronizace výkonu veřejné správy podle místních a regionálních podmínek v technologické oblasti i v oblasti provozního a personálního zajištění jeho rozvoje.

V rámci projektu Konsolidace IT ORP Králíky byly realizovány 4 aktivity komplexně pokrývající výzvu IOP č. 22:

- Konsolidace HW a SW úřadu včetně virtualizace aplikací, desktopů, serverů, infrastruktury – pořízení a zvýšení efektivity HW / SW MěÚ Králíky přímo sloužícího k naplňování postupné elektronizace výkonu veřejné správy
- Rozvoj služeb TC ORP a návaznost na TCK – pořízení HW / SW pro rozšíření služeb úspěšně vybudovaného TC ORP Králíky
- Zvýšení bezpečnosti a bezpečnostní infrastruktura TC ORP Králíky – pořízení bezpečnostních prvků pro zajištění služeb TC ORP Králíky
- Elektronizace procesů, digitalizace dat a propojení lokálních AIS s registry veřejné správy – elektronizace vybraných agend a procesů MěÚ Králíky

Co nám to přineslo:

- Virtualizace aplikací - streaming aplikací, aplikace je nainstalována do malého virtuálního prostředí a v této podobě je aplikace doručována do systému klienta, kde ji lze spustit bez nutnosti její instalace. Takto virtualizovaná aplikace po spuštění využívá výpočetní prostředky serverového operačního systému. Výhody: bezpečnost (data neopouštějí serverovnu), možnost připojení vzdáleně prostřednictvím Internetu (kdykoliv a odkudkoliv využívá SMK).
- Centrální evidence smluv – elektronizace procesu schvalování, evidence, správy a archivace smluvních vztahů organizace.
- Nové moduly stávajícího IS – v rámci podpory nové elektronizace procesů agendy silniční úřad
- Agenda RŽP (Registr Živnostenského Podnikání) – Zavedení oboustranného rozhraní elektronické spisové služby a UniSPIS IS RŽP.
- Nákup 2 multifunkčních zařízení – v návaznosti na digitalizaci vstupů a výstupů nové agendy centrální evidence smluv a elektronické spisové služby (umístění na obě budovy pro možnost operativní digitalizace). Nástroj pro digitalizaci dat pro všechny odbory MěÚ.
- V rámci konsolidace LAN bezdrátové propojení budov MěÚ na infrastruktuře 24 GHz pro rychlost 1Gbit/s v návaznosti na aktivitu vizualizace aplikací a přístupu k datovým zdrojům ve vnitřní LAN (Centrální evidence smluv, agenda Vodoprávní úřad, oboustranné rozhranní UniSPIS).
- Povýšení doménového řadiče a řadičů virtualizace HyperV na OS Windows server 2012 doplnění RAM pro umožnění vizualizace aplikací bez nutnosti pořizovat nový server.
- Výměna aktivních prvků sítě – 10 ks v návaznosti na zvýšení bezpečnosti (možnost řízení toku dat a řízení bezpečnosti před útokem penetrací již na protokolové vrstvě L2.
- Zvýšení objemu datového úložiště v návaznosti na nově elektronizované agendy nárůst digitalizovaných dokumentů.
- Pořízení SW zálohovacího (archivačního) systému v rámci konsolidace HW/SW v návaznosti na zvýšení bezpečnosti a nových požadavků na zálohování a archivaci dat.

  Nákup antivirového systému (předplatné na 4 roky) – v rámci aktivity na zabezpečení dat technologického centra.

Financování - celková částka po ukončení projektu 2 320 314,10 Kč:

	Strukturální fondy (Kč)	Obecní rozpočet (Kč)
Celkem podíly	1 972 266,98	348 047,12

Výzva č. 06 projekt CZ.1.06/2.1.00/06.06838 Technologické centrum ORP Králíky

Plánovací období: 2007 - 2013

Program: IOP – Integrovaný operační program

Prioritní osa: 2 Zavádění ICT v územní veřejné správě

Oblast podpory: 2.1 Zavádění ICT v územní veřejné správě

Žadatel: Město Králíky

Místo realizace projektu: Město Králíky

Datum realizace: leden 2011 - 30. 9. 2011

Účelem projektu je zlepšit dostupnost služeb státní správy všem občanům ve správním obvodu města Králíky, snížit administrativní zátěž a zajistit efektivní komunikaci jak mezi úřady a občanem tak mezi subjekty veřejné správy navzájem. Základem je zefektivnit činnost úřadů veřejné správy, prostřednictvím zavádění ICT a vytvořit tak nové portfolio služeb, které bude dostupné všem skupinám obyvatel.

Celkové náklady: 5 813 459 Kč

	Strukturální fondy a st. rozp. (Kč)	Obecní rozpočet (Kč)
Celkem podíly	4 941 440	872 019

Výzva č. 33 - projekt CZ.03.4.74/0.0/0.0/16_033/0002849 Profesionální MěÚ Králíky

Město Králíky nedisponuje strategickými dokumenty, které by jednoznačně určovaly strategický směr rozvoje města, a to s ohledem na plánovaný rozvoj území a strategie kraje a ČR. Z tohoto důvodu je třeba zpracovat Strategický plán rozvoje města vč. Akčního plánu, který bude identifikovat a hodnotit současné zdroje, kapacity a možnosti rozvoje předmětného území. V rámci MěÚ není koncepčně plánován a řízen ani rozvoj informačních a komunikačních technologií (ICT), a to jak z pohledu podpory výkonu procesů úřadu nástroji ICT / IS, tak i z pohledu bezpečnosti informací a dat. Z pohledu poskytovaných služeb je proto nezbytné posoudit aktuální stav ICT a definovat jednotnou Strategii rozvoje a bezpečnosti ICT. Dle zpětné vazby od občanů města je třeba podpořit oblast transparentního a otevřeného úřadu, a to zejména v oblasti e-komunikace a zajištění on-line přenosů jednání orgánů města na profesionální úrovni. MěÚ chce trvale a transparentně poskytovat služby v souladu s příslušnými předpisy a normou ISO 9001:2015 a požadavky klientů, a tím zvyšovat jejich spokojenost. V neposlední řadě projekt řeší aktuální potřebu zvyšování / prohlubování kvalifikace stávajících úředníků a zaměstnanců města zařazených do organizační struktury MěÚ (dále zaměstnanci) v oblastech souvisejících s oborem jejich působnosti (v souladu se Strategií vzdělávání).

Co nám to přinese (projekt v realizaci):

Systémové zlepšení bude provedeno prostřednictvím následujících dílčích cílů:

- Zpracování Strategického plánu rozvoje města vč. Akčního plánu.
- Zpracování Strategie rozvoje a bezpečnosti ICT.

- Realizace "otevřeného úřadu", který podpoří rozvoj komunikace s veřejností a zajistí transparentní jednání orgánů města prostřednictvím zavedení moderní prezentační a záznamové techniky.
- Certifikace ISO - implementace požadavků ISO 9001:2015.
- Realizace obecných i specifických vzdělávacích a výcvikových školení přispívajících ke zkvalitnění rozvoje konkrétních kompetencí stávajících zaměstnanců (rozvoj potřebných znalostí a dovedností zaměstnanců).
- Zlepšení pracovního prostředí a zatraktivnění MěÚ v pozici zaměstnavatele.

Financování - celková rozpočtovaná částka projektu 2 395 904,25 Kč:

	Strukturální fondy a st. rozp. (Kč)	Obecní rozpočet (Kč)
Celkem podíly	2 276 109,02	119 795,23

3.5 Analýza očekávání rozhodujících „zájmových skupin"

Analýza očekávání a uspokojování potřeb rozhodujících „zájmových skupin" byla zaměřena jak na potřeby z pohledu Městského úřadu, tak z pohledu celého Města Králíky.

Mezi klíčové požadavky uživatelů IS MěÚ Králíky patří:

- **Komunikace s občany**

  Potřeba redesignu, modernizace, zvýšení uživatelské přívětivosti a zrychlení webové prezentace MěÚ Králíky. Potřeba sdílení centralizovaných a aktuálních informací o poskytovaných službách a aktivitách města a úřadu.

  Potřeba lepšího informování veřejnosti prostřednictvím přenosů a záznamů (video i audio) z jednání Zastupitelstva a prohloubení elektronizace jednání Rady města, především s ohledem na adresné hlasování.
- **Informační gramotnost**

  Potřeba vzdělávání zaměstnanců MěÚ Králíky v oblasti využití, vyhledání a zpracování existujících dat. Potřeba zajištění metodické uživatelské podpory práce s klíčovými informačními systémy MěÚ Králíky. Zavedení systému trvalého vzdělávání zaměstnanců MěÚ Králíky v informační gramotnosti.

  Potřeba podpory zavádění nových částí IS MěÚ Králíky školením v oblasti užívání IS, včetně procesních dopadů do fungování MěÚ Králíky. Potřeba provádět školení opakovaně v pravidelných intervalech. Školení jsou v odpovědnosti věcně příslušných útvarů, definujících procesní výkon příslušných nově podpořených agend.
- **Metodická podpora využívání IS MěÚ Králíky**

  Potřeba zřídit pozici metodika, který bude poskytovat metodickou podporu celému úřadu a dotčeným subjektům v oblasti práce s IS MěÚ Králíky.
- **Elektronická distribuce dokumentů pro obce**

  Potřeba umožnění elektronické distribuce dokumentů pro obce a jejich zpřístupnění v úrovních podle přístupových práv.
- **Výkazy příspěvkových organizací a jednotný ekonomický informační systém**

  Příspěvkové organizace nepoužívají pro zpracování účetnictví jednotné programové vybavení. Je vhodné zavést jednotný ekonomický informační systém MěÚ Králíky a umožnit analýzy a porovnání existujících ekonomických dat a další práci s daty a modelování.
- **Bezpečnost IS MěÚ Králíky**

  Potřeba přesnějšího zacílení emailových spamových filtrů a blokování nebezpečných webových prezentací s ohledem na udržení minimálně stejné úrovně zabezpečení IS MěÚ Králíky.

- **Elektronické podepisování**

  Potřeba postupně zavádět a pilotně ověřovat elektronické podepisování v rámci interních procesů MěÚ Králíky, se zohledněním legislativních omezení a nastavené úrovně zabezpečení IS MěÚ Králíky včetně využití časových razítek.
- **Elektronizace vnitřních procesů**

  Potřeba postupného zavádění elektronizace vnitřních procesů (cestovní příkazy, propojení na dovolené, výplatní pásky apod.).
- **Bezpečnost ICT ve školách**

  Potřeba zajistit odpovídající úroveň bezpečnosti provozovaných technologií ve zřizovaných školách.
- **Komunikace s krizovými štáby ORP**

  Potřeba zprovoznění nástroje pro rozšíření komunikace při řešení krizových situací pro předávání informací mezi MěÚ Králíky a managementem obcí, krizovými štáby obcí a složkami Integrovaného záchranného systému (v současné chvíli je funkční pouze SMS kanál a digitální rozhlas).
- **Bezpečnost informací**

  Potřeba udržovat a trvale rozvíjet systém bezpečnosti informací MěÚ Králíky a podniknout kroky nutné k naplnění požadavků Zákona o kybernetické bezpečnosti a GDPR.

Uživatelé IS MěÚ Králíky by uvítali postupnou větší integraci s centrálními IS a registry tak, aby bylo možné více využívat a přebírat data a zamezit tím jejich duplicitnímu sběru.

Jednotlivé strategické cíle reflektující zjištěné požadavky uživatelů IS MěÚ Králíky jsou uvedeny v kapitole 4 tohoto dokumentu.

3.6 Shrnutí analýzy (SWOT)

Matice SWOT je zaměřena na posouzení hlavních důvodů pro realizaci nové strategie. Kromě zhodnocení stávajícího stavu jsou výstupy této analýzy použity k identifikaci rizik a jejich řízení a samozřejmě i k rámcové identifikaci požadavků pro nové období. Tato analýza bude sloužit jako hlavní podklad pro návrhovou část Strategie rozvoje a bezpečnosti ICT.

S - SILNÉ STRÁNKY	W - SLABÉ STRÁNKY

▪ Existence Regionální datové sítě (RDS), Technologického centra města (TC Králíky), Krajské digitální spisovny (KDS), Krajského digitálního úložiště (KDU), a Hostované spisové služby (kraj i ORP)
▪ Byly úspěšně realizovány projekty:
  ▪ Výzva č. 22 - projekt CZ.1.06/2.1.00/22.09380 Konsolidace IT ORP Králíky
  ▪ Výzva č. 06 projekt CZ.1.06/2.1.00/06.06838 Technologické centrum ORP Králíky
▪ Probíhá realizace projektu Výzva č. 33 - projekt CZ.03.4.74/0.0/0.0/16_033/0002849 Profesionální MěÚ Králíky
▪ V přípravě je projekt v rámci výzvy č. 28 IROP
▪ Spokojenost s prací odboru organizačního a správního, velmi dobře nastavené vztahy, z pohledu uživatelů fungující podpora
▪ Specialisté na Informační technologie jako stabilní tým odborníků s dlouholetou zkušeností
▪ Dobrá SW podpora pro hlavní vykonávané agendy
▪ Pořizování a obnova hardware je zavedený a dlouhodobě plánovaný proces
	▪ Nedostatečná metodická podpora výkonu agend a využívaných IS
	▪ Nedostatečné využití existujících dat pro podporu rozhodování managementu a úředníků Města Králíky
	▪ Nízký personální stav a poddimenzovaný rozpočet odboru organizačního a správního
	▪ Velká závislost na externích dodavatelích
	▪ Vzdělávání odborníků v oblasti ICT časově neodpovídající nasazení nových technologií
	▪ Velká roztříštěnost technologií vlivem Zákona o veřejných zakázkách
	▪ Přístup uživatelů k zabezpečení IS MěÚ Králíky a z toho plynoucí nespokojenost uživatelů s bezpečnostními omezeními
	▪ Poddimenzované a nekoordinované ICT na školách

O - PŘÍLEŽITOSTI	T - HROZBY
▪ Využití projektů na státní úrovni a zapojení se do nich ▪ Nasazení Jednotného ekonomického informačního systému do všech příspěvkových organizací ▪ Prohloubení využívání elektronického podepisování dokumentů v IS MěÚ Králíky ▪ Zavádění služeb eGovernmentu ▪ Dotační tituly EU jako zdroj peněz pro možný rozvoj IS/ICT města ▪ Zavedení elektronického schvalování v interních procesech úřadu (požadavků, dokumentů…) ▪ Větší sjednocení a centralizace nákupu ICT v rámci organizací města, minimálně pro některé běžnější komodity	▪ Další tlak na snižování rozpočtu ▪ Změny legislativy vyžadující ad hoc reakci ▪ Zveřejňování smluv / registr smluv ▪ 2018: Předpokládaná platnost zákona o elektronické stopě finančních dokumentů ▪ Prohlubující se propast mezi rostoucí úrovní technologií a znalostmi uživatelů a pracovníků OOS ▪ Nebezpečí kybernetické (digitální) kriminality ▪ Růst počtu IS nebo technologií bez odpovídajícího navýšení počtu ICT správců ▪ Komplikovanost a administrativní překážky v elektronizaci agend veřejné správy

3.7 Analýza rizik a návrhy opatření pro jejich snížení

Analýza rizik přináší přehled základních rizik, která mohou ohrožovat realizaci Strategie a snižovat přínos jejích výstupů.

Riziko	Popis rizika	Dopad rizika	Předcházení /eliminace rizika	Odpovědnost
Nedostatečná podpora realizace Strategie	Nízká priorita a nedostatečná podpora realizace Strategie ve vnímání vrcholového vedení MěÚ Králíky.	Ohrožení realizace Strategie.	Vnímání Strategie jako prioritní vedením MěÚ Králíky. Veřejná deklarace podpory projektu.	Vedení MěÚ Králíky
Nedostatečná kapacita pro realizaci Strategie	Vysoké vytížení interních zaměstnanců MěÚ Králíky a zaměstnanců OOS, nedostatek kapacit pro poskytování potřebné součinnosti / vykonávání přímých činností vyžadovaných realizací Strategie.	Nízká součinnost.	Sestavení kvalitního realizačního týmu, jehož složení odpovídá rozsahu a složitosti Strategie. Vypracování detailního harmonogramu realizace Strategie zahrnujícího lhůty pro poskytnutí součinnosti a jeho pravidelná aktualizace na základě postupu realizace Strategie. Včasné plánování nároků na součinnost, včasná komunikace dotčeným zaměstnancům MěÚ Králíky a OOS a jejich nadřízeným pracovníkům.	OOS
Nesoučinnost s uživateli výstupů Strategie	Nesoučinnost realizačního týmu s vedením / zaměstnanci / MěÚ Králíky a zřizovaných organizací.	Ohrožení praktické využitelnosti výstupů Strategie.	Zapojení klíčových uživatelů již v průběhu přípravy a realizace Strategie do definice jejích výstupů. Zajištění školení uživatelů výstupů Strategie.	OOS
Nedostatečné kompetence či kapacita dodavatelů	Výběr dodavatelů nedisponujících nezbytnou kapacitou a kompetencemi k realizaci Strategie a následnému rozvoji a údržbě výstupů.	Ohrožení kvality výstupů. Nekvalitní / nedostatečné řízení projektů.	Definice nezbytných kompetencí a referencí očekávaných od dodavatelů.	OOS

Riziko	Popis rizika	Dopad rizika	Předcházení /eliminace rizika	Odpovědnost
Nekvalitní realizační tým Strategie (nedostatečné kvalifikační předpoklady členů realizačního týmu)	Nedostatek zkušených a kompetentních kapacit členů realizačního týmu, neodpovídající zkušenosti a kvalifikace úrovni a vážnosti Strategie.	Ohrožení dosažení cíle – např. potenciálních termínů projektů s možným dopadem do nákladů či neschopnost zrealizovat včas očekávané výstupy. Nespokojenost vedení MěÚ Králíky a uživatelů s postupem realizace a ztráta důvěry.	Sestavení kvalitního realizačního týmu, jehož složení odpovídá rozsahu a složitosti Strategie. Nominace členů realizačního týmu na základě definované specializace, odbornosti a zkušeností. Stanovení přesných kompetencí a odpovědností členů realizačního týmu.	OOS
Nedostatečné řízení Strategie, pomalé rozhodování a schvalování	Poptání nedostatečně jasně definovaného plnění, pozdní vyhlášení či pomalé vyhodnocení nabídek.	Dodání nežádoucího plnění či v čase později než by bylo žádoucí.	Vypracování detailního harmonogramu realizace Strategie a jeho pravidelná aktualizace na základě postupu realizace. Plánování nároků na součinnost Zadavatele, stanovení termínů pro schválení předložených podkladů Zadavatelem. Komunikace vzniklých problémů na pravidelných poradách realizačního týmu Strategie.	Vedoucí projektu
Nedodržení harmonogramu (časové zpoždění realizace Strategie)	Zpoždění s dodávkou jednotlivých výstupů Strategie v čase.	Nemožnost využívat výstupy a požívat jejich přínosů v plánovaných časech. Nutnost posunout zahájení případných navazujících projektů.	Nadefinování a vytvoření veškerých podmínek pro zajištění plynulé realizace Strategie. Udržování aktuálního harmonogramu včetně požadované součinnosti definované v čase. Průběžné kontroly plnění aktivit Strategie a požadované součinnosti vůči harmonogramu na jednání realizačního týmu Strategie.	Projektový manažer
Nedostatečná alokace financí pro realizaci Strategie	Nedostatečná alokace finančních prostředků v rozpočtu MěÚ Králíky.	Zpomalení realizace Strategie v důsledku nedostatku financí až možné úplné zastavení realizace.	Alokace finančních zdrojů Strategie s dostatečným předstihem a s přihlédnutím k možnosti následného rozšíření požadovaných výstupů.	Rada a Zastupitelstvo MěÚ Králíky

Riziko	Popis rizika	Dopad rizika	Předcházení /eliminace rizika	Odpovědnost
Nedostatečné využití alternativních finančních zdrojů (granty, dotace, ...)	Nepřiznání dotace z důvodu nekvalitně zpracované žádosti o dotaci.	Nemožnost zajistit financování a realizovat Strategii.	Je nastaven a zajištěn pravidelný monitoring relevantních dotačních programů. Žádosti o dotace jsou zpracovávány ve spolupráci s příslušným odborným útvarem MěÚ Králíky, případně s externím zpracovatelem s odpovídajícími zkušenostmi. Plánování žádostí o čerpání dotačních prostředků je s dostatečných předstihem projednáváno se zástupci Odboru finančního.	OOS
Nedodržení podmínek grantů a dotací (vrácení dotací z důvodů nezvládnutí realizace nebo udržitelnosti projektů) využitých pro spolufinancování realizace Strategie	Čerpání přiznaných dotací je kráceno z důvodů nedodržení cílů (indikátorů) a/nebo termínů projektu. Čerpání přiznaných dotací je kráceno z důvodu pochybení (i formálních) při administraci projektu.	Krácení či odejmutí dotace.	Administrátor dotace Strategie bude dohlížet na to, aby veškeré postupy v rámci realizace projektů byly realizovány dle předepsaných podmínek dotačního titulu. Předpoklady dlouhodobé udržitelnosti výstupů projektů budou předem zohledněny a nárokovány do rozpočtu MěÚ Králíky.	Administrátor dotace
Časové prodlení realizace investičních akcí	Zpoždění procesu veřejné zakázky dle platného zákona o veřejných zakázkách na výběr zhotovitele (realizátora) investiční akce. Časové prodlení z důvodu nastavení rozhodovacích procesů MěÚ Králíky při schvalování změn. Časové prodlení z důvodu nedostatečné součinnosti zhotovitele / zhotovitelů investiční akce. Prodlení z důvodu nedostatečně poznaných rizik při přípravě a	Nespokojenost vedení MěÚ Králíky a uživatelů s postupem realizace a ztráta důvěry.	Zajištění výběrových řízení jsou pověřeni zkušení zaměstnanci a je jim poskytnuta náležitá metodická součinnost. Specifická či jinak náročná výběrová řízení jsou zajišťována s podporou externích expertů. Na výběrové řízení je zajištěna dostatečná časová dotace. Jsou evidována, vyhodnocována a sdílena již poznaná rizika a zkušenosti z dříve realizovaných investičních akcí. Pro schvalování změn týkajících se investičních prací (např. vícepráce apod.) jsou předem nastaveny a všemi zainteresovanými stranami	OOS

Riziko	Popis rizika	Dopad rizika	Předcházení /eliminace rizika	Odpovědnost
	realizaci investiční akce.		odsouhlaseny schvalovací postupy a vymezeny kompetence jednotlivých řídících a výkonných úrovní.	
Chyby ve smluvních dokumentech MěÚ Králíky / nevýhodné smluvní podmínky (prohrané právní spory)	Rizika vyplývající z nejednoznačných nebo pro MěÚ Králíky nevýhodných smluvních ustanovení / smluvních vztahů (obecně nekvalitních smluv). Převzetí díla / akceptace služby v rozporu s podmínkami dodávky / smluvními podmínkami, neuplatňování smluvních sankcí a pokut. Konkrétně se jedná např. o riziko odpovědnosti třetím stranám, riziko změny smlouvy, riziko porušení obecně závazných předpisů, riziko porušování smluvní odpovědnosti, riziko neplatnosti právních úkonů.	Zpoždění projektů nebo zvýšené náklady na projekty. Možné úplné zastavení realizace projektů.	Zajištění formální správnosti smluv a smluvních ujednání podle druhu smlouvy. Zavedení registru vzorových smluv, resp. využívání vzorových smluvních dokumentů. Maximální možné využívání vlastních smluvních dokumentů bez možnosti změn druhé smluvní strany (např. u veřejných zakázek). Nastavení schvalovacích a kontrolních mechanismů před schválením a uzavřením smlouvy. Ošetřování smluvních rizik kvalitními (pro MěÚ Králíky výhodnými) ustanoveními v oblasti sankcí a odpovědností zhotovitele. Průběžná kontrola dodržování podmínek smluvních vztahů. Průběžná revize smluvních vztahů (zejména u dlouhodobých smluvních vztahů).	OOS
Nedostatečná úroveň řídících dokumentů ve vztahu k ICT	Řídící a metodické pokyny pro práci s informačními systémy nejsou aktuální, jejich struktura je nedostatečná nebo zcela chybí. Nejsou zcela využívány možnosti informačních systémů, informační systémy jsou využívány nesprávně.	Dopady na efektivnost práce s IS, a celkovou kvalitu, dopady na bezpečnost informačního systému jako celku.	Průběžná práce na řídících a metodických dokumentech.	OOS

Riziko	Popis rizika	Dopad rizika	Předcházení /eliminace rizika	Odpovědnost
Nepřipravenost na řešení mimořádných situací ve vztahu k ICT technologiím	Krizové plány zahrnují ICT technologie pouze okrajově. Žádný z krizových plánů nepředpokládá vznik krizového scénáře, kde ICT bude hrát hlavní roli.	Bez podpory ICT technologií není město/úřad schopen plnit své základní funkce.	Příprava krizových scénářů, které zahrnou ICT technologie (například scénář pro dlouhodobý „black-out" apod.).	OOS

3.7.1 Metodika hodnocení rizik[2]

Riziko (Risk) je nebezpečí, že určitá událost, jednání nebo stav nastane a bude mít negativní důsledek. Riziko představuje především ohrožení nebo újmu na majetku a právech. Je definováno také jako pravděpodobnost vzniku události či změny, která nepříznivě ovlivní požadovaný výsledek.

Hodnocení rizik je vyjádřeno jako funkce, kterou ovlivňuje dopad, hrozba a zranitelnost.

Stupnice pro hodnocení dopadů

Dopad (Impact) je vznik škody v důsledku působení hrozby na aktivum. Pro hodnocení je použita škála 1 - 4 (nízký - střední - vysoký - kritický).

Úroveň	Popis
Nízký	Dopad je v omezeném časovém období a malého rozsahu a nesmí být katastrofický. Rozsah případných škod nepřesahuje a) 10 zraněných osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty do 5000000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího nejvýše 250 osob.
Střední	Dopad je omezeného rozsahu a v omezeném časovém období. Rozsah případných škod se pohybuje v rozmezí a) do 10 mrtvých nebo od 11 do 100 osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty od 5000000 Kč do 50000000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 251 do 2500 osob.
Vysoký	Dopad je omezeného rozsahu, ale trvalý nebo katastrofický. Rozsah případných škod se pohybuje v rozmezí a) od 11 do 100 mrtvých nebo od 101 do 1000 osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty od 50000000 Kč do 500000000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího od 2501 do 25000 osob.
Kritický	Dopad je plošný rozsahem, trvalý a katastrofický. Rozsah případných škod se pohybuje v rozmezí a) 101 a více mrtvých a 1001 a více osob s následnou hospitalizací po dobu delší než 24 hodin nebo b) finanční nebo materiální ztráty převyšující 500000000 Kč anebo c) představuje dopad na veřejnost s rozsáhlým omezením nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 25000 osob.

Stupnice pro hodnocení hrozeb

Hrozba (Threat) je událost ohrožující bezpečnost aktiva (zneužití zranitelnosti aktiva). Pro hodnocení je použita škála 1 - 4 (nízká - střední - vysoká - kritická).

Úroveň	Popis
Nízká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.

[2] Příloha č. 2 k vyhlášce č. 316/2014 Sb.

Úroveň	Popis
Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.
Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.
Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.

Stupnice pro hodnocení zranitelností

Zranitelnost (Vulnerability) je slabé místo aktiva. Pro hodnocení je použita škála 1 - 4 (nízká - střední - vysoká - kritická).

Úroveň	Popis
Nízká	Zranitelnost neexistuje nebo je zneužití zranitelnosti málo pravděpodobné. Existují kvalitní bezpečnostní opatření, které jsou schopna včas detekovat možné slabiny nebo případné pokusy o překonání opatření.
Střední	Zranitelnost je málo pravděpodobná až pravděpodobná. Existují kvalitní bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné slabiny nebo případné pokusy o překonání opatření je omezena. Nejsou známé žádné úspěšné pokusy o překonání bezpečnostních opatření.
Vysoká	Zranitelnost je pravděpodobná až velmi pravděpodobná. Bezpečnostní opatření existují, ale jejich účinnost nepokrývá všechny potřebné aspekty a není pravidelně kontrolována. Jsou známé dílčí úspěšné pokusy o překonání bezpečnostních opatření.
Kritická	Zranitelnost je velmi pravděpodobná až po víceméně jisté zneužití. Bezpečnostní opatření nejsou realizována anebo je jejich účinnost značně omezena. Neprobíhá kontrola účinnosti bezpečnostních opatření. Jsou známé úspěšné pokusy překonání bezpečnostních opatření.

Stupnice pro hodnocení rizik

Riziko (Risk) je kombinace hrozby a zranitelnosti s dopadem na aktivum. Pro hodnocení je použita škála 1 - 4 (nízké - střední - vysoké - kritické).

Úroveň	Popis
Nízké	Riziko je považováno za přijatelné.
Střední	Riziko může být sníženo méně náročnými opatřeními nebo v případě vyšší náročnosti opatření je riziko přijatelné.
Vysoké	Riziko je dlouhodobě nepřípustné a musí být zahájeny systematické kroky k jeho odstranění.
Kritické	Riziko je nepřípustné a musí být neprodleně zahájeny kroky k jeho odstranění.