EVROPSKÁ UNIE
Evropský fond pro regionální rozvoj
Integrovaný regionální operační program

MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

čj. KrÚ 49987/2016

Pardubický kraj

Komenského náměstí 125, Pardubice 532 11

VÝZVA

k předložení nabídky

na veřejnou zakázku malého rozsahu

Zadavatel - Pardubický kraj tímto vyzývá k podání nabídky na veřejnou zakázku malé hodnoty

„Studie proveditelnosti projektu Rozšíření Regionální datové sítě I.“

1. Identifikační údaje zadavatele

Název:	Pardubický kraj
Právní forma:	Veřejnoprávní korporace
Sídlo:	Komenského náměstí 125, 532 11 Pardubice
IČ:	70892822
DIČ:	CZ70892822
Zastoupen:	JUDr. Martinem Netolickým, Ph.D., hejtmanem Pardubického kraje
Kontaktní osoba:	Mgr. Pavel Menšl, oddělení veřejných zakázek Tel: +420 466 026 282 / +420 605 551 501

Systémové číslo zakázky: P16V00000102
Profil zadavatele: https://zakazky.pardubickykraj.cz/

2. Předmět veřejné zakázky a předpokládaná hodnota

Jedná se o veřejnou zakázku malé hodnoty (dále jen „zakázka“) na služby, jejímž předmětem je zpracování podkladů včetně Studie proveditelnosti (dále jen Studie) a poskytnutí dalších služeb v rámci projektu Pardubického kraje „Rozšíření Regionální datové sítě I.“ Studie musí být zpracována v souladu s výzvou č. 28 – Specifické informační a komunikační systémy a infrastruktura II. (http://www.strukturalni-fondy.cz/cs/Microsites/IROP/Vyzvy/Vyzva-c-28-Specificke-informacni-a-komunikacni-systemy-a-infrastruktu) k předložení žádosti o podporu z Integrovaného regionálního operačního programu v aktuálním znění.

Podrobný rozsah a specifikace předmětu zakázky je součástí přílohy č. 3 této výzvy.

Text Studie proveditelnosti bude veřejným dokumentem.

Zadávání této zakázky nepodléhá zákonu č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů, vyjma povinnosti zadavatele postupovat v souladu se zásadami transparentnosti, rovného zacházení a zákazu diskriminace.

Společný slovník pro veřejné zakázky (CPV): 71241000-9 - Studie proveditelnosti, poradenství, analýza

Předpokládaná hodnota zakázky je 550 000,- Kč bez DPH.

3. Lhůta a místo pro podání nabídek

Lhůta pro podání nabídek je nejpozději do **22. 7. 2016 do 10:30 hodin**.

Místo pro podání nabídek prostřednictvím držitele poštovní licence:
Krajský úřad Pardubického kraje
Komenského náměstí 125
532 11 Pardubice

Místo pro podání nabídek osobně v pracovních dnech Po a St v době od 7:00 do 17:00 hod., ve dnech Út a Čt v době od 7:00 do 15:30 hod., v Pá v době od 7:00 do 14:30 hod. na adresu:
Krajský úřad Pardubického kraje
Podatelna (prostory Czech POINT)
Komenského náměstí 120
532 11 Pardubice

4. Požadavky na prokázání splnění kvalifikace

4.1. Zakázku může plnit dodavatel, který

a) nebyl pravomocně odsouzen pro trestný čin spáchaný ve prospěch organizované zločinecké skupiny, trestný čin účasti na organizované zločinecké skupině, legalizace výnosů z trestné činnosti, podílnictví, přijetí úplatku, podplacení, nepřímého úplatkářství, podvodu, úvěrového podvodu, včetně případů, kdy jde o přípravu nebo pokus nebo účastenství na takovém trestném činu, nebo došlo k zahlazení odsouzení za spáchání takového trestného činu*; jde-li o právnickou osobu, musí tento předpoklad splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu, a je-li statutárním orgánem dodavatele či členem statutárního orgánu dodavatele právnická osoba, musí tento předpoklad splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu této právnické osoby*; *podává-li nabídku zahraniční právnická osoba prostřednictvím své organizační složky, musí předpoklad podle tohoto písmene splňovat vedle uvedených osob rovněž vedoucí této organizační složky; tento základní kvalifikační předpoklad musí dodavatel splňovat jak ve vztahu k území České republiky, tak k zemi svého sídla, místa podnikání či bydliště*,

b) nebyl pravomocně odsouzen pro trestný čin, jehož skutková podstata souvisí s předmětem podnikání dodavatele podle zvláštních právních předpisů nebo došlo k zahlazení odsouzení za spáchání takového trestného činu; *jde-li o právnickou osobu, musí tuto podmínku splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu, a je-li statutárním orgánem dodavatele či členem statutárního orgánu dodavatele právnická osoba, musí tento předpoklad splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu této právnické osoby; podává-li nabídku zahraniční právnická osoba prostřednictvím své*

organizační složky, musí předpoklad podle tohoto písmene splňovat vedle uvedených osob rovněž vedoucí této organizační složky; tento základní kvalifikační předpoklad musí dodavatel splňovat jak ve vztahu k území České republiky, tak k zemi svého sídla, místa podnikání či bydliště,

c) v posledních 3 letech nenaplnil skutkovou podstatu jednání nekalé soutěže formou podplácení podle zvláštního právního předpisu,
d) respektive vůči jeho majetku neprobíhá nebo v posledních 3 letech neproběhlo insolvenční řízení, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh nebyl zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení, nebo nebyl konkurs zrušen proto, že majetek byl zcela nepostačující nebo zavedena nucená správa podle zvláštních právních předpisů,
e) není v likvidaci,
f) nemá v evidenci daní zachyceny daňové nedoplatky, a to jak v České republice, tak v zemi sídla, místa podnikání či bydliště dodavatele,
g) nemá nedoplatek na pojistném a na penále na veřejné zdravotní pojištění, a to jak v České republice, tak v zemi sídla, místa podnikání či bydliště dodavatele,
h) nemá nedoplatek na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti, a to jak v České republice, tak v zemi sídla, místa podnikání či bydliště dodavatele,
i) není veden v rejstříku osob se zákazem plnění veřejných zakázek,
j) nebyl v posledních 3 letech pravomocně potrestán uložením pokuty za umožnění výkonu nelegální práce podle zákona o zaměstnanosti,
k) vůči němuž nebyla v posledních 3 letech zavedena dočasná správa nebo v posledních 3 letech uplatněno opatření k řešení krize podle zákona upravujícího ozdravné postupy a řešení krize na finančním trhu.

K prokázání splnění tohoto předpokladu postačí předložení čestného prohlášení uchazeče podepsaného osobou oprávněnou jednat za uchazeče. Zadavatel nabízí uchazeči ke splnění tohoto požadavku vzorové čestné prohlášení, které tvoří přílohu č. 1 této výzvy.

4.2. Další doklady

Uchazeč dále doloží:

a) aktuální **výpis z obchodního rejstříku** či výpisu z jiné evidence, pokud je v ní zapsán

b) aktuální **doklad o oprávnění k podnikání** podle zvláštních právních předpisů v rozsahu odpovídajícím předmětu veřejné zakázky

c) seznam minimálně **4 realizovaných služeb** v posledních 3 letech v následující struktuře:
   ca) nejméně 3 realizované služby, jejichž předmětem byl design datových telekomunikačních služeb a sítí prostřednictvím optické infrastruktury, přičemž alespoň 2 z uvedených zakázek se musí týkat návrhu MPLS MANových sítí a musí být v minimálním celkovém realizovaném objemu 20 mil. Kč bez DPH.

   cb) nejméně 1 realizovaná služba, jejímž předmětem bylo zpracování zadávací dokumentace nadlimitní veřejné zakázky v rozsahu dle § 44 z. č. 137/2006 Sb., o veřejných zakázkách, týkající se dodávek v oblasti IT infrastruktury.

   Dodavatel je oprávněn prokázat realizaci služeb dle bodu ca), cb) jedinou realizovanou službou. Z čestného prohlášení pak musí vyplývat, že hodnota služeb dle bodu ca dosahuje požadovaného finančního objemu. Ustanovení tohoto odstavce se nedotýká povinnosti předložit nejméně 3 realizované služby dle bodu ca).

Zadavatel žádá uchazeče, aby seznam služeb dle bodu c) předložil ve formě čestného prohlášení, kde strukturovaně (v podobě tabulky) uvede následující údaje:

- identifikační údaje objednatele a kontaktní osoba;
- doba realizace předmětné zakázky;
- předmět zakázky včetně jeho stručného popisu;
- rozsah předmětných služeb.

d) doklady týkající se **odborného týmu**

Splnění tohoto požadavku uchazeč prokáže předložením seznamu členů odborného týmu, jež se bude podílet na plnění veřejné zakázky, bez ohledu na to, zda jde o zaměstnance uchazeče nebo osoby v jiném vztahu k uchazeči.

Zadavatel požaduje pro plnění předmětu veřejné zakázky nejméně **tříčlenný tým** odborných pracovníků zajišťující poskytnutí příslušných služeb.

Projektový manažer – 1x

Požadavky:
- minimálně 5 let praxe v oboru budování infrastruktury (sítě) pro přenos dat a informací,
- zkušenost s realizací (a účast) min. 2 projektů na zpracování odborné studie nebo studie proveditelnosti, na kterých se podílel, z toho nejméně v jednom případě v pozici projektového manažera,

Hlavní architekt řešení – 1x

Požadavky:
- minimálně 5 let praxe v oboru designu budování optické infrastruktury (sítě) pro přenos dat a informací,
- minimálně 5 let praxe v oboru návrhu MPLS MAN,
- zkušenost s realizací (a účast) min. 2 projektů, jejichž předmětem byl design datových telekomunikačních služeb a sítí prostřednictvím optické infrastruktury

Specialista provozu – 1x

Požadavky:
- minimálně 5 let praxe v administraci MPLS MAN
- minimálně 3 roky praxe v oboru designu budování optické infrastruktury (sítě) pro přenos dat a informací,

Zadavatel žádá uchazeče, aby shora uvedené předložil ve formě čestného prohlášení, jehož přílohou budou strukturované profesní životopisy jednotlivých pracovníků/členů týmu s přehledem profesní praxe a zkušeností takto:

- jméno, příjmení,
- úlohu v týmu a oblast dodávky nebo služeb, za kterou bude v rámci realizace zakázky odpovědný,
- kvalifikaci pro plnění úlohy v týmu,
- praxi
- zkušenosti (včetně kontaktu na objednatele projektů),
- čestné prohlášení člena týmu obsahující závazek účasti na této veřejné zakázce případně smlouvu mezi uchazečem a členem týmu (viz také bod 4.3. této výzvy)

Uchazeč je povinen zabezpečit, aby zakázku realizoval tým uvedený v nabídce; případná změna ve složení týmu podléhá schválení zadavatelem.

Doklady dle bodu 4.2. mohou být doloženy v prosté kopii.

4.3. Prokázání kvalifikace prostřednictvím subdodavatele
V případě, že uchazeč prokazuje část kvalifikačních předpokladů, vyjma předpokladů uvedených pod bodem 4.1. a 4.2.a) výzvy, prostřednictvím subdodavatele, přiloží do nabídky doklad (smlouvu se subdodavatelem nebo čestné prohlášení subdodavatele), ze kterého vyplývá povinnost a rozsah plnění subdodavatelského závazku.

5. Termín zahájení a dokončení plnění, místo plnění zakázky,

Předpokládaný termín zahájení plnění:	bezodkladně po podpisu smlouvy
Termín dokončení plnění:	Uchazeč (zhotovitel) předá kompletní dílo zadavateli (objednateli) do 6 měsíců od uzavření smlouvy a to včetně zapracování připomínek objednatele.
Místo realizace zakázky (dodání):	místem plnění a dodání veřejné zakázky je sídlo zadavatele Komenského náměstí 125, 532 11 Pardubice a sídlo zhotovitele

6. Údaje o hodnotících kritériích
Jediným kritériem pro hodnocení nabídek je nejnižší nabídková cena vč. DPH.

7. Způsob podání nabídek
Nabídky se podávají písemně v řádně uzavřené obálce opatřené označením: „Neotevírat – veřejná zakázka „Studie proveditelnosti projektu Rozšíření Regionální datové sítě I.“.
Nabídka bude předložena v jednom originále v českém jazyce v písemné formě, podepsána uchazečem či statutárním orgánem uchazeče či pověřeným zástupcem uchazeče. Všechny listy nabídky včetně příloh budou řádně očíslovány vzestupnou číselnou řadou.
Součástí nabídky bude vyplněný návrh smlouvy podepsaný osobou oprávněnou jednat za uchazeče a doklad, ze kterého toto oprávnění vyplývá (např. výpis z obchodního rejstříku). Jednotlivé listy nabídky nesmí obsahovat překlepy, přepisy, škrty či jiné úpravy, které by mohly zadavatele uvést v omyl.
Nabídka bude předložena v jednom originálním vyhotovení a v jedné kopii odpovídající originálu, tj. tato kopie bude taktéž odevzdána ve vytištěné, pevně spojené podobě tak, aby bylo zabráněno ztrátě či výměně jednotlivých listů. Zadavatel požaduje, aby uchazeč předložil svoji nabídku také v elektronické formě ve formátu DOC nebo PDF na datovém nosiči (CD, DVD), který bude vyjímatelně přiložen k originálu nabídky. Nedodání kopie nabídky není důvodem pro vyřazení nabídky ze zadávacího řízení.
Při rozporu písemného a elektronického vyhotovení nabídky je vždy rozhodující originál v písemné podobě
Nabídka musí obsahovat následující údaje a bude členěna podle následujících bodů:
- Krycí list nabídky (příloha č. 2 této výzvy)
- Doklady o splnění kvalifikačních předpokladů dle bodu 4 této výzvy
- Doplněný návrh smlouvy včetně přílohy. Uchazeč doplní v návrhu smlouvy místa označená červeně slovy: doplní uchazeč.

Zájemce je oprávněn doplnit nabídku též o další doklady nebo informace vztahující se k předmětu zakázky.

8. Požadavky na zpracování nabídkové ceny

8.1. Celková nabídková cena za kompletní plnění předmětu zakázky bude uvedena absolutní částkou v českých korunách a bude stanovena jako nejvýše přípustná po celou dobu plnění zakázky. Ceny musí být uvedeny bez DPH, částka DPH a včetně DPH. Nabídkovou cenu uchazeč uvede v krycím listu a v návrhu smlouvy.
8.2. Nabídková cena musí obsahovat veškeré náklady uchazeče nutné k realizaci předmětu této zakázky. Cena může být měněna pouze v souvislosti se změnou daňových předpisů majících prokazatelný vliv na uvedenou cenu.

9. Dodatečné informace

Dodavatelé jsou oprávněni po zadavateli požadovat dodatečné informace k zadávacím podmínkám. Žádost o dodatečné informace se podává písemně kontaktní osobě na adresu uvedenou pod bodem 1 této výzvy, do datové schránky zadavatele nebo e-mailem na pavel.mensl@pardubickykraj.cz. (v kopii na vladimir.rimanek@pardubickykraj.cz).
Telefonické dotazy nebudou akceptovány.

Žádost musí být zadavateli doručena nejpozději 4 pracovní dny před uplynutím lhůty pro podání nabídek. Dodatečné informace může zadavatel poskytnout i bez předchozí žádosti. Zadavatel odešle dodatečné informace k zadávacím podmínkám, případně související dokumenty, nejpozději do 2 pracovních dnů po doručení žádosti.

10. Obchodní a platební podmínky

10.1. Uchazeč je povinen respektovat obchodní a platební podmínky uvedené ve vzorovém návrhu smlouvy, který tvoří přílohu č. 3 této výzvy.
10.2. Pokud uchazeč nebude respektovat shora uvedené obchodní a platební podmínky a do svého návrhu smlouvy zařadí obchodní a platební podmínky méně výhodné (např. nedodrží stanovené minimální, popř. maximální hodnoty), popř. některou z obchodních či platebních podmínek do svého návrhu smlouvy vůbec neuvede nebo doplní shora uvedené obchodní a platební podmínky o ustanovení jakkoliv zhoršující postavení zadavatele, posoudí toto jednání zadavatel jako nesplnění zadávacích podmínek s následkem vyloučení příslušného uchazeče ze zadávacího řízení.

11. Zadavatel si vyhrazuje právo

- zrušit zadávací řízení bez uvedení důvodu, nejpozději však do uzavření smlouvy
- nevracet podané nabídky
- upřesnit podmínky zakázky
- vyloučit ze soutěže uchazeče, jehož nabídka nebude splňovat podmínky stanovené ve výzvě
- vyžádat si od uchazeče písemné doplnění nabídky a ověřit si informace uvedené uchazečem v nabídce
- nehradit náklady, které uchazeči vznikly v souvislosti s podáním nabídky
- zadavatel nepřipouští variantní řešení nabídek
- uzavřít smlouvu s dodavatelem, který se umístí jako druhý v pořadí, pokud vítězný dodavatel odmítne poskytnout potřebnou součinnost vedoucí k uzavření smlouvy ve lhůtě 15 dnů nebo s dodavatelem, který se umístí jako třetí v pořadí, pokud v pořadí druhý dodavatel odmítne poskytnout potřebnou součinnost vedoucí k uzavření smlouvy ve lhůtě shora.

12. Ostatní požadavky

Zadavatel stanoví, že nepřipouští analogické použití § 101 zákona - zvýhodnění dodavatelů zaměstnávajících osoby se zdravotním postižením.

13. Přílohy:

Příloha č. 1: Čestné prohlášení
Příloha č. 2: Krycí list
Příloha č. 3: Návrh smlouvy vč. přílohy
Příloha č. 4: Studie rozvoje komunikační infrastruktury

V Pardubicích dne: 30. 6. 2016

Mgr. Pavel Menšl
vedoucí oddělení veřejných zakázek
pověřený hejtmanem
schváleno usnesením Rady Pk dne 30. 6. 2016, usnesení R/2695/16

Příloha č. 1 výzvy

„Studie proveditelnosti projektu Rozšíření Regionální datové sítě I.“

Čestné prohlášení o splnění kvalifikačních předpokladů:

Prohlašuji tímto čestně, že dodavatel:

a) nebyl pravomocně odsouzen pro trestný čin spáchaný ve prospěch organizované zločinecké skupiny, trestný čin účasti na organizované zločinecké skupině, legalizace výnosů z trestné činnosti, podílnictví, přijetí úplatku, podplacení, nepřímého úplatkářství, podvodu, úvěrového podvodu, včetně případů, kdy jde o přípravu nebo pokus nebo účastenství na takovém trestném činu, nebo došlo k zahlazení odsouzení za spáchání takového trestného činu*; jde-li o právnickou osobu, musí tento předpoklad splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu, a je-li statutárním orgánem dodavatele či členem statutárního orgánu dodavatele právnická osoba, musí tento předpoklad splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu této právnické osoby*; *podává-li nabídku zahraniční právnická osoba prostřednictvím své organizační složky, musí předpoklad podle tohoto písmene splňovat vedle uvedených osob rovněž vedoucí této organizační složky; tento základní kvalifikační předpoklad musí dodavatel splňovat jak ve vztahu k území České republiky, tak k zemi svého sídla, místa podnikání či bydliště*,
b) nebyl pravomocně odsouzen pro trestný čin, jehož skutková podstata souvisí s předmětem podnikání dodavatele podle zvláštních právních předpisů nebo došlo k zahlazení odsouzení za spáchání takového trestného činu; *jde-li o právnickou osobu, musí tuto podmínku splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu, a je-li statutárním orgánem dodavatele či členem statutárního orgánu dodavatele právnická osoba, musí tento předpoklad splňovat jak tato právnická osoba, tak její statutární orgán nebo každý člen statutárního orgánu této právnické osoby; podává-li nabídku zahraniční právnická osoba prostřednictvím své organizační složky, musí předpoklad podle tohoto písmene splňovat vedle uvedených osob rovněž vedoucí této organizační složky; tento základní kvalifikační předpoklad musí dodavatel splňovat jak ve vztahu k území České republiky, tak k zemi svého sídla, místa podnikání či bydliště*,
c) v posledních 3 letech nenaplnil skutkovou podstatu jednání nekalé soutěže formou podplácení podle zvláštního právního předpisu,
d) respektive vůči jeho majetku neprobíhá nebo v posledních 3 letech neproběhlo insolvenční řízení, v němž bylo vydáno rozhodnutí o úpadku nebo insolvenční návrh nebyl zamítnut proto, že majetek nepostačuje k úhradě nákladů insolvenčního řízení, nebo nebyl konkurs zrušen proto, že majetek byl zcela nepostačující nebo zavedena nucená správa podle zvláštních právních předpisů,
e) není v likvidaci,
f) nemá v evidenci daní zachyceny daňové nedoplatky, a to jak v České republice, tak v zemi sídla, místa podnikání či bydliště dodavatele,
g) nemá nedoplatek na pojistném a na penále na veřejné zdravotní pojištění, a to jak v České republice, tak v zemi sídla, místa podnikání či bydliště dodavatele,
h) nemá nedoplatek na pojistném a na penále na sociální zabezpečení a příspěvku na státní politiku zaměstnanosti, a to jak v České republice, tak v zemi sídla, místa podnikání či bydliště dodavatele,
i) není veden v rejstříku osob se zákazem plnění veřejných zakázek,
j) nebyl v posledních 3 letech pravomocně potrestán uložením pokuty za umožnění výkonu nelegální práce podle zákona o zaměstnanosti,

k) vůči němuž nebyla v posledních 3 letech zavedena dočasná správa nebo v posledních 3 letech uplatněno opatření k řešení krize podle zákona upravujícího ozdravné postupy a řešení krize na finančním trhu.

V …….. dne …….

Toto prohlášení podepisuji jako …… Podpis:

(např. dodavatel fyzická osoba, předseda představenstva a.s., jednatel (é) společnosti s r.o. atd., jedná se pouze o demonstrativní výčet, podepisování se děje způsobem zapsaným v OR)

Příloha č. 2

Krycí list nabídky

Obchodní firma, jméno uchazeče	
Sídlo/místo trvalého pobytu uchazeče	
Adresa pro poštovní styk	
Kontaktní osoba ve věci zakázky, emailová adresa, kontaktní adresa, telefon	
Právní forma uchazeče	
IČ uchazeče (bylo – li přiděleno)	
Jméno a funkce statutárního orgánu	
Jméno, příjmení a podpis osoby oprávněné jednat za uchazeče	

VYPLNÍ UCHAZEČ	**Cena v Kč bez DPH CELKEM**	**Sazba DPH v Kč**	**Cena v Kč včetně DPH CELKEM**
Nabídková cena	0,00	0,00	0,00

Tyto údaje jsou závaznou součástí nabídky a budou využity v rámci procesu hodnocení nabídek. Rozhodující jsou však údaje uvedené ve smlouvě a jejích přílohách.

Příloha č. 3

Návrh smlouvy

Smlouva č. OR/16/XXXXX
na dodávku studie proveditelnosti „Rozšíření Regionální datové sítě I.“

Smluvní strany

1. Objednatel: **Pardubický kraj**
Komenského náměstí 125
532 11 Pardubice
zastoupen: JUDr. Martinem Netolickým Ph. D., hejtmanem Pardubického kraje
Osoba oprávněná jednat ve věcech technických:
Jan Czagan, David Rezler
Bankovní spojení: ČSOB, a. s. Pardubice
č.ú. 239602855/0300
IČ: 708 92 822
DIČ: CZ 708 92 822

2. Zhotovitel: název *(doplní uchazeč)*
adresa *(doplní uchazeč)*
Zapsaný v obchodním rejstříku Krajského soudu v *(doplní uchazeč)*,
spisová značka: *(doplní uchazeč)*
zastoupen: *(doplní uchazeč)*
Osoba oprávněná jednat ve věcech technických: *(doplní uchazeč)*
Bankovní spojení: *(doplní uchazeč)*
č. ú. *(doplní uchazeč)*
IČ: *(doplní uchazeč)*
DIČ: *(doplní uchazeč)*

Článek I.
Předmět smlouvy

1.1 Předmětem smlouvy je závazek zhotovitele provést pro objednatele níže uvedené dílo řádně, v dohodnutém termínu a v kvalitě níže specifikované, tj. zejména bez vad a nedodělků.

1.2 Objednatel se zavazuje při provádění díla řádně spolupůsobit a zhotoviteli řádně provedené dílo zaplatit, a to za podmínek a v termínech touto smlouvou sjednaných.

1.3 Zhotovitel prohlašuje, že na základě svých odborných znalostí a zkušeností je schopen poskytnout objednateli předmět díla v požadovaném termínu, rozsahu a kvalitě.

1.4 Zhotovitel prohlašuje, že se seznámil s rozsahem a povahou díla. Jsou mu známy veškeré technické, kvalitativní a jiné podmínky nezbytné k realizaci díla a disponuje takovými kapacitami a odbornými znalostmi, které jsou nezbytné pro realizaci díla za cenu stanovenou dle čl. 4 této Smlouvy.

1.5 Zhotovitel se zavazuje, že předmět této Smlouvy provede v souladu s právními předpisy, jakož i v souladu se všemi normami obsahujícími technické specifikace a technická řešení, technické a technologické postupy a další kritéria zajišťující, že materiály, výrobky, postupy a služby jsou vyhovující a dostatečné pro zhotovení díla. V případě porušení tohoto ustanovení má objednatel právo od smlouvy odstoupit a požadovat po zhotoviteli smluvní pokutu dle článku 8, a to za každý jednotlivý případ porušení.

1.6 Zhotovitel prohlašuje, že předmět plnění dle této Smlouvy není plněním nemožným a pečlivě zvážil všechny možné důsledky uzavření této Smlouvy.

1.7 Smlouva je uzavřena na základě zadávacího řízení k veřejné zakázce malého rozsahu, systémové číslo P16V00000102 s názvem „Studie proveditelnosti projektu Rozšíření Regionální datové sítě I.“.

Článek II.
Specifikace díla

2.1 Předmětem díla je

a) analýza současného stavu sítí, současných i budoucích potřeb objednatele a vybraných subjektů na území Pardubického kraje s ohledem na možnosti technického i finančního řešení.

b) zpracování Studie proveditelnosti projektu „Rozšíření Regionální datové sítě I.“,

c) poskytnutí potřebné součinnosti při zapracování připomínek a nutných změn v průběhu posuzování Studie proveditelnosti kontrolními orgány a Odborem hlavního architekta eGovernmentu,

d) Vypracování podrobné specifikace rozsahu a parametrů díla pro zadávací dokumentaci k vyhlášení zadávacího řízení, které bude navazovat na výsledky provedené studie.

2.2 Rozsah díla je specifikován v příloze č. 1 této smlouvy.

Článek III.
Doba a místo plnění

3.1 Všechny části veřejné zakázky budou realizovány a předány jako kompletní dílo do 6 měsíců od uzavření smlouvy, a to včetně zapracování všech připomínek objednatele. Harmonogram jednotlivých etap představí zhotovitel objednateli na prvním společném jednání a bude vycházet z reálných možností všech zúčastněných stran a odbornosti zhotovitele.:

3.2 Připomínky objednatele k plnění zhotovitele ve smyslu odst. 3.1 budou poskytnuty bezodkladně, nejpozději však dle podmínek přílohy č. 1 této Smlouvy. Neposkytne-li objednatel připomínky v termínu dle předchozí věty, je zhotovitel oprávněn písemně vyzvat objednatele k jejich poskytnutí. Ode dne doručení takové písemné výzvy k poskytnutí připomínek objednateli do dne jejich poskytnutí není zhotovitel v prodlení s plněním díla.

3.3 Místem plnění jsou prostory zhotovitele, případně po domluvě obou smluvních stran prostory objednatele.

Článek IV.
Cena díla a platební podmínky

4.1 Cena za celé provedené a předané dílo je stanovena jako cena pevná, tj. zahrnuje veškeré náklady zhotovitele související s provedením díla. Dále jsou součástí ceny i služby a dodávky, které nejsou výslovně uvedeny, ale zhotovitel, jakožto odborník o nich ví nebo vědět musel, neboť jsou nezbytné k provedení díla.

4.2 Cena za provedení díla dle článku 2 této Smlouvy:

(doplní uchazeč) Kč bez DPH

(doplní uchazeč) Kč DPH v sazbě 21 %

(doplní uchazeč) Kč včetně DPH

4.3 Právo fakturovat vzniká zhotoviteli až po akceptaci předmětu plnění bez výhrad, a to na základě příslušného akceptačního protokolu.

4.4 Vyúčtování ceny za provedení díla provede zhotovitel na základě daňového dokladu - faktury splňující veškeré podstatné náležitosti dle zvláštních právních předpisů, zejména zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů a zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů4.5 Faktura musí obsahovat číslo jednací smlouvy, název projektu, číslo účtu zhotovitele a všechny údaje uvedené v § 28 odst. 2, zákona č. 235/2004 Sb., o dani z přidané hodnoty, v platném znění a náležitosti obchodní listiny ve smyslu ustanovení § 435 zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů. Společně s fakturou zhotovitel poskytne kopii akceptačního protokolu podepsaného pověřenými zástupci obou smluvních stran.

4.6 Součástí faktury bude specifikace dodaného plnění tak, aby byla v souladu s platnými účetními a daňovými předpisy, a to za účelem řádného vedení evidence majetku objednatele v souladu s těmito právními předpisy.

4.7 Faktura je splatná do 30 kalendářních dnů ode dne jejího doručení objednateli.

4.8 Objednatel je oprávněn do data splatnosti vrátit fakturu, která neobsahuje požadované náležitosti nebo není doložena kopií potvrzeného příslušného akceptačního protokolu, a která obsahuje jiné cenové údaje nebo jiný druh plnění než dohodnuté ve Smlouvě s tím, že doba splatnosti nové (opravené) faktury začíná znovu běžet ode dne jejího doručení objednateli.

4.9 Faktura je považována za proplacenou okamžikem odepsání příslušné částky z účtu objednatele ve prospěch účtu zhotovitele.

4.10 Smluvní strany se dohodly, že objednatel neposkytuje zhotoviteli zálohy.

Článek V.
Práva a povinnosti smluvních stran

5.1 Smluvní strany se zavazují vzájemně spolupracovat a poskytovat si veškeré informace potřebné pro řádné plnění svých závazků. Smluvní strany jsou povinny informovat druhou smluvní stranu o veškerých skutečnostech, které jsou nebo mohou být důležité pro řádné plnění této Smlouvy.

5.2 Smluvní strany jsou povinny plnit své závazky vyplývající z této Smlouvy takovým způsobem, aby nedocházelo k prodlení s plněním jednotlivých termínů a k prodlení splatnosti jednotlivých peněžních závazků.

5.3 Veškerá komunikace mezi smluvními stranami bude probíhat prostřednictvím oprávněných osob, nebo jimi pověřených osob, nebo statutárního orgánu smluvních stran.

5.4 Všechna oznámení mezi smluvními stranami, která se vztahují k této Smlouvě, nebo která mají být učiněna na základě této Smlouvy, musí být učiněna v písemné podobě a druhé straně doručena buď osobně, nebo doporučeným dopisem či jinou formou prostřednictvím doručovatelských a kurýrních společností na adresu sídla smluvních stran, není-li stanoveno, nebo mezi smluvními stranami dohodnuto jinak.

5.5 Ukládá-li Smlouva doručit některý dokument v písemné podobě, může být doručen buď v papírové formě, nebo v elektronické (digitální) formě jako dokument textového procesoru MS Word verze 2007 a vyšší na dohodnutém médiu.

5.6 Zhotovitel se zavazuje, že provede dílo řádně a včas.

5.7 Zhotovitel bude postupovat při plnění předmětu Smlouvy s odbornou péčí, podle nejlepších znalostí a schopností, sledovat a chránit oprávněné zájmy objednatele a postupovat v souladu s jeho pokyny a interními předpisy souvisejícími s předmětem plnění Smlouvy, které objednatel zhotoviteli poskytne nebo s pokyny jím pověřených osob.

5.8 Objednatel poskytne zhotoviteli veškerou nezbytnou součinnost k naplnění účelu Smlouvy.

5.9 Zhotovitel se v souladu s § 2 písm. e) zákona č. 320/2001 Sb., o finanční kontrole ve veřejné správě a o změně některých zákonů ve znění pozdějších právních předpisů stane v rámci zhotovování osobou povinnou spolupůsobit při výkonu finanční kontroly, plnit veškeré povinnosti, které mu jsou z tohoto důvodu tímto zákonem uloženy. Tímto nejsou dotčeny ostatní povinnosti zhotovitele vyplývající ze Smlouvy.

5.10 Zhotovitel je povinen minimálně do konce roku 2028 poskytovat požadované informace a dokumentaci související s realizací projektu zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu a poskytnout jim při provádění kontroly součinnost.

5.11 Objednatel má povinnost převzít kompletní dílo v termínu uvedeném v čl. 3 této Smlouvy.

5.12 Objednatel je povinen zaplatit zhotoviteli cenu za dílo v souladu s ustanovením čl. 4 Smlouvy.

Článek VI.
Převzetí díla

6.1 Zhotovitel umožní objednateli kontrolu provádění kvality prací a dodržování sjednaného termínu plnění.

6.2 Za účelem předání částí díla (etapy) blíže specifikovaných v příloze č. 1 této Smlouvy budou mezi smluvními stranami sepsány předávací protokoly, ve kterých bude jednoznačně specifikováno, které části díla objednatel přebírá a dále zde bude uvedena specifikace případných nedodělků včetně způsobu a termínu pro jejich odstranění.

6.3 Předávací protokol bude podepsán oprávněnými zástupci obou smluvních stran.

6.4 Po řádném předání etapy díla, případně po odstranění nedodělků v termínech uvedených v předávacím protokolu, budou mezi smluvními sepsány akceptační protokoly, které budou podepsány oprávněnými zástupci obou smluvních stran. V akceptačním protokolu mohou být uvedeny 3 stavy:

Akceptováno bez výhrad.

V případě, že Objednatel v průběhu kontroly nenalezne v předaném plnění žádné vady ani nedodělky, uvede Objednatel do zápisu, že kontrolované plnění bylo akceptováno bez výhrad a protokol potvrdí svým podpisem.

Akceptováno s výhradami.

V případě, že budou v průběhu kontroly shledány vady nebo nedodělky, dohodnou se objednatel a zhotovitel na termínu, do kterého zhotovitel tyto vady a nedodělky odstraní. Objednatel do protokolu uvede seznam vad nebo nedodělků s termíny jejich odstranění a obě strany protokol potvrdí svým podpisem. Po odstranění vad se kontrolní procedura opakuje.

Neakceptováno.

V případě, že budou v průběhu kontroly nalezeny takové vady a nedodělky, které by bránily v budoucím užití díla, není dílo akceptováno. Obě strany se dohodnou na termínu nové kontroly, do které zhotovitel dílo přepracuje. Do zápisu se uvede, že plnění akceptováno nebylo. Po přepracování díla vyzve objednatel zhotovitele k provedení nové kontroly.

Článek VII.
Vlastnické právo k dílu

7.1 Vlastnické právo k hmotným součástem díla přechází na objednatele uhrazením ceny za takové hmotné součásti díla. Do doby než na objednatele přejde vlastnické právo k hmotným součástem díla, poskytuje zhotovitel objednateli k takové součásti díla oprávnění k výkonu práva jej užít všemi způsoby nezbytnými pro splnění účelu Smlouvy. Cena za hmotné součásti díla je již zahrnuta v ceně díla.

Článek VIII.
Smluvní pokuta a úrok z prodlení

8.1 Při prodlení se splněním kteréhokoliv termínu dle čl. 3.1 zaplatí zhotovitel smluvní pokutu ve výši 0,05 % z celkové ceny díla za každý započatý den prodlení.

8.2 Neodpovídá-li předmět smlouvy všem požadavkům vyplývajícím z čl. 1.5., má objednatel právo odstoupit od Smlouvy a dále právo na smluvní pokutu ve výši 100.000,- Kč za každý jednotlivý případ porušení.

8.3 Při nedodržení doby splatnosti faktury Objednatelem je Zhotovitel oprávněn požadovat úhradu úroku z prodlení. Výše úroku z prodlení činí nejvýše 0,05 % z fakturované částky za každý den prodlení.

8.4 V případě porušení závazku mlčenlivosti nebo ochrany důvěrných informací vyplývajících z článku 10 této Smlouvy má druhá smluvní strana právo účtovat smluvní pokutu ve výši 100.000 Kč za každý jednotlivý případ porušení.

8.5 Splatnost smluvních pokut činí 30 kalendářních dnů od doručení nároku na její uhrazení druhé smluvní straně.

Článek IX.
Náhrada újmy

9.1 Zaplacením smluvní pokuty není dotčeno právo smluvních stran na úhradu způsobené újmy vzniklé v souvislosti s plněním předmětu Smlouvy v plné výši.

9.2 Zhotovitel odpovídá za způsobenou újmu porušením povinnosti dle této Smlouvy, opomenutím nebo zásadně nekvalitním prováděním smluvní činnosti v plné výši.

9.3 Náhrada újmy se řídí platnými ustanoveními vztahujícími se k náhradě majetkové a nemajetkové újmy stanovené zákonem č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů.

9.4 Jakákoliv ustanovení týkající se omezení výše či druhu škody se nepřipouští.

Článek X.

Ochrana informací

10.1. Smluvní strany se zavazují zachovávat mlčenlivost ohledně skutečností, které se v souvislosti s plněním Smlouvy dozvěděly nebo které označily za důvěrné, jakož i údajů dle zákona č. 89/1995 Sb. (dále jen „důvěrné informace"). Zhotovitel je povinen přijmout opatření k ochraně důvěrných informací. Důvěrné informace mohou být zhotovitelem použity výhradně k plnění Smlouvy.

10.2. Zhotovitel nesdělí či nezpřístupní žádnou z důvěrných informací třetím osobám, nevyužije ji k vlastnímu prospěchu nebo jinak nezneužije. Povinnost mlčenlivosti a zachování důvěrnosti informací se nevztahuje na informace, které se staly obecně známými za předpokladu, že se tak nestalo porušením některé z povinností vyplývajících ze Smlouvy nebo o kterých tak stanoví zákon, zpřístupnění je však možné vždy jen v nezbytném rozsahu. V případě porušení závazku mlčenlivosti či ochrany důvěrných informací je objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 100.000,- Kč za každý jednotlivý případ porušení závazku.

10.3. Smluvní strany jsou povinny chránit osobní údaje. Pro případ, že se v rámci plnění předmětu Smlouvy dostane smluvní strana do kontaktu s osobními údaji, bude je ochraňovat a nakládat s nimi plně v souladu s příslušnými právními předpisy, a to i po ukončení plnění Smlouvy. Strany se v případě kontaktu s osobními údaji, ve smyslu příslušných ustanovení zákona č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, zavazují uzavřít dodatek ke Smlouvě spočívající v dohodě o zpracování osobních údajů. Zhotovitel se rovněž zavazuje pro případ, že se v průběhu plnění předmětu veřejné zakázky dostane do kontaktu s údaji objednatele vyplývajícími z jeho provozní činnosti, tyto údaje v žádném případě nezneužít, nezměnit, ani jinak poškodit, ztratit či znehodnotit. V případě porušení závazku ochrany osobních údajů je Objednatel oprávněn požadovat zaplacení smluvní pokuty ve výši 100.000,- Kč za každý jednotlivý případ porušení tohoto závazku;

10.4. Obě smluvní strany se zavazují, že zachovají jako důvěrné informace a zprávy týkající se vlastní spolupráce a vnitřních záležitostí smluvních stran a předmětu Smlouvy, pokud by jejich zveřejnění mohlo poškodit druhou smluvní stranu. Povinnost poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, není tímto ustanovením dotčena.

10.5. Poskytovatel bude považovat za důvěrné informace takové informace, které budou jako důvěrné označené, nebo informace, u kterých se z povahy věci dá předpokládat, že se jedná o informace podléhající závazku mlčenlivosti, nebo informace o Objednateli, které by mohly z povahy věci být považovány za důvěrné a které se Zhotovitel dozví v souvislosti s plněním Smlouvy.

10.6. Zhotovitel je povinen svého případného subdodavatele zavázat povinností mlčenlivosti a respektováním práv Objednatele nejméně ve stejném rozsahu, v jakém je v tomto závazkovém vztahu zavázán sám.

10.7. Za prokázané porušení ustanovení v tomto článku výslovně uvedeném má druhá smluvní strana právo požadovat náhradu majetkové a nemajetkové újmy.

Článek XI.

Ukončení smluvního vztahu

11.1 Smluvní strany jsou oprávněny odstoupit od této Smlouvy z důvodů uvedených v zákoně a v této Smlouvě a dále z důvodu podstatného porušení této Smlouvy ve smyslu ustanovení § 2001 a násl. zákona č. 89/2012 Sb., občanský zákoník.

11.2 Za podstatné porušení Smlouvy ze strany Zhotovitele se považuje zejména, nikoliv však výlučně, prodlení zhotovitele s předáním předmětu plnění delší než 30 dnů, a dále porušení

jakékoliv povinnosti zhotovitele vyplývající ze Smlouvy a její nesplnění ani v dodatečné přiměřené lhůtě, kterou objednatel dodavateli k tomu poskytne (nevylučuje-li to charakter porušené povinnosti); v pochybnostech se má za to, že dodatečná lhůta je přiměřená, pokud činila alespoň 5 dnů. Odstoupení od Smlouvy ze strany objednatele není spojeno s uložením jakékoliv sankce k jeho tíži.

11.3 Odstoupení od Smlouvy nabývá účinnosti dnem doručení písemného oznámení o odstoupení od smlouvy druhé smluvní straně na adresu jejího sídla uvedenou v záhlaví této Smlouvy. Smluvní strany se dohodly, že odstoupení od Smlouvy se považuje za doručené 10. dnem po jeho uložení u provozovatele poštovních služeb, resp. výslovným odmítnutím přijetí odstoupení druhou smluvní stranou.

11.4 V případě ukončení platnosti Smlouvy z jakéhokoli důvodu má Zhotovitel v každém případě nárok na náhradu prokázaných nákladů, které vzniknou v souvislosti s náhradním řešením, zejména nákladů s pověřením jiných obchodních společností.

Článek XII.
Práva třetích osob a licenční ujednání

12.1 Zhotovitel prohlašuje, že předmět Smlouvy nebude zatížen právy třetích osob, ze kterých by pro Objednatele plynuly jakékoliv další finanční nebo jiné nároky ve prospěch třetích stran. V opačném případě Zhotovitel ponese veškeré důsledky takového porušení práv třetích osob.

12.2 Požívá-li dílo, které je předmětem této smlouvy, ochrany podle zákona č. 121/2000 Sb., autorský zákon, ve znění pozdějších předpisů, je Objednatel na základě této Smlouvy oprávněn užít toto dílo v neomezeném územním a množstevním rozsahu, a ke všem způsobům užití, zejména jej zveřejňovat, upravovat, spojovat s jiným dílem, zařazovat do souborného díla a uvádět jej pod svým jménem, k čemuž Zhotovitel poskytuje Objednateli výhradní oprávnění k užití práv duševního vlastnictví včetně možnosti zcela nebo zčásti poskytnout třetí osobě oprávnění tvořící součást licence a je povinen výše uvedenými povinnostmi zavázat i své případné subdodavatele, budou-li se na realizaci zakázky podílet. Odměna za výše uvedená oprávnění je již zahrnuta v ceně za provedení předmětu této Smlouvy.

12.3 Zhotovitel se zavazuje, že bez předchozího výslovného písemného souhlasu objednatele nepostoupí ani nepřevede jakákoliv práva či povinnosti vyplývající ze Smlouvy na třetí osobu či osoby.

Článek XIII.
Závěrečná ustanovení

13.1 Pokud tato smlouva nestanoví jinak, řídí se právní vztahy jí založené z. č. 89/2012 Sb., občanský zákoník. Pokud některé smluvní ustanovení odkazuje na právní předpis, který bude v průběhu doby trvání této smlouvy novelizován nebo bude přijat (nabude účinnosti) předpis nový, který jej nahradí, budou se smluvní strany při plnění předmětu této smlouvy vždy řídit příslušným aktuálně platným a účinným předpisem upravujícím danou záležitost.

13.2 Tuto smlouvu lze měnit a doplňovat jen písemnými dodatky očíslovanými vzestupnou číselnou řadou a podepsanými oprávněnými zástupci obou smluvních stran.

13.3 Při nebezpečí prodlení se za řádně doručené oznámení považuje i oznámení učiněné telefonicky či e-mailem s tím, že bude příslušnou smluvní stranou následně potvrzeno a předáno písemně v listinné podobě.

13.4 Tato smlouva je platná a účinná dnem jejího podpisu oběma smluvními stranami.

13.5 Tato smlouva se vyhotovuje ve čtyřech stejnopisech, každá strana obdrží dva stejnopisy.

13.6 Smluvní strany jsou povinny zajistit, aby v případě jejich rozdělení, sloučení, jakékoliv jiné přeměně nebo převodu práv na dceřiné společnosti byl právní nástupce zavázán stejně jako smluvní strana této smlouvy a aby v takovém případě nedošlo ke zkrácení práv druhé strany.

13.7 Smluvní strany se dohodly, že objednatel bezodkladně, nejpozději do 30 dnů, po uzavření této smlouvy odešle smlouvu k řádnému uveřejnění do registru smluv vedeného Ministerstvem vnitra ČR.

13.8 Smluvní strany potvrzují, že si tuto smlouvu před jejím podpisem přečetly, porozuměly jejímu obsahu, uzavírají ji svobodně a vážně. Na důkaz toho připojují své níže uvedené podpisy.

13.9 Schváleno na jednání Rady Pardubického kraje dne **. **. 2016 usnesením č. R/****/16.

V Pardubicích dne:

Za objednatele:

_____

Pardubický kraj
JUDr. Martin Netolický Ph. D.
hejtman

V *(doplní uchazeč)* dne:

Za zhotovitele:

_____

(doplní uchazeč)

Příloha č. 1 smlouvy

Podrobný rozsah a specifikace předmětu zakázky

1. Obecné požadavky

Objednatel očekává samostatný způsob práce za součinnosti realizačního týmu projektu na straně objednatele a to zejména ve fázi získávání informací pro analytickou část od zainteresovaných osob a subjektů a při vyhledávání a mapování informačních zdrojů v rámci ČR a EU.

Při zpracování předmětu této veřejné zakázky bude zhotovitel rovněž spolupracovat s dodavateli třetích stran, zajišťujícími smluvní servis a podporu dotčených zařízení a informačních systémů.

Objednatel požaduje při analytickém šetření s klíčovými subjekty osobní formou jednání (tedy ne např. dotazníkové šetření), pokud nebude realizačním týmem schváleno jinak. Každé jednání bude s dostatečným předstihem dohodnuto s příslušnou osobou nebo subjektem, bude o něm proveden zápis a následně předložen objednateli.

Každá z etap je na konci připomínkována objednatelem a zhotovitel poté připomínky zapracovává. Objednatel si vymiňuje u některých etap i prezentaci průběžných výsledků zhotovitelem pro realizační tým.

Objednatel předpokládá čas pro připomínkování jednotlivých částí zhruba 7 pracovních dní, u oponentury zadávací dokumentace čas dvakrát delší. Objednatel si vymezuje možnost přizvat k odbornému připomínkování třetí osobu.

Objednatel předpokládá vysokou odbornost a zkušenost zhotovitele. Zhotovitel je povinen upozorňovat objednatele na nevýhody jednotlivých řešení a v případě lepší varianty navrhovat tuto variantu.

Předmět zakázky bude realizován v etapách. Začíná první a podmínkou začátku realizace každé další etapy je akceptace cílového stavu předchozí etapy objednatelem. Každá etapa vychází z výsledků etap předchozích (číselně nižších).

První etapa

Předmětem plnění této etapy je analýza současného stavu sítě, současných i budoucích potřeb objednatele a vybraných subjektů na území Pardubického kraje (dále také jen kraje) s ohledem na možnosti technického i finančního řešení.

Druhá etapa

Předmětem této etapy je zpracování Studie proveditelnosti (dále jen Studie) v souladu s vyhlášenou výzvou č. 28 Specifické informační a komunikační systémy a infrastruktura II.

Třetí etapa

V této etapě je vyžadována součinnost zhotovitele při zapracování připomínek a nutných změn v průběhu posuzování Studie proveditelnosti kontrolními orgány a Odborem hlavního architekta eGovernmentu.

Čtvrtá etapa

V rámci plnění této etapy zpracovatel vyhotoví pro objednatele podrobné specifikace rozsahu a parametrů díla pro zadávací dokumentaci k vyhlášení výběrové řízení na zhotovitele projektu „Rozšíření Regionální datové sítě I.“

2. Podrobnější členění etap

Etapa I. – Analýza

Předmětem plnění této etapy je analýza vycházející ze současného stavu, z potřeb kraje a z finančních možností realizování takovýchto potřeb. Výchozím dokumentem této etapy je dokument Studie rozvoje komunikační infrastruktury, který byl vytvořen jako součást projektu „Regionální datová síť Pardubického kraje“. Informace v tomto dokumentu budou zhotovitelem revidovány a doplněny příslušnými šetřeními vedoucímu ke konkrétním doporučením. Cílovým stavem má být konkrétní návrh technického řešení Regionální datové sítě s ohledem minimálně na části uvedené ve Studii rozvoje a tyto dané oblasti:

Stanovení a odůvodnění priorit infrastruktury, např.

3. Infrastruktura se buduje jako neukončená
4. Musí být využita část vybudována v rámci projektu „Regionální datová síť Pardubického kraje“, ale v souladu s pravidly a dobou udržitelnosti tohoto projektu
5. 2Gbps ke každému uzlu v redundanci
6. Eliminace Single Point of Failure
7. Redundance v pasivní, aktivní i elektrické části

Passportizace bodů zájmu

1. Zmapování požadavků všech subjektů a jejich pracovišť, jejich připravenosti pro napojení na regionální síť Pardubického kraje
2. Subjekty šetření: Pardubický kraj, zřizované organizace Pardubického kraje, obce s rozšířenou působností Pardubického kraje, organizace s majetkovou spoluúčastí Pardubického kraje
3. Rozdělení zjištěných bodů zájmu do skupin dle společných rysů a požadavků

4. Přiřazení technické varianty napojení jednotlivým skupinám bodů zájmů
5. Definovaní nových lokalit / uzlů. Určení priority nových uzlů
6. Rozdělení požadovaných služeb do skupin. Určení priority služeb.
7. Technické šetření jednotlivých lokalit případných nových uzlů z pohledu připravenosti pro realizaci daného uzlu

Technické aspekty rozšíření stávající sítě

1. RIPE LIR – Definování jednotlivých kroků při převodu Regionální datové sítě jako člena RIPE NCC. Příprava dokumentů, součinnost při procesu
2. Internet edge – technické šetření stavu a definování konkrétního technického doporučení pro napojování Regionální datové sítě vůči dalším sítím z pohledu stávajících nebo nových zařízení
3. Základní síťové služby – technické šetření a definování dalších základních síťových služeb potřebných pro rozšiřování Regionální datové sítě, min. v rozsahu.:
    a. DNS
    b. NTP
    c. Centralizace AAA
    d. Posílení dohledového centra

Bezpečnost – technické šetření a definování konečného dostatečně dimenzovaného stavu bezpečnosti s ohledem na rozšiřování a napojování Regionální datové sítě, minimálně v rozsahu

1. Aplikační firewall, řízení přístupu, blokování nežádoucího obsahu, blokování nežádoucích aplikací
2. Ochranu před DDoS, mitigace provozu
3. Využití NetFlow a NBA při visibilitě a bezpečnosti sítě
4. SLA – technické šetření stávajícího SLA, zhodnocení jednotlivých možností navýšení

Marketingový průzkum trhu - zmapování možnosti pořízení optických tras k jednotlivým novým uzlům, určení náročnosti připojení jednotlivých uzlů. Cenový kalkul nákladů částí rozšíření Regionální datové sítě v jednotlivých dílčích předpokladech.

Celkové technické řešení infrastruktury – jednoznačné doporučení technického řešení sítě z pohledu funkčnosti, financování a priorit infrastruktury, ale zároveň možnosti dalšího rozšiřování sítě v budoucnu bez větších zásahů do už realizované sítě.

Prezentace jednotlivých oblastí včetně vztahů jednotlivých oblastí, např.:

1. Priority bodů zájmu jednotlivých subjektů i jako skupin s ohledem na finanční náročnosti

2. Návrh částí řešitelných díky podpoře výzvy č. 28 – Specifické informační a komunikační systémy a infrastruktura II.
3. Další možnosti financování výstavby infrastruktury (další výzvy EU, ČR, vlastní prostředky)

Etapa II. Vypracování Studie proveditelnosti

Předmětem této etapy je zpracování Studie proveditelnosti (dále jen Studie) v souladu s vyhlášenou výzvou č. 28 Specifické informační a komunikační systémy a infrastruktura II. k předložení žádosti o podporu z Integrovaného regionálního operačního programu dle jeho pravidel v aktuálním znění.

Studie musí splňovat požadavky uvedené v příloze č. 2 Specifických pravidel výzvy č. 28 – Osnova studie proveditelnosti a v příloze č. 4 Specifických pravidel výzvy č. 28 – Pravidla pro vydání stanoviska odboru Hlavního architekta eGovernmentu.

Etapa III. Zapracování připomínek kontrolních orgánů

V této etapě je vyžadována součinnost zhotovitele při bezodkladném zapracování připomínek a nutných změn v průběhu posuzování Studie proveditelnosti kontrolními orgány a Odborem hlavního architekta eGovernmentu.

Etapa IV. Vypracování specifikací pro zadávací dokumentaci

Zhotovitel bude vycházet z informací předešlých etap, případně z aktualizovaných informací vzešlých z nadřazených orgánů a aktuálního stavu infrastruktury a vypracuje podrobné specifikace rozsahu a parametrů díla pro zadávací dokumentaci projektu „Rozšíření Regionální datové sítě I.“

Objednatel očekává základní členění na technickou a procesní.

Veškeré nutné technické specifikace a parametry díla pro zadávací dokumentaci na výběr zhotovitele vybudování Rozšíření Regionální datové sítě I. budou součástí části technické. Zhotovitel doplní specifikace a parametry i o oblasti, které objednatel nezmínil, ale zhotovitel jako odborník si je vědom jejich nutnosti je doplnit.

V procesní části specifikací budou uvedeny požadavky na kvalifikační předpoklady, minimální doporučené složení týmu a návrh smlouvy, které budou nutné pro úspěšnou realizaci projektu „Rozšíření Regionální datové sítě I.“.

Struktura a členění specifikací a parametrů bude dána objednatelem před začátkem dané etapy.

Vypracované specifikace a parametry budou transparentní a nediskriminační, v nejvyšší možné míře bude použito popisů pomocí mezinárodních standardů.

Zhotovené specifikace budou v souladu se stávajícími už realizovanými projekty a bude jednoznačně definovaná zodpovědnost vůči stávající infrastruktuře.

Zhotovitel bude při zapracování připomínek k zadávací dokumentaci aktivně komunikovat s objednatelem, aby došlo ke vzájemnému vyjasnění příčin změn.

Regionální datová síť Pardubického kraje

Studie rozvoje komunikační infrastruktury

Zakázka:	Regionální datová síť Pardubického kraje
Dodavatel:	O2 Czech Republic a.s.

Obsah

Úvod

Tento dokument vznikl v rámci projektu „Projekt: Část VI. Výzvy – Technologické centrum Pardubického kraje ", registrační číslo projektu: CZ.1.06/2.1.00/08.07331, který je kofinancován z Integrovaného operačního programu.

Dokument obsahuje části týkající se celkové koncepce sítě, cílů návrhu, katalog služeb poskytovaných síťovou infrastrukturou, popis páteřní infrastruktury s uvedením základních charakteristik, infrastrukturu sítě, obecné požadavky na aktivní prvky, koncepci bezpečnosti komunikační infrastruktury, popis realizace, připojování subjektů, přístupová místa a také popis zajištění provozu včetně uvedení požadavků na zajištění, varianty a aplikační zajištění chodu sítě.

Vybudováním komunikační infrastruktury Pardubického kraje dojde k vytvoření moderní regionální sítě, která umožní plně zajistit potřeby kraje a připravit infrastrukturu pro další rozvoj území. Infrastruktura bude sloužit jako základní kámen pro rozvojové projekty nejen v oblasti ICT a eGovernmentu ale i pro oblast prevence kriminality, bezpečnosti a telematických systémů. Regionální síť je základním předpokladem pro realizaci dalších systémů, jako je IP telefonie, možnost videokonferenčních přenosů, propojení systémů monitorovacích kamer, připojení zabezpečovacích systémů, atp.

Rozvojem komunikační infrastruktury se Pardubický kraj začlenil do implementace Strategie realizace SMART ADMINISTRATION, kterou vláda ČR vytyčila základní směřování ke zkvalitňování veřejné správy ve strategii Efektivní veřejná správa a přátelské veřejné služby – Strategie realizace Smart Administration v období 2007–2015. V rámci této strategie jsou zásadní stanovené strategické cíle, mezi nimi také zefektivnit činnost úřadů veřejné správy, snížit finanční nároky na chod administrativy a zajistit transparentní výkon veřejné správy, což souvisí především s:

Vytvářením synergických efektů v budování komplexní infrastruktury v rámci regionu (úroveň kraje, statutárního města, ORP, obce a zřizovaných organizací),

Vytvářením standardizovaných prostředí s možností virtualizace,

Vytvářením standardizovaných typových aplikací (z pohledu minimálních nároků na funkcionalitu).

Vybudováním robustní, bezpečné a efektivní komunikační infrastruktury, schopné zprostředkovat přístup k datovým zdrojům s potenciálem dalšího rozvoje tak Pardubický kraj přímo podporuje jednotlivé strategie rozvoje služeb pro „informační společnost“ navazuje na analytické poznatky, rozvíjí a specifikuje cíle v oblasti podpory eGovernment a racionalizace využívání ICT veřejnou správou.

1. Koncepce

Návrh koncepce budování logické a fyzické komunikační infrastruktury Pardubického kraje musí vyhovět náročným současným a budoucím komunikačním požadavkům nejen Pardubického kraje ale i dalších organizací a subjektů veřejné správy v regionu. Strategie rozvoje komunikační infrastruktury bude sloužit jako základní dokument, ze kterého se dále budou odvíjet detailní návrhy jednotlivých částí sítě.

Základními cíli koncepce komunikační infrastruktury Pardubického kraje jsou:

- vytvořit IP MPLS páteř, která by spojila strategické uzly regionální sítě Pardubického kraje paketovou sítí připravenou nativně zvládnout datové a hlasové komunikační potřeby a umožnila transport dalších médií, např. videa
- umožnit připojení datových center
- umožnit přechod ze zastaralých a nepodporovaných technologií na koncových bodech na moderní síťové technologie
- na jednotlivých lokalitách, které budou začleněny do regionální sítě, využít aktivní moderní vysokorychlostní prvky s možností vzdáleného řízení a monitoringu
- definovat standardy pro připojení lokalit, specifikovat požadavky na nově připojené aktivní prvky
- průběžně optimalizovat náklady na provoz a vlastnictví sítě úměrně s jejím rozšiřováním
- vytvořit platformu pro podporu stávajících a budoucích projektů a jejich požadavků na komunikace
- zvýšit dostupnost služeb, ke kterým síť poskytuje přístup a to zvýšením spolehlivosti jednotlivých komponent sítě i sítě jako celku eliminací SPOF (Single Point of Failure)
- vybudovat sít nové generace, která rozlišuje typ přenášených informací a umožní dodržovat definované parametry poskytované služby (tj. SLA).

Síťová infrastruktura se skládá z následujících komponent:

- Transportní síť (páteř, přístupové body, řízení sítě)
- Externí zařízení (hranice s Internetem, zařízení na lokalitách) a komponenty specifických služeb (FW, VPN koncentrátory)
- Aplikace zabezpečující chod a bezpečnost sítě
- Technologická centra v Pardubickém kraji
- Fyzická optická infrastruktura
- Koncové body sítě a MAN sítě lokalit

2. Cíle návrhu

Základní cíle návrhu komunikační infrastruktury Pardubického kraje vychází z následujících bodů:

- Vysoká propustnost – síť by neměla trpět zahlcením, měla by mít neustále schopnost poskytnout požadovanou propustnost. To znamená, že pokud v síti nenastalo selhání směrovače nebo páteřní linky, propustnost by nikdy neměla být omezena kapacitou linky nebo propustností směrovačů či jiných aktivních prvků.
- Zpoždění v jednom směru mezi dvěma PE směrovači by nikdy nemělo přesáhnout 40ms. Pro zabezpečení hlasových služeb, celkové zpoždění mezi dvěma uživatelskými body by nemělo přesáhnout 150ms. Předpokládáme, že hlasové koncové zařízení spotřebuje 50ms na kompresi hlasu a potlačení echa, 60ms rezervujeme pro přístupové směrovače a linky a pro páteřní síť zůstává 40ms.
- Síť musí splňovat bezpečnostní požadavky, definované obecnými standardy a taktéž diktované bezpečnostní politikou Pardubického kraje.
- Škálovatelnost – síť musí být snadno rozšiřitelná o další páteřní a přístupové body.
- Robustnost – v síti jsou minimalizovány rizika možného selhání (SPOF).
- Snížení nákladů na provoz sítě – síť bude využívat především infrastrukturu ve vlastnictví Pardubického kraje nebo organizací Pardubickým krajem zřizovaných za účelem minimalizace provozních nákladů.
- Průběžné zvýšení celkové propustnosti a kapacity sítě a zvýšení přípojné rychlosti jednotlivých lokalit.

2.1 Varianty řešení

Nově budovaná komunikační infrastruktura regionální datové sítě má v porovnání s předchozími technickými řešeními řadu výhod:

- Upuštění od zastaralých technologií a zařízení, dokonalá kontrola parametrů sítě.
- Využití vlastních přenosových kapacit bez nutnosti odebírat nákladné telekomunikační služby od komerčních subjektů, co umožní dramaticky snížit provozní náklady sítě.
- Možnost investovat do infrastruktury na míru šité specifickým požadavkům Pardubického kraje.
- Dodržování požadavků na vysokou dostupnost.
- Možnost důsledného vynucení dodržování bezpečnostní politiky a centrální správu uživatelů a přístupových práv.
- Možnost koordinovat požadavky na propustnost sítě s přihlížením na plánované rozvojové projekty.
- Možnost dokonalé evidence všech aktivních i pasivních prvků, jejich správné dimenzování a monitoring zátěže.
- Možnost budování redundantní infrastruktury pro vysoce dostupná datová centra.
- Možnost snadné správy a dohledu celé komunikační infrastruktury.

Podpora správy sítě dle standardů ITIL.

2.2 Rizika realizace a koncepce (včetně problematiky veřejné podpory)

V rámci analýzy rizik při realizaci koncepce byla identifikována tato hlavní možná rizika:

- Neochota stávajících poskytovatelů komunikační infrastruktury spolupracovat při migraci na novou platformu.
- Neochota stávajících správců aktivních prvků spolupracovat při získávání aktuálních konfigurací síťových prvků.
- Zvýšené nároky na personální zabezpečení a kvalifikaci pracovníků zajišťujících chod sítě.
- Nedostatek investičních prostředků.
- Nutnost zabezpečit (vybudovat) některé optické spoje.

Tato rizika je možné minimalizovat:

Důslednou přípravou na každý krok migrace.

Důslednou revizí současného stavu.

Smluvním vynucením odevzdání konfigurace všech síťových prvků, adresních plánů, topologie a směrování od stávajících dodavatelů a správců infrastruktury.

Umožnění plného administrátorského přístupu na všechna zařízení přímo se podílející na současné infrastruktuře.

Pečlivým výběrem zaměstnanců a externích konzultantů podílejících se na provozování infrastruktury.

- Je nutné vykonat podrobný průzkum možností připojení dalších lokalit a to fyzickou inspekcí přístupové infrastruktury poslední míle od agregačních bodů do fyzických lokalit.

2.2.1 Veřejná podpora

Obecně k veřejné podpoře

Podle čl. 107 odst. 1 Smlouvy o fungování Evropské unie, podpory poskytované v jakékoli formě státem nebo ze státních prostředků, které narušují nebo mohou narušit hospodářskou soutěž tím, že zvýhodňují určité podniky nebo určitá odvětví výroby jsou, pokud ovlivňují obchod mezi členskými státy, neslučitelné s vnitřním trhem, nestanoví-li Smlouva jinak.

DEFINIČNÍ ZNAKY VEŘEJNÉ PODPORY

Na základě uvedené definice je nutné u veřejné podpory zkoumat 4 základní kritéria definice veřejné podpory:

1. JE PODPORA POSKYTNUTA STÁTEM NEBO Z VEŘEJNÝCH PROSTŘEDKŮ?

   Pojem státní podpory se vztahuje na jakoukoli přímo či nepřímo poskytnutou výhodu financovanou ze státních prostředků, poskytnutou státem jako takovým nebo zprostředkujícím subjektem jednajícím na základě svěřených pravomocí.

   Základním předpokladem pro naplnění tohoto definičního znaku je ovlivnění veřejných rozpočtů, přitom není rozhodující, zda jsou veřejné rozpočty ovlivněny přímo (vydáním

finančních prostředků) či nepřímo (nerozšířením jejich příjmové stránky, ke kterému by za normálních okolností došlo). Za veřejné prostředky se považují i fondy, které jsou kontrolovány orgány veřejné správy.

2. ZVÝHODŇUJE PODPORA URČITÉ PODNIKY NEBO URČITÉ ODVĚTVÍ PODNIKÁNÍ A JE SELEKTIVNÍ?

   Pojmem podnik se rozumí jakákoli entita, která vykonává ekonomickou činnost, bez ohledu na její právní status nebo způsob, jakým je financována. V českém právním prostředí je tedy podnikem jakákoliv fyzická nebo právnická osoba, jakékoliv sdružení nebo seskupení osob bez právní subjektivity, jakož i každý veřejný orgán, buď se samostatnou právní subjektivitou, nebo spadající pod orgán veřejné moci, který takovou samostatnou právní subjektivitu má. Podstatná je provozovaná činnost podniku, zda jí lze považovat za ekonomickou či nikoliv. Ekonomickou činností se v souladu s rozhodovací praxí rozumí nabízení zboží a/nebo služeb na trhu. Ani neziskovost v konkrétním případě nehraje zásadní roli.

   Zvýhodnění představuje stav, který by za běžných tržních podmínek nenastal. Ke zvýhodnění dochází už tehdy, kdy podpora snižuje náklady, které by musel příjemce za běžného fungování nést ze svého rozpočtu.

   Selektivní opatření je takové, které není aplikováno vůči všem podnikům na trhu stejně a nelze jej tedy označit za obecné opatření.

3. JE NARUŠENA NEBO HROZÍ NARUŠENÍ SOUTĚŽE?

   Narušení soutěže stejně jako další definiční znak veřejné podpory (ovlivnění obchodu mezi členskými státy) Evropská komise spíše předpokládá.

   Soutěž je narušena tehdy, pokud opatření posílí postavení příjemce podpory oproti jeho konkurentům.

4. JE OVLIVNĚN OBCHOD MEZI ČLENSKÝMI STÁTY?

   Není stanovena žádná hranice, kdy již konkrétní opatření ovlivňuje obchod mezi členskými státy. Z judikatury však vyplývá, že i malá částky či malá velikost příjemce veřejné podpory může ovlivnit trh mezi členskými státy.

   K ovlivnění obchodu zpravidla nedochází, pokud předmětné opatření působí pouze lokálně (regionálně) či příjemci podporovaných služeb pocházejí pouze z jednoho členského státu.

   Podpora de minimis neovlivňuje obchod mezi členskými státy ani nenarušuje soutěž.

   Dne 30.9.2015 byl na stránkách Úřadu pro ochranu hospodářské soutěže zveřejněn dokument Evropské komise, resp. Generálního ředitelství pro hospodářskou soutěž, s názvem „Analytical Grids on the application of State aid rules to the financing of infrastructure projects“, ve verzi ze září 2015.

   Tak, jak je popsáno ve zprávě, nové analytické formuláře nahrazují předchozí verze z roku 2012 (s výjimkou formuláře pro financování vodohospodářské infrastruktury, který zůstává stále aktuální) a reflektují aktuální rozhodovací praxi Komise a modernizovanou legislativu veřejné podpory. Po vydání očekávaného Sdělení o pojmu veřejné podpory budou formuláře ze strany Komise dále operativně aktualizovány.

K rozvoji Komunikační infrastruktury Pardubického kraje patří část dokumentu s názvem „GRID N°1 – BROADBAND NETWORK INFRASTRUCTURES“, která se týká veřejné podpory při budování širokopásmové síťové infrastruktury, ke které Komunikační infrastruktura Pardubického kraje patří. Po prostudování této části je možné konstatovat že:

Lokality budoucího rozvoje jsou obce v regionu Pardubického kraje.

Jedná se tedy o nepodnikatelské subjekty.

Vzhledem k tomu, že primárním úkolem obcí není podnikání, není možné považovat poskytnutí dotace z veřejných zdrojů na výstavbu širokopásmové komunikační infrastruktury za veřejnou podporu. Podmínkou pro takové posouzení je fakt, že služby provozované na Komunikační infrastruktuře Pardubického kraje, nebudou nabízeny komerčně, resp. nebudou nabízeny komerčním subjektům, které podnikají na daném území.

3. Katalog služeb poskytovaných síťovou infrastrukturou

Předchozí typy sítí a kvalita poskytovaných služeb trpěly nedostatky, které vycházely z technologie použité při jejich vzniku a také z nedostatečného aktualizování použitého síťového hardware a software. Sítě neumožňovaly provozování náročných služeb a nevyhovovaly moderním požadavkům z hlediska diferenciace mezi datovými toky. Umožňovaly pouze provozování služby best-effort, kde nejsou garantovány žádné parametry kvality služby a neumožňovaly tudíž uspokojivé provozování VoIP, multimédií, jednoduché konfigurování virtuálních sítí a podobně.

Nová architektura adresuje všechny tyto nedostatky a poskytuje moderní, bezpečnou a vysoce spolehlivou infrastrukturu, která může sloužit nejen krajskému úřadu, ale i organizacím krajem zřizovaným, které z nedostatku funkcionality stávajících sítí využívají služeb jiných organizací a vynakládají nemalé prostředky například pro přístup do Internetu, hostování služeb elektronické pošty a podobně.

Nová síť je bezpečnější, spolehlivější, lehce spravovatelná, poskytuje sofistikované služby s vysokou přidanou hodnotou a umožňuje snazší provozování a vyšší dostupnost stávajících aplikací vnitřních i portálových aplikací pro veřejnost. Umožňuje řízení bezpečnosti v síti, je robustní a odolná vůči výpadkům, zabezpečuje kontinuitu fungování krajského úřadu a dalších organizací a provozovaných služeb i v případě krizových situací.

3.1 Vztah sítě k externímu prostředí

Do regionální sítě Pardubického kraje budou vstupovat tyto typy subjektů:

- Krajský úřad a jeho síť
- Organizace, v nichž je kraj většinovým vlastníkem
- Ostatní organizace krajem zřizované (školy, sociální zařízení, záchranná služba…)
- Externí organizace (Ministerstvo vnitra ČR)
- Externí zdroje distribuované poté sítí (CESNET)

Tyto přístupy budou řízeny pomocí jednoznačných SLA a při zachování maximální úrovně bezpečnosti připojovaných a již připojených subjektů.

Detailní popis připojení k externím subjektům podává prováděcí projekt, kapitola 3.

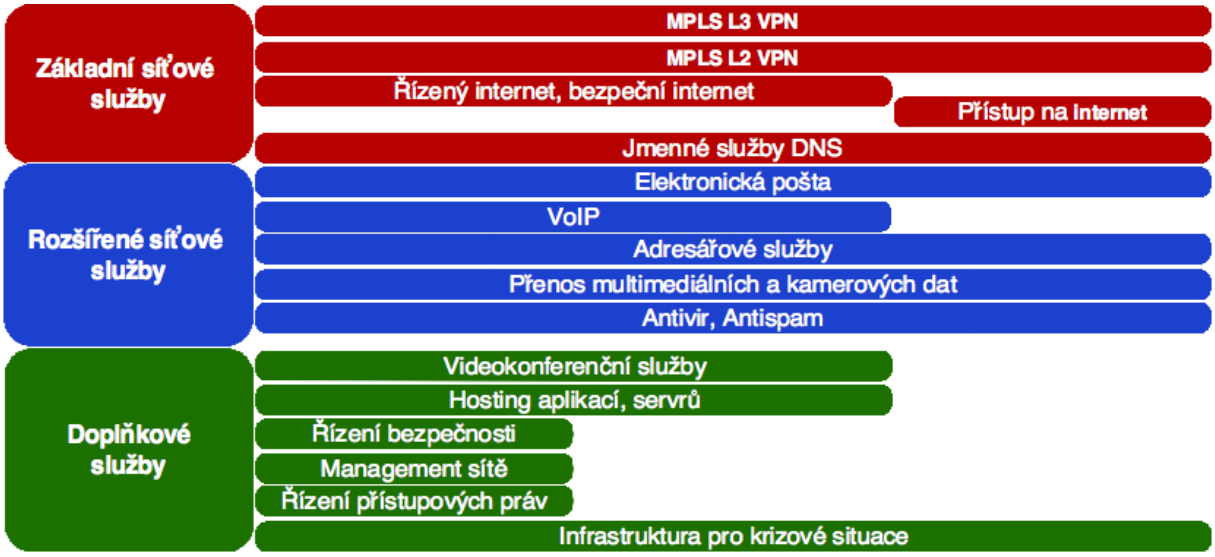
3.2 Služby poskytované sítí

Všechny poskytované služby budou rozděleny do několika základních kategorií. Toto rozdělení umožní lépe přidělovat potřebné pásmo a zabezpečovat další síťové charakteristiky pro aplikace, které budou různě citlivé na tyto parametry.

V obecné rovině musí být zajištěny následující služby:

- Virtuální privátní sítě na třetí vrstvě (L3) referenčního modelu ISO/OSI
- Virtuální privátní sítě na druhé vrstvě (L2) referenčního modelu ISO/OSI

- Řízená vzájemná komunikace mezi jednotlivými připojenými subjekty
- Bezpečný a spolehlivý přístup na Internet, vysoká bezpečnost zaručena využitím služeb síťového perimetru, správa bezpečnostních incidentů
- Rychlý a spolehlivý přístup na Internet i pro organizace s vlastním bezpečnostním perimetrem
- Konsolidovaná síťová jmenná služba DNS za využití dostupných bezpečnostních opatření
- Synchronizace času NTP
- Vzdálený přístup k síti a zdrojům v datových centrech v Pardubickém kraji
- Poskytování a garantování kapacity pro portálové služby
- Garantované parametry infrastruktury pro hlasové služby postavené na bázi protokolu IP
- Řízení bezpečnosti přístupu na Internet, blokování nežádoucího obsahu, blokování nežádoucích aplikací
- Zabezpečení pásma pro přenos multimediálních a kamerových dat
- Poskytnutí platformy pro provozování videokonferencí
- Poskytování poslední míle připojení do páteře a Internetu
- Vzdálený monitoring sítě
- Vzdálený management sítě



3.3 Služby, ke kterým síť zprostředkovává přístup

Regionální síť Pardubického kraje bude moci zajišťovat přístup k řadě služeb poskytovaných zejména z datových center:

- Konsolidované adresářové služby LDAP,
- Konsolidované služby Active Directory,
- Řízení přístupových práv uživatelů na základě bezpečnostní politiky (RBAC),
- Bezpečná elektronická pošta,
- Služby integrační platformy,
- Služby datové integrace,

- Elektronická spisová služba,
- Geografický informační systém GIS,
- Hostování aplikací na sdílených serverech,
- Hostování virtuálních serverů,
- Hostování fyzických serverů se zabezpečením redundance napájení a přístupu do metropolitní sítě,
- Řízené zálohování dat,
- Služby virtuální pobočkové ústředny na bázi VoIP,
- Zřizování videokonferencí a provozování videokonferenčního systému,
- Monitoring zabezpečení sítě, serverů, aplikací, reportování shody s bezpečnostní politikou,
- IP telefonie.

3.4 Stručná charakteristika služeb

Základní síťové služby představují množinu služeb, které budou poskytovány Pardubickému krajskému úřadu a dalším organizacím od samého počátku existence sítě. Vycházejí ze současného stavu, liší se však výrazně vyšší kvalitou a spolehlivostí. Jsou odstraněny možné body selhání (Single Point of Failure). Předpokládáme, že přístup na Internet bude realizován redundantním připojením páteře, redundancí zařízení i redundancí cest. Součástí služby by mělo být provozování plně redundantního systému DNS, řízení síťového provozu a využití služeb perimetru sítě.

Technologie MPLS umožňuje tvorbu virtuálních privátních sítí dokonale oddělených od ostatního provozu a chovajících se jako jediná síť. Součástí této služby je provozování adekvátních směrovacích algoritmů zaručujících rychlou konvergenci sítě v případě výpadku, řízení datových toků v závislosti na jejich typu, jednoduchost správy, flexibilitu topologie, stabilitu a robustnost. Tato technologie dále umožňuje možnost vzájemné řízené komunikace.

Rozšířené síťové služby přinášejí výraznou přidanou hodnotu všem účastníkům sítě. Primárně se jedná o bezpečnou službu elektronické pošty, jejíž volitelnou součástí je antivirová ochrana a filtrace nevyžádané elektronické pošty (spam).

Vzhledem k povaze MPLS infrastruktury, je možné garantovat dostatek přenosového pásma, akceptovatelnou ztrátovost přenášených dat, vyhovující odezvu a stabilitu parametrů sítě na její využití pro telefonování a přenos multimediálních dat v reálném čase.

Doplňkové služby poskytnou uživatelům v regionální síti Pardubického kraje důležité bezpečnostní prvky nutné pro dodržování bezpečnostní politiky, řízení uživatelů a jejich privilegií, provozování, monitoring a kapacitní plánování sítě a jejich zdrojů. Umožní připojeným externím organizacím využit služeb datových center a zabezpečeného přístupu na Internet a tím dramaticky zvýšit bezpečnost, spolehlivost, dostupnost a stabilitu provozovaných aplikací a to i v případě krizové situace.

Nasazené bezpečnostní prvky umožňují pružně reagovat na vzniklé bezpečnostní incidenty a eliminovat bezpečnostní hrozby. Řízení bezpečnosti umožňuje korelovat bezpečnostní a žurnálové informace ze všech relevantních prvků sítě a datové infrastruktury.

Detailní popis poskytovaných služeb podává dokument LabeNET-Veřejný Katalog Služeb.

3.5 Služby třetím stranám

IP síťová infrastruktura a podpůrné aplikace umožní provozovat některé služby i pro organizace zřizované Pardubickým krajem. Jedná se zejména o služby spojené s dohledem, vzdálenou správou a řešením problémů na následujících částech infrastruktury:

- vnitřní WAN linky - řešení problémů spojených s konektivitou, distribucí směrovacích informací, propustností sítě, záložními spojeními
- interní LAN sítě – především dohled a vzdálená správa aktivních prvků, řešení bezpečnostních otázek a incidentů, dokumentace vnitřní LAN infrastruktury
- intranetové servery připojených organizací - monitoring dostupnosti a výkonnosti, monitoring funkcionality intranetových aplikací (DNS, MAIL), monitoring zabezpečení a dodržování bezpečnostních politik a standardů
- centralizace agend
- hosting

3.6 IP telefonie, hlasové a multimediální služby

IP telefonie je v současné době standardní aplikace, která umožňuje organizacím šetřit provozní náklady na vzájemnou komunikaci a zároveň zvyšuje jejich produktivitu díky provázanosti s ostatními zdroji informací.

Vybudování kompletně nové infrastruktury pro telefonování by bylo příliš nákladné a neefektivní, proto je lépe volit cestu postupného přechodu a budování, samozřejmě při zachování celkové koncepce, tak aby bylo možné propojit navzájem již existující izolované ostrůvky.

Budovaná páteřní infrastruktura umožní provoz aplikací, které mají speciální požadavky na síť a které jsou citlivé na jednotlivé charakteristiky provozu. Slabá místa se mohou vyskytovat v samotných lokálních sítích (v jejich designu).

Postup vybudování kompletního systému IP telefonie by mohl vypadat takto:

- analýza současného stavu (kde existují které systémy, v jakém stavu jsou současné PBX, jaký je stav lokální sítě, jaké jsou smluvní závazky).
- Návrh číselného plánu a plánu případné migrace pro nekompatibilní organizace.
- Vybudování centrální IP PBX, v ideálním případě nezávislé na infrastruktuře použité v jednotlivých lokálních sítích, jinými slovy by centrální systém měl umožňovat použití koncových zařízení různých výrobců a neomezovat zásadně jejich funkčnost.
- Provázání centrálního systému se systémy správy uživatelů, implementace pokročilých funkcí (telefonních seznamů, informací o dostupnosti uživatelů atd.).
- Možnost snadného objednávání a změn centrálních služeb (ala IP Centrex).
- Postupná migrace lokálních sítí na IP telefonii.
- Aplikace pro vyšší produktivitu (provázání s prostředím kancelářského software, možnost audiokonferencí s možností rezervace času účastníků, možnost záznamu hovorů a mnohé další).

IP Videokonference

Přenos videa bude páteřní síť umožňovat za podobných podmínek, které jsou potřebné pro IP telefonii. Pravidla budování jsou taktéž podobná. Vzhledem k objemnosti celé problematiky navrhujeme případnou samostatnou studii na téma videokonferencí.

3.7 Regionální síť jako ripe ncc LIR

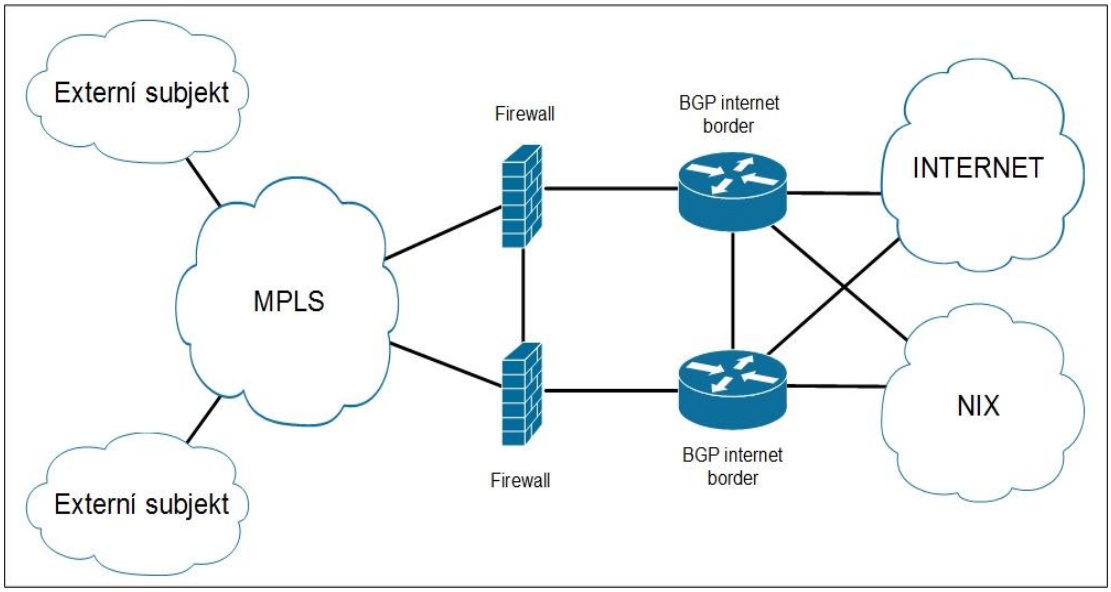
Pro dosažení optimálního způsobu řešení přístupu do sítě Internet by měl Pardubický krajský úřad získat status Local Internet Registry v organizaci spravující IP adresy a čísla AS (autonomních systémů) pro evropský region – RIPE NCC (RIPE Network Coordination Centre). LIR má přidělen vlastní rozsah IP adres, které jsou zcela nezávislé na konkrétních poskytovatelích přístupu do sítě Internet. LIR také zažádá o vlastní číslo autonomního systému (AS), který má vlastní směrovací politiku, vlastní dohody o peeringu a může uzavírat dohody, které mu umožní se chránit před některými typy útoků z Internetu (zvláště DDoS, za pomocí dohod o blackholingu). Krajský úřad Pardubického kraje jako LIR by mohl přidělovat IP adresy organizacím v jeho kompetenci na základě vlastního uvážení a zároveň účinně regulovat připojení do Internetu přes třetí operátory. Vzhledem k velikosti regionální sítě Pardubického kraje a dynamičnosti změn je pouhá žádost o IP adresy nezávislé na poskytovateli (IP adresy) a následná žádost o AS pouze dočasným řešením, které nezabezpečí takovou flexibilitu jako řádné členství v RIPE jako LIR.

Podmínky pro získání vlastního AS (a nezávislých IPv4/v6 adres) jsou detailně specifikovány na webových stránkách RIPE:

https://www.ripe.net/publications/docs/ripe-553

3.8 Směrovací oblast pro Internet

V rámci MPLS infrastruktury by měla vzniknout jedna směrovací oblast sloužící výhradně pro připojení subjektů zřizovaných Pardubickým krajem do Internetu. Tato oblast bude obsahovat pouze IP adresy přidělené uvnitř regionální sítě Pardubického kraje, ne celou směrovací tabulku Internetu (na rozdíl od internetových hraničních směrovačů). V této části bude také síťový perimetr, který umožní jednak regulovaný přístup Pardubického krajského úřadu a jeho organizací na Internet a také přístup z Internetu a dalších externích sítí na informační zdroje provozované v rámci regionální sítě Pardubického kraje.



Vysoce dostupnou bránu do Internetu tvoří dvojice BGP směrovačů redundantně připojených k dvěma různým internetovým poskytovatelům a do NIXu. Tvoří hranici autonomního systému a agregují a propagují do Internetu IP prefixy přidělené RIPE NCC. Bezprostředně za nimi se nachází první bezpečnostní prvek chránící Internet VRF před základními útoky směřujícími do Internet VRF a také zamezuje případným bezpečnostním problémům pocházejícím z organizací připojených do Internet VRF. Je vhodné, aby tento bezpečnostní prvek byl stavěn s ohledem na vysokou dostupnost a propustnost, jeho funkcionalita však bude v této činnosti jen základní, nebude poskytovat virtuální firewally ani jiné sofistikované služby.

Přístupové linky do sítě Internet budou vycházet z obou datových center, popřípadě po linkovém a hardwarovém posílení z jiného síťového uzlu.

3.9 Poskytování připojení do Internetu externím organizacím

Vzhledem k vysoce dostupnému a bezpečnému cílovému stavu navrhovaného řešení, je jedna ze služeb, které bude možné poskytovat i jiným krajem zřizovaným organizacím, případně školám, nemocnicím a dalším, přístup do Internetu. Jedná se zejména o organizace vzdělávací nebo veřejně prospěšné, které v současnosti kupují internetové služby (přístup do Internetu, web hosting, email hosting) od komerčních poskytovatelů těchto služeb. Tyto rozpočtové organizace mohou ušetřit značné prostředky tím, že využijí služeb prostředí regionální sítě Pardubického kraje a případně jejich datových center.

3.10 Logické postavení síťového perimetru

V MPLS páteři jsou a měly by být i nadále konfigurovány ortogonální směrovací oblasti (VRF) pro každou organizaci, která bude mít definovány své komunikační potřeby. Tyto VRF mohou umožňovat komunikaci navzájem mezi připojenými subjekty, do datových center, případně do Internetu prostřednictvím síťového perimetru na základě jasně definovaných pravidel. Perimetr je dimenzován s ohledem na dostatečnou propustnost a vysokou dostupnost. Z hlediska logické struktury budou jednotlivé VRF pro perimetr představovat demilitarizované zóny s řízením provozu, autentizací a

autorizací použitím standardizovaných mechanismů (jednorázová hesla, SSL certifikáty). Síťový perimetr bude pro organizace představovat vstupní bránu do Internetu a do datových center. Organizace, které nedisponují vlastními dostatečně bezpečnými a dostupnými firewally, mohou výrazně zvýšit svou úroveň zabezpečení a spolehlivosti přístupu na Internet. Organizace, které preferují využití vlastních firewallů, mohou mít přímý přístup do Internet VRF.

3.11 VPN

Jednou ze základních funkcí nové infrastruktury je schopnost vytvářet virtuální privátní sítě provozované nad společnou páteřní infrastrukturou. Jedním z cílů koncepce je umožnit jednotlivým připojovaným subjektům využít tuto schopnost na vytvoření vlastních plně nezávislých WAN sítí spojující detašované lokality. Subjekty mohou nahradit svou stávající WAN infrastrukturu moderní, inteligentní a vysokokapacitní MPLS VPN. Zároveň budou mít možnost zveřejnit část svých aplikačních serverů z datového centra a mít k nim bezpečný a spolehlivý přístup. MPLS VPN jsou vzájemně nezávislé, jejich IP adresní rozsahy se mohou bez konfliktu překrývat.

V rámci těchto VPN bude možné realizovat i dohledové služby a služby s přidanou hodnotou a tím snížit náročnost správy sítí.

Detailní popis VPN instancí podává dokument prováděcí projekt, kapitola 1.5.

3.12 Technologická centra

Jedním z elementárních úkolů páteřní infrastruktury je umožnit bezpečný, dostatečně rychlý a robustní přístup koncových uživatelů k aplikacím a agendám nezbytným k chodu administrativy. Infrastruktura samotných datových center je mimo rámec tohoto dokumentu, zde je pouze výčet vlastností, které jsou relevantní k budované regionální síti:

- Datová centra jsou přístupná všem autorizovaným uživatelům.
- Zdroje datových center jsou robustním způsobem připojeny do páteřní sítě.
- Datová centra nejsou přes regionální datovou síť přímo dostupná z externích sítí.
- Infrastruktura a připojení datových center jsou dostatečně dimenzované ať již z pohledu rychlosti odezvy tak z pohledu množství přistupujících uživatelů.
- Datová centra jsou schopna sama zabezpečit vlastní bezpečnost v přiměřené míře.
- Infrastruktura datových center umožní sdílení a rozdělování zátěže mezi jednotlivými servery dle více kritérií.

Komunikační infrastruktura datových center je postavena na standardních technologiích, dle současných poznatků na design moderních datových center. Intenzita vzájemné komunikace mezi datovými centry vychází z požadavků jednotlivých aplikací.

3.13 Požadavky na zavedení nových služeb

Požadavky na zavedení nových služeb musí být řešeny v souladu s touto strategií a s dalšími platnými dokumentacemi. Předpokládáme, že požadavky na nové služby budou generovány jednak z důvodů předpokládané postupné konsolidace ICT prostředí v rámci příspěvkových organizací Pardubického

kraje, tak z důvodů nových technologií, které začnou být používány např. ve zdravotnictví, ve školách, atp.

Při specifikaci nové služby je vhodné využít technické specifikace zařízení, které je použité při realizaci komunikační infrastruktury tak, aby byla zajištěna kompatibilita nově pořizovaných zařízení s ostatními prvky sítě. Dále je nutné ověřit schopnosti stávajících prvků zajistit dodržení potřebných parametrů nové služby např. latence, QoS, specifické protokoly, atp.

4. Páteřní infrastruktura

Architektura páteřní infrastruktury sítě 21. století je postavena na technologii MPLS (Multi-Protocol Label Switching). MPLS je IETF standard založen na proprietárních technologiích dodavatelů jako například Cisco Systems, Nortel a Lucent.

MPLS je možné popsat jako sloučení technologie přepínání na druhé vrstvě a tradičního směrování v IP sítích. MPLS bylo původně uvedeno jako integrace směrování IP do sítí ATM, je však možné jej použít i v sítích kde se ATM nevyužívá. Směrovače schopné funkcionality MPLS se označují také jako Label-Switch Routers (LSR). MPLS se standardně používá v páteřní části komunikační infrastruktury. Datové rámce (pakety) vstupující do sítě jsou označeny jednou nebo více krátkými značkami. Tyto značky jsou určující pro to, jak budou s pakety zacházet LSR. Hlavním rozdílem mezi MPLS a tradičními L2 přepínacími technologiemi jako Frame-Relay nebo ATM je v mechanismu vazby mezi IP adresou paketu a L2 adresou. V MPLS je přepínání IP paketů v rámci MPLS páteře stejné jako kdyby byly směrované za pomoci konvenčních směrovacích protokolů jako OSPF nebo IS-IS. Toho se dosahuje integrováním konvenčního směrovacího protokolu a speciálního protokolu na distribuci značek (label distribution protocol – LDP). LDP zabezpečuje konzistenci vazeb IP-adres a značek napříč celou sítí s obsahem směrovacích tabulek. Jakmile IP paket vstoupí do sítě a je opatřen značkou, IP adresa paketu je pro síť neviditelná až do momentu kdy paket síť opouští a značka je odstraněna. Tato schopnost transparence IP adres umožňuje tvořit mnohonásobné, ortogonální směrovací oblasti, což v praxi znamená možnost provozování mnoha samostatných (bezpečně oddělených) IP sítí nad jednou společnou páteřní infrastrukturou. Ačkoliv tato transparence IP adres je vlastní i konvenčním L2 přepínacím technologiím, výhodou MPLS je možnost kombinovat tuto transparenci se systémem směrování v IP sítích které se ukázalo jako velice robustní a škálovatelné i v obrovských sítích jako je například Internet. Ačkoliv IP adresy paketů jsou pro LSR směrovače transparentní, přepínání uvnitř LSR je založeno na informacích poskytovaných konvenčními směrovacími protokoly jako OSPF, IS-IS a BGP.

5. Základní technologie

5.1 Kvalita služby QoS

Kvalita služby (Quality of Services – QoS) se vyznačuje schopností sítě poskytnout garantované parametry vybraným typům provozu. Zahrnuje množinu technik umožňujících aplikacím požádat o předvídatelnou propustnost, stálost (jitter) a odezvu. Kromě jiného použití QoS poskytuje lepší a předpověditelnější chování sítě pomocí následujících technik:

- Podpora dedikovaného přenosového pásma,
- Vylepšení ztrátovosti,
- Vyhýbání se a zamezení zahlcení sítě,
- Profilování (shaping) síťového provozu,
- Nastavování prioritizace napříč sítí.

K dispozici jsou dva možné způsoby:

- Integratedservices (IntServ)
- Differentiatedservices (DiffServ)

DiffServ se zaměřuje primárně na agregovaný a nastavovaný QoS. Místo toho, aby aplikace signalizovala svoje požadavky na QoS (jako IntServ), DiffServ, využívá DSCP (DiffServCode Point) jako indikaci různých požadavků na kvalitu služby pro různé třídy provozu.

CoS (Class of Service) je způsob řízení provozu v síti za pomoci seskupení podobných typů provozu do jednotlivých tříd a zacházení s nimi s danou prioritou.

Funkční požadavky na síť:

- Přenos dat protokolem IP
- Zabezpečení přístupu na internet
- Virtuální privátní sítě na báze protokolu IP
- Virtuální privátní sítě na druhé vrstvě referenčního modelu OSI/ISO
- Zabezpečení kvality služby (QoS) pro hlasové, multimediální služby a vybrané aplikace

Detail nastavení QoS podává Prováděcí projekt, kapitola 5.4.

6. Základní charakteristiky sítě

Základem páteře regionální sítě Pardubického kraje je technologie MPLS, kterou charakterizují následující vlastnosti:

1. **Schopnost provozovat nezávislé, kompletně oddělené směrovací oblasti** (multiple orthogonal routing realms)

   Směrovací informace importované do sítě na okrajových portech jsou propagované do limitované množiny ostatních portů. Výměna směrovacích informací v rámci podmnožiny portů tvoří směrovací oblast a jednotlivé okrajové porty jsou členy této oblasti.

   V případě, že dvě směrovací oblasti nemají žádné společné členy, hovoříme, že oblasti jsou ortogonální. Síť nesmí umožnit absolutně žádnou konektivitu mezi ortogonálními směrovacími oblastmi. Pakety a cesty v jedné oblasti musí být kompletně neviditelné pro ostatní, ortogonální oblasti. Pro potřeby Pardubického kraje to znamená výhodu v možnosti řízené komunikace mezi doposud oddělenými sítěmi a možnost přístupu k centrálním zdrojům i ze sítí, které používají stejný IP adresní prostor jako některé již existující, respektive připojené subjekty.

2. **Schopnost řídit směrování uvnitř směrovacích oblastí a mezi směrovacími oblastmi**

   Síť musí být schopna řídit datové toky, omezit datové toky a poskytovat dodatkové služby jako například NAT nebo firewall.

3. **Schopnost rozlišovat třídy služeb**

   Účelem je adaptovat chování se sítě k různým typům provozu a zabezpečit kvalitu poskytované služby (QoS), přičemž je nutno rozlišovat alespoň tyto typy provozu:

   - Best effort – nejlepší snaha – pro provoz bez garance kvality služby (typicky Internet, email)
   - Critical – kritické služby – aplikace potřebné pro zabezpečení fungování úřadů a podniků
   - Voice – pro hlasové aplikace citlivé na poskytovanou úroveň kvality služby
   - Multimédia – pro aplikace vyžadující stálou přenosovou kapacitu

   Kritické aplikace jsou citlivé na odezvu (vzdálený přístup k aplikacím a obrazovkám), nestálost (jitter) a ztrátovost přenosu. Ačkoliv tyto aplikace mají většinou mírné nároky na přenosovou kapacitu, v síti musí být neustále k dispozici dostatečná přenosová kapacita. Je potřeba klasifikovat, které aplikace budou zařazeny do této třídy.

4. **Schopnost přímého propojení s dalším poskytovatelem MPLS VPN tak jak je definováno ve standardu RFC2547bis.**

7. Infrastruktura sítě

7.1 Fyzická infrastruktura

Základem nové komunikační infrastruktury je bezesporu infrastruktura fyzická. Hlavním požadavkem je využití interních zdrojů přenosových kapacit, které jsou v majetku Pardubického kraje či organizací jím zřizovaných.

Páteřní konektivita bude postavena na základě optických tras, optickými linkami bude také zajištěna konektivita datových center. Tam, kde nebude možné pokrýt tyto požadavky vlastními zdroji, bude nutné zajistit konektivitu od komerčních subjektů a to na základě podmínek výhodných pro Pardubický kraj (ať již se jedná o cenu, tak především o parametry služby, kvalitu poskytnutého SLA a v neposlední řadě možnost rychlých změn požadovaných parametrů spojení). Jako primární budou pro páteřní spoje vyžadovány nenasvícená optická vlákna. Obecně lze říci, že poskytnutí komerční služby lze stanovit na téměř libovolně krátkou dobu se stejně pružnou dobou výpovědi z takového smluvního stavu. Délka smluvního pronájmu celého nenasvíceného vlákna se většinou pohybuje ve výrazně delších časových úsecích (typicky jde o více než pětileté kontrakty).

V rámci analýz rozložení předpokládaných uživatelů a dalších subjektů je možné uvažovat i o poskytnutí propojení více subjektů pomocí existující MPLS infrastruktury poskytovatele služeb a následné propojení celé takto poskytované služby s regionální sítí Pardubického kraje.

Detail stávající fyzické infrastruktury podává dokument prováděcí projekt, kapitola 1.2.

7.2 Páteř sítě

Páteř sítě se sestává z MPLS (PE) směrovačů ve správě krajského úřadu Pardubického kraje. Vzhledem k rozsahu a topologii sítě nejsou použity páteřní směrovače, ale pouze PE (Provider Edge) směrovače. Jejich funkcí je jak transport v páteřní síti, tak propojení do zákaznické sítě (tj. zásadní role v MPLS síti, což znamená přidávání a odstraňování MPLS značek na routovaném provozu). Tyto směrovače mají také za úkol implementovat různé chování sítě v závislosti na typu provozu (QoS).

Detail topologie sítě podává dokument prováděcí projekt, kapitola 1.4.

7.3 Hraniční směrovače

Primární funkcí hraničních (agregačních, tzv. PE směrovačů) směrovačů je poskytovat rozhraní mezi páteří sítě a externími sítěmi připojenými přes přístupové linky k přístupovým (hraničním) portům. Hraniční směrovač má minimálně jeden hraniční port.

Při budování nové infrastruktury budou použity tyto typy PE směrovačů:

1. Internet edge
2. MPLS VPN hraniční směrovače

Internet edge směrovače, které obsahují plnou internetovou směrovací tabulku, jsou přímo připojeny k tranzitním poskytovatelům konektivity a tvoří hranici autonomního systému. S externími sítěmi (síť poskytovatele připojení, ISP) komunikují protokolem eBGPv4. Dovnitř sítě propagují pouze default gateway. Internet VPN bude jako jedna ze základních služeb, které budou poskytovány všem připojeným subjektům.

ad. 1) Vzhledem k Regionální datové síti Pardubického Kraje přichází v úvahu 2 možná řešení:

a) Využití stávajících PE směrovačů v DC

Jedná se o řešení s nízkými náklady, které nevyžaduje nový HW. Tj. současné PE budou sloužit jako PE, Internet Edge a Firewall (karta v PE). Stávající PE router(L3 switch) není vhodný jako plnohodnotný Internet Edge router (není schopen pojmout plnou internetovou směrovací tabulku, atd.).

Takové řešení znamená privátní autonomní systém(možnost kolize AS s jiným subjektem), přístup k Internetu přes ISP s využitím jeho veřejných IP adres.

b) Nasazení nových PE (Internet Edge) směrovačů

Takové řešení znamená možnost vytvoření veřejného Autonomního systému, vlastní rozsah veřejných IP adres (provider independent adresní rozsah), možnost připojení k jiným externím sítím (jiným AS) bez možné kolize. Schéma zapojení viz obrázek bod 3.8.

Problémem tohoto řešení je získání vlastního veřejného rozsahu adres. V současné době již v podstatě nejsou k dispozici IPv4 adresní rozsahy a proto je jejich získání u RIPE téměř nemožné. Možnou variantou je rozsah IPv6 adres.

ad. 2) MPLS VPN hraniční směrovače (PE směrovače), které poskytují připojení pro koncové sítě, přiřazují paketům značky, které se používají v páteři. Hraniční směrovače také formují (shaping), ořezávají, implementují QoS tím, že značkují pakety v závislosti na jejich nastavení DiffServ.

Považujeme za důležité, aby technologie umožňovala z důvodu pokročilého managementu provozovaných služeb, hierarchické QoS (na fyzický port dle VLAN a zároveň služby setu VLAN).

Každý hraniční směrovač bude mít alespoň jeden port směřující do páteře. V počátečních fázích bude možná nutné připojovat hraniční směrovače vzájemně bez použití páteřního směrovače. Konkrétní zapojení bude vycházet z prováděcích projektů, které budou reflektovat dostupnou fyzickou infrastrukturu.

Hraniční směrovač, který má více než jeden páteřní interface se nazývá hraniční LSR. Přepínání paketů mezi těmito porty je identické s páteřními LSR.

Hraniční směrovače slouží jako přístupová zařízení pro přístupovou technologii Ethernet a Ethernet trunk (802.1q) s rychlostmi portů 1G/10G.

Hraniční směrovače budou připojeny k páteřním směrovačům výhradně technologií Ethernet tak, aby byla zachována podmínka vysoké dostupnosti – odolnost vůči selhání portu, procesoru, linkové karty a napájecího zdroje.

Detail topologie sítě podává dokument prováděcí projekt, kapitola 1.4.

7.4 CE směrovače

Směrovače sloužící pro přístup do sítě umístněné v lokalitách, patřících jenom do jedné směrovací oblasti nazýváme CE (customer edge) směrovače. Tento dokument se primárně nezabývá směrovači, které nejsou a nebudou ve správě Pardubického kraje, pouze obsahuje set doporučení, které má každý subjekt, který se bude připojovat do regionální sítě Pardubického kraje, splňovat.

Nároky na CE směrovače jsou podstatně nižší než na PE a LSR (P) směrovače, jejich hlavní úkol je propojit LAN připojovaného subjektu do nejbližšího PE směrovače. Specifikace rozhraní jednotlivých CE směrovačů bude součástí detailních technických návrhů pro každou lokalitu a bude záviset od možností přístupu do páteře sítě.

Detail požadavků na CE směrovače podává dokument prováděcí projekt, kapitola 1.6.4.

7.5 L2 infrastruktura

V různých místech sítě bude potřeba použít stohovatelné a škálovatelné ethernet přepínače. Ve vybraných situacích musí být schopné poskytnout PoE (power over ethernet) pro telefonní zařízení. Každý přepínač by měl disponovat alespoň 2 gigabitovými uplink porty a podporovat 802.1X, 802.1q trunking, STP, VLAN. Portová rychlost na přepínačích musí být volitelná mezi 10/100/1000 Mbit/s. Všechny přepínače nově instalované a malé přepínače na lokalitách musí splňovat požadavky na centrální autentizaci a autorizaci a musí být umožněn vzdálený dohled pomocí protokolu SNMP.

8. Obecné požadavky na aktivní prvky

8.1 Páteřní směrovače

Modulární architektura (fyzická či virtuální)

Možnost rozšíření o další moduly / rozhraní

Redundance ve všech ohledech (redundance route procesoru, redundance přepínací matice, redundance napájení, redundance portů) – variantně redundance v rámci fyzického chassis nebo virtuálního chassis tvořeného standalone jednotkami

- Linková rozhraní typu 10 gigabit ethernet, gigabit ethernet
- Wire-speed performance
- Možnost přidávání a odebírání modulů provozu (online insertion and removal)
- Podpora 802.1q trunking
- Podpora IPv4 i IPv6 rozhraní / routingu
- Podpora více virtuálních forwardovacích entit / tabulek / instancí
- Podpora statického routingu a L3 protokolů OSPF, BGP
- Podpora MPLS / MPLS VPN
- Podpora VPLS
- Podpora víceúrovňového QoS modelu
- Podpora IPv4/IPv6 multicast

8.2 Hraniční směrovače

- Modulární architektura (fyzická či virtuální)
- Možnost rozšíření o další moduly / rozhraní
- Redundance ve všech ohledech (redundance route procesoru, redundance přepínací matice, redundance napájení, redundance portů) – variantně redundance v rámci fyzického chassis nebo virtuálního chassis tvořeného standalone jednotkami
- Linková rozhraní typu 10 gigabit ethernet, gigabit ethernet
- Wire-speed performance
- Možnost přidávání a odebírání modulů provozu (online insertion and removal)
- Podpora 802.1q trunking
- Podpora IPv4 i IPv6 rozhraní / routingu
- Podpora více virtuálních forwardovacích entit / tabulek / instancí
- Podpora statického routingu a L3 protokolů OSPF, BGP
- Podpora MPLS / MPLS VPN
- Podpora VPLS
- Podpora víceúrovňového QoS modelu
- Podpora prioritizace provozu dle L2 i L3 (COS, DSCP)
- Podpora striktní i váhované prioritizace provozu
- Podpora RED/WRED mechanismu
- Podpora shapingu / policingu

- Podpora IPv4/IPv6 multicast
- Podpora L2 / L3 / L4 ACL (IPv4 i IPv6)

8.3 Standardy pro CE směrovače

Detail včetně variant (L3/L2) podává dokument prováděcí projekt, kapitola 1.6.4.

9. Bezpečnost komunikační infrastruktury

Síťová bezpečnost je jednou ze základních služeb, kterou regionální síť Pardubického kraje nabízí a jako taková musí prostupovat všemi funkčními bloky, ze kterých se komplexní IT infrastruktura Pardubického kraje skládá. Rozsah bezpečnostních prvků a procesů je determinován organizačními požadavky a potenciálními riziky, které Pardubickému kraji hrozí. V této kapitole je pouze stručný souhrn některých faktů, nad kterými se krajský úřad Pardubického kraje musí zamýšlet, souhrnný návrh bezpečnosti je mimo rozsah této koncepce.

9.1 Požadavky na síťovou bezpečnost

Síťová bezpečnost by měla v každém případě zajišťovat minimálně následující výčet požadavků:

- Ochrana regionální sítě před útokem z externích sítí (typicky Internet, propojení s dalšími institucemi, sítě dodavatelů atd.),
- Používání zdrojů v regionální síti musí být povoleno pouze autorizovaným uživatelům,
- Zabránění interním uživatelům v úmyslných i nechtěných či bezděčných incidentech nebo útocích,
- Regionální síť musí nabízet různé úrovně přístupu závislé na typu uživatelů a jejich přístupových práv,
- Regionální síť musí chránit data a datové zdroje před nesprávným použitím či jejich poškozením,
- Regionální síť musí být z hlediska bezpečnosti v souladu s bezpečnostní legislativou, všeobecnými i právními standardy a v neposlední řadě musí odrážet interní bezpečnostní politiku.

Při splnění všech výše vyjmenovaných kritérií musí být regionální síť Pardubického kraje transparentní pro své uživatele, jednoduchá na administraci a nesmí omezovat služby, které Pardubický kraj prostřednictvím regionální sítě bude svým uživatelům nabízet.

9.2 Ohrožení a rizika

Ohrožení bezpečnosti regionální sítě můžeme rozdělit do těchto základních kategorií:

Rekognoskace

Znamená aktivní průzkum a sběr informací o regionální síti, uživatelích, datech a dalších prvcích celého IT systému. V oblasti síťové bezpečnosti obvykle je obvykle pouze přípravnou fází k hlavnímu útoku na vybraný cíl.

Neautorizovaný přístup

Po zjištění nezbytného množství informací pomocí výše zmíněné rekognoskace je hlavním cílem získání přístupu do vybraného zdroje dat či přístupu k vybrané části regionální sítě. Techniky získání neautorizovaného přístupu se pohybují v rozmezí čistě technických (využití bezpečnostní mezery v

určitém systému) až po techniky čistě sociální (vylákání informací nezbytných k přístupu na základě lživých informací či požadavků, jedná se o tzv. social engineering techniky).

Zamezení služby

Pokud pomineme riziko samotného získání přístupu k vybraným informacím, je hlavním ohrožením zamezení přístupu k datům či výpočetním zdrojům autorizovaným uživatelům (jedná se o tzv. Denial of Service útok). Pomocí technických prostředků dochází k zamezení přístupu k informacím, například přetížením části sítě, samotného serveru či databáze.

K zajištění odpovídající úrovně bezpečnosti a ochrany síťových zdrojů musí být síťové procedury a technologie zaměřeny především na tato bezpečnostní rizika:

Důvěrnost dat

Zajištění důvěrnosti dat znamená, že pouze autorizovaní uživatelé mají přístup k senzitivním informacím. Toto opatření minimalizuje možnost ztráty důvěrných dat s následnými převážně ekonomickými dopady na organizaci.

Integrita dat

Odpovídající prostředky musí zabezpečit, že pouze autorizovaní uživatelé mohou měnit senzitivní data a informace a zároveň je zajištěna jejich pravost.

Dostupnost dat

Dostupnost znamená nepřerušitelný přístup ke zdrojům v rámci regionální sítě. Odpovídající bezpečnostní prostředky a procesy zabraňují ztrátě produktivity i dalším problémům způsobených nedostupností zdrojů.

9.3 Realizace bezpečné infrastruktury

Zajištění bezpečnosti zdrojů v regionální síti je nikdy nekončící proces, založený na nastavené bezpečnostní politice organizace. Organizační požadavky, potřeby poskytovaní služeb a analýza rizik Pardubického kraje jsou základními stavebními kameny pro nastavení bezpečnostní politiky a její následné vymáhání.

Hlavní oblasti, které je tedy třeba vzít do úvahy při realizaci bezpečné síťové infrastruktury:

Potřeby Pardubického kraje

Jaké služby a za jakých podmínek chce Pardubický kraj poskytovat svým uživatelům (interním či externím).

Analýza rizik

Výstupem je ohodnocení rizik ze ztrát zmíněných v předchozích odstavcích, ve výsledné analýze musí být v rovnováze rizika a cena za jejich eliminaci.

Bezpečnostní politika

Bezpečnostní politika obsahuje metody, standardy a návody, jak se vyhnout bezpečnostním hrozbám a rizikům.

Standardy

Vždy je třeba zohlednit de-jure i de-facto standardy včetně tzv. best practices doporučených výrobci či nezávislými poradci v oblasti bezpečnosti.

Postupy a procesy

Je nutné nastavit, jakým způsobem bude probíhat monitorování regionální sítě, systém údržby, odpovědi na bezpečnostní a jiné incidenty a v neposlední řadě zajistit vyhovění případným požadavkům auditu.

Bezpečnostní politika je souhrn cílů, plánů, úkolů a pravidel pro uživatele a administrátory regionální sítě, požadavků na samotné součásti regionální sítě a v neposlední řadě na management, které dohromady tvoří celek popisující kompletní prostředí z hlediska informací a bezpečného nakládání s nimi. Stručný a velmi prakticky orientovaný úvod do problematiky bezpečnostní politiky lze nalézt například v dokumentu RFC 2196 (Site Security Handbook).

Nezbytnost bezpečnostní politiky vyplývá z jejího hlavního poslání: informovat uživatele, administrátory a management o požadavcích na jejich chování v prostředí regionální sítě a zároveň na odpovědnost za jejich chování a nutnost ochraňovat prostředky a systémy regionální sítě. Bezpečnostní politika nastavuje rámec pro implementaci jednotlivých technologií, které pomáhají technickými prostředky vymáhat nastavenou politiku.

Mezi otázky, které zcela jistě nastoluje, patří:

- Definuje aktiva společnosti, a jakým způsobem mají být používána,
- Definuje role jednotlivých uživatelů,
- Pomáhá určovat nástroje a procedury nezbytné k implementaci bezpečnostní politiky,
- Definuje, jakým způsobem identifikovat a řešit bezpečnostní incidenty,
- Při nastavování bezpečnostní politiky jsou zcela jistě na místě tyto otázky:
- Která data a zdroje budou pokryta bezpečnostní politikou,
- Na základě jakých podmínek je povolena komunikace mezi jednotlivými síťovými elementy (uživateli, aktivními prvky, zdroji dat, servery atd.),
- Jakým způsobem bude verifikována správnost implementace bezpečnostní politiky,
- Jakým způsobem bude zjišťováno narušení bezpečnostní politiky,
- Jaký je dopad takového narušení,
- Jaké akce se provedou po zjištění takového narušení,
- Jak již bylo řečeno výše, rizika je možné ohodnotit a na základě tohoto ohodnocení nastavit příslušné bezpečnostní politiky a implementovat příslušné nástroje a technologie. Risk management se snaží minimalizovat rizika na akceptovatelnou úroveň (nelze dostupnými prostředky eliminovat rizika úplně, lze je pouze minimalizovat na akceptovatelnou úroveň).
- Každá organizace definuje akceptovatelnou úroveň na základě mnoha faktorů, jako například:
- Hodnota dat uchovávaných a produkovaných dat v rámci organizace
- Pravděpodobnost ztráty dat v případě útoku
- Vážnost a pravděpodobnost útoku

Proces zajištění síťové bezpečnosti je nikdy nekončící, pro uživatele neviditelný či naopak způsobující potíže v jednoduchosti přístupu k požadovaným informacím a pro management nekončící zdroj bitev o velikost prostředků pro zajištění tohoto procesu a následně celé bezpečnosti.

Celý proces je ve skutečnosti poměrně jednoduchý, nicméně sestává ze stovek jednotlivých akcí, jejich souhrn je v těchto čtyřech základních oblastech:

- Chránit. Na základě nastavených pravidel nacházet takové technologické prostředky a následně je implementovat, aby dokázaly pomoci vymáhat nastavenou bezpečnostní politiku.
- Monitorovat. Neustálé monitorování je nezbytným prvkem, který zajišťuje včasné rozpoznání narušení nastavených pravidel či technických prostředků.
- Testovat. Sebelépe vymyšlený systém se neobejde bez testování, zda je schopen reálného provozu. Do této oblasti spadají také veškeré vyžádané i dobrovolné audity, penetrační testování a další možné druhy testů.
- Zlepšovat. Jako všechny ostatní systémy a procesy i bezpečnost prochází svým vývojem a to, co včera bylo nastaveno jako bezpečnostní pravidlo, se může v příštím okamžiku stát bezpečnostním rizikem.
- Detail podává dokument bezpečnostní dokumentace.

10. Realizace

Informaci o průběhu realizace stávající sítě podávají dokumenty: předimplementační analýza, projektová technická dokumentace, prováděcí dokumentace a prováděcí projekt. Realizace budoucích částí sítě budou popsány konkrétněji dle cílů a zdrojových možností.

11. Filozofie nové infrastruktury

11.1 Filozofie síťové infrastruktury

Základní otázka při budování každé nové komunikační sítě je, jak umožnit zároveň fungování stávajících sítí a uživatelů a současně, jak postupně nahradit zastaralou infrastrukturu.

Jediné možné řešení je paralelně se stávajícími sítěmi začít budovat základ nové sítě. K tomuto základu se budou postupně připojovat a kompletně se integrovat stávající oddělené a samostatně existující sítě. Je to jediný použitelný koncept, který dovolí začít s budováním poměrně brzy a který zároveň je schopen co nejméně ovlivnit stávající prostředí (tj. běžnou denní práci uživatelů). Jedná se o koncept, který s úspěchem využívají velcí operátoři ve chvíli, kdy jejich páteřní infrastruktura přestane vyhovovat novým požadavkům. Položí se základ nové páteřní infrastruktury a stávající technologie se posouvá k okrajům sítě. Tato metoda dovoluje začít využívat nové technologie a možnosti postupně tak, jak jsou připraveny jednotlivé skupiny uživatelů (či lokalit) a zároveň maximálně využívá technologii stávající tam, kde je pro uživatelské nároky dostačující. Nová infrastruktura bude postavena na technologii MPLS, která umožňuje pružné řešení pro provoz mnoha logicky oddělených sítí na společné infrastruktuře se zajištěním bezpečnosti a kvality služby.

Před zahájením výstavby nového prostředí je nicméně potřeba definovat požadavky na novou infrastrukturu. To není v případě současného prostředí zcela jednoduché, protože subjektů je mnoho a

provozovaných služeb ještě více. Zároveň vznikají nové požadavky ať už ze strany nových aplikací, tak ze strany zadavatele na typ služeb, které chce poskytovat svým uživatelům a široké veřejnosti.

Je zřejmé, že nové prostředí bude muset být lehce naddimenzováno, nebo postaveno natolik univerzálně, aby pružné změny umožňovalo. Zde navrhujeme využít již existujících zkušeností z podobných prostředí jinde ve světě. Dá se předpokládat, že minimálně 70% požadavků bude stejných, zbývajících 30% budou lokální odlišnosti a jedinečné záležitosti.

Jednou z hlavních otázek je, zda síť vlastnit, provozovat vlastními silami, či využívat služeb externích firem, tj. outsourcingu. Protože se dá předpokládat, že při budování nové sítě je snaha maximalizovat existující zdroje (například optická vlákna) a zároveň možnost síť použít pro řízení například v krizových situacích je jedno z možných řešení vlastnit infrastrukturu a nechat si ji provozovat na základě kontraktu. Pro toto řešení je vhodné použít například metody PCO (PrimaryContractor), což ve skutečnosti znamená vztah Pardubického kraje pouze s jedním dodavatelem, který si na případné další služby sám najímá další organizace (ovšem za podmínek definovaných objednatelem služby, tj. Pardubickým krajem). Otázky správy a dalšího rozvoje celého prostředí budou postupně rozebrány v následujících kapitolách.

Základem nového prostředí jsou komunikační spoje založené na optických trasách. Optické trasy by měly být budovány tak, aby byly v maximální možné míře nezávislé. Je nutno vyvarovat se používání stejných kabelových tras, rozvodů a podobně.

Fyzická topologie sítě by měla být zachována, případně rozšířena, tj. topologie typu full-mesh anebo spojitá jedno nebo víceúrovňová hvězda z pohledu datových center. Optická infrastruktura řešení aktivních prvků i pasivní optické infrastruktury musí umožňovat implementaci technologie CWDM nebo DWDM. Jedná se především o požadavek podpory „barevných“ optických transceiverů všemi nabízenými aktivními prvky a možnosti pasivní infrastruktury rozšířit přenášené kapacity využitím dalších vlnových délek.

Detailní popis (schéma topologie, optické infrastruktury a infrastruktury CWDM multipexů) podává prováděcí projekt, kapitola 1.1.3, 1.2 a 1.3.

11.2 Požadavky na připojované lokality

Aby nová infrastruktura mohla poskytovat všechny služby v předem definované kvalitě, budou muset na druhou stranu připojované subjekty splňovat určité podmínky. Tyto podmínky se zakládají na obecných standardech, ať již se jedná o bezpečnost či různé síťové standardy. Tento set předpokladů bude platný pro lokality spravované centrálně i pro lokality, které budou mít samostatné řešení provozu.

Bez ohledu na pořadí budou mezi tyto požadavky patřit následující:

Koncové zařízení (aktivní prvek) na straně připojované lokality. Ten bude splňovat síťové standardy, které budou definovány týmem pro správu infrastruktury sítě (detailní požadavky jsou definovány v bodě 8.3). Stejným způsobem musí umožňovat nastavení bezpečnostních pravidel, tak jak budou definovány bezpečnostním týmem (detailní popis podává bezpečnostní dokumentace, převážně kapitola 4).

Bezpečnost. Komunikace z každé lokální sítě (oběma směry) bude zajištěna standardními bezpečnostními mechanismy, mezi které bude zcela jistě patřit firewall či antivir a další podobné prostředky (například na filtrování obsahu přenášených dat). Detailní popis podává bezpečnostní dokumentace.

Komunikace s externími subjekty. Lokální sítě a jejich uživatelé, kteří budou chtít využívat všech služeb poskytovaných páteřní infrastrukturou, budou připojeny pouze do páteřní sítě. Veškerá externí připojení (například subjektů, které vykonávají určitý typ vzdálené podpory) budou připojeny centrálně určenými body a jejich komunikace bude pomocí dedikované VPN přivedena do příslušné lokální sítě. Detailní popis připojení k externím subjektům podává prováděcí projekt, kapitola 3.

Design lokální sítě. Pro snadnou údržbu a možnost bezproblémového zavádění nových typů služeb bude nutné dodržovat určitá pravidla a doporučení pro design samotných lokálních sítí (rozdělení sítě do jednotlivých segmentů, typ IP adresace a mnohé další). Detailní popis podává technologická dokumentace, kapitoly 1.4, 1.5, 1.6, 2., 6.2 a dokument katalog služeb.

Management a možnost vzdáleného zásahu. Pro případy nouze či řešení kritických situací ovlivňujících koncové uživatele či poskytované služby bude zajištěna podpora pro zásah centrálního týmu podpory.Detailní popis podává provozní dokumentace, servisní manuál a havarijní plány.

Jak již bylo řečeno dříve, bude pravděpodobně existovat více různých požadavků na parametry připojení koncové lokality do páteřní sítě. Hlavní rozdíly budou v kapacitě připojení (kapacita přístupové linky/ počet vláken v lokalitě), v požadavcích na dostupnost (způsob připojení) a v zajištění dalších služeb sítě (bezpečnost, síťové parametry jako jsou například zpoždění a další). Obecně se dá říci, že budou existovat tyto druhy lokalit:

Lokalita typ I (Datové centrum) znamená největší nároky na dostupnost připojení a zároveň má velké nároky na kapacitu připojení. Tento typ lokality bude připojen pomocí dvou samostatných přístupových linek (linka minimálně s jedním párem optických vláken), které budou každá ukončena v jiném přístupovém bodě páteřní infrastruktury (odlišné PoP – Point of Presence). V ideálním případě bude každá z přístupových linek vedena do jiného listu páteřní infrastruktury (tj. připojena do různých optických kruhů), přičemž pro zvýšení maximální dostupnosti by bylo nutné vést každou z přístupových linek jinými fyzickými trasami od lokality samotné. Lze uvažovat i o využití jiného typu přístupové technologie (například bezdrátové), nicméně pouze v případě, že bude svými parametry rovnocenná primárnímu přístupovému okruhu.

Lokalita typ II (Agregační lokalita) znamená připojení dvěma linkami (linka minimálně s jedním párem optických vláken), které však budou ukončeny ve stejném přístupovém místě páteřní sítě. Vzhledem k tomu, že samotné PoP místa budou budována s vysokou dostupností (popis PoP je uveden dále v textu), je zřejmé, že hlavní důvod pro využití tohoto typu připojení bude nemožnost využít variantu typ I. pro neexistenci adekvátních fyzických tras nebo specifické požadavky na komunikaci v rámci určité části páteřní sítě.

Lokalita typ III (koncová lokalita) bude připojena jednou linkou (linka minimálně s jedním párem optických vláken).

Všechny ze zmíněných variant připojení budou klást nároky na design samotné lokální sítě. Je zřejmé, že v případě lokality prvního typu bude muset být samotná lokální síť postavena jako robustní s vysokou kapacitou, která umožní využít duálního připojení do páteřní sítě. Výše jsou zmíněny obecné zásady, které budou muset lokální sítě splňovat, nicméně konkrétní design či jeho úpravy v konkrétních lokalitách budou vycházet z konkrétních podmínek zjištěných analýzou stávajícího stavu a definicí požadavků na komunikace v rámci lokality samotné. Předpokládané rychlosti připojení jednotlivých typů lokalit by měly korespondovat se současným stavem, tj. kapacity 1Gb, ideálně s možností navýšení na 10Gb.

11.3 Typy lokalit a jejich připojení

Současné lokality:

Typ lokality	Adresa
Datové centrum	Pardubická krajská nemocnice, a.s. Kyjevská 44, 532 03 Pardubice
Agregační lokalita	Litomyšlská nemocnice, a.s. J. E. Purkyně 652, 570 14 Litomyšl
Koncová lokalita	Chrudimská nemocnice, a.s. Václavská 570, 537 27 Chrudim
Koncová lokalita	Orlickoústecká nemocnice, a.s. Čs. armády 1076, 562 18
Koncová lokalita	Svitavská nemocnice, a.s., Kolárova 7, 568 02 Svitavy
Koncová lokalita	Zdravotnická záchranná služba Pardubického kraje, Průmyslová 450, 530 03 Pardubice
Datové centrum	Krajský úřad Pardubického kraje, Komenského náměstí 125, 532 11 Pardubice
Koncová lokalita	Městský úřad Chrudim, Resselovo náměstí 77, 537 16 Chrudim
Koncová lokalita	Městský úřad Litomyšl, Bří Šťastných 1000, 570 20 Litomyšl
Koncová lokalita	Magistrát města Pardubice, Pernštýnské náměstí 1, 530 21 Pardubice
Koncová lokalita	Městský úřad Svitavy, T. G. Masaryka 40/25, 568 02 Svitavy
Koncová lokalita	Městský úřad, Ústí nad Orlicí Sychrova 16, 562 24 Ústí nad Orlicí

Lokality definované pro budoucí rozvoj:

Typ lokality	Adresa
Koncová lokalita	Městský úřad Česká Třebová, Staré náměstí 78, 560 02 Česká Třebová
Koncová lokalita	Městský úřad Hlinsko, Poděbradovo náměstí 1, 539 23 Hlinsko
Koncová lokalita	Městský úřad Holice, Holubova 1, 534 01 Holice
Koncová lokalita	Městský úřad Králíky, Velké náměstí 5, 561 69 Králíky
Koncová lokalita	Městský úřad Lanškroun, nám. Jana Marků 12, 563 16 Lanškroun
Koncová lokalita	Městský úřad Moravská Třebová, T. G. Masaryka 29, 571 01 Moravská Třebová
Koncová lokalita	Městský úřad Polička, Palackého nám. 160, 572 01 Polička
Koncová lokalita	Městský úřad Přelouč, Československé armády 1665, 535 33 Přelouč
Koncová lokalita	Městský úřad Vysoké Mýto, B. Smetany 92, 566 32 Vysoké Mýto
Koncová lokalita	Městský úřad Žamberk, Masarykovo nám. 166, 564 01 Žamberk

12. Propojení s dalšími subjekty

Organizace připojované do páteřní sítě budou mít různé požadavky na samotnou konektivitu i na kvalitu dalších služeb poskytovaných sítí. Jednotlivé organizace se budou lišit dle své velikosti, dle množství poskytovaných agend, dle požadavků na rychlost kapacitu připojení a v neposlední řadě dle toho, zda budou svůj provoz zajišťovat sami nebo s pomocí centrálního týmu a centrálně poskytovaných služeb.

Celá regionální síť bude propojena s mnoha externími sítěmi a uživateli včetně sítě Internet. Pro dodržení standardů a parametrů, které má nová regionální síť poskytovat svým uživatelům bude nutné všechna externí připojení zmapovat a nastavit pokud možno stejná pravidla pro vzájemnou komunikaci mezi nimi a prostředím regionální sítě Pardubického kraje.

Propojení se sítí Internet je popsáno v samostatné kapitole, Internet bude připojen pomocí dvou samostatných linek do dvou datových center, tedy do dvou páteřních prvků.

Všechny externí připojení budou koncentrovány přes centrální VPN koncentrátory/firewally a pomocí samostatných VPN přivedeny do příslušných koncových sítí.

Přístup jednotlivých uživatelů bude řešen podobným způsobem pomocí VPN koncentrátoru/firewallu. Bezpečnost těchto připojení bude řešena standardním způsobem, tj. pomocí AAA mechanismů a při zajištění klasickými bezpečnostními prvky typu firewall a podobně.

13. Design přístupových míst (POP)

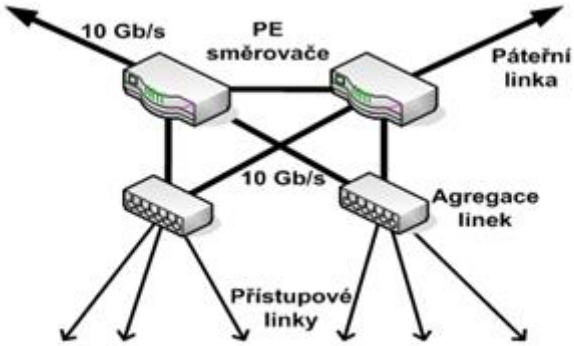
Přístupová místa sítě (PoP – Point of Presence) budou budována na základě těchto zásad:

- Budou umístěna v místech snadno dostupných pro možnosti servisních zásahů.
- Každý z bodů bude poskytovat dostatek prostoru (fyzického i v rámci použitých aktivních prvků) na budoucí rozšiřování.
- Každý z bodů přístupu bude budován s ohledem na vysokou propustnost a dostupnost.
- Všechny body budou postaveny na základě stejných principů.
- V ideálním případě bude pro každý bod zajištěno záložní napájení pro případ výpadku.
- Každý použitý aktivní prvek bude obsahovat redundantní prvky (popsáno výše ve standardech pro PE směrovače).

Každý přístupový bod může koncentrovat mnoho přístupových linek, každý z nich bude mít minimálně dva páteřní spoje. Na následujícím obrázku je znázorněn ideový návrh přístupového bodu, který je vysoce propustný s vysokou dostupností. Vzhledem k výkonnosti a cenové přijatelnosti budování těchto přístupových míst je koncentrace přístupových linek řešena pomocí samostatného aktivního prvku, který obsahuje dostatek portů pro různé přístupové technologie a do samotného PE směrovače je připojen pomocí vysokorychlostního připojení o kapacitě 10 Gb/s. Každý z těchto koncentrátorů je připojen do obou PE směrovačů v přístupovém bodě.

Navržené řešení je vysoce škálovatelné za přijatelných finančních nákladů. Při velkém množství přístupových linek se zvyšuje počet agregačních prvků, pro zvýšení propustnosti komunikace mezi agregačními a PE prvky stačí přidat pouze jeden další 10 Gb/s spoj pro každou cestu. Tyto spoje jsou

schopny fungovat dohromady a z hlediska propustnosti tohoto spojení se tvářit jako jeden spoj (tj. jako 20 Gb/s linka).



Optická pasivní infrastruktura přístupových lokalit, resp. její přivedení do jednotlivých lokalit, bude řešeno dle individuálních projektů pro jednotlivé lokality. Tato optická infrastruktura bude vždy terminována na vybraném místě budovy v místním rozvaděči budovy.

Detail připojení externích sítí (využití PoP) podává dokument prováděcí projekt, kapitola 3.

14. Provoz

Detailní popis stávající sítě podává provozní dokumentace. Tato je dimenzována i pro budoucí rozvoj a její změny se předpokládají pouze v případě výjimek vůči standardům sítě.

15. Provoz a personální zabezpečení provozu komunikační infrastruktury

Detailní popis podává provozní dokumentace včetně popisu personálního zabezpečení – kapitola 2.2.1.

Stav popsaný ve stávající dokumentaci není potřeba v případě rozvoje standardizované sítě dále rozšiřovat.

16. Realizace komunikační infrastruktury

Vlastní realizační tým by měl vždy sestávat z pracovníků zadavatele a vhodným způsobem zapojených externích subjektů. Mezi tyto externí subjekty by měly zcela jistě patřit:

- Externí specializované firmy, které budou dodávat funkční celky celkového řešení na základě zadání zadavatele.
- Externí specialisté a konzultanti, kteří budou najímáni buď pro specializované úkoly, nebo pro celkový dohled nad budovanými systémy.
- Externí projektová kancelář, která bude řídit implementaci všech schválených projektů.
- Specialisté či dedikované osoby ze všech organizací zřizovaných či spravovaných zadavatelem v závislosti na typu implementovaných řešení.
- Veškeré realizované projekty budou probíhat na základě standardních projektových postupů.

17. Požadavky na personální zabezpečení provozu komunikační infrastruktury

Provoz nově vybudované komunikační infrastruktury lze zabezpečit částečně vlastními silami pracovníků Pardubického krajského úřadu, ale část specializovaných služeb bude nutné nakupovat od externích dodavatelů – zejména s ohledem na to, že se jedná o úzce specializované činnosti, pro které nemá běžný úřad typu krajského úřadu Pardubického kraje personální kapacity. V takovém případě hovoříme o jisté formě outsourcingu. V obou zmiňovaných případech počítáme s tím, že infrastruktura samotná je ve vlastnictví Pardubického kraje.

Detailní popis personálního zabezpečení provozu podává provozní dokumentace, kapitola 2.2.1.

Požadavky na skupiny pracovníků, ať již budou zajištěny pracovníky Pardubického kraje, nebo externími dodavateli popisují následující kapitoly.

17.1 Pracovník dohledového centra

Požadavky na znalosti pracovníka dohledového centra se mohou lišit od níže uvedených, vždy bude záviset na rozsahu služeb poskytovaných interními silami. Zde je uveden ideální příklad univerzální odbornosti:

A. Nutné znalosti:

- metody dohledu a řízení sítě (SNMP i za pomoci nástrojů příkazové řádky)
- základy programování v unix shell
- všeobecná konceptuální znalost principů aplikací klient/server
- všeobecné znalosti použitého hardware
- obecné zásady bezpečnosti v Unix prostředí (users/passwords, rights)
- automatizace úloh za pomoci cron
- koncept LAN (switching, bridging)
- koncept WAN (znalost celé sítě od fyzické vrstvy až po síťovou)
- koncept síťové bezpečnosti (firewalls, gateways, proxies)
- OSI model
- TCP/IP (IP adresace, netmasks)
- použité směrování v sítích WAN, LAN
- znalost operačního systému a konfigurace použitých aktivních prvků
- znalost operačních systémů Unix a Windows
- principy fungování support organizace – ITIL - (trouble ticketing systems, eskalační procedury)

B. Doporučené znalosti:

- základy programování v jazyce perl, PHP, http, cgi
- principy fungování LDAP, používání i přes nástroje příkazové řádky
- koncept synchronizace času
- kabeláže (typy konektorů a kabelů)
- UPS, strategie zálohování napájení

17.2 Specialista datového centra

Všechny nepovinné znalosti a zručnosti pracovníka dohledu jsou zde povinné. Kromě již výše zmíněných týkajících se serverových technologií a jejich zapojení mohou být další požadavky tyto:

- strategie zálohování dat
- administrace MS Exchange
- administrace MS SQL
- Fibre Channel koncept
- Shared storage concepts (raid, raid levels)

- konfigurace a troubleshooting DNS
- konfigurace synchronizace času (ntp v4)
- antivir, antispam strategie a koncepty jejich použití v DC
- SMTP koncept
- PAM autentizace
- SSL a S/MIME certifikáty, PKI infrastruktura, digitální podpisy
- znalost šifrovacích algoritmů, principů a software
- rozsáhlé znalosti problematiky síťové bezpečnosti
- virtualizační metody a nástroje
- konfigurace a troubleshooting základních internetových služeb (dns, www, imap, pop3, smtp, ssh)
- bezpečnost v prostředí Unix (selinux, iptables, chroot jails)
- principy fungování support organizace – ITIL - (trouble ticketing systems, eskalační procedury)

Popsaný ideální stav znalostí se může lišit v závislosti na konkrétních realizovaných řešeních a podmínkách. Taktéž může nastat situace, že tento soupis znalostí bude rozdělen mezi více specialistů (typicky mezi odborníky na síť a odborníky na použité servery). V tomto výčtu zcela chybí popis nutných znalostí pro dohled nad konkrétními aplikacemi, tato oblast není kryta touto koncepcí.

17.3 Specialista datové sítě

A. Nutné znalosti:

- všeobecná konceptuální znalost principů aplikací klient/server
- všeobecné znalosti použitého hardware
- koncept LAN (switching, bridging)
- koncept WAN (znalost celé sítě od fyzické vrstvy až po síťovou)
- koncept síťové bezpečnosti (firewalls, gateways, proxies)
- OSI model
- TCP/IP (IP adresace, netmasks)
- použité směrování v sítích WAN, LAN
- znalost operačního systému a konfigurace použitých aktivních prvků (v ideálním případě podložené certifikací příslušného výrobce)
- znalost operačních systémů Unix a Windows
- principy fungování support organizace – ITIL - (trouble ticketing systems, eskalační procedury)

B. Doporučené znalosti:

- obecné zásady bezpečnosti v Unix prostředí (users/passwords, rights)
- koncept synchronizace času
- kabeláže (typy konektorů a kabelů)
- UPS, strategie zálohování napájení

17.4 Administrátor RDS PK

A. Nutné znalosti:

- všeobecná konceptuální znalost principů aplikací klient/server
- všeobecné znalosti použitého hardware
- koncept WAN

B. Doporučené znalosti:

- koncept síťové bezpečnosti (firewalls, gateways, proxies)
- OSI model

17.4.1 Správce PE lokality

A. Nutné znalosti:

- všeobecná konceptuální znalost principů aplikací klient/server
- všeobecné znalosti použitého hardware
- metody dohledu a řízení sítě (SNMP i za pomoci nástrojů příkazové řádky)
- koncept LAN (switching, bridging)
- koncept WAN (znalost celé sítě od fyzické vrstvy až po síťovou)
- principy fungování support organizace – ITIL - (trouble ticketing systems, eskalační procedury)
- koncept síťové bezpečnosti (firewalls, gateways, proxies)
- OSI model
- TCP/IP (IP adresace, netmasks)
- použité směrování v sítích WAN, LAN

B. Doporučené znalosti:

- koncept synchronizace času
- kabeláže (typy konektorů a kabelů)
- UPS, strategie zálohování napájení

17.5 Správce CE lokality

A. Nutné znalosti:

- všeobecná konceptuální znalost principů aplikací klient/server
- všeobecné znalosti použitého hardware
- metody dohledu a řízení sítě (SNMP i za pomoci nástrojů příkazové řádky)
- koncept LAN (switching, bridging)
- koncept WAN (znalost celé sítě od fyzické vrstvy až po síťovou)
- principy fungování support organizace – ITIL - (trouble ticketing systems, eskalační procedury)
- koncept síťové bezpečnosti (firewalls, gateways, proxies)

- OSI model
- TCP/IP (IP adresace, netmasks)
- použité směrování v sítích WAN, LAN

B. Doporučené znalosti:

- kabeláže (typy konektorů a kabelů)
- UPS, strategie zálohování napájení

17.6 Správce sítě TCK

A. Nutné znalosti:

- všeobecná konceptuální znalost principů aplikací klient/server
- všeobecné znalosti použitého hardware
- koncept LAN (switching, bridging)
- koncept WAN (znalost celé sítě od fyzické vrstvy až po síťovou)
- koncept síťové bezpečnosti (firewalls, gateways, proxies)
- OSI model
- TCP/IP (IP adresace, netmasks)
- použité směrování v sítích WAN, LAN
- znalost operačního systému a konfigurace použitých aktivních prvků (v ideálním případě podložené certifikací příslušného výrobce)
- znalost operačních systémů Unix a Windows
- principy fungování support organizace – ITIL - (trouble ticketing systems, eskalační procedury)

B. Doporučené znalosti:

- obecné zásady bezpečnosti v Unix prostředí (users/passwords, rights)
- koncept synchronizace času
- kabeláže (typy konektorů a kabelů)
- UPS, strategie zálohování napájení

17.7 Externí Správce sítě

A. Nutné znalosti:

- všeobecná konceptuální znalost principů aplikací klient/server
- všeobecné znalosti použitého hardware
- koncept LAN (switching, bridging)
- koncept WAN (znalost celé sítě od fyzické vrstvy až po síťovou)
- koncept síťové bezpečnosti (firewalls, gateways, proxies)
- OSI model
- TCP/IP (IP adresace, netmasks)
- použité směrování v sítích WAN, LAN

- znalost operačního systému a konfigurace použitých aktivních prvků (v ideálním případě podložené certifikací příslušného výrobce)
- znalost operačních systémů Unix a Windows
- principy fungování support organizace – ITIL - (trouble ticketing systems, eskalační procedury)

B. Doporučené znalosti:

- obecné zásady bezpečnosti v Unix prostředí (users/passwords, rights)
- koncept synchronizace času
- kabeláže (typy konektorů a kabelů)
- UPS, strategie zálohování napájení

18. Aplikační zabezpečení chodu

18.1 Management sítě

Detailní popis podává dokument provozní dokumentace, kapitoly 3.7, 3.8., dále dokument prováděcí projekt, kapitola 5.7.

18.2 Element management systém (EMS)

Součástí dodávek aktivních prvků musí být element management systém schopný alespoň do určité míry řídit a konfigurovat všechna zařízení v síti. Na speciální úkoly (například MPLS TE) bude nutno používat zvláštní nástroje.

18.3 Management přístupů

Radius

Radius systém musí být schopen autentizovat, autorizovat a účtovat (auditovat) všechny přístupy na všechna zařízení umožňující vzdálený přístup, včetně záložních zdrojů, elektrických distribučních panelů, ethernet přepínačů, P a PE směrovačů a podobně. Musí umožnit rozšířit jeho funkcionalitu o schopnost poskytnout zařízení dodatečnou konfiguraci v závislosti na uživateli, který se pokouší o autentizaci. Tato funkcionalita je nutná zejména při tvorbě L2TP nebo PPTP a PPPoE tunelů. Musí být schopen spolupracovat s LDAP.

LDAP:

LDAP musí být schopen uchovávat hierarchii uživatelů a jejich přístupových práv, musí být schopen autentizovat navazované LDAP spojení (nutné zejména pro autentizaci uživatelů konfiguračních nástrojů na bázi webových nástrojů), musí být schopen replikovat data z jiného LDAP zdroje, musí být schopen využívat jiné úložiště dat (SQL server), musí být schopen používat systém ověřování jednorázových hesel (RSA ACE).

RSA ACE:

Součástí existujícího síťového perimetru a systému zabezpečujícího SSL VPN je RSA ACE. Je nutné ověřit jeho kapacitní dimenzování a možnost jeho využití pro potřeby síťového managementu. Tato otázka a celkový přístup k bezpečnostním otázkám je problematika samostatné koncepce zabývající se čistě bezpečností.

18.4 Shromažďování a vyhodnocování logů (žurnál)

Shromažďování a vyhodnocování logů je zajištěno dohledovým systémem IMC. Detailní popis podává dokument prováděcí projekt, kapitola 5.7.

S ohledem na jeho budoucí širší a další úkoly je potřeba zabezpečit jeho provoz a redundanci a dále pravidelně a intenzivně se věnovat proškolování realizačního a dohledového týmu zadavatele.

18.5 Sledování bezpečnostních nastavení a jejich souladu s bezpečnostní politikou

Sledování bezpečnostních nastavení je zajištěno dohledovým systémem IMC. Detailní popis podává dokument prováděcí projekt, kapitola 5.7, 5.8. a 9.

18.6 Zálohování konfigurací

Detailní popis podává dokument prováděcí projekt, kapitola 5.8.

19. Integrace komunikační infrastruktury do informační platformy Pardubického kraje

Vzhledem k tomu, že služby nabízené subjektům připojeným do regionální sítě budou poskytovány z vnitřních systémů Pardubického kraje, je naprosto klíčovým úkolem zajištění bezpečnosti.

RDS (Regionální datová síť Pardubického Kraje) je a i v budoucnu bude, z důvodu bezpečnosti, provozního a personálního obsazení, samostatná síť oddělená od ostatních subjektů (LAN, MAN sítí, Internetu, případně sítí externích subjektů). RDS bude začleněna do stávajícího řízení informační bezpečnosti Krajského úřadu.

Technické řešení na úrovni aktivních prvků je již implementováno a popsáno výše. Navíc doporučujeme následující kroky:

- Zavedení řízení informační bezpečnosti (připojení k řízení informační bezpečností Pardubického kraje)
- Vytvoření obecného komunikačního a bezpečnostního modelu infrastruktury

19.1 Zavedení řízení informační bezpečnosti

Zavedení globálního řízení informační bezpečnosti v prostředí Pardubického kraje, bude dotčeno následujícími zákony:

1. Zákon o informačních systémech veřejné správy (ISVS),
2. obcích/krajích,
3. svobodnému přístupu k informacím,
4. ochraně osobních údajů,
5. elektronickému podpisu,
6. utajovaných skutečnostech,
7. právu autorském,
8. archivnictví.

Vzhledem k tomu, že Pardubický kraj je díky provozování regionální sítě v roli poskytovatele služeb, má za úkol řešit minimálně následující problematiku:

- rozmach a intenzivní používání ICT (informační a komunikační technologie),
- potřeba urychlit a zefektivnit výkon státní a veřejné správy a samosprávy,
- přizpůsobení současným trendům a vývoji ICT v oblasti e-governmentu,
- závislost na informačních systémech (IS), jejich kvalitě, funkčnosti, kompatibilitě, dostupnosti,
- požadavek důvěryhodnosti provozovaného IS,
- povinnost zajišťovat ochranu a bezpečnost informací ICT, IS, data a informace v souladu s platnou legislativou, standardy či normami,

Komplexní a systematické řešení informační bezpečnosti nepředstavuje pouze implementaci HW-, SW- a ICT-opatření, ale zahrnuje i další, často podceňované aspekty. Souhrnně lze definovat v podstatě čtyři základní navzájem propojené oblasti ovlivňující informační bezpečnost, kterou je nutno řešit jako celek:

organizační (a administrativní) bezpečnost,

- tj. např. struktura řízení, odpovědnosti, povinnosti, interní předpisy atd.;

personální bezpečnost,

- tj. např. zásady bezpečnosti při zahájení/ukončení pracovního poměru, prověřování klíčových uživatelů, školení a vzdělávání, hlášení incidentů apod.;

fyzická (objektová) bezpečnost,

- tj. např. fyzická ochrana přístupu ke kritickým komponentám sítě i jednotlivým PC, opatření proti ztrátě, poškození či zničení;

počítačová a komunikační bezpečnost,

- tj. ochrana logického přístupu k IS - uživatelské účty, přístupová práva, ochrana před škodlivým SW, šifrování, bezpečná skartace dat, zálohování, atd.

Pojem informační bezpečnost představuje komplex technických, technologických, fyzických, personálních a organizačních opatření pro ochranu informací a bezpečné používání informačních a komunikačních technologií (ICT). Organizace by se měly při budování informační bezpečnosti řídit jednak vlastními požadavky a předpisy, jednak mezinárodně uznávanými normami a doporučeními v této oblasti, a dále musí respektovat legislativní nařízení, jež se na ně v této oblasti vztahují.

19.2 Řešení bezpečnosti

Doporučujeme využít ke komplexnímu řešení bezpečnosti obecně doporučovaný a osvědčený procesní přístup k systému řízení bezpečnosti informací, tzv. ISMS (Information Security Management System, viz obrázek).

Systém řízení bezpečnosti informací je založen na mezinárodně uznávaných ISO normách, konkrétně ČSN ISO/IEC 27001 (požadavky) a ČSN ISO/IEC 27002 (cíle a opatření). Pojem bezpečnost informací je v těchto normách definován jako zachování důvěrnosti, integrity a dostupnosti informací, a dalších vlastností jako např. autentičnost, odpovědnost, nepopiratelnost a spolehlivost.

Zavedení modelu PDCA známého jako „Plánuj-Dělej-Kontroluj-Jednej“ (Plan-Do-Check-Act) může být aplikováno na všechny procesy ISMS, které budou v souladu s uvedenými normami zavedeny.

Tento postup je možné použít pro budování ochrany dat a bezpečnosti ICT bez ohledu na potenciální zájem získat certifikát dle normy 27001.

Eliminace rizik a bezpečnostních incidentů způsobovaných nejrůznějšími činiteli (např. počítačovými viry, vnějšími či vnitřními útočníky, výpadky energie, poruchami HW, haváriemi, ale i lidským faktorem, nevědomostí, neznalostí, chybějícími pravidly, nedostatečnou kázní, podceňováním nebezpečí atd.) přináší nejen významné finanční úspory vzhledem k efektivnímu vynakládání prostředků na ochranu (ani málo, ani příliš), ale také tolik potřebnou spolehlivost a důvěryhodnost

V rámci zajištění systematicky budované bezpečnosti IS v souladu s mezinárodně uznávanými normami a standardy (ISO/IEC řady 2700x) nabízíme mj. analytické a konzultační služby, realizaci analýzy rizik, auditu, bezpečnostní dokumentace a implementaci bezpečnostních kontrol a opatření. Řešení pak může být variabilní, prezentované buď jako výběr jednoho či několika jednotlivých a samostatných projektů, nebo může být zpracováno v rámci rozsáhlého komplexního projektu s

několika etapami. To je vždy závislé na potřebách organizace, jejích kapacitních, časových a finančních možnostech, na rozsahu provozovaného IS atd.

19.3 Bezpečnostní architektura

Bezpečnostní architektura je z hlediska požadavku na koordinaci bezpečnosti napříč organizací řešena na společném a jednotném základě spojujícím technickou a procesní oblast. Jedná se o komplex vzájemně provázaných aktivit, které vyžadují pokrytí identifikovaných rizik na všech úrovních, ať už se jedná o celý bezpečnostní projekt, nebo o jednotlivé dílčí části.

Navrhujeme řešení architektury bezpečnosti jako samostatnou kapitolu - bezpečnostní projekt. Výhodou tohoto přístupu je především celistvost a účinnost realizace činností, jako je analýza rizik, příprava projektové a provozní bezpečnostní dokumentace, zavádění procesů informační bezpečnosti, penetrační testování či havarijní plánování. Současně s tím bude zajištěna celková integrita vytvářené bezpečnostní dokumentace prostřednictvím supervize jejího zpracování.

Cíle vybudování jednotné bezpečnostní architektury byly stanoveny na základě potřeby:

- zajištění a prosazení bezpečnosti ve všech fázích životního cyklu informačních a komunikačních technologií;
- vybudování jednotného systému řízení bezpečnosti napříč všemi oblastmi ochrany informací;
- stanovení globální bezpečnostní politiky a uplatňování stejné metodiky a pravidel pro hodnocení bezpečnosti;
- zajištění efektivního způsobu dohledu na řešení bezpečnosti ve všech částech projektu;

Primárním požadavkem je koordinace procesů řešení bezpečnosti prostřednictvím společné bezpečnostní základny. Ta zahrnuje globální část a jednotlivé části týkajících se konkrétních oblastí z hlediska naplňování bezpečnostních požadavků.

Řešení bezpečnosti je založeno na definici bezpečnostních cílů a z nich vyplývajících bezpečnostních požadavků a mechanismů. Jejich úkolem je postihnout globální i specifické aspekty bezpečnosti nejen v případě analýzy rizik a v bezpečnostní dokumentaci, ale dále v rámci zavedení do praxe v běžném provozu, a následně v rámci bezpečnostního auditu, testování a vyhodnocování účinnosti celého systému.

Koordinace bezpečnosti se vztahuje jak k přípravě (návrhu), tak k vlastní realizaci. Aby byla zajištěna v celém životním cyklu, měla by probíhat v následujících krocích:

- návrh bezpečnostního projektu zahrnujícího analýzu požadavků a bezpečnostních aspektů,
- stanovení bezpečnostních cílů,
- realizace analýzy rizik,
- návrh efektivních bezpečnostních opatření ve formě plánu bezpečnosti,
- návrh provozní bezpečnostní dokumentace pro všechny oblasti,
- závěrečný audit systému řízení bezpečnosti informací.

19.4 Zákon o kybernetické bezpečnosti

S platností od 1.1.2015 vstoupil v platnost zákon o kybernetické bezpečnosti.

Tento zákon upravuje práva a povinnosti osob a působnost a pravomoci orgánů veřejné moci v oblasti kybernetické bezpečnosti. Zákon o kybernetické bezpečnosti se nevztahuje na informační nebo komunikační systémy, které nakládají s utajovanými informacemi.

Orgány a osobami, kterým se ukládají povinnosti v oblasti kybernetické bezpečnosti, jsou:

a) poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací1), pokud není orgánem nebo osobou podle písmene b)
b) orgán nebo osoba zajišťující významnou síť, pokud nejsou správcem komunikačního systému podle písmene d),
c) správce informačního systému kritické informační infrastruktury,
d) správce komunikačního systému kritické informační infrastruktury a
e) správce významného informačního systému

V tomto zákoně se rozumí:

a) kybernetickým prostorem digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy, a službami a sítěmi elektronických komunikací),
b) kritickou informační infrastrukturou prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy) v oblasti kybernetické bezpečnosti,
c) bezpečností informací zajištění důvěrnosti, integrity a dostupnosti informací,
d) významným informačním systémem informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci,
e) správcem informačního systému orgán nebo osoba, které určují účel zpracování informací a podmínky provozování informačního systému,
f) správcem komunikačního systému orgán nebo osoba, které určují účel komunikačního systému a podmínky jeho provozování a
g) významnou sítí síť elektronických komunikací1) zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé připojení ke kritické informační infrastruktuře.

V kybernetickém zákoně jsou mj. podle aktuálního stavu definovány povinnosti:

Subjekty spravující/zajišťující: Povinnosti:	elektronické komunikace[2]		významné sítě[3]		informační systémy KII[4]		Komunikační systémy KII[5]		Významné IS[6]	
hlásit kontaktní údaje	✔	✖	✔	✖	✔	✖	✔	✖	✔	✖
detekovat kybernetické bezpečnostní události			✔	✖	✔	✖	✔	✖	✔	✖
hlásit kybernetické bezpečnostní incidenty			✔	✖	✔	✖	✔	✖	✔	✖
zpracovávat bezpečnostní dokumentaci a zavádět bezpečnostní opatření					✔	✖	✔	✖	✔	✖
provádět opatření vydaná NBÚ		✖		✖	✔	✖	✔	✖	✔	✖

✔ standardní stav ✖ stav kybernetického nebezpečí

1 OVM = orgány veřejné moci, 2 OVM = Poskytovatelé služeb elektronických komunikací a subjekty zajišťující sítě elektronických komunikací, 3 OVM = Subjekty zajišťující významné sítě, 4 Správci informačních systémů zařazených do kritické informační infrastruktury, 5 Správci komunikačních systémů zařazených do kritické informační infrastruktury, 6 Správci významných IS

Plné znění zákona o kybernetické bezpečnosti lze nalézt na webu:

http://www.nbu.cz/cs/pravni-predpisy/zakon-o-kyberneticke-bezpecnosti-a-o-zmene-souvisejicich-zakonu-zakon-o-kyberneticke-bezpecnosti/

V současné době dle veřejně dostupných informací se kybernetický zákon nevztahuje na sítě krajů či měst, stejně jako na jejich informační systémy. V případě změny lze k plnění podmínek a požadavků tohoto zákona využít níže popsané činnosti a postupy (body 19.5 až 19.13), jelikož jsou v souladu s kybernetickým zákonem (vycházení z platných norem ISO a platných zákonů).

19.5 Standardy v oblasti bezpečnosti

Při auditní a analytické činnosti je nutné se řídit platnými zákony a vyhláškami v aktuálním znění, národními i mezinárodními normami či standardy, doporučovanými pro danou oblast a také etickými zásadami. Související legislativa, normy a standardy:

Zákon č. 101/2000 Sb., O ochraně osobních údajů;

Zákon č. 111/2009 Sb., O základních registrech;

Zákon č. 227/2000 Sb., O elektronickém podpisu;

Zákon č. 300/2008 Sb., O elektronických úkonech a autorizované konverzi dokumentů;

Zákon č. 365/2000 Sb., O informačních systémech veřejné správy v aktuálním znění;

Vyhláška č. 529/2006 Sb., O dlouhodobém řízení ISVS;

Zákon č. 106/1999 Sb., O svobodném přístupu k informacím;

Zákon č. 412/2005 Sb., O ochraně utajovaných informací a o bezpečnostní způsobilosti;

Zákon č. 499/2004 Sb., O archivnictví a spisové službě;

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti);

ČSN ISO/IEC 27001 – Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – Požadavky;

pův. ČSN ISO/IEC 17799 – Informační technologie – Soubor postupů pro řízení informační bezpečnosti,

a ČSN BS 7799-2 – Systém managementu bezpečnosti informací – Specifikace s návodem pro použití;

ČSN ISO/IEC TR 13335 – Informační technologie – Směrnice pro řízení bezpečnosti IT;

ISO/IEC 27004 – Information Security Management Measurements;

ISO/IEC 27005 – Information Security Risk Management;

BS 25999-1:2006 – Business Continuity Management – Část 1: Code of practice for business continuity management (ČSN BS 25999);

BS 25999-2 – Business Continuity Management – Část 2: Specification;

BS 25777:2008 – Information and communications technology continuity management. Code of practice (původně PAS 77:2006, nově ISO/IEC 27031);

NIST Special Publication 800-34 – Contingency Planning Guide for Federal Information Systems.

19.6 Bezpečnostní projekt

Komplexní „Bezpečnostní projekt“, který pokrývá veškeré potřeby organizace pro systém řízení informační bezpečnosti (dále jen ISMS) zahrnuje následující etapy:

Č.:	Etapa realizace:	Popis:	Požadavek (zákon, norma):
1.	**Informační strategie**	zpracování strategického dokumentu ICT s výhledem cca na 4 roky, příp. se zaměřením na bezpečnost, jako podkladu pro tvorbu rozpočtu	-
2.	**Analýza rizik IS**	identifikace aktiv, katalog hrozeb, identifikace a ohodnocení rizik, akceptace zbytkového rizika,	V rámci SMS (norma ISO 27001, ISO 27005)
3.	**Penetrační testy**	realizace penetračních testů (externí - zvenčí, interních),	Norma ISO 27001
4.	**Plán bezpečnosti**	zpracování plánu bezpečnosti (tj. harmonogramu realizace přijatých bezpečnostních opatření - implementace bezpečnosti do praxe);	V rámci ISMS
5.	**Informační koncepce**	zpracování dokumentace k ISVS a příprava na atestaci:	Zákon č. 365/2000 Sb., o ISVS
		o Informační koncepce je povinná v rámci systému dlouhodobého řízení ISVS do 1. 1. 2009 (definující mj. kvalitativní a bezpečnostní cíle a požadavky na ISVS)	Vyhláška č. 529/2006 Sb. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů
		o atestace povinná do 1. 1. 2010	
6.	**Bezpečnostní dokumentace**	v rozsahu potřebném jak pro ISVS, tak pro ISMS:	V rámci ISMS
		o bezpečnostní směrnice pro bezpečnostního manažera	Zákon č. 365/2000 Sb., o ISVS
		o bezpečnostní směrnice pro správce systému	

		o směrnice pro uživatele o uživatelské příručky a manuály o havarijní plán	Vyhláška č. 529/2006 Sb. Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů
7.	**Příprava na ISMS**	včetně zpracování potřebné dokumentace: o prohlášení o aplikovatelnosti o bezpečnostní politika ISMS (revize, příp. aktualizace stávajícího dokumentu) o plány přezkoumání shody o šablony záznamů o přezkoumání (vč. zprávy z analýzy rizik, penetračních testů atd.)	Norma ISO 27001 Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů
8.	**Bezpečnostní školení**	zajištění bezpečnostního školení a vzdělávání	Norma ISO 27001

Z nabízených služeb podrobněji vybíráme následující:

Analýza rizik IS obnáší - zjištění aktuálního stavu ochrany a návrh potřebných opatření k jejich eliminaci. Detailní kroky analýzy obsahují zpravidla:

- identifikaci aktiv, tj. zjištění hmotných a nehmotných hodnot, jakými jsou např. HW-aktiva, SW-aktiva, data případně služby, budovy, ostatní zařízení a vybavení;
- definici hrozeb, tj. stavů a situací ohrožujících IS, jako jsou např. živelní katastrofy, havárie, technické poruchy, závady, úmyslné a neúmyslné působení lidského faktoru apod.;
- identifikaci zranitelných míst, tzn. zjištění slabin a bezpečnostních děr posuzovaného systému;
- identifikaci rizik, tj. zjištění reálných ohrožení IS potenciálně uskutečnitelných využitím existujících a neošetřených zranitelných míst systému;
- zjištění dopadů, neboli posouzení míry konkrétního rizika, že se uskuteční určitá hrozba, jež využije daného zranitelného místa;
- identifikaci bezpečnostních kontrol (opatření) ve všech oblastech informační bezpečnosti;
- srovnání dostatečnosti bezpečnostních opatření s obvyklými, doporučovanými zásadami a normami, případně s dalšími požadavky (legislativní předpisy apod.);
- návrh opatření a kontrol včetně priorit k eliminaci zjištěných rizik.

Bezpečnostní audit znamená kontrolu a ověření shody, přičemž může být dle požadavků či zjištění analýzy rizik IS zaměřen např. na audit počítačové sítě, serverů, posouzení aktuálnosti, správnosti a úplnosti bezpečnostní dokumentace, kontrolu dodržování definovaných bezpečnostních pravidel v praxi, prověření adekvátní ochrany osobních údajů v souladu se zákonem atd.

Penetrační testy představují zkoušku, která má za účel prověřit odolnost systému vůči průniku potenciálního útočníka, případně jeho možnost získat neoprávněný přístup k systému či datům. Toto testování slouží jako objektivní posouzení úrovně zabezpečení počítačové sítě, neboť útočníkem může být:

- vnější **nepřítel**, který může pro tuto činnost používat hackerské nástroje případně metody sociálního inženýrství a využívat jak známých slabin, tak dosud neodhalených bezpečnostních děr daného systému,
- vnitřní **útočník**, který se rekrutuje např. z řad nespokojených zaměstnanců, nebo jen náhodně objevil skrytou slabinu, kterou využije, případně jde o osobu, která již do podniku vstoupila s úmyslem získat neoprávněný přístup, poškodit data či zneužít informace, nebo jinak způsobit podniku škodu.

Bezpečnostní dokumentace - služby v této oblasti mají za cíl audit, tvorbu, dopracování nebo aktualizaci potřebných interních předpisů pro řízení bezpečnosti obsahujících jednoznačná pravidla, povinnosti a zodpovědnosti pro všechny skupiny uživatelů. K takovým dokumentům patří zejména:

- bezpečnostní politika ICT (celková, popisující zásady informační bezpečnosti v organizaci),
- bezpečnostní politika IS (provozovaného informačního systému) zaměřená na specifikaci opatření pro každou z výše uvedených oblastí bezpečnosti daného IS,
- bezpečnostní směrnice, pokyny a postupy, tj. konkrétní instrukce a návody specifické pro různé skupiny uživatel (samostatně pro uživatele, pro správce systému apod.) popisující detailní procesy - např. postup pro zálohování, postup pro změnu hesla, postup pro antivirovou ochranu, postup pro šifrování, bezpečné používání elektronické pošty atd.,
- havarijní plán IS obsahující postupy pro řešení havárií, plány zajištění kontinuity činnosti a plány obnovy dle priorit kritických procesů a požadavků na zachování provozu.

Plán bezpečnosti - návrh konkrétních řešení bezpečnosti rozpracovaný do harmonogramu pro implementaci jednotlivých bezpečnostních opatření formou samostatných projektů, které obsahují mj. nároky na kapacity, čas, personál a zdroje, finanční náklady a priority. Tato činnost následuje zpravidla po analýze rizik IS, návrhu ochranných opatření, zpracování bezpečnostní politiky a uvedení související bezpečnostní dokumentace do aktuálního stavu.

Konzultace, vzdělávání a školení v oblasti informační bezpečnosti by mělo probíhat opakovaně s ohledem na neustálý vývoj ICT a vznik nových hrozeb pro informační systémy. Školení může být rozděleno na několik samostatných částí, specifických svým obsahem a také určením pro jednotlivé cílové skupiny. Jedná se o jednorázové i pravidelné:

- konzultace na určené téma pro jednotlivce i skupinu osob (pro management bezpečnosti, správu systému, vedoucí zaměstnance);
- prezentace v rámci porad, seminářů, interních školení a jiných akcí;
- opakované vzdělávání v informační bezpečnosti (individuální, skupinové, zaměřené uživatelsky či pro management).

19.7 Analýza rizik

Cílem této etapy je identifikovat a analyzovat rizika týkající se informační bezpečnosti pro každou z oblastí, a dále navrhnout opatření k odstranění či eliminaci zjištěných rizik. Pod pojmem efektivní opatření rozumíme taková opatření, která zohledňují hodnotu daného aktiva, pravděpodobnost realizace hrozby, dopad uskutečnění hrozby na kontinuitu činnosti organizace a hodnotu (cenu) realizovaných protiopatření. To umožní přistupovat k řešení bezpečnosti diferencovaně podle důležitosti a požadavků na zabezpečení a dostupnost dat, a tak zabránit neefektivní paušální aplikaci relativně nákladných nebo naopak nedostatečně účinných bezpečnostních technologií na celý systém.

Analýzu rizik chápeme jako zahájení komplexního procesu, jehož výsledkem bude trvalé zajištění požadované úrovně bezpečnosti aktiv organizace, která jsou uložena a spravována pomocí informačních systémů a technologií. Analýza rizik představuje dále podklad pro vytvoření, případně revizi plánu zvládání rizik (tzv. Plánu bezpečnosti), z jehož změn je následně možné odvozovat i nutné změny metrik bezpečnosti.

Rozsah analýzy musí pokrývat všechny definované oblasti:

- bezpečnost informačních a komunikačních technologií (dále jen ICT),
- fyzická (objektová) bezpečnost,
- personální bezpečnost,
- administrativně-organizační bezpečnost.

19.7.1 Metodika

Analýza rizik musí být realizována na základě doporučení mezinárodních norem řady ISO 2700x, konkrétně ČSN ISO/IEC 27005:2009.

Realizace analýzy rizik musí probíhat v souladu s přijatou a zadavatelem schválenou metodikou, v jejímž rámci bude stanoven:

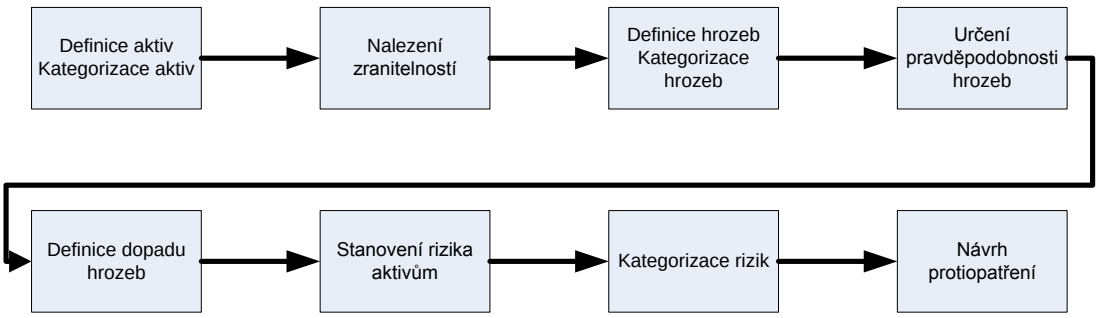
- způsob hodnocení aktiv, pravděpodobností, zranitelností a dopadů uskutečnění hrozeb,
- způsob stanovení míry a akceptovatelnosti rizik,
- způsob měření účinnosti implementovaných opatření,
- způsob určování priorit pro navrhovaná opatření.

Metoda provedení analýzy rizik je zřejmá z jejího cíle – nejprve jsou definována aktiva organizace, následně jsou určeny veškeré hrozby těmto aktivům a ty jsou analyzovány z hlediska zranitelnosti. Z výsledné zprávy (analýzy) vyplývají navrhovaná bezpečnostní opatření.

Pod pojmem analýza je možné si představit posouzení pravděpodobnosti realizace jednotlivých hrozeb vůči jednotlivým aktivům či skupinám aktiv z hlediska jejich hodnoty a dopadu případného uskutečnění jednotlivých hrozeb na jednotlivá aktiva.

Pokud jsou definována aktiva i hrozby, je možné začít posuzovat pravděpodobnost jejich realizace. Z pravděpodobnosti realizace hrozby s definovaným dopadem je potom možné stanovit míru rizika. Jednotlivá rizika jsou následně kategorizována a na základě stanovených kategorií je navrženo protiopatření.

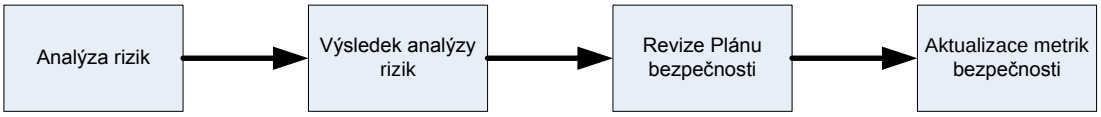
Průběh analýzy rizik je možné schematicky zobrazit takto:



Samotná analýza je ještě rozdělena do organizačních celků souvisejících s jejím vlastním průběhem – přípravné práce (návštěva specialisty nebo specialistů, kteří pomocí interview nebo dotazníkovou metodou získají informace nezbytné pro definici aktiv organizace, definici hrozeb, pravděpodobnost jejich realizace a jejich dopad na funkčnost IS, posouzení organizačních opatření ochrany aktiv a v neposlední řadě informace potřebné pro posouzení technické části opatření), a následná samotná analytická část zpracování informací a výsledků, jejímž výstupem je zpráva o bezpečnosti a navrhovaná bezpečnostní opatření.

Aby bylo možné posuzovat dosažení jednotlivých cílů v oblasti informační bezpečnosti, jsou stanoveny jejich metriky. Metrika je konkrétně definované kritérium, které slouží k měření a hodnocení dosažené úrovně stavu zabezpečení ICT.

Postup lze schematicky zachytit takto:



V okamžiku, kdy jsou známa rizika a tato jsou kategorizována, a je známo i jakým způsobem jim lze čelit, je možné vytvořit nebo provést revizi stávajícího plánu zvládání rizik (dále také Plánu bezpečnosti). Plán bezpečnosti definuje postup realizace jednotlivých bezpečnostních projektů, a je tedy zřejmé, že případná změna rizik nutně vyvolává potřebu revize Plánu bezpečnosti.

19.7.2 Postup realizace

Jak je uvedeno v předchozí obecné části, základním úkolem je definování aktiv organizace, tj. té části, na kterou je třeba se při analýze zaměřit, dále jejich ohodnocení, následně určení jejich zranitelností a jim odpovídajících hrozeb, a poté z nich vyplývající ohodnocení pravděpodobnosti a dopadů hrozeb. V daném okamžiku je také potřeba seznámit se s bezpečnostní dokumentací, systémem řízení bezpečnosti a procesy řízení bezpečnosti, jsou-li nastaveny a dokumentovány.

Pro zpracování analýzy rizik bezpečnosti informací bude použita jednotná metodika, vycházející z normy ČSN ISO/IEC TR 13335 v oblasti přístupu k analýze rizik, a dále z normy ISO 27005 v oblasti realizace a managementu rizik, související s požadavky systému řízení bezpečnosti informací (dále jen ISMS) dle normy ISO 27001.

Analýzu rizik lze realizovat výběrem vhodného přístupu, tj. od základního přes neformální až k detailnímu přístupu, nebo využít kombinovaného způsobu, při kterém lze uplatnit výhody jednotlivých přístupů pro konkrétní potřeby. Nejčastěji se v praxi používá jako nejvhodnější kombinovaný přístup umožňující po zjištění základních informací a požadavků definovat klíčové rizikové oblasti a poté přistoupit k jejich detailní analýze. Analýza rizik pak posuzuje aktiva zejména s přihlédnutím k důsledkům hrozeb.

Navrhovaný kombinovaný přístup k analýze rizik zahrnuje následující:

- zjištění (analýzu) požadavků na bezpečnost (organizačních, legislativních, technologických, personálních);
- vlastní analýzu rizik (v závislosti na aktivech, hrozbách, zranitelnosti, pravděpodobnosti a dopadech) obsahující:
    - identifikaci aktiv, tj. zjištění hmotných a nehmotných hodnot, jakými jsou např. HW-aktiva, SW-aktiva, informační aktiva, tj. data, případně služby, fyzické prostředí, tj. budovy, ostatní zařízení a vybavení;
    - definici hrozeb, tj. stavů a situací s negativním dopadem na činnost zákazníka, jakými jsou např. úmyslné a neúmyslné působení lidského faktoru, živelní katastrofy, havárie, technické poruchy, závady apod.;
    - identifikaci zranitelných míst, tzn. zjištění slabin a bezpečnostních děr posuzovaného systému;
    - identifikaci pravděpodobnosti uskutečnění hrozby a dopadů, neboli kvalitativní posouzení míry konkrétního rizika, že se uskuteční určitá hrozba, jež využije daného

zranitelného místa, ohodnocení bezpečnostních rizik a postup jejich zvládání, stanovení kritérií pro akceptaci rizik a určení odpovědností. Míra rizika je definována v několika úrovních, které mj. dovolují stanovit hranici pro akceptovatelná rizika;
- identifikaci stávajících bezpečnostních opatření v závislosti na procesech;
- srovnání a zhodnocení dostatečnosti a účinnosti stávajících bezpečnostních opatření s definovanými cíli, požadavky a identifikovanými riziky a posouzení reálné pravděpodobnosti selhání přijatých opatření;
- návrh a specifikaci vhodných opatření a kontrol na eliminaci rizik a implementace vhodných prostředků a technologií k zajištění navrhovaných opatření, včetně stanovení priorit k řešení zjištěných neshod;
- ohodnocení důležitosti jednotlivých opatření a přínosů.

V základním zjednodušeném členění pro lepší přehlednost a porozumění posuzujeme rizika v následujících oblastech:

- organizační (a administrativní) bezpečnost tj. např. struktura a hierarchie řízení, odpovědností, pravomocí, kompetencí, povinností, interní předpisy atd.;
- personální bezpečnost tj. nábor/ukončení pracovního poměru uživatelů, školení, bezpečnostní vzdělávání, vymahatelnost odpovědnosti, prověřování, povinnosti týkající se důvěrnosti/mlčenlivosti, dodržování předpisů, řešení incidentů, autorských práv, legálnosti SW apod.;
- fyzická (objektová) bezpečnost tj. ochrana objektu/lokality, bezpečnostní perimetry, zajištění infrastruktury (zdroj energie, telekomunikační služby, klimatizace/vytápění), fyzický přístup ke klíčovým komponentám prostředí zákazníka, opatření proti ztrátě, poškození či zničení fyzických aktiv;
- počítačová a komunikační bezpečnost tj. ochrana logického přístupu do prostředí zákazníka – zabezpečení komunikace, access/identity management (uživatelské účty, přístupová práva), ochrana před škodlivým SW, šifrování, bezpečná skartace dat, zálohování, atd.

19.7.3 Výstupy z analýzy rizik

Výstup z analýzy rizik mj. obsahuje:

- identifikaci a ohodnocení aktiv,
- identifikaci a určení pravděpodobnosti výskytu a dopadů hrozeb,
- identifikaci a ohodnocení zranitelností aktiv,
- určení míry rizik,
- interpretaci výsledků analýzy rizik,
- návrh rozhodnutí o řízení rizik a stanovení postupů pro pokrytí rizik.

Součást výsledné zprávy tvoří podle potřeby a účelnosti samostatně zpracované přílohy např. z technické/technologické části analýzy, přehledové tabulky, případně další specifické výstupy z detailní analýzy rizik.

Detailní popis analýzy rizik podává dokument bezpečnostní dokumentace, kapitola 5.7 a 6.

19.8 Penetrační testy

Penetrační testování bezpečnosti IS je jednou z částí komplexního procesu řízení informační bezpečnosti, který má podobu Demingova procesního cyklu PDCA (kontinuální vylepšování). Penetrační testování tedy primárně zkoumá stávající stav zabezpečení informačního systému a jeho výstupy jsou zpravidla podkladem pro opakovanou analýzu rizik.

Jedním ze základních přínosů této služby je zjištění, jakou míru proniknutelnosti mají aktuálně přijatá opatření ochraňující klíčová aktiva společnosti. Penetrační testy následně umožní:

- správně a účinně investovat do opatření,
- neplýtvat prostředky, ochránit bezpečnostní investice,
- cíleně plánovat zvýšení úrovně zabezpečení,
- implementovat technologie, které poskytnou požadovanou ochranu.

Běžný postup při penetračních testech:

- seznámení s prostředím,
- plánování útoku,
- útok a jeho vyhodnocení,
- dokumentace a interpretace výsledků.

19.8.1 Vyslovení souhlasu s testováním

V současné době nám není znám normativ, který výslovně upravuje aktivity penetračního testování. Nicméně při používání testů může dojít k situacím, u kterých je sporné, zda nedochází k omezování vlastnických práv osob, případně se nejedná o zlý úmysl. Z těchto důvodů je nutné vyslovení souhlasu s testováním – testovací mandát. Tento souhlas opravňuje testovací tým k vykonávání jednotlivých testů.

19.8.2 Mapování

Tato kapitola zahrne ve zvolené tvrdosti, viditelnosti, čase, rozsahu a znalosti prostředí aktivity, které útočníka informačně obohatí. Mapování slouží k simulaci toho, jaké informace je schopen potenciální útočník získat o prostředí zadavatele. Za informační zdroje pro tento krok budou použity veřejné i neveřejné zdroje, invazivní i neinvazivní techniky. Zjištěné informace budou následně využity pro stanovení ideálního postupu útoku. Mezi tyto informace patří např. adresní prostory, otevřené porty, identifikace operačního systému, jmenné konvence apod.

19.8.3 Stanovení postupu

Stanovení postupu bude probíhat na základě zjištění získaných v předchozím bodě, bude vytvořen plán, podle kterého se bude realizovat vlastní útok/y, zejména ve vztahu k parametru času. Zajistí/připraví se např. vhodné body sloužící pro útok(y), stanoví se priority a provázanost jednotlivých kroků, připraví se nezbytné technické vybavení.

19.8.4 Hledání slabin a zranitelností

Tato činnost bude realizována automatizovaně i ručně, zejména ve vztahu k parametru času. Automatická kontrola slouží k objevení chyb, které jsou většinou jednoduše zneužitelné, a jejichž potenciál je již dokumentován. Manuální testy kladou maximální důraz na kreativitu a kombinatoriku simulovaného útočníka a zpravidla odhalují chyby, které nejsou jednoduše zneužitelné, ale mohou být velmi nebezpečné. Ručně budou prověřeny především chyby a komentáře v případně nalezeném kódu www stránek a aplikační logika, vstupy ve formulářích, Session Management, Cookie Management, Directory Traversal, Hidden Directory, Track a případně jiné chyby, které vyplynou z předchozích kroků.

19.8.5 Pokus o průnik

V této fázi je realizován pokus o průnik s využitím zjištěných slabin a zranitelností, zejména ve vztahu k parametru času. Konkrétní způsob útoku bude stanoven v předchozím bodě, předpokládáme i kombinaci různých technik. Cílem útoku je prokázat nebo vyvrátit existenci slabin nalezených v předchozím kroku, které lze potenciálním útočníkem zneužít a uskutečnit tak průnik do interní sítě zadavatele. Jde například o hádání hesel, DoS, SQL Injection, Content Injection, Cross Site Scripting, Web Cache Poinsoning, Buffer Overflow.

19.8.6 Korekce

Korekce v průběhu útoku slouží pro vyhodnocení zjištěných faktů ke zmírnění či rozšíření daného útoku, případně k rozvinutí nového typu útoku. Tento bod se v průběhu testu opakovaně aplikuje na základě výsledků jiných útoků nebo zjištění.

V tomto kroku dojde k vyhodnocení získaných informací a identifikaci rizikových oblastí. Výstupem z celého procesu je popisný dokument zjištěných faktů a jednotlivých pokusů o průnik, včetně doporučení jak řešit problematická místa.

Na základě výše popsaných parametrů je pro související vrstvy použito technik a nástrojů z následujícího výčtu:

- pro fyzické prostředí – místní obhlídka, prostupy do areálů, budov, kanceláří, překonání bariér této vrstvy ať již silou nebo logickými manipulacemi.
- pro boxy, hardware a fyzická propojení – testy manipulace, znefunkčnění propojení, manipulace s boxy, kabely, zásuvkami.
- pro aktivní propojení, připojení – testy manipulace a zmatení a znefunkčnění komponent účastnících se na aktivním propojení systémů, ARP, IP Spoofing, Squatting…
- pro aplikace a data – testy publikovaných zranitelností, například Remote Executing, Script a Code Injection, Cross Site Scripting, Parameter Manipulation.
- pro procesy osoby a role – možnosti průzkumu, manipulace, matení, cyklení, smyčkování.

Volba rozsahu není pro případ nabízeného typu testu stanovena pevně předem a dle zjištěných okolností bude přizpůsobena tak, aby byl maximalizován užitečný výstup.

Výstupem je vždy zpráva – forma sdělení, která je maximálně srozumitelná, odpovídá potřebám zákazníka a zahrnuje:

- Podrobný report, tj. zdokumentování použitých technik a jejich výstupů;

- Manažerské shrnutí, tj. zkrácená forma zaměřená na klíčové nálezy a jejich interpretaci;

Prezentace výsledků – osobní interaktivní konzultace nad výsledky.

19.9 Plán bezpečnosti

Zpracování plánu bezpečnosti chápeme jako vytvoření návrhu harmonogramu realizace přijatých bezpečnostních opatření vyplývajících z předchozí realizace analýzy rizik. Návrh opatření bude konfrontován s hrozícími riziky identifikovanými v etapě Analýza rizik. U každého navrhovaného opatření bude v závislosti na stanovené míře takto eliminovaného rizika možno určit, do jaké míry bude toto riziko zmírněno nebo odstraněno. Tímto způsobem bude možné genericky analyzovat rizika, sledovat účinnost navrhovaných opatření a zvyšovat úroveň zabezpečení.

Plán bezpečnosti bude obsahovat nároky a požadavky na implementaci navrhovaných opatření, tj. zejména:

- kapacity,
- čas,
- personál,
- zdroje,
- finanční náklady,
- požadované priority.

Tento dokument bude mít za cíl definovat veškeré koordinované akce, které mají být realizovány pro zajištění implementace navrhovaných a posléze schválených bezpečnostních opatření v krátkodobém, střednědobém a dlouhodobém horizontu.

V rámci této etapy bude realizováno zpracování Plánu bezpečnosti s ohledem na výsledky analýzy rizik, a to v rozsahu potřebném pro splnění požadavků normy ISO 27005. Plán bezpečnosti stanoví opatření a postupy na straně zadavatele, které povedou ke splnění požadavků platné legislativy, zejména zákona č. 111/2009 Sb., o základních registrech, v platném znění a ke splnění požadavků daných normou ISO 27002.

Na základě zpracované analýzy rizik je možné rozhodnout o dalším postupu, který povede k odstranění zjištěných nedostatků v organizační (procesní) oblasti. V daném okamžiku je i v tomto případě velmi předběžné předjímat výsledek a tudíž stanovovat i další opatření, ale mezi taková opatření zařazená do Plánu bezpečnosti může typicky patřit:

- zavedení bezpečnostní politiky organizace pro oblast řízení/organizace bezpečnosti (vedení, vyhodnocování, kompetence, odpovědnost),
- řízení aktiv,
- klasifikace dat,
- personální bezpečnost (řízení lidských zdrojů, požadavky na personál),
- fyzická (objektová bezpečnost),
- přidělování přístupů a přístupových oprávnění,
- audit a zajištění shody,
- řízení komunikací a provozu,
- akvizice, vývoj a údržba informačních systémů,
- vytvoření plánu zvládání rizik a metrik bezpečnosti,

- řešení bezpečnostních incidentů,
- vytvoření systému bezpečnostních směrnic a pracovních postupů,
- zpracování havarijních plánů, plánů obnovy a zajištění kontinuity a konkrétních postupů,
- testování bezpečnosti – vytvoření testovacího plánu (testování systémů zevnitř, zvenčí, vlastními prostředky a nezávislými externími testery atd.),

Na základě analýzy rizik je dále možné rozhodnout o dalším postupu, který povede k odstranění případně zjištěných nedostatků v technologické oblasti. Mezi technická opatření může patřit:

- návrh a implementace zabezpečení prostředí, tj. např. fyzického perimetru a opatření objektové/fyzické bezpečnosti,
- řešení v oblasti přístupu (fyzického i logického),
- řešení autentizace a autorizace,
- kontrola obsahu,
- IPS/IDS,
- antivirová ochrana vč. antispyware a antispamu,
- šifrování, integrita (PKI),
- systémy patch-managementu,
- systémy identity-managementu,
- řešení zálohování,
- systémy řízení bezpečnosti a incidentů,
- monitoring,
- sledování aktivit serverové a síťové infrastruktury,

Pro výběr opatření eliminujících zjištěná rizika v souladu s jejich kategorizací navrhujeme využít soubor postupů a doporučení z takových zdrojů, jako jsou např. TR 13335, potažmo ISO 27002 apod. Podrobný návrh opatření pro zajištění informační bezpečnosti, optimalizaci procesů a přiřazení bezpečnostních prvků, včetně podrobného harmonogramu implementace navržených opatření, postupů a nástrojů, bude obsahovat:

1. Technologická opatření, která jsou založena na použití konkrétních technik, technických prvků či zařízení, dostupných technologií, bezpečnostních komponent, funkcí a prvků, vč. specializovaného SW apod., a vztahují se na následující oblasti (dle ČSN ISO/IEC 27001):
    - řízení komunikací a provozu,
    - řízení přístupu,
    - akvizice, vývoj a údržba informačních systémů,
    - zvládání bezpečnostních incidentů.
2. Procesní opatření, jež jsou určena k zavedení, prosazování a kontrole dodržování potřebných bezpečnostních politik, procesů, metod, postupů, aktivit a chování zajišťujících bezpečnost prostředí zákazníka, potažmo dat v něm zpracovávaných jak zvenčí (vnějšími uživateli), tak zevnitř (provozovatelem a správcem systému v chráněném prostředí počítačové sítě), která se vztahují na následující oblasti (dle ČSN ISO/IEC 27001):
    - politika bezpečnosti,
    - organizace bezpečnosti informací,
    - řízení aktiv,
    - bezpečnost lidských zdrojů,
    - fyzická bezpečnost a bezpečnost prostředí,
    - řízení kontinuity činnosti,

- soulad s požadavky.

Výstupem z této etapy bude:

- podrobně zpracovaný implementační manuál popisující všechna doporučení a kroky k realizaci nápravných opatření vzešlých z analýzy rizik, dopadů a penetračních testů,
- rozpracování bezpečnostních cílů jednotlivých činností dle plánu zvládání rizik, harmonogramu a způsobů realizace.

19.10 Vytvoření interních předpisů

V rámci této etapy bude realizováno vytvoření, případně aktualizace bezpečnostní předpisové základny zadavatele, a to v rozsahu potřebném pro splnění požadavků systému řízení bezpečnosti informací (ISMS), při zohlednění stávající interní předpisové základny a související dokumentace s vazbou na systémy řízení kvality a procesů souvisejících s provozováním ICT a dlouhodobého řízení informačních systémů veřejné správy (normy ISO 9001, ISO 20000, ISO 27001 a zákon č. 365/2000 Sb., o ISVS).

Vytvoření potřebné dokumentace představuje stanovení a zpracování jednoznačných předpisů pro řízení informační bezpečnosti organizace obsahujících pravidla, povinnosti a zodpovědnosti pro každou definovanou skupinu uživatelů.

V rámci této etapy bude zpracována potřebná bezpečnostní projektová, řídicí a provozní dokumentace, vyhovující jak legislativním požadavkům, tak potřebám systému řízení bezpečnosti informací a interním potřebám organizace. Soulad interních předpisů informační bezpečnosti s legislativou chápeme jako shodu se zákonnými předpisy, které upravují řízení a vykonávání určitých procesů zákazníka pomocí, prostřednictvím nebo za podpory informačních a komunikačních technologií zpracovávajících data, na základě výsledků z analýzy rizik.

K zajištění požadovaného souladu zrealizujeme v prvním kroku analýzu veškerých platných právních předpisů (zákony, vyhlášky, nařízení a předpisy), norem a standardů (např. normy ČSN ISO/IEC, případně doporučení NIST, ISACA, ITIL apod.).

Úkolem druhého kroku bude revidovat stávající předpisovou základnu zákazníka (minimálně v rozsahu stávající bezpečnostní politiky a provozního řádu) ze dvou hledisek:

- prvním z nich je analyzovat její rozsah, určení, obsahovou náplň, citlivost, stanovení odpovědností, úroveň podrobností, správnost a přehlednost, včetně formálních náležitostí a aktuálnosti jednotlivých dokumentů,
- druhým hlediskem je procesní stránka životního cyklu dokumentace, tzn. tvorby, změn, aktualizací, ukládání, evidence, správy, zálohování, archivace a likvidace dokumentů.

V rámci tohoto kroku budou realizovány následující činnosti:

- identifikace dokumentace k informační bezpečnosti,
- analýza obsahu, aktuálnosti, dostatečnosti a správnosti dokumentace,
- analýza souladu dokumentace s legislativou, vnějšími a vnitřními požadavky,
- identifikace neshod,
- obecný návrh opatření a doporučení týkajících se aktualizace dokumentů, tvorby či dopracování specifických, příp. povinně předkládaných dokumentů např. v rámci atestací,

- konkrétní doporučení rozsahu a obsahu potřebné dokumentace, případně vzorových šablon dokumentů s vyžadovanými náležitostmi.

Audit dokumentace se bude týkat následujícího výčtu typických interních dokumentů, jakými mohou být např.:

- informační strategie,
- informační koncepce,
- bezpečnostní politika ICT/IS,
- bezpečnostní směrnice a příručky,
- metodické materiály a pokyny (metodika analýzy rizik, katalog hrozeb),
- bezpečnostní plán (seznam schválených/neschválených opatření, stav implementace, akceptace rizik),
- havarijní plány, plány kontinuity a obnovy,
- a další.

Zaměříme se mj. také na procesy související s posuzovanou dokumentací, které se týkají:

- tvorby,
- schvalování,
- změnového řízení a aktualizace,
- publikování a evidence,
- ověřování správnosti, dostatečnosti, srozumitelnosti a přehlednosti,
- vyhodnocování dodržování dokumentovaných předpisů, stanovených kompetencí a zodpovědností.

Rozsah a objem návrhu vytvoření či aktualizace stávající interní dokumentace bude záviset na aktuálním stavu dokumentace, který bude podroben revizi, jejíž výsledky doplní či upřesní celkový souhrn požadavků identifikovaných z analýzy rizik. Minimální rozsah dokumentace musí odpovídat všem těmto požadavkům a zároveň zaručovat dostatečnou míru přehlednosti a jednotnosti, s vyloučením duplicitní dokumentace a za dodržení diferencovaného přístupu k jednotlivým dokumentům dle oprávnění a citlivosti obsahu.

Z pohledu legislativního se jedná o soubor dokumentů týkajících se utajovaných informací, ochrany osobních údajů nebo ISVS, jako jsou např.:

- bezpečnostní politika, informační koncepce, příp. návrh (plán) bezpečnosti a testy bezpečnosti;
- provozní dokumentace typu bezpečnostní směrnice;
- příručky (pro uživatele a pro bezpečnostního správce).

Z pohledu bezpečnostního se jedná o dokumentaci doporučovanou v normě ČSN ISO/IEC TR 13335 n. ISO 27001, např.:

- strategie bezpečnosti resp. celková bezpečnostní politika ICT;
- politika bezpečnosti systému;
- plán zvládání rizik, n. plán bezpečnosti ICT.

Do provozní dokumentace dále budou spadat např. provozní řády organizace v oblasti ICT, plány pro případ havárií a mimořádných událostí, provozní deníky, evidence a přílohy k těmto řádům či směrnicím, a také veškeré záznamy dokládající výkon popsaných procesů a činností.

Z procesně orientovaných dokumentů jsou to např.:

- popisy bezpečnostních mechanizmů,
- popisy nastavení přístupových oprávnění,
- popisy nastavení technických a programových parametrů,
- způsoby nastavení komunikace jak uvnitř organizace, tak i mimo ni,
- způsob práce s mobilní výpočetní technikou a její připojování do počítačové sítě,
- apod.

Z věcně orientovaných dokumentů je to např.:

- dodatek pracovní smlouvy, ve kterém se zaměstnanci zavazují dodržovat zásady bezpečné práce s ICT a informacemi,
- postup a procedury auditu IS/ICT/ISMS,
- apod.

Z dokumentace orientované na role jsou to např.:

- příručky bezpečnostních manažerů a správců, správců aplikací,
- příručka správce systému,
- příručka pro práci uživatele IS/ICT v organizaci,
- apod.

Samostatnou provozní dokumentaci mohou vyžadovat i některé specifické systémy či aplikace, pokud bude její tvorba účelná a potřebná pro zajištění jejich bezpečného provozu.

V rámci tvorby bezpečnostní dokumentace bude dle potřeby realizována či revidována také stávající Informační koncepce, včetně aktualizace souvisejících dokumentů pro potřeby splnění požadavků zákona o ISVS a prováděcích právních předpisů k tomuto zákonu, v případech, kdy se bude jednat o dodávku nových ISVS.

Informační koncepce je dokument, který je nezbytné vytvořit, revidovat, případně aktualizovat s ohledem na vývoj v uplynulém období, a měnící se zákonné, interní a jiné požadavky tak, aby byly zohledněny veškeré stávající, aktuální i budoucí dlouhodobé kvalitativní a bezpečnostní cíle a požadavky.

Účelem zpracování či revize Informační koncepce ISVS organizace je identifikovat změny, posoudit aktuálnost, zhodnotit provádění činností dle této koncepce, ověřit stav realizace cílů a požadavků bezpečnosti a kvality, a vyhodnotit, do jaké míry je zajištěna shoda se stanovenými požadavky a povinnostmi, které z tohoto dokumentu vyplývají.

Námi navrhovaná revize Informační koncepce v požadovaném rozsahu bude zahrnovat následující činnosti:

- identifikaci změn ISVS od data poslední revize IK (n. jejího vytvoření),
- aktualizaci dokumentovaných ISVS, tj.:
    - přehledu ISVS,
    - popisu jednotlivých ISVS,
    - záměrů na pořízení nebo vytvoření ISVS,

- aktualizaci plánu řízení kvality ISVS,
- aktualizaci plánu řízení bezpečnosti ISVS,
- ověření dodržování pravidel pro správu všech ISVS, tj. pro:
    - pořizování a vytváření,
    - provozování a údržbu,
    - změnové řízení a ukončení činnosti,
    - ověření pravidel financování ISVS v souladu s obecnými předpisy, podmínkami zadávání veřejných zakázek a zakázek malého rozsahu, pro:
    - vytvoření či pořízení ISVS,
    - financování dlouhodobých cílů (realizace cílů a požadavků kvality a bezpečnosti),
    - financování správy (provozu a údržby).

Z dokumentů odpovídajících kategorii bezpečnostní dokumentace budou zpracovány (příp. aktualizovány) následující dokumenty:

Projektová bezpečnostní dokumentace

- Bezpečnostní politika zaměřená na specifická opatření pro všechny uvedené oblasti bezpečnosti;
- Informační koncepce.
- Provozní bezpečnostní dokumentace
- Bezpečnostní směrnice pro bezpečnostní správce;
- Bezpečnostní směrnice pro správce systémů;
- Bezpečnostní směrnice pro uživatele;
- Specifické bezpečnostní metodiky, manuály a příručky;
- Havarijní plány (řešení havárií, kontinuity a obnovy) obsahující:
    - definici kritických procesů,
    - identifikaci uvažovaných typů havárií,
    - definici postupu a koordinace činností při řešení havárie a obnově provozu,
    - definici testování postupů a plánů,
    - definici zodpovědností za jednotlivé činnosti.

19.11 Správa identit (IdM)

Identity Manager automatizuje interní prvky řízení, kterými jsou ovládána přístupová práva uživatelů.

Tento software pro správu identit je zabezpečené a automatizované řešení založené na zásadách, které je určeno pro správu uživatelských oprávnění používaných pro prostředky heterogenního informačního systému.

- Pomáhá posílit správu uživatelských přístupů o komplexní zajišťování založené na požadavcích. Je schopen zajišťovat požadavky a schvalování uživatelského přístupu k rolím, účtům či přesně stanoveným přístupovým právům.
- Disponuje optimalizovaným samoobslužným rozhraním pro uživatele, jehož vzhled a celkovou grafickou koncepci lze snadno přizpůsobit, optimalizovat je pro konkrétní typy uživatelů (auditoři, vedoucí, pracovníci podpory atd.) a integrovat s portály.
- Poskytuje zásady, které lze snadno konfigurovat pomocí průvodců a šablon.

Popis komponenty

- Správa identit pracovníků úřadu.
- Správa rolí a oprávnění.
- Synchronizace identit v informačních systémech

Předpoklady

V personálním informačním systému se nachází:

- Informace o zaměstnancích úřadu včetně jejich zařazení do organizační struktury.

V systému IDM se nachází:

- Uživatelské rozhraní pro manuální uživatelskou samosprávu pro editaci vybraných informací z uživatelského profilu
- Administrátorské rozhraní pro manuální správu systému CSI
- Informace o IS úřadu včetně rolí a oprávnění, které je možné v IS nastavit.
- Definice centrálních rolí daných zařazením pracovníka do organizační struktury, nebo pracovní skupiny a mapování těchto centrálních rolí na uživatelská oprávnění a role v jednotlivých IS.

Požadavky na řešení IDM

Požadované vlastnosti:

- IDM musí pracovat s minimálně 1000 identitami interních uživatelů
- IDM musí připojit libovolné množství spravovaných systémů
- IDM musí udržovat a spravovat kompletní životní cyklus identity uživatele
- IDM musí umožnit práci s více stromovými strukturami (např. interní, externí, příspěvkové organizace, obce)
- IDM musí umožnit obousměrnou synchronizaci dat, tzn. jak z IDM do IS (např. uživatele a jejich atributy), tak z IS do IDM (např. role IS, do kterých je možné uživatele zařazovat)
- IDM podporuje Single Sign-On — Centrální správce identit zajišťuje, že uživatelské jméno a heslo uživatele jsou shodné ve všech informačních systémech napojených na tuto komponentu.
- IDM musí mít rozhraní pro správu hesel a musí umožnit interním uživatelům změnit heslo prostřednictvím dialogového okna operačního systému Windows
- IDM disponuje jednoduchou správou rolí:
    - Vytvoření nové role
    - Změna oprávnění pro roli
    - Smazání role
- IDM musí umožňovat synchronizaci identit v IS (vstupně/výstupní operace) prostřednicím těchto rozhraní:
    - databázová tabulka, view
    - webová služba SOAP
    - CSV textový soubor
    - XML struktura (soubor)
    - LDAP v3
- IDM musí mít podporu českého jazyka z hlediska dat, se kterými pracuje IDM včetně možnosti případného ořezání diakritiky
- v rámci implementace musí být zajištěno školení administrátorů prostředí (pro max. 5 osob) v min. rozsahu 3 MD a pověřených uživatelů (max. 10) v min. rozsahu 0,5 MD.
- IDM musí udržovat heslo uživatelů v nerozšifrovatelné podobě
- Vybrané operace nad identitami jsou zaznamenány v auditním logu
- Možnost definice politik pro zabránění neoprávněné kumulace oprávnění
- Analýza nasazení musí obsahovat:
- Návrh architektury IDM a vazeb na vybrané informační systémy (topologie, technické požadavky, rozhraní, protokoly, grafické schéma celého řešení)
- Návrh a harmonogram nasazení IDM

- Návrh metodiky pro správu identit
- Návrh doporučení a metodiky pro správu identit, práv a popis rozhraní v nově nasazovaných IS (bude používáno při definování požadavků na nové IS)
- Návrh procesů správy životního cyklu uživatelů a způsob integrace CSI
- Minimálně budou zpracovány tyto procesy:
    - Příchod uživatele / Nástup zaměstnance
    - Odchod uživatele/ Ukončení zaměstnaneckého poměru
    - Změna uživatele
    - Žádost o přidělení role
    - Změna organizačního zařazení
- Návrh mechanismu rolí pro přístup do jednotlivých IS a specifikace jejich oprávnění (minimálně bude zpracováno 10 vzorových rolí)
- Specifikaci vývojového, testovacího a produkčního prostředí CSI
- Návrhu pilotního provozu a akceptačních kritérií
- Návrh postupu přechodu do produkce
- Definici bezpečnostních zásad a pravidel pro práci s CSI

19.11.1 Požadavky na manažera informační bezpečnosti

Pojem „manažer informační bezpečnosti“ není v oblasti ICT neznámý. V organizacích však funkci manažera IB zpravidla postrádáme obdobně jako samotný ISMS. Potřeba vytvoření funkce manažera IB ovšem vyplývá nejen z bezpečnostních standardů, ale i z konkrétních doporučení analýzy rizik IS (byla-li u zákazníka již realizována) a zpravidla zejména z interní potřeby jednotně, systematicky a efektivně řídit informační bezpečnost.

19.11.2 Náplň činnosti manažera IB

Náplň práce manažera IB je upravena formou harmonogramu, který definuje jednotlivé požadované a pravidelně se opakující činnosti, jako je např.:

1. kontrola monitoringu a analýzy auditních záznamů (logů);
2. analýza a vyhodnocení bezpečnostních incidentů;
3. revize bezpečnostní dokumentace;
4. ověřování pravidelného testování odolnosti sítě (penetrační testy sítí a serverů);
5. průběžná kontrola aktuálnosti patch-managementu;
6. pravidelná kontrola dodržování bezpečnostních pravidel v organizaci (prověrka stanic);
7. pravidelná kontrola dodržování licenční politiky (SW audit);
8. pravidelný reporting o bezpečnostní situaci pro management organizace;
9. pravidelná bezpečnostní školení zaměstnanců;
10. další služby dle individuálních požadavků zákazníka.

Každá z činností má definován:

- rozsah,
- četnost/frekvenci,
- formu a způsob evidence,
- formu a způsob reportingu,
- kontaktní a zodpovědné osoby.

Manažer IB v žádném případě nepřebírá odpovědnost za bezpečnostní incidenty v IS zákazníka. Tomu odpovídá charakter této funkce, neboť není (a nebude pověřen) žádnou rozhodovací ani výkonnou pravomocí. Jeho povinností je v tomto směru pouze sledovat, kontrolovat, reportovat a upozorňovat management na anomálie, nové hrozby, zranitelná místa či vzniklá rizika, ohrožující IS.

Na orgány státní/veřejné správy a samosprávy se vztahují specifické legislativní předpisy upravující požadavky na kvalitu a bezpečnost informačních systémů veřejné správy. Náležitosti, rozsah a obsah „povinné“ dokumentace a další podmínky byly poměrně striktně a detailně definovány příslušným zákonem, resp. prováděcími vyhláškami a jsou popsány v následujících kapitolách.

19.12 Související legislativa, normy a standardy

Zákon č. 101/2000 Sb. o ochraně osobních údajů;

Zákon č. 227/2000 Sb. o elektronickém podpisu;

Zákon č. 365/2000 Sb. o informačních systémech veřejné správy v aktuálním znění;

Vyhláška č. 529/2006 Sb. o dlouhodobém řízení ISVS;

Zákon č. 106/1999 Sb. o svobodném přístupu k informacím;

Zákon č. 412/2005 Sb., o ochraně utajovaných skutečností a o bezpečnostní způsobilosti;

Zákon č. 499/2004 Sb., o archivnictví a spisové službě.

Zákon č. 181/2014 Sb. o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti);

ČSN ISO/IEC 27001 - Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky;

- pův. ČSN ISO/IEC 17799 - Informační technologie - Soubor postupů pro řízení informační bezpečnosti,
- a ČSN BS 7799-2 - Systém managementu bezpečnosti informací - Specifikace s návodem pro použití;

ČSN ISO/IEC TR 13335

- Informační technologie - Směrnice pro řízení bezpečnosti IT.

Používaná metodika

Rozhodující jsou na straně zákazníka jeho požadavky a potřeby, kapacitní, časové a finanční možnosti, ale také současný stav a rozsah ISVS, platnost dosavadních atestací, dostupnost a aktuálnost stávající dokumentace.

Na straně zpracovatele je největší důraz kladen na spokojenost zákazníka s kvalitou a bezpečností nabízeného řešení a na poskytování komplexních služeb. Usilujeme také o efektivitu řešení. To znamená, že posuzujeme ekonomické hledisko a hledáme pro zákazníka přijatelné řešení jen takových služeb a v takovém rozsahu, aby nebyl nucen vynakládat zbytečně víc, než je nezbytné.

Konkrétní kroky realizace projektu zpracování dokumentace jsou zpravidla následující:

- smluvními stranami odsouhlasen harmonogram projektu;
- stanoven detailní postup realizace projektu nebo jeho etap;
- definovány požadavky součinnosti ze strany zákazníka (účast na osobních konzultacích formou dotazování za účelem vyplnění podkladových dotazníků);
- určeni respondenti zodpovídající za poskytnutí potřebných informací, údajů a dokumentace;
- dohodnut způsob zabezpečení informací poskytovaných zpracovateli elektronickou formou;
- dohodnuto poskytnutí všech relevantních materiálů, které mají vypovídací schopnost o ISVS;
- uskutečněny schůzky na půdě organizace za účelem získání informací, důležitých pro zpracování;
- analýza a vlastní zpracování získaných informací zpracovatelem, tj. kompletace podkladových informací, vyhodnocení obdržených informací a dalších požadovaných materiálů;
- vytvoření dokumentů, jež tvoří výsledný výstup z projektu;
- prezentace výsledků, schvalovací a akceptační proces, předání díla.

Součástí je proto nejen zpracování požadovaných dokumentů, ale také zajištění spolupráce s vybraným atestačním střediskem, garance shody zpracované dokumentace s požadavky legislativy a úspěšné atestace.

19.13 Dlouhodobé řízení bezpečnosti informací

Povinnosti orgánů veřejné správy spravujících ISVS

Novelizovaný zákon č. 365/2000 Sb., o ISVS, ukládá orgánům veřejné správy (dále jen OVS) povinnosti pro zajištění kvalitních dat veřejné správy a bezpečné technologické výměny informací za předem stanovených podmínek.

Prováděcí právní předpis k tomuto zákonu - vyhláška č. 529/2006 Sb., o dlouhodobém řízení ISVS - stanovuje pro OVS spravující ISVS povinný rozsah a obsah dokumentace. Tato dokumentace je předkládána při atestaci, kterou OVS prokazuje splnění zákonných požadavků.

Orgán veřejné správy jako správce ISVS[1] je povinen zajistit atestaci shody dlouhodobého řízení ISVS s požadavky zákona, resp. vyhlášky, přičemž musí:

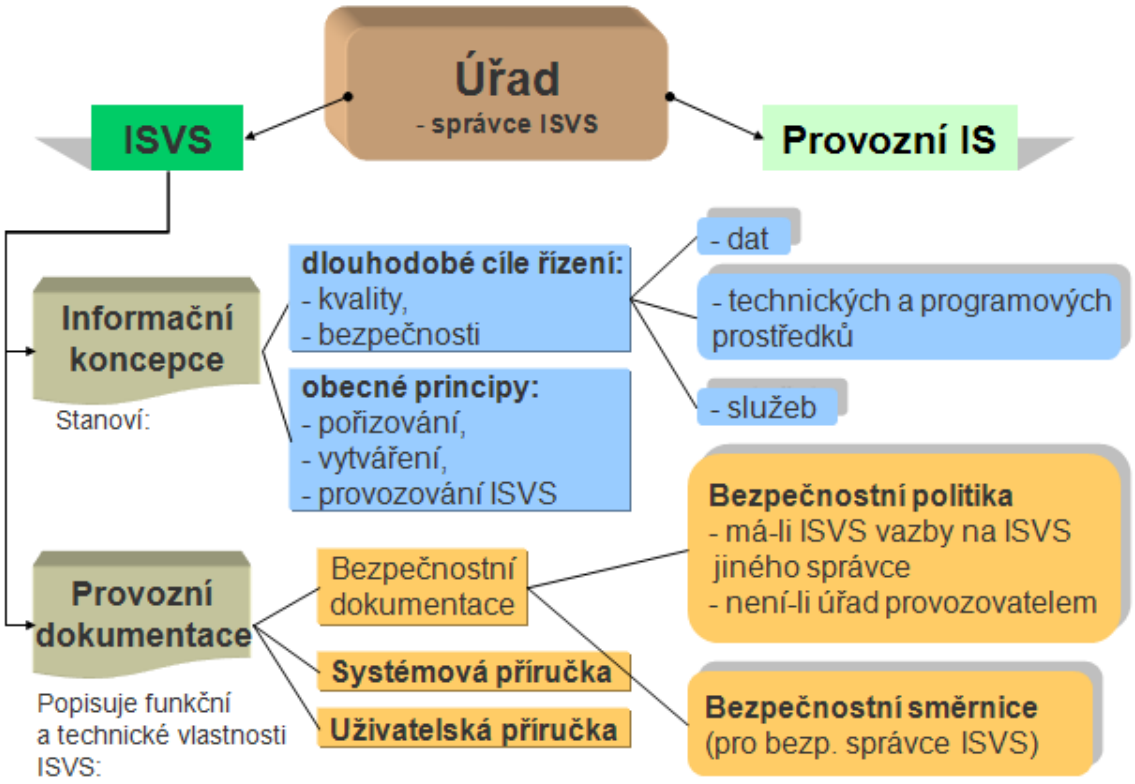
- mít zpracovánu „informační koncepci“ a „provozní dokumentaci“ - do 1. 1. 2009,
- zajistit atest dlouhodobého řízení ISVS do 1. 1. 2010.

V rámci komplexního řešení jsme schopni nabídnout své služby při zpracování informační koncepce a provozní dokumentace ve vyhláškou požadovaném rozsahu a připravíme tuto dokumentaci k atestaci dlouhodobého řízení ISVS.

[1] **ISVS** (Informační systém veřejné správy) slouží pro výkon veřejné správy (např. rejstříky, evidence, IS pro e-podatelnu, pro spisovou službu, webové stránky zpřístupňující informace z ISVS způsobem umožňujícím dálkový přístup atd.).
Správce ISVS je subjekt, který podle zákona určuje účel a prostředky zpracování informací a za informační systém odpovídá.
Provozovatel ISVS je subjekt, který provádí alespoň některé informační činnosti související s informačním systémem, tj. provozuje ISVS, příp. vedením/provozováním ISVS pověřuje externí firmu.

Pro zpracování systému dlouhodobého řízení v souladu s příslušnou legislativou se jeví jako logické (viz následující obrázek) a také optimální rozčlenění do dvou samostatných etap:

- zpracování **informační koncepce** (viz kapitola 19.14),
- zpracování **provozní dokumentace** (viz kapitola 19.14.1).



19.14 Informační koncepce

Jedním z vyhláškou požadovaných dokumentů je tzv. informační koncepce (dále také IK), která tvoří základ dlouhodobého řízení ISVS. Její obsah je patrný z následujícího výřezu obrázku:

Činnosti v rámci tvorby informační koncepce jsou následující:

- zpracování přehledu ISVS
  - jedná se v podstatě o inventuru IS/ISVS úřadu, která zahrnuje požadované údaje, jako např. název, dodavatel, správce, bezpečnostní správce, vazby na jiné ISVS atd.;
- popis jednotlivých ISVS
  - zpracování popisu ISVS s uvedením charakteristiky, určení, zpracovávaných dat, zajišťovaných služeb a používaných technických a programových prostředků, současného stavu a předpokládaných změn;
- zpracování záměrů na pořízení nebo vytvoření ISVS
  - tj. shromáždění údajů o uvažovaných ISVS, jež má úřad v plánu pořídit či vytvořit na základě plánovaných změn;
- zpracování plánu řízení kvality ISVS
  - jež obnáší definici cílů a požadavků na kvalitu ISVS z hlediska dat, služeb a technických a programových prostředků;
- zpracování plánu řízení bezpečnosti ISVS
  - jež obnáší definici cílů a požadavků na bezpečnost ISVS z hlediska dat, služeb a technických a programových prostředků;
- zpracování pravidel pro správu všech ISVS
  - tj. zásad a postupů pro pořizování a vytváření, provozování a údržbu, a dále pro změnové řízení a případné ukončení činnosti;
- zpracování pravidel financování
  - tzn. popis pravidel financování pro vytvoření či pořízení ISVS, financování dlouhodobých cílů (realizace cílů a požadavků kvality a bezpečnosti) a financování správy (provozu a údržby);
  - v souladu s obecnými předpisy, podmínkami zadávání veřejných zakázek a zakázek malého rozsahu a s popisem rolí a odpovědností při získávání finančních prostředků;
- zpracování pravidel pro kontrolu a vyhodnocování IK
  - v jejichž rámci jsou popsána pravidla pro provádění změn v IK, vyhodnocování a dodržování IK, a definice rolí a odpovědností za jednotlivé činnosti;
- zpracování pravidel pro realizaci IK
  - v nichž budou stanoveny kontrolní mechanismy a odpovědnosti za realizaci a za plnění zákonných povinností při dlouhodobém řízení ISVS.

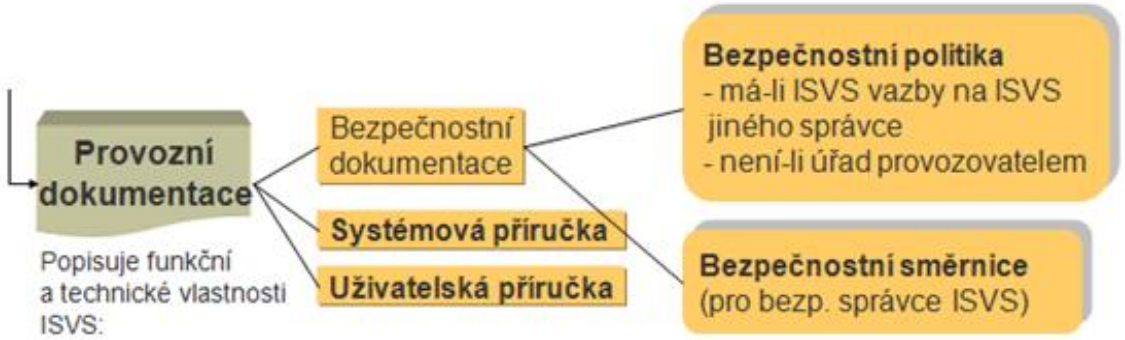
V rámci této etapy projektu zpracování systému dlouhodobého řízení ISVS budou mj. vytvořeny vstupní dotazníky a podkladové tabulky. Tyto vzory poslouží dvěma účelům zároveň:

- jednak ke sběru a shromáždění vstupních údajů, a jejich zpracování do informační koncepce,
- jednak v pozdějších fázích – naplňování systému budou fungovat jako opakovaně použitelné šablony a mustry pro praktické naplňování pravidel dlouhodobého řízení, pro vedení potřebné evidence, záznamů a změn.

19.14.1 Provozní dokumentace

Souhrnem dokumentů pro podporu dlouhodobého řízení ISVS je tzv. provozní dokumentace (dále také PD). Vyhláškou je obdobně jako u informační koncepce určen rozsah provozní dokumentace a jsou definovány typy dokumentů včetně těch, jež úřad povinně předkládá při atestaci ISVS.

Obsah je patrný z následujícího výřezu obrázku:



Zpracování bezpečnostní politiky a související bezpečnostní dokumentace organizace považujeme zpravidla za krok následující logicky po analýze rizik IS. Z jejích závěrů totiž vyplývají nejen rizika, ale také návrhy protiopatření, vhodných k jejich detekci, prevenci a eliminaci. Zohlednění výsledků analýzy rizik IS v bezpečnostní politice a souvisejících dokumentech je důležité při výběru a implementaci bezpečnostních opatření do každodenní praxe. Provedení analýzy rizik IS však nepodmiňuje vlastní zpracování bezpečnostní dokumentace, byť je doporučováno.

Rozsah bezpečnostní dokumentace uvedený v této nabídce bude přizpůsoben konkrétnímu požadavku na zpracování provozní dokumentace (dle Vyhlášky o dlouhodobém řízení ISVS).

19.14.2 Bezpečnostní dokumentace

Bezpečnostní dokumentace by se neměla omezit pouze na obecně definovanou bezpečnostní politiku, ale měla by odrážet cíle, strategie a politiky úřadu v oblasti informačních a komunikačních technologií (ICT). Bezpečnostní politika v dokumentované podobě tak, jak vyplývá např. z normy ČSN ISO/IEC 27001, tvoří základ řízení informační bezpečnosti, a jako taková by měla obsahovat mj. souhrn všech relevantních předpisů, pravidel, povinností a zodpovědností určených ke správě a ochraně IS (včetně ISVS) a informací v organizaci.

Bezpečnostní politika

Bezpečnostní politika bude obsahovat specifikaci bezpečnostních požadavků a opatření pro určený informační systém (nebo subsystém) veřejné správy. Stručně vyjádřeno tato politika popisuje technická a technologická opatření a konkrétní prostředky, jimiž má být daný IS/ISVS chráněn.

Pojem informační systém pro potřeby této nabídky představuje ucelený soubor specifických informačních a komunikačních technologií včetně informací organizace, skládající se případně z dalších podsystémů, které tvoří jeden kompaktní celek a mají shodné požadavky na způsob zabezpečení a ochrany. Bude-li identifikován odlišný informační systém s rozdílnými požadavky na úroveň zajištění bezpečnosti, budou tyto specifické požadavky zohledněny v samostatné bezpečnostní politice určené jen pro tento IS/ISVS.

Bezpečnostní politika je dokument povinně předkládaný při atestaci.

Bezpečnostní směrnice

Další potřebné dokumenty, které by měly být součástí bezpečnostní dokumentace, mohou mít charakter bezpečnostních směrnic. Důvod tohoto členění dokumentace spočívá mj. v cílové skupině jejích uživatelů, jimž je ten který dokument určen. Výhodou odděleného zpracování je mj. možnost definovat skupiny uživatelů oprávněných seznamovat se s příslušnými dokumenty, odpovídající distribuce jednotlivých dokumentů, zjednodušení aktualizace a přizpůsobení dokumentů potřebným změnám. Jinou bezpečnostní směrnici bude např. vyžadovat správce sítě (administrátor), jinou bezpečnostní správce ISVS.

Bezpečnostní směrnice dle Vyhlášky představuje konkrétní závazný dokument definující bezpečnostní pravidla, povinnosti a odpovědnosti konkrétně pro bezpečnostního správce.

19.14.3 Příručky

V rámci tvorby provozní dokumentace mohou být zpracovány také detailní postupy pro konkrétní situace a procesy. Tyto postupy charakteru systémové nebo uživatelské příručky dle Vyhlášky obsahují instrukce a návody pro různé skupiny uživatel a mely by být zpracovány (nelze-li např. systémovou příručku v souladu se zněním vyhlášky sloučit s bezpečnostní dokumentací) odděleně tj.:

- systémová příručka pro správce systému,
- uživatelská příručka pro uživatele IS.

20. Další rozvoj

20.1 Koncepce připojení do komunikační infrastruktury v segmentu ORP

Základním předpokladem pro plošnější připojování jednotlivých bodů zájmů je systematické zmapování subjektů, jejich požadavků a následné rozčlenění do skupin.

20.1.1 Pasportizace bodu zájmu

Navrhujeme, aby bylo postupováno následujícím způsobem:

- pasportizace bodu zájmu Pardubického kraje – zmapování požadavků všech subjektů a jejich připravenosti pro napojení na regionální síť Pardubického kraje
- rozdělení bodů zájmů do skupin dle společných rysů a požadavků
- přiřazení formy připojení, typů aktivních prvků a variant služeb jednotlivým skupinám
- zmapování možností pořízení optických tras k jednotlivým bodům
- vypracování harmonogramu připojování podle priorit a podle náročnosti připojení

20.1.2 Způsob připojení PON

Pro zachování a rozšíření současného řešení je vhodné použití optických vláken, které umožňují použití frekvenčního multiplexu (xWDM). Díky vlastnostem optického vlákna je možné jejich plné využití pro nasazení optických technologií typu dělení vlnových délek DWDM nebo CWDM.

Tato topologie sítě je typická pro architekturu AON (Active Optical Network), avšak vzhledem k celkové ekonomické stránce projektu není možná výstavba výhradně touto architekturou. Proto doporučujeme architekturu optických sítí – PON (Passive Optical Network).

Technologie vlnového dělení WDM umožňuje paralelně přenášet po jednom optickém vlákně několik navzájem oddělených vlnových délek a tím znásobit jeho celkovou kapacitu.

Pro hrubé vlnové dělení CWDM byly definovány jednotlivé kanály s první nosnou 1270 nm a poslední 1610 nm, s odstupem mezi jednotlivými nosnými 20 nm a tolerancí nosné ±6,5 nm. Větší rozteč kanálů a dodatečná tolerance je nutná z důvodu použití obecně méně kvalitních optických zdrojů v optických přístupových sítích a závislosti vysílané vlnové délky na teplotě. Pro standardní jednovidové vlákno 9/125 μm je definováno 18 kanálů [3] rozdělených do následujících pásem:

Pásmo O (Original): vlnové délky 1260-1360 nm, nosné číslo 1-5

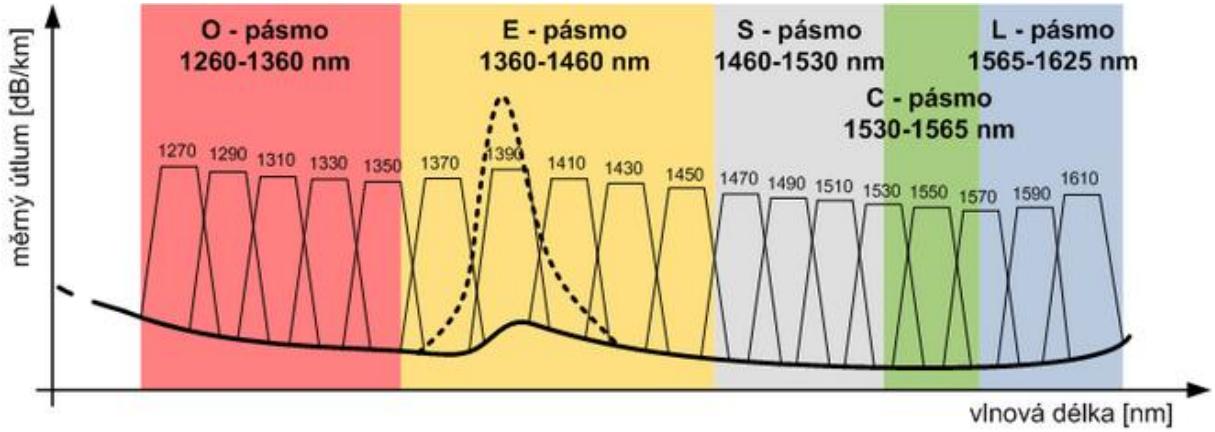
Pásmo E (Extended): vlnové délky 1360-1460 nm, nosné číslo 6-10 (počítá se s optickým vláknem s potlačenými ionty OH-, v obr. 1 naznačeno čárkovaně)

Pásmo S (Short): vlnové délky 1460-1530 nm, nosné číslo 11-14

Pásmo C (Conventional): vlnové délky 1530-1565, nosná číslo 15

Pásmo L (Long): vlnové délky 1565-1625 nm, nosné číslo 16-18

CWDM pásma dle standardu ITU-T (ITU-T G.694.2):



20.1.3 Lokality pro rozšíření

Typ lokality	Název ORP	Adresa zakončení RDS	Číslo místnosti/patro
Koncová lokalita	Česká Třebová	Staré náměstí 78, 560 02 Česká Třebová	012/1.nadzemní podlaží
Koncová lokalita	Hlinsko	Adámkova 554, Hlinsko	1.04/1.patro
Koncová lokalita	Holice	Holubova 1, Holice	208/2.nadzemní podlaží
Koncová lokalita	Králíky	Velké náměstí 5, 561 69 Králíky	serverovna/4.nadzemní podlaží
Koncová lokalita	Lanškroun	nám. J. M. Marků 5, 563 01 Lanškroun	35/2. patro
Koncová lokalita	Moravská Třebová	Olomoucká 178/2 571 01 Moravská Třebová	110/1.nadzemní podlaží
Koncová lokalita	Polička	Palackého nám. 160, 57201 Polička	7C/přízemí
Koncová lokalita	Přelouč	Československé armády 1665	4.11A/4.patro
Koncová lokalita	Vysoké Mýto	B. Smetany 92, 566 32 Vysoké Mýto	114/1.patro
Koncová lokalita	Žamberk	Nádražní ulice 833	31/ 2.patro

20.1.4 Ideální varianta rozvoje RDS

Pro zajištění vysoké dostupnosti, bezpečnosti, celkové kvality a zachování možnosti bezproblémového rozvoje je ideální tzv. "maximalistická" varianta, tj. technicky nejvhodnější řešení s

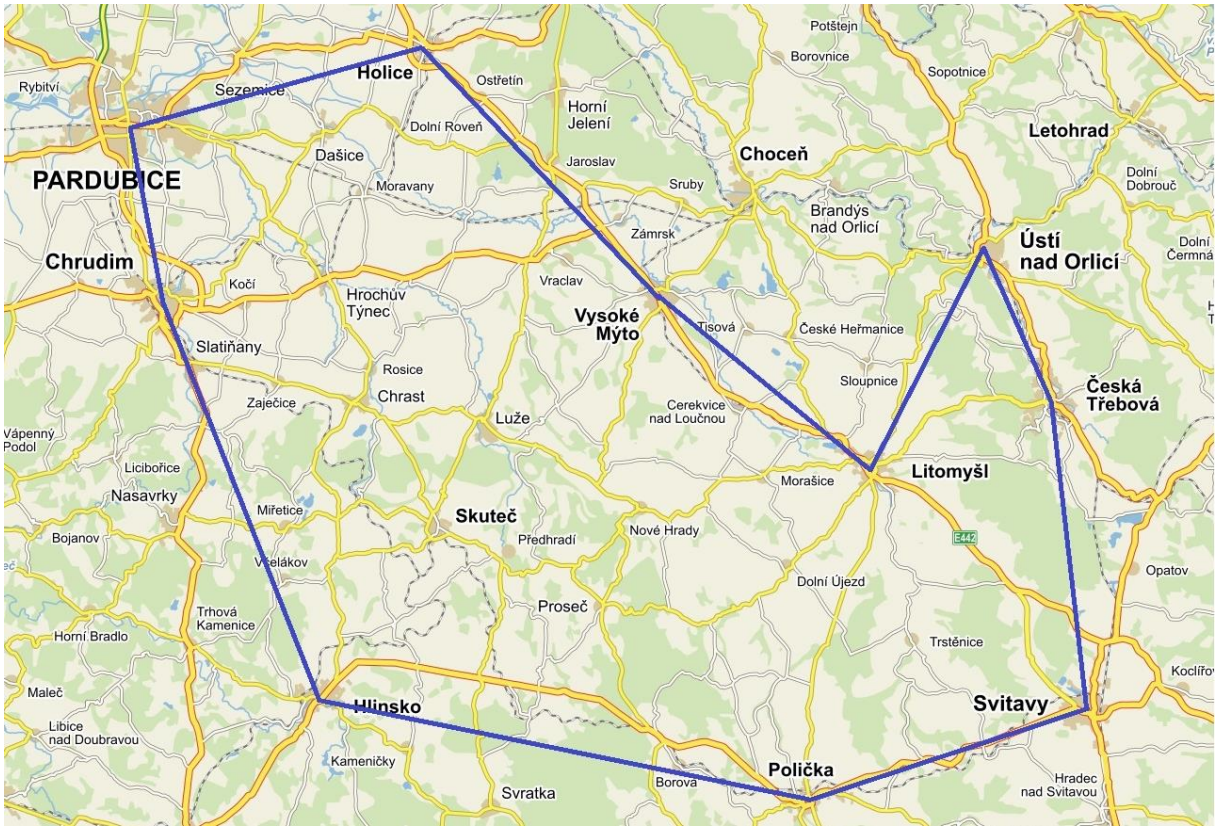
minimálním ohledem na finanční náročnost. Smyslem budoucího rozvoje by mělo být přiblížit se této variantě v maximální možné míře.

1. Fyzická topologie

Pro zajištění maximální dostupnosti jsou ideální variantou redundantní trasy do každé lokality, tj. dvojice optických vláken s nezávislým vedením v celém průběhu, případně zakruhování lokalit, aby při výpadku jakékoli trasy nedošlo k výpadku žádné z lokalit (v kruhu).

V případě RDS se jeví jako vhodná varianta zakruhování lokalit Pardubice (obě DC), Chrudim, Hlinsko, Polička, Svitavy, Česká Třebová, Ústí nad Orlicí, Litomyšl, Vysoké Mýto, Holice. Pasivní trasy by byly vedeny pouze mezi nejbližšími městy (ne do agregačních lokalit či datových center). V takovém případě by bylo možné využít kapacity (N x 10Gb) na všech zmíněných spojích, čímž bude zachován požadavek na 1Gb pro každou lokalitu do DC. I v tomto modelu je počítáno s CWDM řešením, které by umožnilo multiplexovat právě (N x 10Gb).

Nákres možného zakruhování:



Ostatní lokality by byly připojeny pasivně jedním vláknem k nebližší lokalitě v kruhu a druhým vláknem k druhé nejbližší lokalitě v kruhu s maximální snahou o zachování nezávislého vedení těchto vláken.

Toto řešení vyžaduje redundanci na úrovni pasivních i aktivních prvků (viz bod 2 a 3).

Z hlediska dalšího rozvoje předpokládáme 2 nová vlákna mezi datovými centry.

2. Pasivní část sítě

Ve všech lokalitách by byly využity Add/Drop nebo MUX komponenty CWDM systému pro využití možnosti přenosu (N x 10Gb), kde N je počet využitých lambd. Vzhledem k požadavku gigabitové konektivity z každé lokality do centra je vhodné uvažovat již nyní min. 2 x 10 GE řešení (je nutné počítat s kapacitou jako gigabitovým násobkem počtu koncových lokalit v libovolném místě kruhu).

3. Aktivní část sítě

Pro fungování redundance v síti jako celku je nutné zajistit ji i na úrovni aktivních prvků (PE). To znamená 2 aktivní prvky v každé lokalitě (nejen v agregační a datových centrech). Pro zajištění kompatibility, jednoduché správy a konfigurace a možnosti dalšího rozšíření předpokládáme zapojení těchto 2 aktivních prvků do Stacku/Virtuálního chassis.

Požadavky na aktivní prvky jsou definovány v bodě 8.

4. Dohled sítě

Další částí RDS vyžadující vysokou dostupnost je HW a SW pro dohled této sítě. Vhodným řešením je druhý server s dohledovým systémem v režimu active/standby umístěným v druhém datovém centru pro zajištění geografické redundance. Alternativou je virtualizace, tj. dohledový systém na virtualizované platformě (ideálně taktéž s geografickou redundancí).

5. Bezpečnost

S předpokládaným nárůstem komunikace uvnitř, ale především s externími sítěmi včetně internetu se bude snižovat bezpečnost v RDS. Pro její zajištění je nutné zajistit veškeré perimetry v síti (přístupy do externích sítí) a stejně tak je nutné monitorovat provoz v síti.

Pro zajištění bezpečného přístupu na Internet, případně ochranu serverů dostupných z internetu předpokládáme využití dvojice aplikačních firewallů v HA konfiguraci (pracujících až do 7 vrstvy OSI modelu). Ty by měly být umístěny mezi RDS a aktuální dvojicí FW.

Pro monitoring sítě předpokládáme využití systému sond, konektorů, záznamu kompletního datového provozu, detekci a ochranu před útoky.

Řešení by mělo zajišťovat:

- Detailní přehled o dění v počítačové síti
- Rychlé a efektivní řešení problémů na síti
- Zvýšení bezpečnosti sítě a možnost odhalení vnějších i vnitřních útoků
- Detekce síťových anomálií – komunikace s C& C servery, infikované stanice, DDoS a další útoky
- Analýza dlouhodobých statistik s rozlišením na jednotlivé počítače, aplikace až na úroveň jednotlivých spojení)
- Monitorování uživatelů a používaných služeb
- Efektivní plánování kapacit sítě
- Dlouhodobé uložení statistik o síťovém provozu
- Sledování výkonových parametrů sítě i aplikací, identifikace příčin výkonnostních problémů
- Snadné plánování a monitorování QoS

V geograficky redundantním módu předpokládáme zajištění Radius Serveru (dvojice Radius Serverů) pro řízení přístupů k managementu sítě, aktivním prvkům, případně dalším systémům/aplikacím.

6. Přístup k Internetu

Detailní popis v bodě 3.8. (částečně 7.3, Internet Edge)

7. odhad nákladů ideální varianty

Řešení	Odhadovaný náklad	Poznámka
Fyzická topologie	144 000 000 Kč	Předpokladem je 450 km nových tras dvou optických vláken, odhadovaná cena 160 Kč/m.
Pasivní část sítě	2 000 000 Kč	Ceny jsou odhadovány na základě list price (GPL) případných výrobců
Aktivní část sítě	9 000 000 Kč	Ceny jsou odhadovány na základě list price (GPL) případných výrobců
Dohled sítě	1 000 000 Kč	Ceny jsou odhadovány na základě list price (GPL) případných výrobců
Bezpečnost	8 500 000 Kč	Ceny jsou odhadovány na základě list price (GPL) případných výrobců
Přístup k Internetu	800 000 Kč	Ceny jsou odhadovány na základě list price (GPL) případných výrobců

20.1.5 Možnosti připojení jednotlivých lokalit

Pro možnost připojení nových lokalit byly dotázány dvě společnosti (CETIN, ČD Telematika), u kterých předpokládáme nejvíce rozvinutou optickou síť v kraji. Při realizaci poptávky doporučujeme oslovit také lokální společnosti poskytující optickou infrastrukturu v jednotlivých lokalitách. Kombinací globálních a lokálních poskytovatelů může dojít k výraznému snížení nákladů za optickou síť.

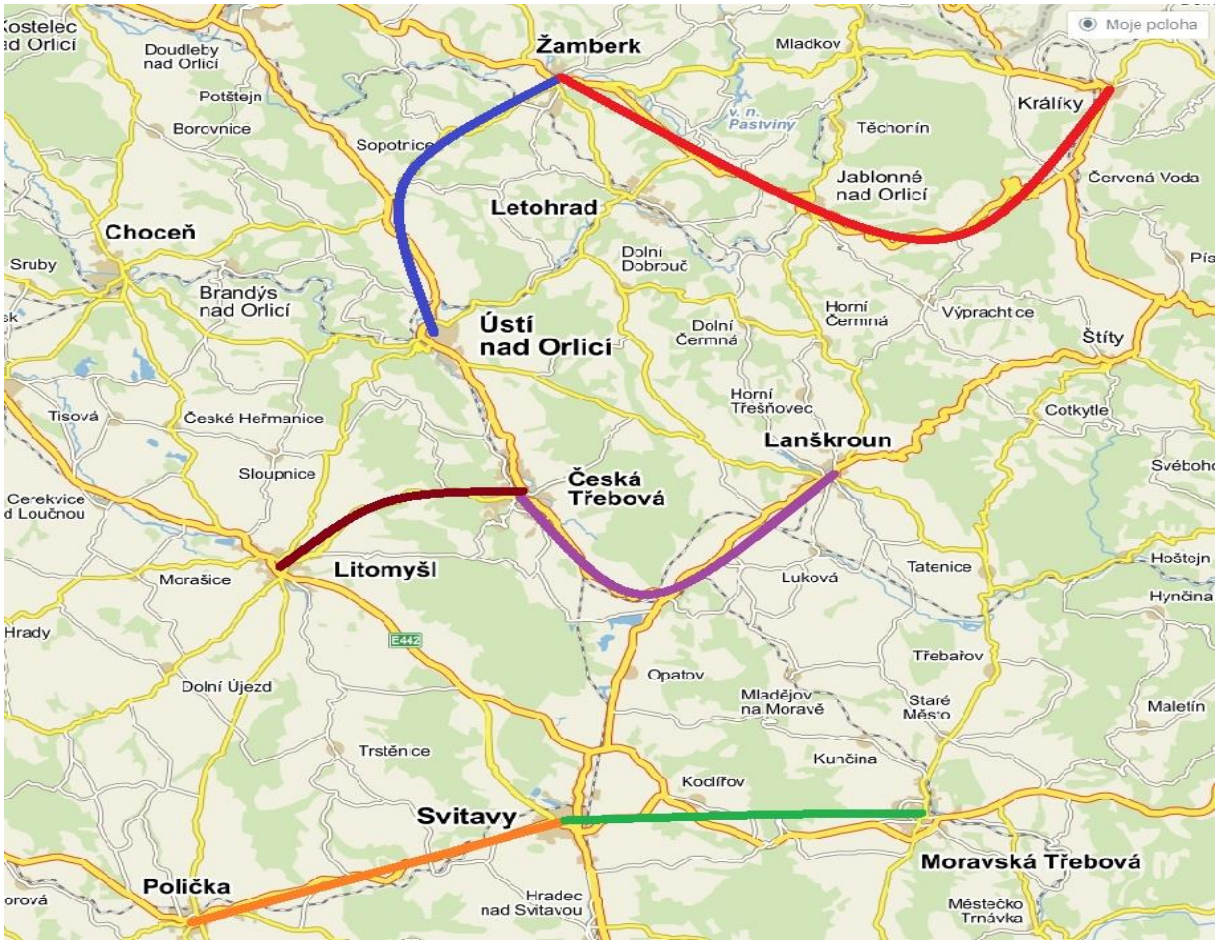
ČD Telematika

Název úřadu	Délka trasy	Délka dokopů	Délka záfuku	Průběh
MÚ Česká Třebová	10 km	0 m	-	Ústí – Č. Třebová
MÚ Holice	30 km	500 m	-	Pardubice - Moravany - Holice
MÚ Lanškroun	30 km	700 m	-	Č. Třebová - Lanškroun
MÚ Polička	80 km	250 m	-	Pardubice - Moravany - Chrudim - Skuteč - Polička
MÚ Přelouč	20 km	500 m	-	Pardubice - Přelouč
MÚ Žamberk	30 km	750 m	-	Ústí - Žamberk
MÚ Hlinsko	X	-	-	Trasu není možné realizovat
MÚ Králíky	X	-	-	Trasu není možné realizovat
MÚ Moravská Třebová	X	-	-	Trasu není možné realizovat
MÚVysoké Mýto	X	-	-	Trasu není možné realizovat

CETIN

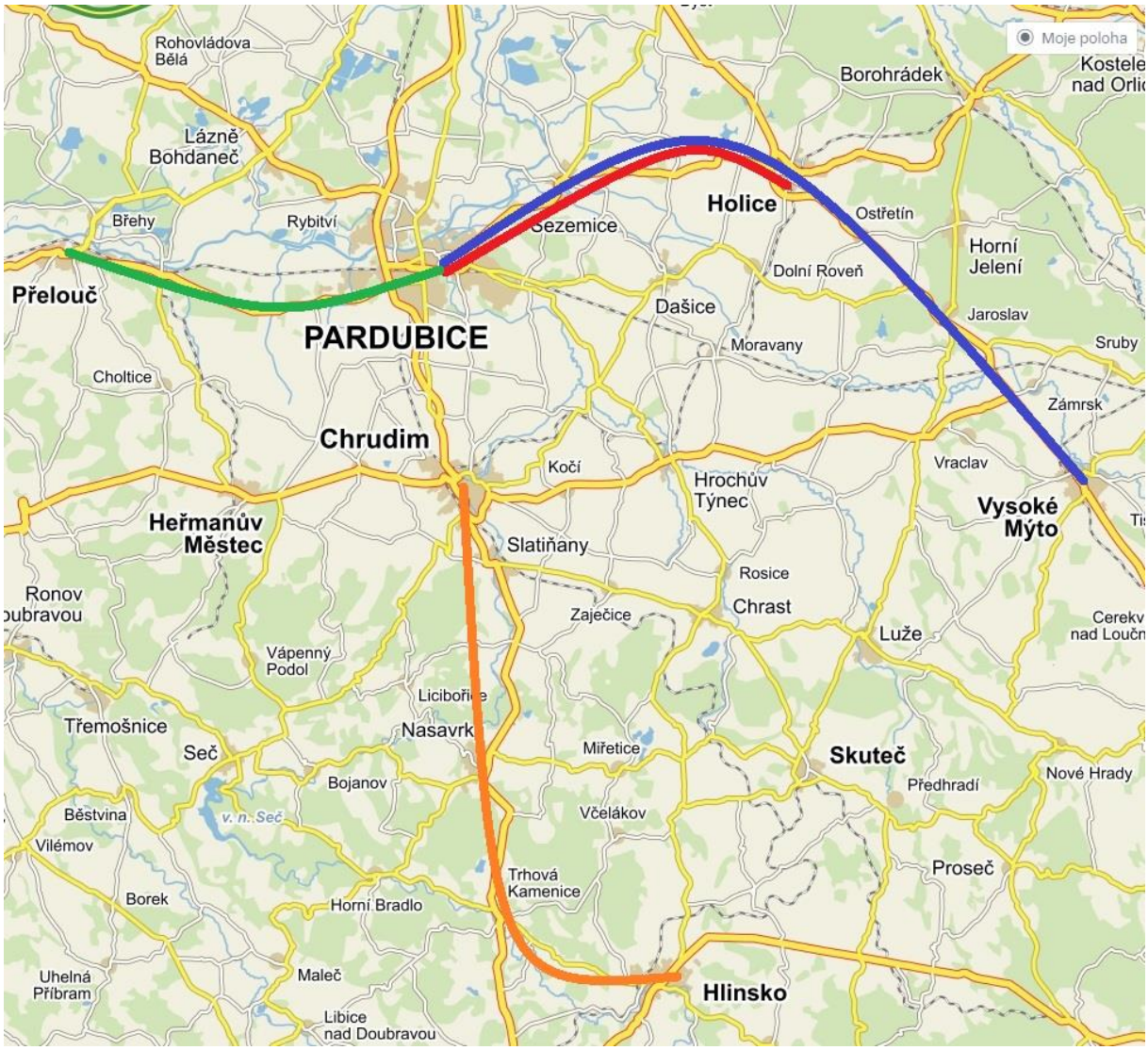
Název úřadu	Délka trasy	Délka dokopů	Délka záfuku	Průběh
MÚ Česká Třebová	10 km	0 m	550 m	Litomyšl – Česká Třebová
MÚ Holice	25 km	0 m	650 m	Pardubice - Sezemice - Holice
MÚ Lanškroun	30 km	0 m	480 m	Č. Třebová - Lanškroun
MÚ Polička	25 km	0 m	500 m	Svitavy - Polička
MÚ Přelouč	20 km	0 m	1300 m	Pardubice - Přelouč
MÚ Žamberk	30 km	0 m	640 m	Ústí – Žamberk
MÚ Hlinsko	45 km	0 m	1400 m	Chrudim - Hlinsko
MÚ Králíky	35 km	0 m	220 m	Žamberk - Králíky
MÚ Moravská Třebová	20 km	0 m	330 m	Svitavy - Moravská Třebová
MÚ Vysoké Mýto	50 km	0 m	0 m	Pardubice - Vysoké Mýto

Připojení lokalit v mapovém podkladu (východ)



Lokality Polička a Moravská Třebová mohou být ukončeny v lokalitě Svitavy. Odtud předpokládáme pasivní přenos po již existující optice na volných vlnových délkách do Agregační lokality Litomyšl. Z dostupných podkladů vyplívá, že délka optického kabelu, tj. i jeho útlum by měl toto řešení umožňovat. Českou Třebovou lze připojit přímo do agregační lokality Litomyšl, Lokalitu Lanškroun do České Třebové a odtud opět pasivně do agregační lokality Litomyšl. Lokalitu Žamberk předpokládáme připojit do Ústí nad Orlicí a dále pasivně do agregační lokality Litomyšl. Lokalitu Králíky je možné připojit do Žamberku a dále pasivně do Ústí nad Orlicí. Jelikož celková optická trasa z Králíků do Litomyšle s velkou pravděpodobností přesáhne 100 km a není znám útlum trasy, jsou možné 2 varianty řešení - ukončit tuto lokalitu pasivně v Ústí, nebo v případě nízkého útlumu vést trasu pasivně až do agregační lokality Litomyšl.

Připojení lokalit v mapovém podkladu (západ)



Z mapových podkladů vyplívá, že lokality Přelouč, Holice a Vysoké Mýto mohou být připojeny párem optických vláken do datových center v Pardubicích. Optiku z lokality Hlinsko předpokládáme zakončit

v ORP Chrudim. Odtud předpokládáme pasivní přenos po již existující optice na volných vlnových délkách do Datových center v Pardubicích. Z dostupných podkladů vyplívá, že vzdálenost po optickém kabelu, tj. i útlum toto řešení umožňuje.

20.1.6 Předpokládaná topologie

Z důvodu zachování vysoké dostupnosti a možnosti síť dále rozšiřovat je vhodné uvažovat nad vznikem nových agregačních bodů. Z dostupných dat vyplívá, že budou využita datová centra a agregační lokalita Litomyšl k připojení nových lokalit. Dále se nabízejí 2 varianty úpravy topologie - vzniku agregačních lokalit, které přispějí ke zvýšení dostupnosti a také propustnosti sítě:

1) Agregační lokalita Vysoké Mýto

Vytvořením agregační lokality ve Vysokém Mýtě by bylo možné rozdělit koncové lokality (které nejsou ukončeny v datových centrech) mezi obě agregační, čímž by došlo ke zvýšení dostupnosti sítě. Případně připojit koncové lokality k oběma agregačním (per vlákno), pokud to dovolí vzdálenost/útlum.

Dále by bylo možné rozdělit současnou trasu Litomyšl - Pardubice. Zkrácením optické trasy a tudíž i útlumu by bylo možné na současných vláknech využít kapacitu 10Gb a tím zajistit neagregovanou rychlost pro každou z koncových lokalit min. 1 Gb.

2) Agregační lokality Vysoké Mýto a Ústí nad Orlicí

Důvody a výhody vytvoření agregační lokality ve Vysokém Mýtě jsou totožné i pro tuto variantu (viz popis výše - varianta 1)).

V případě, že by útlum z lokality Králíky neumožňoval pasivní připojení až do agregační lokality Litomyšl, bylo by možné vytvořit novou z lokality Ústí nad Orlicí. V takovém případě by mělo smysl ukončit zde i lokality Králíky, Žamberk, případně Česká Třebová a Lanškroun. Pro zvýšení dostupnosti sítě by tato agregační lokalita mohla být připojena do datových center severní trasou (kolem Hradce Králové, tj. rozdílnou od té současné). Toto řešení má bohužel i 2 nevýhody. Dlouhá optická trasa znamená velké náklady a zřejmě i nutnost opakovače.

20.1.7 Podmínky pro rozšíření

Ve všech lokalitách musí být umožněna výstavba vnitřního vedení a zajištěna součinnost pro výstavbu. Stejně tak je nutné zajistit místnost vhodnou pro provoz technologií (klimatizovanou, ideálně se stálou teplotou a vlhkostí). V této místnosti musí být k dispozici minimálně 4U v racku pro aktivní a pasivní prvky a vyvázání optických vláken. Dále musí být zajištěno napájení pro aktivní prvky (v ideálním případě zálohované).

Nedílnou součástí řešení jsou aktivní a pasivní prvky. Jejich kompatibilita se stávajícími aktivními prvky je podstatnou podmínkou pro funkčnost řešení jako celku. U aktivních prvků se jedná zejména o slučitelnost komunikačních protokolů, dohledu (management systému) a správy. Taktéž musí splňovat podmínku jejich možného využití i pro agregační lokality (v případě rozšíření z lokality koncové). Detailní popis požadavků na aktivní prvky je v kapitole 8.3.

20.1.8 Předpokládané náklady minimální varianty

Kromě varianty ideální, existuje varianta připojení nových uzlů do stávající topologie bez výrazných změn v ní. Tato varianta bere v potaz možnosti jednotlivých lokalit, stejně jako varianta ideální, pouze už pracuje s omezenými hledisky dostupnosti, kvality a rozvoje dané sítě. Z hlediska sítě se jedná přibližně o 290 km nových tras dvou optických vláken. Odhad nákladů je velmi problematický, jelikož prodej optických vláken poskytovatelem telekomunikačních služeb není běžný a cena je stanovována individuálně (s ohledem na typ a stáří optických vláken, případných inkrementálních nákladů a možného rozšíření počtu vláken v daných trasách bez nutnosti dokopů). Z dostupných informací a praktických zkušeností na trhu lze hrubě odhadnout cenu 160 Kč za metr optického vlákna. Při 290 km dvou vláken se jedná o 92 800 000 Kč za optickou infrastrukturu.

Zbylé náklady za vnitřní vedení, aktivní a pasivní prvky, projektové vedení, instalaci, konfiguraci a dokumentaci lze hrubě odhadnout v rozsahu deseti až patnácti milionů korun.

20.2 Koncepce připojení do komunikační infrastruktury v segmentu zdravotnictví

Z pohledu topologie sítě by měla být zdravotnická zařízení připojena jako koncové lokality.

Zabezpečení segmentu zdravotnictví doporučujeme vlastními HW i SW nástroji.

Koncept připojení zdravotnictví do komunikační infrastruktury je v dalších parametrech totožný se segmentem ORP uvedeným v bodě 20.1.

20.3 Možnosti vytvoření kolaboračního prostředí nad komunikační infrastrukturou

Díky nasazení technologie MPLS v páteřní síti lze např. v datových centrech vhodným routováním jednotlivých uživatelských vrf vytvořit kolaborační prostředí nejen pro krajský úřad Pardubického kraje, ale i pro organizace jím zřizované, které budou připojeny do regionální sítě. Tento koncept je vhodný zejména pro sdílení HW zdrojů anebo aplikací více uživateli z různých organizací (např. IP telefonie a aplikace nad ní provozované, file servery, zálohovací zařízení…).

Doporučujeme primárně provozovat sdílené aplikace pro více uživatelů z různých vrf v prostředí datových center.

20.4 Provozní řád

Detail provozního řádu popisuje dokument provozní dokumentace, kapitola 4.5.

20.5 Bezpečnostní pravidla

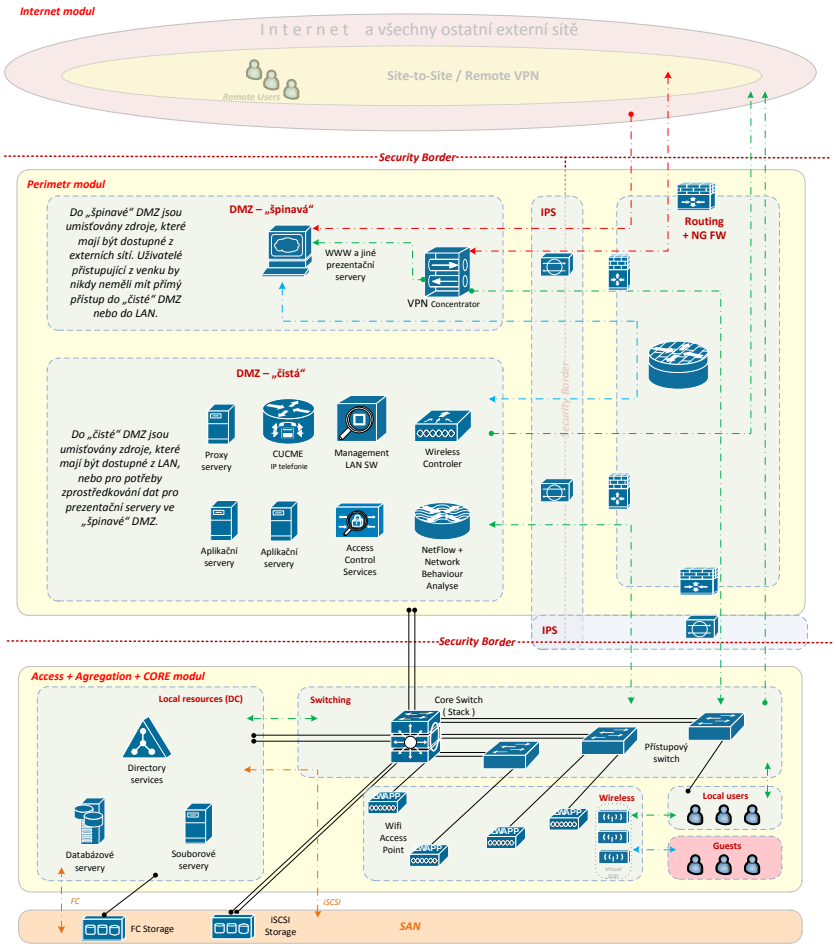
20.5.1 Komunikační model

RDS (Regionální datová síť Pardubického Kraje) je a i v budoucnu bude, z důvodu bezpečnosti, provozního a personálního obsazení, samostatná síť oddělená od ostatních subjektů (LAN, MAN sítí, Internetu, případně sítí externích subjektů). RDS bude začleněna do stávajícího řízení informační bezpečnosti Krajského úřadu.

Na konečnou volbu aktivních prvků v rámci rozšiřování sítě, ale hlavně na celkový design má vliv komunikační model, podle kterého bude provoz v infrastruktuře řízen. Také určuje datové toky v rámci tzv. perimetru a jeho komunikaci do externích sítí, jako je Internet, a také naopak. Z pohledu regionální sítě Pardubického kraje je i LAN síť chápána jako externí síť. Uvnitř MAN sítě (RDS) v případě řešení pomocí protokolu MPLS se jedná o rozdělení provozu do jednotlivých oddělených segmentů tzv. VPN (VRF) a jejich forma distribuce a řízení přístupu k nim.

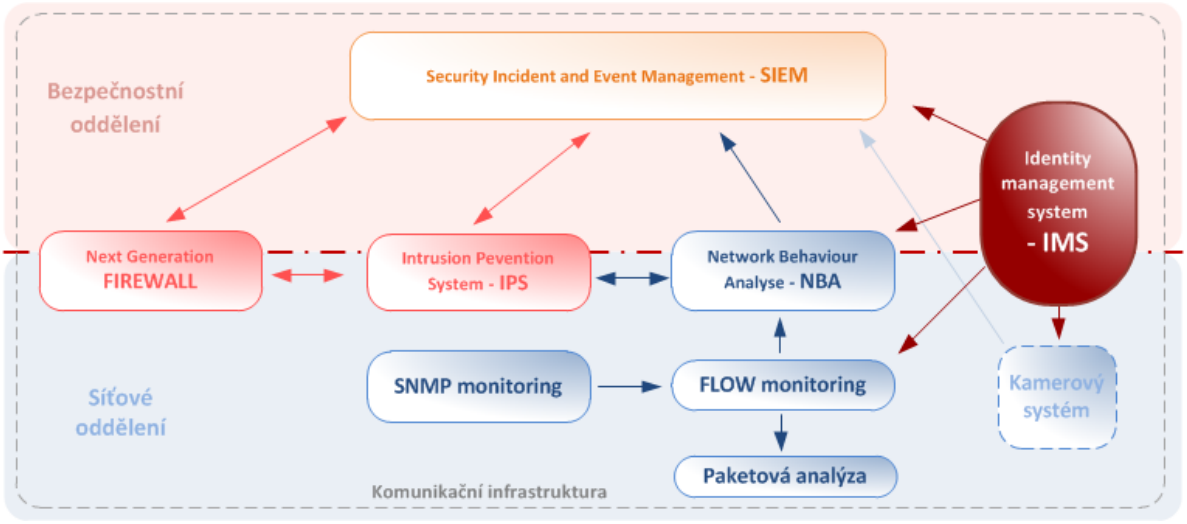
Uvedený komunikační model má za úkol demonstrovat princip abstrakce od aktivních prvků směrem k „bezpečnostním oblastem“. Důležité je identifikovat oblasti s různou bezpečnostní povahou a ty následně zahrnout do komunikačního modelu. Následně se doplní potřebné komunikační kanály mezi oblastmi. Samotné technické řešení propojení je již následně triviální záležitostí.

Následující obrázek znázorňuje návrh, jak by takový komunikační model mohl vypadat.



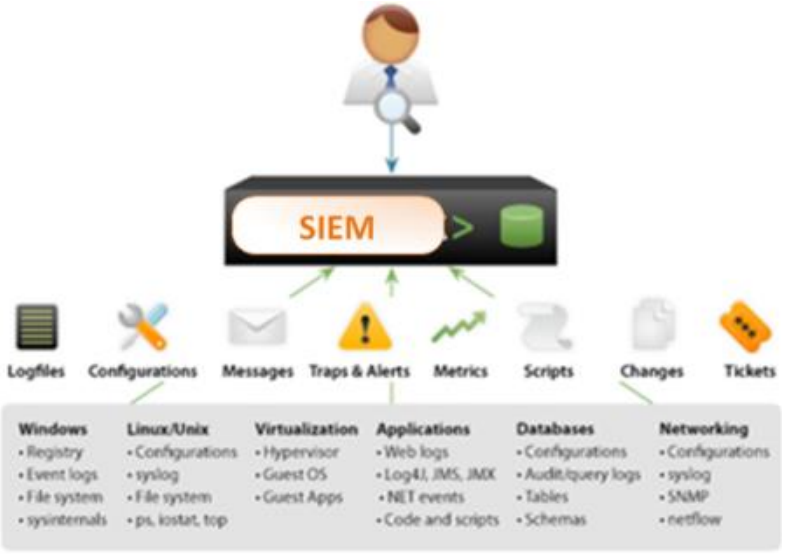
20.5.2 Bezpečnostní model

Na komunikační model navazuje bezpečnostní model, který se na infrastrukturu dívá z pohledu vynucování bezpečnosti, auditu a dohledu bezpečnosti. V rámci řízení informační bezpečnosti musí být stanoveny, které z uvedených částí bezpečnostního modelu musí být implementovány a v jaké formě. Jedná se o následující stavební bloky (včetně organizačního přiřazení):



Základní kameny koncepce se pohybují v úrovních monitoringu (modré) a také exekuce (červené), přičemž klíčovou roli hraje jednoznačná identifikace identity, která je propojovacím prvkem mezi kompetencemi síťového oddělení a bezpečnostního oddělení subjektů. Mnohdy bývají role bezpečnostního oddělení kompletně přeneseny do oddělení síťového.

Zastřešujícím elementem je systém SIEM. (Security Incident and Event Management) který, sbírá a indexuje tzv. „strojová data“ z jiných systémů a provádí jejich korelaci a vyhodnocení do formy konsolidovaných událostí a incidentů.



20.6 Koncept zabezpečení komunikační infrastruktury a koncových lokalit

Koncept zabezpečení komunikační infrastruktury a koncových lokalit podává dokument bezpečnostní dokumentace, převážně kapitola 4.

20.7 Koncept koordinace rozvojových aktivit komunikační infrastruktury na regionální úrovni

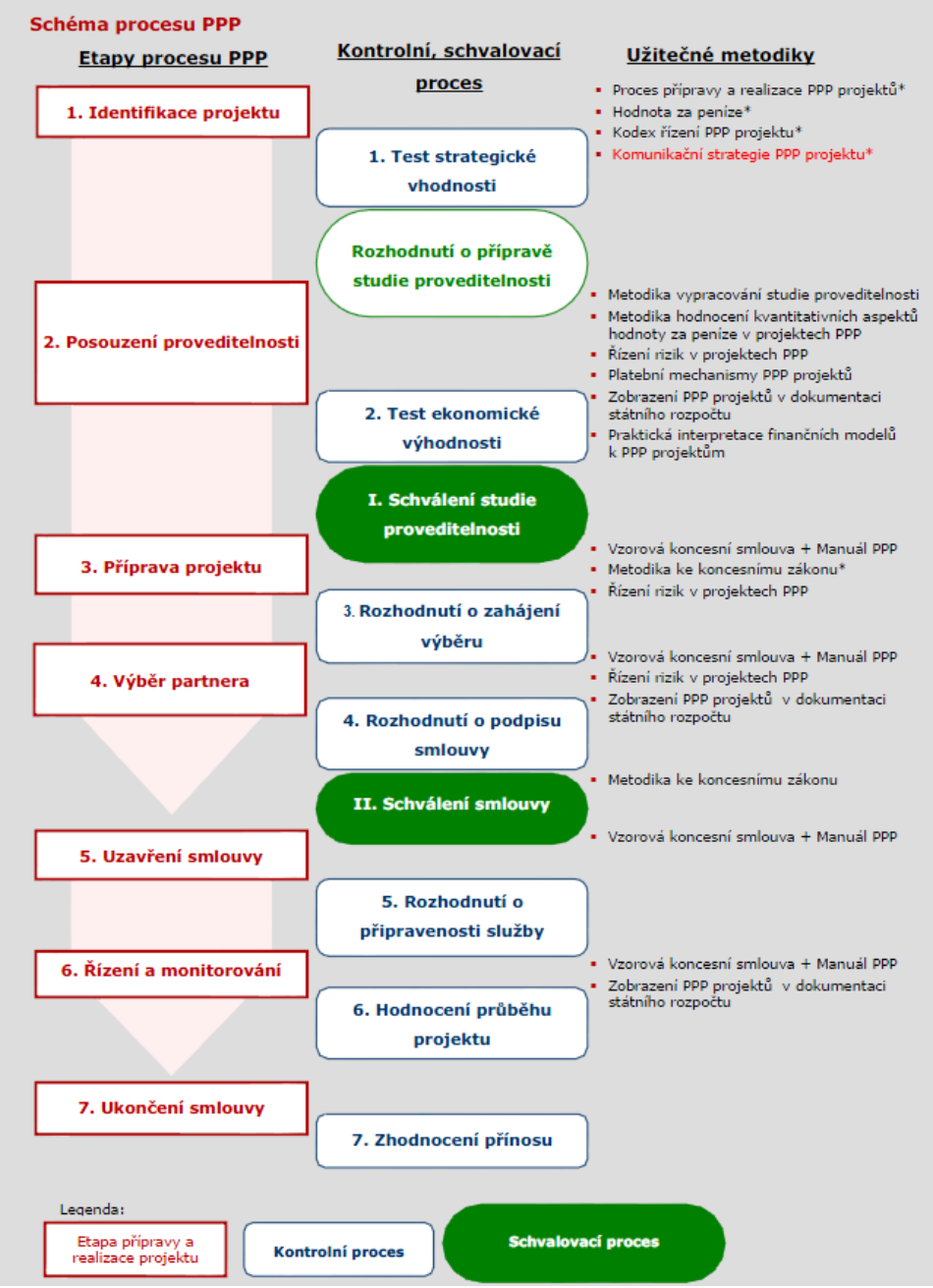
20.7.1 Výstavba optických tras

Pro připojování dalších subjektů do regionální stě Pardubického kraje bude nutné další rozšiřování optických tras. Vzhledem k optimalizaci nákladů, je doporučeno použít prioritně jiné než přímé metody financování. Jako jedny z možných se jeví:

- trasy pořízené formou PPP
- výstavba NGA/OAN sítí

20.7.2 PPP financování

Postup výstavby PPP sítí probíhá obvykle v následujících krocích:



Praxe ani předpisy žádné země, ve které je rozvinutý trh PPP projektu, pojem „PPP“ ani žádný obdobný pojem přesně nedefinují. Obvykle se však v praxi pod pojmem PPP míní projekty, které mají následující charakteristiky (či alespoň některé z nich):

- Zadavatel přenáší na soukromého partnera (dále také „koncesionář“) odpovědnost a rizika, která by v tradiční formě zajištění infrastruktury či služeb nesl sám (např. riziko vyšších nákladu či zpoždění výstavby či riziko malé poptávky po příslušných službách). Je budována infrastruktura, obvykle hmotná, avšak jsou známy i projekty, které spočívají v zajištění služeb,

jejichž těžiště je například v zajištění dodávek tepla, vody, školního stravování, provozu sportovních areálu apod.

- Náklady projektu spočívají nejen v nákladech výstavby (a poskytování služeb), ale i v postupné výměně a údržbě jednotlivých částí infrastruktury během „života“ projektu a zajištění provozu této infrastruktury (tzv. celoživotní náklady).
- Koncesionář vybudování infrastruktury sám financuje (obvykle z větší části úvěrem) a náklady na vybudování infrastruktury jsou nepřímo „spláceny“ během trvání smlouvy v platbách placených veřejným sektorem a/nebo uživatelem služeb v delším období, jsou však známy i projekty, ve kterých většinu nákladu na vybudování infrastruktury financuje veřejný sektor přímo již po vybudování infrastruktury. Stejně tak je možné využít kombinaci financování veřejného a soukromého sektoru, popř. využití různých typu dotací při zachování podmínek pro poskytování těchto dotací (např. strukturální fondy EU)
- Financování soukromého koncesionáře, kterým je obvykle společnost účelově založená pouze pro konkrétní projekt (tzv. SPV – Special Purpose Vehicle neboli zvláštní účelová společnost) má formu tzv. projektového financování, založeného pouze na peněžních tocích koncesionáře plynoucích z koncesní smlouvy, bez rekursu (nároku) vůči koncesionářovým akcionářům. Institut SPV je využíván zejména u velkých (investičně náročných) PPP projektu.

Nejlepší praxe a hodnota za peníze

Nejlepší praxí je míněn obecně souhrn poznatku a postupu používaných úspěšnými zadavateli při realizaci úspěšných projektu, které dosahují hodnoty za peníze (viz níže). Nejde o žádný uzavřený ani závazný seznam pravidel, nýbrž o jakýsi ekvivalent pojmu „odborná péče“ či postup „lege artis“, který čerpá z předchozích zkušeností zadavatelových předchůdců v České republice i v zahraničí. Hodnota za peníze je nejdůležitějším pojmem PPP projektu. Znamená, že veřejný sektor získává nejvyšší možnou a současně využitelnou hodnotu za utrácené veřejné prostředky. Pokud PPP projektem zadavatel nerealizuje „hodnotu za peníze“ ve srovnání s tradičním způsobem zadání projektu, neměl by být projekt realizován formou PPP2, nýbrž tzv. tradičním způsobem. Hodnotou za peníze je míněno dosažení stavu, kdy zadavatel za veřejné prostředky získává nejvyšší protihodnotu, kterou reálně získat může a kterou dosahuje přínosu pro veřejný sektor. Byt by zadavatel prokazatelně nakupoval službu za nejvýhodnějších podmínek, pokud nakupuje službu, která není potřeba či v kvalitě, která není potřeba, nerealizuje hodnotu za peníze. V kontextu PPP projektu to např. znamená, že i když jsou uchazeči ve výběrovém řízení ochotni se zavázat k určitým hodnotným závazkům (např. extrémně krátká doba zásahu při poruše zařízení či vybavení, která nepřináší zadavateli dodatečný užitek), jsou takové závazky vykupovány vyšší cenou. Zadavatel nerealizuje hodnotu za peníze, pokud je přidaná hodnota takového závazku nižší, než jakou činí odpovídající zvýšení ceny. Vedle toho zadavatel hodnotu za peníze obtížně dosáhne i prokáže, pokud nebude zadání projektu provedeno otevřeným a transparentním výběrovým řízením, či pokud v takovém výběrovém řízení nebude dostatečně intenzivní reálná konkurence (což je např. problém, který musí zadavatelé řešit v souvislosti se změnami projektu, jež v budoucnosti mohou být často prakticky realizovány pouze koncesionářem, který příslušné zařízení vybudoval a dlouhodobě je provozuje). Více o problematice hodnoty za peníze viz metodika „Hodnota za peníze“ nebo „Metodika hodnocení kvantitativních aspektu hodnoty za peníze v projektech PPP“ – www.mfcr.cz.

Rozdíl mezi PPP a tradičním způsobem pořizování infrastruktury a služeb

PPP je obecným odborným, nikoliv zákonným, pojmem pro určitý okruh projektu s určitými

vlastnostmi (viz výše). Ministerstvo financí nepovažuje pro aplikaci principu uvedených v tomto dokumentu a pro aplikaci rozpočtového dozoru podle KZ za rozhodné, zda je projekt označován jako PPP či nikoliv, nýbrž jeho finanční význam. Pokud projekt představuje významný dlouhodobý závazek zadavatele, doporučuje Ministerstvo financí, aby zadavatel respektoval doporučení uvedená v tomto manuálu a ve vzorové koncesní smlouvě. Současně, pokud projekt realizovaný územním samosprávným celkem splňuje parametry §30 KZ, bude předmětem rozpočtového dozoru Ministerstva financí, bez ohledu na to, zda je za PPP označován či nikoliv.

20.7.3 Výstavba NGA/OAN metodou

Jedná se o formu výstavby, při které se uplatňuje princip sdílení investičních nákladů mezi více subjektů. V tomto případě pravděpodobně mezi Pardubický kraj a komerční společnost. Další možností je poskytnutí infrastruktury Pardubického kraje jako velkoobchodní komoditu širšímu spektru poskytovatelů. Příjmy z této formy lze následně použít pro údržbu a rozvoj regionální sítě.

Legislativa

V současné době je možné obecně ukládat povinnosti týkající se přístupu pouze podniku s významnou tržní silou na relevantním trhu. Výjimku tvoří povinnost poskytovat společné umístění nebo jiné formy sdílení prostředků, například sdílení kabelovodů, objektů nebo stožárů, kdy z taxativně vymezených důvodů lze tuto povinnost uložit i podniku, který nemá na relevantním trhu významnou tržní sílu podle § 84 odst. 3. zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (dále jen „ZEK"). V rámci novely ZEK, která nabyla účinnosti 1. 7. 2010, je možno uložit (podle § 79 odst. 2 písm. a) zpřístupnění prostředků nebo služeb podnikatelům ovládajícím přístup ke koncovým uživatelům. Avšak podle revize předpisového rámce pro sítě a služby elektronických komunikací, Směrnice Evropského parlamentu a Rady 2009/140/ES ze dne 25. listopadu 2009, kterou se mění směrnice 2002/21/ES o společném předpisovém rámci pro sítě a služby elektronických komunikací, směrnice 2002/19/ES o přístupu k sítím elektronických komunikací a přiřazeným zařízením a o jejich vzájemném propojení a směrnice 2002/20/ES o oprávnění pro sítě a služby elektronických komunikací (tzv. směrnice o lepší regulaci), se možnost uložit sdílení vnitřních rozvodů či kabelových tras předpokládá (viz upravený článek 12 rámcové směrnice 2002/21/ES) ve větším rozsahu.

Technicky připadají v úvahu následující formy výstavby, které mohou být komerčně zajímavé pro soukromé subjekty a mohou tudíž podpořit spoluúčast na investičních nákladech společného projektu:

FTTH (Fibre to the Home)

Prvním scénářem výstavby NGA sítí je scénář FTTH, ve kterém je výhradně uplatněna technologie optických vláken až ke koncovému uživateli. Výstavba přístupových sítí NGA podle tohoto scénáře se zpravidla uplatňuje při nové výstavbě („na zelené louce"), v ostatních případech vyžaduje výměnu stávajících kovových vedení za optická. Scénář FTTH může být realizován jako point-to-point (PtP, P2P). V tomto případě má každý uživatel vyhrazeno jedno optické vlákno, které vede od uživatele až do optického rozvaděče ODF (optical distribution frame), který tvoří hranici mezi přístupovou a páteřní sítí. Druhou možností je řešení typu point-to-multipoint (PtMP, P2MP) realizované pasivní optickou

sítí PON (passive optical network). Zde je provoz veden z ODF jedním vláknem do pasivního koncentrátoru (splitter) a odtud samostatným optickým vláknem k jednotlivým koncovým uživatelům.

FTTB (Fibre to the Building)

Druhou základní variantou je scénář FTTB. V tomto scénáři je optické vlákno přivedeno až k budově nebo do budovy a odtud až ke koncovému uživateli jsou využity vnitřní kovové rozvody.

FTTCab (Fibre to the Cabinet)

Třetí scénář FTTCab spočívá v současném využití jak optického, tak kovového vedení v přístupové síti. Od páteřní sítě z ODF ke kabinetu/rozvaděči vedou optická vlákna a od kabinetu/rozvaděče ke koncovému uživateli se využije již instalované kovové vedení. Tento scénář je zejména vhodný pro fázi výstavby NGA sítí, kdy budou postupně nahrazovány jednotlivé stávající úseky kovových vedení optickým vedením.

20.8 Koncept koordinace složek IZS a krizového řízení

Tento integrovaný systém doporučujeme provozovat v plně redundantním módu v zabezpečeném prostředí datových center. Regionální síť Pardubického kraje je možné efektivně využít jako prostředku k zabezpečené výměně informací tohoto systému a jejím prostřednictvím předávat data v systému začleněným uživatelům a organizacím.

20.9 Koncept zajištění provozu a správy služeb komunikační infrastruktury

Vzhledem k rozsahu a odlišné povaze jednotlivých projektů v rámci regionální sítě, není vhodné, aby interní IT oddělení Pardubického krajského úřadu kompetenčně pokrývalo všechny aspekty. Dlouhodobě se ukazuje jako nejvhodnější model, kdy má krajský úřad jediného partnera pro zajištění správy a provozu celé infrastruktury (servisní organizaci). Servisní organizace následně svými silami nebo kontraktory zajišťuje provoz dílčích částí. Garance funkčností a dodržení SLA je vůči krajskému úřadu v Pardubicích řešena pouze mezi dvěma stranami.

Existuje také varianta, kdy výběr servisní organizace není předmětem veřejné soutěže, ale organizace je přímo založena městem. Ekonomicky tato varianta neposkytuje odpovídající výhody, jelikož pro město vznikají náklady se založením organizace a vyšší jsou také provozní náklady (organizace není motivována tržně). V tomto případě také nelze v případě potřeby změnit dodavatele služeb. Nespornou výhodou však, že veškerá kontrola nad provozem infrastruktury zůstává blíže ke krajskému úřadu.

20.10 Možnosti připojení dalších systémů

20.10.1 Disaster Recovery pro zřizované organizace

Vzhledem k současným schopnostem virtualizačních serverových nástrojů a k nasazení MPLS L2 VPN v komunikační infrastruktuře, je možné sdílení výpočetního výkonu mezi prostředím Pardubického kraje a zřizovanými organizacemi. Je tudíž možné „přesouvat“ virtualizované servery mezi organizacemi a datovými centry, aniž by koncoví uživatelé zpozorovali jakékoli omezení provozu. Tento scénář lze využít pro:

1. **konsolidaci infrastruktury** – lze omezit investice do infrastruktury zřizovaných organizací a využít infrastruktury Pardubického kraje. Toto řešení se jeví jako dlouhodobě ekonomicky nejvýhodnější.
2. **Distaster Recovery** – v tomto případě slouží infrastruktura Pardubického kraje jen jako záložní lokalita, kdy v případě výpadku infrastruktury zřizované organizace dochází k nastartování serverů v prostředí datových center.

20.10.2 Distribuované diskové úložiště

Díky využití diskové virtualizace, lze dosáhnout stejné míry přínosů, jako v případě serverové virtualizace. Lze tak vytvořit distribuované diskové úložiště mezi jednotlivými lokalitami a organizacemi připojenými regionální sítí. V tomto případě je však důležité koncepčně zvládnout úvodní analytickou část. Je podstatné správné navržení diskových kapacit, způsobů replikací a celého životního cyklu dat. Pozitivní rysem diskové virtualizace je otevřenost vůči klientským systémům (díky využití standardizovaného protokolu iSCSI a běžné ethernetové komunikace). Neklade tak žádné specifické požadavky na infrastrukturu zapojených subjektů.