



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

**NÁVRH MIGRACE ČÁSTI ICT INFRASTRUKTURY
DO DATOVÉHO CENTRA**

DESIGN OF PART OF ICT INFRASTRUCTURE MIGRATION TO THE DATA CENTER

DIPLOMOVÁ PRÁCE

MASTER'S THESIS

AUTOR PRÁCE

AUTHOR

Bc. Iveta Kočíbová

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Viktor Ondrák, Ph.D.

BRNO 2016

ZADÁNÍ DIPLOMOVÉ PRÁCE

Kočíbová Iveta, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Návrh migrace části ICT infrastruktury do datového centra

v anglickém jazyce:

Design of Part of ICT Infrastructure Migration to the Data Center

Pokyny pro vypracování:

Úvod

Cíle práce, metody a postupy zpracování

Teoretická východiska práce

Analýza současného stavu

Vlastní návrhy řešení

Závěr

Seznam použité literatury

Přílohy

Seznam odborné literatury:

DOLEŽAL, J., P. MÁCHAL a B. LACKO. Projektový management podle IPMA. 2., aktualiz. a dopl. vyd. Praha: Grada, 2012. ISBN 978-80-247-4275-5.

JOSYULA, V., M. ORR a G. PAGE. Cloud computing: automating the virtualized data center. Indianapolis: Cisco Press, 2012. ISBN 978-1-58720-434-0.

LOWE, S. Mistrovství ve VMware vSphere 5: Kompletní průvodce profesionální virtualizací. Brno: Computer Press, 2013. ISBN 978-80-251-3774-1.

SCHWALBE, K. Řízení projektů v IT: kompletní průvodce. 1. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-2882-4.

VELTE, A. T., T. J. VELTE a R. ELSENPETER. Cloud computing: praktický průvodce. 1. vyd. Brno: Computer Press, 2011. ISBN 978-80-251-3333-0.

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2015/2016.

L.S.

doc. RNDr. Bedřich Půža, CSc.
Ředitel ústavu

doc. Ing. et Ing. Stanislav Škapa, Ph.D.
Děkan fakulty

V Brně, dne 29.2.2016

Abstrakt

Tato Diplomová práce se zabývá návrhem migrace části ICT infrastruktury dvou lokalit mezinárodní společnosti do externího datového centra. Analyzuje současný stav ICT společnosti, popisuje virtualizační infrastrukturu a náklady na její provoz. Hlavní část práce popisuje možné řešení migrace virtualizační infrastruktury do externího datového centra s využitím nástrojů a metod projektového řízení. Závěrem jsou uvedeny přínosy projektu pro společnost.

Abstract

This Master Thesis deals with the design of part of ICT infrastructure migration of two sites of the international company to the external data center. It analyzes the current status of company ICT, describes the virtualization infrastructure and its operational costs. Main part of the Thesis describes a possible solution of migration of virtualization infrastructure to external data center by using project management tools and methods. Finally, the Thesis summarizes project benefits for the company.

Klíčová slova

virtualizace, migrace, rack housing, serverhosting, outsourcing, datové centrum, cloud computing, projektové řízení, TIER, MPLS, TCO, ICT, VMware, ESXi

Keywords

virtualization, migration, rack housing, serverhosting, outsourcing, data center, cloud computing, project management, TIER, MPLS, TCO, ICT, VMware, ESXi

Bibliografická citace

KOČÍBOVÁ, I. *Návrh migrace části ICT infrastruktury do datového centra*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2016. 89 s. Vedoucí diplomové práce Ing. Viktor Ondrák, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená diplomová práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu Zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 1. června 2016

.....

Iveta Kočíbová

Poděkování

Ráda bych poděkovala všem, kteří mi poskytli radu při tvorbě této práce, zejména pak jejímu vedoucímu panu Ing. Viktorovi Ondrákovi, Ph.D.

Dále bych ráda poděkovala společnosti Dust CR, s.r.o. za poskytnutí prostoru a zázemí, bez něhož by tato práce nemohla vzniknout.

Největší dík patří mé rodině, která pro mne byla velkou inspirací a oporou po celou dobu mých studií.

OBSAH

ÚVOD.....	10
CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ.....	11
1 TEORETICKÁ VÝCHODISKA PRÁCE.....	12
1.1 Virtualizace.....	12
1.2 Outsourcing	15
1.2.1 Definice outsourcingu	15
1.2.2 Varianty outsourcingu	16
1.2.3 Důvody, výhody a nevýhody outsourcingu	16
1.3 Cloud computing.....	20
1.3.1 Umístění ICT infrastruktury	21
1.3.2 Modely nasazení cloud computingu.....	21
1.3.3 Distribuční modely cloud computingu	24
1.3.4 Výhody cloud computingu.....	24
1.3.5 Nevýhody cloud computingu	25
1.3.6 Bezpečnost v cloudu.....	25
1.3.7 Smluvní úprava odpovědnosti za ztrátu dat v cloudu.....	27
1.3.8 ISMS a cloud computing	27
1.4 Serverhosting	29
1.4.1 Varianty serverhostingu.....	30
1.4.2 IP Konektivita	31
1.5 Datové centrum.....	31
1.5.1 Klasifikace datových center dle TIER.....	32
1.6 SLA	34
1.7 Poměr cena/kvalita/přidaná hodnota.....	35
1.8 Projektové řízení	36
1.8.1 Definice projektu.....	36
1.8.2 Trojimperativ projektu.....	37
1.8.3 Znalostní oblasti projektového řízení	37
1.8.4 Fáze řízení projektu	38
1.8.5 Projektové procesy	41
1.8.6 Nástroje projektového řízení.....	41

2	ANALÝZA SOUČASNÉHO STAVU	42
2.1	Základní informace o společnosti	42
2.2	Strategie IT	43
2.3	ICT infrastruktura	44
2.3.1	Virtualizační infrastruktura	45
2.4	Analýza nákladů virtualizační infrastruktury	48
2.5	Současný stav serverových místností.....	50
2.5.1	Náklady na rekonstrukci serveroven	51
2.6	Shrnutí analýzy	51
3	VLASTNÍ NÁVRHY ŘEŠENÍ	52
3.1	Plán projektu.....	52
3.2	Studie proveditelnosti.....	53
3.2.1	Upřesnění cíle projektu:.....	53
3.2.2	Organizační struktura projektu:.....	53
3.2.3	Určení hardware k migraci do DC	54
3.2.4	Stanovení rychlosti připojení	55
3.2.5	Analýza zainteresovaných stran.....	55
3.2.6	Analýza rizik	58
3.2.7	Rozpočet projektu	62
3.3	Shrnutí studie proveditelnosti	63
3.4	Projektová fáze	63
3.4.1	Zahájení	63
3.4.2	Plánování	63
3.4.3	Realizace a ukončení	75
3.5	Shrnutí projektové fáze	76
3.6	Poprojektová fáze.....	76
3.6.1	Uložení projektové dokumentace a uzavření projektu	76
3.6.2	Přínosy migrace ICT infrastruktury do DC	76
	ZÁVĚR.....	81
	SEZNAM POUŽITÉ LITERATURY	82
	SEZNAM OBRÁZKŮ	87
	SEZNAM TABULEK	88
	SEZNAM GRAFŮ	89
	SEZNAM PŘÍLOH	89

ÚVOD

Tato diplomová práce je vytvořena pro účely společnosti Dust CR, s.r.o. a slouží jako návrh řešení migrace virtualizační ICT infrastruktury podniku do externího datového centra. Tato práce by měla sloužit jako základ pro možný způsob realizace projektu dle přístupů projektové řízení, a to i pro společnosti s podobným charakterem ICT infrastruktury.

Protože v této práci nechci uvádět skutečné názvy subjektů, z důvodu jejich ochrany a možného vyjádření citlivých nebo strategických informací, vystupují zde tyto subjekty pod pseudonymem. Jméno podniku, pro který je tato práce zpracována, uvádím pod fiktivním názvem Dust CR, s.r.o. Poskytovatelé ve výběrovém řízení jsou označeni jako poskytovatel A a poskytovatel B.

Pro téma této práce jsem se rozhodla z důvodu moderního pojetí řízení a rozvoje ICT, jakou outsourcing ICT v datovém centru zcela jistě je. Je to směr, kterým se v dnešní době vydává stále více společností, jelikož si uvědomují jeho nesporné benefity, které, pokud je řešení vhodně uchopeno, převyšují jeho nevýhody a rizika. Tento projekt se mi zamlouval i z toho důvodu, že pomůže společnosti s její současnou situací a posune koncept řízení a rozvoje ICT na vyšší úroveň. Má tedy reálné využití a dopady v praxi.

V této společnosti pracuji již delší dobu, proto jsem vcelku dobře seznámena s fungováním, vztahy a strategií podniku. Společnost se chce neustále zlepšovat a rozvíjet, sleduje trendy rozvoje IT. Proto je outsourcing části ICT rozumným strategickým rozhodnutím a já jsem velmi ráda, že můžu být součástí tohoto projektu, neboť mne přinesl, a zajisté ještě přinese cenné zkušenosti v oblasti IT i projektového managementu.

CÍLE PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem této práce je navrhnout migraci části ICT infrastruktury společnosti Dust CR, s.r.o. do datového centra.

Celý návrh je koncipován jako projekt, proto se tato práce obsahově a strukturálně přibližuje rozdělení projektu na předprojektovou, projektovou a poprojektovou fázi. Předprojektová fáze obsahuje nezbytné analýzy naplňující obsahově studii příležitosti a proveditelnosti. Analyzuji současný stav virtualizační ICT infrastruktury, zatížení sítě, a provozní náklady na infrastrukturu. Dále provádím výběr hardware, který se bude do datového centra přesouvat, analýzu zainteresovaných stran a analýzu rizik projektu. Na tyto analýzy v projektové fázi navazuje stanovení požadavků na poskytovatele služeb datového centra. Tyto požadavky vstupují jako výběrová kritéria do výběrového řízení na poskytovatele, kdy objektivním způsobem vyhodnotím nabídky poskytovatelů na rack housing a budu se snažit pro společnost Dust CR vybrat tu, která nejvíce vyhovuje stanoveným požadavkům. Dále navrhuji plán samotné migrace, který obsahuje návrh WAN sítě, logiku zapojení zařízení v DC, způsob migrace hardware a dat a možnou variantu rozdělení virtuálních serverů na hostitele. V poprojektové fázi jsou zhodnoceny přínosy projektu pro společnost, které jsou založeny především na kvalitativních výhodách.

Teoretické informace, ze kterých budu při návrhu řešení vycházet, budu čerpat z odborných informačních zdrojů. Rovněž využiji poznatků a znalostí získaných během mého studia na této škole a uplatním je v praxi.

Výsledkem této práce by mělo být takové řešení, které by bylo realizovatelné, mělo by společností Dust CR zajistit vysokou dostupnost ICT infrastruktury a zvýšit její provozní úroveň.

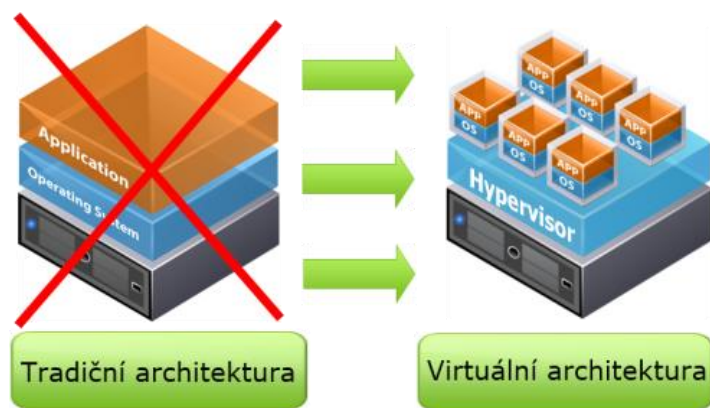
1 TEORETICKÁ VÝCHODISKA PRÁCE

V této kapitole se budu věnovat oblastem, které souvisejí s virtualizací, outsourcingem, cloud computingem a datovými centry. Popíšu výhody, nevýhody a také problematiku týkající se bezpečnosti takto koncipovaného řešení ICT. Dále uvedu možný způsob, jak nahlížet na zhodnocení investic do ICT, zaměřím se na TCO a nahlížení na přínosy z pohledu ceny, kvality a přidané hodnoty. Poslední část této kapitoly obsahuje základy projektového řízení při řízení projektů obecně, nejenom v IT.

1.1 Virtualizace

Virtualizace zásadně mění způsob provozování IT a zvyšuje efektivitu dostupných technologií. Je to technologie, která prostřednictvím virtualizačního software (*hypervisor*) umožňuje provozovat více operačních systémů na stejném fyzickém stroji současně. Tím vznikají virtuální stroje (*VM*), v terminologii virtualizace hosté (*guest*), které jsou zcela soběstačné a navenek působí jako samostatné stroje. Tito hosté jsou hostováni na fyzickém serveru – hostiteli (*host*). Virtuální stroje využívají přidělenou výpočetní kapacitu hostitele a jeho systémové prostředky – paměť, čas procesoru, kapacitu úložiště, apod. (1, 2).

Při virtualizaci se o vše stará hypervisor – hostitelský operační systém, který je umístěn na hostiteli, tedy na fyzickém stroji. Jeho hlavní funkcí je oddělit výpočetní prostředí hostitele a poskytovat jej virtuálním strojům, dále spravovat přístup mezi operačním systémem hosta, který běží na virtuálních strojích a hardwarovou vrstvou fyzického počítače (3). Hypervisor tedy díky separaci výpočetních prostředků stroje může sdílet a přidělovat kapacitu těchto prostředků vícero virtuálním strojům. Vytvoří iluzi, kde jsou výpočetní zdroje rozmnoženy v podobě kopií prostředků. Vznikají tak virtuální objekty – virtuální paměť (*vRAM*), virtuální procesor (*vCPU*), virtuální disk (např. *VHD*), virtuální síťová karta (*vNIC*) atd. Každý virtuální stroj se tedy sestává z přidělených virtuálních objektů mající požadovanou kapacitu. Virtuální stroje se vzájemně neovlivňují, „nevidí na sebe“ a v případě pádu některého z nich, není ovlivněn chod ostatních. Uživatelé mají v konečném důsledku pocit, že pracují se skutečným fyzickým strojem a nejsou virtualizací nijak negativně uživatelsky ovlivněni (2, 4, 5). Srovnání tradiční a virtuální architektury je znázorněn na obrázku č. 1.



Obrázek č. 1: Srovnání tradiční a virtuální architektury - upraveno (6)

Hypervisor hospodaří se svěřenými prostředky fyzického stroje tak, aby byl celý systém co nejefektivněji využíván. V důsledku virtualizace dochází ke snižování nákladů, a to jak provozních (OPEX) tak investičních (CAPEX), ke zjednodušení infrastruktury, správě a údržbě zařízení, ke zvýšení dostupnosti, spolehlivosti a flexibility (7, 8).

Virtualizovat lze v dnešní době téměř cokoliv. Můžeme se tak setkat například s:

- virtualizací serverů,
- virtualizací sítí,
- virtualizací úložiště,
- virtualizací aplikací,
- virtualizací pracovních ploch (1).

Virtualizace serverů

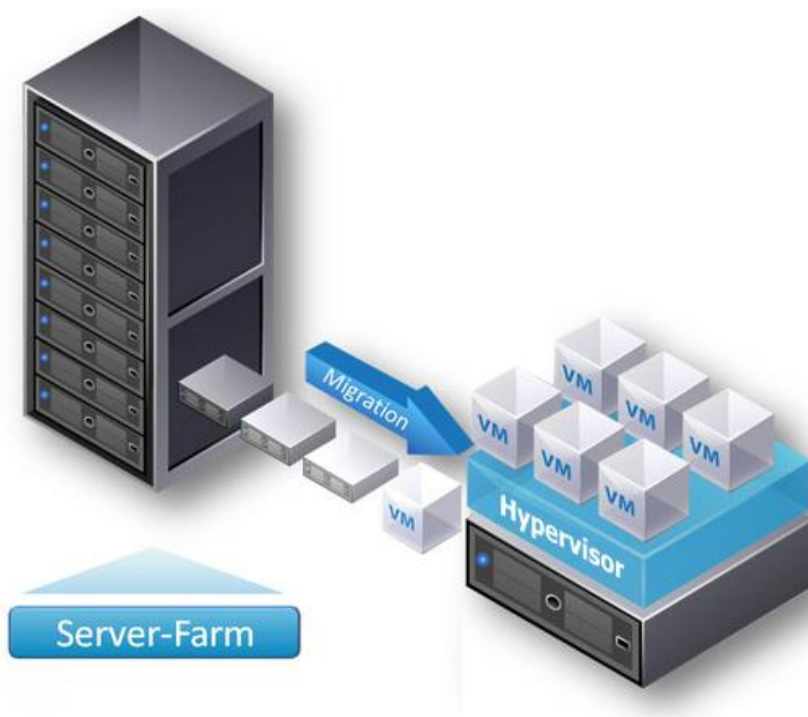
Význam a smysl virtualizace se nejvíce projevuje v řešení virtualizace serverů. Je to z toho důvodu, že servery jsou často naddimenzovány, co se týče kapacity a výkonu hardware, a tyto zdroje jsou nedostatečně nebo neefektivně využívány - hw je obvykle využíván na méně než na 15 % (1, 2).

Jelikož virtualizace umožňuje na jednom fyzickém stroji provozovat více virtuálních strojů, lze tedy využít jeden dostatečně dimenzovaný fyzický server a spouštět na něm několik virtuálních serverů. O přerozdělování výpočetního výkonu fyzického serveru virtuálním serverům se stará hypervisor, který tuto kapacitu zdrojů poskytuje jednotlivým VM na základě jejich aktuální vytiženosti a potřeb. Pokud máme k dispozici více

hostitelů, může hypervisor v případě přetížení jednoho z nich přesunout některé virtuální stroje na jiný fyzický stroj – na jiného hostitele, který je méně vytížen. Jelikož jsou virtuální disky virtuálních strojů tvořeny soubory se specifickou příponou dle použité virtualizační platformy (např. vhdx, vmdk, vdi), je přesun takového virtuálního stroje velmi jednoduchý. Přesun z jednoho hostitele na jiný je záležitostí několika minut, záleží však na propustnosti a rychlosti sítě (2).

Virtualizace serverů tedy zvyšuje efektivitu využití kapacity fyzických serverů, dále zjednodušuje infrastrukturu, správu a snižuje náklady na údržbu. Dochází k velké úspoře časových nároků na správu a rozšiřování této virtualizační infrastruktury (2, 9).

Následující obrázek č. 2 znázorňuje princip virtualizace serverů.



Obrázek č. 2: Schéma virtualizace serverů – upraveno (10)

1.2 Outsourcing

V této kapitole se věnuji vysvětlení pojmu outsourcing, uvádím jeho možné varianty, výhody, nevýhody a důvody proč se pro outsourcing rozhodnout. Kapitola obsahuje i informace získané z dotazníkového průzkumu na téma outsourcing.

1.2.1 Definice outsourcingu

Obecně pod pojmem outsourcing chápeme formu externího obstarávání činností, které původně podnik zajišťoval vlastními silami. Jedná se o zajištění vnitropodnikových aktivit, které nejsou pro organizaci klíčové, jiným subjektem, pro něhož naopak klíčové jsou. Procesy a aktivity podniku zajišťuje externí poskytovatel, kdy je smluvně stanovena délka a předmět poskytování outsourcingu (11, 12, 13).

Outsourcing je vnímán jako dodávka služby, kdy poskytovatel je v roli garanta za stanovenou oblast, je za ni smluvně odpovědný, udržuje ji na požadované technologické úrovni a patřičným způsobem pracuje na jejím neustálém zlepšování (13). Z hlediska IT se jedná o částečné nebo i kompletní odklonění ICT infrastruktury z interního prostředí podniku, kde její provoz zajišťuje specializovaná společnost. Díky outsourcingu nemusí podnik vynakládat prostředky na pořízení majetku či personálních zdrojů a může je investovat efektivněji jinak (11).

Tento model však vyžaduje adekvátní nabídku na straně dodavatele, ale i přístup zákazníka, který musí být založen na celopodnikové a z ní vycházející informační strategii firmy. Zákazník musí vědět, co je jeho core business, tedy na co primárně soustředí své zdroje a co považuje za klíčové oblasti svého podnikání. Dále by zákazník měl vědět, které oblasti, činnosti či procesy je vhodné přenechat specializovaným dodavatelům na danou problematiku. Častou chybou je nevhodně zvolený proces pro outsourcing. Zákazník musí mít proces dostatečně popsáný, jinak nelze zajistit, že poskytovatel zajistí dodávku procesu v požadovaném rozsahu a kvalitě. Aby nedošlo mezi oběma stranami smluvního vztahu k nedorozumění z hlediska očekávání, je nutné definovat požadavky na rozsah a kvalitu poskytovaného procesu, typicky ve formě SLA, která specifikuje úroveň poskytované služby. Také nesmíme opomenout stanovit vhodný způsob, jakým budeme řídit rizika týkající se bezpečnosti a rizika vycházející ze závislosti na poskytovateli služby (12).

1.2.2 Varianty outsourcingu

Obecně můžeme definovat následující varianty outsourcingu:

- a) **Outsourcing vybraného procesu** – dodavatel přebírá odpovědnost jen za určitou oblast či proces, který pro zákazníka není efektivní zajišťovat interně, typicky se jedná o podpůrný proces – účetnictví, HR, atd.
- b) **Outsourcing kompletního IS/ICT** – veškerý provoz a chod ICT oddělení, včetně personálních zdrojů, je odsunut na dodavatele.
- c) **Částečný outsourcing IS/ICT** – selektivní outsourcing - outtasking
 - informatického procesu - vývoje, implementace ERP, integrace IS/ICT,
 - informatické služby (aplikační outsourcing) – dodavatel zajišťuje provoz konkrétní aplikace či IS, typicky ve formě SaaS (CRM, el. pošta),
 - informatického zdroje (technologický outsourcing) – dodavatel zajišťuje technologické zázemí pro podnikové IT, typicky ve formě PaaS, IaaS (datové centrum, LAN/WAN, koncové stanice).
- d) **Personální outsourcing** – dodavatel poskytuje po smluvenou dobu kapacitu zaměstnance (12, 14).

1.2.3 Důvody, výhody a nevýhody outsourcingu

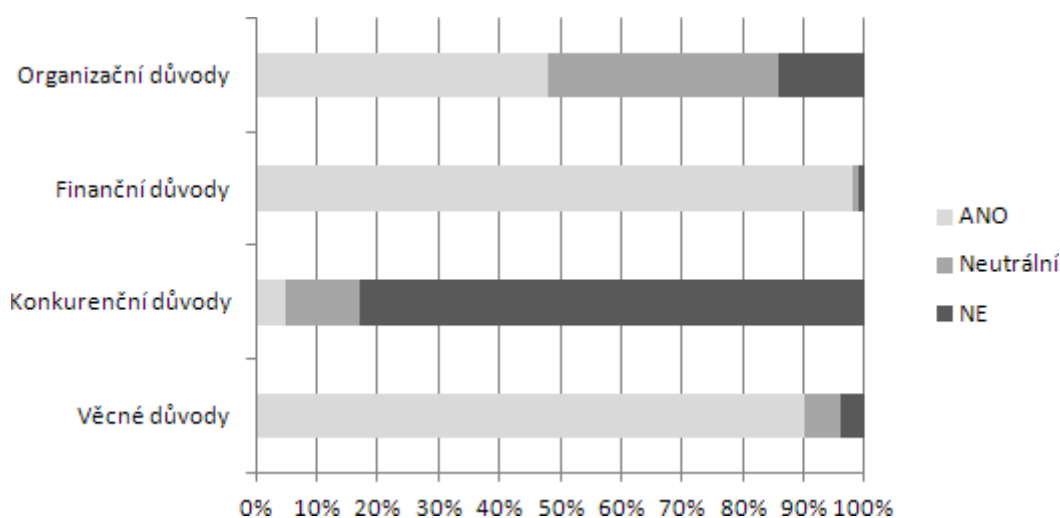
Cílem každé společnosti je zvyšovat její hodnotu. Hodnotu podniku pro vlastníky můžeme měřit například na základě ukazatele ROE, který představuje ziskovost podniku. Vyšší ziskovosti můžeme dosáhnout buď snížením nákladů anebo zvýšením tržeb. Proto bychom měli o outsourcingu ICT uvažovat pouze v případě, kdy to podniku přinese zvýšení tržeb, nebo naopak sníží náklady a tím dojde ke zvýšení hodnoty podniku (15).

Důvody

- *Věcné důvody* – soustředění se na hlavní činnost podniku, sdílení nebo přenesení rizika na jiný subjekt, kvalita dodávaných služeb, atd.
- *Konkurenční důvody* – získání konkurenční výhody, přístup k novým technologiím, apod.
- *Finanční důvody* – snížení nákladů, zvýšení přínosů, zprůhlednění nákladů, změna fixních nákladů na variabilní náklady, uvolnění zdrojů pro investice, atd.
- *Organizační důvody* – zjednodušení organizační struktury, efektivnější využití personálních zdrojů, apod. (16).

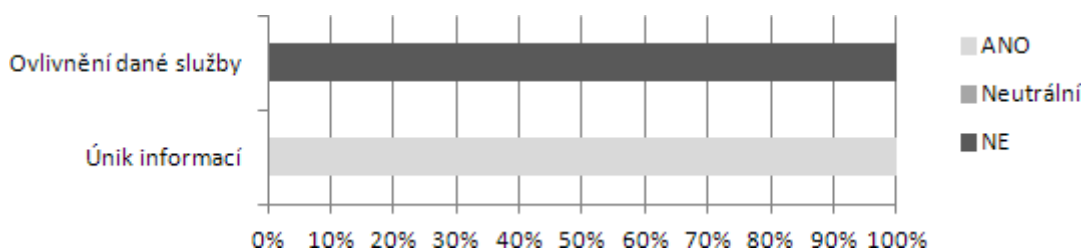
Následující grafy vychází z dotazníkového šetření provedeného v sektoru malých a středních firem v České Republice. Šetření se zúčastnilo 103 respondentů z řad managementu společností a bylo provedeno na začátku roku 2015 studentkami VUT Brno (16).

Jako nejčastější důvody podniků, které se rozhodly pro outsourcing, označili respondenti jednoznačně **finanční důvody** – což koresponduje s informacemi uvedenými na obrázku č. 3 a to, že podnik by měl outsourcovat v případě, kdy mu tento krok přináší zvýšení hodnoty podniku.



Obrázek č. 3: Důvody k realizaci outsourcingu (16)

Graf na obrázku č. 4 zachycuje důvody, kvůli kterým se podniky nerozhodly pro outsourcing. Nejdůležitějším důvodem je **obava z úniku informací**.



Obrázek č. 4: Důvody k nerealizaci outsourcingu (16)

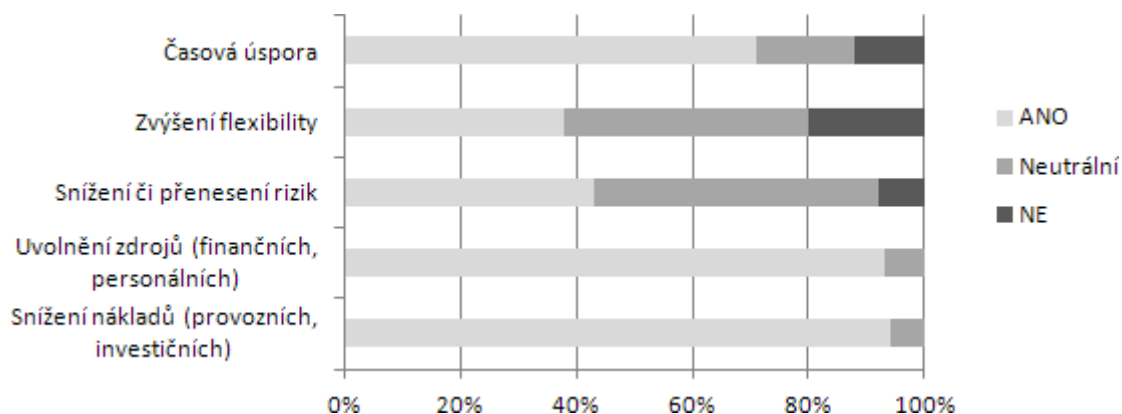
Výhody

Při změně požadavků na technické či personální zdroje společnost není nucena hledat dodatečné zdroje nebo naopak řešit problém jak snížit přebytečné kapacity, kterými disponuje. Veškeré povinnosti, agenda a rizika vyplývající z vlastnictví majetku a lidských zdrojů je přesunuta na stranu poskytovatele. Další nespornou výhodou je možnost pronajímat si kapacity podle aktuálních potřeb, ať už se jedná o výpočetní výkon, kapacitu úložiště či čas zaměstnance. Investice do IT nepředstavují jednorázový výdaj, ale jsou rozprostřeny do delšího časového horizontu ve formě pravidelných měsíčních plateb v očekávané výši. Díky tomu může manažer zodpovědný za investice do IT lépe plánovat a rozvrhovat v delším časovém úseku, což může pozitivně ovlivnit stanovení strategie IT. Rovněž dochází k redukci investic do IT (11).

Vytěsněním podpůrného procesu roste specializace podniku, který se tak může zaměřovat na svou hlavní činnost a získat konkurenční výhodu (12).

Outsourcing je dodáván specializovanou firmou, která se orientuje v aktuálních trendech nových technologií, metod přístupů a znalostí, což poskytuje podniku rychlejší nástup moderních technologií a profitovat na nejlepších praktikách poskytovatele (17).

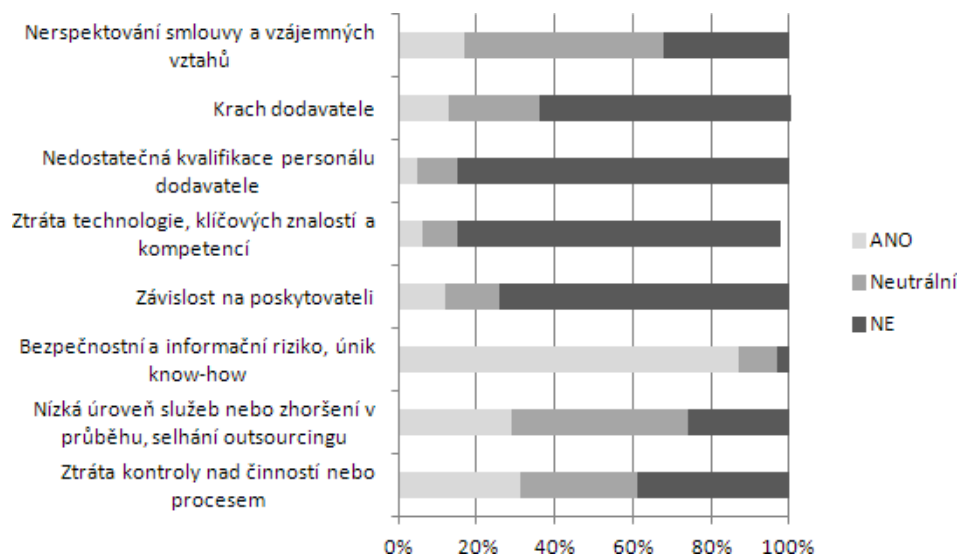
Obrázek č. 5 zobrazuje, které výhody outsourcingu považují respondenti za pro ně rozhodující. Jako největší výhodu považují **snížení nákladů a uvolnění zdrojů**, dále pak získání **časové úspory**. Naopak nepovažují za důležité snížení rizik a zvýšení flexibility. Zajímavé také je, že právě k oblasti nakládání s riziky se staví z velké části neutrálně (16).



Obrázek č. 5: Výhody outsourcingu (16)

Nevýhody a rizika

Outsourcingem procesu společnost do jisté míry ztrácí přímou kontrolu a vládu nad ním a vzdává se určitého know-how. Částečně ztrácí kontrolu nad tokem interních informací mimo podnik, což může představovat nemalé riziko v závislosti na typu informací. Toto potvrzuje i graf na obrázku č. 6, který zachycuje odpovědi na otázku, v čem respondenti spatřují rizika spojená se zajištěním činnosti externím dodavatelem (16).



Obrázek č. 6: Rizika outsourcingu (16)

Další nevýhodou může být nižší pružnost reakce ze strany poskytovatele na požadavky zákazníka, tedy nižší operabilita. Může se také stát, že outsourcingem nedojde k očekávanému snížení nákladů, naopak může dojít ke zvýšení nákladů a to především transakčních. Nesmíme zapomenout na vyšší počáteční transakční náklady. Rovněž také může vyvstat potřeba změnit smluvní podmínky, což s sebou samozřejmě nese další zvýšení nákladů. V případě, kdy zákazník požaduje nějakou změnu kontraktu, musí být tato změna výhodná pro dodavatele a ten ji může nebo také nemusí akceptovat. Odebírání takovéto služby pak může být pro zákazníka nevýhodné a v případě, kdy chce kontrakt zrušit, značně rizikové (15). Je nezbytné vzít v úvahu všechna rizika a nastavit formu a úroveň outsourcingu tak, aby společnost nebyla v ohrožení v situaci, když by došlo k neplnění smlouvy nebo jejímu vypovězení ze strany dodavatele. Také je vhodné uvažovat o záložním dodavateli v případě nutnosti vypovězení smlouvy a přechodu k jinému poskytovateli a to v dostatečně krátkém čase. Je samozřejmě důležité si vybrat spolehlivého poskytovatele, který zajistí dodávku služby na patřičné úrovni a v daném rozsahu (17).

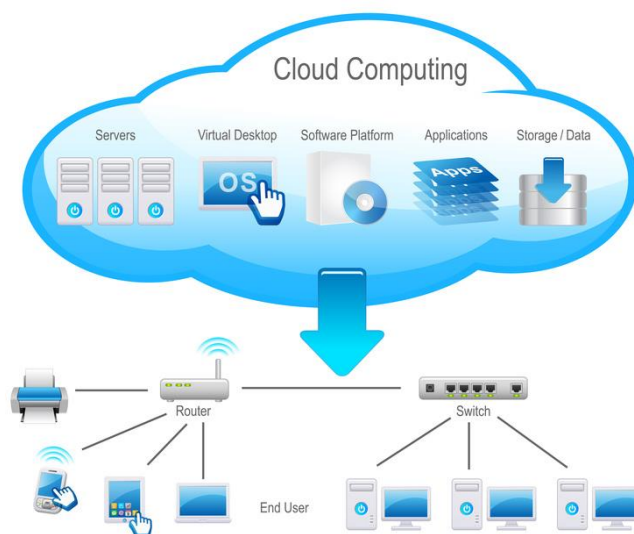
Výsledky šetření ukázaly, že cílem outsourcingu je vytěsnit podpůrné činnosti a soustředit se na hlavní činnosti podnikání, za účelem zvýšení konkurenceschopnosti a především snížení provozních nákladů a uvolnění zdrojů, což odpovídá prioritám každého podniku, kterými jsou růst hodnoty firmy a ziskovosti.

1.3 Cloud computing

Institut NIST definuje cloud computing jako síťový přístup ke sdíleným škálovatelným výpočetním zdrojům na vyžádání, jejichž kapacita může být rychle navýšena nebo naopak uvolněna a to při minimálním úsilí nebo interakci s poskytovatelem služby (18).

Cloud computing je metoda poskytování IT ve formě služby, kterou poskytuje svým zákazníkům provozovatel cloudu. Jedná se o koncepci, jež umožňuje vzdálený přístup k IT zdrojům a službám umístěným v Internetu, tedy mimo podnikovou síť a to prakticky odkudkoliv. Princip spočívá v tom, že výpočetní technologie jsou hostovány externí společnostmi na jejich serverech. Poskytovatel cloudu se stará o provoz IT infrastruktury, což zahrnuje její údržbu, obměnu, apod. Na této infrastruktuře je poté možné provozovat operační systémy, aplikaci a další, které může odebírat velký počet zákazníků. Odběratel však platí poskytovateli jen za ty služby, které si vybral a které využívá, ve formě měsíční platby odvislé zpravidla od počtu obsluhovaných koncových uživatelů. Cloud computing je vyústěním trendu, kdy zákazník nemusí nic instalovat na své počítače či servery a nemusí do nich ani investovat finanční prostředky (19).

Následující obrázek č. 7 princip fungování cloud computingu osvětluje.



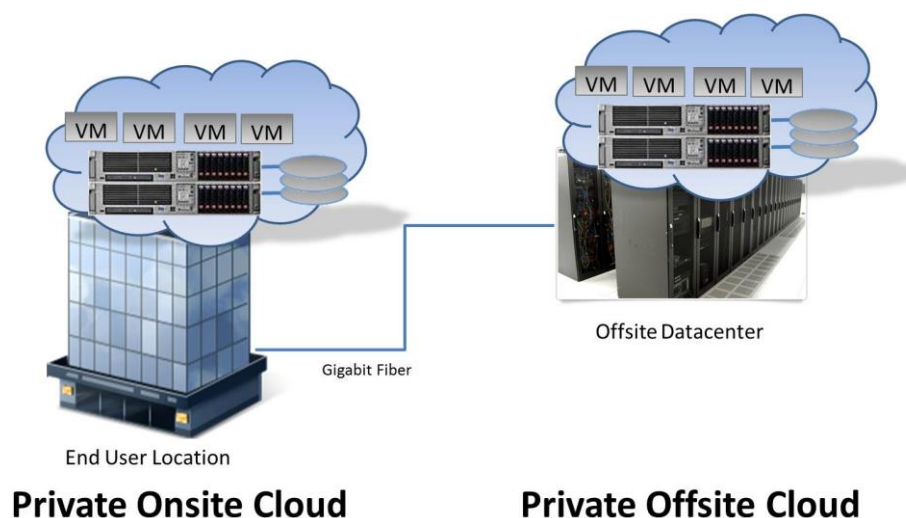
Obrázek č. 7: Cloud computing (19)

1.3.1 Umístění ICT infrastruktury

On-premises – řešení, kdy ICT infrastruktura nebo její část je umístěna a provozována lokálně, u cloud computingu jde v podstatě o privátní cloud, který podnik provozuje lokálně vlastními silami.

On demand (off-premises) – jde o řešení, kdy ICT infrastruktura nebo její část je provozována v cloudu ve formě služby na vyžádání (20, 21).

Porovnání výše definovaných řešení zachycuje obrázek č. 8.

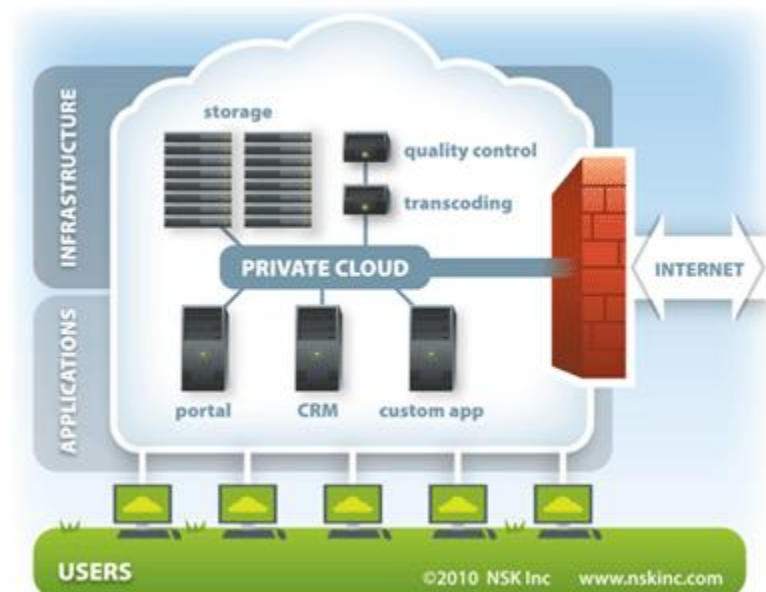


Obrázek č. 8: Privátní cloud - Onsite a Offsite (21)

1.3.2 Modely nasazení cloud computingu

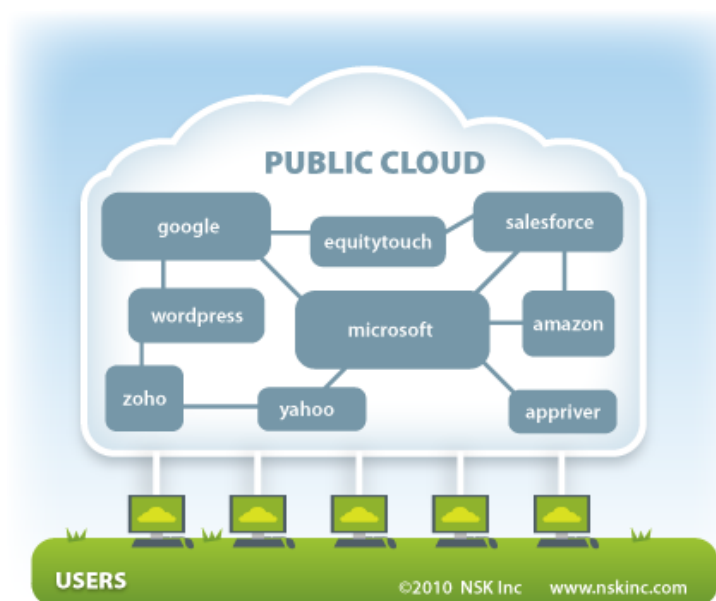
Modely nasazení definují, jakým způsobem je cloud zákazníkovi poskytován. Dle toho rozlišujeme tyto modely nasazení cloudu:

Soukromý (Private cloud) - v modelu soukromého cloudu je cloud poskytován a provozován pouze pro dedikovanou společnost. Cloud není sdílený s žádnou jinou společností, proto tento model nabízí nejvyšší úroveň bezpečnosti a kontroly. Soukromý cloud může buď provozovat společnost sama pro sebe (on-site) nebo pro ni cloud může poskytovat třetí strana v bezpečném datovém centru (off-site). Je vhodný pro ty, kteří mají citlivá data, podléhají přísným bezpečnostním požadavkům na uchovávání a nakládání s daty, nebo se jedná o dostatečně velký podnik, který může efektivně provozovat své vlastní datové centrum (20, 22). Schéma privátního cloudu je na obrázku č. 9.



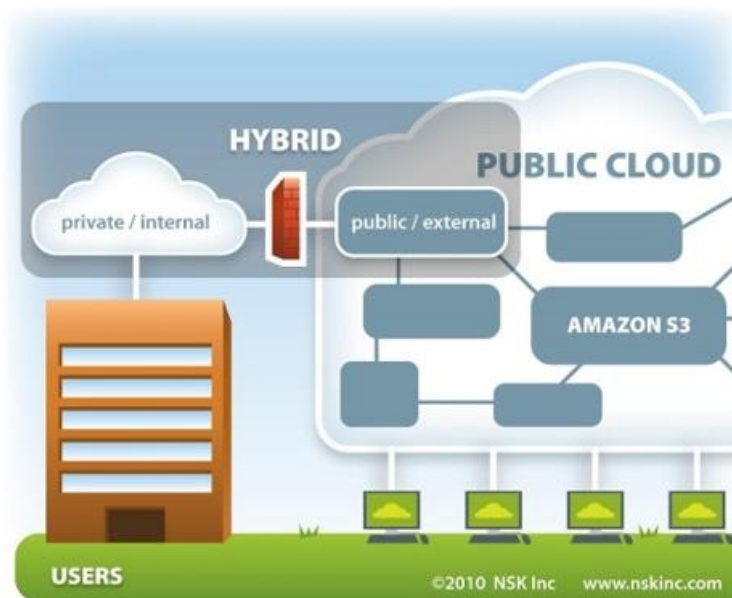
Obrázek č. 9: Privátní cloud (23)

Veřejný (Public cloud) – jde o model, kdy je výpočetní služba poskytována a nabízena široké veřejnosti. Veřejný cloud poskytuje všem stejnou nebo velmi podobnou funkcionalitu, spadá zde například Skype nebo Seznam.cz. Veřejný cloud nabízí vysokou efektivitu využití sdílených prostředků, avšak je zranitelnější než soukromý cloud. Je vhodný pro ty, kteří používají standardizované aplikace, například email, nebo při spolupráci na projektech (20, 22). Princip veřejného cloudu je na obrázku č. 10.



Obrázek č. 10: Veřejný cloud (23)

Hybridní (Hybrid cloud) – jedná se o kombinaci veřejného a soukromého cloudu, kdy navenek vystupují jako jeden cloud, ale ve skutečnosti jsou propojeny pomocí standardizačních technologií. Společnost pro své standardní interní činnosti využívá privátní cloud v kombinaci ostatních činností hostovaných ve veřejném cloudu (20). Jak je tvořen hybridní cloud zachycuje obrázek č. 11.



Obrázek č. 11: Hybridní cloud (24)

Komunitní (Community cloud) – v tomto modelu je mezi několika organizacemi skupinou lidí sdílena infrastruktura cloudu. Organizace mají něco společného, např. obor zájmu, sdílené hodnoty apod. Jedná se o speciální případ veřejného cloudu (20). Schéma komunitního cloudu je na obrázku č. 12.



Obrázek č. 12: Komunitní cloud (25)

1.3.3 Distribuční modely cloud computingu

Distribuční model definuje, co je předmětem poskytované služby ve formě cloudu.

IaaS (Infrastructure as a Service) – Infrastruktura jako služba. Předmětem poskytování služby je virtualizovaná infrastruktura (datové centrum, server, úložiště). O veškerý hardware a problémy spojené s provozováním se v tomto modelu stará poskytovatel infrastruktury. Zákazník se zbavuje starostí a nákladů vyplývajících z nákupu a provozu infrastruktury, neboť si ji kupuje jako službu. Tento model je vhodný pro podniky, které vlastní licence nebo software, ale nechťejí se starat o hardware, na kterém by je provozovali (11, 20).

PaaS (Platform as a Service) – Platforma jako služba. Dodavatel v tomto modelu poskytuje veškeré prostředky pro podporu životního cyklu tvorby a poskytování webových aplikací. To představuje kompletní hardwarovou a softwarovou platformu pro vývoj aplikace (IDE, API) ale také pro jejich údržbu. Problémem je uzavřenost, jelikož každý poskytovatel může používat jinou platformu, jiný programovací jazyk (11, 20).

SaaS (Software as a Service) – Software jako služba. Předmětem služby je aplikace, která je pronajímána zákazníkovi. Zákazník si tedy kupuje samotnou aplikaci. Tento model je vhodný zejména tam, kde potřebujeme přistupovat k aplikacím odkudkoliv (11, 20).

XaaS (Anything as a Service) – Cokoliv jako služba. Kvůli problematickému zařazení předmětu poskytované služby do výše jmenovaných kategorií si každá společnost stanovuje vlastní distribuční model XaaS, například DaaS (Database), NaaS (Network), BPaaS (Business Process). Avšak každý tento model je odvozen od některého ze základních distribučních modelů jmenovaných výše (26).

1.3.4 Výhody cloud computingu

- nízké požadavky na technologické znalosti – uživatelé nemusejí znát technické principy fungování HW a SW,
- vzdálená podpora, která je poskytována odborníky na danou problematiku,

- díky virtualizace dochází ke sdílení HW prostředků, což umožňuje efektivněji přerozdělovat výpočetní výkon strojů dle potřeby mezi uživatele,
- flexibilní přidělování kapacity výpočetních prostředků, které je realizováno přímo v datovém centru u poskytovatele, které nabízí efektivnější provoz a vyšší výkon pro uživatele,
- datové centrum musí splňovat vysoké požadavky na zabezpečení a dostupnost (27).

1.3.5 Nevýhody cloud computingu

- možné vysoké náklady na změnu poskytovatele, který používá proprietární (uzavřené) technologie,
- možné zdražení služeb cloudu poskytovatelem, tím pádem vyšší provozní náklady a růst TCO,
- migrační náklady na přechod do cloudu (organizační změny, školení uživatelů, řízení změny, kdy se většinou setkáváme s odporem ke změně),
- špatná pověst cloud computingu pramenící ze strachu, který se týká úrovně zabezpečení cloudu; tento strach mnohdy přerůstá až v paranoii, kdy společnost spatřuje umístění interních informací mimo podnik jako vysoce rizikové,
- riziko střetu právních řádů poskytovatele a klienta (může se stát, že poskytovatel má data fyzicky umístěna v datovém centru v zemi, kde platí jiné zákony, než v zemi klienta),
- vyžaduje internetové připojení (z toho pramenící riziko výpadku internetu, což znemožní přístup do cloudu – k datům/aplikacím/infrastruktuře a může mít na klienta vysoký ekonomický dopad) (27).

1.3.6 Bezpečnost v cloudu

Protože jsou data umístěna v Internetu, který se rozvíjí vysokým tempem, objevují se stále nové hrozby, kterým je potřeba čelit a je aplikovat nové přístupy k zabezpečení dat. To ovšem platí, ať už jsou data uložena kdekoli.

Správa identit, role a práva

Podniky, které využívají cloudových služeb, používají velmi často zdvojený bezpečnostní mechanismus – kontroluje se nejprve přístup k samotnému cloudu a poté přístup k aplikaci jako takové. Zde je nutná dvojí autentizace (v návaznosti na zdvojenou kontrolu přístupu). Přístup zaměstnanců je zřízen pouze k takovým datům a aplikacím, které jsou nutné pro jejich práci – to nejlépe zajistí přístupové systémy, pracující na principu rolí a digitální identit zaměstnanců (27).

Infrastruktura firmy a bezpečná komunikace v cloudu

Aby byla zajištěna bezpečná komunikace v prostředí cloud computingu, je nutné používat vždy šifrovaný přenos dat. Rovněž je nutné implementovat ochranné systémy sítě, jako bezpečnostní firewall, systémy pro detekci průniků (IDS), či systémy s proaktivním přístupem k průnikům do sítě (IPS). V případě, kdy jsou síťové komunikační služby poskytovány dodavatelem, je nezbytné aplikovat integrované mechanismy MPLS (Multi Protocol Label Switching), které oddělují toky dat od různých uživatelů a služeb. MPLS pro směrování dat mezi síťovými uzly nepoužívá protokolově závislé síťové adresy, ale krátká „návěští“ pevné délky. Návěští neidentifikují koncové body, ale virtuální spoje (cesty) mezi uzly. Hlavní výhodou MPLS je, že umí zapouzdřovat pakety různých síťových protokolů, protože není závislá na určité technologii linkové vrstvy OSI modelu (jako ATM – Asynchronous Transfer Mode, či Ethernet). MPLS patří k sítím s přepojováním paketů a může přenášet různé druhy provozu (IP pakety, Ethernetové rámce). MPLS přináší vyšší spolehlivost a výkonnost sítě, proto je vhodná pro VPN (Virtual Private Network) připojení (27, 28).

Ochrana IT systémů

Pro vzájemné oddělení systémů se používají VLAN (Virtual Local Area Network) a firewally. Tyto prostředky zabraňují, aby různí klienti/nájemci/uživatelé přistupovali k serveru, datům či aplikacím jiných uživatelů. Firewally sledující komunikaci, porty a aplikace, firewally s funkcionalitou DPI (Deep Packet Inspection) a systémy IDS/IPS zajišťují efektivní ochranu segmentů sítě (27).

Právní prostředí a správa služeb

Co se týče legislativy, souladu se zákonem se nejsnáze dosahuje u poskytovatelů privátního cloudu. Ve smlouvě o úrovni služeb SLA (Service Level Agreement – dohoda o úrovni služeb) je možné definovat země, kde je možné mít data uložena a kde budou zpracovávána (na rozdíl od poskytovatele veřejného cloudu). Zeměpisná poloha umístění dat je velmi důležitá, kvůli zákonům, které mohou být v různých zemích jiné. Je důležité předem jasně stanovit, kdo bude dodávat jaké služby a kdo je právně odpovědný za jakékoli nejasnosti, které mohou nastat (27).

1.3.7 Smluvní úprava odpovědnosti za ztrátu dat v cloudu

Jak pro poskytovatele, tak pro odběratele cloudových služeb, je klíčové vhodně upravit smlouvu a především jasně určit odpovědnosti za ztrátu dat. Smlouva o poskytování cloudových služeb by měla jasně stanovit tyto odpovědnosti a také konkrétní povinnosti:

- **Odpovědnost za ztrátu dat při migraci** – přesun dat je realizován nejenom na počátku, kdy zákazník migruje svá data do úložiště cloudu, ale také při případném ukončení kontraktu, kdy se data přesouvají zpět do úložiště k zákazníkovi (nebo k jinému poskytovateli). Je vhodné stanovit, kdo je v tomto případě odpovědný za ztrátu dat, pokud jím není poskytovatel datového přenosu.
- **Odpovědnost za umístění dat** – čili kde se data fyzicky nacházejí, ve kterém datovém centru jsou uložena. Poskytovatel je povinován vyžádat si od zákazníka souhlas v případě, kdy by data měla být přesunuta do jiného datového centra. Je důležité upozornit, že uživatel by vždy měl vědět, kde se jeho data právě nacházejí. Stává se totiž, že poskytovatel nabízí hosting služeb, avšak tento poskytovatel nedisponuje vlastním datovým centrem, nýbrž tuto službu zajišťuje u jiných poskytovatelů (27).

1.3.8 ISMS a cloud computing

ISMS – (Information Security Management System) – Systém řízení informační bezpečnosti, je součástí integrovaného systému řízení organizace (IMS). Zavedení ISMS v organizaci je postaveno na modelu PDCA (Demingova cyklu) ve čtyřech etapách:

1. Ustavení ISMS – určuje se rozsah a odpovědnosti,
2. Zavádění a provoz – prosazují se vybraná bezpečnostní opatření,
3. Monitorování a přezkoumání ISMS - zajišťuje se zpětná vazba a hodnocení řízení,
4. Údržba a zlepšování – odstraňují se slabiny, což vede k soustavnému zlepšování.

Posledním krokem zavedení ISMS je certifikace podle platných ČSN norem. Normy jsou buďto obecně platné pro danou problematiku, nebo jsou specifické dle oboru činnosti organizace (27).

Obecně platné normy:

*ČSN ISO/IEC 27000:2014 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – **Přehled a slovník***

- jedná se o mezinárodní normu, která poskytuje přehled systémů řízení bezpečnosti informací, jenž tvoří rodinu norem ISMS a dále definuje související termíny. Tato norma definuje pojmy a terminologický slovník pro ostatní normy z řady 27000 (27).

*ČSN ISO/IEC 27001:2013 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – **Požadavky***

- jde o hlavní normu ISMS, která obsahuje doporučení jak aplikovat vybraná opatření uvedená v normě ISO/IEC 27002 v rámci procesu zavádění ISMS. Obsahuje požadavky na vybudování, zavedení, provoz, monitorování, přezkoumání, udržování, zlepšování a případnou certifikaci ISMS. Podle této normy se ISMS certifikuje (27).

*ČSN ISO/IEC 27002:2013 Informační technologie – Bezpečnostní techniky – Systémy managementu bezpečnosti informací – **Soubor postupů***

- norma obsahuje více než 5000 bezpečnostní opatření, které jsou strukturované do 133 oblastí a rozdělené do 11 kapitol. Podle této normy se bezpečnostní opatření přímo aplikují/implementují v organizaci (27).

Specifické normy pro cloud computing:

ISO/IEC 27018:2014 – Information technology – Security techniques – Code of practice for protection of Personally Identifiable Information (PII) in public clouds acting as PII processors.

- norma poskytuje **doporučení** vztahující se k **ochraně osobních údajů** v prostředí cloud computingu

- dává vhodná bezpečnostní opatření poskytovatelům cloudových služeb pro zabezpečení soukromí zákazníků
- norma obsahuje kromě opatření z normy ISO 27002 také **nová specifická opatření týkající se ochrany soukromí a osobních údajů** v cloudu (27).

ISO/IEC 27017:2015 – Information technology – Security techniques – Code of practice for information security controls based on ISO/IEC 27002 for cloud services

- norma poskytuje **doporučení** vztahující se k **bezpečnosti informací** pro cloud computing.
- norma obsahuje kromě opatření z normy ISO 27002 taktéž **specifická opatření pro cloud computing** (27).

1.4 Serverhosting

Serverhosting je forma služby IaaS a jedná se o službu poskytující pronájem serveru nebo umístění vlastního serveru ve specializovaném datovém centru, které je pro tyto účely vybaveno odpovídajícím způsobem na profesionální úrovni. Připojení do datového centra je prostřednictvím sítě Internet. Nabídku serverhostingu mohou doplňovat další služby, jako monitoring dostupnosti, vzdálené podpora (remote hands), KVM over IP (klávesnice/video/myš; jde o rozhraní, díky kterému se lze odkudkoliv připojit přes IP, získat tak vzdálený přístup k zařízení a mít stejné možnosti při práci se strojem jako při fyzické přítomnosti na místě) (29, 30).

Zákazník využívající tuto službu server s nikým dalším nesdílí, je k dispozici výhradně jemu pro jeho vlastní účely, může na něm provozovat libovolné aplikace, k serveru má administrátorský přístup a není limitován v rozsahu využívání serveru.

Servery se umísťují do datových center, které nabízejí adekvátní prostředí pro serverhosting. Datová centra musí splňovat požadavky kladené na dostupnost, bezpečnost a spolehlivost provozu mnoha serverů a telekomunikačních technologií. Běžné datové centrum, je dnes vybaveno zálohovanou elektrickou sítí (UPS a diesel agregáty), klimatizací, redundantním připojením do Internetu, monitoringem odběru energie, ostrahou objektu, evidencí přístupů osob, hasicím zařízením, kamerovým systémem a bezprašným prostředím se stálou vlhkostí (29).

1.4.1 Varianty serverhostingu

Hosting serverů se nabízí v několika variantách, od kterých se odvíjí cena služby:

Server housing

U služby nabízející housing serverů se nejedná o pronájem serveru od dodavatele, ale o umístění vlastního serveru (nebo i jiného hardware) zákazníka do prostorů poskytovatele – do datového centra. Starostí poskytovatele je pouze připojení hardware do Internetu (zajišťuje IP konektivitu) a běh serverovny. Zákazník se stará o vše ostatní, proto se jedná o nejlevnější variantu služby serverhostingu (29).

Rack housing

Tato služba v sobě zahrnuje pronájem rackové skříně nebo části racku pro jakákoliv zařízení zákazníka (tzn. server, router, firewall, switch, NAS, atd.). Pronájem racku je využíván nejčastěji za účelem snížení nákladů firmy na standardní housing jednotlivých zařízení. V rámci rack housingu je zajištění konektivity a elektrické energie (29).

Dedikované servery

Jde o standardní pronájem hardware, který je umístěn v datovém centru poskytovatele, o ostatní se stará zákazník sám – o správu serveru, instalaci software, zabezpečení a provoz služeb a aplikací. Poskytovatel ručí pouze za funkčnost pronajímaného HW a nastane-li porucha, provádí bezplatně nezbytné opravy. Dedikovaný fyzický server není sdílený s nikým dalším. Tato varianta služby je vhodná pro ty zákazníky, kteří nechtějí investovat do vlastního hardware (29).

Virtuální dedikované servery

Na hw fyzického serveru běží virtuální stroje/servery (VM), se kterými zákazník může pracovat jako by byly dedikovány jen pro něj, ale ve skutečnosti jsou hardwarové prostředky sdíleny mezi více uživateli. Poskytovatel však garantuje u každého VM výkon procesoru, vyhrazenou operační paměť RAM a kapacitu diskového prostoru. Virtuální servery nabízejí výhodu z hlediska úspory nákladů na pronájem fyzického serveru a flexibility při rozšiřování nebo navyšování potřebné vyhrazené kapacity (29).

Managed servery

Při této variantě jsou předmětem pronájmu dedikované servery včetně jejich správy ze strany poskytovatele. Managed servery jsou optimální volbou pro ty zákazníky, kteří nemají ke správě a údržbě serveru potřebné znalosti a zkušenosti, či kompetentní zaměstnance. Poskytovatel v rámci této služby zabezpečuje funkčnost serveru, softwarový update a záplaty, monitoring služeb atd. Managed servery jsou však nejdražší nabízenou variantou (29).

1.4.2 IP Konektivita

V případě serverhostingu má připojení serveru do sítě Internet dvě možné varianty:

- *Omezení rychlosti připojení* - je nastavena maximální přenosová rychlost, kterou mohou být data ze serveru přenášena z/do Internet, ale není omezen celkový objem přenesených dat.
- *Omezení objemu přenesených dat* - počítá se objem skutečně přenesených dat (v součtu za oba směry – z/do Internetu). Při překročení povoleného (většinou měsíčního) limitu jsou aktivována různá omezení (29).

1.5 Datové centrum

Datové centrum je možné definovat jako prostor, který slouží pro uložení ICT technologií a přidružených technologií, jako jsou telekomunikační a centralizovaná úložiště a to ať už fyzické nebo virtuální, pro ukládání, řízení a šíření dat a informací (31).

„Datovým centrem se rozumí centrum, které má optimalizovanou spotřebu elektrické energie, využívá hospodárný hardware a jeho virtualizaci. Poskytuje pronájem a provoz aplikací včetně pronájmu výpočetního výkonu ve vysoce bezpečném prostředí (32).“

Vybudování takového datového centra, zkráceně datacentra, zahrnuje velmi přísně specifikované řešení objektu (pozemek, umístění, stavba, zabezpečení, apod.), které musí být dotaženo dokonce včetně všech podsystémů, které zajišťují fungování datového centra a jeho životaschopnost. Požadavky na výstavbu datových center specifikují normy, např. ANSI-TIA/EIA 942A, či norma ČSN EN 50600 (33). Cloudová datová centra musí být ověřena podle mezinárodně uznávané normy ISO 27001 a shoda s touto normou musí být pravidelně ověřována nezávislými auditory. Norma ISO 27001 vyžaduje, aby

poskytovatelé datových center používali ISMS, který zavádí řízení bezpečnosti a rizik a zahrnuje rozsáhlý bezpečnostní rámec. Na poskytovatele DC se rovněž vztahují specifické normy ISO 27017 a ISO 27018. Proto je ISMS klíčovým nástrojem pro dosažení a udržení požadovaného stupně bezpečnosti (33).

1.5.1 Klasifikace datových center dle TIER

Organizace Uptime Institute klasifikuje datacentra do čtyř tříd: TIER I, II, III a IV (viz tabulka č. 1). Jedná se o klasifikaci pro porovnávání vlastností, výkonnosti a dostupnosti infrastruktury datových center, která je uznávána celosvětově (34, 35, 36).

Tabulka č. 1: Parametry serveroven a datových center dle klasifikace TIER (35)

	Třída			
	Tier I	Tier II	Tier III	Tier IV
	Základní (Basic) Technologická místnost	Redundantní prvky (Redundant components) Serverovna	Servisovatelné za provozu (Concurrently maintainable) Datové centrum	Odolné vůči poruše (Fault tolerant) Datové centrum
Počet elektrických přívodů (větví) do racku (datového rozvaděče)	1	1	1 aktivní 1 pasivní	2 aktivní
Redundance prvků	žádná (N)	N+1	minimálně N+1	2N+1
Průměrná počáteční hustota zátěže	1,9 - 2,8 kW/m ²	3,7 - 4,7 kW/m ²	3,7 - 5,6 kW/m ²	4,6 - 7,4 kW/m ²
Průměrná koncová hustota zátěže			9,3 - 13,9 kW/m ²	13,9 a více kW/m ²
Single Point of Failure (SPOF)	Mnoho + selhání lidského faktoru	Mnoho + selhání lidského faktoru	Málo + selhání lidského faktoru	Žádný + selhání lidského faktoru
Průměrná doba výpadku způsobená infrastrukturou	28,8 hod/rok	22 hod/rok	1,6 hod/rok	15 min/rok
Dostupnost (Availability) $A = MTBF / (MTBF + MTTR)$	99,671%	99,749%	99,982%	99,995%

Srovnání Tier III a Tier IV

- **Datové centrum - Tier III**

Výhody:

- částečná možnost údržby a servisu za provozu
- redundance UPS a chlazení
- náhradní zdroj elektrické energie - motorgenerátor
- optimalizované TCO
- nepřetržitý provoz 7x24

Nevýhody:

- nelze servisovat všechny systémy za provozu
- **existence SPOF**
- vyšší investiční náročnost

- **Datové centrum Tier IV**

Výhody:

- možnost provádět údržbu a servis za plného provozu
- plná redundance systémů pro napájení (přívody – elektrické okruhy, UPS) a chlazení
- **neexistence SPOF**
- vysoká dostupnost
- nepřetržitý provoz 7x24x365
- maximálně optimalizované TCO

Nevýhody:

- vysoké investiční nároky

Zásadním rozdílem mezi Tier III a Tier IV je, že DC třídy Tier IV vyžaduje dva nezávislé dodavatele energie, což není v podmínkách České republiky v současné době možné (34, 35).

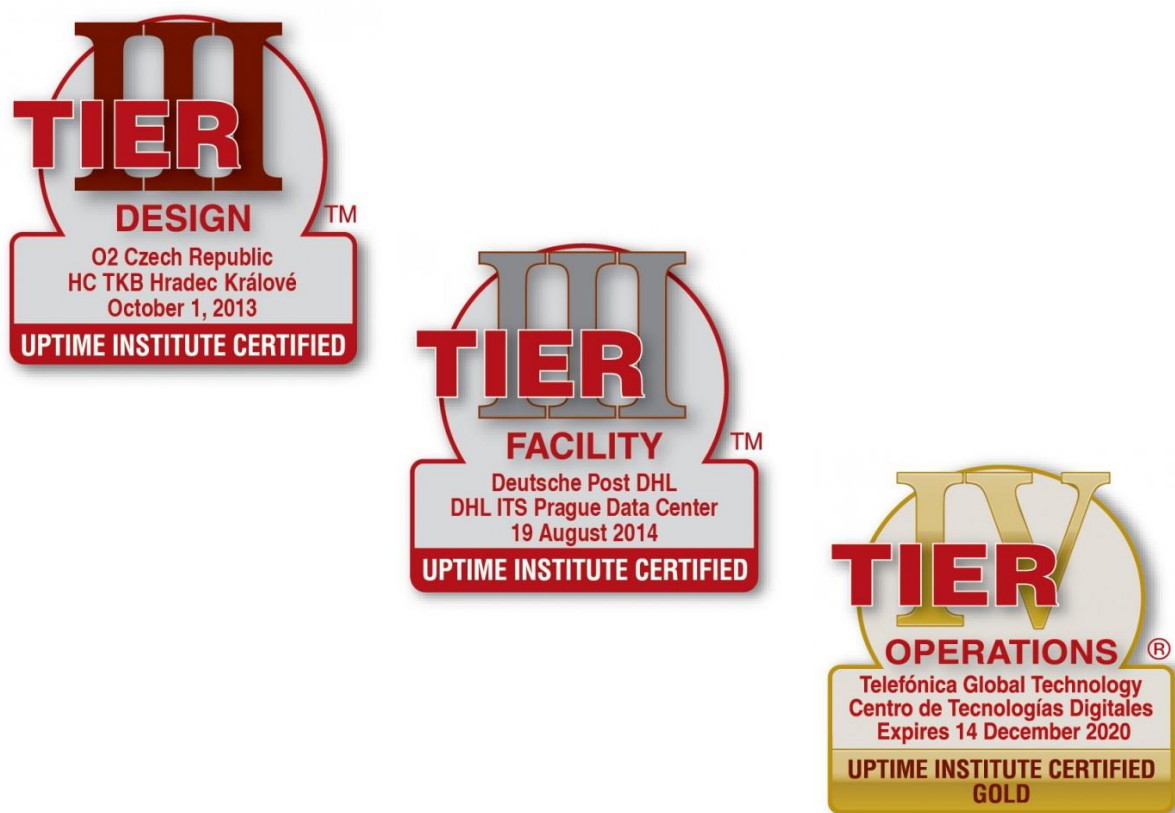
Termínem SPOF (Single Spot Of Failure) se rozumí jediný bod selhání, tzv. úzké hrdlo. Jde o část systému, která když selže, selže celý systém (35).

Existují tři variace certifikace Tier:

1. Tier Design – jde o certifikát návrhu, tedy certifikuje se projektová dokumentace.
2. Tier Facility – jedná se o certifikát konstrukce DC. Certifikát určuje úroveň Tier, kterou naplňuje výstavba DC a klasifikuje, jak byl projekt implementován dle projektové dokumentace.
3. Tier Operation – jde o provozní certifikát, certifikuje se reálný provoz datacentra dle kritérií klasifikace Tier (36).

Z toho plyne, že i když je určité datové centrum ve fázi konstrukce certifikováno jako Tier III, při provozu nemusí této úrovni dosahovat. Je tedy důležité, jakou třídu Tier datové centrum skutečně splňuje při svém provozu.

Jak vypadají TIER certifikáty od společnosti Uptime Institute znázorňuje obrázek č. 13.



Obrázek č. 13: TIER klasifikace – upraveno (36)

1.6 SLA

SLA – Service Level Agreement, je doslova dohoda o úrovni poskytovaných služeb, uzavíraná mezi poskytovatelem a zákazníkem. Je to smlouva, která definuje klíčové parametry poskytované služby, především rozsah, úroveň a kvalitu. Dále může obsahovat komunikační kanály pro zákazníka v případě řešení problémů, reakční doby na incident a doby pro odstranění poruchy, stanovuje odpovědnosti, atd.

SLA definuje např.:

- Garantovanou časovou dostupnost služby (např. 24/7/365 - 24 hodin, 7 dnů v týdnu a 365 dní v roce),
- Garantovanou cenu služby,
- Garantovanou rychlost řešení potíží se službou – reakční dobu (např. do 30 minut po oznámení problému) (37).

V případě outsourcingu je SLA nepostradatelným nástrojem pro vytvoření partnerského vztahu mezi dodavatelem a zákazníkem poskytované služby. Prostřednictvím SLA se přesně určí odpovědnosti a povinnosti obou stran ve smluvním vztahu, což vede k lepší efektivitě dlouhodobé spolupráce (38).

Dokument SLA má podle ITIL v3 následující strukturu:

1. Základní podmínky,
2. Popis služby,
3. Rozsah ujednání,
4. Doba provozu služby (service hours), dostupnost služby a spolehlivost služby,
5. Zákaznická podpora, kontaktní místa a způsob eskalace (incidentů),
6. Výkon služby,
7. Změnové řízení, zajištění kontinuity a bezpečnosti služby,
8. Odpovědnosti,
9. Cena,
10. Reportování a revize (38).

1.7 Poměr cena/kvalita/přidaná hodnota

Pokud chce podnik hodnotit přínos ICT infrastruktury, měl by se zaměřit na dosažení co nejlepšího možného poměru cena/kvalita/přidaná hodnota.

Cenu, jakou podnik zaplatí za **pořízení**, **implementaci** a v neposlední řadě také **provoz** ICT infrastruktury nejlépe vyjadřují celkové náklady na vlastnictví. Ty jsou součtem provozních nákladů a nákladů na změnu:

$$TCO = RTC + CTC$$

- TCO (Total Cost of Ownership) – představují celkové náklady na vlastnictví IS/ICT.
- RTC (Run to Costs) – zahrnují provozní náklady, tedy náklady na obsluhu a správu ICT infrastruktury, náklady na řešení výpadku/nedostupnosti infrastruktury, náklady na vzdělávání a školení IT pracovníků.

- CTC (Change to Costs) – označuje náklady na změnu, či přizpůsobení ICT novým podmínkám. Zahrnuje náklady na vylepšení či změnu procesu, dodatečný hardware, nové licence, služby konzultantů. CTC jsou důležité především pro možnost vyhodnocené náklady porovnávat s budoucími přínosy, které změna přinese a lépe tak rozhodovat o zamýšlené investici.

U velkých podniků je tendence tlačit na úsporu nákladů, tedy dosahovat co nejnižších TCO. Toho lze dosáhnout právě prostřednictvím outsourcingu.

Kvalitu ICT infrastruktury představuje primárně její spolehlivost, funkčnost, udržitelnost, zabezpečení, uživatelský komfort, škálovatelnost a schopnost dalšího rozvoje.

Přidanou hodnotu vytváří ve spolupráci se zákazníkem implementační partner projektu. Ten dokáže do projektu vnést své jedinečné know-how a také nejlepší praktiky (best practices) osvědčené léty praxe, s cílem podpořit výkonnost podniku a dosáhnout konkurenční výhody zákazníka (12).

1.8 Projektové řízení

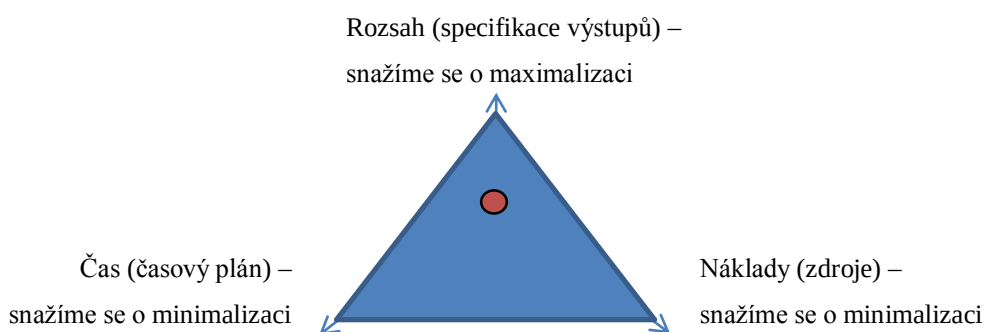
Tato kapitola pojednává o problematice projektového řízení, definuje projekt a zmiňuje některé nástroje používané při řízení projektů v jednotlivých fázích projektu. Projektovým řízením se myslí aplikování nabytých znalostí a osvojených dovedností při realizaci projektových aktivit a činností, s pomocí nástrojů, technik a metodik projektového managementu, pro účely dosažení požadovaných výstupů projektu (39).

1.8.1 Definice projektu

Projekt můžeme definovat jako jedinečný, časově, nákladově a zdrojově omezený sled aktivit, které realizujeme za účelem vytvoření unikátního výstupu v požadované kvalitě a dle odsouhlasených požadavků. Opakem projektu jsou každodenní, opakující se provozní činnosti. Projekt se od operativních činností liší tím, že končí ve chvíli, kdy je dosaženo cíle projektu (39, 40).

1.8.2 Trojimperativ projektu

Plnění cíle každého projektu je omezeno z hlediska rozsahu, času a nákladů. Tyto tři dimenze cíle jsou často vzájemně protichůdné, a abychom zajistili úspěch projektu, musíme tyto dimenze co nejlépe sladit a dosáhnout rovnováhy. Samozřejmě musíme stanovit určující osu, tedy, která dimenze je pro zákazníka nejdůležitější. Pokud je jako nejdůležitější uvažováno maximální naplnění rozsahu, pak může dojít k růstu nákladů a/nebo k prodloužení časového plánu projektu. Abychom však zajistili určitou jakost výstupu projektu, je nutné uvažovat kvalitu dosažených výsledků. Pokud chceme projekt řídit úspěšně, musíme naplnit nejen všechny tři dimenze cíle – rozsah, čas a náklady, ale musíme také uspokojit zákazníka projektu, tedy odevzdat projekt v požadované kvalitě (39). Trojimperativ projektu znázorňuje obrázek č. 14.



Obrázek č. 14: Trojimperativ projektu (25)

1.8.3 Znalostní oblasti projektového řízení

Znalostní oblasti projektové řízení definují klíčové kompetence, v nichž se musí projektový manažer orientovat a nadále je rozvíjet.

Mezi základní čtyři oblasti, které definují cíl projektu, patří:

- **Řízení rozsahu** – definice a řízení všech prací, které jsou nezbytné k úspěšnému dokončení projektu,
- **Řízení času** – odhady trvání prací, vypracování harmonogramu a zajištění včasného dokončení projektu,
- **Řízení nákladů** – příprava, sledování a aktualizace rozpočtu,
- **Řízení kvality** – zajištění, že výsledky projektu uspokojí potřeby zákazníka projektu (39).

Mezi pomocné oblasti patří:

- **Řízení lidských zdrojů** – motivace a řízení osob zapojených do projektu,
- **Řízení komunikace** – vytváření, sběr, ukládání, distribuce a archivace informací a projektové dokumentace,
- **Řízení rizik** – identifikace, analýza a zvládání rizik projektu,
- **Řízení dodávek** – zajištění zboží a služeb nezbytných pro realizaci projektu, včetně řízení dodavatelů a firem (39).

Integrované řízení projektu zahrnuje znalosti ze všech výše definovaných oblastí řízení, neboť projektový manažer musí mít komplexní znalost a orientaci ve všech oblastech týkající se problematiky projektového řízení (39).

1.8.4 Fáze řízení projektu

Jakmile přijde nápad na projekt, není možné začít s jeho okamžitou realizací, ale je nutné akci nejprve důkladně zanalyzovat a posoudit především její proveditelnost. Až poté je možné projekt naplánovat a zrealizovat. Po jeho realizaci nesmíme zapomenout na vyhodnocení úspěšnosti projektu, jeho uzavření a uvolnění přiřazených zdrojů na projekt. Řízení projektu proto můžeme rozdělit do tří fází a to na předprojektovou, projektovou a poprojektovou (41).

Předprojektová fáze

V rámci této fáze je potřeba provést **studii příležitostí**, která se zabývá tím, jestli je vhodná doba pro realizaci projektu a zda je vůbec potřeba jej realizovat. Na studii příležitostí navazuje **studie proveditelnosti**, která ukazuje nejvhodnější způsob k realizaci projektu a v rámci ní se upřesňuje obsah projektu, termíny, náklady a zdroje (41).

Projektová fáze

Po tom, co z předprojektových úvah vyplynulo doporučení pro realizaci projektu, následuje vytvoření základací listiny projektu, její schválení a uvolnění projektu k realizaci, což spadá do projektové fáze. Tato fáze má čtyři hlavní etapy, kterými jsou zahájení, plánování, realizace a dokončení projektu, a představují jeho životní cyklus (viz obrázek č. 15) (42).



Obrázek č. 15: Etapy projektové fáze (25)

V počátcích životního cyklu projektu jsou nároky na zdroje nejnižší a naopak stupeň nejistoty je nejvyšší. Jak se postupuje v projektu dále, klesá nejistota a rostou nároky na zdroje, ať už lidské, časové nebo finanční. Někde uprostřed cyklu jsou nároky na zdroje nejvyšší, neboť dochází k samotné realizaci naplánovaných aktivit a činností v projektu, tím dochází ke snižování nejistoty, neboť se přibližujeme k dosažení stanovených cílů, které jsou jasnější, máme hmatatelné výsledky. Ve fázi dokončení jsou nároky na zdroje nízké, probíhá většinou vyřizování administrativních a formálních záležitostí, výsledek projektu je převzat zákazníkem (39, 42).

Dále uvádím dva nejdůležitější dokumenty, které by měl obsahovat každý projekt, nehledě na jeho velikost.

Zakládací listina projektu

Zakládací listina projektu je identifikačním listem projektu, který vzniká poté, kdy je schváleno zahájení projektu řídicí komisí. Je to nejdůležitější listina ve fázi návrhu projektu, formálně deklaruje jeho existenci a uděluje projektovému manažerovi pravomoc používat zdroje organizace na projektové aktivity.

V zakládací listině je jmenován projektový manažer. Její podoba není nijak pevně stanovena, měla by však obsahovat minimálně tyto základní údaje:

- Název, číslo projektu,
- Plánované datum zahájení a ukončení projektu, případně harmonogram milníků,
- Rozpočet,
- Cíl projektu, účel projektu, výstupy a rozsah projektu,
- Identifikace hlavních rizik, předpokladů a kritérií úspěšnosti projektu,
- Zadavatel projektu, sponzor, zákazník, projektový tým, projektový manažer,
- Datum schválení projektu, jméno a podpis schvalovatele (42).

V praxi bývá často podepsaná Zakládací listina projektu opomíjena, což však vede k nejasnému zadání projektu, ze kterého vyplývá obtížná kontrola plnění rozsahu projektu. Pokud v průběhu projektu dochází ke změnám v zadání, je poté problém dohledat, jaké bylo původní zadání projektu a proč například došlo k nesplnění časové dimenze cíle projektu. Existence Zakládací listiny projektu tak chrání nejenom zadavatele projektu, neboť je definován jeho rozsah a požadované výstupy, ale také projektového manažera, který je odpovědný za naplnění cíle projektu a musí zajistit stanovené výstupy v požadované kvalitě (42).

Možná podoba Zakládací listiny projektu je uvedena v příloze č 1.

Plán řízení projektu

Každý projekt by měl být řízen, a proto je nutné mít plán řízení projektu. Plán řízení projektu zahrnuje v podstatě všechny plány, které se mohou v projektu vyskytovat. Míra detailnosti plánu a obsah záleží na charakteru projektu, plánujeme do takové úrovně, do které chceme projekt sledovat. Je to dokument, podle kterého se poté projekt realizuje, proto by měl být podrobný natolik, nakolik je projekt rozsáhlý.

Plán řízení projektu by měl řešit následující otázky:

PROČ = > za jakým účelem projekt realizujeme (definováno např. BSC = Balanced Score Card – hodnotící systém vyvážených ukazatelů),

CO = > specifikace cílů a výstupů projektu (prostřednictvím WBS = Work Breakdown Structure – Hierarchická struktura prací),

KDO => kdo bude pracovat na realizaci výstupů, jejich odpovědnost a časové možnosti (RACI matice odpovědnosti propojená na WBS, histogram zdrojů),

KDY = > kdy bude výstupů dosaženo (časový harmonogram s vazbou na disponibilní zdroje, Ganttův graf, milníky),

ZA KOLIK => finanční náročnost projektu (rozpočet, ROI, TCO, CBA, NPV) (39,43).

Poprojektová fáze

Poprojektová fáze bývá mnohdy opomíjena např. z důvodu neúspěšného projektu, realizace nových projektů či únava projektového týmu. Tato fáze je však velmi důležitá. Zahrnuje především administrativní kroky k vyhodnocení a uzavření projektu. Musí se zpracovat, zkontrolovat a archivovat veškerá projektová dokumentace a také musí dojít k vyhodnocení projektu, např. pro budoucí potřeby - poučení se z chyb. Výstupem je závěrečná zpráva projektu, jejíž možná podoba je uvedena v příloze č. 2 (42).

1.8.5 Projektové procesy

Procesy v projektovém řízení začínají u zahajovacích aktivit, přes plánovací, realizační, monitorovací a kontrolní a končí u uzavíracích aktivit. Je důležité *nezaměňovat projektové procesy a etapy v projektové fázi*, neboť každá etapa obsahuje všech 5 projektových procesů (39).

Procesy zahájení – zahrnují definování a schválení projektu či projektové fáze.

Procesy plánovací – zahrnují návrh a údržbu plánů projektu (plán řízení rozsahu, plán řízení času, plán řízení nákladů, atd.).

Procesy realizace – zahrnují koordinaci lidských a dalších zdrojů za účelem vytvoření výsledků projektu či projektové fáze.

Procesy monitorování a kontroly – zahrnují pravidelné hodnocení a monitorování postupu na projektu za účelem dosažení vytyčených cílů projektu. Při zjištění odchylky od plánu je nutné přijmout korekční opatření.

Procesy uzavření – zahrnutí formální schválení projektu nebo jeho fáze a zajišťují efektivní ukončení projektu/fáze, nejčastěji se jedná o administrativní činnosti (39).

Příloha č. 3 uvádí vztahy mezi vybranými oblastmi řízení a projektovými procesy, během nichž jsou obvykle dokončeny projektové aktivity týkající se dané oblasti řízení. Pro zajištění úspěchu projektu je nutné především řádně plánovat, neboť plánovací procesy se vyskytují nejčastěji a to napříč všemi oblastmi. Nejvíce zdrojů je dedikováno na samotnou realizaci projektu (39).

1.8.6 Nástroje projektového řízení

V příloze č. 4 je zpracován přehled možných nástrojů a technik, kterých je možné využít jako podporu při řízení projektu ve vztahu k oblasti řízení. Použití konkrétního nástroje je na zvážení projektového manažera, závisí na jeho zkušenostech, na typu a náročnosti projektu a použité metodiky projektového řízení (39).

2 ANALÝZA SOUČASNÉHO STAVU

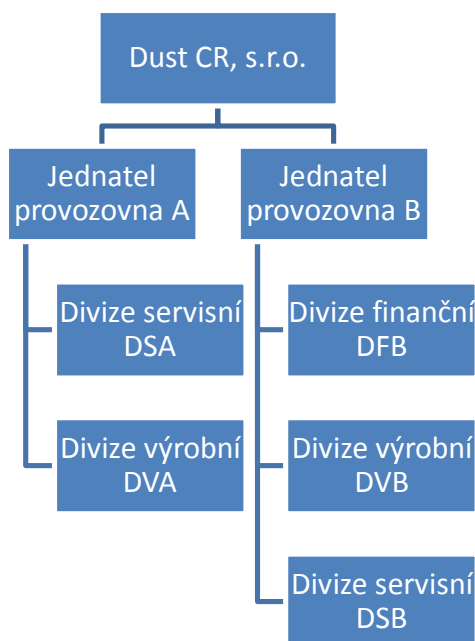
Vedení společnosti se rozhodlo pro hosting serverů v externím datovém centru a z tohoto rozhodnutí budu vycházet. Proto je tato část práce pojata jako část předprojektové fáze, ve formě studie příležitosti, kde zmiňuji základní informace o společnosti Dust CR, stručně uvádím informační strategii IT a popisuji stávající ICT infrastrukturu. Dále analyzuji zatížení sítě a náklady na provoz virtualizační infrastruktury v současné době. Tyto analýzy, slouží jako podklad pro zpracování studie proveditelnost, a jako příprava pro návrh migrace virtualizační infrastruktury do datového centra.

2.1 Základní informace o společnosti

Společnost Dust CR, s.r.o. je výrobní podnik, který v současnosti zaměstnává okolo 600 zaměstnanců a je součástí skupiny Dust s mateřskou společností v zahraničí v rámci Evropy. Skupina Dust se zaměřuje zejména na odvětví průmyslu domácích spotřebičů, farmaceutický průmysl, solární energii, elektroniku, optiku a také automobilový průmysl. V České republice se nacházejí dvě provozovny společnosti Dust CR ve dvou různých lokalitách. Každá provozovna má svého jednatele.

V lokalitě A se nacházejí dvě divize. Výrobní divize (DVA) je zaměřena na montáž výrobků z průmyslových optických vláken a LED diod, které slouží pro osvětlení. Divize se rovněž zabývá zakázkovou výrobou pro automobilový a letecký průmysl, osvětlení a zdravotnictví. Divize servisní (DSA) poskytuje služby ostatním společnostem Dust v lokalitě A v oblasti ekonomiky, personalistiky, logistiky, informačních technologií, technických servisů, bezpečnosti, kvality a ekologie.

V lokalitě B se nachází výrobní divize (DVB) zabývající se výrobou v oblasti automobilového průmyslu a optoelektroniky. Je vyhlášeným dodavatelem hermetických pouzder a průchodek, zabývá se také technologiemi zpracování speciálních skel. Dále provozovna zahrnuje servisní divizi (DSB), která kopíruje činnosti servisní divize lokality A. Navíc se zde nachází divize poskytující finanční služby (DFB) pro více poboček společnosti Dust v Evropě.



Obrázek č. 16: Organizační struktura Dust CR, s.r.o. (25)

2.2 Strategie IT

Misí IT oddělení společnosti Dust CR, jakožto i posláním celé skupiny Dust, je vystupovat jako obchodní partner, který pomáhá koncernu Dust dosahovat úspěchu ve svém podnikání.

Hlavním strategickým cílem centrálního IT (CIT), je **vytvořit jednotné IT** (One-IT) a dosáhnout tak synergického efektu z této spolupráce. Strategii jednotného IT podporují dílčí dlouhodobé cíle, mezi které patří v první řadě poskytovat stabilní IT služby a řídit IT projekty za účelem neustálého zlepšování všech podnikových procesů. Dále se každá funkční jednotka IT snaží o snižování nákladů na IT a zabezpečení plynulého provozu IT prostřednictvím optimalizace a standardizace ICT infrastruktury.

Dílčí cíle v jednotlivých oblastech

Dílčím cílem v oblasti *financí IT* je definovat vhodný způsob řízení nákladů a efektivní využívání již investovaného kapitálu.

Cílem v oblasti *řízení IT*, je zajistit bezpečnost ve výrobě prostřednictvím bezporuchových IT systémů, díky čemuž IT přispívá k tvorbě hodnoty pro společnost. Strategická rozhodnutí v oblasti IT musí být diskutována a odsouhlasena spolu s CIT, přičemž lokální IT přebírá odpovědnost za provoz lokální sítě, služeb a infrastruktury.

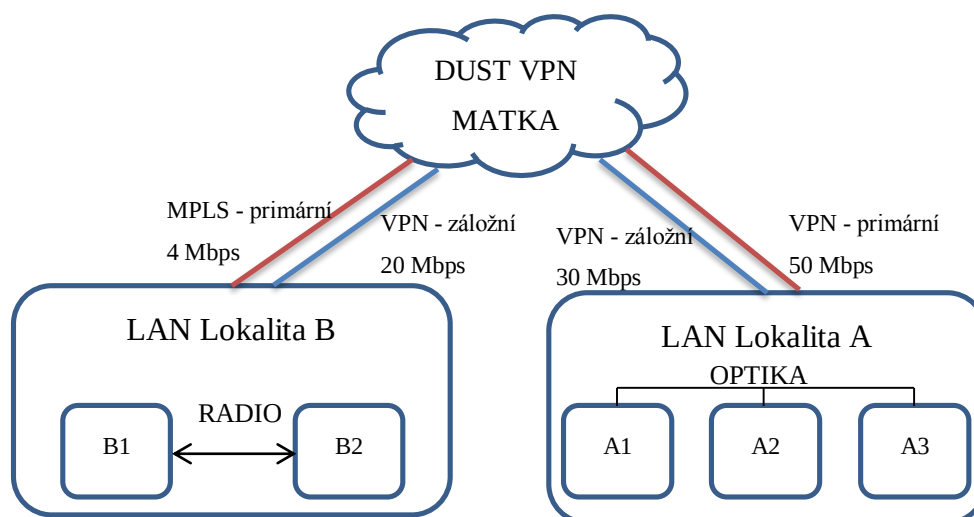
Stavebními kameny, díky kterým chce společnost dosáhnout jednotného IT, je *standardizovaná infrastruktura, operační systém, aplikační software, databázové platformy, hardware, služby, IT pravidla a bezpečnostní politika.*

V oblasti infrastruktury je cílem společnosti využívat pouze virtualizační platformu VMware jako standard pro datová centra a provoz serverové infrastruktury, nasadit ve všech lokalitách switche od společnosti CISCO (a to včetně výrobní sítě), centrální zálohování a přístup ke standardizované zabezpečené bezdrátové síti.

2.3 ICT infrastruktura

Veškerá ICT infrastruktura je umístěna v serverových místnostech. Lokalita B obsahuje jednu serverovnu, v lokalitě A se nacházejí dvě, které se nacházejí ve fyzicky oddělených budovách. Počítačová síť v obou lokalitách společnosti je postavena především na aktivních prvcích CISCO Systems. Páteřní spoje mezi budovami jsou v lokalitě A zajištěny pomocí optických spojů, v lokalitě B jsou budovy propojeny rádiovým spojem. Připojení do internetu je odděleno pomocí serveru s funkcí firewall. Obě lokality používají pro připojení k webu proxy server, který je umístěn v centrálním IT (CIT) v zahraničí. Vnitřní síťová struktura je zajištěna metalickými kabely typu Ethernet cat.5 na rychlosti 100 Mbps, která je ovšem závislá na typu switche. Veškerá infrastruktura podniku je v jeho vlastnictví. Ve vlastnictví poskytovatele internetových služeb je zařízení pro připojení do internetu o rychlosti 50 Mbps symetricky. Společnost platí poplatek za pronájem internetové trasy a měsíční poplatek za používání internetu. Spojení s mateřskou společností v zahraničí je v lokalitě A realizováno pomocí dvou VPN připojení, primární spoj rychlostí 50 Mbps, záložní 30 Mbps. Lokalita B je s matkou spojena primárně pomocí MPLS sítě rychlostí 4 Mbps, záložní VPN připojení 20 Mbps. Nevýhodou VPN konektivity je negarantovaná dostupnost a šířka pásma. MPLS spoj má vyhrazenou a garantovanou šířku pásma a umožňuje prioritizaci provozu.

Na obrázku č. 17 je znázorněno schéma WAN sítě. Ani v jedné lokalitě se nenachází optický přípojný bod jiného poskytovatele, než je současný poskytovatel konektivity a zavedení optiky by trvalo cca 12 měsíců.



Obrázek č. 17: Schéma propojení WAN sítě Dust CR, s.r.o. (25)

Rozdělení VLAN

V obou lokalitách je síťový provoz rozdělen do několika samostatných virtuálních sítí LAN (VLAN), jak z důvodu bezpečnosti, tak pro zpřehlednění a zjednodušení správy sítě (viz tabulka č. 2).

Tabulka č. 2: Rozdělení VLAN (25)

Rozdělení VLAN
Management (iDRAC, switch, konzole)
Výroba
Administrativa (office)
Servery
Tiskárny
Veřejný Internet
WiFi
Kamery
VoIP telefonie

2.3.1 Virtualizační infrastruktura

V lokalitě A i B je provozována virtualizační infrastruktura v prostředí VMware, která je založena na hostitelských serverech, zálohovacím serveru, vCenter Serveru pro správu infrastruktury, páskové zálohovací jednotce, diskového pole a switchů pro propojení. Společnost Dust CR aktuálně používá produktovou řadu VMware vSphere 5 Standard a vCenter Server Standard.

Hardware

V lokalitě A jsou dva fyzické servery Dell Power Edge R720xd, slouží jako hostitelé ESXi pro hostování virtuálních serverů. Jako zálohovací server je zde Dell Power Edge R610. Pro ukládání dat je použito diskové pole SAN DELL EqualLogic PS4100E s 12x 3TB disky, celková využitelná kapacita přiděleného svazku je okolo 12 TB. Diskové pole a fyzické servery jsou propojeny dvěma gigabitovými 24 portovými iSCSI switchi DELL PowerConnect 6224. Dále je nasazena pásková zálohovací jednotka DELL PowerVault TL2000 LTO5, knihovna obsahuje 24 slotů pro uložení magnetických pásek LTO Ultrium 5, které disponují kapacitou 1,5 až 3 TB (v případě komprese 2:1). Pro zálohování elektrické energie jsou k dispozici 3x Smart UPS RT 3000 VA od firmy APC, s kapacitou 2100 W až 2700 W.

V lokalitě B jsou provozovány dva servery DELL PowerEdge R620, které slouží jako ESXi servery, dále server DELL PowerEdge R530, který je určen pro zálohování. Jako úložiště je k dispozici diskové pole Dell Equallogic PS4210 s 24x 900 GB SAS disky s využitelnou kapacitou dedikovaného svazku 5 TB. Diskové pole se servery je propojeno prostřednictvím dvou 24 portových gigabitových iSCSI switchů DELL PowerConnect 5424. Pro zálohování je použita pásková zálohovací jednotka DELL PowerVault TL2000 LTO6 s 24 sloty pro pásky LTO Ultrium 6, každá s kapacitou 2,5 až 6,25 TB (v případě komprese 2,5:1). Jako záložní zdroj napájení je připojena UPS APC 5000VA, s celkovou kapacitou 4000 W.

Přehled hardwaru a jeho parametrů je uveden v příloze č. 5.

Virtuální servery

V lokalitě A je aktuálně provozováno 24 virtuálních serverů, v lokalitě B 23. Na virtuálních strojích jsou nainstalovány operační systémy Windows a Linux, na nich běží veškeré podnikové aplikace, které jsou spravovány interními pracovníky IT.

Přehled virtuálních serverů je uveden v příloze č. 6 a 7.

Tabulka č. 3 ve stručnosti uvádí přehled parametrů virtualizační infrastruktury jak pro jednotlivé lokality, tak v součtu pro celý Dust CR. Z této tabulky je také vidět, že celkový objem dat uložených na diskových polích SAN, dosahuje v obou lokalitách celkem 12,83 TB.

Tabulka č. 3: Stručný přehled parametrů virtualizační infrastruktury (25)

Lokalita	Počet hostitelů	Počet VMs	Kapacita CPU GHz	Využitá kapacita CPU GHz	Využitá kapacita CPU v %	Kapacita RAM GB	Využitá kapacita RAM GB	Využitá kapacita RAM v %	Vyčleněná kapacita SAN TB	Využitá kapacita SAN TB	Využitá kapacita SAN %
Dust CR	4	47	115,15	9,99	9%	448	224	50%	18	12,83	71%
z toho lokalita B	2	23	83,17	4,39	5%	256	123	48%	5	3,55	71%
z toho lokalita A	2	24	31,98	5,60	18%	192	101	53%	13	9,28	71%

V obou lokalitách jsou hostitelé nakonfigurováni s funkcí HA (High Availability), díky čemuž je zabezpečena dostupnost virtuálních serverů a aplikací na nich běžících v případě výpadku jednoho z hostitelů, neboť se virtuální servery přesunou a spustí na druhém hostiteli. Hostitelé ESXi a virtuální stroje se spravují prostřednictvím nástroje vSphere Client, který se spouští skrz webové rozhraní prohlížeče. Přes tohoto klienta se lze pomocí doménového ověření přihlásit do prostředí vCenter Server, který je provozován rovněž jako virtuální stroj, a provádět potřebnou správu virtualizační infrastruktury.

Provozované služby

V podniku běží jak lokálně provozované služby IT (např. tisk, síťové disky, docházkový systém a další lokální systémy a aplikace), tak centrálně provozované služby (ERP systém, pošta, Internet, a další).

Zatížení sítě

Pro zjištění, jak je síť zatížena, bylo nutné provést měření pomocí nástroje Netsight. Ten generuje i grafy o propustnosti sítě, které jsou k dispozici v příloze č. 8. Na grafech je zachycena vytíženost 100 Mbps FullDuplex linky za období 14 dnů. Monitoring probíhal tak, že páteční switch byl připojen na 100 Mbps portu a za tento port byla připojena provozní podniková síť. Na grafech v příloze č. 8 jsou viditelné mimořádné špičky, toto jsou jednorázové výkyvy, které byly způsobeny probíhajícími instalacemi klientů z obrazu a distribucí instalačních balíčků ze sítě. Tyto případy lze ošetřit prioritizací provozu službou QoS (Quality of Service). Průměrná rychlost se tedy pohybovala okolo 45 Mbps.

2.4 Analýza nákladů virtualizační infrastruktury

Tato kapitola uvádí, jaké jsou roční náklady na virtualizační infrastrukturu v současném stavu. Jedná se o náklady na hardware a software, náklady na aplikační podporu - správu (lidské zdroje) a náklady na WAN (konektivita).

Náklady na aplikační podporu, či správu infrastruktury, jsou vyjádřeny ve formě superhrubé mzdy pracovníka a velikostí FTE (Full Time Equivalent - ekvivalent jednoho pracovníka na plný úvazek, či kapacita zatížení pracovníka, 1 FTE = 100 % kapacity pracovníka). Průměrná superhrubá mzda pracovníka IT oddělení činí 90 000 Kč měsíčně (tedy 1 080 000 Kč ročně). Jak ukazuje tabulka č. 4, při provozu serveroven v současném stavu je FTE rovno 1, tedy 1.080.000 Kč ročně.

Tabulka č. 4: Roční náklady na aplikační podporu (25)

Náklady na správu virtualizační infrastruktury			
Položka	Velikost FTE	Náklady na FTE	Náklady na FTE roční
Superhrubá mzda pracovníka IT	1	90 000 Kč	1 080 000 Kč

Položky tvořící náklady na zařízení a software tvořící virtualizační infrastrukturu v současné době, jsou rozepsány v tabulce č. 5. Náklady jsou detailně rozpadnuty na infrastrukturu jedné provozovny, přičemž jsou poté jednoduše zdvojeny, a tak jsou vyjádřeny náklady obou provozoven současně.

Tabulka č. 5: Roční náklady na hw a sw virtualizační infrastruktury v současném stavu (25)

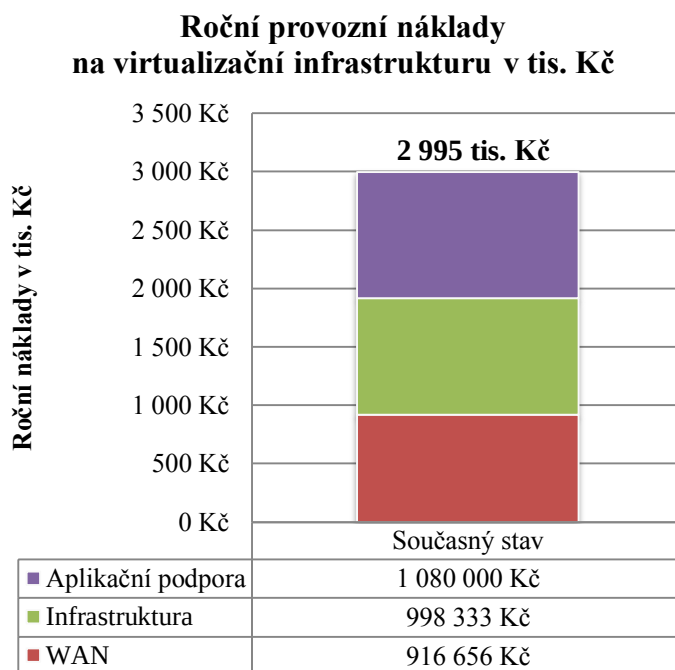
Roční náklady na hw a sw virtualizační infrastruktury v současném stavu			
Položka	Pořizovací náklady	Životnost (v letech)	Roční náklady
Hostitelé ESXi (2x)	300 000,00 Kč	3	100 000 Kč
Pásková zálohovací jednotka	200 000,00 Kč	5	40 000 Kč
Diskové pole SAN	500 000,00 Kč	4	125 000 Kč
SQL Server	200 000,00 Kč	3	66 667 Kč
Operační systémy serverů	300 000,00 Kč	3	100 000 Kč
Podpora VMware	135 000,00 Kč	2	67 500 Kč
Roční náklady na 1 provozovnu celkem:			499 167 Kč
Roční náklady na 2 provozovny celkem:			998 333 Kč

Náklady na WAN tvoří především pravidelné platby poskytovatelům připojení a pronájem routerů, jak je uvedeno v tabulce č. 6.

Tabulka č. 6: Roční náklady na WAN v současném stavu (25)

Roční náklady na WAN v současném stavu		
Položka	Provozovna	Náklady
Platba za VPN 4 Mb	B	551 846,52 Kč
Pronájem routeru	B	12 798,00 Kč
Platba za připojení 20 Mb	B	60 000,00 Kč
Rádiový spoj 320 Mb mezi budovami	B	49 215,60 Kč
Pronájem routeru č. 1	A	12 798,00 Kč
Platba za připojení 20 Mb č. 1	A	114 000,00 Kč
Pronájem routeru č. 2	A	12 798,00 Kč
Platba za připojení 50 Mb č. 2	A	103 200,00 Kč
Náklady na WAN za obě provozovny celkem:		916 656,12 Kč

Rozložení ročních provozních nákladů na virtualizační infrastrukturu v tis. Kč zachycuje graf č. 1.



Graf č. 1: Roční náklady na provoz virtualizační infrastruktury v současném stavu (25)

Jak je vidět z grafu č. 1, náklady na virtualizační infrastrukturu v současné době stojí podnik 2 994 989 Kč.

2.5 Současný stav serverových místností

V roce 2014 proběhl v obou lokalitách interní audit serveroven, který byl vyžadován ze strany CIT v zahraničí. Tento audit zahrnoval posouzení serveroven z hlediska jejich vybavení (racky, kabeláž), kontroly přístupu (zabezpečení, kontrolní systémy), zdrojů napájení (záložní zdroje, UPS), klimatizace, požární ochrany (hasící systémy, detektory kouře), ochrany proti vodě a výstražných hlásících systémů obecně.

Audit byl proveden formou kontrolního seznamu (checklistu), jehož výsledky jsou uvedeny v přílohách č. 9, 10, 11. Výsledkem tohoto auditu je zjištění současného stavu serveroven, včetně odhadu nákladů v EUR na nápravu nevyhovujících položek.

Lokalita A provozuje jednu serverovou místnost, kde jsou umístěny jak servery, tak síťové prvky a také telefonní ústředna. Tato serverová místnost má však spoustu nevyhovujících vlastností. Patří mezi ně především malý prostor, který způsobuje problémy s rozmístěním racků a dalších komponent. Následkem toho jsou nutné dvoje vstupní dveře do místnosti, které zajišťují přístup k rackům, jak zepředu, tak zezadu. Problém je také v kabelážním systému, chybí dostatečné značení kabelů a jejich organizace. I když jsou v místnosti umístěny dvě klimatizační jednotky, hardware se kvůli špatnému rozmístění a termocirkulaci nedaří optimálně chladit. Místnost navíc nedisponuje dvojitou podlahou, dále chybí sledování teploty a vlhkosti, není zde zabudováno zařízení proti neoprávněnému přístupu a protipožární dveře.

V lokalitě B jsou provozovány dvě serverovny, každá v jiném objektu. Jedna serverovna slouží jako telefonní ústředna a pro umístění síťových prvků (centrální switch), ve druhé jsou umístěny servery a koncové switche. Žádná ze serverových místností nedisponuje zdvojenou podlahou, protipožárními dveřmi a chybí monitoring neoprávněného vstupu. Místnosti mají uvnitř jednu klimatizační jednotku, kabelážní systém je nutné reorganizovat a lépe označit. Obě lokality nemají samostatný záložní zdroj energie ve formě naftového motorgenerátoru, jehož pořízení je velmi nákladné.

2.5.1 Náklady na rekonstrukci serveroven

Zjištěný současný stav serverových místností není z hlediska požadavků CIT vyhovující. Proto vedení společnosti rozhodlo o housingu serverů v externím datovém centru. V tomto případě musejí stávající serverovny projít menší modernizací a budou sloužit jako místnosti pro uložení switchů a telefonní ústředny. V příloze č. 12 jsou vyčísleny náklady na tuto rekonstrukci. Obsahují nejpodstatnější a nekritičtější položky kontrolního seznamu auditu a přesnější vyčíslení nákladů na nápravu zjištěných nedostatků v jednotlivých oblastech. Náklady na rekonstrukci pro dosažení provozní úrovně jako switchovny a/nebo telefonní ústředny činí v přepočtu 750.600 Kč.

2.6 Shrnutí analýzy

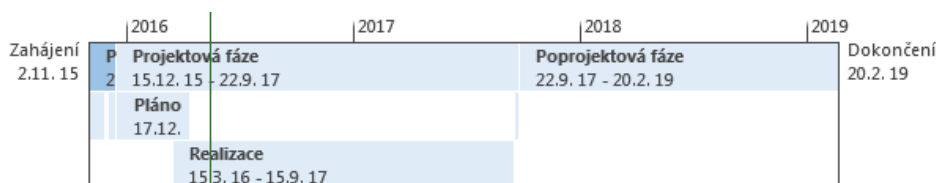
Ze studie příležitostí plyne, že pro podnik je dle současného stavu jeho ICT a nevyhovujícího stavu serverových místností, vhodná doba pro migraci virtualizační infrastruktury do datového centra. Přínosy jsou patrné především v oblasti bezpečného a spolehlivého provozu ICT, předcházení ztrátám dat a výpadkům IT systémů a zvýšení kvality poskytovaných služeb všem koncovým uživatelům. V rámci migrace virtualizační infrastruktury bude vhodné přesouvat hardware postupně, nikoli obě lokality najednou.

3 VLASTNÍ NÁVRHY ŘEŠENÍ

V této kapitole se budu na žádost investora (společnosti Dust CR), věnovat návrhu migrace části ICT infrastruktury do datového centra formou projektu. Struktura této kapitoly je rozdělena na studii příležitostí v rámci předprojektové fáze, dále doporučení pro projektovou a poprojektovou fázi. Nejprve je nutné sestavit hrubý plán projektu, poté vybrat hardware vhodný k přesunu a stanovit rychlost linky pro připojení. Na základě těchto i předešlých informací z kapitoly analýzy, provedu analýzu stakeholderů, zpracuji analýzu rizik vztahujících se k projektu a stanovím vhodná opatření pro významná rizika. Posledním bodem studie proveditelnosti je sestavení rozpočtu projektu. V rámci projektové fáze je nejprve třeba stanovit základní požadavky pro výběrové řízení na poskytovatele housingu a v návaznosti na to provést porovnání a výběr vhodného poskytovatele služby v datovém centru. Následně sestavím možný plán migrace, jak by mohl přesun virtualizační infrastruktury do DC probíhat. Závěrem vyhodnotím přínosy tohoto řešení pro společnost.

3.1 Plán projektu

Projektový plán jsem vytvořila v nástroji MS Project a je k dispozici v příloze č. 13. Projektový plán obsahuje tři základní fáze (předprojektová, projektová, poprojektová), každá fáze zahrnuje podstatné kroky pro úspěšnou realizaci projektu migrace. U činností v plánu jsem dobu trvání odhadla metodou brainstormingu na schůzce s projektovým týmem. Při termínu zahájení 2. 11. 2015, je plánovaný termín dokončení projektu stanoven na 20. 2. 2019, a to včetně jeho vyhodnocení po roce. Kritické úkoly jsou uvedeny v příloze č. 14 a uzlový síťový graf s kritickou cestou v příloze č. 15. Časový plán čistě projektové fáze je graficky znázorněn pomocí Ganttova diagramu v příloze č. 16. Na obrázku č. 18 je časová osa projektu, samotné dokončení projektové fáze je plánováno na 22. 9. 2017 (doba trvání cca 464 dnů) a zahrnuje Zahájení, Plánování, Realizaci a Ukončení projektové fáze.



Obrázek č. 18: Časová osa projektu (25)

3.2 Studie proveditelnosti

3.2.1 Upřesnění cíle projektu:

Cílem projektu je přesunout virtualizační ICT infrastrukturu obou lokalit společnosti Dust CR do externího datového centra, s délkou trvání projektové fáze nejdéle 2 roky a při dodržení rozpočtu projektu.

Charakteristika cíle projektu dle metody SMART:

S (strategic/significant) – přesun části ICT infrastruktury zcela jistě podporuje informační strategii společnosti a představuje udržitelnou formu provozu ICT. Pro společnost je tedy cíl projektu významný a to i z pohledu příležitosti pro rozvoj do budoucna.

M (measurable) – cíl je měřitelný, neboť bude snadno ověřitelné, jestli jej bylo dosaženo. Tedy jestli byl cíl projektu splněn z pohledu dodržení časového rámce, rozpočtu a splněn v požadované kvalitě a definovaném rozsahu.

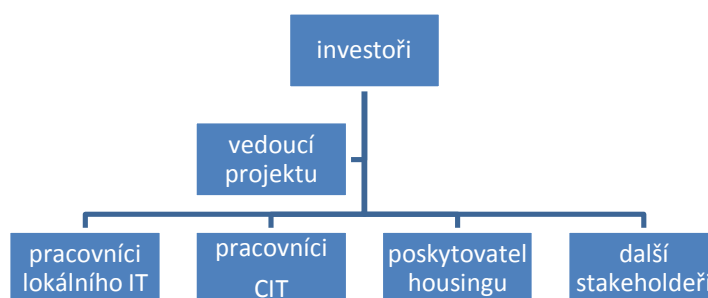
A (achievable/agreed) – cíl je zcela jistě dosažitelný a to jak z pohledu rozsahu tak časového rámce. Je rovněž pochopen, odsouhlasen a podporován ze strany CIT i vedení společnosti.

R (realistic) – přesun virtualizační infrastruktury do DC je reálný, nejedná se o experimentální záležitost, podobné projekty úspěšně realizovaly již dříve jiné společnosti.

T (timed) – cíl má stanovený časový rámec a je tedy termínovaný.

3.2.2 Organizační struktura projektu:

Sponzorem projektu bude společnost Dust CR v zastoupení jednatelů společnosti. Za realizaci a řízení projektu bude odpovědný vedoucí oddělení IT Dust CR. Do plánování a realizace celého projektu budou dále zapojeni především dva pracovníci lokálního IT jako projektový tým, ve spolupráci s pracovníky CIT, odpovědnými osobami ze strany poskytovatele housingu a další zainteresované osoby, jako stávající dodavatelé služeb (např. poskytovatel připojení). Schéma organizační struktury je uvedeno na obrázku č. 19.



Obrázek č. 19: Organizační struktura projektu (25)

3.2.3 Určení hardware k migraci do DC

Jako výchozí krok, pro další postup, je potřeba stanovit hardware, který se bude do DC přesouvat. Soupis hardware je uveden v tabulce č. 7. Jde především o stávající hardware tvořící virtualizační infrastrukturu, tedy hostitelské ESXi servery, zálohovací server, diskové pole SAN, páskovou zálohovací jednotku, ale je také o nový hardware. V rámci strategie CIT, musím vzít v potaz standard v oblasti infrastruktury, kterým jsou aktivní prvky od společnosti CISCO Systems. Proto nejsou stávající DELL switche vyhovující a musí se dokoupit nové CISCO switche. Rovněž v oblasti bezpečnosti jsou nutné firewally, taktéž CISCO. Pro připojení k matce se počítá také s CPE routery stávajících subdodavatelů. Ze stávajícího hardware virtualizační infrastruktury jsem vybrala hardware s co nejnižším stářím a nejlépe vyhovujícími parametry.

Tabulka č. 7: Hardware určený k migraci (25)

Zařízení	Účel	Stáří roky	Lokalita	Velikost U	Spotřeba W	Max. spotřeba W
DELL PowerEdge R530	Zálohovací server	2	B	2	200	320
DELL PowerEdge R620	Produkční ESXi server	3	B	1	200	320
DELL PowerEdge R620	Produkční ESXi server	3	B	1	200	320
Dell Equallogic PS4210	iSCSI SAN	1	B	2	320	750
Cisco C-3850 24x 1Gbps	Pátevní switch	0	-	1	60	110
Cisco C-3850 24x 1Gbps	Pátevní switch	0	-	1	60	110
DELL PowerVault TL2000 LTO6	Pásková mechanika	2	B	2	60	60
Dell Equallogic PS4100E	iSCSI SAN	3	A	2	320	750
DELL PowerEdge R720xd	Produkční ESXi server	3	A	2	320	540
CPE subdodavatel 1	Cisco Router	3	B	1	60	60
CPE subdodavatel 2	Cisco Router	3	B	1	60	60
Modem	Vzdálená správa pro CPE	3	B	0	5	5
Modem	Vzdálená správa pro CPE	3	B	0	5	5
Cisco ASA 5512-X	Firewall	0	-	1	350	350
Cisco ASA 5512-X	Firewall	0	-	1	350	350

Celková reálná spotřeba HW, který bude migrován do DC, činí 2 570 W a celková potřeba místa v racku pro tento hardware je 18 U. Tyto informace jsou důležité pro stanovení požadavků na poskytovatele housingu, neboť potřebujeme vědět, kolik místa v racku a s jakým příkonem budeme požadovat. Od těchto parametrů se bude také odvíjet cena housingu.

3.2.4 Stanovení rychlosti připojení

Na základě sledování provozu na síti, doporučuji zvolit rychlost připojení do MPLS sítě alespoň 100 Mbps. Pro připojení do datového centra doporučuji rovněž rychlost 100 Mbps, do sítě Internet taktéž. Je možné, že v reálném provozu bude nutná jiná rychlost připojení, bylo by tedy vhodné provést testovací provoz při různých rychlostech připojení. Aby byla zajištěna vysoká dostupnost, je nutné samostatné záložní připojení, bude tedy nezbytné vybudovat primární spoj a nezávislý záložní spoj.

3.2.5 Analýza zainteresovaných stran

Účelem analýzy zainteresovaných stran, neboli stakeholderů, je identifikace všech subjektů, které mají na splnění cíle projektu jakýkoliv vliv nebo zájem, zjištění velikosti tohoto vlivu či zájmu a stanovit směrem k nim vhodný způsob a strategii komunikace. Pro ohodnocení vlivu a/nebo zájmu dané zainteresované strany jsem definovala stupnici se slovní interpretací dle tabulky č. 8, pro posouzení významnosti a zvolení komunikační strategie stupnici dle tabulky č. 9.

Tabulka č. 8: Stupnice pro hodnocení vlivu a zájmu stakeholderů (25)

Vliv/zájem	
vysoký	4
střední	3
nízký	2
nevýznamný	1

Tabulka č. 9: Stupnice pro posouzení významu stakeholderů (25)

Posouzení významu zainteresovaných stran	
Nevýznamný = komunikační strategie není potřeba	<1;4)
Střední = komunikační strategie je doporučena	<4;8)
Kritický = komunikační strategie je nutná	<8;16>

Seznam stakeholderů projektu a stanovení komunikační strategie vůči nim je k dispozici v tabulce č. 10. Jako kritické stakeholdery jsem identifikovala management společnosti, CIT a poskytovatele hostingových služeb, tedy provozovatele datového centra. Vůči těmto zainteresovaným stranám je nutné zaujmout vhodnou komunikační strategii, tak aby byl projekt úspěšně dokončen s co nejvyšší pravděpodobností.

Posouzení významnosti stakeholderů slouží dále také jako podklad pro identifikaci rizik.

Tabulka č. 10: Analýza stakeholderů (25)

Číslo	Stakeholder / Zainteresaná strana	Popis zájmů/očekávání	Vliv	Zájem	Významnost	Komunikační strategie
1	Management	Vliv: financování a prosazování projektu, rozhodování o realizaci, přijetí/bojkotování změny, vliv na termín dokončení projektu Zájem: úspěšná realizace projektu, přínosy (kvalitativní, kvantitativní), snížení operativních nákladů na IT, optimalizace TCO	4	3	12	pravidelný reporting o stavu a vývoji projektu schvalování důležitých milníků vedení proti podpisu zapojení vedení do projektu
2	CIT Německo	Vliv: financování a prosazování projektu, rozhodování o realizaci, návrh bezpečnostních opatření, stanovení standardů v oblasti infrastruktury a bezpečnosti (platforma VMware, design firewallů a LAN) Zájem: úspěšná realizace projektu, přínosy, zjednodušení a zprůhlednění infrastruktury, standardizace, dodržování strategických rozhodnutí, optimalizace TCO	4	3	12	pravidelný reporting a meetingy o stavu a vývoji projektu schvalování důležitých milníků strategická rozhodnutí v rukou CIT zapojení pracovníků CIT do projektového týmu transparentní a podrobná projektová dokumentace
3	Poskytovatel housingu	Vliv: dokončení projektu v termínu, spolupráce při stěhování, dodržení smluvních podmínek, nastavení SLA, kvalita dodávky služeb a tím celková kvalita projektu, nastavení podmínek migrace, změna smluvních podmínek Zájem: úspěšná realizace projektu, dokončení v termínu při daných nákladech a nastavených podmínkách, dodávka WPs v požadované kvalitě a termínech, dlouhodobá spolupráce, dobré odběratelsko-dodavatelské vztahy, pravidelné platby za poskytované služby, rozšiřování poskytování služeb	4	4	16	zapojení kontaktní osoby do projektového týmu schůzky k projektu v předprojektové fázi v potřebné četnosti konkrétní formulace cíle projektu a zadání projektu oboustranné odsouhlasení konečného řešení projektu oboustranné výhodná smlouva o poskytování služeb a nastavení garance SLA
4	Subdodavatelé	Vliv: plnění termínů a kvality WPs, splnění projektu v termínu, dodatečné náklady na změny Zájem: dobré odběratelsko-dodavatelské vztahy, pravidelné platby za služby, udržení a prodloužení trávajícího kontraktu	3	2	6	informovat subdodavatele o termínech projektu a důležitých milnících
5	Koncoví uživatelé	Vliv: odpor ke změně Zájem: žádný dopad na koncového uživatele v oblasti uživatelského komfortu, nedotčení změnou	1	2	2	-

3.2.6 Analýza rizik

Analýza rizik slouží pro identifikaci možných hrozeb působících na projekt (ale také příležitostí plynoucích z projektu), jejich ohodnocení a následně jejich zvládání. To znamená, že u rizik, která identifikujeme jako významná, je nutné navrhnout opatření pro snížení jejich hodnoty. Pokud bychom na základě analýzy rizik zjistili, že projekt je vysoce rizikový, můžeme doporučit jeho nerealizaci.

Pro zpracování analýzy rizik, jsem použila jednoduchou metodu hrozba-scénář, kdy se identifikuje hrozba a její průběh (scénář), dále se na definované stupnici ohodnotí pravděpodobnost (P), že se hrozba projeví a dopad (D) v případě jejího výskytu. Následně vynásobením těchto dvou hodnot získáme celkovou hodnotu rizika (H), tj. $H = P \times D$.

Pro pravděpodobnost i dopad jsem si stanovila stupnici 1-4 se slovní interpretací dle tabulky č. 11.

Tabulka č. 11: Stupnice pravděpodobnost a dopad pro ohodnocení rizika (25)

Pravděpodobnost (P)		Dopad (D)	
vysoká	4	vysoký	4
střední	3	střední	3
nízká	2	nízký	2
nepravděpodobná	1	nevýznamný	1

Pro celkovou hodnotu rizika jsem definovala tři intervaly se slovní interpretací dle tabulky č. 12.

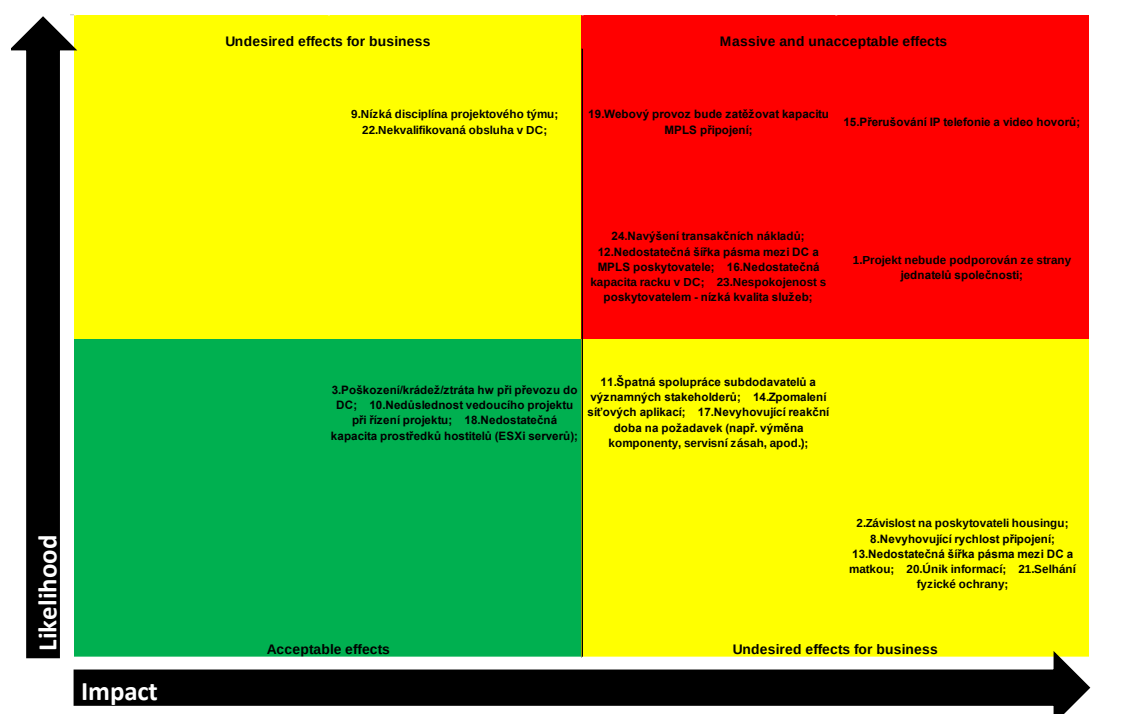
Tabulka č. 12: Intervaly pro určení celkové hodnoty rizika (25)

Celková hodnota rizika (H)	
Nízké a přijatelné riziko	<1;4)
Střední riziko	<4;8)
Vysoké a významné riziko	<8;16>

Seznam rizik a jejich ohodnocení je uveden v tabulce č. 13 a mapa rizik je zobrazena v grafu č. 2 na následující straně.

Tabulka č. 13: Analýza rizik projektu migrace do externího DC (25)

Č. rizika	Hrozba	Scénář	P	D	H
1	Projekt nebude podporován ze strany jednatelů společnosti	Bojkotování projektu, nespolupráce, prodloužení termínu dokončení projektu, omezení financí	3	4	12
2	Závislost na poskytovateli housingu	Nízká úroveň služeb, pozdější reakce na incidenty nebo na požadavky zákazníka, nižší operativní flexibilita	1	4	4
3	Poškození/krádež/ztráta při převozu HW do DC	Vznik nákladů v důsledku ztráty/poškození zařízení => zpoždění projektu a navýšení rozpočtu	1	3	3
4	Špatné zapojení HW/konfigurace serverů	Omezený provoz nebo zcela nefunkční provoz, zpoždění projektu	2	3	6
5	Problémy se SAN při migraci hw	Ztráta či poškození dat na SAN	3	4	12
6	Chyba při konfiguraci zařízení (pravidla na firewaltech, IP adresy)	Nefunkční konfigurace, nutná změna, prodloužení termínu projektu	2	4	8
7	Dlouhá doba odstávky z důvodu přesunu hw do DC	Příliš velké narušení kontinuity práce, dopad na business a zisk podniku	3	3	9
8	Nevyhovující rychlost připojení	Latence při přenosu Nespokojenost koncových uživatelů a omezení jejich práce	1	4	4
9	Nízká disciplína projektového týmu	Prodloužení termínů projektu a/nebo nedodržení požadované kvality projektu	2	2	4
10	Nedůslednost vedoucího projektu při řízení projektu	Prodloužení časového harmonogramu projektu a/nebo nedodržení požadované kvality projektu	1	3	3
11	Špatná spolupráce subdodavatelů a významných stakeholderů	Prodloužení termínů projektu a/nebo nedodržení požadované kvality projektu	2	3	6
12	Nedostatečná šířka pásma mezi DC a MPLS poskytovatele	Omezení plynulosti práce Nespokojenost koncových uživatelů	2	4	8
13	Nedostatečná šířka pásma mezi DC a matkou	Omezení plynulosti práce Nespokojenost koncových uživatelů	1	4	4
14	Zpomalení síťových aplikací	Omezení plynulosti práce Nespokojenost koncových uživatelů	2	3	6
15	Přerušování IP telefonie a video hovorů	Neschopnost používat tuto formu komunikace	4	4	16
16	Nedostatečná kapacita racku v DC	Dodatečné náklady na rozšíření nebo neschopnost se rozšířit u stávajícího poskytovatele a nutnost hledat jiného	2	4	8
17	Nevyhovující reakční doba na požadavek (např. výměna komponenty, servisní zásah, apod.)	Omezení kontinuity práce, nižší pružnost reakce ze strany poskytovatele na požadavky zákazníka, tedy nižší operabilita	2	3	6
18	Nedostatečná kapacita prostředků hostitelů (ESXi serverů)	Dodatečné náklady na rozšíření	1	3	3
19	Webový provoz bude zatěžovat kapacitu MPLS připojení	Omezení provozu, snížená rychlost/propustnost	4	3	12
20	Únik informací	Ztráta konkurenční výhody, poškození podniku, únik strategické informace	1	4	4
21	Selhání fyzické ochrany	Poškození HW a následná hrozba únik informací	1	4	4
22	Nekvalifikovaná obsluha v DC	Nevhodné zacházení s HW a plnění servisních služeb	2	2	4
23	Nespokojenost s poskytovatelem - nízká kvalita služeb	Nutnost odstoupení od smlouvy a hledání jiného řešení	2	4	8
24	Navýšení transakčních nákladů	Navýšení rozpočtu	3	3	9
25	Nutnost změny smluvních podmínek ze strany zákazníka	Dodatečné náklady na projekt	2	3	6
26	Neakceptování změny smluvních podmínek poskytovatelem	Zrušení smlouvy - utopené náklady, změna poskytovatele	2	3	6
27	Nevhodné uložení dat a nakládání s daty/aktivy	Odlíšný přístup k ochraně informací Obtížné vymáhání práva soudní cestou	1	3	3



Graf č. 2: Mapa rizik (25)

Rizika, která se nacházejí v červeném segmentu (vpravo nahoře), mají významný vliv na projekt, a proto je nutné přijmout opatření pro snížení jejich hodnoty. Také je vhodné uvažovat, zdali dané opatření s sebou nenesé dodatečné náklady a pokud je to možné, odhadnout jejich výši. Tato opatření snižují pravděpodobnost a/nebo dopad rizika a tak celkovou hodnotu sníženého rizika. Původní hodnoty významných rizik, opatření a snížené hodnoty rizik jsou v tabulce č. 14 na následující straně.

Tabulka č. 14: Opatření pro snížení významných rizik projektu (25)

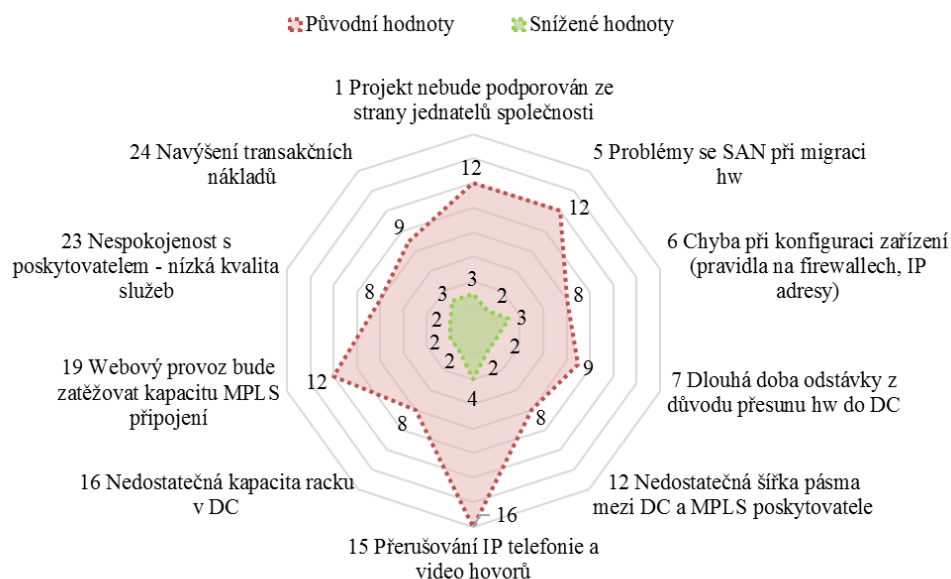
Č. rizika	Hrozba	Scénář	Původní			Opatření	Dodatečné náklady	Snížené		
			P	D	H			P'	D'	H'
1	Projekt nebude podporován ze strany jednatele společnosti	Bojkotování projektu, nespolečnost, prodloužení termínu dokončení projektu, omezení financí	3	4	12	Vyžadovat oficiální schválení projektu od vedení, schvalování důležitých milníků, zvolení vhodné komunikační strategie, pravidelný reporting o průběhu projektu	ne	1	3	3
5	Problémy se SAN při migraci hw	Ztráta či poškození dat na SAN	3	4	12	Zkušební replikace dat před ostrou replikací Vytvořit záložní kopii SAN na jinou SAN (zapůjčení)	10 000 Kč	1	2	2
6	Chyba při konfiguraci zařízení (pravidla na firewallch, IP adresy)	Nefunkční konfigurace, nutná změna, prodloužení termínu projektu	2	4	8	Otestování konfigurace na testovacím serveru - zapůjčení ESXi serveru	8 000 Kč	1	3	3
7	Dlouhá doba odstávky z důvodu přesunu hw do DC	Příliš velké narušení kontinuity práce, dopad na business a zisk podniku	3	3	9	Migrace na etapy (přesouvat virtualizační servery postupně) Využití dostatečné kapacity ESXi serverů	ne	1	2	2
12	Nedostatečná šířka pásma mezi DC a MPLS poskytovatele	Omezení plynulosti práce Nespokojenost koncových uživatelů	2	4	8	Navýšení šířky pásma	ano	1	2	2
15	Přerušování IP telefonie a video hovorů	Neschopnost používat tuto formu komunikace	4	4	16	Nastavení QoS	ne	2	2	4
16	Nedostatečná kapacita racku v DC	Dodatečné náklady na rozšíření nebo neschopnost se rozšířit u stávajícího poskytovatele a nutnost hledat jiného	2	4	8	Propočet nároků na místo a spotřebu v DC Smlouva s poskytovatelem o možnosti navýšení kapacity	ano	1	2	2
19	Webový provoz bude zatěžovat kapacitu MPLS připojení	Omezení provozu, snížení rychlosti/prostupnosti	4	3	12	Nastavení QoS	ne	1	2	2
23	Nespokojenost s poskytovatelem - nízká kvalita služeb	Nutnost odstoupení od smlouvy a hledání jiného řešení	2	4	8	Objektivně provedené výběrové řízení, kde jediným kritériem není cena	ne	1	2	2
24	Navýšení transakčních nákladů	Navýšení rozpočtu	3	3	9	Vytvoření finančního polštáře	50 000 Kč	3	1	3

Jak je vidět ze seznamu významných rizik, nejvíce hrozeb se v projektu může projevit při jeho realizaci, konkrétně tedy fyzicky při přesunu hardware a jeho konfiguraci na místě. Dále také při následném provozu, zde plynou hrozby týkající se rychlosti připojení a omezení kontinuity práce z důvodu zpoždění. Největší hodnotu rizika má přerušování IP telefonie, tato hrozba provozu dat na síti.

Navrženými opatřeními na rizika identifikovaná jako významná však dojde ke snížení hodnoty rizik na takovou úroveň, při níž je projekt realizovatelný a mohou doporučit jeho zahájení a realizaci.

Původní hodnoty významných rizik a nové, snížené hodnoty rizik jsou graficky znázorněny prostřednictvím pavučinového grafu č. 3. Zelená plocha představuje původní hodnoty, červená plocha snížené hodnoty významných rizik.

PAVUČINOVÝ GRAF RIZIK



Graf č. 3: Pavučinový graf významných rizik (25)

3.2.7 Rozpočet projektu

Plánovaný rozpočet na realizaci projektu se skládá z položek týkajících se přímo projektu, tj. nákladů na přesun virtualizační infrastruktury. Rozpočet tedy zahrnuje náklady na předimplementační analýzy, dále je nutné započítat náklady na nově pořízený hardware, tj. na páteřní switche a firewally CISCO. Musím také počítat s případnými náklady vyplývajících z analýzy rizik, tj. na zapůjčení hardware (SAN, ESXi server). Je vhodné připočíst i finanční polštář cca 50.000 Kč, včetně něj celkový rozpočet činí 378.000 Kč. Položky rozpočtu jsou uvedeny v tabulce č. 15.

Tabulka č. 15: Rozpočet projektu (25)

Položka	Náklad
Předimplementační analýzy	20 000 Kč
Zapůjčení ESXi serveru	8 000 Kč
Zapůjčení SAN (2x)	20 000 Kč
Nákup firewallů Cisco ASA 5512-X (2x)	120 000 Kč
Nákup switchů Cisco C-3850 24x 1Gbps (2x)	160 000 Kč
Celkem bez rezervy	328 000 Kč
Finanční polštář	50 000 Kč
Celkem včetně rezervy	378 000 Kč

3.3 Shrnutí studie proveditelnosti

Dle identifikovaných stakeholderů je nutné následovat navrženou komunikační strategii směrem k těmto zainteresovaným stranám, pro zajištění úspěšného průběhu a realizace projektu. Projekt obsahoval významná rizika, která se navrženými opatřeními povedlo snížit na takovou úroveň, kdy projekt není vysoce rizikový a lze jej doporučit k realizaci. Vzhledem k objemu dat (téměř 13 TB) a k navrhované rychlosti linky 100 Mbps, není možné tato data migrovat online, ale fyzicky úložiště dat do DC převést. Pro zajištění vysoké dostupnosti služeb v DC, bude nezbytná redundance linek. Kromě hardware, který již společnost vlastní, bude nutné také dokoupit nové prvky (switche, firewally).

3.4 Projektová fáze

Tato fáze obsahuje část Zahájení a Plánování, které slouží jako podklady pro Realizaci a následné Ukončení projektové fáze.

3.4.1 Zahájení

V rámci Zahájení, je výchozím krokem vytvoření zakládací listiny projektu (viz příloha č. 1) a její odsouhlasení vedením. Tímto bude projekt oficiálně uvolněn k dalším krokům projektové fáze.

3.4.2 Plánování

Tato část obsahuje plánovací aktivity, jejíž výstupy slouží jako podklady a plán pro samotnou realizaci projektu.

Stanovení kritérií pro výběrové řízení na poskytovatele housingu

Pro účely výběrového řízení, lokální oddělení IT stanovilo jejich požadavky na poskytovatele housingu v datovém centru. Tyto jsou sepsány přehledně v tabulce č. 16 níže. Požadavky na spotřebu a velikost místa v racku vycházejí z hardwaru určeného k přesunu, přičemž kapacita je pro jistotu mírně navýšena.

Tabulka č. 16: Požadavky na poskytovatele housingu v DC (25)

Požadavky na poskytovatele rack housingu v DC
Housing serverů a serverové techniky
Uzamykatelný rack, respektive část, o velikosti min. 18 (až 20 U)
Předpokládaná reálná spotřeba max. 3 000 W
Min. konektivita DC 1 Gbps, zálohovaná konektivita
Rychlost linky min. 100 Mbps, nepočítaná přenesená data
Zálohovaný zdroj el. energie - diesel agregáty, elektrocentrála - bez nutnosti použít vlastní UPS
Dostupnost datového centra - dojezd do 2 h z lokality B
Bezpečnost - řízený přístup, kamery, ostraha 24x7
Automatický hasicí systém
Lokální podpora, dohled 24x7
Minimální dostupnost 99 %
Možnost do budoucna přejít na řešení v privátním cloudu

Vysoká priorita, co se týče výběrových kritérií, je přisuzována zabezpečení datového centra a dostupnosti. Proto bud při výběrovém řízení zohledňovat dosaženou úroveň TIER, a zdali má DC i certifikaci od společnosti Uptime Institute, protože pouze u certifikovaného DC jsou zajištěny proklamované parametry. Dále bude zohledněna certifikace normy ISO 27001 a managementu kvality obecně. Důležitá je také konektivita a napájení datového centra el. energií a způsob zálohování obojího. Společnost si přeje, aby datové centrum bylo na dojezd do 2 h z lokality B, kvůli zajištění operability lokálních IT pracovníků.

Srovnání nabídek poskytovatelů housingu

V této části popíšu nabídky na hostingové služby dvou významných poskytovatelů ICT služeb, jedná se o mobilní operátory. Tyto společnosti mají postavena datová centra pro své vlastní účely a rozhodly se nabízet služby datového centra i dalším subjektům. Díky tomu, že v těchto datových centrech provozují i vlastní ICT infrastrukturu, splňují DC vysoké nároky kladené jak na výstavbu a provoz, tak na bezpečnost a dostupnost.

Cenová nabídka poskytovatele A

Provozovatel A disponuje v tuto chvíli na území České Republiky datovými centry v Praze, Ostravě a Brně, přičemž nejbližší se nachází DC Brno (dojezd 1,5 h z lokality B). Poskytovatel A pro zřízení VPN nabízí službu IP VPN, kterou provozuje na síti s MPLS protokolem. Díky tomu je každá VPN bezpečně oddělena od ostatních VPN sítí i veřejné

sítě internet. Pro obě lokality bude služba IP VPN zajištěna pomocí přenosové technologie mikrovln (MW), na jednom primárním spoji a druhém nezávislém redundantním spoji o rychlosti 100 Mbps. Aby poskytovatel zajistil nezávislost přípojných tras, v lokalitě B bude pro primární linku použit spoj od provozovatele A, pro záložní linku spoj od subdodavatele. V lokalitě A lze jak pro primární linku, tak pro záložní linku, využít spoje od subdodavatelů. Služba IP VPN bude takto v obou lokalitách plně redundantní. Pro připojení VPN do datového centra nabízí poskytovatel službu IP VPN s rychlostí 200 Mbps a do sítě internet službu Profesionální internet o rychlosti 100 Mbps. V rámci nabídky server housingu, poskytovatel nabízí pronájem jednoho uzamykatelného racku pro umístění fyzických serverů. Dále za příplatek nabízí doplňkovou službu remote hands – vzdálenou podporu techniků v DC. Pro uchování datových zálohovacích pásek lze využít ohnivzdorný trezor. Další doplňkovou službou je QoS, která umožňuje alokovat kapacitu linek do servisních tříd, kdy každá třída garantuje výkonnostní parametry (zpoždění, apod.) pro aplikace v dané třídě. V tabulce č. 17 jsou uvedeny jednorázové náklady na housing a v tabulce č. 18 pravidelné měsíční náklady za nabízené služby. Ceny jsou platné v rámci nabídky hostingových služeb pro Dust CR, s.r.o.

Tabulka č. 17: Jednorázové náklady na housing – nabídka od poskytovatele A (25)

Jednorázové náklady na housing poskytovatel A				
Položka	Množství	Lokalita	Název služby	Cena v Kč
Instalace služby IP VPN primární	100 Mbps	B	IP VPN	1 Kč
Aktivace služby IP VPN záložní	100 Mbps	B	IP VPN	- Kč
Instalace služby IP VPN primární	100 Mbps	A	IP VPN	1 Kč
Aktivace služby IP VPN záložní	100 Mbps	A	IP VPN	- Kč
Instalace služeb datového centra	1 ks	DC	Služby DC	7 500 Kč
Aktivace služby IP VPN připojení do DC	200 Mbps	DC	IP VPN	1 Kč
Aktivace služby Profesionální internet	100 Mbps	DC	Profesionální internet	1 Kč
Jednorázové náklady celkem				7 504 Kč

Tabulka č. 18: Pravidelné měsíční platby za housing – nabídka od poskytovatele A (25)

Pravidelné měsíční platby za housing poskytovatel A				
Položka	Množství	Lokalita	Název služby	Cena v Kč/měsíc
IP VPN primární MW	100 Mbps	B	IP VPN	12 500 Kč
IP VPN záložní MW	100 Mbps	B	IP VPN	12 500 Kč
IP VPN primární MW	100 Mbps	A	IP VPN	12 500 Kč
IP VPN záložní MW	100 Mbps	A	IP VPN	12 500 Kč
Housing, pronájem racku 24 U	1 ks	DC	Datacentrum	14 500 Kč
Spotřeba el. energie	3 kW	DC		9 750 Kč
Služba remote hands	2 h	DC	Remote hands	1 980 Kč
Služba IP VPN připojení do DC	200 Mbps	DC	IP VPN	8 000 Kč
Služba Profesionální Internet	100 Mbps	DC	Profesionální internet	3 800 Kč
Pravidelné měsíční platby celkem				88 030 Kč

Cenová nabídka poskytovatel B

Provozovatel B má v tuto chvíli na území České Republiky datová centra v Hradci Králové a v Praze. Všechna jeho datová centra mají certifikaci TIER III Uptime Institute na Design. DC Hradec Králové je z nich nejmladší, bylo vystavěno v roce 2008 a z lokality B je cca 1,5 h jízdy autem, čili je vhodným kandidátem do výběrového řízení na poskytovatele server hostingu.

Nabídka DC v Hradci Králové, je založena na službě IP Connect, která umožňuje vybudovat virtuální privátní síť (VPN), zřídit primární přípojky pro lokalitu B a A optickým kabelem a spustit na nich službu s názvem IP Connect Giga Optics na rychlosti 100 Mbps pro připojení k páteřní síti poskytovatele. V obou těchto lokalitách bude nutné zřídit záložní nezávislou přípojku pomocí rádiového spoje (MW) se službou IP Connect Giga Optics, rovněž s rychlostí 100 Mbps. Tímto způsobem zálohovaného připojení bude dosaženo takové úrovně SLA, která se vyznačuje garantovanou dostupností 99,9 %, maximální délkou poruchy 4 hodiny, odezvou do 60 minut, nezávislým záložním připojením a slevou za nedodržení garantovaných parametrů na pronájem přípojky IP Connect v následujícím období. Pro připojení VPN obou lokalit do datového centra, poskytovatel nabízí službu IP Connect Hostingové centrum s rychlostí přípojky 100 Mbps prostřednictvím páteřní sítě s využitím protokolu MPLS a s doplňkovou službou QoS, součástí je i záložní 100 Mbps linka do DC.

Pro připojení VPN do sítě internet poskytovatel nabízí službu IP Connect Internet s rychlostí 100 Mbps. Konektivita mezi datovým centrem a matkou v zahraničí, bude zajištěna prostřednictvím stávající mezinárodní přípojky.

Nabízené řešení vyžaduje zákaznická koncová zařízení (CPE – Customer Premises Equipment), která jsou umístěna přímo v lokalitě u zákazníka. Dále řešení vyžaduje přístupovou síť (Ethernet, ATM) a pátevní IP síť vystavenou na Cisco routerech a protokolu MPLS. Služba IP Connect je realizována výhradně na hardwaru a datových okruzích společnosti B a v rámci této služby je zajištěna konfigurace okruhů, dodávka, instalace, konfigurace a vzdálená správa CPE u zákazníka.

V tabulce č. 19 jsou uvedeny nabízené služby a jejich cena, která je platná pro firmu Dust CR, v rámci poptávky po hostingových službách.

Tabulka č. 19: Pravidelné měsíční platby za housing – nabídka od poskytovatele B (25)

Pravidelné měsíční platby za housing poskytovatel B				
Položka	Množství	Lokalita	Název služby	Cena v Kč/měsíc
Přípojka optiky primární	100 Mbps	B	IPC GO I	18 320 Kč
Přípojka optiky primární	100 Mbps	A	IPC GO I	23 266 Kč
Přípojka záložní MW	100 Mbps	B	IPC GO II	- Kč
Přípojka záložní MW	100 Mbps	A	IPC GO II	- Kč
Připojení do Internetu	100 Mbps	DC	Internet hosting	1 970 Kč
Připojení do datového centra	100 Mbps	DC	IPC hosting	1 Kč
Služby datového centra	1 ks	B	SLA 3	5 496 Kč
Služby datového centra	1 ks	A	SLA 3	6 980 Kč
Záložní linka (z MPLS do DC)	100 Mbps	DC	SLA 3	3 000 Kč
Služby datového centra	1 ks	B	IPC Proaktiv	100 Kč
Služby datového centra	1 ks	A	IPC Proaktiv	100 Kč
Housing, pronájem racku 20U, příkon 2,9 kW	1 ks	DC	20U	14 900 Kč
Služba remote hands	2 h	DC	Remote hands	500 Kč
Uložení pásek se zálohou	25 ks	DC	Tape secure deposit	1 000 Kč
Pravidelné měsíční platby celkem				75 633 Kč

Souhrnné porovnání nabídek poskytovatelů hostingů

Tabulka č. 20 na následující straně, srovnává nabídky obou poskytovatelů. Pro každé uvedené kritérium je stanovena váha (od 0 do 4), tj. důležitost a vliv na výběrové řízení. Nejvyšší váhu 4, má certifikace TIER. Jak je vidět, certifikaci od Uptime Institute má pouze datové centrum poskytovatele B. Poskytovatel A uvádí, že jeho datové centrum je provozováno na úrovni TIER III, ovšem tato informace není podložena certifikátem,

jehož získání je velmi finančně a časově náročný proces, a datové centrum musí splnit velmi přísná kritéria.

Jak je vidět z dalších uvedených kritérií, obě datové centra jsou téměř na stejné úrovni, která je velmi vysoká. Obě mají certifikaci ISO 27001, důkladně pokryto fyzické zabezpečení objektu, protipožární systém a nabízejí rovněž podobné doplňkové služby. Společnost B je navíc zapojena do projektu FENIX, jehož smyslem je v případě DoS útoku zajistit dostupnost internetových služeb subjektů, které jsou členy toho projektu, což představuje zajištění vysoké dostupnosti a zabezpečení sítě. Poskytovatel B nabízí připojení na vlastní komunikační infrastrukturu, poskytovatel A má tyto služby zajištěné od subdodavatelů. Co se týče celkového počtu bodů, nabídka od poskytovatele A ve výběrovém řízení dosáhla 139 bodů, nabídka od poskytovatele B 178. Na základě stanovených kritérií a dosaženém počtu bodů, doporučuji jako poskytovatele server housingu vybrat datové centrum v Hradci Králové, provozované poskytovatelem B.

Tabulka č. 20: Porovnání nabídek housingu (25)

Kritérium	Váha	Poskytovatel A	Body A	Poskytovatel B	Body B
Rok založení	1	1999	1	2008	3
TIER úroveň	4	na úrovni TIER III, bez certifikace	1	certifikace Uptime Institute TIER III - Design	3
Prostor v racku	2	24U	3	20U	2
Zálohované napájení	3	ANO, diesel + UPS	3	ANO, diesel + UPS	3
Příkon	2	3000 W	2	2900 W	3
Dva okruhy napájení v racku	2	ANO	3	ANO	3
Kapacita poskytovaných portů	2	100 Mbps, 1 Gbps, 10 Gbps	3	od 100 Mbps do 10 Gbps	3
Konektivita DC	2	2x20 Gbps	2	2x100 Gbps	3
Mezinárodní konektivita DC	2	2x10 Gbps	2	2x100 Gbps	3
Zálohovaná konektivita DC	3	ANO, dvě nezávislé optické trasy	3	ANO, dvě nezávislé optické trasy	3
Topologie	3	kruhová	3	kruhová	3
Dostupnost	3	99,99 (max. doba výpadku 1,6 h)	3	99,99 (max. doba výpadku 1,6 h)	3
Lokalita	3	Brno	3	Hradec Králové	3
Fyzické zabezpečení	3	CCTV, biometrická kontrola vstupu v kombinaci s personální HID kartou a pinem, fyzická ostraha 24/7, dvě bezpečnostní závory, senzory otevření dveří na všech přístupech, dálkově řízené magnety na dveřích, uzamykatelné racky	3	kamerové systémy (CCTV), ostraha 24x7, autorizace osob HID kartou a PIN, uzamykatelné racky s možností individuální identifikace a kamerových okruhů, bezpečnostní perimetr DC napojen na PČR	3
Protipožární systém	2	ANO, plyn FM200	3	ANO, plyn FM200	3
Certifikace	3	ISO 27000	2	ISO 27001:2005, ISO 9001:2008, ISO 18001:2007, ISO 14001:2004, ISO 20000-1:2011	3
Telekomunikační řešení	2	Lokalita B - primární MW spoj od poskytovatele A, záložní MW spoj od subdodavatele Lokalita A - MW spoje od subdodavatelů	3	vlastní telekomunikační infrastruktura	3
Podpora na dálku (remote hands)	2	ANO	2	ANO, 24x7	3
Asistence při instalaci	2	na vyžádání	2	ano	3
Další služby	2	KVM over IP firewall SIEM trezor pro uložení páse	3	KVM over IP možnost využití skladu pro uložení technologií zákazníka konfigurační místnost firewall trezor pro uložení pásek	3
Člen projektu FENIX (bezpečná síť)	3	NE	0	ANO	3
Nabízené připojení	3	Lokalita A i B - mikrovlny: - služba IP VPN primární 100 Mbps - služba IP VPN záložní 100 Mbps Připojení do datového centra: - služba IP VPN 200 Mbps Připojení do sítě Internet: - služba Profesionální Internet 100 Mbps	2	Lokalita A i B - optika: - služba IP Connect Giga Optics primární 100Mbps Lokalita A i B - mikrovlny: - služba IP Connect Giga Optics záložní 100Mbps Pro připojení do datového centra: - služba IP Connect Hostingové centrum 100Mbps - záložní linka 100 Mbps Pro připojení do sítě internet - služba IP Connect Internet 100Mbps	3
Pravidelné měsíční platby za nabízené připojení	2	88 030,00 Kč	2	75 633,00 Kč	3
Jednorázové náklady	2	7 504,00 Kč	2	- Kč	3
Termín realizace od uzavření smlouvy	2	do 8 týdnů	2	do 4 týdnů	3
		Body celkem:	139		178

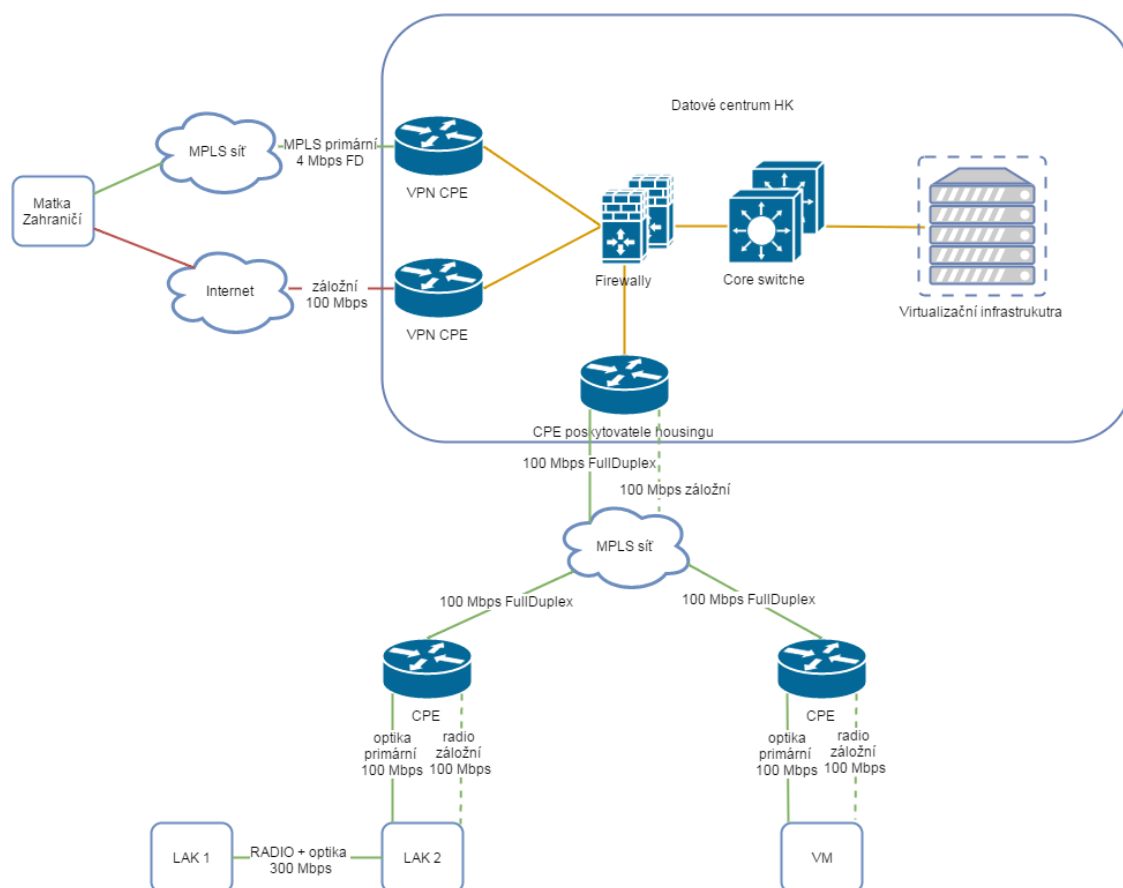
Plán migrace

V rámci příprav přesunu části ICT infrastruktury do datového centra je potřeba nejprve navrhnout způsob zapojení WAN sítě mezi oběma lokalitami a datovým centrem. Také je potřeba definovat způsob zapojení LAN sítě v datovém centru. Poskytovatel rovněž musí připravit spoje pro připojení optiky a zprovoznit na nich své služby k zajištění konektivity. Následuje příprava prostoru v datovém centru a přichystat rack pro zařízení společnosti Dust CR. Po dodávce služeb od stávajících subdodavatelů, bude následovat otestování nastavení na zapůjčeném hardware. Poté se provede přidělení nových adresních prostorů. Následně může začít migrace hardware, která bude probíhat na etapy, nejprve lokalita B, poté A.

Návrh schéma WAN

Návrh zapojení sítě WAN stojí na routování veškerého provozu přes MPLS síť poskytovatele datového centra. Veškerý provoz tak bude v obou lokalitách směřován přes dvě primární 100 Mbps optické spoje a dvě záložní 100 Mbps mikrovlnné spoje, s automatickým převzetím při výpadku (failover). Řešení vyžaduje koncová zákaznická zařízení (CPE), kdy toto CPE u zákazníka bude do MPLS sítě poskytovatele připojeno 100 Mbps FullDuplex linkou. Spoj z MPLS sítě k CPE u poskytovatele, bude připojen rovněž primární 100 Mbps FullDuplex linkou a záložní 100 Mbps linkou. Dále bude nezbytné, aby veškerá data procházela přes firewall, který bude umístěn na straně datového centra u poskytovatele a tím bude zajištěn zabezpečený tok dat.

Spojení s mateřskou firmou do zahraničí a mezi datovým centrem, bude na žádost investora zajištěno primární MPLS 4 Mbps linkou a redundantní 100 Mbps linkou přes síť internet. Toto spojení bude zajišťovat stávající poskytovatel (subdodavatel 1), který řeší připojení k mateřské firmě v současné době. Nastavení switchů a firewallů v datovém centru, a zařízení na straně zákazníka, bude řešit stávající subdodavatel (subdodavatel 2) síťových služeb. Schéma sítě WAN je uvedeno na obrázku č. 20.



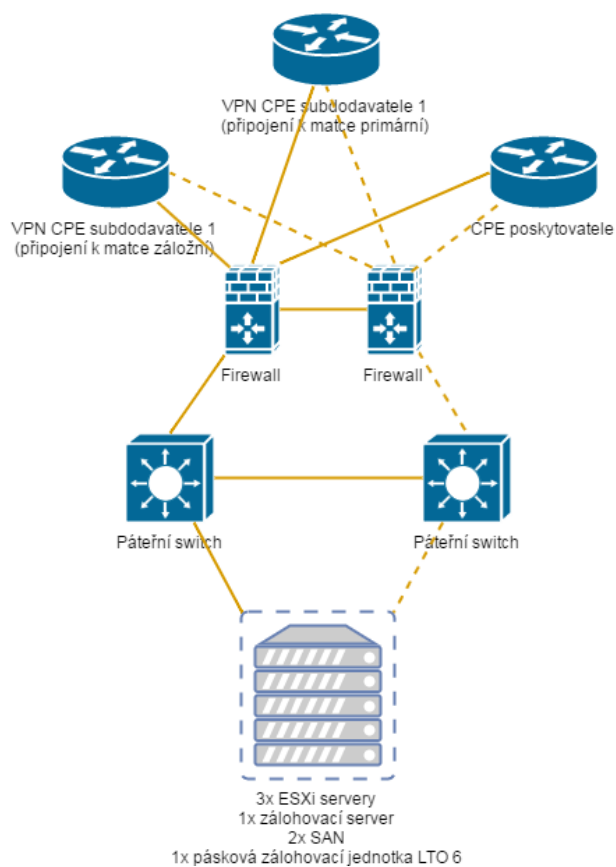
Obrázek č. 20: Návrh schéma WAN (25)

Zařízení LAN sítě v DC

V rámci server hostingu bude pro infrastrukturu vyhrazen uzamykatelný rack s prostorem 20 U. Zde se budou nacházet zařízení společnosti Dust CR určená k přesunu dle kapitoly 3.2.3. Přesouvat se tedy budou tři hostitelské servery ESXi, zálohovací server, pásková zálohovací jednotka LTO 6, obě diskové pole SAN a nově pořízený hardware, tj. Cisco switche a firewally. Koncové zařízení CPE poskytovatele hostingů a CPE subdodavatele 1 (pro připojení k matce), budou umístěna rovněž uvnitř racku. Seznam zařízení je uveden v tabulce č. 21 a schéma zapojení na obrázku č. 21 na následující straně. Aktivní prvky budou zapojeny redundantně, pro případ výpadku jednoho z nich.

Tabulka č. 21: Umístění hardware v datovém centru (25)

Zařízení	Účel	Umístění	Velikost U
DELL PowerEdge R530	Zálohovací server	uvnitř racku	2
DELL PowerEdge R620	ESXi server	uvnitř racku	1
DELL PowerEdge R620	ESXi server	uvnitř racku	1
DELL PowerEdge R720xd	ESXi server	uvnitř racku	2
Dell Equallogic PS4210	iSCSI SAN	uvnitř racku	2
Dell Equallogic PS4100E	iSCSI SAN	uvnitř racku	2
DELL PowerVault TL2000 LTO6	Pásková mechanika	uvnitř racku	2
Cisco C-3850 24x 1Gbps	Páteční switch	uvnitř racku	1
Cisco C-3850 24x 1Gbps	Páteční switch	uvnitř racku	1
Cisco ASA 5512-X	firewall	uvnitř racku	1
Cisco ASA 5512-X	firewall	uvnitř racku	1
CPE subdodavatel 1	Cisco router	uvnitř racku	1
CPE subdodavatel 2	Cisco router	uvnitř racku	1
CPE poskytovatel hostingu	Cisco router	uvnitř racku	1
Modem	Vzdálená správa pro CPE	mimo rack	-
Modem	Vzdálená správa pro CPE	mimo rack	-
Celkem zabraný prostor v racku (U)			19



Obrázek č. 21: Schéma LAN v DC (25)

Návrh rozdělení přenášených dat do tříd dle priorit

Na základě systémů a aplikací, které společnost Dust CR používá, navrhuji rozdělit komunikaci dle priorit přenosu v síti do tříd QoS (Quality of Service). VOIP telefonie má nejvyšší prioritu, co se týče nároků na přenos, a je nezbytné tato data přenášet v reálném čase. Dále je nutné zajistit komunikaci produkčních systému (ERP systém), pro plynulý chod výroby a uživatelský komfort zaměstnanců při práci s těmito systémy. Následuje zajištění managementu sítě jako řízení uživatelských účtů a domén, dále přenos dat aplikací, přenos souborů a externí komunikace jako přenos firemní pošty, zálohování dat a komunikace do internetu. Rozdělení QoS je uvedeno v tabulce č. 22.

Tabulka č. 22: Návrh rozdělení přenášených dat do tříd dle priorit (25)

Třída QoS	Popis	Určení
1	Reálný čas	VOIP
2	Data 1	ERP systém
3	Management	AD, DHCP, DNS WiFi controller WMware
4	Data 2	SQL server Aplikační servery
5	Data 3	Souborové služby
6	Externí	WEB (proxy) Pošta Antivirus Zálohování

Rozdělení virtuálních strojů na hostitele

Jelikož nyní virtualizační infrastruktura obsahuje 4 hostitele ESXi a v rámci migrace a konsolidace serverů budou postačovat pouze 3 hostitele, bude potřeba přerozdělit virtuální stroje na tyto tři fyzické servery. Na všech hostitelích se nyní dohromady nachází 47 virtuálních strojů, přičemž na každém z nich je průměrně 12 VMs. Lze tedy tyto virtuální stroje přerozdělit na 3 hostitele rovnoměrně, 2x po 16 a 1x po 15 VMs. V příloze č. 17 je návrh, jak by toto rozdělení mohlo vypadat. Do budoucna se také počítá s konsolidací serverů, neboť při jednotné správě je zbytečné provozovat více virtuálních serverů se stejnou funkcionalitou. Efekt konsolidace se projeví v úspoře vytížení zdrojů, a to jak dedikovaných zdrojů virtualizačního hardware, tak v úspoře času lidských zdrojů pro správu virtuálních serverů. Dále tam, kde lze sloučit práci uživatelů ze dvou stejných, ale oddělených aplikací do jedné společné, se dá předpokládat i úspora za licence sw.

Způsob migrace hardware

Přesun hardware se musí uskutečnit až ve chvíli, kdy budou provedeny všechny přípravy pro přesun. V datovém centru v racku již musejí být dovezeny a přichystány switche, firewally a CPE. Dopředu také musí být přichystány nové IP adresy. Jejich přidělování proběhne formou routování. Změní se DNS servery na firewallech, klienti při dotazu na stávající DNS budou přesměrováni na nový DNS server, kde obdrží nové IP adresy. Migrace bude probíhat na etapy, kdy v 1. etapě bude přesunuta do datového centra virtualizační infrastruktura lokality B a po jejím zprovoznění, bude s malým časovým odstupem přesunuta v 2. etapě virtualizační infrastruktura lokality A. V lokalitě B se nejprve odpojí ESXi servery od sítě, provede se záloha diskového pole z důvodu prevence ztráty či poškození dat při přesunu. Jeden server a zapůjčená SAN se zálohou zůstanou v lokalitě B, druhý server a SAN se převezí do DC, kde se zařízení namontují do racku a zapojí se. Po tu dobu, budou služby provozovány ze zbývajících částí infrastruktury, která zůstane v lokalitě B, tedy jeden ESXi server, zálohovací server a pásková zálohovací jednotka. Tato se s časovým odstupem 1 týdne přesune rovněž do DC, poté bude obnoven redundantní stav serverů (failover) a virtualizační infrastruktura bude plně provozována z datového centra. Tímto bude dokončena 1. etapa migrace. V rámci 2. etapy bude přesunuta virtualizační infrastruktura lokality A, kdy se rovněž odpojí servery od sítě, provede se záloha SAN a do DC se přesune jeden server a SAN. Další hardware se již přesouvat nebude. Od této chvíle bude virtualizační infrastruktura a aplikace provozovány plně z datového centra, a to na třech ESXi serverech, dvou SAN, zálohovacím serveru a páskové zálohovací jednotce LTO 6. Díky tomu, že fyzické ESXi servery mají dostatečnou kapacitu na to, aby všechny virtuální stroje byly hostovány na jednom serveru, lze hardware přesunout postupně. Tímto se zkrátí doba odstávky serverů. Je nezbytné v dostatečném předstihu informovat všechny koncové uživatele odstávce, neboť po určitou dobu budou zařízení off-line a uživatelé nebudou moci pracovat. Informace o odstávce je možné poslat uživatelům emailem a to alespoň 3 dny předem, s následujícím připomenutím v den blackoutu. Díky tomu, že část hw bude v DC již nachystán, a pokud půjde vše podle plánu, doba odstávky by neměla trvat déle než 7 hodin. Doba na odpojení, zálohování a převoz poloviny infrastruktury do DC odhaduji na cca 4 hodiny. Poté je třeba infrastrukturu na místě zapojit (cca půl hodiny), nahrát potřebné síťové konfigurace a otestovat funkčnost, což odhaduje celkově asi na 3 hodiny.

Způsob migrace dat

Celkový objem dat uložených na diskových polích SAN, pro obě lokality, činí 12,83 TB. V lokalitě B jde o objem dat 3,55 TB, v lokalitě A pak o 9,28 TB. Z důvodu 100 Mbps linky, není možné takovýto objem dat po síti migrovat, neboť by to trvalo cca 80 hodin pro lokalitu B cca 216 hodin pro lokalitu A. Jelikož tedy nebude možné provést migraci po síti, bude nutné přesun dat provést off-line. To znamená, že se provede záloha aktuálních dat na jiné úložiště a stávající diskové pole se fyzicky převezou do datového centra. Záloha dat je nutná pro případ poškození SAN při převozu nebo jiné příčiny, která může způsobit ztrátu dat. Pro tyto účely je potřeba zapůjčit diskové pole SAN, na které se budou data zálohovat.

Doporučená doba pro migraci

Aby byl dopad odstávky na uživatele a chod podniku co nejmenší, doporučuji stanovit čas pro migraci mimo pracovní dobu. Vhodné by bylo plánovat dobu odstávky na datum a čas, kdy probíhá celozávodní dovolená. Vzhledem k tomu, že v lokalitě B se pracuje v režimu nepřetržité pracovní doby, není možné toto uskutečnit. Šlo by tedy odstávku a migraci realizovat o víkendu, v tomto případě by však bylo nutné mít zajištěnou technickou podporu subdodavatelů a poskytovatele housingu v případě výskytu problémů. Je také možné provést migraci v pracovní dny a dobu, tímto však dojde k výpadku lokálně provozovaných služeb na dobu cca 7 hodin.

Služby ovlivněné migrací

Migrací, potažmo odstávkou, budou ovlivněny služby, které jsou provozovány lokálně, a nebudou tedy po její dobu uživatelům k dispozici. Migrace se nedotkne služeb provozovaných centrálně.

3.4.3 Realizace a ukončení

Po ukončení plánovacích aktivit, bude následovat realizace projektu, kdy fyzicky dojde k přesunu hardware tak, jak navrhuje plán migrace. Po dokončení přesunu lze projektovou fázi administrativně ukončit, vyhotovit report o průběhu projektu (např. ve formě závěrečné zprávy projektu – viz příloha č. 2), předat projekt vedení a uvolnit projektový tým.

3.5 Shrnutí projektové fáze

V projektové fázi, jsem objektivním způsobem nejprve vybrala vhodného poskytovatele housingu, následovalo sestavení plánu migrace. Ten obsahuje návrh sítě WAN, způsob zapojení prvků virtualizační infrastruktury v racku v datovém centru a samotný způsob migrace hardware a dat, který je navržen tak, aby odstávka infrastruktury byla co nejkratší a měla co nejmenší dopad na uživatele a business.

3.6 Poprojektová fáze

V rámci poprojektové fáze je vhodné projekt vyhodnotit s časovým odstupem po jednom roce od ukončení projektové fáze, aby se daly jasně a přesně vyčíslit skutečné náklady spjaté s provozem virtualizační infrastruktury v DC. Poté musíme zkontrolovat a archivovat veškerou dokumentaci, která vznikla v průběhu projektu a projekt zcela ukončit.

3.6.1 Uložení projektové dokumentace a uzavření projektu

Během projektu již bylo a jistě ještě bude vytvořeno množství analýz, plánů, schémat, smluv a dalších. Tyto musejí být správně ukládány a u všech dokumentů doporučuji uchovávat i jejich verze, tak jak se postupně obsahově měnily a upravovaly, včetně označení finální schválené verze dokumentu. Toto zajistí zpětnou dohledatelnou a v případě nejasností, dohadů či vzniku chyb je dokumentace a její verze nepostradatelná. Následně po kontrole dokumentace, je nutné ji archivovat na vhodné místo. Uložení, kontrola a archivace projektové dokumentace je v kompetenci vedoucího projektu.

3.6.2 Přínosy migrace ICT infrastruktury do DC

U projektu můžeme vyhodnotit jak ekonomické přínosy, tedy kvantitativní, tak přínosy kvalitativní. Kvalitativní přínosy vstupují do určení poměru ceny/kvality/přidané hodnoty projektu, podle kterého je vhodné hodnotit investice do ICT.

Ekonomické přínosy

V rámci projektu migrace a housingu virtualizační infrastruktury v externím DC, by v obou lokalitách bylo nutné zajistit konektivitu do MPLS sítě poskytovatele a směrem do datového centra (s rychlostí 100 Mbps). V tomto případě by z datového centra postačovala jedna primární linka směrem k mateřské společnosti do zahraničí

(VPN 4 Mbps) a jedna záložní. Pravidelné platby za konektivitu (do sítě MPLS, do datového centra a připojení k matce do zahraničí) dosahují celkem 1.230.023 Kč ročně (viz tabulka č. 23).

Tabulka č. 23: Náklady na WAN při housingu v externím DC (25)

Náklady na WAN v případě housingu u poskytovatele B				
Položka	Množství	Lokalita	Cena v Kč/měsíc	Cena v Kč/rok
Připojka optiky primární MPLS	100 Mbps	B	18 320 Kč	219 840 Kč
Připojka optiky primární MPLS	100 Mbps	A	23 266 Kč	279 192 Kč
Připojka záložní MW MPLS	100 Mbps	B	- Kč	- Kč
Připojka záložní MW MPLS	100 Mbps	A	- Kč	- Kč
Připojení do Internetu	100 Mbps	DC	1 970 Kč	23 640 Kč
Připojení do DC primární	100 Mbps	DC	1 Kč	12 Kč
Připojení do DC záložní	100 Mbps	DC	3 000 Kč	36 000 Kč
Platba za VPN k matce	4 Mbps	DC	45 987 Kč	551 847 Kč
Platba za záložní připojení k matce	100 Mbps	DC	9 958 Kč	119 492 Kč
Náklady celkem:			102 502 Kč	1 230 023 Kč

Jak je vidět v tabulce č. 24, roční náklady na rack housing v externím datovém centru u poskytovatele včetně služeb datového centra, činí 348.912 Kč

Tabulka č. 24: Náklady na housing a služby datového centra (25)

Náklady na housing a služby DC u poskytovatele B					
Položka	Množství	Lokalita	Název služby	Cena v Kč/měsíc	Cena v Kč/rok
Služby datového centra	1 ks	B	SLA 3	5 496 Kč	65 952 Kč
Služby datového centra	1 ks	A	SLA 3	6 980 Kč	83 760 Kč
Proaktivní monitoring sjednaných služeb	1 ks	B	IPC Proaktiv	100 Kč	1 200 Kč
Proaktivní monitoring sjednaných služeb	1 ks	A	IPC Proaktiv	100 Kč	1 200 Kč
Housing, pronájem racku 20U, příkon 2,9 kW	1 ks	DC	Rack housing	14 900 Kč	178 800 Kč
Služba vzádelé podpory	2 h	DC	Remote hands	500 Kč	6 000 Kč
Uložení pásek se zálohou	25 ks	DC	Tape secure deposit	1 000 Kč	12 000 Kč
Náklady celkem:				29 076 Kč	348 912 Kč

Dále se předpokládají snížené nároky na kapacitu pracovníka aplikační podpory na úroveň 0,5 FTE. Je to z toho důvodu, že v rámci provozu jedné virtualizační infrastruktury namísto nyníšších dvou, dojde díky konsolidaci virtuálních serverů ke zjednodušení správy. Ta bude rezervovat méně kapacity správce virtualizační infrastruktury, proto se bude tento pracovník moci věnovat jiným činnostem.

Tabulka č. 25: Náklady na správu virtualizační infrastruktury (25)

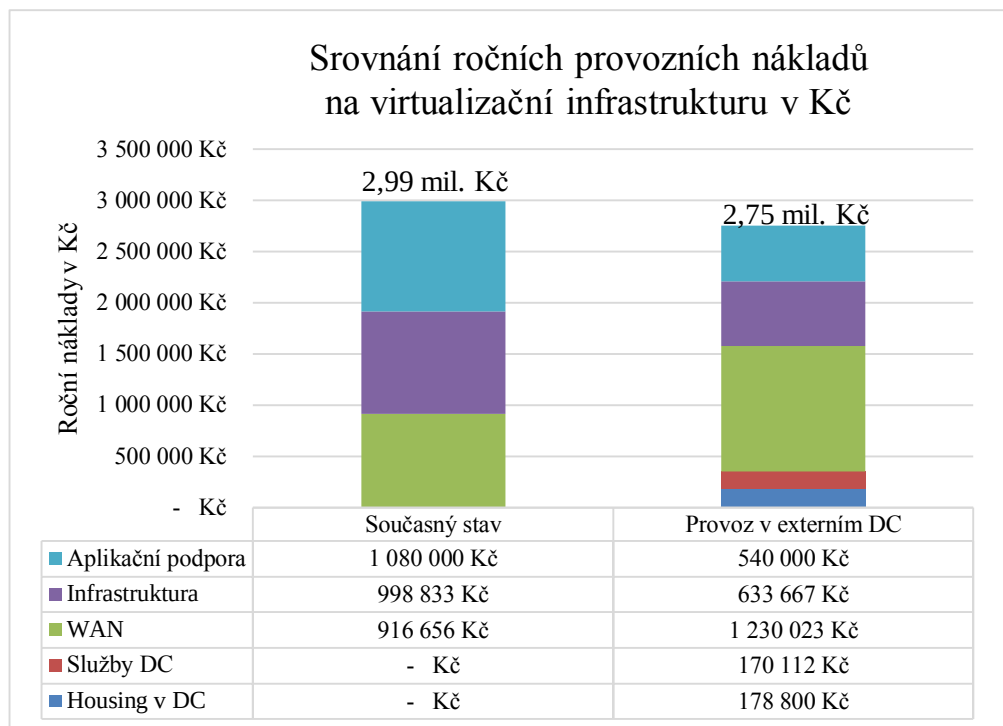
Náklady na správu virtualizační infrastruktury			
Položka	Velikost FTE	Náklady na FTE měsíční	Náklady na FTE roční
Superhrubá mzda pracovníka IT	0,5	45 000 Kč	540 000 Kč

V případě migrace a housingu v externím DC (viz tabulka č. 26), nebude zapotřebí provozovat 4 virtualizační servery, ale pouze 3, neboť jejich kapacita je pro provoz virtuálních serverů obou lokalit dostačující. Navíc, v případě konsolidace stávajících virtuálních serverů by dostačovala kapacita i dvou hostitelů, je zde tedy dostatečný prostor pro rozšiřování služeb, aplikací a nové servery.

Tabulka č. 26: Náklady na hw a sw virtualizační infrastruktury v externím DC (25)

Náklady na hw a sw virtualizační infrastruktury v externím DC			
Položka	Pořizovací náklady	Životnost (v letech)	Roční náklady
Hostitelé ESXi (3x)	450 000 Kč	3	150 000 Kč
Pásková zálohovací jednotka	200 000 Kč	5	40 000 Kč
Diskové pole SAN (2x)	1 000 000 Kč	4	250 000 Kč
SQL Server	200 000 Kč	3	66 667 Kč
Operační systémy serverů	300 000 Kč	3	100 000 Kč
Podpora VMware	54 000 Kč	2	27 000 Kč
Náklady celkem:			633 667 Kč

Jak je z grafu č. 4 vidět, celkové roční provozní náklady na virtualizační infrastrukturu budou v případě jejího provozu v externím DC nižší o 242.887 Kč, než při jejím provozu v současném stavu.



Graf č. 4: Srovnání provozních nákladů na virtualizační infrastrukturu (25)

Kvalitativní přínosy hostingu

Datová centra jsou navržena, konstruována a provozována tak, aby bylo dosaženo co nejvyšší možné úrovně provozu, zabezpečení ICT infrastruktury a služeb. Jak je vidět v tabulce č. 27, která znázorňuje kvalitativní srovnání, rack housingem v externím DC společnost dosáhne nesrovnatelně lepší provozní úrovně své virtualizační infrastruktury, než v současné době.

Tabulka č. 27: Kvalitativní srovnání provozní úrovně ICT (25)

Oblast	Úroveň serveroven současný stav			Úroveň externího DC
	Lokalita B serverovna 1	Lokalita A - serverovna 1	Lokalita A - serverovna 2	Externí DC
Vybavení	velmi nízká	nízká	nízká	velmi vysoká
Řízení přístupu	nízká	velmi nízká	velmi nízká	velmi vysoká
Zdroje napájení	nízká	nízká	nízká	velmi vysoká
Klimatizace	nízká	průměrná	průměrná	velmi vysoká
Požární ochrana	nízká	průměrná	průměrná	velmi vysoká
Systém hlášení	průměrná	průměrná	průměrná	velmi vysoká

Přidaná hodnota housingu

V situaci, kdy by např. vznikl ve společnosti požár, a došlo by k vyhoření serverovny, právě z důvodu nízkého či průměrného zabezpečení (požární ochrana, systém hlášení, monitoring, apod.), se projeví přidaná hodnota housingu ICT v externím DC. V tomto případě by tento incident měl kritický dopad na business, neboť společnost by přišla o veškerý hardware a obnova by trvala velmi dlouho. Data by se dala obnovit ze záloh (pokud by tyto nebyly také požárem zasaženy), avšak s dlouhou dobou obnovení. Oproti tomu, pokud bude mít podnik část své ICT infrastruktury (servery, data) hostovanou v datovém centru, při požáru sice přijde o část vybavení, nicméně se nejedná o kritický hardware (např. office počítače, switche) a doba pro jeho nahrazení je krátká. Pokud jeden den, kdy podnik nevyrábí/neposkytuje služby, představuje pro společnost ztrátu ve výši např. 1.000.000 Kč, pak se dá stanovit, jakou ztrátu společnost zaznamená v případě obnovy celé své ICT infrastruktury nebo jen její části.

TCO hostingu

RTC dosahují 2.752.602 Kč ročně, plánované počáteční CTC 378.000 Kč (rozpočet projektu), TCO tedy dosahují v prvním roce 3.130.602 Kč. Výše TCO se dá dále optimalizovat, např. pokud by společnost dokázala vyjednat lepší smluvní podmínky, nebo využila nejenom služby rack housingu, ale širšího outsourcingu ICT v cloudu (tedy např. služba dedikovaných serverů, nebo virtuálních dedikovaných serverů).

Cena/kvalita/přidaná hodnota hostingu

Dle mého názoru, hosting v externím DC představuje pro podnik nejlepší možný poměr ceny, kvality a přidané hodnoty. Jen obtížně a s vysokými náklady by společnost sotva dosáhla takové kvality provozních podmínek, jaké nabízí specializovaná datová centra. Navíc vedení společnosti musí zvážit, na kolik si cení svých aktiv, jaká je potřeba jejich zabezpečení a ochrany, a především, jaký vliv může mít výpadek ICT na business a zisk podniku.

ZÁVĚR

Cílem mé práce bylo navrhnout možný způsob migrace části ICT infrastruktury obou lokalit společnosti Dust CR, s.r.o., do datového centra. Tímto projektem jsem se zabývala na základě rozhodnutí centrálního IT společnosti, z důvodu nevyhovujícího současného stavu serveroven. V části analýzy jsem se zabývala zjištěním současného stavu ICT, z těchto informací jsem poté vycházela při navrhování možného způsobu řešení migrace. Kvalitativní rozměr cíle projektu jsem z mého pohledu naplnila, neboť jsem zpracovala kompletní projektový plán včetně všech analýz a plánu migrace, zahrnující podstatné kroky, které musejí být splněny pro úspěšnou realizaci projektu. Cíl práce, z hlediska jeho rozsahu, se mi tedy podařilo dosáhnout, neboť plán migrace je sestaven z činností, zajišťujících přesun virtualizační infrastruktury obou lokalit. Plánované projektové aktivity, by měly být podle časového harmonogramu dokončeny do dvou let od zahájení projektu. Rozpočet, včetně finančního polštáře, je odhadován na 378.000 Kč.

Přínosy tohoto řešení spočívají především ve zvýšení kvality poskytovaných služeb, úrovni provozu, zabezpečení, řízení a rozvoje ICT společnosti Dust CR, s.r.o. Rovněž provoz virtualizační infrastruktury v externím DC, oproti současnému stavu, přináší podniku i ekonomické úspory ve výši 242.887 Kč ročně.

SEZNAM POUŽITÉ LITERATURY

- (1) VMWARE. Virtualization. *VMware.com*. [online]. © 2013
[cit. 2016-02-09]. Dostupné z: <http://www.vmware.com/virtualization>
- (2) KOČÍBOVÁ, I. *Návrh virtualizace a konsolidace serverů*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2014. 75 s. Vedoucí bakalářské práce Ing. Viktor Ondrák, Ph.D.
- (3) GÁLA, L., J. POUR a Z. ŠEDIVÁ. *Podniková informatika* [online]. 2. přeprac. a aktual. vyd. Praha: Grada, 2009 [cit. 2013-12-02]. ISBN 978-80-247-2615-1. Dostupné z: <http://books.google.cz>
- (4) MATYSKA, L. Virtualizace výpočetního prostředí. *Zpravodaj ÚVT MU* [online]. 2006, roč. 17, č. 2, s. 9-11 [cit. 2016-02-09]. ISSN: 1212-0901. Dostupné z: <http://www.ics.muni.cz/bulletin/articles/540.html>
- (5) SMEJKAL, T. *Návrh na optimalizaci serverů využitím virtuálního prostředí*. Brno, 2009. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská.
- (6) OLDANYGROUP. Co je to virtualizace?. *OldanyGroup.cz* [online]. © 2013 [cit. 2013-12-03]. Dostupné z: <http://www.oldanygroup.cz/virtualizace-vmware-zakladni-informace-9/>
- (7) STREIT, J. *Virtualizace a konsolidace serverů*. Brno, 2011. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská.
- (8) LEŠTINA, P. Ekonomický pohled na cloud computing. *IT SYSTEMS* [online]. 2012, 4/2012, str. 26 [cit. 2016-02-15]. Dostupné z: <http://www.systemonline.cz/virtualizace/ekonomicky-pohled-na-cloud-computing.htm>
- (9) BERAN, R. Virtualizace operačních systémů. *Beranr.webzdarma.cz* [online]. © 2006 [cit. 2013-12-10]. Dostupné z: <http://www.beranr.webzdarma.cz/virtualizace.html#coUmoznujeVirtualizace>

- (10) REVOLUTIONARY TECHNOLOGY. Virtual Server Migration. *Revolutionarytechnology.net* [online]. ©2013 [cit. 2013-12-10]. Dostupné z: <https://revolutionarytechnology.net/Cloud-Virtual-Server-Administration/virtual-server-migration.html>
- (11) LACKO, L. *Osobní cloud pro domácí podnikání a malé firmy*. 1. vyd. Brno: Computer Press, 2012. ISBN 978-80-251-3744-4.
- (12) SODOMKA, P. a H. KLČOVÁ. *Informační systémy v podnikové praxi*. 2. aktualiz. a rozš. vyd. Brno: Computer Press, 2010. ISBN 978-80-251-2878-7.
- (13) TRČKA, A. Lesk a bída outsourcingu IT. *IT SYSTEMS* [online]. 2011, č. 3 [cit. 2016-02-15]. Dostupné z: <http://www.systemonline.cz/virtualizace/ekonomicky-pohled-na-cloud-computing.htm>
- (14) VOŘÍŠEK, J. *Výhody a rizika outsourcingu formou cloud computingu* [online]. Vysoká škola ekonomická v Praze, Katedra informačních technologií: 2009 [cit. 2016-02-15]. Dostupné z: http://www.komora.cz/Files/FITPRO/Prezentace/19_symposium/Vorisek-CSFCloudComputingu.pdf
- (15) FANTA, P. *Outsourcing*. Praha, 2004. Autoreferát k doktorské disertační práci. Vysoká škola ekonomická v Praze, Fakulta podnikohospodářská. Dostupné z: <https://webhosting.vse.cz/ekisl/prace/Fanta.pdf>
- (16) NOVOTNÁ, L. a A. TICHÁ. Outsourcing jako nástroj facility managementu pro zefektivnění provozu firmy. *Tzb-info.cz* [online]. Vysoké učení technické v Brně, Fakulta stavební: 2016 [cit. 2016-02-15]. Dostupné z: <http://www.tzb-info.cz/fm-sluzby/12643-outsourcing-jako-nastroj-facility-managementu-pro-zefektivneni-provozu-firmy>
- (17) VOŘÍŠEK, J. a T. BRUCKNER. *Outsourcing IS/IT z hlediska zadavatelského podniku* [online]. Vysoká škola ekonomická v Praze, Katedra informačních technologií: 1998 [cit. 2016-02-15]. Dostupné z: http://nb.vse.cz/~vorisek/FILES/Clanky/1998_Outsourcing_IS.htm

- (18) NIST. The NIST Definition of Cloud Computing. *Recommendations of the National Institute of Standards and Technology*. [online] 2011 [cit. 2016-04-04]
Dostupné z: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>.
- (19) MODERNTech COMPUTER & PERIPHERAL. Datacenter - Cloud Computing. *Moderntech.com.hk* [online]. ©1985-2016 [cit. 2016-02-15].
Dostupné z: <http://www.moderntech.com.hk/en/solution/103>
- (20) MÁCHA, P. Historie a základní principy cloud computingu. *IT SYSTEMS: Cloud computing a virtualizace IT I* [online]. 2015, č. 4 [cit. 2016-02-15]. Dostupné z: <http://www.systemonline.cz/clanky/outtasking-aneb-vice-ict-sluzeb-s-mensim-rozpocetem.htm>
- (21) SYNERGY. Private Cloud Server Virtualization. *Synergygs.com* [online]. © 2016 [cit. 2016-02-15]. Dostupné z: <http://www.synergygs.com/Solutions/Cloud Services/ServerVirtualization/>
- (22) HURWITZ, J. *Cloud computing for dummies*. Hoboken, NJ: Wiley Pub., 2009. ISBN:978-0-470-48470-8. Dostupné z: <http://www.dummies.com/how-to/content/comparing-public-private-and-hybrid-cloud-computin.html>
- (23) BRIGGETTE, C. Cloud Computing 101: Public Vs Private Clouds. *Blog.nskinc.com* [online]. 2011 [cit. 2016-02-15]. Dostupné z: <http://blog.nskinc.com/it-services-boston/resources/blog/cloud-computing-101-public-vs-private-clouds>
- (24) NSKINC. White Paper: "Hybrid Clouds-The Best of Both Worlds". *Nskinc.com* [online]. 2016 [cit. 2016-02-15]. Dostupné z: http://www.nskinc.com/hybrid-clouds-the-best-of-both-worlds?bi_campaign=Brightinfo&bi_medium=referral&bi_source=app.brightinfo.com
- (25) Vlastní zpracování
- (26) KOVANDA, P. *Cloudy a jejich poskytovatelé v rámci regionu střední Evropy* [online]. Bakalářská práce. České vysoké učení technické v Praze, Fakulta informačních technologií, Katedra softwarového inženýrství: 2014

- [cit. 2016-02-15]. Dostupné z: https://dip.felk.cvut.cz/browse/pdfcache/kovanpa2_2014bach.pdf
- (27) ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. *Problematika ISMS v manažerské informatice*. Vyd. 1. Brno: Akademické nakladatelství CERM, 2013, 377 s. ISBN 978-80-7204-872-4.
- (28) WIKIMEDIA FOUNDATION. Multiprotocol Label Switching. In: *Wikipedia: the free encyclopedia* [online]. 2011 - 2016 [cit. 2016-02-15]. Dostupné z: https://cs.wikipedia.org/wiki/Multiprotocol_Label_Switching
- (29) MASTER INTERNET. Serverhosting - Kategorizace služeb. *Master.cz* [online]. ©1996-2014 [cit. 2016-02-15]. Dostupné z: <http://www.master.cz/serverhosting/>
- (30) MASTER INTERNET. KVM over IP. *Master.cz* [online]. ©1996-2014 [cit. 2016-02-15]. Dostupné z: <http://www.master.cz/kvm-over-ip/>
- (31) CONTEG. Datová centra. *Conteg.cz* [online]. © 2016 [cit. 2016-02-15]. Dostupné z: <http://www.conteg.cz/design-datovych-center>
- (32) CZECHINVEST. Definice datového centra. *Czechinvest.org* [online]. 2011 [cit. 2016-02-15]. Dostupné z: <http://www.czechinvest.org/data/files/priloha-c-10-definice-datoveho-centra-2737-cz.pdf>
- (33) SEDLÁK, P. *Bezpečnost informací: Datová centra* (přednáška). Brno: VUT v Brně, Fakulta podnikatelská, 16. 03. 2015
- (34) ITBIZ. Jsou datacentra s TIER certifikací opravdu bezpečnější? *Itbiz.cz* [online]. 2014 [cit. 2016-02-15]. Dostupné z: <http://www.itbiz.cz/clanky/jsou-datacentra-s-tier-certifikaci-opravdu-bezpecnejsi>
- (35) PŘIBYL J. *Základní parametry tříd serveroven a datových center TIER* [online]. 2008 [cit. 2016-02-15]. Dostupné z: <http://docplayer.cz/6764409-Zakladni-parametry-trid-serveroven-a-datovych-center-tier.html>
- (36) UPTIME INSTITUTE. *UptimeInstitute.com* [online]. ©2013-2016 [cit. 2016-02-15]. Dostupné z: <https://uptimeinstitute.com/>

- (37) MANAGEMENTMANIA. SLA (Service Level Agreement).
ManagementMania.com [online]. ©2011-2013 [cit. 2016-02-15]. Dostupné z:
<https://managementmania.com/cs/service-level-agreement>
- (38) FISCHER, R. SLA a OLA pro různé druhy služeb. *Fischer-software.com*
[online]. 2012 [cit. 2016-02-15]. Dostupné z: <http://www.fischer-software.cz/a-sla-ola-ruzne-druhy-sluzeb.htm>
- (39) SCHWALBE, K. *Řízení projektů v IT: kompletní průvodce*. Vyd. 1. Brno: Computer Press, 2011. ISBN 978-80-251-2882-4.
- (40) SMOLÍKOVÁ, L. *Řízení projektů* (přednáška). Brno: VUT v Brně, Fakulta podnikatelská, 18. 02. 2014
- (41) SMOLÍKOVÁ, L. *Řízení projektů* (2. přednáška). Brno: VUT v Brně, Fakulta podnikatelská, 23. 02. 2014
- (42) SMOLÍKOVÁ, L. *Řízení projektů* (3. přednáška). Brno: VUT v Brně, Fakulta podnikatelská, 26. 02. 2014
- (43) SMOLÍKOVÁ, L. *Řízení projektů: Zahájení projektu* (přednáška). Brno: VUT v Brně, Fakulta podnikatelská, 20. 11. 2014

SEZNAM OBRÁZKŮ

Obrázek č. 1: Srovnání tradiční a virtuální architektury - upraveno (6)	13
Obrázek č. 2: Schéma virtualizace serverů – upraveno (10)	14
Obrázek č. 3: Důvody k realizaci outsourcingu (16)	17
Obrázek č. 4: Důvody k nerealizaci outsourcingu (16).....	17
Obrázek č. 5: Výhody outsourcingu (16)	18
Obrázek č. 6: Rizika outsourcingu (16).....	19
Obrázek č. 7: Cloud computing (19)	20
Obrázek č. 8: Privátní cloud - Onsite a Offsite (21).....	21
Obrázek č. 9: Privátní cloud (23)	22
Obrázek č. 10: Veřejný cloud (23).....	22
Obrázek č. 11: Hybridní cloud (24)	23
Obrázek č. 12: Komunitní cloud (25).....	23
Obrázek č. 13: TIER klasifikace – upraveno (36).....	34
Obrázek č. 14: Trojimperativ projektu (25).....	37
Obrázek č. 15: Etapy projektové fáze (25)	39
Obrázek č. 16: Organizační struktura Dust CR, s.r.o. (25).....	43
Obrázek č. 17: Schéma propojení WAN sítě Dust CR, s.r.o. (25).....	45
Obrázek č. 18: Časová osa projektu (25).....	52
Obrázek č. 19: Organizační struktura projektu (25).....	54
Obrázek č. 20: Návrh schéma WAN (25).....	71
Obrázek č. 21: Schéma LAN v DC (25).....	72

SEZNAM TABULEK

Tabulka č. 1: Parametry serveroven a datových center dle klasifikace TIER (35).....	32
Tabulka č. 2: Rozdělení VLAN (25).....	45
Tabulka č. 3: Stručný přehled parametrů virtualizační infrastruktury (25).....	47
Tabulka č. 4: Roční náklady na aplikační podporu (25)	48
Tabulka č. 5: Roční náklady na hw a sw virtualizační infrastruktury v současném stavu (25)	48
Tabulka č. 6: Roční náklady na WAN v současném stavu (25)	49
Tabulka č. 7: Hardware určený k migraci (25).....	55
Tabulka č. 8: Stupnice pro hodnocení vlivu a zájmu stakeholderů (25)	56
Tabulka č. 9: Stupnice pro posouzení významu stakeholderů (25)	56
Tabulka č. 10: Analýza stakeholderů (25).....	57
Tabulka č. 11: Stupnice pravděpodobnost a dopad pro ohodnocení rizika (25).....	58
Tabulka č. 12: Intervaly pro určení celkové hodnoty rizika (25).....	58
Tabulka č. 13: Analýza rizik projektu migrace do externího DC (25).....	59
Tabulka č. 14: Opatření pro snížení významných rizik projektu (25)	61
Tabulka č. 15: Rozpočet projektu (25).....	62
Tabulka č. 16: Požadavky na poskytovatele housingu v DC (25)	64
Tabulka č. 17: Jednorázové náklady na housing – nabídka od poskytovatele A (25)	65
Tabulka č. 18: Pravidelné měsíční platby za housing – nabídka od poskytovatele A (25)	66
Tabulka č. 19: Pravidelné měsíční platby za housing – nabídka od poskytovatele B (25)	67
Tabulka č. 20: Porovnání nabídek housingu (25)	69
Tabulka č. 21: Umístění hardware v datovém centru (25)	72
Tabulka č. 22: Návrh rozdělení přenášených dat do tříd dle priorit (25)	73
Tabulka č. 23: Náklady na WAN při housingu v externím DC (25)	77
Tabulka č. 24: Náklady na housing a služby datového centra (25)	77
Tabulka č. 25: Náklady na správu virtualizační infrastruktury (25)	78
Tabulka č. 26: Náklady na hw a sw virtualizační infrastruktury v externím DC (25)....	78
Tabulka č. 27: Kvalitativní srovnání provozní úrovně ICT (25)	79

SEZNAM GRAFŮ

Graf č. 1: Roční náklady na provoz virtualizační infrastruktury v současném stavu (25)	49
Graf č. 2: Mapa rizik (25)	60
Graf č. 3: Pavučinový graf významných rizik (25)	62
Graf č. 4: Srovnání provozních nákladů na virtualizační infrastrukturu (25)	79

SEZNAM PŘÍLOH

Příloha č. 1: Zakládací listina projektu (25)	I
Příloha č. 2: Závěrečná zpráva projektu (25)	II
Příloha č. 3: Vztah mezi projektovými procesy a oblastmi řízení (25, 39)	III
Příloha č. 4: Nástroje a techniky PM používané dle oblasti řízení (25, 39)	IV
Příloha č. 5: Přehled a parametry hardware virtualizační infrastruktury (25)	V
Příloha č. 6: Parametry virtuálních serverů lokalita A (25)	VI
Příloha č. 7: Parametry virtuálních serverů lokalita B (25)	VII
Příloha č. 8: Simulace využití 100 Mbps linky FD (25)	VIII
Příloha č. 9: IT audit checklist – serverovna č. 1 lokalita B (25)	IX
Příloha č. 10: IT audit checklist – serverovna č. 1 lokalita A (25)	X
Příloha č. 11: IT audit checklist – serverovna č. 2 lokalita A (25)	XI
Příloha č. 12: Náklady na úpravu serveroven (25)	XII
Příloha č. 13: Projektový plán – seznam úkolů a zdroje (25)	XIII
Příloha č. 14: Seznam kritických úkolů projektu (25)	XVII
Příloha č. 15: Síťový uzlový graf s kritickou cestou (25)	XIX
Příloha č. 16: Ganttův diagram pro projektovou fázi (25)	XXI
Příloha č. 17: Rozdělení virtuálních serverů na 3 hostitele (25)	XXII

Příloha č. 1: Zakládací listina projektu (25)

ZAKLÁDACÍ LISTINA PROJEKTU		
Číslo projektu: 001/2016	Předpokládaný termín zahájení:	15.12.2015
Název projektu: Migrace virtualizační infrastruktury do datového centra	Předpokládaný termín ukončení:	22.9.2017
	Předpokládané náklady Kč:	378 000 Kč
	Předpokládané náklady EUR:	14 000 €
	Předpokládané přínosy Kč:	242 887 €
	Předpokládané přínosy EUR:	8 996 €
Účel projektu: Projekt by měl být realizován za účelem zvýšení kvality úrovně provozu, řízení a rozvoje ICT společnosti, měl by přispět k vyšší kvalitě poskytovaných služeb, dále zlepšit provozní úroveň ICT a zvýšit zabezpečení a dostupnost prostředků a aplikací.		
Cíl projektu: Cílem projektu je přesunout virtualizační infrastrukturu obou lokalit společnosti do externího datového centra, nejpozději do dvou let od zahájení realizace projektu, při dodržení plánovaného rozpočtu a být odevzdán v požadované kvalitě a rozsahu.		
Klíčové ukazatele (KPIs): - přesunout obě lokality - dodržení rozpočtu - dodržení časového rámce projektové fáze (2 roky) - vytvořit a odevzdat zákazníkovi projektovou dokumentaci		
Rozsah projektu: Tento projekt řeší kompletní přesun virtualizační infrastruktury obou lokalit společnosti do datového centra. Neřeší rekonstrukci serveroven na úroveň switchovny/telefonní ústředny.		
Sponzor:	Složení týmu:	
Jednatel společnosti	pracovníci lokálního IT	
Vedoucí projektu:	pracovníci CIT	
Vedoucí IT		
Zákazník:		
Společnost Dust		
Cílová odměna:	Částka:	
Jednorázová odměna ve výši:		
Steering committee:		
Jednatel společnosti		

Příloha č. 2: Závěrečná zpráva projektu (25)

ZÁVĚREČNÁ ZPRÁVA							
Číslo projektu: 001/2016		Předpokládaný termín zahájení:		15.12.2015			
Název projektu:		Předpokládaný termín ukončení:		22.9.2017			
Migrace virtualizační infrastruktury do datového centra		Předpokládané náklady Kč:		378 000 €			
		Předpokládané přínosy Kč:		242 887 €			
		Skutečná doba trvání od-do:					
		Skutečné náklady celkem:		- €			
		Skutečné přínosy celkem:		- €			
Účel projektu: Projekt by měl být realizován za účelem zvýšení kvality úrovně provozu, řízení a rozvoje ICT společnosti, měl by přispět k vyšší kvalitě poskytovaných služeb, dále zlepšit provozní úroveň ICT a zvýšit zabezpečení a dostupnost prostředků a aplikací.							
Cíl projektu: Cílem projektu je přesunout virtualizační infrastrukturu obou lokalit společnosti do externího datového centra, nejpozději do dvou let od zahájení realizace projektu, při dodržení plánovaného rozpočtu a být odevzdán v požadované kvalitě a rozsahu.							
Klíčové ukazatele (KPIs): - přesunout obě lokality - dodržení rozpočtu - dodržení časového rámce projektové fáze (2 roky) - vytvořit a odevzdat zákazníkovi projektovou dokumentaci							
Výchozí stav KPI: - plánovaný rozpočet 378.000 Kč (14.000 €) - plánovaný termín ukončení projektové fáze 22.9.2017							
Srovnání plán/skutečnost KPI:							
Rozsah projektu: Tento projekt řeší kompletní přesun virtualizační infrastruktury obou lokalit společnosti do datového centra. Neřeší rekonstrukci serveroven na úroveň switchovny/telefonní ústředny.							
Hodnocení projektu:							
	Celkové hodnocení	Rizika	Náklady	Úspora/ Přínos	Časový plán	Disciplína	zeleňá nevyskytl se žádný významný problém v rámci projektu
Shrnutí							žlutá nastaly drobné odchylky v rámci projektu, byla realizována opatření k nápravě těchto odchylek a nedošlo k nesplnění cíle projektu ani významné změně v zadání projektu
							červená nastaly významné odchylky v rámci projektu, které vedly k nesplnění cíle projektu a nebo významné změně v zadání projektu
Komentář pro výskyt odchylek v projektu:							
Shrnutí výsledků projektu a ponaučení:							
Zpracoval:							
Schválil:							
Dne:							
V:							

Příloha č. 3: Vztah mezi projektovými procesy a oblastmi řízení (25, 39)

Oblast řízení	Projektový proces				
	Zahájení	Plánování	Realizace	Monitorování a kontrola	Uzavření
Integrované řízení projektu	Vytvoření zadávací listiny projektu	Vytvoření projektového plánu	Řízení realizace projektu	Řízení a kontrola projektové práce Realizace integrovaného řízení změn	Dokončení projektu nebo fáze
Řízení rozsahu		Sběr požadavků Definování rozsahu Zpracování WBS		Ověření rozsahu Řízení rozsahu	
Řízení času		Definování aktivit Posloupnost aktivit Odhad zdrojů a trvání jednotlivých aktivit Vytvoření harmonogramu projektu		Kontrola harmonogramu	
Řízení nákladů		Odhad nákladů Vytvoření rozpočtu		Kontrola nákladů	
Řízení kvality		Plánování kvality	Zajišťování kvality	Kontrola kvality	
Řízení lidských zdrojů		Vytvoření plánu lidských zdrojů	Sestavení, rozvoj a řízení projektového týmu		
Řízení komunikace	Identifikace zainteresovaných stran projektu	Plánování komunikace	Distribuce informací Řízení očekávání zainteresovaných stran projektu	Zprávy o postupu v projektu	
Řízení rizik		Plán řízení rizik Identifikace rizik Realizace kvalitativní a kvantitativní analýzy rizik Plán opatření		Kontrola a řízení rizik	
Řízení dodávek		Plán dodávek	Realizace nákupů	Administrace nákupů	Dokončení nákupů

Příloha č. 4: Nástroje a techniky PM používané dle oblasti řízení (25, 39)

Oblast řízení	Nástroje a techniky
Integrované řízení projektu	Metody výběru projektu, metodiky projektového řízení (PMBOK, PRINCE2), analýza zainteresovaných stran (stakeholderů), projektové smlouvy, plány řízení projektu, software k řízení projektu, řízení změn v projektu, změnová komise, porady ke kontrole stavu projektu, hodnotící zprávy, reporty
Řízení rozsahu	Deklarace rozsahu projektu, hierarchická struktura prací (WBS), definice cílů a rozsahu prací, analýzy požadavků, plány řízení rozsahu, techniky ke kontrole stavu rozsahu projektu, řízení změn rozsahu projektu
Řízení času	Ganttův diagram, síťová analýza, kritická cesta, monitorování stavu projektu z hlediska času (MTA)
Řízení nákladů	Čistá současná hodnota (NPV), návratnost investice (ROI), analýza doby návratnosti investice, řízení získané hodnoty (EVM), odhady nákladů, plánování nákladů, rozpočty
Řízení kvality	Metriky kvality, kontrolní seznamy (checklisty), kontrolní diagramy kvality (regulační diagramy), Paretovy diagramy (80/20), diagramy rybí kosti (Fishbone/Ishikawa), statistické metody
Řízení lidských zdrojů	Motivační techniky, matice zodpovědnosti (RACI), schéma organizace projektu, histogram zdrojů, teambuilding
Řízení komunikace	Komunikační plány, zahajovací meetingy (kick-off), řízení konfliktů, reporty o stavu a postupu projektu, virtuální komunikace, šablony, webové stránky projektu, portál
Řízení rizik	Analýza rizik, plány řízení rizik, metriky pravděpodobnosti a dopadu, kvantitativní a kvantitativní hodnocení rizik
Řízení dodávek	Analýza vlastní síly, smlouvy, požadavky na návrhy a nabídky, výběr zdrojů, metrika hodnocení dodavatele

Příloha č. 5: Přehled a parametry hardware virtualizační infrastruktury (25)

Zařízení	Účel	Č. hostitele	Lokalita	Stáří roky	Počet CPU	Počet jader CPU	Počet logických CPU	Frekvence CPU GHz	Kapacita CPU GHz	RAM GB	Počet NICs	Počet hostovaných VMs	Velikost U	Spotřeba W	Max. spotřeba W
DELL PowerEdge R720xd	ESXi server	1	A	3	1	8	16	2	16	96	6	12	2	320	540
DELL PowerEdge R720xd	ESXi server	2	A	3	1	8	16	2	16	96	6	12	2	320	540
DELL PowerEdge R620	ESXi server	3	B	2	2	16	32	2,6	41,6	128	8	13	1	200	320
DELL PowerEdge R620	ESXi server	4	B	2	2	16	32	2,6	41,6	128	8	10	1	200	320
DELL PowerEdge R530	Zálohovací server	-	B	1	1	6	12	2,4	14,4	16	4	0	2	200	320
DELL PowerEdge R610	Zálohovací server	-	A	5	1	8	16	2,6	20,8	16	4	0	2	320	540

Zařízení	Účel	Lokalita	Stáří roky	Počet disků SAS	Nominální kapacita 1 disku GB	Nominální kapacita celkem	Využitelná kapacita pole TB	Vyčleněná kapacita TB	Využitá kapacita TB	Volná kapacita TB	Raid	Velikost U	Spotřeba W	Max. spotřeba W
Dell Equallogic PS4100E	iSCSI SAN	A	3	12	3000	35,16	13,44	13	9,28	0,44	10	2	270	320
Dell Equallogic PS4210	iSCSI SAN	B	1	24	900	21,09	14,91	5	3,55	9,91	6	2	320	750

Zařízení	Účel	Lokalita	Stáří roky	Kapacita baterií Ah	Počet baterií	Kapacita baterií celkem Ah	Výkon W	Výstup A	Potenciální kapacita VA	Doba napájení min	Velikost U	Spotřeba W	Max. spotřeba W
APC UPS 5000VA	UPS	B	1	17	8	136	4000	8x10	5000	9	5	4000	4000
APC UPS RT 3000 VA	UPS	A	1	17	4	68	2100	8x10	3000	15	3	2300	2300
APC UPS RT 3000 VA	UPS	A	1	5	16	80	2700	8x10	3000	15	2	2300	2300
APC UPS RT 3000 VA	UPS	A	1	9	8	72	2700	8x10	3000	15	2	2300	2300

Zařízení	Účel	Lokalita	Stáří roky	Počet kazet	Kapacita pásek TB	Max. rychlost zápisu MB/s	Kompatibilita čtení	Kompatibilita zápisu	Enkrypce	Velikost U	Spotřeba W	Max. spotřeba W
DELL PowerVault TL2000 LTO6	Pásková mechanika	B	2	24	2,5 - 6,25	160	LTO 4,5,6	LTO 5,6	ano	2	600	600
DELL PowerVault TL2000 LTO5	Pásková mechanika	A	3	24	1,5 - 3	140	LTO 3,4,5	LTO 4,5	ano	2	600	600

Zařízení	Účel	Lokalita	Stáří roky	Kapacita baterií Ah	Počet baterií	Kapacita baterií celkem Ah	Výkon W	Výstup A	Potenciální kapacita VA	Doba napájení min	Velikost U	Spotřeba W	Max. spotřeba W
APC UPS 5000VA	UPS	B	1	17	8	136	4000	8x10	5000	9	5	4000	4000
APC UPS RT 3000 VA	UPS	A	1	17	4	68	2100	8x10	3000	15	3	2300	2300
APC UPS RT 3000 VA	UPS	A	1	5	16	80	2700	8x10	3000	15	2	2300	2300
APC UPS RT 3000 VA	UPS	A	1	9	8	72	2700	8x10	3000	15	2	2300	2300

Příloha č. 6: Parametry virtuálních serverů lokalita A (25)

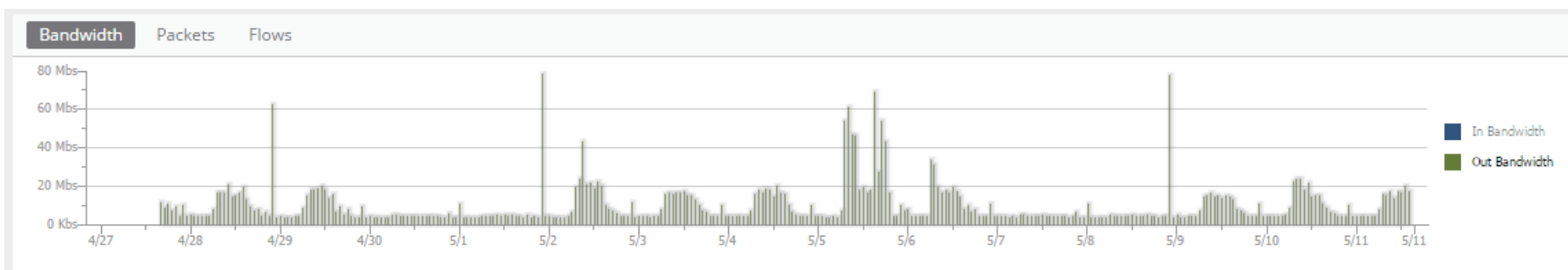
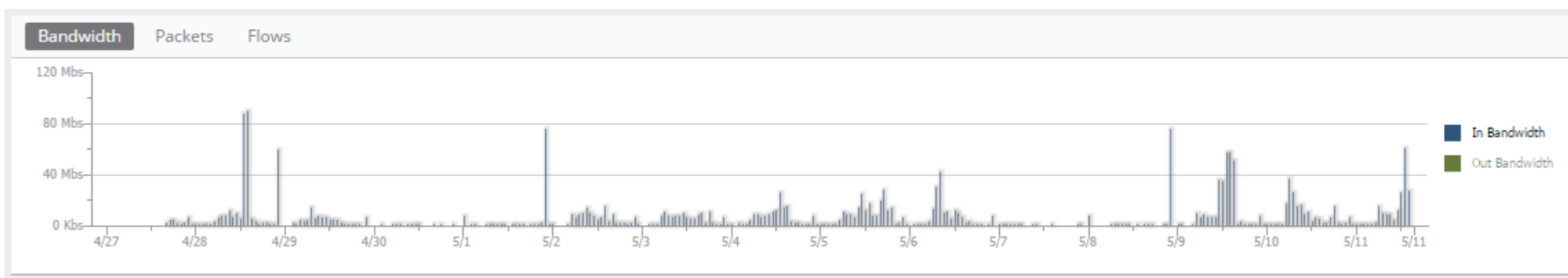
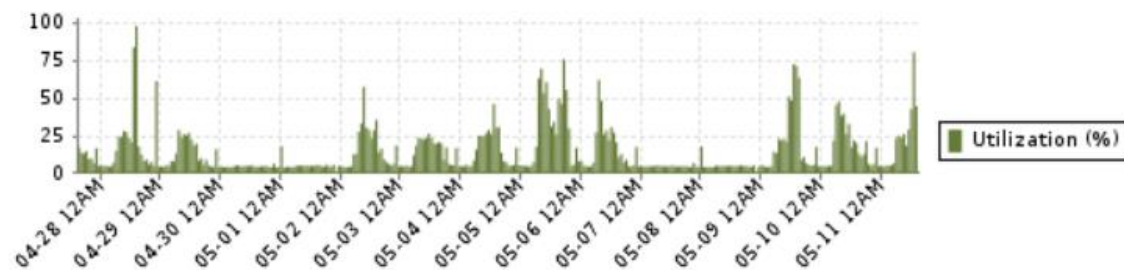
Virtuální servery lokalita A							
Umístěn na hostiteli č.	Označení VM	Využitá kapacita GB	vRAM MB	Využití paměti RAM %	vCPU	Přidělené CPU hostitele MHz	vNIC
1	VMA1	513,65	2000	25	6	59	1
	VMA2	214,11	4096	3	2	19	1
	VMA3	208,13	8192	11	4	279	1
	VMA4	168,12	8192	13	2	179	1
	VMA5	151,40	4096	8	2	79	1
	VMA6	60,00	4096	0	2	0	1
	VMA7	54,12	4096	8	2	239	1
	VMA8	54,11	4096	2	2	19	1
	VMA9	44,12	4096	1	2	19	1
	VMA10	38,17	4096	18	2	39	1
	VMA11	10,62	512	20	1	0	1
	VMA12	8,62	512	2	1	0	1
2	VMA13	3491,84	4096	8	2	59	1
	VMA14	1105,92	8192	25	8	439	1
	VMA15	683,51	16384	0	4	0	1
	VMA16	308,18	12288	25	6	2738	2
	VMA17	275,39	3972	0	2	0	1
	VMA18	273,41	2060	0	4	0	1
	VMA19	216,13	16384	10	4	279	1
	VMA20	108,13	8192	3	4	19	1
	VMA21	106,12	6144	11	2	79	1
	VMA22	55,28	4096	0	2	0	1
	VMA23	50,12	4096	10	2	19	1
	VMA24	29,12	1024	10	1	19	1

Příloha č. 7: Parametry virtuálních serverů lokalita B (25)

Virtuální servery lokalita B							
Umístěn na hostiteli č.	Označení VM	Využitá kapacita GB	vRAM MB	Využití paměti RAM %	vCPU	Přidělené CPU hostitele MHz	vNIC
3	VMB1	1710,08	4096	7	4	25	1
	VMB2	168,12	8192	81	2	1117	1
	VMB3	133,11	8192	27	2	207	1
	VMB4	114,11	14336	3	6	103	1
	VMB5	59,03	8192	11	5	77	1
	VMB6	52,80	2048	4	2	51	1
	VMB7	52,11	12288	0	5	25	2
	VMB8	52,11	2048	12	1	181	1
	VMB9	48,13	8192	8	5	155	1
	VMB10	42,11	2048	7	1	0	1
	VMB11	29,01	1024	31	1	337	1
	VMB12	19,14	1024	2	2	0	1
	VMB13	10,32	2048	7	4	233	3
4	VMB14	407,05	4096	7	2	103	1
	VMB15	184,13	24576	16	4	1741	1
	VMB16	111,24	8192	2	4	25	1
	VMB17	68,13	8192	4	8	311	1
	VMB18	64,13	4096	5	4	25	1
	VMB19	50,13	4096	22	2	389	1
	VMB20	50,12	4096	2	2	0	1
	VMB21	48,50	8192	0	4	25	2
	VMB22	40,00	4096	0	2	0	1
	VMB23	25,13	1024	6	1	0	3

Příloha č. 8: Simulace využití 100 Mbps linky FD (25)

Interface Utilization (End Time: Wed May 11 14:29:10 CEST 2016, Category: Hourly, Date Range: Last 2 Weeks)



Příloha č. 9: IT audit checklist – serverovna č. 1 lokalita B (25)

Checklist pro audit serverovny		Lokalita A - serverovna č. 1				
		Spíňuje	Částečně spíňuje	Nespíňuje	Odhad nákladů	Opatření
1 Vybavení						
1.1	Serverovna je umístěna odděleně v bezpečné části budovy	x				
1.2	Serverovna je permanentně bezpečně uzamčena vhodnými dveřmi			x	3 000 €	nové dveře
1.3	V případě nebezpečí je možné snadno otevřít dveře a opustit místnost	x				
1.4	Všechny dvířka racků lze zcela otevřít a zavřít, aniž by došlo k zablokování východu	x				
1.5	Okna serverovny jsou zabezpečeny vhodným způsobem	x				
1.6	Serverovna je dostatečně osvětlena	x				
1.7	Serverovna není využívána pro další účely, např. jako sklad nebo kancelář		x		0 €	úklid serverovny interními zdroji
1.8	V serverovně nejsou umístěny žádné hořlaviny nebo výbušniny	x				
1.9	Je zabudována přepětová ochrana a ochrana proti zásahu bleskem	x				
1.10	Systém kabeláže je dobře zdokumentován		x		0 €	zdokumentovat interními zdroji
1.11	Nepotřebné kabely jsou odstraněny		x		0 €	zajistit interními zdroji
1.12	Napájecí a datové kabely jsou kryty izolací bez obsahu chlórů					nelze určit
1.13	V serverovně je pravidelně prováděn úklid kvalifikovaným personálem			x	0 €	zajistit interními zdroji
1.14	Pokud v serverovně provádí úklid nekvalifikovaný personál, je na něj dohlíženo					nerrelevantní
1.15	Dveře serverovny jsou zvenku označeny neutrálním nápisem (např. technická místnost)	x				
1.16	Veškeré komponenty nejsou přímo vystaveny slunečnímu záření	x				
1.17	Kabeláž je přehledně organizována, je k ní jednoduchý přístup a kabely jsou označeny štítkem			x	1 000 €	zajistit externími zdroji
1.18	Napájecí a datové kabely jsou vedeny v oddělených kabelových trasách			x	750 €	externí spol. nebo zajistit vlastními zdroji
1.19	Všechny racky jsou dostatečně chlazený suchým vzduchem z klimatizace	x				
1.20	Všechny racky jsou postaveny do vertikální polohy	x				
1.21	Všechny komponenty uvnitř racku jsou přístupné jak ze své přední, tak ze zadní strany	x				
1.22	Všechny racky jsou 800 mm široké a 1000 mm hluboké			x	2 000 €	nové racky
1.23	Serverovna je vybaveny zdvojenou nebo zvýšenou podlahou			x	4 000 €	
2 Řízení přístupu						
2.1	Přístup do serverovny je umožněn pouze omezené skupině oprávněných osob	x				pracovníci IT mají vlastní klíče, rezervní klíč je umístěn na vratnici
2.2	Rozvodné skříně jsou chráněny před neoprávněným přístupem			x	200 €	pojistky jsou umístěny na chodbě, je možno zabezpečit dveře s klíči
2.3	Přístup do serverovny je dohledován a dokumentován	x				log přístupový systém SBI
2.4	Serverovna je zabezpečena systémem detekce neoprávněného vstupu (systém PZTS)		x		2 000 €	je umožněn přístup na kartu zvnějšku, dále zadání PINu uvnitř místnosti, alarm; nutné nasadit systém detekce průniku
2.5	V serverovně je nainstalován kamerový systém			x	1 000 €	kamerový systém
2.6	Systém řízení přístupu je dostatečně popsán			x	0 €	zajistit interními zdroji
2.7	Je implementován elektronický systém řízení přístupu			x	1 500 €	KABA
3 Zdroje napájení						
3.1	Je k dispozici redundance běžného zdroje napájení			x	0 €	náprava je vysoce nákladná, žádný záložní generátor v případě nouze
3.2	Je nainstalována redundantní UPS s automatickým převzetím při výpadku zdroje napájení			x	1 500 €	druhý UPS/Rack
3.3	Dostatečná doba provozu z náhradního zdroje napájení (nejméně 2 hodiny)			x		maximální doba provozu 30 min., s novými UPS déle
3.4	Je prováděna údržba zdrojů napájení, včetně pravidelného testování a dokumentace			x	0 €	zajistit interními zdroji
3.5	Prodlužovačky odpovídají náročnosti na napájení a jsou pravidelně revidovány		x		750 €	průmyslové prodlužovačky
3.6	Systém napájení je dostatečně zdokumentován			x	0 €	zajistit interně, oddělení správy budov
4 Klimatizace						
4.1	Teplota se pohybuje mezi min. +10°C a max.+35°C	x				
4.2	Relativní vlhkost se pohybuje od 20 % do 80 %, přičemž nedochází ke kondenzaci vody ze vzduchu	x				
4.3	Klimatizovaný vzduch je filtrován od prachu	x				
4.4	Je prováděna pravidelná údržba klimatizačních jednotek	x				
4.5	Je k dispozici redundantní klimatizační jednotka	x				
4.6	Teplota je monitorována	x				PRTG systém
4.7	Systém klimatizace je dostatečně zdokumentován			x	0 €	zajistit interními zdroji
5 Požární ochrana						
5.1	Systém požární ochrany je v souladu s národní legislativou	x				
5.2	Požární ochrana odpovídá normě ČSN EN 13 501-2 (REI30)			x		
5.3	Uspořádání serverovny nepřispívá k riziku nekontrolovatelného šíření požáru	x				
5.4	Serverovna je monitorována automatickým systémem detekce požáru/kouře	x				
5.5	Detektory kouře/ohně jsou umístěny jak ve zdvojené podlaže, tak zavěšeny na stropu		x			zavěšeny na stropě
5.6	Jsou instalovány schválené požární uzávěry pro zpomalení hoření a zařízení pro odvod tepla a kouře			x	741 €	
5.7	V serverové místnosti platí zákaz kouření a není povoleno vykonávat horké práce (svařování, apod.)	x				zákaz kouření v celé budově
5.8	V serverovně, nebo poblíž ní, je k dispozici ruční hasicí přístroj bez obsahu prášku		x		200 €	hasicí přístroj plněný CO2
5.9	Systém požární ochrany je dostatečně zdokumentován		x			obecně pro celou lokalitu
5.10	Je instalován systém automatického hašení ohně (pokud tento systém není instalován, je nutný ruční hasicí přístroj)			x	0 €	ruční hasicí přístroj
5.11	Je instalován systém pro včasnou detekci požáru (EPS)			x		
6 Ochrana proti vodě - pokud je relevantní						
6.1	Je instalován systém pro detekci vody					nerrelevantní
6.2	Potrubí s kapalinou obsahuje ochranu proti úniku kapaliny					nerrelevantní
6.3	Potrubí je pravidelně kontrolováno, jestli není poškozeno nebo z něj neuniká kapalina					nerrelevantní
6.4	Systém ochrany proti vodě je dostatečně zdokumentován					nerrelevantní
7 Systém hlášení						
7.1	Všechny nezbytné strany jsou o vzniklém problému informovány vhodným způsobem			x	0 €	zajistit interními zdroji
7.2	Všechny systémy jsou monitorovány		x		750 €	upozornění jsou zasílány na sdílený email IT; zasílat sms zprávy systémem PRTG
7.3	Systém monitoringu a hlášení je dostatečně zdokumentován			x	0 €	zajistit interními zdroji
					19 390,74 €	

Příloha č. 10: IT audit checklist – serverovna č. 1 lokalita A (25)

Checklist pro audit serverovny		Lokalita A - serverovna č. 1				
		Splňuje	Částečně splňuje	Nesplňuje	Odhad nákladů	Opatření
1 Vybavení						
1.1	Serverovna je umístěna odděleně v bezpečné části budovy	x				
1.2	Serverovna je permanentně bezpečně uzamčena vhodnými dveřmi			x	3 000 €	nové dveře
1.3	V případě nebezpečí je možné snadno otevřít dveře a opustit místnost	x				
1.4	Všechny dvířka racků lze zcela otevřít a zavřít, aniž by došlo k zablokování východu	x				
1.5	Okna serverovny jsou zabezpečeny vhodným způsobem	x				
1.6	Serverovna je dostatečně osvětlena	x				
1.7	Serverovna není využívána pro další účely, např. jako sklad nebo kancelář		x		0 €	úklid serverovny interními zdroji
1.8	V serverovně nejsou umístěny žádné hořlaviny nebo výbušniny	x				
1.9	Je zabudována přepětová ochrana a ochrana proti zásahu bleskem	x				
1.10	Systém kabeláže je dobře zdokumentován		x		0 €	zdokumentovat interními zdroji
1.11	Nepotřebné kabely jsou odstraněny		x		0 €	zajistit interními zdroji
1.12	Napájecí a datové kabely jsou kryty izolací bez obsahu chlórů					nelze určit
1.13	V serverovně je pravidelně prováděn úklid kvalifikovaným personálem			x	0 €	zajistit interními zdroji
1.14	Pokud v serverovně provádí úklid nekvalifikovaný personál, je na něj dohlíženo					nerelevantní
1.15	Dveře serverovny jsou zvenku označeny neutrálním nápisem (např. technická místnost)	x				
1.16	Veškeré komponenty nejsou přímo vystaveny slunečnímu záření	x				
1.17	Kabeláž je přehledně organizována, je k ní jednoduchý přístup a kabely jsou označeny štítkem			x	1 000 €	zajistit externími zdroji
1.18	Napájecí a datové kabely jsou vedeny v oddělených kabelových trasách			x	750 €	externí spol. nebo zajistit vlastními zdroji
1.19	Všechny racky jsou dostatečně chlazeny suchým vzduchem z klimatizace	x				
1.20	Všechny racky jsou postaveny do vertikální polohy	x				
1.21	Všechny komponenty uvnitř racku jsou přístupné jak ze své přední, tak ze zadní strany	x				
1.22	Všechny racky jsou 800 mm široké a 1000 mm hluboké			x	2 000 €	nové racky
1.23	Serverovna je vybavena zdvojenou nebo zvýšenou podlahou			x	4 000 €	
2 Řízení přístupu						
2.1	Přístup do serverovny je umožněn pouze omezené skupině oprávněných osob	x				pracovníci IT mají vlastní klíče, rezervní klíč je umístěn na vátnici
2.2	Rozvodné skříně jsou chráněny před neoprávněným přístupem			x	200 €	pojistky jsou umístěny na chodbě, je možno zabezpečit dveřmi s klíči
2.3	Přístup do serverovny je dohledován a dokumentován	x				log přístupový systém SBI
2.4	Serverovna je zabezpečena systémem detekce neoprávněného vstupu (systém PZTS)		x		2 000 €	je umožněn přístup na kartu zvnějšku, dále zadání PINu uvnitř místnosti, alarm; nutné nasadit systém detekce průniku
2.5	V serverovně je nainstalován kamerový systém			x	1 000 €	kamerový systém
2.6	Systém řízení přístupu je dostatečně popsán			x	0 €	zajistit interními zdroji
2.7	Je implementován elektronický systém řízení přístupu			x	1 500 €	KABA
3 Zdroje napájení						
3.1	Je k dispozici redundance běžného zdroje napájení			x	0 €	náprava je vysoce nákladná, žádný záložní generátor v případě nouze
3.2	Je nainstalována redundantní UPS s automatickým převzetím při výpadku zdroje napájení			x	1 500 €	druhý UPS/Rack
3.3	Dostatečná doba provozu z náhradního zdroje napájení (nejméně 2 hodiny)			x		maximální doba provozu 30 min., s novými UPS déle
3.4	Je prováděna údržba zdrojů napájení, včetně pravidelného testování a dokumentace			x	0 €	zajistit interními zdroji
3.5	Prodlužovačky odpovídají náročnosti na napájení a jsou pravidelně revidovány		x		750 €	průmyslové prodlužovačky
3.6	Systém napájení je dostatečně zdokumentován			x	0 €	zajistit interně, oddělení správy budov
4 Klimatizace						
4.1	Teplota se pohybuje mezi min. +10°C a max.+35°C	x				
4.2	Relativní vlhkost se pohybuje od 20 % do 80 %, přičemž nedochází ke kondenzaci vody ze vzduchu	x				
4.3	Klimatizovaný vzduch je filtrován od prachu	x				
4.4	Je prováděna pravidelná údržba klimatizačních jednotek	x				
4.5	Je k dispozici redundantní klimatizační jednotka	x				
4.6	Teplota je monitorována	x				PRTG systém
4.7	Systém klimatizace je dostatečně zdokumentován			x	0 €	zajistit interními zdroji
5 Požární ochrana						
5.1	Systém požární ochrany je v souladu s národní legislativou	x				
5.2	Požární ochrana odpovídá normě ČSN EN 13 501-2 (RE30)			x		
5.3	Uspořádání serverovny nepřispívá k riziku nekontrolovatelného šíření požáru	x				
5.4	Serverovna je monitorována automatickým systémem detekce požáru/kouře	x				
5.5	Detektory kouře/ohně jsou umístěny jak ve zdvojené podlaze, tak zavěšeny na stropu		x			zavěšeny na stropě
5.6	Jsou instalovány schválené požární uzávěry pro zpomalení hoření a zařízení pro odvod tepla a kouře			x	741 €	
5.7	V serverové místnosti platí zákaz kouření a není povoleno vykonávat horké práce (svařování, apod.)	x				zákaz kouření v celé budově
5.8	V serverovně, nebo poblíž ní, je k dispozici ruční hasicí přístroj bez obsahu prášku		x		200 €	hasicí přístroj plný CO2
5.9	Systém požární ochrany je dostatečně zdokumentován		x			obecně pro celou lokalitu
5.10	Je instalován systém automatického hašení ohně (pokud tento systém není instalován, je nutný ruční hasicí přístroj)			x	0 €	ruční hasicí přístroj
5.11	Je instalován systém pro včasnou detekci požáru (EPS)			x		
6 Ochrana proti vodě - pokud je relevantní						
6.1	Je instalován systém pro detekci vody					nerelevantní
6.2	Potrubí s kapalinou obsahuje ochranu proti úniku kapaliny					nerelevantní
6.3	Potrubí je pravidelně kontrolováno, jestli není poškozeno nebo z něj neuniká kapalina					nerelevantní
6.4	Systém ochrany proti vodě je dostatečně zdokumentován					nerelevantní
7 Systém hlášení						
7.1	Všechny nezbytné strany jsou o vzniklém problému informovány vhodným způsobem			x	0 €	zajistit interními zdroji
7.2	Všechny systémy jsou monitorovány		x		750 €	upozornění jsou zasílány na sdílený email IT; zasílat sms zprávy systémem PRTG
7.3	Systém monitoringu a hlášení je dostatečně zdokumentován			x	0 €	zajistit interními zdroji
					19 390,74 €	

Příloha č. 11: IT audit checklist – serverovna č. 2 lokalita A (25)

Checklist pro audit serverovny		Lokalita A - serverovna č. 2				
		Splňuje	Částečně splňuje	Nesplňuje	Odhad nákladů	Opatření
1 Vybavení						
1.1	Serverovna je umístěna odděleně v bezpečné části budovy	x				
1.2	Serverovna je permanentně bezpečně uzamčena vhodnými dveřmi			x	3 000 €	nové dveře
1.3	V případě nebezpečí je možné snadno otevřít dveře a opustit místnost	x				
1.4	Všechny dvířka racků lze zcela otevřít a zavřít, aniž by došlo k zablokování východu	x				
1.5	Okna serverovny jsou zabezpečeny vhodným způsobem	x				
1.6	Serverovna je dostatečně osvětlena	x				
1.7	Serverovna není využívána pro další účely, např. jako sklad nebo kancelář		x		0 €	úklid serverovny interními zdroji
1.8	V serverovně nejsou umístěny žádné hořlaviny nebo výbušniny	x				
1.9	Je zabudována přepětová ochrana a ochrana proti zásahu bleskem	x				
1.10	Systém kabeláže je dobře zdokumentován		x		0 €	zdokumentovat interními zdroji
1.11	Nepotřebné kabely jsou odstraněny		x		0 €	zajistit interními zdroji
1.12	Napájecí a datové kabely jsou kryty izolací bez obsahu chlórů					nelze určit
1.13	V serverovně je pravidelně prováděn úklid kvalifikovaným personálem			x	0 €	zajistit interními zdroji
1.14	Pokud v serverovně provádí úklid nekvalifikovaný personál, je na něj dohlíženo					nerrelevantní
1.15	Dveře serverovny jsou zvenku označeny neutrálním nápisem (např. technická místnost)	x				
1.16	Veškeré komponenty nejsou přímo vystaveny slunečnímu záření	x				
1.17	Kabeláž je přehledně organizována, je k ní jednoduchý přístup a kabely jsou označeny štítkem			x	2 000 €	zajistit externími zdroji
1.18	Napájecí a datové kabely jsou vedeny v oddělených kabelových trasách			x	300 €	externí spol. nebo zajistit vlastními zdroji
1.19	Všechny racky jsou dostatečně chlazený suchým vzduchem z klimatizace	x				
1.20	Všechny racky jsou postaveny do vertikální polohy	x				
1.21	Všechny komponenty uvnitř racku jsou přístupné jak ze své přední, tak ze zadní strany	x				
1.22	Všechny racky jsou 800 mm široké a 1000 mm hluboké			x	2 500 €	nové racky
1.23	Serverovna je vybaveny zdvojenou nebo zvýšenou podlahou			x	0 €	
2 Řízení přístupu						
2.1	Přístup do serverovny je umožněn pouze omezené skupině oprávněných osob	x				pracovníci IT mají vlastní klíče, rezervní klíč je umístěn na vratnici
2.2	Rozvodné skříně jsou chráněny před neoprávněným přístupem			x	200 €	pojistky jsou umístěny na chodbě, je možno zabezpečit dveře s klíči
2.3	Přístup do serverovny je dohledován a dokumentován	x				log přístupový systém SBI
2.4	Serverovna je zabezpečena systémem detekce neoprávněného vstupu (systém PZTS)		x		2 000 €	je umožněn přístup na kartu zvnějšku, dále zadání PINu uvnitř místnosti, alarm; nutné nasadit systém detekce průniku
2.5	V serverovně je nainstalován kamerový systém			x	1 000 €	kamerový systém
2.6	Systém řízení přístupu je dostatečně popsán			x	0 €	zajistit interními zdroji
2.7	Je implementován elektronický systém řízení přístupu			x	1 500 €	KABA
3 Zdroje napájení						
3.1	Je k dispozici redundance běžného zdroje napájení			x	0 €	náprava je vysoce nákladná, žádný záložní generátor v případě nouze
3.2	Je nainstalována redundantní UPS s automatickým převzetím při výpadku zdroje napájení			x	1 500 €	druhý UPS/Rack
3.3	Dostatečná doba provozu z náhradního zdroje napájení (nejméně 2 hodiny)			x		maximální doba provozu 30 min., s novými UPS déle
3.4	Je prováděna údržba zdrojů napájení, včetně pravidelného testování a dokumentace			x	0 €	zajistit interními zdroji
3.5	Prodlužovačky odpovídají náročnosti na napájení a jsou pravidelně revidovány		x		750 €	průmyslové prodlužovačky
3.6	Systém napájení je dostatečně zdokumentován			x	0 €	zajistit interní, oddělení správy budov
4 Klimatizace						
4.1	Teplota se pohybuje mezi min. +10°C a max.+35°C	x				
4.2	Relativní vlhkost se pohybuje od 20 % do 80 %, přičemž nedochází ke kondenzaci vody ze vzduchu	x				
4.3	Klimatizovaný vzduch je filtrován od prachu	x				
4.4	Je prováděna pravidelná údržba klimatizačních jednotek	x				
4.5	Je k dispozici redundantní klimatizační jednotka	x				
4.6	Teplota je monitorována			x	500 €	systém pro monitoring teploty
4.7	Systém klimatizace je dostatečně zdokumentován			x	0 €	zajistit interními zdroji
5 Požární ochrana						
5.1	Systém požární ochrany je v souladu s národní legislativou	x				
5.2	Požární ochrana odpovídá normě ČSN EN 13 501-2 (REI30)			x		
5.3	Uspořádání serverovny nepřispívá k riziku nekontrolovatelného šíření požáru	x				
5.4	Serverovna je monitorován automatickým systémem detekce požáru/kouře	x				
5.5	Detektory kouře/ohně jsou umístěny jak ve zdvojené podlaze, tak zavěšeny na stropu		x			zavěšeny na stropě
5.6	Jsou instalovány schválené požární uzávěry pro zpomalení hoření a zařízení pro odvod tepla a kouře			x	741 €	
5.7	V serverové místnosti platí zákaz kouření a není povoleno vykonávat horké práce (svařování, apod.)	x				zákaz kouření v celé budově
5.8	V serverovně, nebo poblíž ní, je k dispozici ruční hasicí přístroj bez obsahu prášku		x		200 €	hasicí přístroj plněný CO2
5.9	Systém požární ochrany je dostatečně zdokumentován		x			obecně pro celou lokalitu
5.10	Je instalován systém automatického hašení ohně (pokud tento systém není instalován, je nutný ruční hasicí přístroj)			x	0 €	ruční hasicí přístroj
5.11	Je instalován systém pro včasnou detekci požáru (EPS)			x		
6 Ochrana proti vodě - pokud je relevantní						
6.1	Je instalován systém pro detekci vody					nerrelevantní
6.2	Potrubí s kapalinou obsahuje ochranu proti úniku kapaliny					nerrelevantní
6.3	Potrubí je pravidelně kontrolováno, jestli není poškozeno nebo z něj uniká kapalina					nerrelevantní
6.4	Systém ochrany proti vodě je dostatečně zdokumentován					nerrelevantní
7 Systém hlášení						
7.1	Všechny nezbytné strany jsou o vzniklém problému informovány vhodným způsobem			x	0 €	zajistit interními zdroji
7.2	Všechny systémy jsou monitorovány		x		750 €	upozornění jsou zasílány na sdílený email IT; nahradit novým systémem monitoringu PRITG
7.3	Systém monitoringu a hlášení je dostatečně zdokumentován			x	0 €	zajistit interními zdroji
					16 940,74 €	

Příloha č. 12: Náklady na úpravu serveroven (25)

Oblast	Položka	Zajistit Externě/Interně	Využití		
			Switchovna/Telefonní ústředna	Switchovna	Switchovna/Telefonní ústředna
			Lokalita B - serverovna 1	Lokalita A - serverovna 1	Lokalita A - serverovna 2
Vybavení	Protipožární dveře	Externě	3 000 €	-	3 000 €
	Změna pozice racků	Interně	-	-	-
	Úklid serverovny, aby nesloužila jako sklad	Interně	-	-	-
	Dostatečně zdokumentovat systému kabeláže	Interně	-	-	-
	Reorganizace kabeláže externí společností	Externě	2 000 €	1 000 €	1 000 €
	Oddělit trasy napájecích a datových kabelů	Interně	300 €	300 €	300 €
	Nové racky 800 mm široké a 1000 mm hluboké	Interně	-	-	-
	Zdvojená podlaha	Externě	-	-	-
Řízení přístupu	Zabezpečit rozvodnou skříň s jističi (uzamykatelné dveře)	Interně	100 €	100 €	100 €
	Systém detekce neoprávněného vstupu (PZTS)	Externě	2 000 €	-	2 000 €
	Kamery systém	Externě	-	-	500 €
	Elektronické řízení přístupu	Externě	1 500 €	1 500 €	1 500 €
Zdroje napájení	Redundantní zdroj napájení	Interně	-	-	-
	Redundantní UPS s automatickým převzetím při výpadku	Externě	2 000 €	-	2 000 €
	Doba provozu nejméně 2 hodiny z náhradního zdroje napájení (dieselový agregátor)	Externě	-	-	-
	Průmyslové prodlužovačky	Externě	400 €	400 €	400 €
Klimatizace	Monitoring teploty	Interně	500 €	-	500 €
Požární ochrana	Automatický hasicí systém	Externě	-	-	-
	Dokumentace požární ochrany	Interně	-	-	-
	Hasicí přístroje s CO2	Externě	200 €	-	200 €
	Splnění standardu REI30	Externě	sádkokarton	zděné stěny	zděné stěny
Systém hlášení	Monitoring všech systémů	Interně	500 €	-	500 €
			12 500 €	3 300 €	12 000 €
		Náklady celkem			27 800 €
			kurz EUR	27	750 600 Kč

Příloha č. 13: Projektový plán – seznam úkolů a zdroje (25)

Číslo úkolu	Název úkolu	Doba trvání	Zahájení	Dokončení	Předchůdci	Náklady
1	Předprojektová fáze	31 dny	2. 11. 2015	14. 12. 2015		70.000 Kč
2	Analýza současného stavu (=studie příležitostí)	19 dny	2. 11. 2015	26. 11. 2015		20.000 Kč
3	Přehled hardware a jeho parametrů	5 dny	2. 11. 2015	6. 11. 2015		0 Kč
4	Přehled virtuálních serverů, software a aplikací	5 dny	2. 11. 2015	6. 11. 2015		0 Kč
5	Zjištění zatížení sítě	14 dny	2. 11. 2015	19. 11. 2015		0 Kč
6	Identifikace množství dat k migraci	3 dny	9. 11. 2015	11. 11. 2015	3;4	0 Kč
7	Analýza provozních nákladů na virtualizační infrastrukturu	14 dny	9. 11. 2015	26. 11. 2015	3;4	0 Kč
8	Vyhodnocení studie příležitostí	3 dny	27. 11. 2015	1. 12. 2015	5;7;6	0 Kč
9	Studie příležitostí vyhodnocena	0 dny	1. 12. 2015	1. 12. 2015	8	0 Kč
10	Studie proveditelnosti	9 dny	2. 12. 2015	14. 12. 2015		50.000 Kč
11	Určení hardware k přesunu	3 dny	2. 12. 2015	4. 12. 2015	9	0 Kč
12	Stanovení rychlosti připojení	1 den	2. 12. 2015	2. 12. 2015	9	0 Kč
13	Analýza stakeholderů	1 den	7. 12. 2015	7. 12. 2015	11;12	0 Kč
14	Analýza rizik	2 dny	8. 12. 2015	9. 12. 2015	13	50.000 Kč
15	Sestavení rozpočtu projektu	3 dny	10. 12. 2015	14. 12. 2015	14	0 Kč
16	Schválení projektu vedením	0 dny	14. 12. 2015	14. 12. 2015	15	0 Kč
17	Projektová fáze	463,72 dny	15. 12. 2015	22. 9. 2017		308.000 Kč
18	Zahájení	2 dny	15. 12. 2015	16. 12. 2015		0 Kč
19	Vytvoření zadávací listiny projektu	1 den	15. 12. 2015	15. 12. 2015	16	0 Kč
20	Odsouhlasení zadání Projektu vedením	1 den	16. 12. 2015	16. 12. 2015	19	0 Kč
21	Plánování	83 dny	17. 12. 2015	11. 4. 2016		0 Kč
22	Stanovení kritérií pro výběrové řízení na poskytovatele	2 dny	17. 12. 2015	18. 12. 2015	20	0 Kč

23	Výběrové řízení na poskytovatele	30 dny	21. 12. 2015	29. 1. 2016	22	0 Kč
24	Posouzení nabídek a výběr poskytovatele	10 dny	1. 2. 2016	12. 2. 2016	23	0 Kč
25	Poskytovatel vybrán	0 dny	12. 2. 2016	12. 2. 2016	24	0 Kč
26	Návrh WAN do DC	10 dny	15. 2. 2016	26. 2. 2016	25	0 Kč
27	Návrh LAN v DC	5 dny	15. 2. 2016	19. 2. 2016	25	0 Kč
28	Stanovení tříd QoS pro aplikace	3 dny	15. 2. 2016	17. 2. 2016	25	0 Kč
29	Nastavení smluvních podmínek	10 dny	29. 2. 2016	11. 3. 2016	26;27;28	0 Kč
30	Podpis smlouvy	1 den	14. 3. 2016	14. 3. 2016	27;28;29	0 Kč
31	Smluvní vztah s poskytovatelem uzavřen	0 dny	14. 3. 2016	14. 3. 2016	30	0 Kč
32	Návrh způsobu migrace hardware a dat	20 dny	15. 3. 2016	11. 4. 2016	31	0 Kč
33	Řešení odsouhlaseno	0 dny	11. 4. 2016	11. 4. 2016	32	0 Kč
34	Realizace	393,72 dny	15. 3. 2016	15. 9. 2017		308.000 Kč
35	Nákup zařízení (switche, firewally)	30 dny	15. 3. 2016	25. 4. 2016	31	280.000 Kč
36	Přidělení rozsahu IP adres	2 dny	15. 3. 2016	16. 3. 2016	31	0 Kč
37	Návrh pravidel na firewallech	5 dny	17. 3. 2016	23. 3. 2016	31;36	0 Kč
38	Příprava prostoru v datovém centru (rack+CPE+switche +firewally)	30 dny	26. 4. 2016	6. 6. 2016	35	0 Kč
39	Rack v DC připraven	0 dny	6. 6. 2016	6. 6. 2016	38	0 Kč
40	Příprava CPE u zákazníka	2 dny	15. 3. 2016	16. 3. 2016	31	0 Kč
41	Zprovoznění služby IP connect (MPLS) v lokalitě B	365 dny	15. 3. 2016	7. 8. 2017	31	0 Kč
42	Zprovoznění služby IP connect (MPLS) v lokalitě A	365 dny	15. 3. 2016	7. 8. 2017	31	0 Kč
43	Optika připravena	0 dny	7. 8. 2017	7. 8. 2017	41;42	0 Kč
44	Zprovoznění služby Internet	30 dny	7. 6. 2016	18. 7. 2016	39	0 Kč
45	Zprovoznění připojení k matce - Subdodavatel 1	75 dny	7. 6. 2016	19. 9. 2016	39	0 Kč
46	Konfigurace switchů u zákazníka a v DC + nastavení pravidel	90 dny	20. 9. 2016	23. 1. 2017	45	0 Kč

	na firewall - Subdodavatel 2					
47	Otestování nastavení rozsah IP, propustnost sítě na testovacím zařízení (vypůjčený ESXi server)	14 dny	24. 1. 2017	10. 2. 2017	36;39;40;44;45;46	8.000 Kč
48	Zahájení etapy 1 - migrace lokality B	0 dny	7. 8. 2017	7. 8. 2017	47;43	0 Kč
49	Oznámení uživatelům o odstávce	1 den	8. 8. 2017	8. 8. 2017	48	0 Kč
50	Odpojení serverů od sítě	0,04 dny	14. 8. 2017	14. 8. 2017	49FS+3 dny	0 Kč
51	Zálohování SAN	0,08 dny	14. 8. 2017	14. 8. 2017	50	10.000 Kč
52	Převoz hardware 1. polovina	0,08 dny	14. 8. 2017	14. 8. 2017	51	0 Kč
53	Instalace hardware v DC	0,02 dny	14. 8. 2017	14. 8. 2017	52	0 Kč
54	Oživení infrastruktury a otestování	0,14 dny	14. 8. 2017	14. 8. 2017	53	0 Kč
55	Infrastruktura zprovozněna - zahájení provozu z DC	0 dny	14. 8. 2017	14. 8. 2017	54	0 Kč
56	Migrace 2. poloviny HW	1 den	21. 8. 2017	22. 8. 2017	55FS+5 dny	0 Kč
57	Obnovení failover stavu a ukončení etapy 1 - migrace lokality B	0 dny	22. 8. 2017	22. 8. 2017	56	0 Kč
58	Zahájení etapy 2 - migrace lokality A	0 dny	11. 9. 2017	11. 9. 2017	57FS+14 dny	0 Kč
59	Oznámení uživatelům o odstávce	1 den	11. 9. 2017	12. 9. 2017	58	0 Kč
60	Odpojení serverů od sítě	0,04 dny	15. 9. 2017	15. 9. 2017	59FS+3 dny	0 Kč
61	Zálohování SAN	0,08 dny	15. 9. 2017	15. 9. 2017	60	10.000 Kč
62	Převoz hardware	0,08 dny	15. 9. 2017	15. 9. 2017	61	0 Kč
63	Instalace hardware v DC	0,02 dny	15. 9. 2017	15. 9. 2017	62	0 Kč

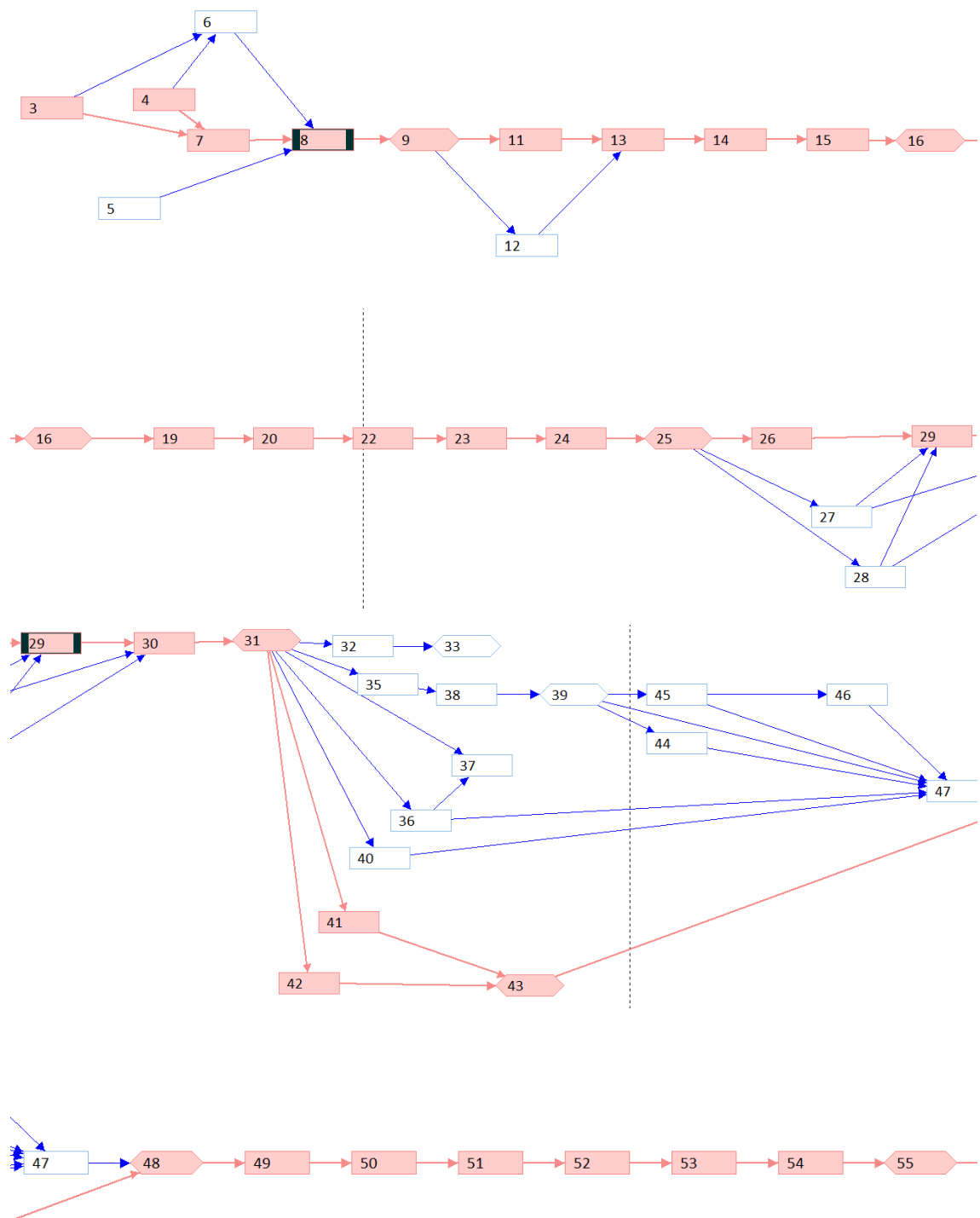
64	Oživení infrastruktury a otestování	0,14 dny	15. 9. 2017	15. 9. 2017	63	0 Kč
65	Infrastruktura zprovozněna - ukončení etapy 2 - migrace lokality A	0 dny	15. 9. 2017	15. 9. 2017	64	0 Kč
66	Ukončení	5 dny	15. 9. 2017	22. 9. 2017		0 Kč
67	Administrativní ukončení projektu, vyhotovení reportu a předání projektu vedení	5 dny	15. 9. 2017	22. 9. 2017	65	0 Kč
68	Projektová fáze ukončena	0 dny	22. 9. 2017	22. 9. 2017	67	0 Kč
69	Poprojektová fáze	368 dny	22. 9. 2017	20. 2. 2019		0 Kč
70	Vyhodnocení přínosů projektu - okamžité	3 dny	22. 9. 2017	27. 9. 2017	68	0 Kč
71	Vyhodnocení projektu - dlouhodobé hledisko	365 dny	22. 9. 2017	15. 2. 2019	67	0 Kč
72	Uzavření projektu	3 dny	15. 2. 2019	20. 2. 2019	71	0 Kč
73	Projekt ukončen	0 dny	20. 2. 2019	20. 2. 2019	72	0 Kč

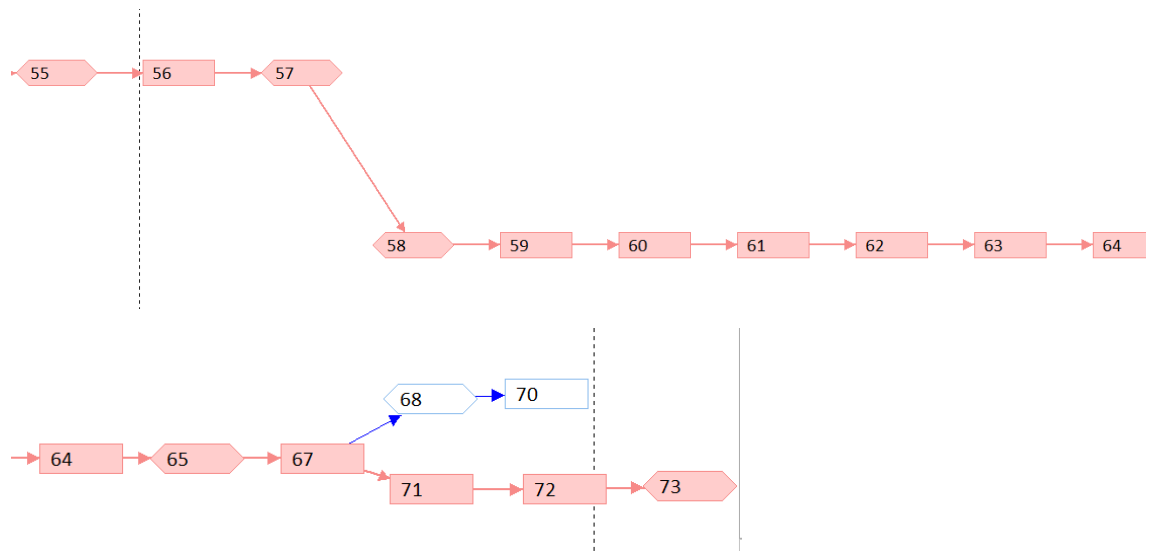
Příloha č. 14: Seznam kritických úkolů projektu (25)

ID	Název	Zahájení	Dokončení	Doba trvání	Nejdříve možné dokončení	Nejdříve možné zahájení	Nejpozději možné dokončení	Nejpozději možné zahájení
1	Předprojektová fáze	2.11. 15	14.12. 15	31 dny	14.12. 15	2.11. 15	15.12. 15	2.11. 15
2	Analýza současného stavu (=studie příležitosti)	2.11. 15	26.11. 15	19 dny	26.11. 15	2.11. 15	26.11. 15	2.11. 15
3	Přehled hardware a jeho parametrů	2.11. 15	6.11. 15	5 dny	6.11. 15	2.11. 15	6.11. 15	2.11. 15
4	Přehled virtuálních serverů, software a aplikací	2.11. 15	6.11. 15	5 dny	6.11. 15	2.11. 15	6.11. 15	2.11. 15
7	Analýza provozních nákladů na virtualizační infrastrukturu	9.11. 15	26.11. 15	14 dny	26.11. 15	9.11. 15	26.11. 15	9.11. 15
8	Vyhodnocení studie příležitostí	27.11. 15	1.12. 15	3 dny	1.12. 15	27.11. 15	1.12. 15	27.11. 15
9	Studie příležitostí vyhodnocena	1.12. 15	1.12. 15	0 dny	1.12. 15	1.12. 15	2.12. 15	2.12. 15
10	Studie proveditelnosti	2.12. 15	14.12. 15	9 dny	14.12. 15	2.12. 15	14.12. 15	2.12. 15
11	Určení hardware k přesunu	2.12. 15	4.12. 15	3 dny	4.12. 15	2.12. 15	4.12. 15	2.12. 15
13	Analýza stakeholderů	7.12. 15	7.12. 15	1 den	7.12. 15	7.12. 15	7.12. 15	7.12. 15
14	Analýza rizik	8.12. 15	9.12. 15	2 dny	9.12. 15	8.12. 15	9.12. 15	8.12. 15
15	Sestavení rozpočtu projektu	10.12. 15	14.12. 15	3 dny	14.12. 15	10.12. 15	14.12. 15	10.12. 15
16	Schválení projektu vedením	14.12. 15	14.12. 15	0 dny	14.12. 15	14.12. 15	15.12. 15	15.12. 15
17	Projektová fáze	15.12. 15	22.9. 17	463,72 dny	22.9. 17	15.12. 15	20.2. 19	15.12. 15
18	Zahájení	15.12. 15	16.12. 15	2 dny	16.12. 15	15.12. 15	16.12. 15	15.12. 15
19	Vytvoření zadávací listiny projektu	15.12. 15	15.12. 15	1 den	15.12. 15	15.12. 15	15.12. 15	15.12. 15
20	Odsouhlasení zadání projektu vedením	16.12. 15	16.12. 15	1 den	16.12. 15	16.12. 15	16.12. 15	16.12. 15
21	Plánování	17.12. 15	11.4. 16	83 dny	11.4. 16	17.12. 15	20.2. 19	17.12. 15
22	Stanovení kritérií pro výběrové řízení na poskytovatele	17.12. 15	18.12. 15	2 dny	18.12. 15	17.12. 15	18.12. 15	17.12. 15
23	Výběrové řízení na poskytovatele	21.12. 15	29.1. 16	30 dny	29.1. 16	21.12. 15	29.1. 16	21.12. 15
24	Posouzení nabídek a výběr poskytovatele	1.2. 16	12.2. 16	10 dny	12.2. 16	1.2. 16	12.2. 16	1.2. 16
25	Poskytovatel vybrán	12.2. 16	12.2. 16	0 dny	12.2. 16	12.2. 16	15.2. 16	15.2. 16
26	Návrh WAN do DC	15.2. 16	26.2. 16	10 dny	26.2. 16	15.2. 16	26.2. 16	15.2. 16
29	Nastavení smluvních podmínek	29.2. 16	11.3. 16	10 dny	11.3. 16	29.2. 16	11.3. 16	29.2. 16
30	Podpis smlouvy	14.3. 16	14.3. 16	1 den	14.3. 16	14.3. 16	14.3. 16	14.3. 16
31	Smluvní vztah s poskytovatelem uzavřen	14.3. 16	14.3. 16	0 dny	14.3. 16	14.3. 16	15.3. 16	15.3. 16
34	Realizace	15.3. 16	15.9. 17	393,72 dny	15.9. 17	15.3. 16	20.2. 19	15.3. 16
41	Zprovoznění služby IP connect (MPLS) v lokalitě B	15.3. 16	7.8. 17	365 dny	7.8. 17	15.3. 16	7.8. 17	15.3. 16
42	Zprovoznění služby IP connect (MPLS) v lokalitě A	15.3. 16	7.8. 17	365 dny	7.8. 17	15.3. 16	7.8. 17	15.3. 16

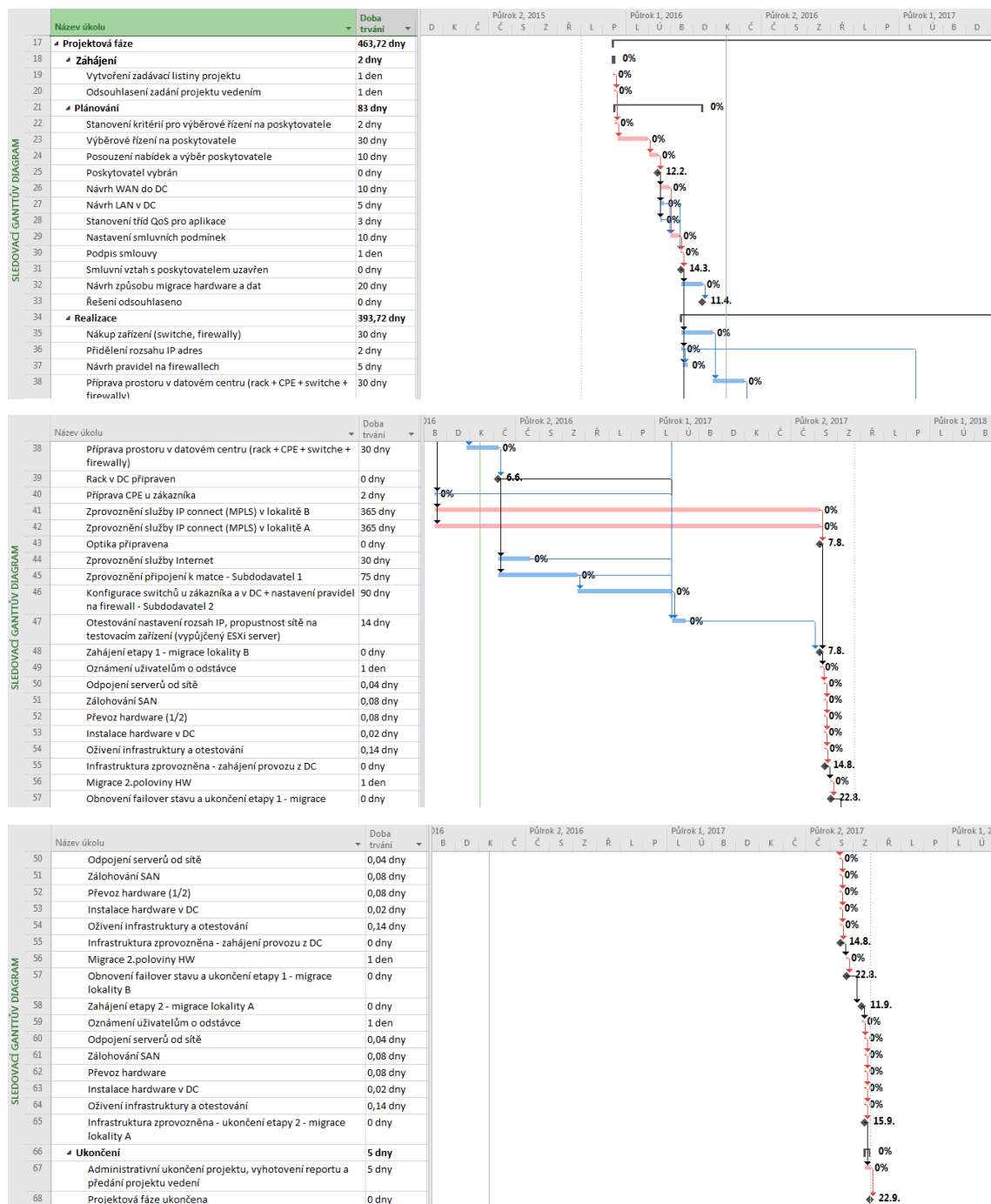
43	Optika připravena	7.8. 17	7.8. 17	0 dny	7.8. 17	7.8. 17	8.8. 17	8.8. 17
48	Zahájení etapy 1 - migrace lokality B	7.8. 17	7.8. 17	0 dny	7.8. 17	7.8. 17	8.8. 17	8.8. 17
49	Oznámení uživatelům o odstávce	8.8. 17	8.8. 17	1 den	8.8. 17	8.8. 17	8.8. 17	8.8. 17
50	Odpojení serverů od sítě	14.8. 17	14.8. 17	0,04 dny	14.8. 17	14.8. 17	14.8. 17	14.8. 17
51	Zálohování SAN	14.8. 17	14.8. 17	0,08 dny	14.8. 17	14.8. 17	14.8. 17	14.8. 17
52	Převoz hardware (1/2)	14.8. 17	14.8. 17	0,08 dny	14.8. 17	14.8. 17	14.8. 17	14.8. 17
53	Instalace hardware v DC	14.8. 17	14.8. 17	0,02 dny	14.8. 17	14.8. 17	14.8. 17	14.8. 17
54	Oživení infrastruktury a otestování	14.8. 17	14.8. 17	0,14 dny	14.8. 17	14.8. 17	14.8. 17	14.8. 17
55	Infrastruktura zprovozněna - zahájení provozu z DC	14.8. 17	14.8. 17	0 dny	14.8. 17	14.8. 17	14.8. 17	14.8. 17
56	Migrace 2.polovin HW	21.8. 17	22.8. 17	1 den	22.8. 17	21.8. 17	22.8. 17	21.8. 17
57	Obnovení failover stavu a ukončení etapy 1 - migrace lokality B	22.8. 17	22.8. 17	0 dny	22.8. 17	22.8. 17	22.8. 17	22.8. 17
58	Zahájení etapy 2 - migrace lokality A	11.9. 17	11.9. 17	0 dny	11.9. 17	11.9. 17	11.9. 17	11.9. 17
59	Oznámení uživatelům o odstávce	11.9. 17	12.9. 17	1 den	12.9. 17	11.9. 17	12.9. 17	11.9. 17
60	Odpojení serverů od sítě	15.9. 17	15.9. 17	0,04 dny	15.9. 17	15.9. 17	15.9. 17	15.9. 17
61	Zálohování SAN	15.9. 17	15.9. 17	0,08 dny	15.9. 17	15.9. 17	15.9. 17	15.9. 17
62	Převoz hardware	15.9. 17	15.9. 17	0,08 dny	15.9. 17	15.9. 17	15.9. 17	15.9. 17
63	Instalace hardware v DC	15.9. 17	15.9. 17	0,02 dny	15.9. 17	15.9. 17	15.9. 17	15.9. 17
64	Oživení infrastruktury a otestování	15.9. 17	15.9. 17	0,14 dny	15.9. 17	15.9. 17	15.9. 17	15.9. 17
65	Infrastruktura zprovozněna - ukončení etapy 2 - migrace lokality A	15.9. 17	15.9. 17	0 dny	15.9. 17	15.9. 17	15.9. 17	15.9. 17
66	Ukončení	15.9. 17	22.9. 17	5 dny	22.9. 17	15.9. 17	15.2. 19	15.9. 17
67	Administrativní ukončení projektu, vyhotovení reportu a předání projektu vedení	15.9. 17	22.9. 17	5 dny	22.9. 17	15.9. 17	22.9. 17	15.9. 17
69	Poprojektová fáze	22.9. 17	20.2. 19	368 dny	20.2. 19	22.9. 17	20.2. 19	22.9. 17
71	Vyhodnocení projektu - dlouhodobé hledisko	22.9. 17	15.2. 19	365 dny	15.2. 19	22.9. 17	15.2. 19	22.9. 17
72	Uzavření projektu	15.2. 19	20.2. 19	3 dny	20.2. 19	15.2. 19	20.2. 19	15.2. 19
73	Projekt ukončen	20.2. 19	20.2. 19	0 dny	20.2. 19	20.2. 19	20.2. 19	20.2. 19

Příloha č. 15: Síťový uzlový graf s kritickou cestou (25)





Příloha č. 16: Ganttův diagram pro projektovou fázi (25)



Příloha č. 17: Rozdělení virtuálních serverů na 3 hostitele (25)

Virtuální servery							
Umístěn na hostiteli č.	Označení VMs	Využitá kapacita GB	vRAM MB	Využití paměti RAM %	vCPU	Přidělené CPU hostitele MHz	vNIC
1	VMA1	513,65	2000	25	6	59	1
	VMA2	214,11	4096	3	2	19	1
	VMA3	208,13	8192	11	4	279	1
	VMA4	168,12	8192	13	2	179	1
	VMA5	151,40	4096	8	2	79	1
	VMA6	60,00	4096	0	2	0	1
	VMA7	54,12	4096	8	2	239	1
	VMA8	54,11	4096	2	2	19	1
	VMA9	44,12	4096	1	2	19	1
	VMA10	38,17	4096	18	2	39	1
	VMA11	10,62	512	20	1	0	1
	VMA12	8,62	512	2	1	0	1
	VMA13	3491,84	4096	8	2	59	1
	VMB14	407,05	4096	7	2	103	1
	VMB15	184,13	24576	16	4	1741	1
	VMB23	25,13	1024	6	1	0	3
2	VMA14	1105,92	8192	25	8	439	1
	VMA15	683,51	16384	0	4	0	1
	VMA16	308,18	12288	25	6	2738	2
	VMA17	275,39	3972	0	2	0	1
	VMA18	273,41	2060	0	4	0	1
	VMA19	216,13	16384	10	4	279	1
	VMA20	108,13	8192	3	4	19	1
	VMA21	106,12	6144	11	2	79	1
	VMA22	55,28	4096	0	2	0	1
	VMA23	50,12	4096	10	2	19	1
	VMA24	29,12	1024	10	1	19	1
	VMB7	52,11	12288	0	5	25	2
	VMB20	50,12	4096	2	2	0	1
	VMB21	48,50	8192	0	4	25	2
	VMB22	40,00	4096	0	2	0	1
3	VMB1	1710,08	4096	7	4	25	1
	VMB2	168,12	8192	81	2	1117	1
	VMB3	133,11	8192	27	2	207	1
	VMB4	114,11	14336	3	6	103	1
	VMB5	59,03	8192	11	5	77	1
	VMB6	52,80	2048	4	2	51	1
	VMB8	52,11	2048	12	1	181	1
	VMB9	48,13	8192	8	5	155	1
	VMB10	42,11	2048	7	1	0	1
	VMB11	29,01	1024	31	1	337	1
	VMB12	19,14	1024	2	2	0	1
	VMB13	10,32	2048	7	4	233	3
	VMB16	111,24	8192	2	4	25	1
	VMB17	68,13	8192	4	8	311	1
	VMB18	64,13	4096	5	4	25	1
	VMB19	50,13	4096	22	2	389	1