Univerzita Pardubice
Fakulta ekonomicko-správní
Ústav systémového inženýrství a informatiky

Plán obnovy po katastrofě

Jan Černý

Bakalářská práce
2013

Univerzita Pardubice
Fakulta ekonomicko-správní
Akademický rok: **2012/2013**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan Černý**
Osobní číslo:	**E09864**
Studijní program:	**B6209 Systémové inženýrství a informatika**
Studijní obor:	**Informační a bezpečnostní systémy**
Název tématu:	**Plán obnovy po katastrofě**
Zadávající katedra:	**Ústav systémového inženýrství a informatiky**

Zásady pro vypracování:

Plánování obnovy po katastrofě je významným prvkem v otázce řízení rizik a krizového managementu. Tvoří scénář jak postupovat v případě aktivace očekávané, ale i neočekávané hrozby.

Cílem práce je:

- formulovat postup tvorby plánu obnovy po katastrofě,
- vytvořit studijní materiály - případovou studii tvorby plánu obnovy po katastrofě pro účely výuky předmětu "Úvod do bezpečnosti a ochrany informací".

Rozsah grafických prací:

Rozsah pracovní zprávy:

Forma zpracování bakalářské práce: **tištěná**

Seznam odborné literatury:

BASL, J., BLAŽIČEK, R. Podnikové informační systémy: Podnik v informační společnosti. 2. vyd. Praha: Grada Publishing, 2008. 283 s. ISBN 978-80-247-2279-5.
BRABEC, F. Ochrana bezpečnosti podniku. 1. vyd. Praha: Eurounion, 1996. 203 s. ISBN 8080-85858-29-0.
GREGORY P. IT Disaster Recovery Plannig For Dummies. 1. vyd. Hoboken: Wiley Publishing, Inc., 2007. 360 s. ISBN 978-0-470-03973-1.
SMEJKAL, V., RAIS, K. Řízení rizik, 1. vyd. Praha: Grada Publishing., 2003. 270 s. ISBN 80-247-0198-7.
SNEDAKER, S. Business Continuity and Disaster Recovery Planning for IT Professionals. Burlington: Syngress, 2007. 456 s. ISBN 1-59749-172-1.

Vedoucí bakalářské práce: **Ing. Miloslav Hub, Ph.D.**
Ústav systémového inženýrství a informatiky

Datum zadání bakalářské práce: **1. října 2012**
Termín odevzdání bakalářské práce: **30. dubna 2013**

L.S.

doc. Ing. Renáta Myšková, Ph.D.
děkanka

prof. Ing. Jan Čapek, CSc.
vedoucí ústavu

V Pardubicích dne 3. října 2012

PROHLÁŠENÍ

Prohlašuji, že jsem tuto práci vypracoval samostatně. Veškeré literární prameny a informace, které jsem v práci využil, jsou uvedeny v seznamu použité literatury.

Byl jsem seznámen s tím, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorský zákon, zejména se skutečností, že Univerzita Pardubice má právo na uzavření licenční smlouvy o užití této práce jako Školního díla podle § 60 odst. 1 autorského zákona, a s tím, že pokud dojde k užití této práce mnou nebo bude poskytnuta licence o užití jinému subjektu, je Univerzita Pardubice oprávněna ode mne požadovat přiměřený příspěvek na úhradu nákladů, které na vytvoření díla vynaložila, a to podle okolností až do jejich skutečné výše.

Souhlasím s prezenčním zpřístupněním své práce v Univerzitní knihovně Univerzity Pardubice.

V Pardubicích dne 13. 8. 2013 Jan Černý

PODĚKOVÁNÍ:

Tímto bych rád poděkoval svému vedoucímu práce doc. Ing. Miloslavu Hubovi, Ph.D. za jeho odbornou pomoc, cenné rady a poskytnuté materiály, které mi pomohly při zpracování bakalářské práce. Dále velké poděkování patří celé mé rodině za bezmeznou podporu a trpělivost.

ANOTACE

Plánování obnovy po katastrofě je významným prvkem v otázce řízení rizik a krizového managementu. Tvoří scénář, jak postupovat v případě aktivace očekávané, ale i neočekávané hrozby. V reálném světě je tvorba plánu po katastrofě podceňována, přičemž dopady této absence jsou většinou nevratné. Cílem práce je formulace postupu tvorby plánu po katastrofě a vytvoření případové studie tvorby plánu po katastrofě pro účely výuky předmětu „Úvod do bezpečnosti a ochrany informací“.

KLÍČOVÁ SLOVA

Plánování, katastrofa, zálohování, obnova, případová studie.

TITLE

Disaster recovery plan

ANNOTATION

Disaster recovery plan is significant element in risk and risk management. It creates a scenario of a procedure in case of activation expected as well as unexpected threat. In the reality is creation of disaster recovery plan underestimated, while impacts of its absence are mostly irreversible. A goal of this work is formulation of the disaster recovery plan, studies of creation of disaster recovery plan of individual cases for the purpose of teaching topic "Introduction to safety and protection of information".

KEYWORDS

Planning, disaster, backup, recovery, case study.

OBSAH

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

AHS	Automatický hasící systém
BCP	Plán kontinuity podnikových procesů (Business Continuity Plan)
BP	Bakalářská práce
DRP	Plán obnovy po katastrofě (Disaster Recovery Plan)
DTT	Metoda disk páska (Disc To Tape)
EPS	Elektronický požární systém
EZS	Elektronický zabezpečovací systém
FES	Fakulta ekonomicko-správní
HA	Vysoká dostupnost (High Availability)
HW	Hardware
ICT	Informační a komunikační technologie (Information and Communication Technology)
IS	Informační systém (Information System)
MTD	Maximální doba tolerované nedostupnosti (Maximum Torelable Downtime)
NBD	Následující pracovní den (Next Business Day)
PCO	Pult centrální ochrany
PDCA	Systém kontinuálního zlepšování kvality (Plann, Do, Check, Act)
RTO	Akceptovatelný čas obnovy (Recovery Time Objective)
RPO	Akceptovatelná ztráta dat (Recovery Point Objective)
SLA	Smlouva o garantované úrovni služeb (Service Level Agreement)
SMB	Malé a střední podniky (Small and Medium Business)
SW	Software
UPa	Univerzita Pardubice

ÚVOD

Problematika plánování obnovy po katastrofě (DRP) je významným prvkem v otázce řízení rizik a krizového managementu. V reálném světě je tvorba plánu po katastrofě podceňována, přičemž dopady této absence jsou většinou nevratné. Pro ochranu dat a běh informačních systémů (IS), na kterých je v současné době závislá většina společností, institucí a úřadů, se jedná o jeden z klíčových prvků pro zajištění kontinuity podnikových procesů (BCP). Taktéž jsou čím dál více vyžadovány znalosti s tvorbou DRP i po absolventech vysokých škol se zaměřením na informační a komunikační technologie (ICT) ze strany zaměstnavatelů.

Problematikou DRP v prostředí ICT se na Fakultě ekonomicko-správní Univerzity Pardubice (FES UPa) zabývá předmět „Úvod do bezpečnosti a ochrany informací“ a ač se DRP v osnovách předmětu nachází, je při jeho výuce zmiňováno pouze okrajově. Zároveň pro výuku neexistuje žádný dostatečně ucelený studijní materiál, který by problematiku komplexně pokrýval. Na problém reflektuje tato bakalářská práce (BP) a nabízí řešení v podobě formulace a následné demonstrace postupu tvorby DRP na případové studii imaginární advokátní kanceláře LAW+. Takto vzniklé podklady jsou následně transformovány do studijního materiálu a prezentace pro výuku zmíněného předmětu.

Na tomto místě je vhodné zmínit, že problematika tvorby DRP je poměrně rozsáhlá a pokrývá široké spektrum oblastí. Obsah BP se primárně zaměřuje na obnovu ICT zdrojů potřebných pro chod společnosti jako je infrastruktura, hardwarové (HW) a softwarové (SW) vybavení, dodávka energií, ale samozřejmě se zároveň zabývá otázkou potřebných lidských zdrojů, provozních prostor, dodavatelských služeb a nákladů.

1 ANALÝZA SOUČASNÉHO STAVU VÝUKY DRP NA FES UPA

Aby bylo možné zjistit, zda v některém předmětu vyučovaném v rámci bakalářského studia na FES UPa je problematika DRP vyučována do potřebné hloubky, bylo v první řadě nutné analyzovat obsah všech předmětů. Zde posloužil jako zdroj relevantních informací obsah webového portálu FES UPa na jehož základě bylo možné vytvořit tabulku č. 1, která reprezentuje množinu předmětů s potencionální vazbou na DRP. Následně byli kontaktováni vyučující všech vybraných předmětů s žádostí o potvrzení předchozí domněnky.

Tabulka č. 1: Předměty s vazbou na DRP [7].

Studijní program a zkr. předmětu	Předmět	Vyučující	Vyučováno DRP
Ekonomika a provoz podniku, 6208R146/99			
USII/KUBOI	Úvod do bezpečnosti a ochrany informací	doc. Ing. Miloslav Hub, Ph.D.	Ano
USII/KISVS	Úvod do informačních systémů	doc. Ing. Komárková Jitka, Ph.D. Ing. Kopáčková Hana, Ph.D.	Ne
USII/KDBS1	Databázové systémy I	Ing. Šimonová Stanislava, Ph.D.	Ano
URBV/KKRM	Krizový management	doc. Ing. Roudný Radim, CSc.	Ano
UPEM/KORZ	Organizace provozu podniku	doc. Ing. Buchta Miroslav, CSc.	Ne
UPEM/KZMR	Základy manažerského rozhodování	doc. Ing. Roudný Radim, CSc.	Ano
UPEM/KPLO	Podniková logistika	doc. Ing. Kampf Rudolf, CSc. doc. RNDr. Linda Bohdan, CSc.	Ne
UPEM/KEIK	Externí a interní komunikace podniku	PaedDr. Šenec Alexandr doc. Dr. Ing. Siegl Milan, CSc.	Ne
URBV/KAPO	Audit podniku a jeho operací	doc. Ing. Kraftová Ivana, CSc. Ing. Svoboda Ondřej	Ne
URBV/KPR	Podnik v regionálním prostředí	Ing. Mandysová Ivana, Ph.D.	Ne
UPEM/KSTM	Strategický management	doc. Ing. Myšková Renáta, Ph.D.	Ne
Management ochrany podniku a společnosti, 6208R147/99			
URBV/KOSP	Ochrana společnosti	doc. Ing. Roudný Radim, CSc. doc. Ing. Janošec Josef, CSc.	Ano
URBV/KSPBK	Bezpečnost a krize	doc. Ing. Roudný Radim, CSc.	Ano
URBV/KOOT	Ochrana obyvatelstva a terorismus	doc. Ing. Janošec Josef, CSc. Ing. Svoboda Ondřej	Ne
URBV/KTRS	Teorie rizika a spolehlivosti	doc. Ing. Roudný Radim, CSc.	Ano
URBV/KRIP	Rizika podniku	doc. Ing. Kampf Rudolf, CSc.	Ano
USII/KIKS	Informační a komunikační systémy	prof. Ing. Dvořák Jiří, DrSc. doc. Ing. Komárková Jitka, Ph.D. Ing. Kopáčková Hana, Ph.D.	Ne

Management podniku: Management malých a středních podniků, 6208R126/11			
Management podniku: Manažerská etika, 6208R126/22			
Veřejná ekonomika a správa, 6202R055/1			
Veřejná ekonomika a správa: Ekonomika pro kriminalisty a celníky, 6202R055/2			
Ekonomika a celní správa, 6202R068/99			
Ekonomika pro kriminalisty, 6202R069/99			
Veřejná ekonomika a správa, 6202R055/11			
Informační a bezpečnostní systémy, 6209R029/99			
USII/PZDE	Počítačové zpracování dat	Ing. Jonášová Hana, Ph.D. Ing. Jirava Pavel, Ph.D. Ing. Horák Oldřich	Ne
USII/PSBT	Speciální bezpečnostní technika	Ing. Novák Martin	Ne
USII/PISR	Informační systémy regionů	Ing. Jonášová Hana, Ph.D. Ing. Horák Oldřich	Ne
USII/PPSI1	Počítačové sítě I	Ing. Horák Oldřich	Ne
USII/PSIN	Úvod do systémové integrace	prof. Ing. Dvořák Jiří, DrSc. Ing. Bílková Renáta	Ne
Informatika ve veřejné správě, 6209R019/88			
Management finančních rizik, 6209R035/99			
UEV/PMRFI	Modelování rizik finančních institucí	prof. RNDr. Sekerka Bohuslav, CSc. Mgr. Slavíček Ondřej	Ne
Regionální a informační management, 6209R028/99			

V rámci emailové ankety a osobních konzultací došlo k získání potřebných informací o výuce a studijních materiálech pokrývajících tvorbu DRP a k přiřazení příznaků o vazbě na výuku DRP u dotčených předmětů. Závěr analýzy pak ukázal, že ač 8 předmětů z celkových 23 problematiku plánování obnovy po katastrofě obsahuje, tak pouze ve všeobecné rovině, jako jednu z částí obecného řízení rizik.

Na základě těchto výsledků bylo možné konstatovat, že se na FES UPa problematice DRP detailně nevěnuje žádný z předmětů vyučovaných v rámci bakalářského studia a tím pádem pro jeho výuku neexistují dostatečné studijní materiály.

2 VYTYČENÍ CÍLŮ A NÁVRH ŘEŠENÍ

Na základě závěru z analýzy výuky DRP na FES UPa bylo možné formulovat cíle BP a navrhnout řešení.

- Hlavní cíl - formulace postupu tvorby plánu po katastrofě a vytvoření případové studie tvorby plánu po katastrofě pro účely výuky předmětu „Úvod do bezpečnosti a ochrany informací“.
- Dílčí cíl 1 – vytvoření jedné kapitoly skript.
- Dílčí cíl 2 – vytvoření prezentace pro výuku předmětu.

BP nabízí řešení v podobě vytvoření studijních materiálů, které seznámí čtenáře se základními pojmy problematiky a formulují postup tvorby DRP na reálném příkladu případové studie.

3 DEFINICE ZÁKLADNÍCH POJMŮ

3.1 Pojem „plán obnovy po katastrofě“

Jedná se o scénář, který je uplatněn v případě, že je aktivována hrozba a dojde ke katastrofě. Obsahuje povinnosti jednotlivých osob a subjektů dle jejich zodpovědnosti a dále pak postupy, které jsou aplikovány na opravné prostředky s cílem zabezpečit funkci klíčových systémů a činností a to v co nejkratším možném časovém intervalu.

Samotné slovo katastrofa hraje ve vytyčení pojmu zásadní roli a je nutné definovat hned na začátku i jeho význam.

Podle přísné definice je v užším smyslu katastrofa procesem, který za sebou zanechá lidské oběti a materiální škody. Kolik to má být minimálně obětí a jaké škody, na tom se odborníci neshodli. Podle terminologie používané významnými světovými organizacemi, jako jsou Organizace spojených národů, Světová banka a Evropská banka, musí být počet obětí nejméně 25 a škod alespoň za 25 milionů dolarů. Jedna položka však stačí. Buď počet obětí, nebo materiální škody. Pokud jsou následky menší, dávají tyto organizace přednost termínu „disaster“ (česky pohroma). Jiným jazykovým problémem je slovo „rychlý“. Katastrofa má být „rychlým procesem“. Co však tím přesně rozumíme? Geologové pod slovem „rychlý“ mohou chápat i něco, co trvá desetitisíce let. Je-li však něco „rychlého“ v případě přírodních katastrof, pak to jsou vteřiny, minuty, hodiny, dny, někdy i týdny. Pochod samotný může trvat vteřiny, jeho následky však i mnoho let. [9]

Důvody vytváření plánů obnovy po katastrofě

Důvodů pro vytváření DRP je hned několik. Asi nejdůležitější je, aby společnost, popř. jiný subjekt, na který je plán aplikován, byl připraven a zároveň smířen s faktem možného propuknutí katastrofy. DRP přináší výhody v podobě zkrácení potřebného času pro obnovu, maximální eliminace ztrát a finanční transparentnosti nákladů (veškeré časy, ztráty a náklady jsou již dopředu známy) na základě řízeného procesu. S tím je spojena další nesporná výhoda a tou je možné začlenění DRP do BCP.

3.2 Klíčové faktory při tvorbě DRP

Doba nedostupnosti (Downtime)

Dostupnost můžeme definovat jako časový interval, po který je systém nebo služba, k dispozici dalším systémům, v konečné fázi uživatelům. Nedostupnost je pak pravým opakem dostupnosti. Ač se může zdát, že je vhodnější v DRP pracovat s dostupností, opak je pravdou. Právě nedostupnost je klíčovým faktorem v plánování. Její maximální tolerovaná doba (MTD) se může pro jednotlivé systémy lišit dle důležitosti a pracovní náplně každé organizace provozující nějakou formu ICT.

Čas jsou peníze a v případě nedostupnosti dat to platí bezezbytku. Společnost Contingency Planning Research spočítala, že běžnou americkou společnost stojí hodina nedostupnosti dat přibližně 18 000 dolarů (342 000 českých korun). Pro organizace je tak prvořadou prioritou vědět, jak rychle se data podaří obnovit, respektive jak dlouho nebude fungovat společnost či její část. [6]

Obnova terabajtů dat z magnetických pásek znamená nejprve určit, které pásky je konkrétně nutné vybrat, poté poslat požadavek na jejich doručení z externí společnosti, kde jsou pásky uloženy (nemá smysl je ukládat na stejném místě, kde by je mohla přírodní katastrofa zničit spolu s primárními daty), následuje korelace každé pásky se záznamy určení, kterou pásku nahrát jako první. Následně začíná skutečné nahrávání záložních dat. Tento poměrně náročný proces může v závislosti na rozsahu zabrat i několik dní. Obnova dat přímo z HDD umístěných přímo v prostorách organizace je operativnější a rychlejší, nicméně jak už bylo zmíněno, takový disk je pak vystaven stejným vnějším ohrožením jako primární data. [6]

Integrita dat

Tradiční procesy obnovy dat jsou jen málokdy stoprocentně úspěšné. Jinak řečeno některé soubory jsou prostě nenávratně ztraceny. Pokud se tyto údaje týkají zákazníků, obchodních transakcí, či jiných oblastí kde nemohou být data snadno reprodukována, vede to k tomu, že ztracené informace jsou i ztracenými příjmy. [6]

Jako úložiště dat je magnetická páska chronicky nespolehlivá. Jde také o to, že je nepoužitelná pro průběžné zálohování. Obvykle se zálohy provádějí jednou denně. Z toho plyne, že v průměru jsou zálohovaná data o 12 hodin starší než data právě ztracená. Některé průzkumy ukazují, že až 20 % pravidelných nočních záloh neproběhne úspěšně.

To znamená, že se nezkopírují všechna data. Ještě horší jsou některé údaje, které říkají, že až 40% případů obnovy dat z pásek zcela selže. [6]

Disk mirroring čili duplikace dat na druhý pevný disk, nabízí klasickou, spolehlivou datovou redundanci, nicméně v případě nenadálé události stále dochází ke ztrátě dat vzniklých od poslední zálohy. Synchronní replikace plně nechrání před ztrátou dat, protože pokud je poškozen software, např. z důvodu kolapsu operačního systému (OS), napadení virem apod., dojde k přenesení chybových stavů i na repliku. Následně je chybový stav zkopírován i do záloh. Takto vzniklé zálohy není možné následně použít pro obnovu. [6]

Bezpečnost

Stejně jako musí být dobře chráněno primární úložiště dat, tak musí být zabezpečeno i zálohovací místo. Některé prostory nabízejí perfektní zabezpečení. Nicméně stále přetrvává riziko poškození datových pásek při převozu. V krajním případě může dojít k jejich ztrátě – nedovřené dveře, díra v tašce, nepozorný personál a citlivá firemní data se povalují na ulici. V případě pevných disků je bezpečnost dat zcela závislá na interních bezpečnostních mechanizmech. [6]

Jednoduchost

Havárie je sama o sobě velký problém, obnova dat by jím proto být neměla. Tradiční strategie posouvají IT administrátory do klikatých cestiček starostí o hardware a vedení datového účetnictví, ať již jde o to vložit pásky do čtečky a čekat, až (a jestli vůbec) se data přehrají, popřípadě o snahu dát dohromady z vadných disků použitelná data. Zrcadlení disků umístěných na fyzicky odděleném vzdáleném místě přispívá ke spolehlivosti, nicméně vyžaduje nemalý úkol v podobě nalezení druhého vhodného místa i vytvoření dostatečně robustního datového připojení. [6]

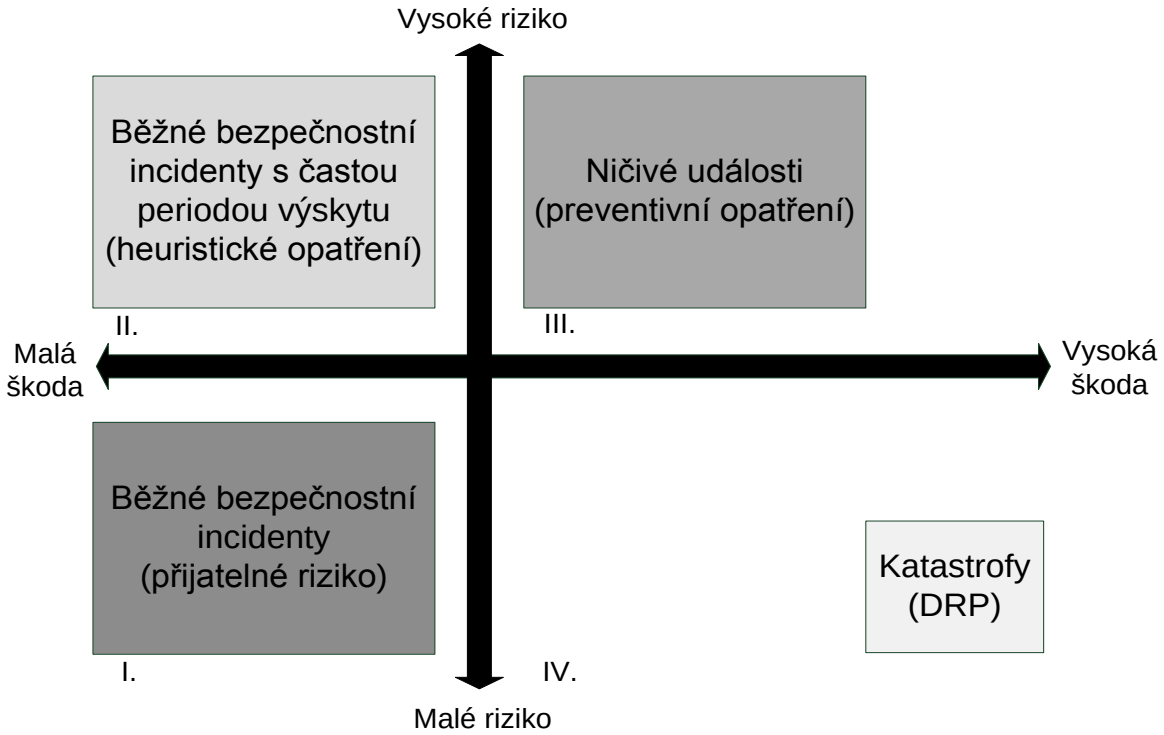
Náklady

Podnikání je stále více závislé na nepřetržitém přístupu k uloženým datům. Zároveň roste objem zpracovávaných i skladovaných dat a tedy i objem, který je nutný zálohovat. Zpráva The Cost of Lost Data (Cena ztracených dat), kterou zpracovala americká univerzita Pepperdine, říká, že jeden nenávratně ztracený megabajt dat stojí až 10 000 dolarů (200 000 korun). [6]

Magnetické pásky jsou samy o sobě poměrně levné, ale vzhledem k jejich chybovosti by bylo riskantní se spoléhat při zálohách jen na médium, u kterého dochází postupně ke snižování spolehlivosti a jež může být snadno zničeno při pádu na zem, nebo při ohnutí. Stejná logika platí i u pevných disků, tam se však připojují vysoké náklady. Zrcadlení disků totiž v zásadě vyžaduje nákup dvou stejných datových serverů. [6]

3.3 Skupiny nežádoucích událostí

Při provozu jakéhokoliv informačního systému je možné se setkat s několika druhy nežádoucích událostí. Rozdělení dle druhů a způsobu nápravných opatření zobrazuje obrázek č. 1. Z něj je jednoduchým způsobem možné vyčíst, které nežádoucí události (katastrofy) DRP pokrývá.



Obrázek č. 1: Rozdělení nežádoucích událostí dle velikosti rizika a očekávané škody [10]

- Běžné bezpečnostní incidenty – jedná se o události vyskytující se s nízkou, ale i vysokou periodickou četností. Jejich výskyt komplikuje užívání IS, avšak s minimálním dopadem na funkci a rozsah škod. Incidenty umístěné v prvním kvadrantu jsou bez zásadních výhrad akceptovatelné z pohledu rizika i škody. V případě incidentů v druhém kvadrantu je stále výška škody akceptovatelná, ale četnost výskytu je již na vysoké úrovni. Zde je již doporučeno aplikovat heuristické opatření, která by vedla k přesunu části incidentů do prvního kvadrantu.

- Ničivé události – jejich výskyt a tím pádem riziko je poměrně vysoké. Dopad je také vysoký, ale menší, než u katastrof. Pro jejich eliminaci je nutné zavést některé z preventivních opatření.
- Katastrofy – mají velice nízké a zároveň nahodilé riziko výskytu, avšak s maximálním dopadem na rozsah škod. Nedá se před nimi rozumným způsobem bránit, ale je možné se na ně připravit. V tomto bodu je zakořeněna podstata DRP.

3.4 Katastrofy

Odbornou literaturou jsou katastrofy členěny do mnoha skupin a podskupin, avšak v obecné rovině je možné je rozdělit do dvou základních oblastí a to na katastrofy přírodní a antropogenní.

Přírodní katastrofy [8]:

- Meteorologické – povětrnostní anomálie, bouře, krupobití.
- Geologické – sesuvy půdy, pohyby zemské kůry, zemětřesení, výbuch sopky.
- Hydrologické – anomálie spojené s koloběhem a distribucí vody, potopa, přílivové vlny.
- Klimatologické – extrémní klimatické změny probíhající v krátkém časovém období, výkyvy teplot, požáry.
- Biologické – plošně se šířící nemoci a infekce, zamoření živými organizmy.
- Kosmické – sluneční erupce, pád meteoritu.

Antropogenní katastrofy (způsobené člověkem) [8]:

- Průmyslové (technologické) – zamoření prostředí chemickými a biologickými látkami, jaderné záření, úniky ropy, požár.
- Dopravní – katastrofa některého z prostředků hromadné dopravy a přepravy (nejčastěji se jedná o leteckou, vlakovou, nebo lodní dopravou), zablokování klíčových dopravních spojů a cest.
- Sociální – válka, násilné jednání, teroristický útok, rabování.[1]

[1] U katastrof jsou uvedeny pouze orientační příklady, nejedná se o kompletní výčet všech možných variant.

V odstavci 3.1 bylo řečeno, že pokud má být nežádoucí událost klasifikována jako katastrofa, musí dojít ke ztrátám na životech v počtu minimálně 25 obětí, nebo k materiálním škodám v rozsahu přesahujícím 25 milionů dolarů. V případě tvorby DRP tyto podmínky úplně neplatí. Důvodem je fakt, že plán obnovy po pohromě si mohou vytvořit organizace libovolné velikosti. Například v případě vypuknutí požáru v malé organizaci a zničení, nebo poškození velké části infrastruktury a datových zdrojů musí dojít ke spuštění procesu obnovy stejným způsobem, jako ve společnosti obrovských rozměrů. Škody samozřejmě nejsou v těchto dvou případech stejné, ale dopad na fungování organizace ano.

Z tohoto faktu vyplývá, že pod pojmem katastrofa v rámci problematiky DRP a ve vztahu k ICT, je možné definovat jako nežádoucí událost, která způsobí plošnou a běžnými prostředky nevratnou nedostupnost klíčových systémů a datových zdrojů. V technické literatuře se také můžeme setkat s tím, že pojem katastrofa je suplován pojmy **pohroma**, či **havárie**, které lépe vyjadřují anglické slovo „disaster“.

3.5 Riziko

Velikost rizika je v případech jakéhokoliv plánování obnovy klíčovým faktorem. Podle velikosti rizika jsou vytvořeny různé modely obnovy, na něž jsou alokovány riziku adekvátně úměrné finanční prostředky.

U DRP tento postup platí také, avšak konkrétně v případě obnovy po katastrofě právě pojem katastrofa definuje, že je nutné počítat s aktivací hrozeb v maximalistické podobě.

3.6 Infrastruktura

Oblast infrastruktury potřebné pro provoz ICT se v posledních desetiletích zásadním způsobem změnila. Koncem minulého století si menší až středně velké organizace (SMB) vystačily převážně s počítačovou sítí jednoduché architektury, pobočkovou ústřednou a serverem, který zastával většinu rolí potřebných pro provoz infrastruktury. Vybudování rozsáhlých systémů, komunikujících napříč geograficky oddělenými destinacemi, bylo reálné pouze pro velké nadnárodní společnosti. Výrazné změny bylo možné pozorovat po masivním rozšíření internetu. S tím byla spojena i dostupnost vysokokapacitních datových spojů. Taktéž na poli ICT vybavení došlo k zásadním změnám. HW již netvoří v rámci infrastruktury klíčové náklady a většina nákladů se tak přesouvá do provozu a služeb. Výkon HW již převážně není limitujícím faktorem. Čím dál více se využívá

virtualizace, která se uplatňuje v prostředí serverů, desktopů, síťových prvků, datových úložišť a dokonce i samotné infrastruktury. ICT systémy již nejsou dominantou gigantických korporací, ale provozovat IS dostupný stovkám, nebo i tisícům uživatelů, již mohou i menší úřady či instituce.

Se zvýšením dostupnosti (z pohledu pořízení) ICT prostředků zároveň vzrostly požadavky na infrastrukturu a její dostupnost (z pohledu přístupu). Tento požadavek je v praxi řešen zmíněnou virtualizací nad fyzickou infrastrukturou. Aby byl možný výpadek systémů minimalizován, většina fyzických prvků je nasazována v redundantním režimu. **Redundance** pak zajišťuje nepřetržitý provoz i v případě kolapsu některého fyzického zařízení.

3.7 Zálohování a obnova

Ač spolu zálohování a obnova velice úzce souvisí, je možné označit proces obnovy za nejdůležitější krok v rámci celého DRP. Všechny činnosti před obnovou se dají popsat jako přípravné a jsou vykonávány za jediným účelem a tím je zajištění postupu, osob, dat a prostředků potřebných pro obnovu. V případě, že by jakýkoliv ze zmíněných prvků nebyl v případě potřeby dostupný, stává se obnova nerealizovatelnou a tím pádem není možné zajistit chod subjektu, na který bylo DRP aplikováno.

Při nastavování a parametrizaci zálohovacího systému musí být brán zřetel na několik stěžejních faktorů.

- Kapacita zálohovaných dat.
- Rychlost a způsob zálohování.
- Typy/druhy datových úložišť a médií.
- Požadovaná doba dostupnosti.
- Cena záloh a archivace (z pohledu přímých nákladů).

Způsoby zálohování

- Off-line – probíhá při „odstavených“ zálohovaných systémech od produkce a cílové médium je některý z externích datových nosičů (magnetická páska, optický disk, externí pevný disk, flash paměť apod.)

- On-line – probíhá za běhu produkčního systému. Při tomto druhu zálohování se ke konkrétnímu časovému okamžiku vytvoří otisk systému, anglicky **snapshot** a ten je pak následně uložen. Pro zálohování jsou převážně využívána vysokokapacitní datová úložiště jako např. disková pole, interní pevné disky nebo datová úložiště dostupná přes vzdálený přístup, v současné době nejčastěji označovaná jako řešení typu **Cloud.**

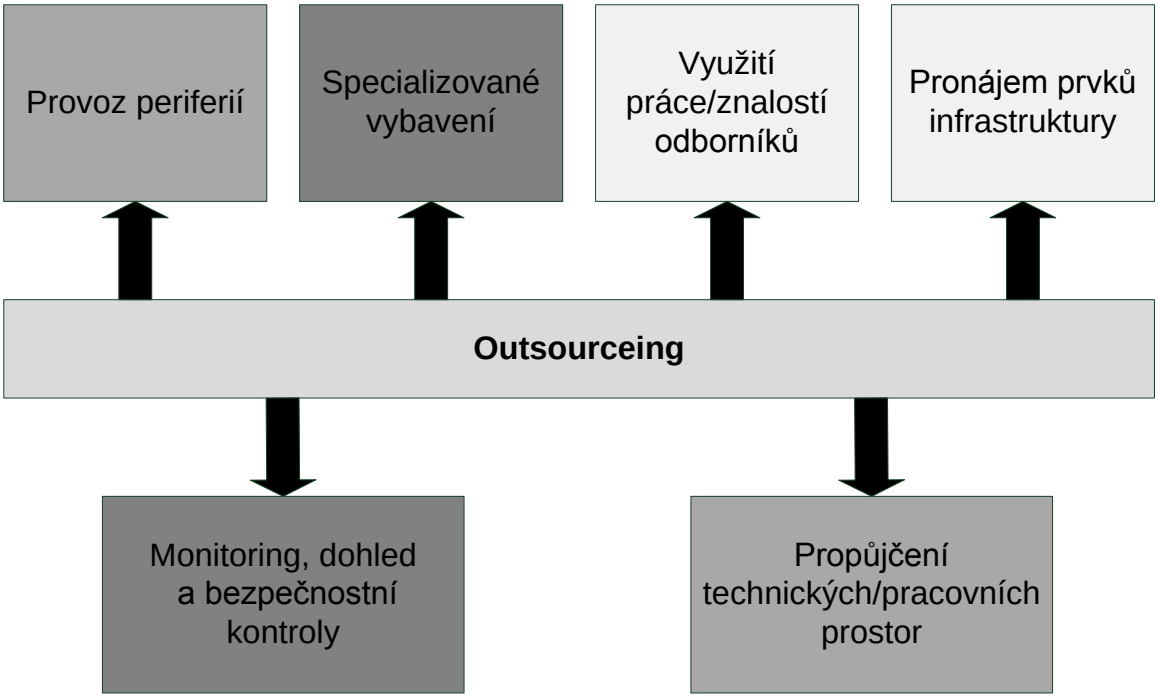
Z popisu obou způsobů je možné jednoduše vyčíst k čemu je která z variant vhodnější. Off-line zálohování je vhodnou variantou pro uložení médií, mimo infrastrukturu a prostory provozovatele, přičemž média pro tento způsob zálohování jsou většinou nezávislá na zdroji energie. Z tohoto důvodu je možné jejich uskladnění realizovat např. v bezpečnostních schránkách bankovních institucí. Off-line zálohy mají z principu věci tři negativa proti on-line zálohám a těmi jsou kapacita médií, rychlost čtení/zápisu a neaktuálnost uložených dat. Neaktuálnost se dá považovat za největší negativum, jelikož v případě katastrofy většinou omezují zajištění běžného provozu činnosti spojené se zajištěním náhradních prostor a nezbytného vybavení.

V případě on-line zálohování se problémy s neaktuálností a kapacitou většinou stírají. Otázkou je pak pouze rychlost. Pokud probíhají zálohy v prostředí přímo umístěném v místě provozování systémů, probíhá zálohování/obnova maximální rychlostí, kterou limitují pouze technologické vlastnosti systému. V okamžiku zálohování do prostředí dostupných přes vzdálený přístup je rychlost zálohování/obnovy omezena rychlostí datové konektivity mezi produkčním a zálohovacím prostředím. Aby bylo možné zásadním způsobem snížit riziko omezení nebo zastavení činnosti organizace, je možné společně se zálohovacím systémem umístit do oddělené lokality také sekundární produkční prostředí. Toto prostředí je on-line aktualizováno buď na bázi **clusteru**, nebo **replikace.** Pokud to technologické a finanční prostředky instituci dovolí, je vhodnější použít metodu clusterového propojení systémů. Jejím prostřednictvím je pak možné zajistit nepřetržitý provoz bez ztráty dat.

Pro zajištění zálohování/obnovy je možné využít buď nástroje integrované do OS, což většinou nepokrývá požadavky provozovatele na komplexnost, jelikož klade zvýšené nároky na obsluhu a omezuje možnost použít některé typy zálohovacích médií, nebo je možné využít nástroje třetích stran. Mezi nejznámější společnosti specializujících se na tuto problematiku patří Acronis, Veeam Software, Symantec, nebo IBM.

3.8 Outsourcing

Je možné charakterizovat jako službu propůjčení technických nebo lidských zdrojů za předem dohodnuté jednotkové nebo paušální periodické poplatky. Primárně slouží ke snížení nákladů a zároveň snížení míry rizika, které vyplývá z pořízení prostředků, pro které nemusí být za nějakou dobu využití nebo rozsah využití nekoresponduje s předem plánovaným. Při využití outsourcingu dostává společnost přidanou hodnotu v možnosti flexibilního řízení nákladů a cashflow a zároveň tak může získat služby odborníků nebo nákladné vybavení, které by bylo těžko dosažitelné. Další klíčovou výhodou outsourcingu v otázce DRP je přenesení rizika a z toho vyplývající zodpovědnosti na externí subjekt. Další výhodou je pak snížení administrativní náročnosti na provoz.



Obrázek č. 2: Nejčastější využití outsourcingu v prostředí ICT [zdroj: autor].

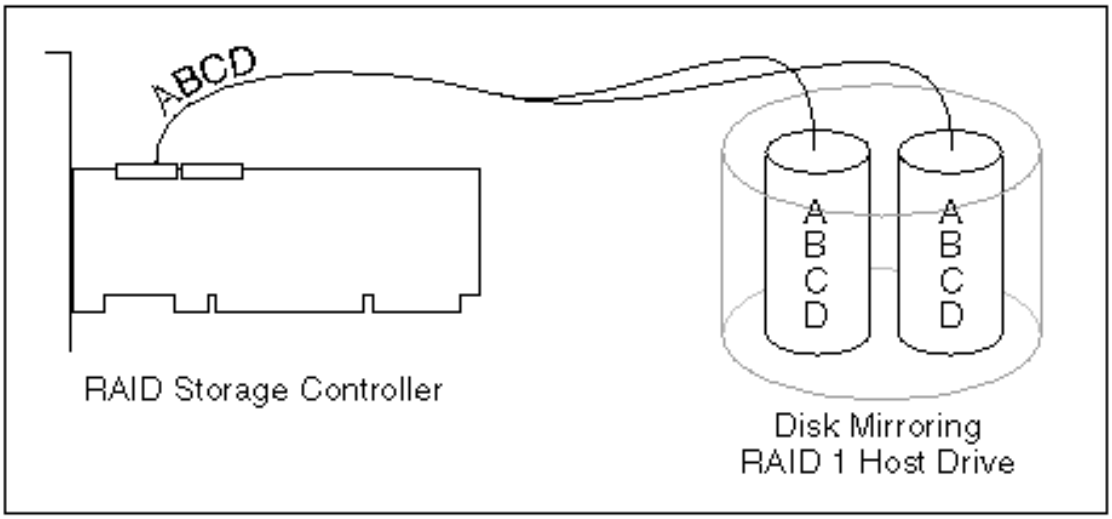
Nevýhodou je dostupnost, protože o zdroje provozovatele služby se dělí několik klientů. Zde outsourcing nemůže konkurovat provozu vlastních zdrojů. Tato nevýhoda je obzvláště v ICT kompenzována snížením nákladů spojených s dostupností. V případě využití outsourcingu není nutné držet v pohotovostním stavu prostředky potřebné na zajištění provozu systémů s vysokou dostupností (HA). To se převážně týká skladu náhradních dílů a záložního vybavení jako jsou prvky páteřní infrastruktury, součásti produkčních serverů, ústředen a systémů zajišťujících internetovou konektivitu, tiskové zařízení apod. Typickým příkladem využití outsourcingu je řešení v podobě cloudových služeb.

3.9 Redundance

Odborný slovník IT terminologie definuje redundanci jako: nadbytečnost, přebytečnost, označení situace, kdy je použito více prvků, než je nutné [17]. V prostředí ICT zajišťuje redundance pokrytí funkce jednoho zařízení, nebo systému prostřednictvím minimálně dvou nezávislých zdrojů. Redundance je pak nejčastěji využita pro případ zajištění náhradní dodávky el. energie a havárie HW, ale i SW. Do návrhu DPR pak velkou měrou zasahují oblasti týkající se zajištění provozních prostor a lidských zdrojů.

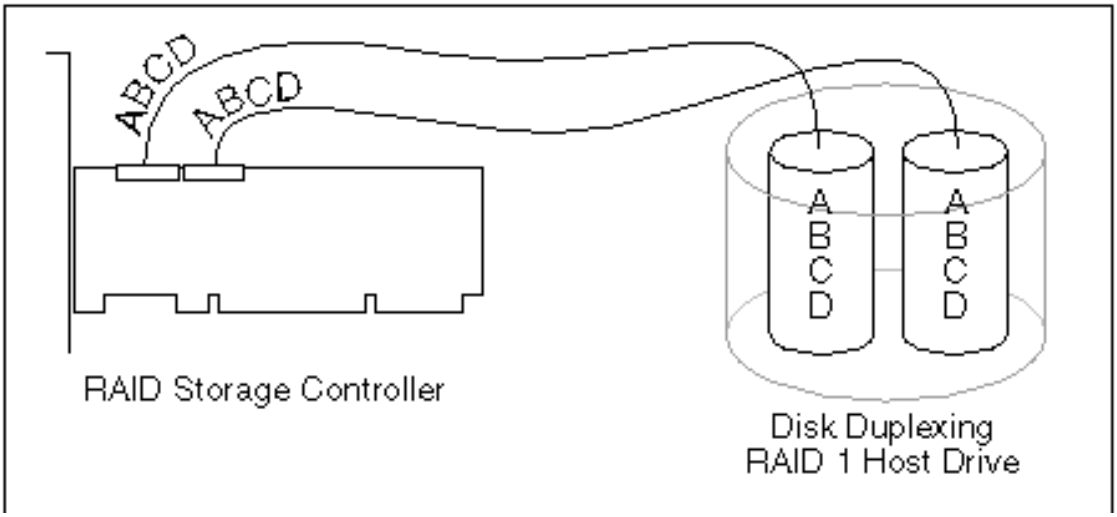
3.9.1 Technologie zajišťující redundanci ICT

- Disk mirroring – spojení dvou pevných disků v režimu RAID 1. Technologie zajišťuje zápis identický dat na oba pevné disky (čtení dvojnásobnou rychlostí). V případě výpadku jednoho z disků, je automaticky dostupný obsah disku druhého. Bohužel technologie nezaručuje dostupnost dat v případě SW selhání, výpadku řadiče, popř. výpadku obou disků. Částečné řešení zajišťují použití vyšších verze technologie RAID.



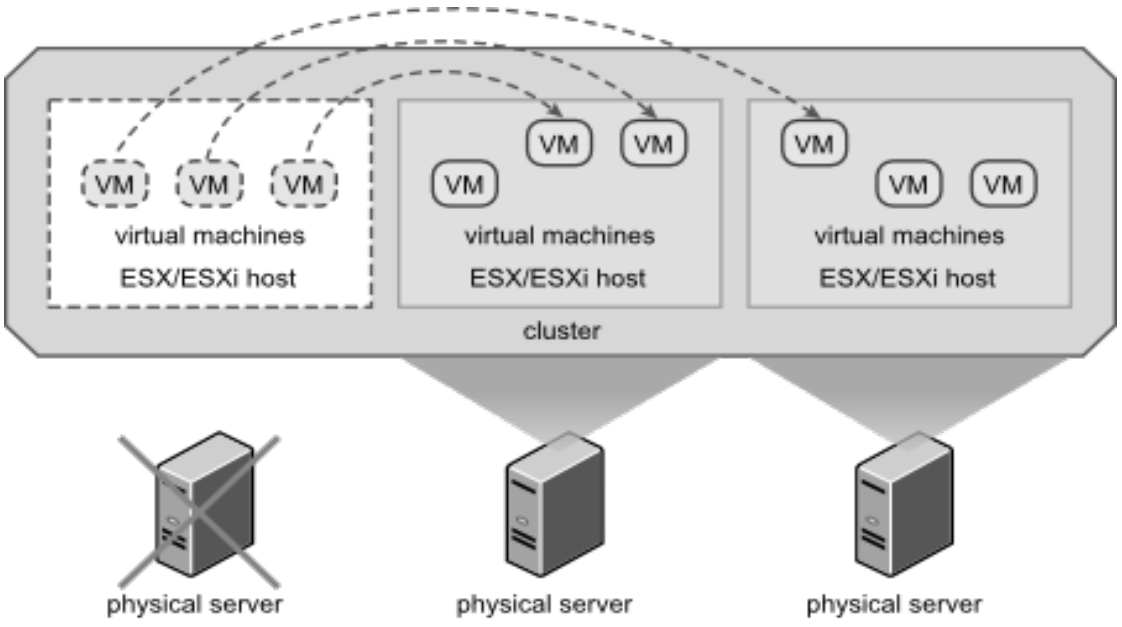
Obrázek č. 3: Ukázka technologie disk mirroring [11].

- Disk duplexing – pro přístup k diskovému úložiště jsou použity dva diskové řadiče. Výpadek jednoho z řadičů neohrozí dostupnost diskového úložiště.



Obrázek č. 4: Ukázka technologie disk duplexing [11].

- Cluster s vysokou dostupností (High Availability Cluster) – technologie zajišťující spojení minimálně dvou fyzických serverů uvnitř jednoho prostředí (např. VMware vSphere, nebo Microsoft Hyper-V). V případě výpadku jednoho ze serverů, zajišťuje prostředí automatické spuštění systémů provozovaných na tomto serveru na ostatních dostupných serverech. Nezbytnou podmínkou je lokálně umístěná kopie všech provozovaných systémů na každém z fyzických serverů, nebo dostupnost sdíleného datového úložiště s těmito systémy.



Obrázek č. 5: Ukázka HA clusteru v prostředí VMware vSphere [21].

3.9.2 Provozní prostory

Zajištění redundance provozních prostorů spočívá v zajištění prostor v alternativní lokalitě, dokud primární lokalita není opět dostupná [20].

- Studená místa - záložní vybavení dostatečně velké, kde mohou pokračovat podnikové procesy. Jedná se o velké sklady, prázdné administrativní budovy. Nemají výpočetní vybavení (HW a SW) a širokopásmové komunikační linky. Zpravidla několik málo telefonních linek.

  Klady: relativně nízká cena.

  Zápory: časová prodleva (zpravidla týdny) než proběhne znovunastolení podnik. procesů. Servery a pracovní stanice musí být přineseny a nakonfigurovány, data musí být obnovena ze záloh, komunikační linky musí být aktivovány. [20]

- Horká místa - opak „studeného místa“. Vybavení připravené k okamžitému provozu. Doporučeno jiné geografické umístění, než je umístění původního provozu. Data z primárních serverů musí být průběžně umísťována na servery v „horkém místě“.

  Klady: výhodou je možnost okamžitého pokračování podnikových procesů.

  Zápory: vysoké náklady. [20]

- Teplá místa - kompromis mezi „horkým místem“ a „studeným místem“. Obsahuje pracovní stanice, servery, komunikační zařízení, ale ne aktuální data. Vybavení je nakonfigurováno a připraveno k použití. Je třeba zajistit transport zálohových médií a umístění aktuálních dat na server. Aktivace tohoto místa zpravidla do 12 hodin po události.

  Klady: kompromisní řešení obsahuje klady studených i teplých míst.

  Zápory: minimální. [20]

- Mobilní místa - alternativa k běžným přístupům. Realizováno prostřednictvím soběstačných přívěsů nebo jednotek, které se dají snadno přemístit. Zpravidla konfigurována jako „studená místa“. Konfigurace jako „horké místo“ je obtížná, často není předem známo, kde budou použita.

  Klady: geografická nezávislost a možnost outsourcingu.

  Zápory: vysoké nároky na uskladnění, závislost na dodavateli. [20]

- Vícenásobná místa - rozdělení vybavení mezi různé divize, oddělení, kanceláře. Redukce důsledku pohromy.

  Klady: čím více míst, tím menší riziko.

  Zápory: vyšší nároky na řízení a administraci v celé společnosti. [20]

3.9.3 Lidské zdroje

Pokud má být zajištěno plnohodnotné fungování DRP za jakékoliv situace, je nezbytné vyřešit také redundanci lidských zdrojů (bohužel v případě plánování obnovy po katastrofě je nutné počítat i se ztrátami na životech). Ta spočívá ve vytvoření realizačních týmů, kde každá klíčová osoba musí mít vždy minimálně jednoho zástupce, na kterého je možné kompetence v případě propuknutí katastrofy delegovat. V případě osob na vrcholu kompetenčního žebříčku je žádoucí zajistit vždy minimálně dva zástupce.

4 PŘÍPADOVÁ STUDIE

Aby bylo možné lépe demonstrovat DRP v praxi, bylo přistoupeno k vytvoření případové studie. Ta byla zároveň vytyčena jako jeden z cílů BP.

Pro tento účel bylo zapotřebí vybrat dosti všeobecný reprezentativní vzorek společnosti. Z tohoto důvodu byla vybrána imaginární společnost LAW+ zabývající se poskytováním právních služeb, která však v mnoha ohledech supluje roli libovolného úřadu nebo instituce malé až střední velikosti administrativního charakteru, která pořizuje, zpracovává a uchovává dokumenty a informace v nich obsažené, komunikuje s okolním světem a provozuje běžné informační systémy spojené se zajištěním chodu.

4.1 Popis činnosti společnosti LAW+

Jak již bylo zmíněno, pracovní náplní společnosti je poskytování právních služeb. To se ve stručnosti převážně skládá z péče o současné klienty a vyhledání nových klientů. Společnost poskytuje komplexní služby počínaje právním poradenstvím pro jednotlivce, až po zastupování mezinárodních korporací.

Charakter činnosti lze názorně popsat na obecném klientském případu.

1. Klientem je LAW+ oslovena s nabídkou na právní zastupování v nové kauze.
2. LAW+ si s klientem specifikuje rozsah spolupráce a vyčleňuje realizační tým, který je zodpovědný za poskytnutí požadovaných služeb.
3. Na souborovém serveru jsou vytvořeny klientské složky pro ukládání dokumentace a zároveň je klient zaveden do billingového systému (v případě stávajícího klienta jsou použity již vytvořené struktury)
4. Tým začíná s klientem komunikovat a shromažďuje potřebné relevantní poklady a dokumentaci pro realizaci projektu. Ty ukládá do vytvořených složek na datovém úložišti. Veškeré práce a s tím spojené náklady jako administrativní poplatky, kolky, překlady apod., jsou členy realizačního týmu zaznamenávány do billingového systému.
5. Po realizaci projektu dochází k procesu akceptace ze strany klienta. Proces akceptace obsahuje odsouhlasení rozsahu prací a nákladů.

6. Na akceptaci přímo navazuje finanční plnění. Klientovi je na základě podkladů z billingu vystaven a odeslán daňový doklad z účetního systému.
7. V rámci periodických denních kontrol bankovních účtů dochází k párování příchozích plateb se záznamy vystavených faktur v účetním systému LAW+. Jakmile je platba spárována s fakturou, je informace o zaplacení propisována zpět do billingového systému. Pro manažera projektu (vedoucího advokáta) je tento krok indikátorem úspěšné realizace projektu.
8. Projekt je označen za realizovaný a veškerá dokumentace archivována.

Aby bylo možné takovéto služby poskytovat, je nezbytné využívání prostředků ICT, na které jsou kladeny vysoké nároky z pohledu dostupnosti, spolehlivosti a bezpečnosti, což jsou klíčové faktory podněcující zavedení DRP.

4.2 Charakteristika a geografické rozdělení

Společnost situuje svou působnost do dvou geograficky rozdělených destinací. V Brně je umístěno sídlo společnosti, kde sídlí vedení, velká část právních týmů a skupiny primárně zabezpečující chod celé společnosti jako je marketingové, finanční, provozní a IT oddělení. Pardubická pobočka disponuje menšími právními týmy, call centrem a několika členy podpůrného personálu.

Klíčové datové zdroje a systémy jsou směřovány do Brna. Podpůrné komunikační systémy pro zajištění datové konektivity a IP telefonie jsou pak v režii každé destinace.

Tabulka č. 2: Popisná specifikace společnosti LAW+ [zdroj: autor].

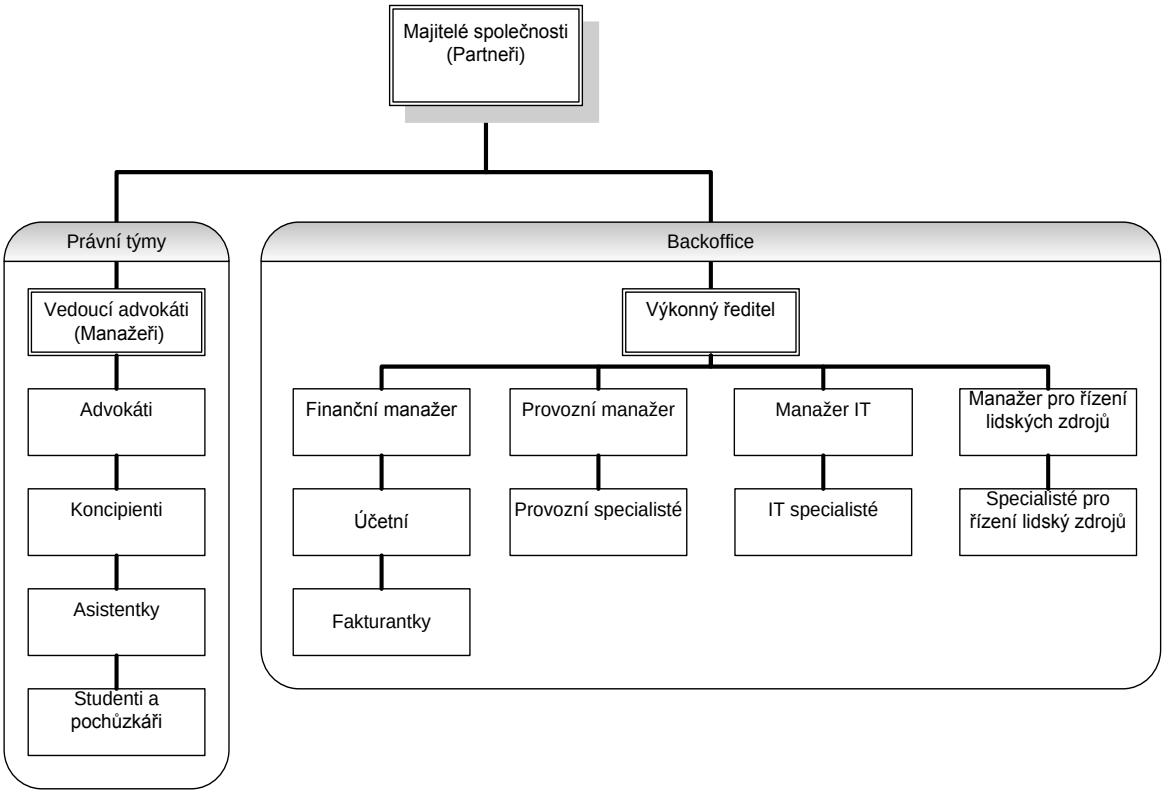
Popis	Sídlo společnosti	Pobočka	Celkem
Geografické rozdělení	Centrum Brna.	Okrajová část Pardubic.	
Počet pracovních stanic	80 stacionárních stanic, 40 notebooků.	10 stacionárních stanic, 20 notebooků.	150
Počet fyzických serverů	2	0	6
Počet uživatelů	120	30	180
Serverovna	ANO	NE	
Budova			
Typ	Samostatně stojící administrativní budova kvádrového tvaru.	Administrativní budova v běžné zástavbě.	
Počet nadzemních pater	3	2	
Počet podzemních pater	1	0	
Půdní prostory	NE	ANO	

Stáří	Počátek 21. století.	Konec první poloviny 20. století.	
Elektronický požární systém (EPS)	ANO	ANO	
Elektronický zabezpečovací systém (EZS)	ANO	NE	
Automatický hasicí systém (AHS)	NE	NE	
Záplavová čidla	NE	ANO	
Napojení na pult centrální ochrany (PCO)	NE	NE	

4.3 Organizační struktura

Společnost je možné v rámci organizační struktury rozdělit do následujících skupin:

1. Majitelé a top management – majitelé, vedoucí advokáti a výkonný ředitel.
2. Jednotlivé právní týmy – řídí advokáti a na manažerské úrovni zastřešují vedoucí advokáti.
3. Backoffice – zajišťuje provoz kanceláře prostřednictvím jednotlivých provozních oddělení, přičemž všechna oddělení spadají pod pravomoc výkonného ředitele.



Obrázek č. 6: Organizační struktura společnosti LAW+ [zdroj: autor].

4.4 Prostředí

Díky využití virtualizace se prostředí ICT systémů, které společnost LAW+ využívá, dá rozdělit do dvou skupin a to na síťovou a serverovou infrastrukturu. Infrastruktury jsou pak dále dělené na fyzickou a virtuální vrstvu. Výhodou tohoto řešení je možnost oddělitelnosti a přenositelnosti vrstev.

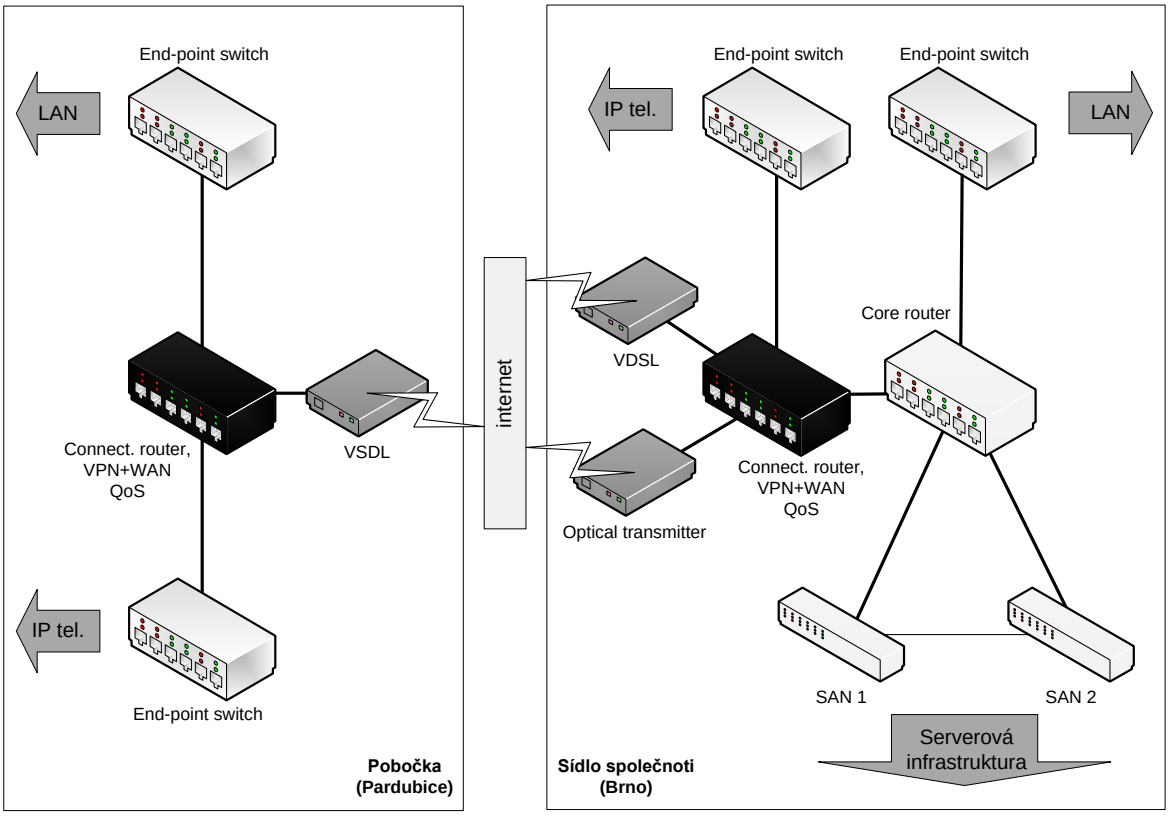
Síťová infrastruktura

Geografické rozdělení společnosti je také dělícím kritériem pro infrastrukturu. Aby bylo možné zajistit dostupnost systémů a datových zdrojů, které jsou převážně situovány v Brně, zajišťují internetovou konektivitu v této lokalitě dva technologicky nezávislé datové spoje. Internetová konektivita je jak v sídle společnosti, tak na pardubické pobočce, zakončena na routeru, který zajišťuje separaci konektivity na jednotlivé WAN porty (pro LAN a IP telefonii) a navíc vytváří šifrované VPN spojení mezi destinacemi. Priorizace síťového provozu je v tomto prvku zabezpečena aplikací QoS, přičemž pakety pro IP telefonii jsou upřednostňovány před provozem prostřednictvím běžné LAN.

Síťový provoz uvnitř firmy zastřešuje páteřní router, který se stará o propojení SAN switchů pro serverovou infrastrukturu a switchů pro koncové uživatele a periferie.

Tabulka č. 3: Technická specifikace síťové infrastruktury [zdroj: autor].

Název	Výrobce	Model	Specifikace
Connect. router	Cisco	1812	8x100Mbit ports,2xFE WAN
Core router	HP	ProCurve 2824	20x1Gbit ports, 4xmini-GBIC
SAN1	IBM	SAN24B-4	24x8Gbit ports
SAN2	IBM	SAN24B-4	24x8Gbit ports
End point switch LAN	HP	ProCurve 2510	48x1Gbit ports, 2x mini-GBIC
End point switch IP tel.	HP	ProCurve 2610	48x100Mbit ports, 2xmini-GBIC



Obrázek č. 7: Schéma síťové infrastruktury [zdroj: autor].

Serverová infrastruktura

Jak již bylo zmíněno, společnost LAW+ vsadila v případě serverové infrastruktury na virtualizaci prostřednictvím vSphere 5 od společnosti VMware. Při zavádění bylo také zvažováno nasazení konkurenčního řešení na bázi Hyper-V Serveru od Microsoftu, ale v daný okamžik bylo z důvodu technologické vyzrálosti zvoleno vSphere.[2]

Serverovou infrastrukturu kompletně pokrývají výrobky od IBM. Provoz je zajištěn dvěma produkčními ESX servery a jedním backup serverem, který plní roli systému pro zálohování a dále roli nástroje pro administraci infrastruktury. Komunikaci mezi servery a ostatními periferiemi zajišťují dva redundantní optické SAN switche.

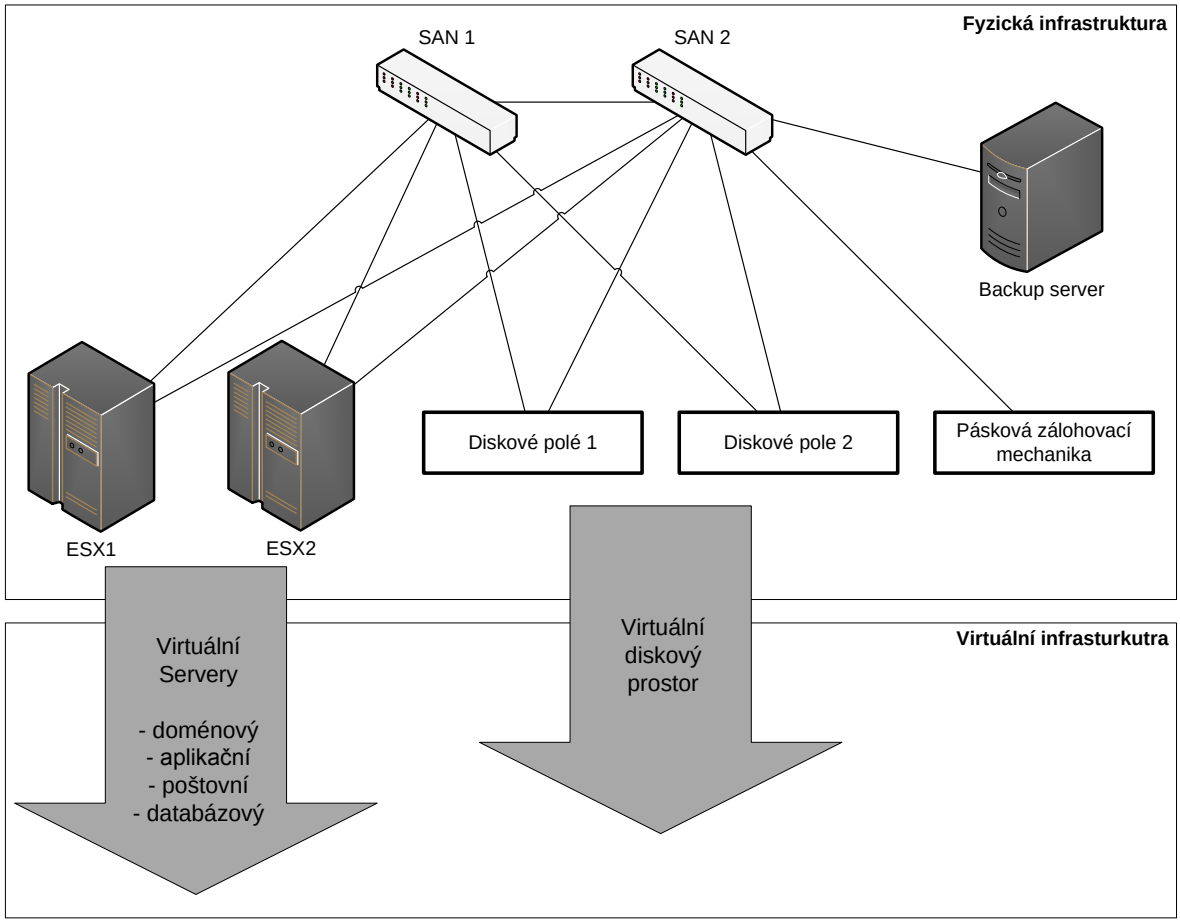
Prostor pro provoz virtuálních serverů a ukládání dat poskytují dvě fyzická disková pole. Aby bylo možné docílit finančně optimální alokace nákladů, je každé z polí osazeno jiným typem pevných disků. Pro produkční servery jsou použity disky typu SAS a jako datová úložiště pro zálohování slouží disky SATA. Ochranu proti výpadku vždy

[2] V současné době se nacházejí řešení na bázi vSphere i Hyper-V na velice srovnatelné úrovni a případné nové rozhodování by již nebylo tak jednoznačné.

maximálně jednoho disku v rámci pole zajišťuje provoz v režimu RAID 5. O zálohování na externí média se stará pásková mechanika.

Tabulka č. 4: Technická specifikace serverové infrastruktury [zdroj: autor].

Název	Model	CPU	RAM
ESX 1	X3650	2x Xenon/4 jádra 3Ghz	26GB
ESX 2	X3650	2x Xenon/4 jádra 3Ghz	26GB
Backup Server	X3400	1x Xenon/4 jádra 2Ghz	8GB
	Model	Typ disků	Kapacita pole
Diskové pole 1	DS3400	SAS	2,7 GB
Diskové pole 2	DS3400	SATA	4,5 GB
	Model	Typ	Kapacita pásky
Pásková mechanika	TS3100	LTO-4	800GB



Obrázek č. 8: Schéma serverové infrastruktury [zdroj: autor].

Internetová konektivita

K zajištění internetové konektivity pro sídlo společnosti jsou využívány dva druhy připojení. Primární je realizováno prostřednictvím optického spoje a jako záložní připojení slouží spoj metalický. Konektivitu pardubické pobočky zajišťuje taktéž metalický spoj, přičemž v obou případech je použita technologie VDSL.

O redundanci konektivit se na straně centrály stará router, v němž jsou oba spoje zakončeny. V případě výpadku primární linky je tak do 120 vteřin zajištěn automatický „přepad“ na sekundární linku. Následně je routerem testován v 10 min. periodách stav primární linky. Pokud je zjištěna její dostupnost, je konektivita opět převedena na primární spoj.

Tabulka č. 5: Technická specifikace internetové konektivity [zdroj: autor].

Název	Technologie	Specifikace
Optický spoj	Fibre Channel	30Mbit (download)/30Mbit (upload)
Metalický spoj	VDSL	20Mbit (download)/2Mbit (upload)

4.5 Koncové zařízení a periférie

Klientské stanice

Oblast koncových stanic je pokryta produkty společnosti Lenovo v podobě notebooků řady Thinkpad a desktopů řady Thinkcentre. Obě řady patří do sféry produktů primárně určených pro korporátní využití. Smluvně je ošetřena on-site záruka v režimu Next Business Day (NBD), jež zajišťuje potřebnou opravu stanic následující pracovní den v prostorách kanceláře. Jako jednotný operační systém je využíván Windows 7 Professional.

Telefony

Kancelář používá pro potřeby interní a externí hlasové komunikace mobilní a stacionární telefonní přístroje.

- Mobilní telefony – celé spektrum smartphonů, bez výhradního výrobce, založené na platformách Windows Mobile 7 a 8, Symbian a iOS. Telefony jsou využívány jednak pro hlasovou a dále pro emailovou komunikaci a synchronizaci kalendářů, upomínek a kontaktů s poštovním serverem.
- Stacionární telefony – pro hlasovou komunikaci, kde není nutný požadavek na mobilitu, využívá kancelář IP telefonii. Ta je zajišťována formou outsourcingu

telefonní ústředny, kterou poskytuje a ve vlastních prostorách provozuje smluvní operátor. Telefonní přístroje jsou zastoupeny rozsáhlým spektrem výrobků značky Polycom. Pro realizaci hlasových hovorů prostřednictvím IP telefonie se kancelář rozhodla z následujících důvodů:

- Eliminace nákladů za telefonní poplatky při volání mezi sídlem společnosti a pobočkou a samozřejmě dalšími vybranými operátory.
- Flexibility při rozšiřování počtu telefonních linek.
- Jednoduché údržby při konfiguraci systému a telefonních přístrojů.
- Možnosti prezentace a dostupnosti všech telefonních čísel pod jedním systémem provoleb s možností přesměrování a přepojování napříč lokalitami.

Jelikož je v případě poruchy, ztrátě nebo odcizení telefonní přístroj poměrně jednoduše nahraditelný, nepřistoupila LAW+ k uzavření žádné rozšířené záruky, která by pokrývala tato zařízení.

Tisková zařízení

Tato oblast je zastoupena multifunkčními tiskovými zařízeními od společnosti Canon z řady imageRunner Advance. Každé zařízení je vybaveno duplexní skenovací jednotkou, duplexní tiskovou jednotkou a modulem pro síťové připojení. Pro minimalizaci vstupních nákladů a provozních činností spojených s provozem zařízení, byl opět využit outsourcing. Dodavatelská firma garantuje dostupnost spotřebních materiálů, běžných náhradních dílů a v případě nutnosti zápůjčku celého tiskového zařízení do 24 hod. od oznámení požadavku.

4.6 Systémy a jejich rozdělení dle funkce

Pro provoz serverů zvolila LAW+ 64bitové operační systémy na platformě Microsoft Windows Server 2008. Kvůli jednodušší integraci do jednotného homogenního prostředí jsou na stěžejních serverech použity také produkty společnosti Microsoft.

Tabulka č. 6: Technická specifikace serverů [zdroj: autor].

Server	CPU	RAM	HDD 1	HDD 2
Doménový/souborový server	1xvirtual.CPU/4 jádra	4GB	80GB	500GB
Aplikační server	1xvirtual.CPU/4 jádra	4GB	80GB	100GB
Poštovní server	1xvirtual.CPU/4 jádra	8GB	80GB	300GB
Databázový server	1xvirtual.CPU/4 jádra	8GB	80GB	200GB
Backup server	2x Xenon/4 jádra 2Ghz	8GB	300GB	

Doménový server

Je nejdůležitějším serverem v celé infrastruktuře, jelikož zastává funkci doménového řadiče. Mezi jeho klíčové funkce je zařazena správa uživatelských účtů a účtů zařízení přistupujících k doménovým prostředkům, řízení a vynucování doménových politik, zajištění provozu DHCP a DNS serveru. V prostředí společnosti LAW+ plní také roli souborového serveru. Na něm pak končí veškerá zmiňovaná klientská dokumentace.

Aplikační server

Role aplikačního serveru je primárně směřována na zajištění třech základních funkcí.

- Provoz aplikací - billingový systém, fakturační systém, systémy pro přístup k sbírkám zákonu atd.
- Webový server - přístup k aplikacím prostřednictvím webového rozhraní.
- Tiskový server - zpřístupnění tiskových zařízení pro koncové uživatele.

Poštovní server

O správu emailové komunikace, kalendářů, úkolů a kontaktů se stará Microsoft Exchange Server 2010, který veškerá data uchovává ve vlastních databázích. Jeho výhodou je zmíněná možnost integrace do doménového prostředí a správa uživatelských účtů napříč systémy.[3]

Databázový server

Pro uložení dat systémů „běžících“ na aplikačním serveru slouží Microsoft SQL Server. Společností LAW+ je databázový server také využíván pro tvorbu reportů a analýz, přičemž jako vstupní data jsou použity informace uložené v databázích serveru.

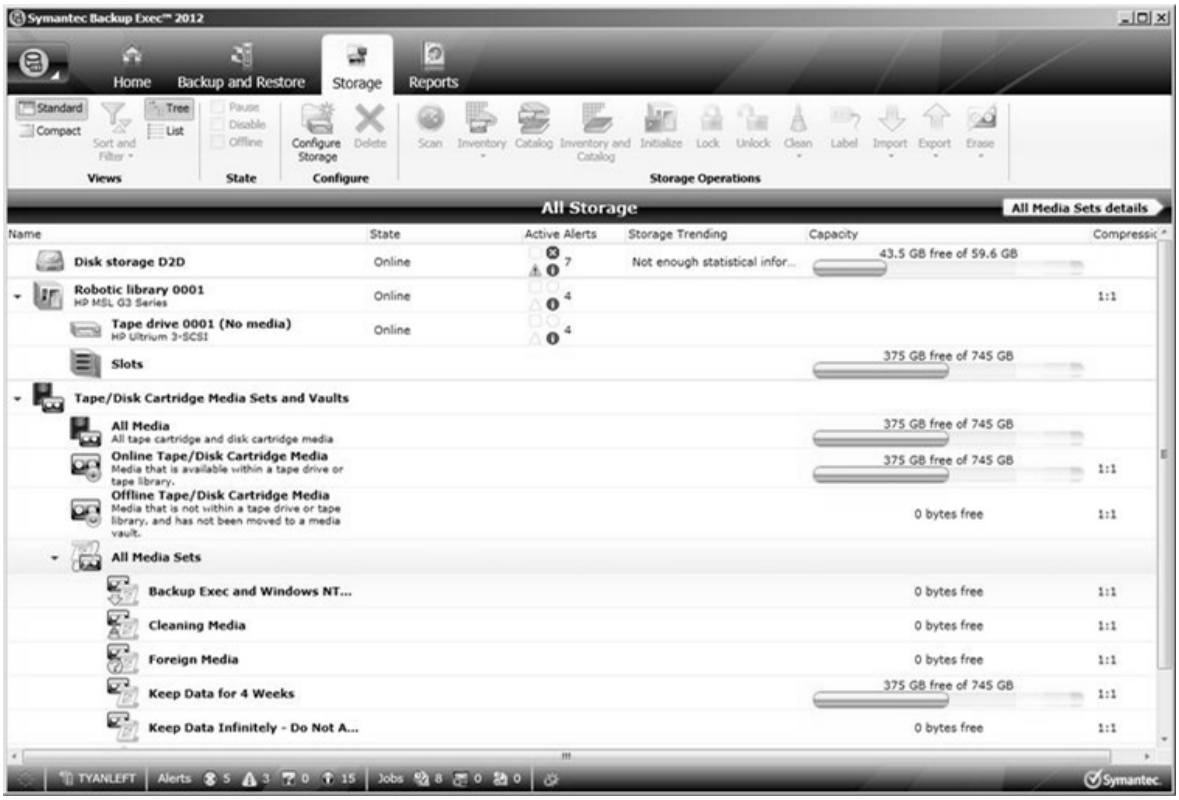
[3] Společnost využívá pro přístup k prostředkům poštovního serveru také vzdálený přístup přes Outlook Web Access (OWA), který je dostupný i z prostředí internetu.

Backup server

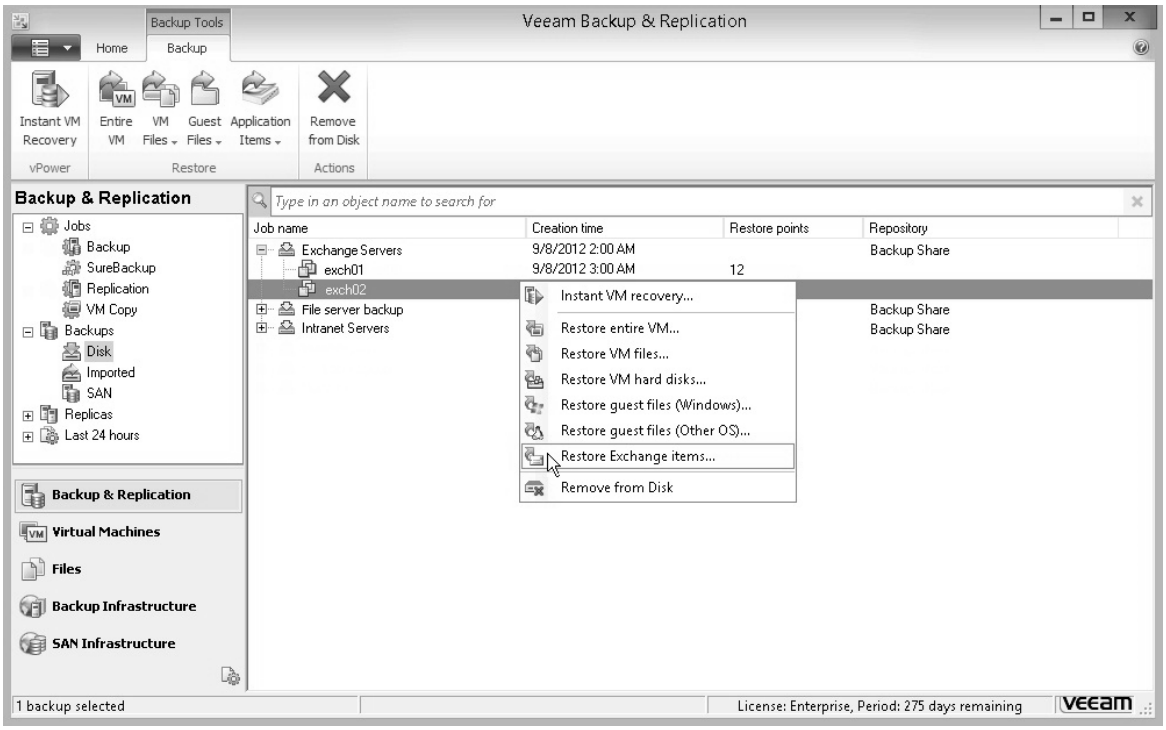
Jak specifikuje tabulka č. 4 tak backup server není součástí skupiny virtuálních serverů, ale je provozován jako samostatná fyzická jednotka. Důvody tohoto řešení jsou spjaté s jeho funkci managemetnu vSphere a dále s eliminací vytěžování ESX serverů v okamžiku zálohování.

Pro zálohování je použita metoda Disc To Tape (DTT), kdy probíhá nejprve záloha na diskové pole osazené SATA disky a interní disky backup serveru. Následně jsou tyto zálohy přeneseny na pásky pro externí uložení. Pro obsluhu páskové zálohovací mechaniky je využíván Symantec Backup Exec.

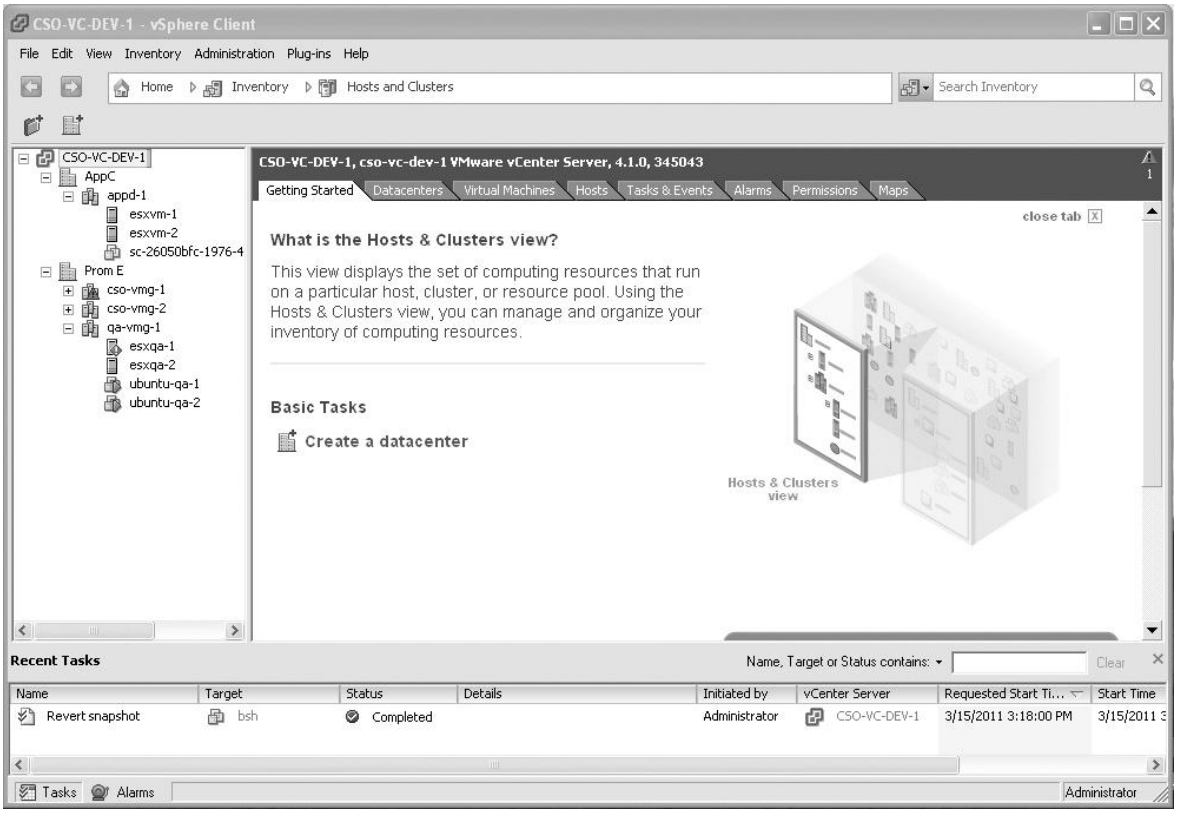
Ač patří zálohování k základním funkcím backup serveru, je jeho hlavním úkolem v prostředí LAW+, periodická tvorba replik produkčních serverů prostřednictvím Veeam Backup & Replication. Repliky je v případě potřeby možné využít jako druh zálohy, nebo v okamžiku havárie jako v čase posunutou bitovou kopii produkčního serveru. Díky použití VMwaru je zpřístupnění serverové repliky otázkou několika minut.



Obrázek č. 9: Ukázka prostředí Symantec Backup Exec 2012 [19]



Obrázek č. 10: Ukázka prostředí Veeam Backup & Replication [18]



Obrázek č. 11: Ukázka prostředí vSphere tenkého klienta [14]

Z důvodu snížení rizika je Backup server umístěn mimo serverovnu s produkčními ESX servery.

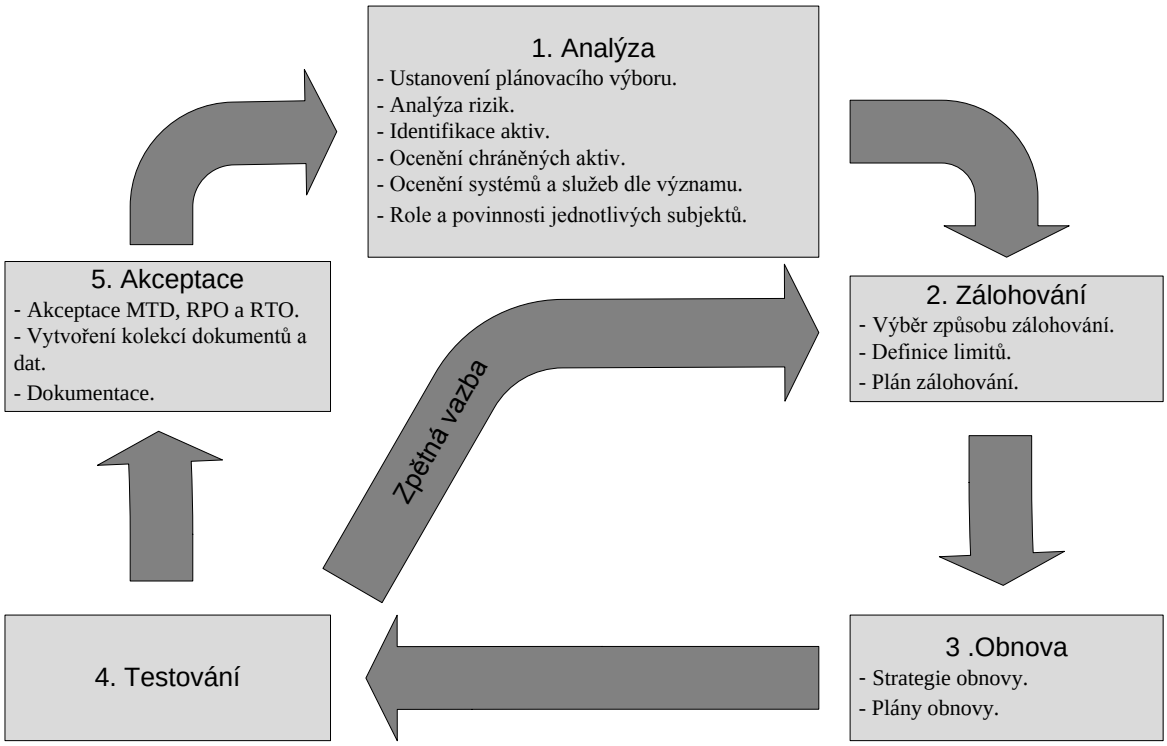
5 FORMULACE POSTUPU TVORBY DRP NA REÁLNÉM PŘÍKLADU

Technická literatura obsahuje mnoho postupů a pravidel jak k tvorbě DRP přistupovat. Dělícím prvkem je v tomto případě velikost organizace, na kterou mají být postupy aplikovány. U SMB je možné zajistit plánování obnovy po katastrofě menším pracovním týmem, přičemž jeho udržování v aktuálním stavu nezabere členům více jak několik hodin měsíčně. Opakem jsou samozřejmě nadnárodní organizace. Vše závisí na rozsáhlosti systémů a množstvím změn, které musí DRP pokrývat.

Podle Geoffrey H. Wolda, který prezentoval na webovém portálu Disaster Recovery Jurnal sérii tří odborných článků na téma Disaster Recovery Planning Process, je možné proces plánování obecně rozdělit do následujících deseti kroků [16]:

1. Začlenění DRP do zodpovědnosti Top Managementu.
2. Ustanovení plánovacího výboru.
3. Analýza rizik.
4. Stanovení priorit pro zpracování a provoz.
5. Definování strategie obnovy.
6. Vytvoření kolekce dat.
7. Zajištění dokumentu se sepsaným plánem.
8. Vytvoření testovacího kritéria a procedury.
9. Otestování plánu.
10. Odsouhlasení plánu.

Jelikož Wold popisuje kroky DRP, které pokrývají celou problematiku, bylo nutné některé body zredukovat a upravit tak, aby bylo možné postup zacílit na ICT. Výsledná podoba metodiky dále vychází z metody Plan Do Check Act (PDCA). Obsahuje pět okruhů tvořících periodicky se opakující životní cyklus DRP, přičemž jednotlivé okruhy jsou dále děleny na detailnější kroky.



Obrázek č. 12: Životní cyklus DRP ve vztahu k ICT [zdroj: autor].

5.1 Analýza

5.1.1 Ustanovení plánovacího výboru

Plánovací výbor by se měl v každém případě skládat minimálně ze dvou členů a to ze zástupce Top managementu a IT oddělení. Zástupce Top managementu zastává roli hlavního garanta plánu a je zodpovědný za specifikaci chráněných aktiv, akceptaci plánu a zajištění dodržování plánu. Zástupce IT oddělení je přímo zainteresován v návrhu řešení, monitoringu, testování a samozřejmě akceptaci.

V případě LAW+ je vhodné ustanovit plánovací výbor v rozsahu.

1. Hlavní garant – partner společnosti.
2. Provozní garant – výkonný ředitel.
3. Garant klientské operativy – vedoucí advokát.
4. Technický garant – IT manažer.

5.1.2 Analýza rizik

Jak již bylo zmíněno v odstavci 3.5, analýza rizik a samotné vyčíslení rizika je pro plánování obnovy velice důležité, avšak v případě plánování obnovy po katastrofě je

nutné počítat se scénáři charakteru zatopení objektů společnosti, požáru, zemětřesení, ale i pádu letadla apod. Ve všech těchto případech dochází buď ke kompletnímu, nebo minimálně k zásadnímu poškození budov, infrastruktury a systémů nezbytných pro provoz společnosti. S katastrofou je většinou spojeno i přerušení dodávky el. energie a přerušení komunikačních linek.

Analýza rizik tak přímo nesouvisí s plánováním obnovy po katastrofě, ale souvisí s procesem řízení rizik, jehož úkolem je identifikace rizika, vyhodnocení pravděpodobnosti výskytu a zajištění jeho snížení na tolerovatelnou míru.

Aby bylo možné sestavit plán obnovy, je vždy nutné vydefinovat krizové situace, které má DRP pokrývat. Definice se pak stává zásadním prvkem pro řízení očekávání, které je většinou z pohledu Top managementu neúměrné realitě. V případě LAW+ je možné rozdělit situace do následujících modelových skupin.

Model 1: Částečné poškození budovy a síťové, nebo serverové infrastruktury a menšího počtu klientských stanic a telefonních přístrojů (<10).

Obnova je podmíněna zachováním síťové infrastruktury uvnitř serverovny, backup serveru a alespoň jednoho ESX serveru.

Model 2: Odcizení, zničení (ohněm, vodou, elektrickým výbojem, násilným jednáním apod.) kompletního vybavení serverovny v sídle společnosti.

Obnova je podmíněna dostupností backup serveru.

Model 3: Rozsáhlé poškození budovy a síťové, nebo serverové infrastruktury a většího počtu klientských stanic a telefonních přístrojů.

5.1.3 Identifikace aktiv

Z pohledu ICT jsou nejdůležitějšími a zároveň nejcennějšími aktivy data/informace. Jejich vysoká hodnota spočívá v nenahraditelnosti.

Systémy, ve kterých jsou data uložena, jsou většinou snadno obnovitelné a ač se jedná také o aktivum, není nutné je v tomto kroku zmiňovat.

Identifikaci aktiv na případu LAW+ reprezentuje tabulka č. 7. Při její tvorbě bylo postupováno tak, že byla postupně procházena celá serverová infrastruktura a u každého serveru byla zkoumána přítomnost chráněných aktiv. Data na klientských stanicích a smartphonech nejsou zahrnuta do chráněných aktiv a uživatelé jsou na

základě interní směrnice povinni veškerou dokumentaci ukládat výhradně na souborovém serveru.

Tabulka č. 7: Rozmístění chráněných aktiv [zdroj: autor].

Server	HDD 1	HDD 2
Doménový/souborový server	OS	Klientská dokumentace, provozní dokumentace.
Aplikační server	OS	Neobsahuje chráněná aktiva.
Poštovní server	OS	Emailová komunikace a sdílené složky.
Databázový server	OS	V databázích se nachází data z billingového a fakturačního systému.
Backup server	OS	Neobsahuje chráněná aktiva.

5.1.4 Ocenění chráněných aktiv

Cenu aktiv je možné vnímat v mnoha rovinách. Jako na první pohled nejlogičtější se nabízí finanční rovina ocenění. Ta však nemusí být ve všech případech nejvhodnější, jelikož ocenění neslouží k vyčíslení možných škod v případě katastrofy, ale k zacílení stěžejních dat v podobě chráněných aktiv. Vhodnější než finanční je ocenění pomocí bodovací škály. Ve většině případů pokryje cenu dat tříbodová škála, přičemž hodnota 1 představuje data s největší a 3 s nejmenší cenou. Na základě ocenění je možné sestavit plán zálohování, který by měl reflektovat na maximální akceptovatelnou ztrátu (RPO).

Za předpokladu, že vezmeme v potaz charakter činnosti LAW+ je možné ocenit aktiva definovaná v tabulce č. 7 následovně. Klientská dokumentace a data v databázích jsou nejčastěji modifikovanými a zároveň nejcennějšími aktivy. K nim je možné opodstatněně přiřadit hodnotu 1. Emailová komunikace je důležitá, ale díky tomu, že klientské stanice obsahují uvnitř emailových klientů off-line kopie uživatelských poštovních schránek, je v tomto případe hodnota RPO vyšší. Databáze poštovního serveru je možné ocenit hodnotou 2. Hodnotou 3 je možné ocenit provozní dokumentaci, která má nejvyšší hodnotu RPO.

Tabulka č. 8: Ocenění chráněných aktiv [zdroj: autor].

Popis	Cena
Klientská dokumentace	1
Provozní dokumentace	3
Emailová komunikace	2
Data pro billing	1
Data pro fakturaci	1

5.1.5 Ocenění systémů a služeb dle významu

Na stejném principu, jako probíhala identifikace a ocenění aktiv, je nutné rozdělit systémy a služby nezbytné pro chod společnosti podle významu. Zde se nabízí použít víceprvkovou hodnotící škálu. V návaznosti na množství systémů a služeb byla použita pětibodová hodnotící škála, kde hodnota 1 představuje nejvyšší význam a 5 význam nejmenší.

Tabulka č. 9: Ocenění systémů a služeb dle významu [zdroj: autor].

Popis	Význam
Dodávka el. energie	1
Internetová konektivita	2
Páteřní síťové prvky	2
Síťová infrastruktura	3
Fyzická serverová infrastruktura	3
Virtuální síťová infrastruktura	4
Virtuální serverová infrastruktura	4
Koncové síťové prvky	5
Koncové stanice a telefony	5
Tiskárny	5

5.1.6 Role a povinnosti jednotlivých subjektů.

Aby bylo možné zajistit po katastrofě co nejrychlejší obnovení provozu, je nezbytné již při plánování přiřadit k jednotlivým rolím i jejich povinnosti pro případ obnovy. Interní pracovníky je možné k povinnostem zavázat pracovním příkazem, ale u externích subjektů je vhodné si povinnosti pojistit smluvně. Pro tyto účely se používá smlouva o garantované úrovni služeb (SLA). Bohužel v případě tohoto smluvního svazku je nutné počítat s měsíčními náklady. Částka se pak odvíjí od garance požadované dostupnosti.

Tabulka č. 10: Role a povinnosti jednotlivých subjektů [zdroj: autor].

Popis pozice	Povinnosti
Zaměstnanci LAW+	
Top management	Rozhodnutí o spuštění procesu obnovy po katastrofě.
Manažer pro řízení lidský zdrojů	Plošné oznámení informace všem pracovníkům společnosti, v případě zranění, nebo ztrátách na životech řídí přenos zodpovědnosti a zastoupení.
Provozní manažer	Oprava stávajících objektu, pokud není oprava možná, zajištění náhradních prostor a následného přesunu.
Provozní specialista	Nákup nezbytného kancelářského a provozního vybavení
IT manažer	Zajištění spuštění všech nezbytných ICT systémů a služeb pro provoz společnosti, koordinace činností IT specialistů a dodavatelů.
IT specialista	Nákup potřebného množství koncových stanic, telefonních přístrojů (konfigurace a distribuce koncovým uživatelům) a zpřístupnění externě uložených záloh.
Dodavatelé	
Dodavatel síťové infrastruktury	Oprava, nebo rozšíření síťové infrastruktury.
Dodavatel serverové infrastruktury	Oprava, nebo dodání nové serverové infrastruktury pokryté SLA smlouvou, obnova virtuální infrastruktury a datových zdrojů ze záloh dodaných LAW+
Dodavatel aktivních síťových prvků	Dodání aktivních prvků pokrytých SLA smlouvou.
Poskytovatel internetové konektivity	Zajištění internetové konektivity, přenesení domény a jejich služeb na nový IP rozsah, přesměrování klíčových tel. čísel na mobilní telefony.
Dodavatel koncových stanic	Dodání potřebného počtu koncových stanic (instalace SW) spolupráce s IT specialistou.
Dodavatel stacionární telefonních přístrojů	Dodání potřebného počtu stacionární telefonních přístrojů (instalace SW) spolupráce s IT specialistou.

5.2 Zálohování

Při návrhu zálohování je nutné vnímat problematiku z komplexního hlediska a je jím nezbytné pokrýt všechny prvky celého systému a to jak z pohledu SW, tak HW. Zálohování je primárně využíváno k vytvoření bodu obnovy pro SW vybavení a data. Zálohovat se vyplatí nejen konfiguraci aktivních prvků, ale i periférií jako jsou disková pole, páskové mechaniky apod., přičemž právě tato oblast je často opomíjena a v případě problému zbytečně prodlužuje čas obnovy.

Zálohu HW vybavení je možné pokrýt buď redundantními prvky, nebo prostřednictvím outsourcingu, nebo SLA smlouvy s dodavatelem. Outsourcing a SLA zde suplují redundanci a je vždy důležité rozhodnout, zda pro daný DRP a jeho požadavky, je vhodnější vynaložit vyšší finanční náklady za nákup záložních prvků, nebo zda se spolehnout na dodavatele a zajistit dostupnost formou menších měsíčních nákladů.

5.2.1 Výběr způsobu zálohování

Aby bylo možné zajistit obnovu ICT systému jako celku, je nezbytné zajistit zálohování všech dílčích prvků. V tomto kroku stojí každý IT manažer před rozhodnutím, do jaké míry ponechat konkrétní způsob zálohování na interních IT specialistech, na co využít specializovaný zálohovací systém, či službu, co pokrýt redundancí a co ponechat na dodavatelích. Zde se situace výrazně zjednodušuje v případě, že organizace používá virtualizaci. Při použití infrastruktury bez virtuální vrstvy je nezbytné počítat s nutností zajištění identického HW vybavení. Virtualizací je tato nutnost výrazně eliminována.

Tabulka č. 11: Přiřazení způsobů zálohování [zdroj: autor].

Popis	Způsob zálohování
Dodávka el. energie	Chod serverové a síťové infrastruktury zabezpečen bateriovými záložními zdroji.
Internetová konektivita	V návaznosti na umístění produkčních serverů je zálohování konektivity v Brně realizováno redundantními spoji odlišné technologie a pokryto smlouvou SLA. Spoj pro pobočku není zálohován.
Páteřní síťové prvky	Optické SAN switche pracují v redundantním režimu. Zálohu páteřního routeru zajišťuje druhý "odstavený" prvek umístěný mimo serverovnu. Všechny páteřní prvky jsou pokryty smlouvou SLA.
Síťová infrastruktura	Pokryto dodavatelsky bez SLA.
Fyzická serverová infrastruktura	Provozováno na dvou ESX serverech, přičemž jeden server je z krátkodobého hlediska schopný zajistit běh všech virtuálních serverů. Pokryto smlouvou SLA.
Virtuální síťová infrastruktura	Zálohováno v rámci jednorázových záloh po každé změně prostředí. Pokryto smlouvou SLA.
Virtuální serverová infrastruktura	Zajišťuje zálohovací SW prostřednictvím periodické replikace serverů. Pokryto smlouvou SLA.
Klientská dokumentace **Provozní dokumentace** **Emailová komunikace** **Data pro billing** **Data pro fakturaci**	Zajišťuje zálohovací SW prostřednictvím periodických záloh a replikace serverů.
Koncové síťové prvky	Pokryto dodavatelskou smlouvou bez SLA.
Koncové stanice a telefony	Pokryto dodavatelskou smlouvou bez SLA.
Tiskárny	Pokryto smlouvou SLA.

5.2.2 Definice limitů

Faktorem, na který musí zálohování reflektovat, jsou hodnoty MTD a RPO. Velikost MTD se vztahuje na systémy a jejich rozdělení dle významu a RPO na chráněná aktiva a jejich cenu. Specifikace MTD a RPO je v praxi provázena několikakolovým vyjednáváním plánovacího výboru s cílem nalezení kompromisního řešení z pohledu rychlosti obnovy a nákladů s tím spojených. Prvotní hodnoty MTD a RPO vychází ze současného systému zálohování v LAW+.

Tabulka č. 12: Maximální doba tolerované nedostupnosti systémů [zdroj: autor].

Popis	Model 1	Model 2	Model 3
Dodávka el. energie	1 hodina	8 hodin	V rámci náhradních prostor
Internetová konektivita	2 hodiny	12 hodin	60 hodin od zajištění náhradních prostor
Páteřní síťové prvky	2 hodina	48 hodin	48 hodin
Síťová infrastruktura	24 hodin	48 hodin	V rámci náhradních prostor
Fyzická serverová infrastruktura	24 hodin	48 hodin	48 hodin
Virtuální síťová infrastruktura	4 hodiny	108 hodin	108 hodin
Virtuální serverová infrastruktura	4 hodiny	108 hodin	108 hodin
Koncové síťové prvky	24 hodin	Nedotčeno	60 hodin od přesunu do náhradních prostor
Koncové stanice a telefony	60 hodin	Nedotčeno	14 kalendářních dní
Tiskárny	60 hodin	Nedotčeno	14 kalendářních dní

Tabulka č. 13: Akceptovatelná ztráta dat [zdroj: autor].

Popis	Model 1	Model 2	Model 3
Klientská dokumentace	4 hodiny	1 týden	1 týden
Provozní dokumentace	12 hodin	1 týden	1 týden
Emailová komunikace	8 hodin	1 týden	1 týden
Data pro billing	4 hodiny	1 týden	1 týden
Data pro fakturaci	4 hodiny	1 týden	1 týden

5.2.3 Plán zálohování

Jedná se o řízený dokument, který popisuje, kdy má být provedena záloha, způsoby definovanými v tabulce č. 11, tak aby byly vždy dodrženy limitní hodnoty MTD a RPO v tabulkách č. 12 a 13. Plán zálohování slouží jako kontrolní dokument, který umožňuje sjednotit požadavky, zálohování a obnovu. Je klíčovým dokumentem pro IT manažera z pohledu řízení a zároveň pro IT specialistu, který je zodpovědný za nastavení a samotný průběh zálohování.

Je velmi pravděpodobné, že v průběhu procesu testování dojde k identifikaci situací, které nebudou pokrývat definované požadavky. V takovém případě bude nutné upravit hodnoty, nebo postupy tak, aby korespondovaly s realitou. Jedná se o:

- Optimalizaci ukládání a archivaci dat.
- Hledání jiných technologických řešení.
- Dokoupení přísnějších SLA a služeb.

Tabulka č. 14: Plán zálohování [zdroj: autor].

Popis	Model 1	Model 2	Model 3
Dodávka el. energie	Permanentně zálohováno bateriovými záložními zdroji.	Permanentně zálohováno umístěním prodlužovacích kabelů v prostorách provozního oddělení.	V rámci náhradních prostor.
Internetová konektivita	Permanentní záloha v podobě redundantní konektivity.	Permanentní záloha konektivity prostřednictvím obnovy síťové infrastruktury.	V rámci náhradních prostor.
Páteřní síťové prvky	Jednorázové zálohy při každé změně konfigurace. Uloženo na Backup serveru. Permanentní záloha prvků prostřednictvím on-line a off-line redundance prvků.	Je uplatněno SLA.	Je uplatněno SLA.
Síťová infrastruktura	Permanentně zálohováno umístěním strukturované kabeláže v prostorách IT oddělení.	Permanentně zálohováno umístěním strukturované kabeláže v prostorách IT oddělení.	V rámci náhradních prostor.
Fyzická serverová infrastruktura	Permanentní záloha prostřednictvím redundance ESX serverů.	Je uplatněno SLA.	Je uplatněno SLA.

Virtuální síťová infrastruktura	Jednorázové zálohy při každé změně infrastruktury. Uloženo na Backup serveru.	Víkendový full backup celé infrastruktury zkopírovaný na externě uloženou pásku.	Víkendový full backup celé infrastruktury zkopírovaný na externě uloženou pásku.
Virtuální serverová infrastruktura	Periodická tvorba replik serverů každé 4h. Uloženo na Backup serveru.	Periodická tvorba replik serverů každé 4h. Uloženo na Backup serveru.	Víkendový full backup celé infrastruktury zkopírovaný na externě uloženou pásku.
Klientská dokumentace **Provozní dokumentace** **Emailová komunikace** **Data pro billing** **Data pro fakturaci**	Periodická tvorba replik serverů každé 4h. Uloženo na Backup serveru.	Periodická tvorba replik serverů každé 4h. Uloženo na Backup serveru.	Víkendový full backup celé infrastruktury zkopírovaný na externě uloženou pásku.
Koncové síťové prvky	Není dotčeno.	Není dotčeno.	Není dotčeno.
Koncové stanice a telefony	Není dotčeno.	Není dotčeno.	Není dotčeno.
Tiskárny	Je uplatněno SLA.	Není dotčeno.	Je uplatněno SLA.

5.3 Obnova

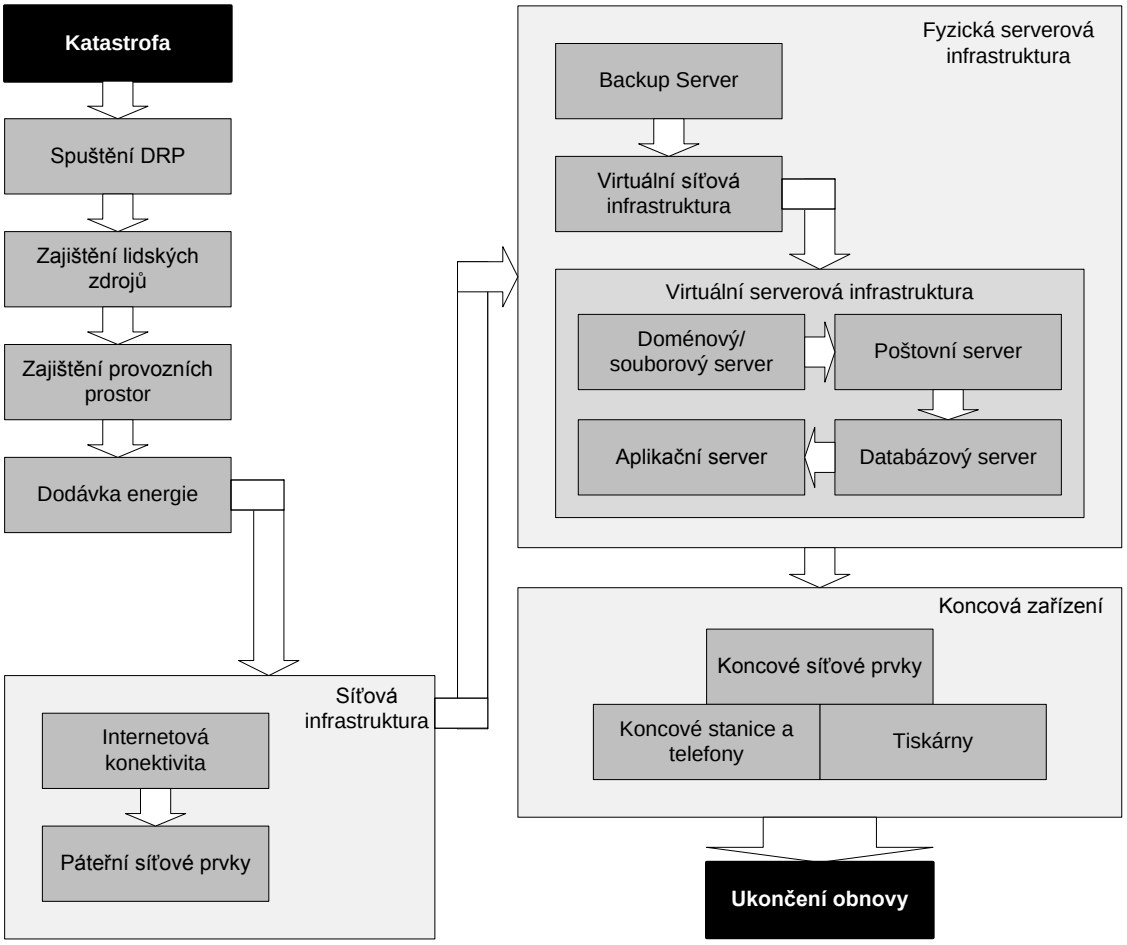
Pokud dojde k propuknutí katastrofy je popsaný, předem definovaný a v hlavní řadě realizovatelný proces obnovy to jediné co dělí organizaci od další katastrofy a tou je nemožnost obnovy, nebo obnova mimo vytyčené limity MTD a RPO. Kromě zmíněných limitů je možné se setkat také s pojmem akceptovatelného času obnovy (RTO). V otázce obnovy je RTO spojeno s obnovou dat a limitním časem nezbytným pro tuto obnovu.

V modelování procesu zálohování sloužily hodnoty MTD k definici limitních časových intervalů, mezi kterými muselo vždy dojít k vytvoření alespoň jedné zálohy (výjimkou byly systémy, nebo data, která se v průběhu času neměnila). U obnovy je princip podobný a musí platit, že hodnota RTO ≤ MTD. V opačném případě pak musí přijít na řadu proces optimalizace, při kterém dochází k:

- Separaci dat na menší logické celky.
- Hledání jiných technologických řešení.
- Restrukturaci procesu a obsahu zálohování.

5.3.1 Strategie obnovy

Všeobecně platným souborem pravidel zvyšujícím pravděpodobnost úspěšné obnovy je definice strategie obnovy. Strategii může mít každá organizace jinou, avšak konkrétně v případě ICT jsou si principiálně velice podobné. Strategie je předem akceptovanou taktikou priorizace obnovy zdrojů na základě ocenění systémů a chráněných aktiv dle tabulek č. 8 a 9. Na příkladu LAW+ je možné strategii vytýčit následovně.



Obrázek č. 13: Strategie obnovy v prostředí LAW+ [zdroj: autor].

5.3.2 Plány obnovy

Stejně tak, jako v případě plánu zálohování, je plán obnovy řízeným dokumentem, který popisuje postup při aktivaci katastrofy. Plán přiřazuje k jednotlivým modelovým situacím způsoby obnovy a je jedním z dokumentů, které musí být po finální akceptaci umístěny mimo prostor pokrytý DRP. Dále je nezbytné, aby byl v případě potřeby plán dostupný a to bez výjimky.

Tabulka č. 15: Plán obnovy [zdroj: autor].

Popis	Model 1	Model 2	Model 3
Dodávka el. energie	Bateriové záložní zdroje jsou aktivovány ihned po výpadku dodávky el. energie.	Ihned po přerušení dodávky el. energie do serverovny je spuštěn proces obnovy dodávky z jiného zdroje prostřednictvím prodlužovacích kabelů.	V rámci náhradních prostor.
Internetová konektivita	Po výpadku primární konektivity na dobu delší než 2 min. dochází k automatickému "přepadu" na sekundární linku.	Ihned po přerušení internetové konektivity do serverovny je spuštěn proces obnovy síťové infrastruktury.	V rámci náhradních prostor.
Páteřní síťové prvky	Při výpadku SAN switche přebírá okamžitě provoz druhý switch. V případě ostatních prvků spuštěn proces výměny za jiný kus.	Uplatněno SLA a dodán prvek do 24h po nahlášení.	Uplatněno SLA a dodán prvek do 24h po nahlášení.
Síťová infrastruktura	Ihned po přerušení je spuštěn proces obnovy prostřednictvím natažení provizorní strukturované kabeláže.	Ihned po přerušení síťové infrastruktury do serverovny je spuštěn proces obnovy prostřednictvím natažení provizorní strukturované kabeláže.	V rámci náhradních prostor.
Fyzická serverová infrastruktura	Při výpadku ESX serveru přebírá okamžitě provoz druhý server.	Uplatněno SLA a dodán prvek do 24h po nahlášení.	Uplatněno SLA a dodán prvek do 24h po nahlášení.
Virtuální síťová infrastruktura	Ihned po výpadku analýza problému a pokus o vyřešení. Pokud do 30 min. nevyřešeno spuštěn proces obnovy z dat na Backup serveru.	Zajištění externě uložené pásky a spuštěn proces obnovy.	Zajištění externě uložené pásky a spuštěn proces obnovy.

Virtuální serverová infrastruktura	Obnova serverové repliky uložené na Backup serveru.	Obnova serverové repliky uložené na Backup serveru.	Zajištění externě uložené pásky a spuštěn proces obnovy.
Klientská dokumentace **Provozní dokumentace** **Emailová komunikace** **Data pro billing** **Data pro fakturaci**	Obnova dat a dokumentace ze serverové repliky uložené na Backup serveru.	Obnova dat a dokumentace ze serverové repliky uložené na Backup serveru.	Zajištění externě uložené pásky a spuštěn proces obnovy.
Koncové síťové prvky	Dodavatelem je dodán nový prvek.	Dodavatelem je dodán nový prvek.	Dodavatelem je dodán nový prvek.
Koncové stanice a telefony	Dodavatelem jsou dodány nové koncové stanice a telefony.	Dodavatelem jsou dodány nové koncové stanice a telefony.	Dodavatelem jsou dodány nové koncové stanice a telefony.
Tiskárny	Uplatněno SLA a dodány tiskárny do 60h od nahlášení.	Není dotčeno.	Uplatněno SLA a dodány tiskárny do 60h od nahlášení.

5.4 Testování

Předposlední fází, kterou musí každé DRP projít je fáze testování. Zde je prakticky ověřeno, zda hodnoty a limity specifikované v předcházejících fázích jsou reálně dosažitelné. Pro případ, že testování prokáže neslučitelnost hodnot s realitou, je použita zpětná vazba, která proces plánování vrátí zpět k fázi zálohování a zde nezbývá než plánované hodnoty upravit, nebo modifikovat proces zálohování a obnovy. Testování může probíhat dvěma způsoby.

- Simulací – při simulaci jsou procházeny jednotlivé kroky zálohování a obnovy a je sledován čas potřebný na realizaci jednotlivých kroků.

  Klady: simulace ovlivňuje provoz produkčních systémů pouze v minimální míře.

  Zápory: DRP není komplexně otestován a v limitních případech nemusí být zajištěna komplexní funkčnost.

- Odstávkou – je vytvořena fiktivní katastrofa a dochází k prověření reálné funkce celého DRP.

  Klady: minimalizace rizika na maximální možnou míru.

  Zápory: odstávka zásadním způsobem ovlivňuje provoz a fungování organizace a je nezbytné, aby byla podpořena Top managementem.

Jakmile je testováním ověřena korektnost a reálná použitelnost plánu, je možné přistoupit k fázi akceptace.

5.5 Akceptace

Jedná se o závěrečný krok DRP, který se skládá z finální akceptace plánu. Plán musí být jednoznačně akceptován ze strany plánovacího výboru a následně ještě ze strany Top managementu. Teprve po odsouhlasení Top managementem, který akceptací přijímá veškerá rizika v plánu obsažená, je možné zahrnout DRP mezi interní směrnice, či nařízení organizace. Samotná akceptace se skládá z následujících třech dílčích kroků.

5.5.1 Akceptace MTD, RPO a RTO

V tomto kroku dochází k akceptaci maximální doby nedostupnosti, maximální přípustné ztráty dat a času nezbytného na obnovu, přičemž plánovací výbor schvaluje detailní podobu návrhu a Top managementu je předložena redukovaná verze klíčových stavů a hodnot.

5.5.2 Dokumentace

Pro efektivní řízení, udržování a jednoznačnou prokazatelnost DRP je nezbytné zajištění procesně-technické řízené dokumentace. Každý dokument, který spadá do jakékoliv části DRP, musí projít životním cyklem **tvorby/aktualizace, akceptace a platnosti**.

Tvorba a aktualizace může být prováděna libovolným kompetentním pracovníkem. Akceptovat dokument může pouze zodpovědná předem specifikovaná osoba (ideálně člen plánovacího výboru). V poslední řadě musí být každý dokument označen datem platnosti. Povinností zodpovědné osoby je udržování dokumentů v aktualizovaném a platném stavu, popř. tato osoba zajišťuje vyřazení neplatných dokumentů.

Název dokumentu:	Oceněný systémů a služeb dle významu		
Kód dokumentu:	DRP/023		
Vytvořil:	Petr Vomáčka	**Datum:**	12. 10. 2012
Funkce:	IT specialista	Podpis:	_____
Schválil:	Richard Novák	**Datum:**	12. 10. 2012
Funkce:	IT manažer	Podpis:	_____
Platnost od:	1. 11. 2012		
Platnost do:	1. 11. 2013		
Verze:	03		
Počet stran:	6		

Obrázek č. 14: Ukázka hlavičky řízeného dokumentu [zdroj: autor].

5.5.3 Vytvoření kolekcí dokumentů a dat pro obnovu

Při vytváření kolekcí dokumentů a dat pro obnovu dochází jednak k definici samotných kolekcí z pohledu složení a obsahu a zároveň k akceptaci plánu uložení.

Kolekce

- Data – kolekce obsahují veškeré full backup zálohy uložené na externích nosičích. V případě katastrofy jsou kolekce externě uložených dat to jediné z čeho je možné data obnovit a tím pádem je nezbytné, aby pokrývaly obsah kompletní virtuální infrastruktury. LAW+ zvolilo dle akceptovaných limitních hodnot periodické týdenní ukládání kolekcí.
- Dokumenty – do kolekcí dokumentů jsou zařazeny veškeré seznamy a pokyny potřebné pro provedení obnovy a to v papírové a ideálně i v elektronické podobě. V kolekcích dokumentů nesmí chybět nejen strategie obnovy, seznam rolí a povinností jednotlivých subjektů, ale i např. seznam kontaktů a telefonních čísel na klíčové pracovníky.

Uložení

Vytvořené kolekce je nezbytné uložit mimo prostor pokrytý DRP (je nezbytné prověřit, zda úložiště nemůže být postiženo identickou katastrofou, jako chráněný subjekt) a zajistit u nich akceptovatelnou dobu dostupnosti v okamžik požadavku na zpřístupnění. Ač následující navržený postup částečně vyvrací předchozí

tvrzení, v případě LAW+ je, díky geograficky rozděleným lokalitám působnosti, vhodné využít pro uložení prostory pardubické pobočky. Pokud katastrofa postihne pobočku a kancelář tak přijde o kolekce, je stále zabezpečen chod centrály a v opačném případě je možné využít kolekce uložené na pobočce.

Jako ideální úložiště mohou posloužit prostory bankovních institucí, bezpečnostní schránky, prostory bezpečnostních agentur apod.

ZÁVĚR

Při tvorbě BP bylo zjištěno, že plánování obnovy po katastrofě je rozsáhlou problematikou, která je ovlivněna výrazně větším množstvím faktorů, než autor předpokládal na počátku práce. Z tohoto důvodu bylo nutné vhodně redukovat nashromážděné podklady a vyseparovat klíčové informace s přímou vazbou nebo dopadem na ICT.

Jako vstupní informace byly použity podklady z emailové ankety, na jejímž základě byla provedena analýza současného stavu výuky DRP na FES UPa. Jelikož bylo anketou potvrzeno, že problematiku komplexně nepokrývá žádný z vyučovaných předmětů v rámci bakalářského studia, bylo pro tvorbu BP nezbytné využít převážně externích informačních zdrojů.

V první řadě bylo přistoupeno k definici základních pojmů, jež slouží k úvodnímu seznámení čtenářů s problematikou a zároveň plní funkci nezbytného know-how potřebného k objasnění dalších kroků. Aby bylo možné splnit hlavní vytyčený cíl, pokračuje BP sestavením případové studie. Na příkladu imaginární společnosti LAW+ je demonstrován postup analýzy nezbytné pro zacílení prostředků DRP na stěžejní chráněná aktiva a systémy. Následuje krok, ve kterém dochází k formulaci samotného postupu tvorby DRP na reálném příkladu. Postup je názorně představen na základě průchodu všemi fázemi životního cyklu DRP ve vztahu k ICT.

Obsah celé práce v závěru posloužil k vytvoření elektronické verze jedné kapitoly skript a prezentace pro výuku předmětu „Úvod do bezpečnosti a ochrany informací“, jež jsou přílohou této BP.

Na základě předchozího shrnutí je možné konstatovat, že v rámci BP došlo ke splnění hlavního a zároveň obou dílčích cílů. Doufám, že BP se stane dostatečně odborným a uceleným studijním materiálem pro výuku DRP na FES UPa a umožní tak zvýhodnit studenty na trhu práce.

POUŽITÁ LITERATURA

[1] BASL, J., BLAŽIČEK, R. *Podnikové informační systémy: Podnik v informační společnosti.* 2. vyd. Praha: Grada Publishing, 2008. 283 s. ISBN 978-80-247-2279-5.

[2] BRABEC, F. *Ochrana bezpečnosti podniku.* 1. vyd. Praha: Eurounion, 1996. 203 s. ISBN 8080-85858-29-0.

[3] GREGORY P. *IT Disaster Recovery Plannig For Dummies.* 1. vyd. Hoboken: Wiley Publishing, Inc., 2007. 360 s. ISBN 978-0-470-03973-1.

[4] SMEJKAL, V., RAIS, K. *Řízení rizik,* 1. vyd. Praha: Grada Publishing., 2003. 270 s. ISBN 80-247-0198-7.

[5] SNEDAKER, S. Business *Continuity and Disaster Recovery Planning for IT Professionals.* Burlington: Syngress, 2007. 456 s. ISBN 1-59749-172-1.

[6] *Business World* [On-line]. 2011 [cit. 2012-11-18]. Co zvážit při plánování disaster recovery. Dostupné z WWW: [http://businessworld.cz/it-strategie/co-zvazit-pri-planovani-disaster-recovery-7138].

[7] *Univerzita Pardubice, Fakulta ekonomicko-správní* [On-line]. 2011 [cit. 2012-11-18]. Přehled bakalářských studijních programů a oborů. Dostupné z WWW: [http://www.upce.cz/fes/studium/bakalarske-studium/prehled_bc.html].

[8] *EM-DAT, The International Disaster Database* [On-line]. 2009 [cit. 2013-01-15]. Mezinárodní databáze katastrof. Dostupné z WWW: [http://www.emdat.be/].

[9] KUKAL, Z. *Přírodní katastrofy.* 2. vyd. Brno: Horizont, 1983. 264 s.

[10] ŘÍHA, J. *Kritická infrastruktura a riziko mimořádné události* [On-line]. 2007 [cit. 2013-01-16]. Urbanismus a územní rozvoj. Dostupné z WWW: [http://www.uur.cz/images/publikace/uur/2007/2007-04/08_kriticka.pdf].

[11] *Oracle* [On-line]. 2003 [cit. 2013-08-01]. Portál podpory produktů společnosti Oracle. Dostupné z WWW: [http://docs.oracle.com/cd/E19088-01/v65x.srvr/817-2023-11/APPA.html].

[12] *ICT Security* [On-line]. 2010 [cit. 2013-03-25]. Nezávislý odborný on-line magazín. Dostupné z WWW: [http://www.ictsecurity.cz/09/09/2-zalohovani/maly-prehled-zalohovacich-medii.html].

[13] *3S.cz s.r.o.* [On-line]. 2011 [cit. 2013-04-05]. Webový portál společnosti 3S.cz. Dostupné z WWW: [http://www.storage.cz/775-lto-dlt-slr-co-je-lepsi].

[14] *VMware* [On-line]. 2013 [cit. 2013-06-01]. Webový portál společnosti VMware. Dostupné z WWW: [http://labs.vmware.com/flings/thinapp-vsphere].

[15] *Symantec* [On-line]. 2011 [cit. 2013-06-01]. Webový portál společnosti Symatec. Dostupné z WWW: [http://www.symantec.com/about/news/release/article.jsp?prid=20110111_01].

[16] *Disaster Recovery Jurnal* [On-line]. 2013 [cit. 2013-06-02]. Odborný magazín zabývající se problematikou obnovy po pohromě. Dostupné z WWW: [http://www.drj.com/].

[17] *IT slovník* [On-line]. 2008 [cit. 2013-06-23]. Výkladnový slovník IT terminologie. Dostupné z WWW: [http://it-slovnik.cz/].

[18] *Veeam Modern Data Protection* [On-line]. 2013 [cit. 2013-06-01]. Prezentace Veeam Backup & Replication pro VMware a Hyper-V. Dostupné z WWW: [http://www.veeam.com/cz/vmware-esx-backup.html].

[19] *PCPro-Computing in the Real World* [On-line]. 2013 [cit. 2013-07-12]. Odborný ICT portál. Dostupné z WWW: [http://www.pcpro.co.uk/gallery/reviews/374467/symantec-backup-exec-2012/177901].

[20] HUB, M. *Plánování obnovy po pohromě* [On-line]. 2007 [cit. 2013-07-24]. Prezentace pro výuku DRP. Dostupné z WWW: [http://files.it-enclave.webnode.cz/200000030-d9882da81c/10_Planovani_obnovy_po_pohrome.pdf].

[21] *VMware* [On-line]. 2013 [cit. 2013-08-01]. Produktový portál vSphere 4 společnosti VMware. Dostupné z WWW: [http://pubs.vmware.com/vsphere-4-esx-vcenter/index.jsp?topic=/com.vmware.vsphere.intro.doc_41/c_vmware_infrastructure_distributed_services.html].

SEZNAM PŘÍLOH

Příloha A