VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

ZAVEDENÍ BUSINESS CONTINUITY AND DISASTER RECOVERY STRATEGIE
BUSINESS CONTINUITY AND DISASTER RECOVERY STRATEGY IMPLEMENTATION

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — **Bc. Matúš Solár**
AUTHOR

VEDOUCÍ PRÁCE — **Ing. Petr Sedlák**
SUPERVISOR

BRNO 2017

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Matúš Solár**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Petr Sedlák**
Akademický rok:	2016/17

Ředitel ústavu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává diplomovou práci s názvem:

Zavedení Business Continuity and Disaster Recovery strategie

Charakteristika problematiky úkolu:

Úvod
Vymezení problému a cíle práce
Teoretická východiska
Analýza současného stavu
Vlastní návrh řešení
Zhodnocení a přínosy práce
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je vlastní návrh pro zlepšení Business Continuity and Disaster Recovery strategie v pobočce banky. Jako podklad pro zpracování návrhu bude sloužit analýza současného stavu a standard platný v rámci celé organizace. Metoda Business Impact Analysis (BIA), která je základní metodou při vytváření plánů kontinuity činností, odhalí slabá místa organizace, potřeby jednotlivých týmů a možná rizika. Na základě uvedených analýz a komunikace s týmy navrhnu řešení pro zlepšení efektivity BCDR strategie. Navržené řešení a vypracování samotné strategie budou sloužit společnosti jako „manuál“ v případě katastrofy nebo krize.

Základní literární prameny:

BARTA, J., O. SVOBODA a J. URBÁNEK. Krizová interoperabilita. Brno: Univerzita obrany Brno, 2015. ISBN 978-80-7231-428-7.

ONDRÁK, V., P. SEDLÁK a V. MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

POŽÁR, J. Informační bezpečnost. Plzeň: Vydavatelství a nakladatelství Aleš Čeněk, 2005. ISBN 80-86898-38-5.

SZABADOS, Ľ., M. BRADÁČ a M. ĎORDA. Business Continuity Management. Bratislava: TATE International Slovakia, 2008. ISBN 978-80-969747-2-6.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2016/17

V Brně dne 28.2.2017

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Táto diplomová práca sa zaoberá a analyzuje problematiku stratégie kontinuity činností a obnovy po katastrofe. Navrhuje možné riešenia a ich praktickú implementáciu v reálnom prostredí banky. Súčasťou práce sú teoretické východiská, analýza súčasného stavu, ktorá vypovedá o nedostatkoch v danom prostredí a v neposlednom rade návrhy na zavedenie samotnej stratégie.

Abstract

This master thesis deals and analyzes the problems in the area of Business Continuity and Disaster Recovery strategy. It proposes a possible solutions, its practical implementation in the real environment of bank. Part of this work speaks about theoretical background, second part of this work analyzes the current situation, which describes the deficiencies in the given directions and in the end are explained my practical advices for implementation of the Business Continuity and Disaster Recovery strategy.

Kľúčové slová

riadenie kontinuity činností, obnova po katastrofe, analýza dopadu na business, testovanie, plán kontinuity činností, plán obnovy po katastrofe, kritická situácia, katastrofa, riziko

Key words

business continuity, disaster recovery, business impact analysis, testing, business continuity plan, disaster recovery plan, criticall situation, disaster, risk

SOLÁR, M. *Zavedení Business Continuity and Disaster Recovery strategie.* Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2017. 73 s. Vedoucí diplomové práce Ing. Petr Sedlák.

Prehlásenie autora o pôvodnosti práce

Prehlasujem, že predložená diplomová práca je pôvodná a spracoval som ju samostatne. Prehlasujem, že citácia použitých prameňov je úplná, že som vo svojej práci neporušil autorské práva (v zmysle zákona 121/2000 Zb., o práve autorskom a o právach súvisiacich s právom autorským).

V Brne dňa 30.mája 2017 .....

Podpis študenta

Poďakovanie

Týmto by som sa rád poďakoval vedúcemu mojej diplomovej práce, pánovi Ing. Petrovi Sedlákovi za cenné pripomienky, poskytnuté rady a v neposlednom rade za ochotu prejavenú pri spracovávaní tejto diplomovej práce.

OBSAH

ÚVOD

V súčasnej dobe, viac ako kedykoľvek predtým, je každá spoločnosť vystavená vysokému riziku možných ohrození. Teroristické útoky, prírodné katastrofy, strata kľúčových zamestnancov a mnoho ďalších nepredvídateľných udalostí môže viesť k úplnej likvidácií spoločnosti, alebo jej postavenia na trhu. Preto dnes organizácie venujú čoraz viac pozornosti plánovaniu kontinuity činností (Business Continuity Management) a riadeniu obnovy po katastrofe (Disaster Recovery). Schopnosť organizácie obnoviť svoje kľúčové procesy a tak zachovať poskytovanie služieb zákazníkom je závislá na vyspelosti Business Continuity and Disaster Recovery stratégie.

Business Continuity and Disaster Recovery je nikdy nekončiaci a neustále sa zdokonalujúci proces v každej organizácií. Základom takéhoto procesu je poznanie všetkých rizík a analýza slabých miest, ktoré môžu narušiť činnosť spoločnosti.

Výstupom riadenia kontinuity činností je Business Continuity Plan – zásadný dokument definujúci stratégiu riadenia krízových situácií. Podobne to platí aj pre podoblasť Disaster Recovery a DR plánov. Takéto plány, aby mohli byť efektívne a použiteľné, musia byť neustále aktualizované. Vypracovanie kompletnej Business Continuity and Disaster Recovery stratégie je rozsiahla činnosť, ktorá sa týka každého teamu, procesu a zamestnanca v spoločnosti.

Moja práca je rozdelená do troch hlavných častí.
V prvej časti sa budem zaoberať teoretickými východiskami v odbore Business Continuity and Disaster Recovery a objasnením základných pojmov.
V druhej časti bude spracovaná analýza súčasného stavu BCDR stratégie v spoločnosti a definovaná projektová stránka zavádzania stratégie.
V tretej, poslednej, časti mojej práce budem navrhovať vlastné riešenia pre zavedenie Business Continuity and Disaster Recovery stratégie do spoločnosti.

CIELE PRÁCE

Cieľom tejto práce je spracovanie vlastného návrhu pre zavedenie Business Continuity and Disaster Recovery stratégie do banky. Ako podklad bude pre spracovanie návrhu slúžiť analýza súčasného stavu. Metóda Business Impact Analysis (BIA), ktorá je základnou metódou pri vytváraní plánov kontinuity činností, odhalí slabé miesta organizácie, potreby jednotlivých teamov a možné riziká. Na základe uvedených analýz a komunikácie s tímami navrhnem riešenia BCDR stratégie. Navrhnuté riešenia a vypracovanie samotnej stratégie budú slúžiť spoločnosti ako „manuál“ v prípade katastrofy.

1. TEORETICKÉ VÝCHODISKÁ PRÁCE

V súčasnej dobe a vysokej konkurencie v oblasti bankových služieb je zaručenie nepretržitého poskytovania služieb zákazníkom veľmi významným elementom. Každý jednotlivec a o to viac firmy sú závislé na okamžite prístupných bankových službách či už sa jedná o internet banking alebo iné produkty. V rozsahu tejto práce neodkážem popísať všetky vedomosti doposiaľ známe o Business Continuity and Disaster Recovery, preto sa budem snažiť popísať základnú terminológiu a základné metódy používané pre riadenie kontinuity činností, z ktorých budem ďalej vychádzať pri návrhu samotných riešení.

1.1. Business Continuity Management

Business Continuity Management v takej podobe ako ho poznáme v súčasnosti, sa začal formovať v USA v 80. rokoch minulého storočia ako reakcia na opakujúce sa prírodné katastrofy (tornáda, hurikány, zemetrasenia a povodne). Mal vyslovene hospodársky podtón a oddelil sa od krízového riadenie štátu. Nosnou úlohou bolo pre organizáciu stanoviť správnu reakciu na nepredvídateľné udalosti tak, aby škody boli minimalizované a aby narušené činnosti boli v čo najkratšom čase obnovené v primeranom rozsahu a kvalite. Terminológia v tom čase zatiaľ nebola ujednotená až do chvíle, kým vznikla inštitúcia Disaster Recovery Institute International (USA, 1988). Táto inštitúcia v roku 1993 vydala Professional Practices for Business Continuity Planners. Toto sa stalo prvým štandardom pre oblasť BCM. Informačné technológie vniesli do BCM radikálne zmeny. Organizácie sa stali závislími na funkčnosti ICT. Vďaka tejto závislosti sa BCM často zamieňal s obnovou funkčnosti ICT a celková zodpovednosť za obnovu bola prenesená na útvary ICT. Následne dochádzalo k paradoxom, napr. Po havárií by bola funkčnosť ICT obnovená v rekordne krátkom čase, ale nemal by na nej kto pracovať (1).

„Business Continuity Management – BCM (Riadenie kontinuity činností organizácie) je riadiaci proces na úrovni vedenia spoločnosti, ktorého cieľom je vytvoriť v spoločnosti také postupy a prostredie, ktoré umožní zaistiť kontiniutu a obnovu kľúčových procesov a činností organizácie na dopredu stanovenú minimálnu úroveň (pre prípad ich narušenia alebo straty napríklad vplyvom požiaru, výpadku napájania, prírodnej katastrofy apod.) BCM ochraňuje záujmy kľúčových podieľnikov, akcionárov a ďalších záujmových skupín, dobrú povesť a značku spoločnosti (2, s.125).“

V rámci BCM sa riešia Plány kontinuity činností (BCP), ktorých cieľom je definovať náhradné postupy pre poskytovanie dôležitých obchodných služieb spoločnosti a Plány obnovy funkčnosti (DRP), ktorých cieľom je znížiť dĺžku prípadného výpadku informačného systému v prípade závažných havarijných situácií v hlavnom výpočtovom stredisku spoločnosti (1).

1.1.1. Životný cyklus BCM

Business Continuity Management je nikdy nekončiaci proces. Business Continuity plány musia byť neustále aktualizované aby reflektovali zmeny, ktoré prebiehajú v rámci organizácie eventuálne aj mimo nej.

Obrázok č.1.: Životný cyklus BCM

Zdroj: (vlastné spracovanie)

1.1.2. Business Continuity Strategy

Business Continiuty stretégia vychádza z akčného plánu a musí byť podložená analýzami. Jednou z nich je BIA (Business Impact Analysis) a LRA (Location Risk Assesment) – obe analýzy sú rozvinuté a popísané ďalej v tejto práci.

„Na základe Business Impact Analysis by mal generálny riaditeľ, prípadne predstavenstvo spoločnosti schváliť stratégiu pre zvládanie havarijných situácií. Táto stratégia by mala riešiť napríklad:

- *Ktoré obchodné aktivity je potrebné v prípade havarijnej situácie obnoviť,*
- *Aké sú priority pre obnovu jednotlivých obchodných aktivít.*

Samozrejme, tak ako každá stratégia, aj táto by mala už pri predložení na schválenie byť podporená akčným plánom, ktorý popisuje:

- *Úlohy, ktoré je potrebné vykonať pre napĺňanie stratégie,*
- *Predpokladaný časový harmonogram,*
- *Predpokladané náklady (1, s.23).“*

1.1.3. Business Continuity Plan – BCP

Business Continuity Plan je súbor dokumentovaných procedúr zahrňujúci všetky činnosti a informácie potrebné na zabezpečenie nepretržitej dodávky služieb a produktov na požadovanej úrovni a v požadovaných časoch v prípade ich prerušenia. BCP môžeme označiť ako „návod“ ako postupovať v prípade krízovej situácie. Obsahuje všetky potrebné informácie k zabezpečeniu zvoleného procesu/činnosti sústredené na jednom mieste.

BCP musí byť vypracovaný pre všetky aktivity, ktoré boli definované v BIA, vrátane outsourcovaných. Takýto plán zahŕňa konkrétne postupy, ako danú aktivitu obnoviť, po prípade popiseuje alternatívne postupy obnovy danej aktivity. Aktivity, ktoré nie sú definované v BIA, nie sú predmetom Business Continuity plánu.

Možných scenárov pre spustenie BCP je mnoho. Môže ísť o:

- Katastrofu – neštandardnú udalosť spôsobujúcu rozsiahle zničenie alebo nebezpečenstvo (požiar, explózia, povovdeň, nebezpečie bombového útoku, zemetrasenie, havária technickej infraštruktúry).
- Následky katastrofy – zničené, nepoužiteľné budovy
- Ďalšie udalosti – napríklad štrajk, kybernetický útok a s tým spojená nefunkčnosť rôznych systémov a podobne.

S týmto je spojené vytváranie BCP plánov zvlášť pre rôzne situácie, napríklad BCP pre stratu budovy bude odlišný od BCP pre stratu dodávateľa.

1.1.4. Metriky BCP

Maximálne tolerovateľná doba nedostupnosti – MTPD

Maximum tolerable period of disruption - MTPD je metrika definovaná v každom riadne spracovanom Business Continuity pláne.

„Doba, počas ktorej ešte nie je ohrozené poskytovanie produktov, služieb alebo činností organizácie v prípade ich nedostupnosti (1, s.36).“

Doba obnovy činností – RTO

„Časový úsek, v ktorom musí byť obnovená činnosť kritického procesu (1, s.37).“

Ide o hodnotu odvodenú z hodnôt MTPD, ktoré boli získané na odborných útvaroch organizácie v priebehu realizácie analýzy dopadov (BIA). Pri stanovovaní RTO je potrebné brať ohľad na vzťahy a závislosti medzi jednotlivými procesmi.

RTO (Recovery time objectives) je časový úsedk, v rámci ktorého musia byť obnovené dôležité procesy po zlyhaní. Časy RTO sa používajú ako základ na vývoj stratégie obnovy a ako podklad pre rozhodovanie, či iniciovať alebo neiniciovať stratégiu obnovy v prípade havárie (1).

Maximálne tolerovateľná strata údajov – MTDL

Maximum tolreable data loss MTDL - jedná sa o maximálny objem údajov, o ktorý je možné prísť v prípade mimoriadnej situácie bez závažného dopadu na kľúčové procesy organizácie (1).

Minimálna úroveň služieb – MRSL

Minimal required service level MRSL je minimálna úroveň služieb, ktorá je akceptovateľná na dosiahnutie cieľov organizácie.

Kritický prvok zlyhania

Jedná sa o jedinečný zdroj služieb, aktivít alebo procesov, ku ktorému neexistuje žiadna alternatíva a jeho zlyhanie vedie k totálnemu zlyhaniu kľúčových procesv organizácie.

1.2. Disaster Recovery

„V prípade, že organizácia má zavedený Business Continuity plán alebo Incident Management, DR plán je tvorený ako kompatibilná súčasť týchto metodík a procesov.

Disaster Recovery (DR – obnova po havárii) je proces, politiky a postupy týkajúce sa prípravy na zaistenie chodu technologickej infraštruktúry kritickej pre organizáciu po prírodnej alebo človekom vyvolanej katastrofe.

DR je podmnožinou zaistenia kontinuity chodu BCM. Zatiaľ čo zachovávanie kontinuity chodu zahŕňa plánovanie pre udržanie všetkých aspektov fungovania podniku uprostred rušivých udalostí, DR sa zameriava na IT technológie alebo systémy, ktoré podporujú podnikové funkcie (2, s. 125).“

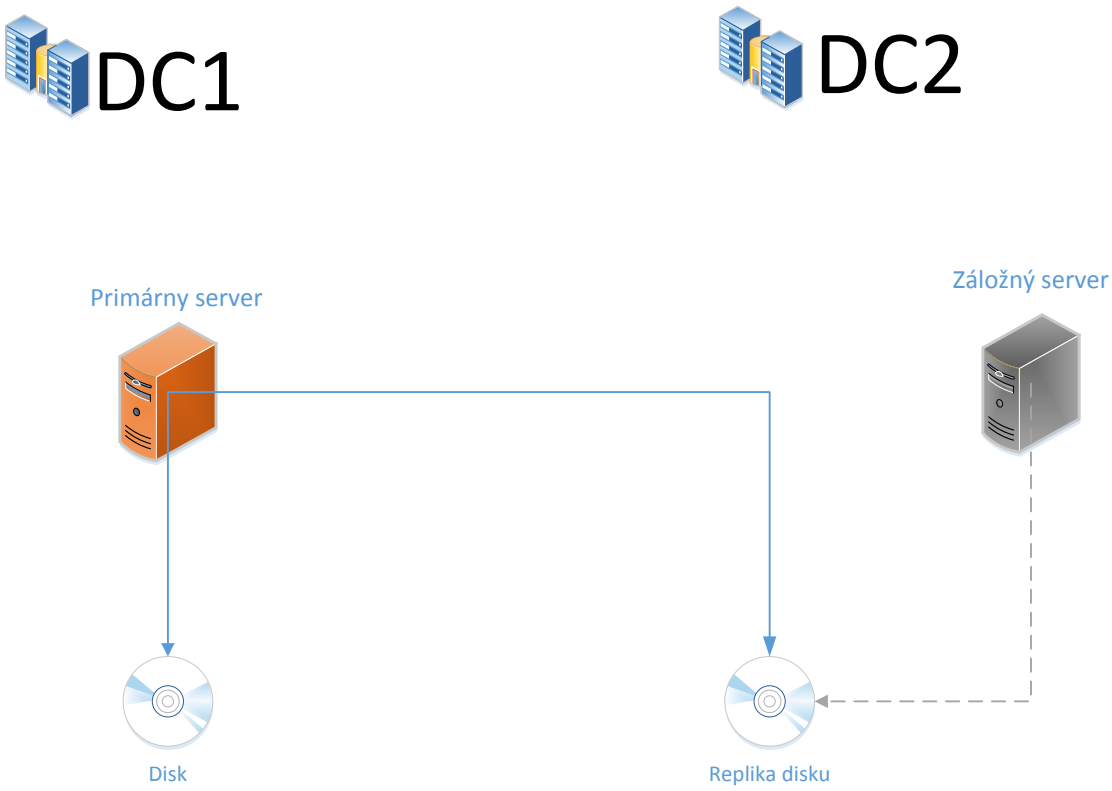
1.2.1. Disaster Recovery Plan

Disaster Recovery plán zhromažďuje postupy pre zaistenie obnovy IT služieb po živelných pohromách a iných závažných udalostiach. Je to vpodstate návod ako v čo najkratšom čase a s minimom výdavkov obnoviť chod kritických aplikácií.

Obsah DR plánu:

- Reťazec konkrétnych krokov,
- Definícia assessment týmu pre analýzu problémov,
- Definícia recovery týmu pre obnovenie spracovania,
- Definícia management týmu pre riadenie procesu,
- Špecifikácia rolí, menné zoznamy, telefónne kontakty,
- Rozhodovacie procesy, metódy eskalácie problémov, logovanie procesov.

DR plán je veľmi úzko spojený s organizáciou IT a technologickou infraštruktúrou. Z tohto dôvodu je dôležitá pravidelná aktualizácia plánov a testovanie procesov v reálnom prostredí (2).



Obrázok č.2.: Spustenie služieb zo záložného serveru v druhom datacentre

Zrdoj: (vlastné spracovanie)

Na obrázku vyššie vidíme tzv. Failover – spustenie služieb zo záložného serveru s replikovaným diskom z druhého datacentra. Aby sme mohli hovoriť o Disaster Recovery, tak musí byť prevedený ďalší krok a to obnova funkčnosti primárneho serveru a spustenie služieb z pôvodeného datacentra.

Architektúra takýchto riešení môže byť rôzna či už stand-alone servery, architektúra typu active-active alebo rôzne druhy clusterov. Uvedený obrázok slúži iba ako príklad a vysvetlenie rozdielu medzi Failover a Disaster Recovery.

1.2.2. Disaster Recovery v Cloude

Cloud computing založený na virtualizácií umožuje celkom nový prístup k Disaster Recovery. Prostredníctvom virtualizácie je celý server zahŕňajúci operačný systém, aplikácie, záplaty a dáta skombinovný do jednej softwarovej entity – Virtuálneho serveru.

Kompletný Virtuálny Server môže byť skopírovaný alebo zálohovaný do vzdialeného datového centra a sprístupnený behom niekoľkých minút.

Nakoľko je Virtuálny Server nezávislý na hardwarovej vrstve, môžu byť operačný systém, aplikácie, záplaty a dáta bezpečne a kompletne transferované medzi datovými centrami bez nutnosti inštalácie jednotlivých komponentov.

Táto metóda dramaticky znižuje čas obnovenia v porovnaní s konvenčnými prístupmi k Disaster Recovery, kde je na reálne servery postupne inštalovaný OS, aplikácie, najaktuálnejšie záplaty podla konkrétnej konfigurácie.

1.2.3. Architektúra DR v Cloude

Privátny Cloud na zariadení umiestnenom u koncového užívateľa na dedikovanej fyzicky oddelenej platforme.

Riadený Cloud na zariadení umiestnenom u poskytovateľa služieb na fyzicky či logicky oddelenej platforme.

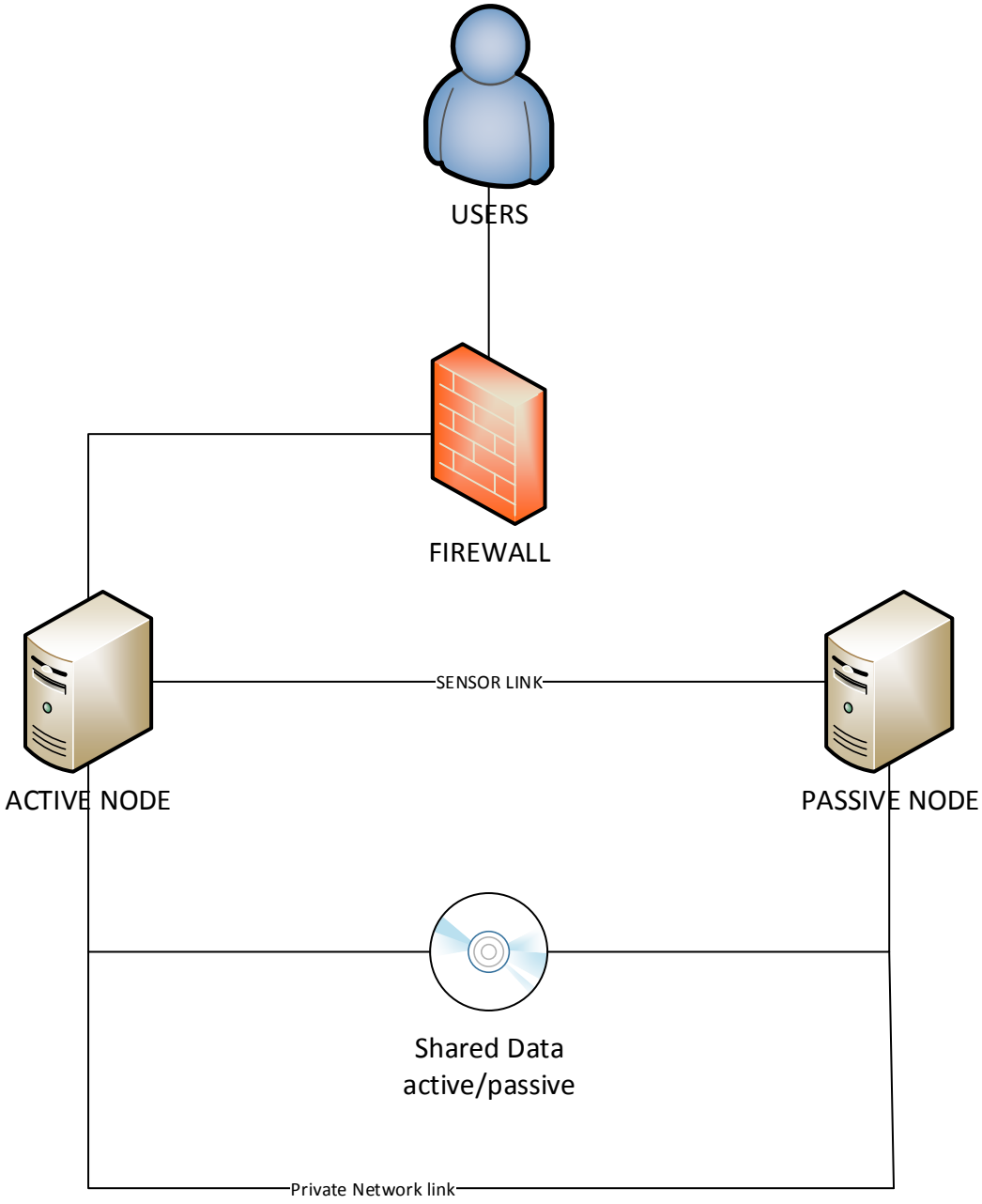
Verejný Cloud na zariadení umiestnenom u poskytovateľa služieb pre viacero zákazníkov na logicky oddelenej platforme.

1.2.4. High Availability / Failover Clustery

High Availability clustery predstavujú zoskupenie počítačov, podporujúce serverové aplikácie, ktoré môžu byť spolahlivo použité s minimálnymi časmi odstávky.

Tieto clustery používajú software s vysokou dostuponosťou (High Availability), ktorý dokáže využiť reduntantné počítače v clustery a poskytuje neprerušené služby aj pri výpadku systémových komponentov.

High Availability clustery zvyšujú celkovú odolnosť prostredníctvom detekcie HW/SW výpadkom a okamžitým reštartom na inom systéme bez zásahu administrátora – tzv. **Failover.**



Obrázok č. 3.: High Availability Cluster

Zdroj: (vlastné spracovanie)

1.3. Podporné procesy

1.3.1. Business Impact Analysis

„Analýza dopadov (na podnikateľské funkcie Business Impact Analysis –BIA) organizácie patrí medzi najdôležitejšie etapy v procese riadenia kontiniuty činností organizácie. Jej cieľom je identifikovať kritické procesy a podprocesy v organizácií a určiť dopady nedostuponosti týchto procesov v prípade straty, narušenia a lebo prerušenia týchto procesov. Taktiež má za úlohu nájsť a odhodnotiť závislosti kritických procesov od ostatných procesov a podprocesov organiyácie, ktoré neboli kritické. V prípade závislosti sú potom aj tieto procesy a podprocesy považované za kritické. V prípade vzniku incidentu alebo kritickej situácie organizácia najskôr obnoví tie procesy, ktoré BIA analýza vyhodnostila ako kritické (1, s.115).“

Prostredníctvom tejto analýzy organizácia

A) Kvantitatívne (napr. na základe finančnej straty, úrovni poskytovaných služieb)

B) Kvalitatívne (napr. na základe reputácie, právnych a regulačných aspektov)

zhodnotí dopady a straty, ktoré môžu nastať v prípade závažného incidentu. V tomto procese sa taktiež určí minimálna úroveň zdrojov potrebných na obnovu kritických činností.

Súčasťou analýzy je identifikácia nákladov, ktoré by bolo potrebné vynaložiť na obnovu pri zlyhaní kritického procesu. Ich vyjadrenie je možné formou:

- Priameho finančného ohodnotenia,
- Nákladov na náhradu majetku,
- Nákladov spojených s obnovením činností,
- Ušlého zisku (1).

Dopady je možné vyjadriť aj v nefinančnej form, čo však neznamená, že v konečnom dôsledku nebudú znamenať finančnú ujmu, napr.: strata dobrého mena organizácie alebo dopad na súlad s platnou legislatívou.

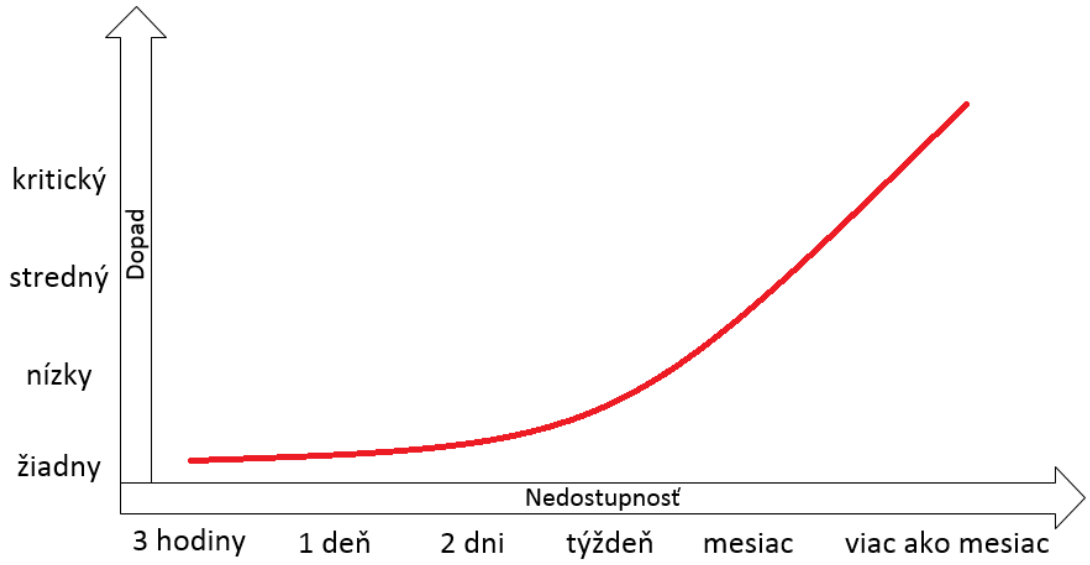
„Analýza dopadov pozostáva z nasledujúcich krokov:

- *Identifikácia a ohodnotenie oblastí,*
- *Identifikácia procesov a podprocesov v každej oblasti,*
- *Hodnotenie procesov a podprocseov,*
- *Vyhodnotenie analýzy,*
- *Správa z BIA (1, s.115).“*

Ciele BIA:

- Stanovenie kľúčových procesov organizácie,
- Zistenie finančných a nefinančných dopadov, ktoré by mohli mať mimoriadna alebo krízová udalosť,
- Určenie minimálnej výšky zdrojov (materiálne, technické, technologické, ľudské, kapacitné...)
- Stanovenie požadovaného časového horizontu obnovy,
- Stanovenie priorít pri obnove procesov/činností,
- Porovnanie výšky strát a nákladov na obnovu procesu v závislosti na čase,
- Prevencia – stanovenie požadovaného spôsobu zabezpečenia kľúčových procesov, systému a dát.

Pre väčsinu organizácií, definovanie obsahu BIA je založené na troch faktoroch: časový faktor, rozpočtový faktor a procesy generujúce zisk (6).



Obrázok č.4.: Finančné dopady v prípade nedostupnosti

Zdroj: (1, s.121)

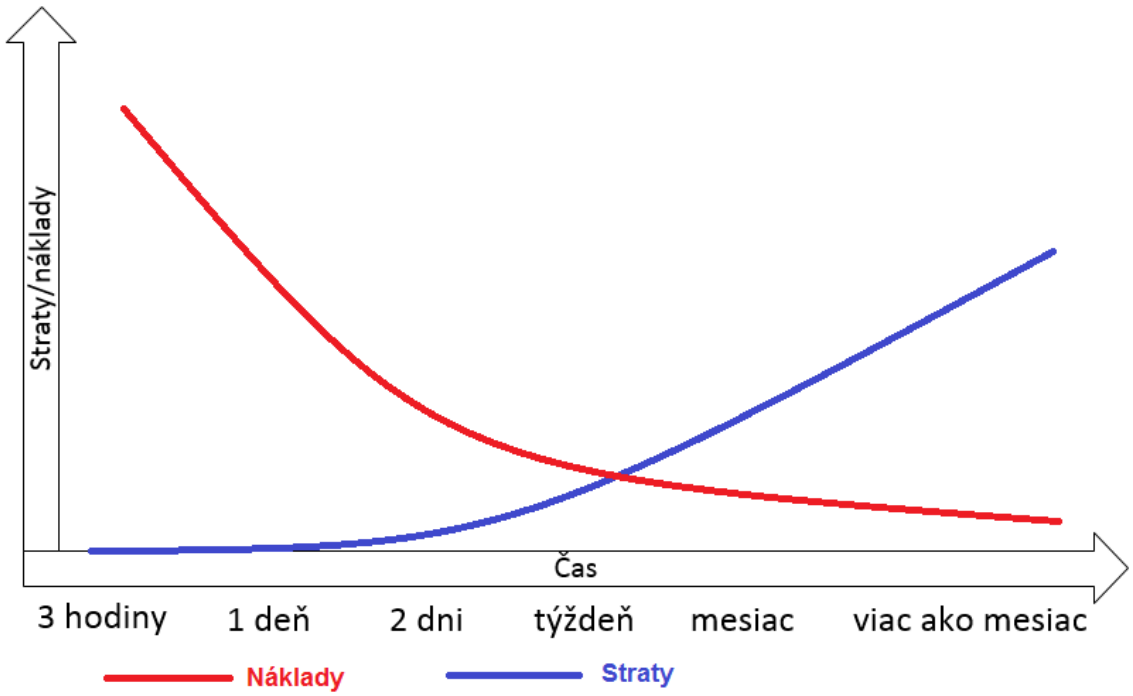
Hodnotenie dopadov pre nedostuponosť procesu sa všeobecne definuje finančnými stratami vyplývajúcimi z nedostupnosti procesu. Presné určenie finančných strát je v niektorých prípadoch dosť komplikované, preto si môžeme pomôcť definovaním funančných strát v niekoľkých základných úrovniach.

Štandardným súhrnom o vykonanej BIA analýzy je Výstupná správa z BIA. Slúži ako jeden z výstupnýc dokumentov analytickej fázy. Mala by obsahovať minimálne:

- Zámer organizácie, ciele,
- Kritické procesy organizácie,
- Finančné alebo nefinančné dopady spôsobené stratou alebo narušením procesu,
- Ciele BCM pre každý kritický proces,
- Minimálne požiadavky na zdroje nutné na obnovu kritického procesu,
- Dôležité záznamy, kľúčových klientov, dodávateľov,
- Stanovenie RTO,

- Časový rozpis s prioritami aktivít pri obnovovaní kritických procesov,
- Rozpis priorít a investícií do kontinuity činnosti organizácie,
- Profil obnovy zdrojov potrebných na obnovu ktritických procesov,
- Kritériá pre viacúrovňovú analýzu dopadov (1).

Analýza dopadov musí byť spracovaná predtým ako sa začne v organizácií stanovovať prijateľná úroveň rizika. Túto úroveň stanovuje práve analýza dopadov a s ňou súvisiace hodnotenie rizík.



Obrázok č.5.: Straty nedostupnosti voči nákladom na obnovu

Zdroj: (1, s.122)

1.3.2. Ohodnotenie rizík

Dôležitou súčasťou BCM je ohodnotenie rizík, tzv.: Risk Assessment. Riziká musia byť ohodnotené tak, aby možnosť toho, že kritické procesy budú ovplyvnené, bola minimalizovaná na čo najnižšiu úroveň. Na dosiahnutie tohto stavu je potrebné zostaviť a implementovať súbor vhodných opatrení.

„Zachytáva zoznam hrozieb pôsobiacich na IS a stanovuje riziká príslušné každému zraniteľnému miestu a hrozbe. Účelom takého dokumentu je zníženie rizík na prijateľnú úroveň, respektíve akceptáciu zbytkových rizík tam, kde je ich minimalizácia neefektívna (2, s.90).“

Príklad hrozieb:

Fyzické prostredie		
Budova	Vonkajšie hrozby	Okolie
dlhodobý výpadok el. energie výpadok UPS zlyhanie údržby terorizmus požiar neautorizovaný prístup	krádež poistný podvod poškodenie IS poškodenie majetku sabotáž podpaľačstvo	záplavy prudké dažde zemetrasenie priemyselné nehody víchrica
ICT technológie		
nedostupnosť ICT systémov nedostupnosť SW alebo HW narušenie alebo strata údajov neautorizovaná činnosť poruchy a chyby SW alebo HW infiltrácia nedostatočné testovanie odmietnutie služby		

Tabuľka č.1.: Príklady hrozieb

Zdroj: (vlastné spracovanie)

1.3.3. Testovanie

Testovanie Business Continuity / Disater Recovery plánov slúži k ich validácií a odhaleniu slabých miest v procesoch. Podstatou testu je uistenie o tom, že v prípade akejkoľvek krízovej situácie, plán bude fungovať korektne a efektívne a všetky aktivity budú obnovené v dopredu definovaných časoch a na dopredu definovanej minimálnej úrovni. Výsledky testovania musia byť vždy dokumentované a reportované manažérovi, prípadne vedeniu spoločnosti.

Z každého testu musí byť vytovorený písomný záznam, tzv. Protokol o testovaní. Protokol o testovaní musí dávať jasnú informáciu, aké aktivity sme testovali, akým spôsobom a aké sú závery testovania.

1.3.4. Continuity Requirement Analysis

CRA alebo Continuity Requirement Analysis je jednou z ďalších podporných aktivít, ktoré pomáhajú pri tvorbe a aktualizovaní krízových plánov. Definuje ako chceme zvolenú činnosť zabezpečiť – s kým, kde, čo k tomu potrebujeme, koho máme informovať atď.

1.3.5. Location Risk Assesment

LRA – Location Risk Assesment je ďalším z podporných nástrojov, pomozou ktorého analyzujeme prírodné nebezpečenstvá pre danú lokáciu. Pred vybudovaním Datacentra alebo novej pobočky spoločnosti by mali byť zohladnené všetky riziká vyplývajúce z prostredia v ktorom sa bude lokácia nachádzať. Ide napríklad o prírodné živly, politické a spoločenské hrozby a tak ďalej. Jedným zo zdrojov, z ktorého môžme pri tejto analýze vychádzť sú záznamy štatistických úradov.

1.4. Ďalšie dôležité pojmy

1.4.1. Aktívum

Aktíva sú všetky hmotné aj nehmotné statky, všetko, čo má pre majiteľa informačného systému istú hodnotu. Za najcennejšie aktíva sa považujú peniaze, majetok a predovšetkým dáta a informácie, ktorých zeužitie, strata alebo modifikácia by organizácií alebo osobe spôsobili určitú škodu (4, s. 37).

1.4.2. Bezpečnosť

Bezpečnosť IS je stupeň odolnosti Informačného systému proti udalostiam, ktoré môžu ohroziť dôvernosť, integritu alebo dostupnosť informácií (2).

1.4.3. Incident

Je prípad zlyhania bezpečnosti. Pre IS musí byť stanovené (najlepšie v bezpečnostných smerniciach) čo je považované v danom IS za Bezpečnostný incident a aké sú formálne procedúry jeho riešenia (2, s. 346).

1.4.4. Hrozba

Hrozbou označujeme skutočnosť, udalosť, silu alebo osoby, ktorých pôsobenie môže spôsobiť poškodenie, zničenie, stratu dôvery alebo hodnoty aktíva. Hrozba môže ohroziť bezpečnosť (4).

1.4.5. Riziko

Riziko je pravdepodobnosť, s akou bude daná hodnota aktíva zničená alebo poškodená pôsobením konkrétnej hrozby, ktorá pôsobí na slabú stránku tejto hodnoty. Je to miera ohrozenia konkrétneho aktíva (4).

1.4.6. Dopad

Dopad (Impact) je škoda, ktorú spôsobí hrozba pri jednom pôsobení na určité aktívum (2, s. 347).

1.5. Normy v oblasti BCDR

1.5.1. ISO/IEC 27000

ISO (International Organization for Standardization) rezervoavala sériu ISO 27000 pre normy z oblasit bezpečnosti informácií.

Podobne, ako tomu je pri normách pre riadenie kvality série ISO 9000. Na základe štandardu „ISO Guide 83“ publikovaného v apríli 2012, majú všetky štandardy rodiny 27K definovanú jednotnú štruktúru a pravidlá pre začlenenie špecifických požiadaviek (6).

1.5.2. ISO/IEC 27031

Medzinárodná norma z rady 27k ISO/IEC 27031:2011 *Information technology – Security techniques – Guidelines for information and communication technology readiness for business continuity* nahrádza stávajúci BS 2577:2008. Norma popisuje celkový koncept a jednotlivé princípy pripravenosti informačných a komunikačných technologií na mimoriadne udalosti.

Prevažná väčšina organizácií je na ICT doslova kriticky závislá. Prerušenie TI služieb je obvykle spojené so vznikom nedostupnosti Business procesov a taktiež najväčšími dopadmi na spoločnosť.

Norma je tak dobre využiteľná pri zavádzaní systému riadenie kontinuity činností – Business Continuity Management System (7).

1.5.3. ISO/IEC 22301

Business Continuity Management System. V tejto medzinárodnej norme sú špecifikované požiadavky na vytvorenie a riadenie účinného Systému managementu kontinuity podnikania (BCMS).

1.5.4. ISO/IEC 24762

Medzinárodná norma ISO/IEC 24762 *Information technology – Security techniques – Guidlines for information and communications technology disaster recovery servicers.*

Táto medzinárodná norma popisuje základné praktiky Disaster Recovery, ktoré by mal zohladniť každý poskytovateľ ICT. Pokrýva požiadavky, ktoré by mali splniť poskytovatelia služieb. Jednotlivé organizácie môžu mať ďalšie požiadavky, ktoré sú špecifické pre nich a mali by byť riešené v dohodách a zmluvách s poskytovateľmi služieb. Príklady takýchto požiadaviek organizácií môžu obsahovať napríklad špeciálny šifrovací software, vybavenie, skúsený personál a dokumentácku k aplikáciám.

Špecifické požiadavky ďalších organizácií sú obvykle predmetom dohody a podrobných rokovaní medzi organizáciami a ich poskytovateľmi DR ICT služieb a nie sú obsahom tejto medzinárodnej normy (9).

2. ANALÝZA SÚČASNÉHO STAVU

2.1. Základné údaje

Vzhľadom na citlivosť informácií, ktoré sú spracovávané v obsahovej časti tejto diplomovej práce, nemôžem uviesť pravý názov dotknutej banky. Názov banky teda ďalej ponechávam ako **TB Bank.**

- **Obchodný názov:** TB Bank
- **Právna forma:** Akciová spoločnosť
- **Sídlo:** Slovenská Republika
- **Počet zamestnancov:** 1 500

2.1.1. Popis spoločnosti

TB Bank, a.s. pôsobí na slovenskom trhu od roku 1993, kedy mala iba 2 pobočky a zamestnávala 45 zamestnancov. Ponúka široké spektrum služieb pre súkromnú aj podnikovú klientelu. V dnešnej dobe má po Slovenskej Republike 120 pobočiek a klientských centier. Okrem obsluhy klientov poskytuje služby špecializovaných hypotekárnych centier, osobných, firemných a podnikateľských poradcov. Za 20 rokov sa vyvinula v tretiu najväčšiu banku na slovenskom trhu.

TB Bank ponúka mnoho kvalitných služieb, vďaka ktorým získava veľa domácich i medzinárodných ocenení. Pravidelného ocenenia sa jej dostáva za kvality svojich služieb a poradenstva. Internetbanking, aplikácie a správa účtov cez smartphone je považovaný za najlepší na trhu.

Majoritným akcionárom je istá rakúska finančná inštitúcia, ktorá sa zameriava na poskytovanie služieb firemným a investičným klientom v Rakúsku a v rade zemí strednej a východnej Európy.

2.1.2. Produkty TB Bank, a.s.

TB poskytuje kvalitné služby súkromným osobám, podnikateľom, malým firmám a v neposlednej rade aj veľkým firmám a korporáciám.

Produkty pre občanov:

- Intrenetbanking,
- kreditné karty,
- pôžičky,
- hypotéky.

Produkty pre podnikateľov a malé firmy:

- Podnikateľské účty,
- zhodnotenie financií,
- financovanie.

Produkty pre firmy a korporácie:

- Transakčné bankovníctvo,
- zhodnocovanie finančných prostriedkov,
- financovanie,
- finančné a kapitálové trhy.

Každá z týchto služieb má veľký význam z hľadiska poskytovania kvality zákazníkom TB Bank. V dnešnej dobe je bankvníctvo úplne závislé na bezchybnom chode ICT technológií a výpadky napríklad na internetbankingu sú neprípustné. Každá minúta nefunkčnosti ICT technológie znamená pre banku obrovské náklady a škody.

Zavedenie Business Continuity and Disaster Recovery stratégie znižuje dopad rizík spôsobených či už živelnou pohromou, zlyhaním hardwaru/softwaru, ale aj úmyselným poškodením IT technológií alebo teroristickým útokom.

2.1.3. Súčasný stav BCDR stratégie

Globálne smernice spoločnosti špecifikujú štandard Business Continuity, Disaster Recovery a fyzickú bezpečnosť. Smernice sú vypracované v kontexte veľkých centralizovaných lokalít – „One size fits all".

Je plánovaný roll-out smerníc do všetkých organizačných jednotiek spoločnosti a je kladený dôraz na compliance a ochranu akcionárskej hodnoty. Nutnosť spracovania štandardu pre konkrétnu časť korporácie.

Adaptácia riešení musí rešpektovať kontext rizík a hodnotu zabezpečenia.

2.2. Kritická analýza

2.2.1. Analýza všeobecného okolia (SLEPT analýza)

Sociálne faktory – vzhľadom na zákazníkov a povahu činností sa medzi zákazníkov radia ľudia od 20 rokov. Nakoľko takmer každý zo zákazníkov využíva na správu svojho účtu internetbanking, alebo inú technológiu závislú na dostupnosti služieb pomocou internetu, je nevyhnutné nastaviť Business Continuity and Disaster Recovery stratégiu na čo najlepšej úrovni, aby nedochádzalo k výpadkom poskytovaných služieb a tým k nespokojnosti zákazníkov – stratám v banke. Ďalším, veľmi dôležitým prvkom, ktorý je životne dôležitý pre banku sú firmy a korporácie, ktoré využívajú ich bankové služby. Kritickým prvkom z hľadiska BCDR stratégie sú IT firmy, ktoré majú zavedenú svoju vlastnú BCDR stratégiu a požadujú úroveň BCDR stratégie minimálne takú, akú prevádzkujú oni samy.

Legislatívne faktory – nakoľko ide o spoločnosť pôsobiacu v Slovenskej Republike, musí TB Bank dodržiavať slovenskú legislatívu. Business Continuity and Disaster Recovery stratégia je v mnohých štátoch, prevažne USA, povinná pre všetky finančné inštitúcie

pôsobiace v danom štáte. Inštitúcie pôsobiace v týchto štátoch musia striktne dodržiavať štandardy a normy platné pre daný región. V najbližšej dobe môžeme očakávať požiadavky z Európskej Únie na zavedenie podobných stratégií chrániacich banky pred bankrotom alebo kritickou stratou. Zákon platný na území SR zatiaľ nepojednáva o zavedení BCDR stratégie v rámci kritickej infraštruktúry štátu, no v blízkej budúcnosti sa toto môže zmeniť.

Ekonomické faktory – v súčasnej dobe je veľký dopyt po hypotékach a úveroch, ktoré sú momentálne pomerne lacné a jednoducho dostupné. Z tohoto dôvodu je trend získavania nových klientov rastúci.

Politické faktory – vláda Slovenskej republiky môže byť označená ako stabilná a nie je očakávaná žiadna rapídna zmena vo forme vlády, ktorá by mohla negatívne či významne pozitívne ovplyvniť spoločnosť. Banky sú pre chod štátu podstatným a neoddeliteľným prvkom a sú štátom podporované.

Technologické faktory – bankovníctvo je v dnešnej dobe, ako to už bolo spomenuté vyššie v tejto práci, životne závislé na informačných technológiách a požiadavky od zákazníkov neustále rastú. Banka kontinuálne zdokonaluje a vyvýja vlastné technológie a snaží sa poskytovať zákazníkom čo najlepšie služby. Banka disponuje vlastnými datacentrami, no značná časť serverov je uložená aj v outsorcovanom datacentre spravovanom nemenovanou IT firmou, na ktorú budú kladené požiadavky pre prijatie štandardu Business Continuity and Disaster Recovery.

2.2.2. Analýza oborového okolia (Porterova analýza)

Stávajúca konkurencia – Spoločnosť má na slovenskom ale aj celosvetovom trhu pomerne veľa konkurentov, ktorý poskytujú podobné služby. Stále viac firiem požaduje od svojich bánk, aby mali zavedenú BCDR stratégiu, čo im zaručí minimálne straty pri katastrofe, ktorá postihne ich banku. Konkurenti s dobre vypracovanou a zákazníkovi prezentovanou Business Continuity and Disaster Recovery stratégiou sa dostávajú na trhu do výhody a môžu prebrať zákazníkov. Medzi hlavných a najsilnejších konkurentov patria banky spadajúce pod finančné inštitúcie Reiffeissen.

Nová konkurencia – nakoľko banka má na slovenskom trhu pomerne dobré a prezentované meno, vznik novej konkurencie priamo neohrozuje spoločnosť. Dôvodom je teda hlavne veľkosť spoločnosti, ktorá má vo svojich radoch mnoho zákazníkov a pomerne dobre sa jej darí si zákazníkov udržať. Spoločnosť má jeden z najprepracovanejších internet bankingov a aplikácie na vysokej úrovni, čo priťahuje hlavne mladých klientov, ktorým prístup k ich účtom pomocou smartphonov zjednodušuje ich správu. Vstup novej konkurencie je navyše regulovaný vládou Slovenskej republiky a nie je úplne jednoduchý. Ďalšou z bariér pre vstup na trh je potrebná infraštruktúra IT potrebná k vedeniu podobných služieb a s tým spojený vysoký vstupný kapitál.

Vplyv odberateľov – Spoločnosť má vysoký celkový počet zákazníkov, ktorých môžeme rozdeliť na malých (súkromných) klientov, stredných (firmy) a veľkých (korporácie) klientov. Malý a stredný klienti prevažne využívajú definované služby a nemajú ďalšie požiadavky na cenu poprípade navýšenie špecializovaných služieb a produktov a z dôvodu vysokého počtu podobných klientov nemajú veľký priestor pre vyjednávanie o cene. Veľký klienti majú naopak vysoký vplyv na chod banky aj ich požiadavky na dodávané produkty, služby a ceny sú špecifické. Z pohľadu stratégie BCDR požadujú nižšie až žiadne doby výpadkov poskytovaných služieb podľa kritikality aplikácií a služieb definovaných v zmluvách a SLAs. Spoločnosť má samozrejme strategicky klienta na prvom mieste a musí preto požiadavkám vyhovieť.

Vplyv dodávateľov – ako už bolo vyššie spomenuté, niektoré servery banky TB sú spravované dodávateľskou IT firmou v ich vlastnom datacentre, čiže infraštruktúra patrí dodávateľovi – z tohto dôvodu je potrebné aby dodávateľ mal vypracovanú stratégiu Businness Continuity and Disaster Recovery na úrovni minimálne ako TB Bank.

Substitučné produkty – V prípade Business Continuity and Disaster Recovery stratégie nemôžeme hovoriť o substitučnom produkte, pretože táto stratégia je natoľko špecifická, že nemôže byť nahradená ničím iným v rámci spoločnosti TB. Alternatívy pre zákazníkov teda existujú iba u konkurencie.

2.2.3. Analýza vnútorných faktorov (McKnisey 7s)

Stratégia – stratégia spoločnosti spočíva v zlepšovaní informačných technológií a poskytovaní čo najlepších informačných technológií zákazníkovi. Spoločnosť sa snaží ulahčiť prístup k správe účtu zákazníka no nezabúda ani na potrebné zabezpečenie aplikácií a dát, ktoré sú pre užívateľa kritické. Veľkou časťou stratégie je marketing smerovaný na mladých ľudí, prevažne študentov, usporiadavaním rôznych súťaží a propagácia prostredníctvom sociálnych sietí. Zabezpečenie informačných technológií je v dnešnej dobe v oblasti bankovníctva veľmi diskutovaná téma a každý zákazník chce mať svoje účty, peniaze a dáta pod kontrolou a v bezpečí. Z tohto dôvodu môžeme označiť zavedenie Businness Continuity and Disaster Recovery stretégia ako dobrý krok s ohľadom na predbehnutie konkurencie v oblasti bezpečnosti ICT.

Štruktúra – Spoločnosť má z globálneho hladiska predsedu a svoje predstavenstvo. Títo potom ďalej riadia jednotlivých manažérov divízií. Vo všeobecnosti však môžeme označiť štruktúru spoločnosti za líniovo-štábnu, kde je jeden útvar nadriadený druhému so špecializovanými pracovníkmi pre jednotlivé oblasti činností. Jeden útvar má viacero nadriadených.

Systémy – spoločnosť je životne odkázaná na informačné technológie. Procesy sú riadené metodológiou ITIL a podporované rôznymi internými špecializovanými systémami. Na rôznych úrovniach sú využívané odlišné systémy ako napríklad HR IS alebo systémy pre riadenie financií, či Change management systémy.

Štýl – riadenie spoločnosti je jasne definované organizačnou štruktúrou a tým pádom aj komunikácia medzi manažérmi a podriadenými, zákazníkmi či spolupracovníkmi. Efektívnosť vedenia spoločnosti je na vysokej úrovni. Rýchlosť rozhodovania je podmienená riešeným problémom, jeho dôležitosťou a rizikom, ktoré môže nastať po implementovaní rozhodnutia. Pracovné prostredie spoločnosti je príjemné, budovy prebehli v posledných rokoch re-designom dôležitým pre príjemn pocit v práci, čo je neoddeliteľnou podmienkou pre efektívnosť práce zamestnancov. Štýl riadenia môžeme

označiť za demokratický, nakoľko zamestnanci majú možnosť sa vyjadrovať na podnikovom rozhodovaní a prinášať vlastné nápady do produkcie.

Spolupracovníci – medzi spolupracovníkmi panuje prevažne priateľská nálada. Interná politika spoločnosti je taká, že si všetci navzájom tykajú, čo mnohí považujú za veľmi príjemné a priateľské prostredie. Zamestnanci majú svojich people managerov, ktorí sa starajú a pomáhajú im s ich personálnym rozvojom.

Schopnosti – pre spoločnosť je dôležité mať vo svojich radách skúsených a schopných pracovníkov, čo vedie samozrejme k tomu, že spoločnosť prepláca svojim zamestnancom rôzne školenia, certifikácie či kurzy.

Zdieľané hodnoty – podniková kultúra a etiketa odráže motto „Customer first“ a tomu sú podriadené aj zdieľané hodnoty. Spoločným cieľom je riešiť problém a poskytovať zákazníkom čo najlepší servis.

2.2.4. SWOT analýza

Silné stránky

- Silné postavenie na trhu
- Veľký počet zákazníkov
- Kvalita zamestnancov
- Jednotka na trhu v eBankingu

Slabé stránky

- Náklady spojené s prevádzkovaním IT infraštruktúry
- Komplikované interné procesy
- Náročná komunikácia so zákazníkom
- Zdĺhavé zavádzanie zmien a rozhodnutí
- Pôsobnosť iba na Slovensku

Príležitosti

- Expandovanie na zahraničné trhy
- Využitie nových komunikačných kanálov so zákazníkom
- Zefektívnenie interných procesov
- Spolupráca s veľkými IT spoločnosťami
- Zefektívnenie zavádzania zmien

Hrozby

- Konkurencia
- Ekonomická situácia
- Nedostatok kvalifikovaných záujemcov o voľné pozície

2.3. Návrh zmeny

Po posúdení všetkých prevedených analýz je zavedenie novej Business Continuity and Disaster Recovery stratégie považované za vhodnú zmenu. Táto zmena by mala po zavedení chrániť hlavné činnosti, procesy a zákazníkov spoločnosti po katastrofe. Stratégia sa zavádza na zníženie možných strát po nečakanej havárií s možným dopadom na spoločnosť.

2.3.1. Postup uskutočnenia zmeny

Pre úspečné zavedenie a uskutočnenie zmeny je nutné vykonať viacero činností, ktoré sú uvedené nižšie:

- Analýza rizikovosti oblasti – LRA (Location Risk Assesment)
- Analýza dopadov na business – BIA (Business Impact Analysis)
- Technická analýza infraštruktúry IT
- Vypracovanie plánu pre obnovu činností – BCP (Business Continuity Plan)
- Vypracovanie plánu obnovy infraštruktúry – DRP (Disaster Recovery Plan)
- Vypracovanie popisu obnovy jednotlivých serverov – DRD (Disaster Recovery Description)
- Testovanie plánov BCP a DRP
- Školenie zamestnancov
- Odsúhlasenie a distribuovanie plánov do produkcie

2.3.2. Lewinov model

Dôvod k zmene: spoločnosť je kriticky závislá od poskytovania služieb zákazníkom. Každá minúta výpadku poskytovaných služieb stojí banku veľký finančný obnos. Zavedenie Business Continuity and Disaster Recovery stretégie môže spoločnosti priniesť:

- Nižšiu dobu obnovy po katastrofe
- Nižšie náklady spojené s katastrofou
- Kratšie výpadky v poskytovaní služieb zákazníkovi
- Konkurenčnú výhodu
- Vyššiu dôveru od zákazníkov vzhľadom k poskytovaným službám

Agent zmeny: Agentom zmeny bude CISO – Chief Information Security Officer

Intervenčné oblasti: Zmena ovlplyvní všetky činnosti spoločnosti, primárne však team z oddelenia Security and Compliance, pretože oni budú zavádzať zmenu a udržiavať stratégiu aktuálnu. V prípade katastrofy sa však BCDR stratégia môže dotknúť ktorejkoľvek časti spoločnosti a tak každý zo zamestnancov musí byť preškolený vzhľadom k stratégii.

Zhodnotenie zmeny: zmena zníži náklady po dopade neočakávanej situácie na spoločnosť. Zavedená stratégia umožní obnovenie poskytovania služieb zákazníkom v pomerne krátkom čase po havárií. Ďalším, nie menej dôležitým, faktom je že mnohé IT firmy, ktorí sú potencionálnymi zákazníkmi, vyžadujú od svojich dodávateľov funkčnú Business Continuity and Disaster Recovery stratégiu pre urdžanie svojich peňazí a prístupu k svojim bankovým produktom pod kontrolou s maximálnou dostupnosťou.

Časový a obsahový harmonogram: nasledujúca tabuľka charakterizuje časový a obsahový harmonogram zmeny a obsahuje:

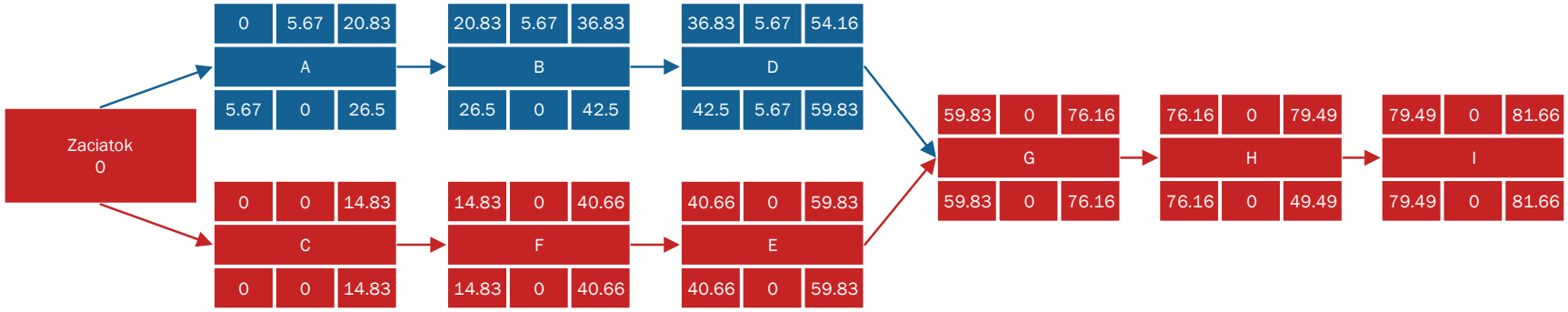
- Špecifikáciu činností
- Odhad doby trvania činností (pre metódu sieťovej analýzy PERT), kde:
  - a = optimistický odhad
  - m = normálny odhad
  - b = pesimistický odhad
- Postuponosť samotných činností (odhady trvaní sú udané v pracovných dňoch)

ID	Činnosť	Nasled.	Odhad doby trvania			Očakávaná doba trvania	Rozptyl	Smerodatná odchýlka
			a	m	b			
A	Analýza	B	10	20	35	20.83	17.361	4.167
B	Analýza	D	6	15	30	16.00	16	4
C	Analýza	F	8	14	25	14.83	8.028	2.833
D	Vypraco	G	10	16	30	17.33	11.111	3.333
E	Vypraco	G	11	18	32	19.17	12.25	3.5
F	Vypraco	E	15	25	40	25.83	17.361	4.167
G	Testovan	H	10	16	24	16.33	5.444	2.333
H	Školenie	I	2	3	6	3.33	0.444	0.667
I	Nasadeni		1	2	4	2.17	0.25	0.5

Tabuľka č.2.: Činnosti a doba trvania

(Zdroj: vlastné spracovanie)

Sieťový graf

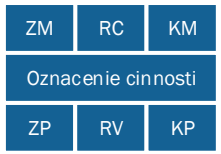


Obrázok č.6.: Sieťový graf

(Zdroj: vlastné spracovanie)

Činnosti C, F, E, G, H, I ležia na kritickej ceste, čo je vyznačené v grafe červenou farbou. Pre tieto činnosti neexistujú žiadne časové rezervy a je nutné sledovať priebeh projektu a dbať na ich včasné dokončenie. Omeškanie niektorej z týchto činností by malo vplyv na včasné dokončenie a dodržanie termínu projektu.

Celková doba trvania projektu je predpokladaná na **82 pracovných dní.**



ZM = Začiatok možný KP = Koniec prípustný

RC = Rezerva celková KM = Koniec možný

RV = Rezerva voľná ZP = Začiatok prípustný

2.4. Analýza rizík projektu

Pre analýzu rizík zavedenia projetku som si zvolil metódu RIPRAN.

2.4.1. Identifikácia rizík

Nižšie sú uvedené riziká, ktoré môžu ohrozovať projekt:

- Nízke skúsenosti zamestnancov so zavádzaním stratégie BCDR
- Neochota tímov poskytnúť informácie dôležité k vytvoreniu plánov
- Nedodržanie interných procesov
- Odchýlenie sa od globálneho štandardu spoločnosti
- Slabá podpora od vedenia spoločnosti
- Nezáujem zamestnancov vytvoriť si povedomie o BCDR
- Chyby v plánoch BCP a DRP
- Zle prevedená analýza BIA
- Zle prevedená analýza LRA
- Nedostatočné informácie pre ananlýzu infraštruktúry ICT

2.4.2. Hodnotenie rizík

Hodnoty pravdepodobnosti a dopadu sú definované v nasledujúcich tabuľkách

Hodnoty pravdepodobnosti:

Pravdepodobnosť	Hodnota	Definícia
Nízka	0.00 – 0.33	0% až 33%
Stredná	0.34 – 0.66	34% až 66%
Vysoká	0.67 – 1.00	67% až 100%

Tabuľka č.3.: Hodnoty pravdepodobnosti

(Zdroj: vlastné spracovanie)

Hodnoty dopadu:

Dopad	Hodnota	Popis
Malý	1	do 15 dní; do 5% rozpočtu
Stredný	2	od 16 do 30 dní; od 5% do
Vysoký	3	nad 31 dní; nad 20% rozpočtu

Tabuľka č.4.: Hodnoty dopadu

(Zdroj: vlastné spracovanie)

Hodnoty rizika:

Hodnota rizika		Pravdepodobnosť		
		0.00 – 0.33	0.34 – 0.66	0.67 – 1.00
Dopad	1	Bežná	Bežná	Závažná
	2	Bežná	Závažná	Kritická
	3	Závažná	Kritická	Kritická

Tabuľka č.5.: Hodnoty rizika

(Zdroj: vlastné spracovanie)

Násobkom pravdepodobnosti a hodnoty dopadu dostávame hodnotu rizika uvedenú v tabuľke č.4.

2.4.3. Analýza rizík

Riziko	Scenár	Pst.	Dopad	Hod.	Opatrenie
Nízke skúsenosti zamestnancov so zavádzaním stratégie BCDR	Neefektívna stratégia BCDR	Stredná	Vysoký	**Kritická**	Školenie zamestnancov
Neochota tímov poskytnúť informácie dôležité k vytvoreniu	Plány nebudú odrážať skutočnosť a nebudú použiteľné	Vysoká	Stredný	**Kritická**	Prezentácia zámeru stratégie a poukázanie na dôležitosť
Nedodržanie interných procesov	Zdržanie implementácie	Stredná	Vysoký	**Kritická**	Analýza procesov spoločnosti
Odchýlenie sa od globálneho štandardu spoločnosti	Stratégia neschválená vedením spoločnosti	Nízka	Stredný	**Bežná**	Interné školenie zamestnancov
Slabá podpora od vedenia spoločnosti	Zdržanie zavedenia stratégie	Stredná	Malý	**Bežná**	Prezentácia projektu
Nezáujem zamestnancov vytvoriť si povedomie o BCDR	Zamestnanci nevedia ako použiť plány v prípade havárie	Nízka	Stredný	**Bežná**	Pravidelné prezentácie a školenia v oblasti BCDR
Chyby v plánoch BCP a DRP	Neefektívna obnova po haváriі	Stredná	Vysoký	**Kritická**	Školenie a dvojitá kontrola
Zle prevedená analýza BIA	Stratégia skreslená zlými inf.	Nízka	Stredný	**Bežná**	Postup podľa všeob.
Zle prevedená analýza LRA	Stratégia skreslená zlámi inf.	Stredná	Malý	**Bežná**	Vypracovanie špec. tímom
Nedostatočné informácie pre ananlýzu infraštruktúry ICT	DRD dokumenty neobsahujú potrebné informácie	Vysoká	Vysoký	**Kritická**	Vyžiadanie dokumentácie od vedenia spoločnosti

Tabuľka č.6.: Analýza rizík

(Zdroj: vlastné spracovanie)

2.4.4. Opatrenia

Jednotlivé opatrenia boli navrhnuté pre každé riziko, čo spôsoilo zníženie hodnôt rizík a to z veľkej časti znížením pravdepodobností. Každé z opatrení si vyžaduje určité náklady, ako je znázornené v nasledujúcej tabuľke.

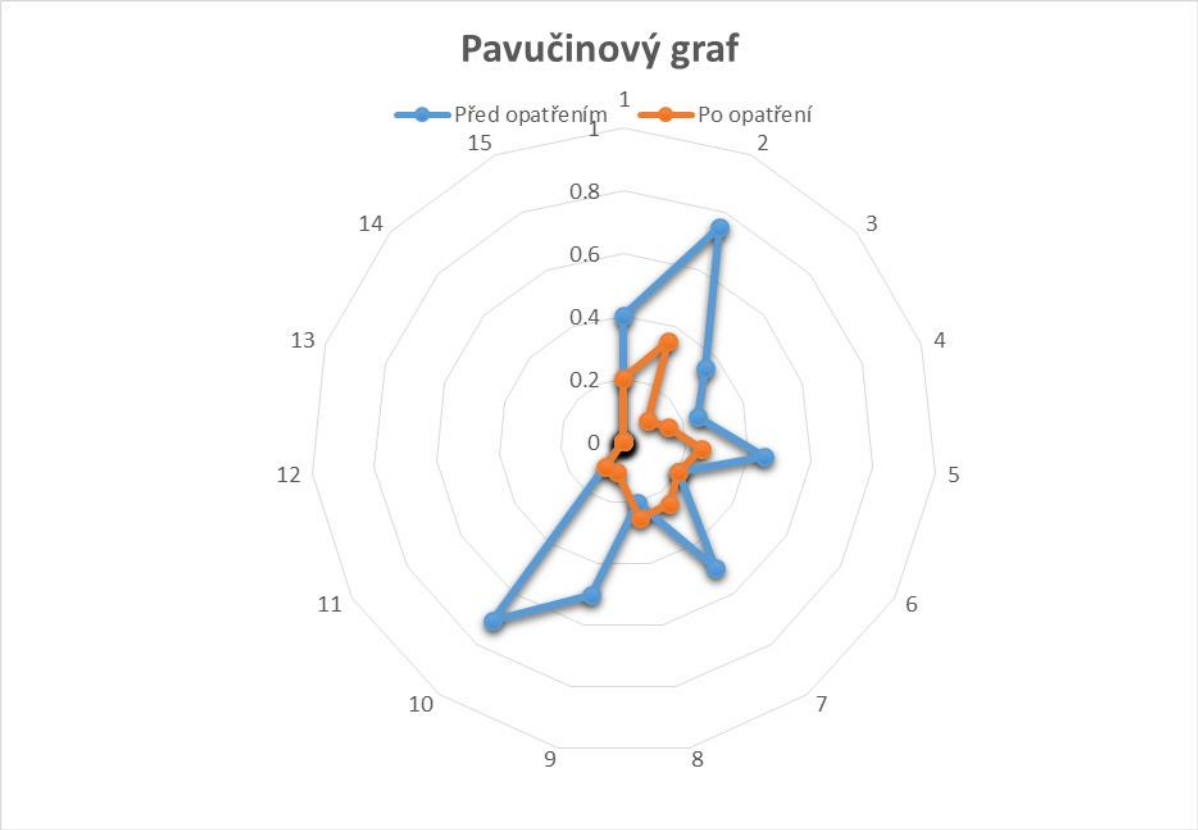
Riziko	Náklady	Opatrenia	Pst.	Dopad	Hodnota
Nízke skúsenosti zamestnancov so zavádzaním stratégie	25 000 Kč	Školenie zamestnancov	Nízka	Vysoký	**Závažná**
Neochota tímov poskytnúť informácie dôležité k vytvoreniu plánov	15 000 Kč	Prezentácia zámeru stratégie a poukázanie na dôležitosť projektu	Stredná	Stredný	**Závažná**
Nedodržanie interných procesov	20 000 Kč	Analýza procesov spoločnosti	Nízka	Výsoký	**Závažná**
Odchýlenie sa od globálneho štandardu	22 500 Kč	Interné školenie zamestnancov	Nízka	Stredný	**Bežná**
Slabá podpora od vedenia spoločnosti	12 000 Kč	Prezentácia projektu	Nízka	Malý	**Bežná**
Nezáujem zamestnancov vytvoriť si povedomie o BCDR	0 Kč	Pravidelné prezentácie a školenia v oblasti BCDR	Nízka	Stredný	**Bežná**
Chyby v plánoch BCP a DRP	30 000 Kč	Školenie a dvojitá kontrola	Nízka	Vysoká	**Závažná**
Zle prevedená analýza BIA	0 Kč	Postup podľa všeob. metodologie	Nízka	Stredný	**Bežná**
Zle prevedená analýza	12 000 Kč	Vypracovanie špec.	Nízka	Malý	**Bežná**
Nedostatočné informácie pre ananlýzu infraštruktúry	0 Kč	Vyžiadanie dokumentácie od	Nízka	Vysoký	**Závažná**

Tabuľka č.7.: Opatrenia

(Zdroj: vlastné spracovanie)

2.4.5. Pavučinový graf

Na pavučinovom grafe môžeme veľmi dobre sledovať zmenu hodnôť pravdepodobností, ktorá bola spôsobená zavedením opatrení k jednotlivým rizikám. Ako vidíme z grafu, pravdepodobnosti jednotlivých rizík sa znížili, čiže zavedené opatrenia boli efektívne.

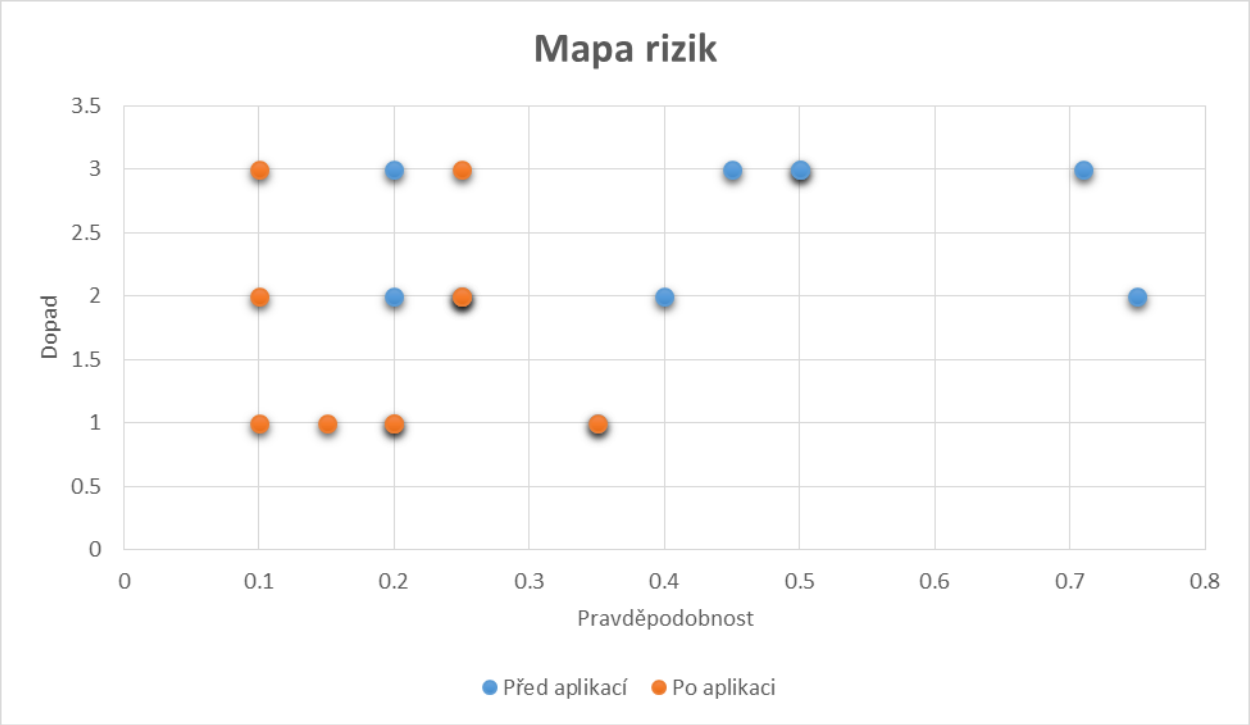


Obrázok č.7.: Pavučinový graf

(Zdroj: vlastné spracovanie)

2.4.6. Mapa rizík

Mapa rizík projektu reflektuje stav pred aplikáciou proiopatrení a po ich zavedení. Na grafe môžeme pozorovať posun hodnôt rizika vplyvom zníženia pravdepodobností, čo je znázornené posunutím bodov vľavo. Aj tento graf nám ukazuje, že zavedené riziká boli efektívne.



Obrázok č.8.: Mapa rizík

(Zdroj: vlastné spracovanie)

2.5. Zhodnotenie zmeny

Zavedením Business Continuity and Disaster Recovery Stratégie si spoločnosť chráni vlastný majetok, aktíva, zákazníkov a finančné prostriedy po určitej katastrofe, alebo havárií. Udržanie alebo znovuobnovenie procesov a poskytovania služieb po neočakávanej udalosti je v prípade banky nesmierne dôležité a najbližšie hodiny po katastrofe ukážu aké veľké budú škody. Stratégia Business Continuity and Disaster Recovery je veľmi ťažko zhodnotiteľná kým sa nedostane do reálneho prostreda po udalosti, ktorá si vyžiada jej spustenie. Testovanie tejto stratégie by malo byť na každoročnej úrovni a preverovanie plánov kontinuity činností a plánov obnovy po havárií by malo čo najviac reflektovať reálnu situáciu. Týmto testovaním dokáže spoločnosť aspom do istej miery zhodnotiť efektivitu zavedenej stratégie a tým ju naďalej zlepšovať.

Doba implementácie tejto stratégie je odhadovaná na 82 pracovných dní. Ako nám odhalila analýza rizík, projekt je ohrozený viacerými rizikami na ktoré boli navrhnuté opatrenia. Opatrenia boli navrhnuté k zníženiu pôsobenia rizík. Náklady na tieto opatrenia sú 136 500 Kč čo je v porovnaní s rozsahom a veľkosťou daného projektu prijateľné. Po zhodnotení je teda odporúčané pristúpiť k zmene.

3. VLASTNÉ NÁVRHY RIEŠENÍ

3.1. Location Risk Assessment

Hodnotenie rizika lokality, alebo LRA sa skladá z rizík, ktoré môžeme zaradiť do nasledujúcich piatich skupín : Riziká spojené s budovou, politické riziká, prírodné riziká, riziká spojené s infraštruktúrou a riziko zločinnosti v danej lokalite. Hodnoty daných rizík sú vypĺňané do vopred definovaného formuláru.

3.1.1. Riziká spojené s budovou

Číslo	Definícia	Odpoveď
1	**Je TB Bank jediným nájomcom v budove?**	ANO
2	**Sú všetky prvky TB Bank situované v danej budove?**	NIE
3	**Je kancelária vedenia TB Bank situovaná v danej budove?**	ANO
4	**Je kancelária dozornej rady TB Bank situovaná v budove?**	ANO
5	**Je umiestnená v obchodnom centre krajiny?**	ANO
6	**Sú v tejto budove umiestnené významné aktíva?**	-
	• Akciové certifikáty	NIE
	• Citlivé dokumenty	ANO
	• Hotovosť banky	NIE
7	**Sú v budove umiestnené kritické systémy?**	-
	• Server rooms	ANO
	• Data centers	NIE
8	**Má budova bezpečnostné opatrenia?**	-
	• Alarm	ANO
	• Systém kontroly fyzického prístupu	ANO
	• Bezpečnostná služba	ANO
9	**Sú bezpečnostné opatrenia monitorované z kontrolnej miestnosti?**	ANO
10	**Funguje kontrolná miestnosť 24/7?**	ANO
11	**Má budova vlastný diesel generator?**	ANO
12	**Má budova alternatívnu lokáciu v prípade aktivovania BCP?**	ANO
13	**Ako ďaleko je alternatívna lokácia od primárnej?**	viac ako 50 km

Tabuľka č.8.: LRA - Riziká spojené s budovou

(Zdroj: vlastné spracovanie)

3.1.2. Politické riziká

Číslo	Definícia	Odpoveď
1	**Boli v danej lokalite demonštrácie alebo nepokoje v posledných 2**	-
	• Verejný protest	ANO
	• Vojenský prevrat	NIE
	• Priemyselný protest	NIE
2	**Bol v danej lokalite vojenský konflikt v posledných dvoch rokoch?**	NIE
3	**Sú v lokalite známe teroristické skupiny?**	NIE

Tabuľka č.9.: LRA – Politické riziká

(Zdroj: vlastné spracovanie)

3.1.3. Prírodné riziká

Číslo	Definícia	Odpoveď
1	**Aká je frekvencia prírodných katastrof za posledných 20 rokov?**	-
	Tornado/Hurikán	Nikdy
	Zemetrasenie/Vulkanická činnosť	Nikdy
	Požiar	Nikdy
	Povodeň	1 až 2 krát
	Snehová búrka	1 až 2 krát
2	**Aká je frekvencia katastrof spôsobená človekom za posledných 5**	-
	Chemické znečistenie	Nikdy
	Nukleárna katastrofa	Nikdy
	Epidémia	Nikdy
	Znečistenie vzduchu	Nikdy

Tabuľka č.10.: LRA – Prírodné riziká

(Zdroj: vlastné spracovanie)

3.1.4. Riziká spojené s infraštruktúrou

Číslo	Definícia	Odpoveď
1	**Aká je frekvencia výpadkov za posledných 5 rokov?**	-
	Elektrická energia	Nikdy
	Plyn / dodávky pitnej vody	Nikdy
	Telekomunikačné systémy	Nikdy
	IT infraštruktúra	Nikdy
	Doprava	Nikdy

Tabuľka č.11.: LRA – Riziká spojené s infraštruktúrou

(Zdroj: vlastné spracovanie)

3.1.5. Riziko zločinnosti

Riziko zločinnosti je vypĺňané formou dotazníku, v ktorom môže hodnota jednotlivých rizík nadobudnúť možnosti: „žiadne“ - „slabé“ - „stredné“ - „silné“.

Číslo	Definícia	Odpoveď
1	**Miera rizika zločineckých aktivít v danej lokalite**	-
	• Organizovaný zločin	Slabé
	• Gangy	Slabé
	• Individuálny kriminálnici	Slabé
2	**Miera rizika nasledujúcich typov zločinov:**	-
	Krádeže	Stredné
	Ozbrojená lúpež	Slabé
	Vandalizmus	Stredné
	Vražda	Slabé
	Podpaľačstvo	Slabé

Tabuľka č.12.: LRA – Riziko zločinnosti

(Zdroj: vlastné spracovanie)

3.1.6. Zhodnotenie LRA

Z uvedených analýz vyplýva, že budova v danej lokalite môže byť ohodnotená ako nízko riziková bez veľkého vplyvu na stratu majetku, dobrú povesť kontinuity podnikania, avšak v kombinácií s inými rizikami môže dôjsť k určitému nebezpečenstvu.

3.2. Business Impact Analysis

Analýza dopadov na podnikateľské funkcie Business Impact Analysis patrí medzi najdôležitejšie etapy v procese riadenie kontinuity činností a z nej vychádza tvorba plánov. Je cieľom je identifikovať kritické procesy v organizácií a určiť dopady nedostupnosti týchto procesov v prípade straty, narušenia alebo prerušenia týchto procesov.

3.2.1. Proces BIA podľa ISO/IEC 22301:2012

Proces BIA sa môže v každej organizácií líšiť avšak mojim návrhom je postupovať podľa **štandardu BS 25999-2.** Týmto štandardom budú dosiahnuté všetky nutné podmienky pre analýzu BIA a identifikované všetky kritické prvky zasahujúce do plánovania riadenia kontinuity činností.

Bod	Kontrolný list požiadaviek
I.	Mala by byť jasne definovaná a zdokumentovaná vhodná metóda pre stanovanie dopadu prerušenia činností, ktoré podporujú dodávku kľúčových produktov a služieb organizácie.
II.	Organizácia by mala:
	A) Identifikovať činnosti, ktoré sú kritické pre jej kľúčové činnosti a služby
	B) Identifikovať dopady, vyplývajúce z výpadkov činností a určiť vývoj v čase
	C) Stanoviť max. akceptovateľnú dobu výpadku pre každú aktivitu a to:
	• Maximálny časová horizont, v ktorom je schopná akceptovať výpadok aktivity
	• Minimálnu úroveň funkčnosti aktivity potom, čo je po prerušení obnovená
	• Časový horizont po obnovení aktivity na bežnú úroveň
	D) Stanoviť priority pre obnovu činností a identifikovať kritické činnosti
	E) Identifikovať závislosti, ktoré sa vzťahujú ku kritickým činnostiam, vrátane dodávateľských a ďalších vzťahov
	F) Stanoviť príslušné BCM opatrenia pre kritické činnosti na strane dodávateľov
	G) Určiť RTO pre výpadok kritických činností
	H) Odhadnúť zdroje potrebné pre obnovu kritickej činnosti

Tabuľka č.13.: Proces BIA

(Zdroj: 12)

3.2.2. Postup tvorby BIA

Postup tvorby BIA môže byť realizovaný viacerými spôsobmi, avšak ak sa rozhodneme pre jeden konkrétny, tak všetky prvky musia byť analyzované práve týmto konkrétnym.

Rôzne prístupy k BIA:

- Spracovanie u procesov (prierezové)
- Spracovanie u organizačných jednotiek (samostatná zodpovednosť, podieľ na procesoch a službách)
- Spracovanie BIA na strategickej, taktickej a operačnej úrovni

Pre potreby analyzovanej spoločnosti odporúčam použiť metódu **spracovania u organizačných jednotiek**, nakoľko umožňnuje lepšiu interakciu so zamestnancami a nahliadnutie do samotných procesov, čo je veľmi dôležité pri prevádzaní analýzi BIA.

Metódy a techniky vedenia BIA – najčastejšími formami vedenia BIA sú dotazníky, semináre alebo rozhovory. Každá z týchto metód má svoje výhody i nevýhody zobrazené v nasledujúcej tabulke:

Metóda	Výhody	Nevýhody
Dotazník	- Časovo nenáročné - Možnosť komparácie výsledkov	- Chýba interakcia - Možnosť nepochopenia otázok - Riziko nízkej návratnosti výstupov
Seminár	- Bezprostredná reakcia (feedback) - Možnosť diskusie (brainstorming)	- Chýba individuálny prístup
Rozhovor	- Veľká vypovedajúca schopnosť výst. - Individuálny prístup, priamy kontakt	- Časová náročnosť - Chýba previazanosť s ostatnými BIA

Tabuľka č.14.: Techniky vedenia BIA

(Zdroj: vlastné spracovanie)

S prihliadnutím na uvedené výhody/nevýhody a zo skúsenosti navrhujem pri analýze BIA použiť kombináciu postupov formou **elektonického dotazníku s následným individuálnym rozhovorom,** čo umožní získať relevantné informácia a vyjasní prípadné nepochopené otázky v dotaníku.

Účastníci procesu BIA sú zodpovedný za relevantnosť informácií a spracovanie analýzy v danom čase a kvalite. Navrhujem rozdeliť účastníkov do troch skupín s rôznymi požiadavkami:

A) **Spracovateľ –** vlastník procesu – zodpovedá za zhromaždenie a vyhodnotenie potrebných dát, kvalifikovaný odhad dopadu výpadkov, aplikáciu získaných výstupov do plánov BCM a aktualicázií BIA – **BC koordinator**

B) **Dodávateľ** – podpora procesu – spolupracuje so spracovateľom na častiach analýzy, týkajúcich sa podporných procesov a možných dopadov

C) **Koordinátor –** manažér BCM – metodická spolupráca a riadenie BIA

Dátum	**Verzia**		**Útvar/proces/služba**		**Názov dokumentu**
1.4.2017	1.0		Help desk		BIA dotazník
Spracovateľ					
Meno	Meno vlastníka procesu				
Pozícia	TL Help desk team				
Kontakt	Mobil, email, sekretariát				
BCM koordinácia					
Meno	Meno koordinatora				
Pozícia	BCM manager				
Kontakt	Mobil, email, sekretariát				
Definujte					
MTPD			Alternatívna lokácia:		
MTO			Počet členov teamu:		
RTO					
RPO					
Zoznam členov teamu:					
Meno	Pozícia	Mobil	Email	Manager	Laptop Y/N

Obrázok č.9.: Príklad dotazníku BIA

(Zdroj: vlastné spracovanie)

Elektornický dotazník môže mať rôzne formy no z hľadiska prehľadnosti a následnej jednoduchosti práce s informáciami navrhujem použiť dokument vo formáte .xls.

Hodnotenie dopadov je nasledujúcim krokom po získaní informácií prostredníctvom dotazníkov a interakcii s vlastníkmi procesov. Hodnotenie dopadov navrhujem rozdeliť do nasledujúcich podoblastí a prideliť ku každej časti relevantné skóre. Skóre môže nadobúdať hodnoty: nízky dopad/stredný dopad/vysoký dopad.

Dopad na konkrétnu činnosť	**Skóre**			
Reputačný dopad	**(0 až 24h>**	**(24 až 72h>**	**(3 až 5 dní>**	**viac ako 5**
Sťažnosti klientov na zákaznícku linku, správa v regionálnych/celoštátnych	skóre	skóre	skóre	skóre
Finančný dopad	**(0 až 24h>**	**(24 až 72h>**	**(3 až 5 dní>**	**viac ako 5**
% možnej straty na zisku, penále, sankcie, priame škody	skóre	skóre	skóre	skóre
Právny dopad	**(0 až 24h>**	**(24 až 72h>**	**(3 až 5 dní>**	**viac ako 5**
Porušenie zmluvných podmienok, súdne spory, odobratie licencie...	skóre	skóre	skóre	skóre
Dopad na bezpečnosť	**(0 až 24h>**	**(24 až 72h>**	**(3 až 5 dní>**	**viac ako 5**
Priame i nepriame dopady na bezpečnosť zamestnancov, klientov	skóre	skóre	skóre	skóre
Dopad na klientov	**(0 až 24h>**	**(24 až 72h>**	**(3 až 5 dní>**	**viac ako 5**
Obmedzenie služieb pre interných	skóre	skóre	skóre	skóre
Ďalšie dopady	**(0 až 24h>**	**(24 až 72h>**	**(3 až 5 dní>**	**viac ako 5**
napr. ohrozenie životného prostredia	skóre	skóre	skóre	skóre

Tabuľka č.15.: Hodnotenie dopadov

(Zdroj: vlastné spracovanie)

Zdroje pre zaistenie kontinuity činností sú ďalším objektom analýz. Je možné ich identifikovať a ohodnotiť pomocou skóre podobne ako dopady.

Zdroje pre konkrétenu činnosť	**Skóre**			
Alternatívna lokácia	**(0 až 24h>**	**(24 až 72h>**	**(3 až 5 dní>**	**viac ako 5**
Home office, iná kapacita...	skóre	skóre	skóre	skóre
Ľudia a schopnosti	**(0 až 24h>**	**(24 až 72h>**	**(3 až 5 dní>**	**viac ako 5**
Know-how, kapacity, zodpovednosť...	skóre	skóre	skóre	skóre
ICT	**(0 až 24h>**	**(24 až 72h>**	**(3 až 5 dní>**	**viac ako 5**
HW, mobily, linky...	skóre	skóre	skóre	skóre
Aplikácie a systémy	**(0 až 24h>**	**(24 až 72h>**	**(3 až 5 dní>**	**viac ako 5**
	skóre	skóre	skóre	skóre
Dáta	**(0 až 24h>**	**(24 až 72h>**	**(3 až 5 dní>**	**viac ako 5**
	skóre	skóre	skóre	skóre

Tabuľka č.16.: Zdroje pre zaistenie BC

(Zdroj: vlastné spracovanie)

3.2.3. Výstup analýzy BIA

Výstupom analýzy BIA bude záverečná práca spracovaná BC koordinátorom a schválená BC managerom. Doporučujem pre výstupný dokument zvoliť formát .pdf, ktorý musí obsahovať:

- Zámer a ciele BIA
- Identifikáciu kritických procesov vrátane kľúčových vstupov a výstupov
- Možné dopady zapríčinené výpadkom
- Doporučený postup pri obnove vrátane časov
- Minimálnu úroveň a štruktúru zdrojov pre obnovu kritického procesu na tolerovateľnej úrovni vrátane spôsobov jeho zistenia a vytvorenia rezerv
- Stanovenie RTO – doby, v ktorej musí byť kritický proces obnovený na minimálnej úrovni

Skupina procesov	2h	2 - 12h	12 - 48h	48 plus h
Tuzemský platobný styk	0%	50%	100%	100%
Zahraničný platobný styk	0%	0%	100%	100%
Čerpanie úveru	0%	0%	50%	100%
Trading	50%	100%	100%	100%

Tabuľka č.17.: Ukážka RTO vo vybraných procesoch

(Zdroj: vlastné spracovanie)

Aktualizácia analýzy dopadov na podnikanie je kontinuálny a nikdy nekončiaci proces, ktorý je nutný pre udržiavanie plánov kontinuity činností aktuálnych a s relevantnými informáciami. Navrhujem preto aktualizovať BIA vždy keď:

- Je stanovený cyklus aktualizácií – daný na jeden rok
- Dôjde k podstatnej zmene vstupných podmienok
- Dôjde k podstatnej zmene procesu samotného
- Zmení sa legislatívn úprava s dopadom na proces
- Je identifikovaný nový proces, ktorá je vyhodnotený ako kritický
- Dôjde k mimoriadnej udalosti a v jej dôsledku organizácia utrpí stratu prevyšujúcu dopady predpokladané na základe BIA

3.3. Analýza infraštruktúry IT

3.3.1. Data Centrum

Banka disponuje dvomi datacentrami certifikovanými úrovňou **TIER III.** Datacentrum klasifikované touto úrovňou je vybavené záložným bezpečnostným systémom, resp. plne redundantným napájaním a chladením. Maximálny možný povolený výpadok nesmie presiahnuť ročne 1,6 hodiny, čiže dostupnosť datacentra je na úrovni 99,98%. Datacentrum je vybavené štandardom N+1, teda existencia najmenej jednej nezávislej zálohy nad nutný počet použitých komponentov.

Datacentrá sú lokalizované v dvoch rôznych lokalitách s dostatočnou vzdialenosťou aby dosahovali certifikácie.

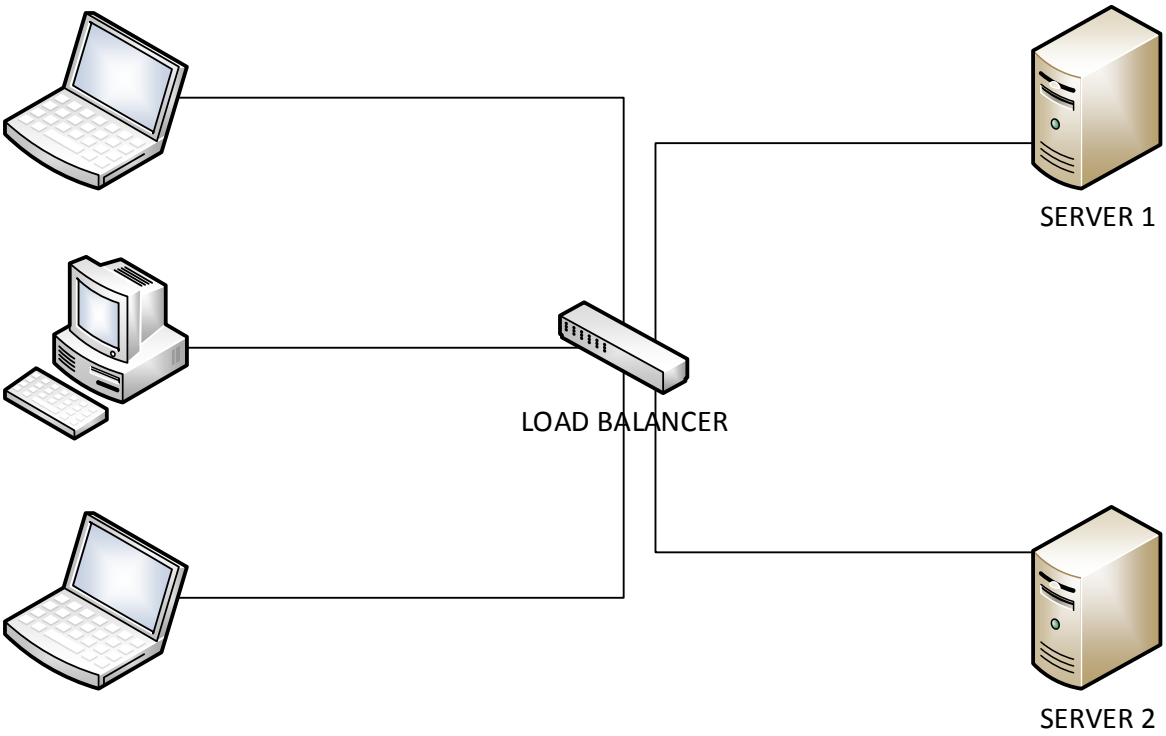
3.3.2. Klasifikácia serverov

Stand-alone servery – prvým z typov serverov pod správou banky sú stand-alone servery. Tieto servery bežia samostatne a nie sú súčasťou žiadnej skupiny (cluster). Na týchto serveroch by nemali bežať žiadne dôležité či kritické aplikácie, nakoľko server nemá vlastnú repliky ani DR kapabilitu a v prípade poruchy neexistuje záložné riešenie. Navrhujem tieto servery využívať na aplikácií vo vývoji a na testovanie vývojármi.

Cluster – ďalším typom serverov sú clustery, skupiny počítačov vystupujúcich navonok ako jeden systém. Clustery sú nasadzované pre zvýšenie rýchlosti a spoľahlivosti s väčšou efektivitou. Navrhujem využívať clustery pre aplikácie s vysokou kritikalitou a vypracovať DR plány pre obnovu služieb na týchto serveroch.

High-availability clusters – používané pre kritické databázy, zdielanie kritických dokumentov, aplikácie kritické pre business a klientské služby ako napríklad internet banking. Tieto clustery využívajú SW s vysokou dostupnosťou, ktorý dokáže využiť redundantné komponenty v clustery a poskytuje neprerušené služby aj pri výpadku systémových komponentov. Tieto servery je nutné zahrnúť do Disaster Recovery plánov a popísať v nich dôležité funkcie systému a správne prevedenie FAILOVER fáze.

ACTIVE – ACTIVE HA cluster – High availability cluster, ktorý je zapojený v móde active – active je typicky zložený z najmenej dvoch serverov, ktoré aktívne spravujú jeden druh služby simultánne. Hlavným cieľom takéhoto typu serveu je zaistenie vyrovnania záťaže tzv. Load balancing.

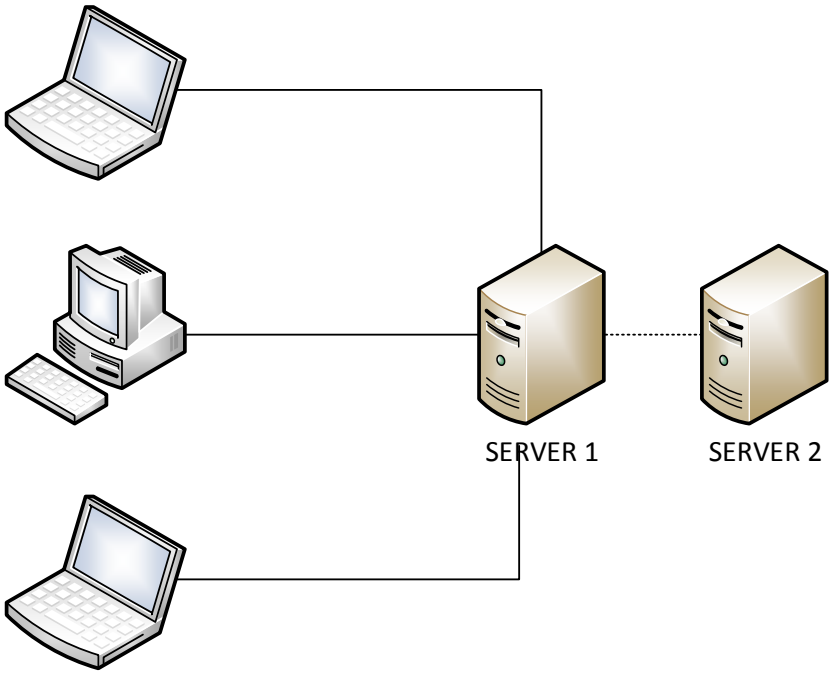


Obrázok č.10.:Active-Active HA cluster

(Zdroj: vlastné spracovanie)

ACTIVE – PASIVE HA cluster

Podobne ako v predchádzajúcom zapojení, active – pasive móde pozostáva z najmenej dvoch serverov. Tieto servery však nie sú aktívne simultánne. V prípade dvoch serverov v clustery, ak je prvý server aktívny, druhú musí byť pasívny alebo stand-by. Pasívny server nazývaný aj „failover“ musí byť pripravený prevziať všetku záťaž v prípade nedostupnosti primárneho serveru. Toto všetko musí byť dokumentované a testované na základe Disaster Recovery plánov a Disaster Recovery popisu danej technológie.



Obrázok č.11.: Active – Pasive HA cluster

(Zdroj: vlastné spracovanie)

3.3.3. Klasifikácia aplikácií

Banka spravuje veľké množstvo aplikácií, ktoré sú menej či viac potrebné pre business a majú rôzne povolené časy výpadkov, čiže dostupnosť. Navrhujem na základe dostupnosti aplikácií navrhnúť ich kritikalitu na stupnici „Nízka“ – „Stredná“ – „Vysoká“ a následne podľa toho vytvoriť Disater Recovery plány s ohľadom na technológiu na ktorej aplikácie bežia.

System name	Criticality	Owner	RTO	Location
Datawarehouse and Business Intelligence app.	Medium	#name	24 h	DC1
Credit & Current Accounts	High	#name	2 h	DC2
International Payments	Medium	#name	24 h	DC2
Customer Reporting	Low	#name	48 h	DC1
Domestic Payments	High	#name	2 h	DC1
Loans	Medium	#name	24 h	DC2
Management Information System	Medium	#name	24 h	DC1

Tabuľka č.18.: Príklad klasifikácie aplikácií

(Zdroj: vlastné spracovanie)

3.4. Business Continuity Plán

Business Continuity plán musí byť vypracovaný pre všetky aktivity, ktoré boli definované v BIA, vrátane outsourcovaných, so stanovenou dobou obnovy do jedného týždňa. Tento plán musí zahŕňať postupy, ako daný proces obnoviť, eventuálne by mal popisovať alternatívne postupy obnovy daného procesu. Aktivity, ktoré nie sú definované v BIA nebudú predmetom Business Continuity plánov.

3.4.1. Druhy BCP plánov

Druhy BCP plánov navrhujem rozdeliť do skupín podľa zamerania na:

- Strategické plány – na úrovni celej organizácie, rieši Top management. Napríklad: Plány krízovej pripravenosti alebo komunikačný plán
- Taktické plány – na úrovni divízií, produktov, procesov, lokalít
- Pracovné plány – na úrovni jednotlivých útvarov

Vzhľadom k tomu, že môžu nastať rôzne udalosti, navrhujem pripraviť plány pre rôzne scenáre na zaistenie kontinuity podnikania, ktoré sú združované do **krízových scenárov:**

- **Nedostupnosť budovy**
- **Neodstatok ľudských zdrojov**
- **Neposkytovanie služieb spolupracujúcich tretích strán**

3.4.2. Štruktúra BC plánov

Štruktúru BC plánov podľa scenáru navrhujem:

I. Scenár krízovej situácie

- Popis spustenia plánu – na základe rozhodnutia Krízového výboru
- Postup informovania všetkých zmestnancov - počas pracovnej doby musia byť všetci zamestnanci informovaný emailom, telefonicky alebo osobne; mimo pracovnej doby sú všetci zamestnanci informovaný kaskádou
- Komunikácia o spoustení BCP – Interná (líniový management); Externá (v spolupráci s útvarom komunikácie sú informovaný o spustení plánu tretie strany – klienti, médiá, dodávatelia...)

II. Náhradná prevádzka

- Popis náhradnej prevádzky
- Podmienky pre vykonávanie BCP

III: *Ukončenie*

- Popis ukončenia BCP
- Popis prechodu do štandardného provozu

3.4.3. Aktualizácia a tvorba BCP plánov

Za tvorby BCP plánov je zodpovedný BC koordinátor a plán musí byť schválený managementom.

Aktualizácia Business Continuity plánov je nikdy nekončiaci proces a jej cieľom je aby plány reflektovali zmeny, ktoré prebiehajú v rámci organizácie eventuálne aj mimo nej.

Dôvody k aktualizácií plánov navrhujem takto:

- Zmena samotného procesu
- Zmena v ICT technológii
- Významné personálne zmeny
- Testovanie alebo vznik krízovej situácie – ak je to nutné a z testu vyplýva nutnosť aktualizovať plán
- Pravidelná aktualizácia raz za rok – ak nebol plán v danom roku aktualizovaný na základe predchádzajúcich bodov

3.5. Disaster Recovery Plán

Disaster Recovery plán vychádza z analýzy infraštruktúri IT a musí popisovať obnovu technológií po nečakanej situácií s negatívnym dopadom. Najdôležitejším cieľom v takejto situácií je obnovenie služieb pre zákazníkov a služieb kriticky dôležitých pre banku. Disaster Recovery plán musí obsahovať časť Disaster Recovery Description pre jednotlivé prvky infraštruktúri zvlášť. Po spustení Disaster Recovery plánu krízovým managementom je DRD dokument základným návodom ako obnoviť služby narušené daným dopadom a previesť tzv. Failover – číže spustenie služby z replikovaného serveru.

3.5.1. Disaster Recovery Description

Disaster Recovery Description, teda popis (návod) ako obnoviť služby na úrovni infraštruktúri sú súčasťou Disaster Recovery plánov a v prípade krízovej situácie sú častokrát jediným použiteľným dokumentom.

3.5.2. Štruktúra DR plánov

Štruktúru tohto dokumentu navrhujem nasledovne:

- **Základné informácie** (vlastník dokumentu, posledná platná verzia...)
- **Technické detaily** (Popis technológie, typ serveru, kritikalita, RTO...)
- **Disaster Recovery mód** (Failover inštrukcie, udržiavanie DR módu, ukončenie DR módu, znovuobnovenie primárneho serveru)
- **Testovanie**
- **Ostatné dôležité body** (aplikácie, databázy...)

3.5.3. Aktualizácia a tvorba Disaster recovery plánov

Za tvorbu Disaster Recovery plánu je zodpovedný DR koordinátor s podporou od vlastníka danej aplikácie / serveru. Dôvody k aktualizácie týchto plánov navrhujem:

- Významná zmena v infraštruktúre
- Testovanie alebo vznik krízovej situácie – ak je to nutné a z testu vyplýva nutnosť aktualizovať plán po prípade DRD
- Pravidelná aktualizácia raz za rok – ak nebol plán v danom roku aktualizovaný na základe predchádzajúcich bodov

3.6. Testovanie plánov

Plány Business Continuity ako aj Disaster Recovery navrhujem testovať minimálne raz za rok alebo po významnej zmene a aktualizácií plánu. Druh testu závisí od scenáru danej situácie. Vo všeobecnosti však navrhujem rozdeliť testovanie na: **ohlásené** a **neohlásené.**

Podstatou testu BCP je uistenie o tom, že v prípade akejkoľvek krízovej situácie bude plán fungobať korektne a efektívne a preveriť je použiteľnosť v praxi. Cieľom testu je dosiahnuť obnovu daných služieb v dopredu stanovených časoch a na minimálnej definovanej úrovni.

Za testovanie sú zodpovední koordinátori z týmu BCDR a z každého testu musí byť vytvorený report, ktorý je odoslaný na schávlenie BC managerovi, ktorý ich na konsolidovanej úrovni ďalej reportuje predstavenstvu spoločnosti.

Protokol o testovaní musí dávať jasnú informáciu, aké aktivitu sme testovali, akým spôsobom a aké sú závery testovania.

3.6.1. Testovanie BC plánov

Testovanie plánov Business Continuity závisí od stanovených krízových scenárov. Navrhujem nasledujúce testy pre dané scenáre:

- Nedostupnosť budovy – **Test alternatívnej lokácie** – premiestnenie vybraných členov týmov (testerov) do ich alternatívnej lokácie definovanej v BIA (HO / alternatívna lokácia banky)
- Neodstatok ľudských zdrojov – Tento scenár je komplivaný v tom, že nemôžeme predpokladať koho sa bude nedostupnosť týkať a aký bude konkrétna situácia. V BC plánoch musí byť definovaná pre tento scenár kritická hranica – minimálny počet ľudí a musí tam byť uvedené, odkiaľ môžu byť povolané náhradné zdroje. To, čo môžeme čiastočne **testovať je aktuálnosť zoznamu náhradných zdorojov** mimo banku (ľudia v penzii, na mateskej, s ukončeným pracovným pomerom). Porminekou samozrejme musí byť, že títo ľudia majú skúsenosti s vykonávaním danej aktivity.
- Neposkytovanie služieb spolupracujúcich tretích strán – testovanie zazmluvnených náhradných dodávateľov, napr.: elektrická energia.

3.6.2. Testovanie DR plánov

Testovanie Disaster Recovery plánov závisí od kritikality popisovaného prvku infraštruktúry. Každá aplikácia označená kritikalitou „Medium“ alebo „High“ musí byť testovaná minimálne raz za rok.

Ďalším faktom na ktorom závisií Disaster Recovery test je typ daného systému. V prípade High Availabilty clusteru v móde Active – Active je možné spustiť test s názvom **Simulácia kompletnej straty datacentra.** Do tohto testu sú zahrnuté všetky clustery v móde Active – Active a ide o kompletnú izoláciu, čiže odpájanie portov od primárnych serverov a stabilizácie load balancingu na sekundárny server. Nasledovne je na sekundárny server spustená záťaž produkcie a testuje sa funkčnosť všetkých implementovaných aplikácií a databáz. Navrhujem previesť takýto test raz ročne na každé z datacentier zvlášť.

Servery bežiace v móde Active – Pasive alebo Stand – alone servery navrhujem testovať ako **Individuálny aplikačný test** kde je testovný v jednom okamihu jeden alebo len niekoľko málo serverov vzhľadom na náročnejší proces tohto testu.

Testovanie preverí relevantnosť informácií uvedených v Disaster Recovery plánoch a Disaster Recovery popisoch.

3.7. BCDR Awareness

Business Continuity and Disaster Recovery je pomerne mladé odvetvie, ktoré nemá zatiaľ nemá medzi zamestnancami a verejnosťou veľké povedomie. Je však dôležitým prvkom v prípade nečakanej situácii či katastrofe. Z tohto dôvodu navrhujem pravidelné elektornické školenie zamestnancov na ročnej bázi a každoročný BCDR workshop s prezentovaním podnikovej BCDR stratégie.

4. ZÁVER

V rámci tejto diplomovej práce som sa zaoberal zavedením Business Continuity and Disaster Recovery stratégie do reálneho prostredia banky. Podarilo sa mi analyzovať požiadavky, hrozby a riziká, z ktorých som vychádzal pri vypracovaní konkrétnych opatrení nutných pre zavedenie stratégie.

Počas vypracovávania tejto práce som zistil, že stratégia BCDR nie je zatiaľ stále v povedomí verejnosti a samotných zamestnancov spoločnosti. Zavedením tejto stratégie celý proces iba začína, nakoľko musí byť kontinuálne zlepšovaná a aktualizovaná.

Ciele mojej práce boli splnené a po zavedení mojich návrhov do praxe, bude spoločnosť pripravená na zvládanie krízových situácií za pomoci stratégie kontinuity činností a obnovy po katastrofe.

5. ZOZNAM POUŽITÝCH ZDROJOV

Knihy:

(1) SZABADOS, Ľ. - BRADÁČ, M. - ĎORDA, M.: *Business Continuity Management.* Bratislava: TATE International Slovakia, 2008. ISBN 978-80-969747-2-6

(2) ONDRÁK, V. - SEDLÁK, P. – MAZÁLEK, V.: *Problematika ISMS v manažerské informatice.* Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

(3) BARTA, J. – SVOBODA, O. – URBÁNEK, J.: *Krizová interoperabilita.* Brno: Univerzita obrany Brno, 2015. ISBN 978-80-7231-428-7

(4) POŽÁR, J.: *Informační bezpečnost.* Plzeň: Vydavatelství a nakladatelství Aleč Čeněk, 2005. ISBN 80-86898-38-5.

Elektronicé zdroje:

(5) Fundamentals of business continuity: the business impact analysis. [online] Copyright © 2017. [cit. 29.01.2017]. Dostupné z: http://www.continuitycentral.com/index.php/news/business-continuity-news/1415-fundamentals-of-business-continuity-the-business-impact-analysis

(6) Řada norem ISO/IEC 27000. [online] Copyright © 2017 Risk Analysis Consultants. [cit. 17.03.2017]. Dostupné z: http://www.iso27000.cz/

(7) ISO/IEC 27031:11. [online] Copyright © 2017 Risk Analysis Consultants. [cit. 17.03.2017]. Dostupné z: http://www.iso27000.cz/rac/homepage.nsf/CZ/27031

(8) ČSN EN ISO 22301. [online] Copyright © 2003 - 2017 Ing. Jiří Hrazdil [cit. 17.03.2017]. Dostupné z: https://shop.normy.biz/detail/94064

(9) ISO 24762:2008. [online] © 2008 ISO/IEC [cit. 17.03.2017]. Dostupné z: https://www.iso.org/obp/ui/#iso:std:iso-iec:24762:ed-1:v1:en

Technické normy a zákony:

(10) *Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary ISO/IEC 27000:2009*

(11) Information technology -- Security techniques -- Guidelines for information and communication technology readiness for business continuity ISO/IEC 2703:2011

(12) Societal security -- Business continuity management systems --- Requirements ISO/IEC 22301:2012

(13) Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services ISO/IEC 24762:2008

6. ZOZNAM POUŽITÝCH TABULIEK A OBRÁZKOV

Obrázky:

Tabuľky: