Systém riadenia kontinuity obchodných činností

UniCredit Bank Slovakia, a. s., vznikla fúziou UniBanky, a. s., a HVB Bank Slovakia, a. s., v apríli 2007. Obe banky už predtým pôsobili na slovenskom trhu vyše 17 rokov a vybudovali si výnimočné renomé v niekoľkých oblastiach. Zlúčením dvoch bánk s rozdielnou stratégiou a zameraním sa vyprofilovala nová univerzálna banka so silným zameraním na retailové bankovníctvo, s pevnou pozíciou v oblasti firemného bankovníctva a s ambíciou stať sa značkou pre oblasť privátneho bankovníctva na Slovensku. Spojenie sa pozitívne prejavilo vo všetkých oblastiach, čím banka potvrdila svoju silnú a stabilnú pozíciu kľúčového hráča na trhu. UniCredit Bank patrí na slovenskom trhu medzi banky s najvyššou kapitálovou primeranosťou.

Riešenie

Spoločnosť TEMPEST pripravila a zaviedla v prostredí UniCredit Bank Slovakia, a. s. (ďalej UCBSK alebo banka), systém riadenia kontinuity obchodných činností – business continuity management (BCM). Projekt pozostával z viacerých etáp, počnúc zhodnotením aktuálneho stavu cez prípravu stratégie obnovy, návrhu plánov kontinuity až po návrh typových plánov revízie a údržby vytvorených plánov a typového plánu školení pre vybrané skupiny zamestnancov. Do projektu boli zainteresované tímy banky i TEMPEST-u pozostávajúce z viacerých odborníkov na rôzne oblasti analytickej, aplikačnej i sieťovej bezpečnosti.

Výsledkom projektu je banka kvalitne pripravená na vznik mimoriadnej, neočakávanej udalosti alebo havárie a záruka, že kritické procesy nebudú v prípade katastrofy narušené, resp. budú obnovené v čo najkratšom čase, ktorý bol definovaný biznis garantmi ako akceptovateľný a negatívne dopady na banku budú minimálne.

1. Analýza dopadov a analýza (ohodnotenie) rizík

Východiskovým krokom projektu bola analýza dopadov (Business Impact Analysis – BIA) a ohodnotenie rizík (analýza rizík).

Cieľom BIA bola identifikácia a kvantifikácia dopadov na banku v prípade straty alebo prerušenia jej kritických procesov. Súčasťou analýzy bolo aj stanovenie časového intervalu, dokedy je potrebné dané procesy obnoviť, aby bol prípadný negatívny dopad na banku minimálny. Analýza dopadov je východiskovým bodom pre navrhnutie stratégie obnovy, plánov kontinuity činností, definovanie havarijných tímov a rozpracovanie ich úloh a povinností.

Počas realizácie analýzy dopadov boli získavané hlavne nasledujúce typy informácií:

- minimálna akceptovateľná úroveň procesov
- časový rámec, počas ktorého musia byť procesy obnovené
- väzby procesov na okolie
- dopad (finančný aj funkčný) na banku v prípade prerušenia/výpadku procesov (v závislosti od času nedostupnosti)
- časové požiadavky na obnovu
- požiadavky na dostupnosť spracúvaných údajov

Prínos:

- schopnosť rýchlo reagovať na neočakávanú udalosť, ktorá má alebo by mohla mať negatívny dopad na kritické procesy
- minimalizovanie prípadných strát vyplývajúcich z prerušenia kritických procesov
- pripravenosť zamestnancov banky na krízové situácie
- zvýšená odolnosť banky voči hrozbám, ktoré ovplyvňujú kritické procesy,
- schopnosť zabezpečiť návrat do bežnej prevádzky, do stavu pred vznikom mimoriadnej udalosti,
- splnenie právnych požiadaviek a noriem

Priebeh a etapy projektu

1. etapa:
Analýza dopadov a analýza (ohodnotenie) rizík

1a: Analýza dopadov (Business Impact Analysis – BIA)

1b: Analýza (ohodnotenie) rizík (Risk Assessment – RA)

2. etapa:
Stratégia obnovy

3. etapa:
Tvorba plánov kontinuity

4. etapa:
Riadiace dokumenty BCM

5. etapa:
Údržba plánov, tréningové programy a audit

Tempest
IT makes sense

- existencia alternatívnych riešení v prípade výpadku procesu
- právne, regulačné, zmluvné a iné požiadavky
- zoznam aktív potrebných na zabezpečenie kontinuity procesu
- stanovenie priorít kritických procesov pre proces obnovy

Na základe výsledkov analýzy dopadov boli identifikované kritické procesy banky, ktoré boli následne rozdelené podľa požiadaviek na obnovu a zahrnuté do prípravy plánov kontinuity.

Analýza rizík poskytla informácie o stave informačnej bezpečnosti, slabých a silných stránkach implementovaných bezpečnostných mechanizmov. Základným cieľom bolo vytvoriť predpoklady na efektívne riadenie informačnej bezpečnosti a rozhodnutie o riadení (správe) rizík, ktoré sa vzťahujú na základné funkcie banky. Analýza rizík bola zameraná predovšetkým na kritické procesy a bola pri nej použitá kvalitatívna metóda. Súčasťou analýzy rizík bola identifikácia a ohodnotenie hrozieb, zraniteľností a rizík a aj návrh na správu identifikovaných rizík. Vstupom pre analýzu rizík boli rokovania s definovanými zamestnancami banky (zamestnanci IT, bezpečnosti, vybraných biznis oddelení), interné dokumenty týkajúce sa bezpečnosti (bezpečnostná politika, smernice, pracovné postupy a pod.) a obhliadky vybraných priestorov.

Údaje a podklady pre analýzu dopadov a analýzu rizík boli získavané formou štruktúrovaných formulárov a na osobných stretnutiach so zamestnancami banky. Týmto stretnutiam predchádzala prezentácia, ktorej obsahom bolo oboznámenie respondentov s projektom, systémom riadenia obchodnej kontinuity a ohodnocovaním rizík, ako aj so spôsobom vypĺňania inventarizačných formulárov. Prínosom takéhoto spôsobu zbierania vstupov bolo minimalizovanie opakovaného získavania požadovaných informácií a podkladov v projekte BCM a nízka časová zaťaženosť zamestnancov banky pri ich každodenných pracovných činnostiach. Vďaka tomu mohol byť optimalizovaný harmonogram projektu a realizované činnosti predovšetkým v analytických etapách. Najvýznamnejším prínosom takéhoto prístupu bolo teda minimalizovanie tých činností (analytické rozhovory, pracovné stretnutia), ktoré v najväčšej miere zasahovali do bežnej operatívy vedúcich zamestnancov banky a zdržiavali ich od pracovných povinností. Optimalizácia vstupných analytických činností mala skrátiť harmonogram celého projektu a urýchliť vybrané etapy.

2. Stratégia obnovy

Druhým krokom tvorby plánov kontinuity činností pre kritické procesy banky bolo vypracovanie stratégie obnovy pre tieto procesy.

Stratégia obnovy vychádza z analytických záverov prvej etapy, a to najmä z analýzy dopadov. Na jej základe bola stanovená vhodná stratégia obnovy v súlade s požiadavkami a potrebami banky tak, aby bola zachovaná kontinuita kritických procesov v prípade, že nastane mimoriadna udalosť. Z viacerých variantov bola po zhodnotení požiadaviek a možností banky vybraná stratégia, ktorá bola podkladom pre tvorbu detailných plánov kontinuity činností. Táto stratégia bola schválená predstavenstvom banky. V rámci stratégie obnovy boli definované konkrétne východiská a princípy realizácie jednotlivých činností v havarijnom stave a k tomu prislúchajúce nevyhnutné zdroje (materiálne, personálne a pod.).

Schválená stratégia obnovy pre kritické procesy a stratégia obnovy IT na jednej strane rešpektujú požiadavky a potreby banky (biznis oddelení) a na druhej strane zohľadňujú možnosti a reálne zdroje banky, oddelenia IT a zamestnancov, ktorí sú zodpovední za korektnú a spoľahlivú prevádzku jednotlivých ICT aktív.

V prostredí banky bola zvolená stratégia obnovy pre ICT komponenty založená na modeli „Aktiv – Aktiv". Táto stratégia bola pre banku vhodná z viacerých hľadísk:

- banka má k dispozícii viacero lokalít, ktoré boli pripravené na prevádzkovanie dôležitých ICT komponentov = > nebolo potrebné budovať alebo inak zaobstarať iné priestory
- banka používa virtualizované prostredie na prevádzku viacerých systémov a mala v pláne jeho rozširovanie = > jednoduchým spôsobom sa tak dajú presúvať servery a systémy medzi zvolenými lokalitami a dá sa škálovať ich výpočtový výkon a zaťaženie
- v oblasti konektivity na pobočky, materskú spoločnosť a externé prostredie boli vybrané vzájomne zastupiteľné lokality = > záložná/náhradná konektivita bola už vyriešená

Navrhnutá stratégia obnovy rieši aj obnovu kritických procesov z hľadiska personálnych zdrojov, zabezpečenia náhradných priestorov a ostatných požiadaviek na potrebné zdroje (napr. kancelárske vybavenie a kancelárske potreby, telefóny, faxy, spotrebný materiál a pod.).

Opisovaný kombinovaný prístup zberu informácií (formulár + osobné stretnutia), i napriek spomínaným komplikáciám, možno hodnotiť ako prínosný. Je však veľmi dôležité zainteresovať už v úvodných fázach projektu tých zamestnancov, ktorí budú primárnym zdrojom vstupných údajov a budú minimalizovať odovzdávanie informácií z „druhej a tretej ruky".

Cieľom stratégie obnovy bolo definovanie základného rámca na zaistenie kontinuity činností v banke metódou „Worst Case Scenario". Stratégia sa zamerala predovšetkým na:

- výber alternatívnych metód, ktoré budú použité v prípade narušenia alebo mimoriadnej udalosti na zabezpečenie kontinuity kritických procesov v súlade so stanovenou prioritou počas analýzy dopadov
- zraniteľnosti a kritické prvky zlyhania (single points offailure) v kritických procesoch, ktoré boli identifikované počas analýzy rizík

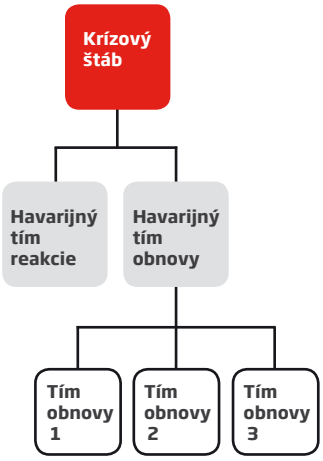
3. Tvorba plánov kontinuity

Nasledujúcim krokom projektu bol návrh detailných plánov kontinuity činností. Tieto plány konkretizujú schválenú stratégiu obnovy, dokumentujú jednotlivé kroky reakcie a obnovy a ďalšie potrebné informácie nevyhnutné na zachovanie alebo obnovenie kontinuity kritických procesov banky.

Plány kontinuity definujú postup reakcie na mimoriadnu udalosť a postupy obnovy ICT a kritických procesov banky. Plány obsahujú najmä nasledovné informácie:

- opisné informácie jednoznačne identifikujúce verziu a platnosť plánov
- opis kritických procesov:
  - vlastníkov
  - väzby procesov na okolie
  - zdroje potrebné na zachovanie kontinuity
- členenie havarijných tímov a ich zloženie – personálne zdroje (vedúci tímu, zástupca vedúceho, členovia tímu)
- určenie záložných lokalít, doprava do týchto lokalít
- základné vybavenie potrebné na obnovu (kancelárske vybavenie, technické zariadenia [HW], programové vybavenie [SW], komunikačné prostriedky, dopravné prostriedky a pod.)
- zoznam dodávateľov (interných, externých), zmluvy, SLA a pod.
- opis činností a úloh potrebných na zabezpečenie kontinuity kritických procesov, zodpovednosti, právomoci na riadenie procesu obnovy
- spôsob komunikácie s okolím

Hierarchia havarijných tímov



Úroveň detailu jednotlivých plánov kontinuity závisí od charakteru a zložitosti prostredia, v ktorom banka pôsobí, a takisto aj od výšky akceptovateľného rizika. Plány kontinuity boli z logického hľadiska rozdelené na plán reakcie a plán obnovy.

Reakcia na vzniknutú mimoriadnu udalosť je veľmi dôležitá, a tak bola vyčlenená ako úvodná, samostatná časť plánov kontinuity. Celý proces bol naviazaný na proces hlásenia a správy bezpečnostných incidentov, ktorý bol v banke zavedený pre oblasť IT. Na základe odporúčania riešiteľov (pozri aj 4. etapu: Riadiace dokumenty BCM) bol rozšírený o bezpečnostné incidenty aj v ostatných oblastiach. Navrhované centrálne hlásenie incidentov zjednoduší ich správu a riešenie a v prípade významných udalostí urýchli naštartovanie potrebnej reakcie. Nie každý bezpečnostný incident prerastie až do havarijného stavu, ale ak sa to stane, je nevyhnutná rýchla, správna a adekvátna reakcia. Detailný postup, ako si treba v takomto prípade počínať, opisuje práve plán reakcie.

Plán reakcie definuje konkrétne kroky, ktoré je nutné vykonať v prípade vzniku mimoriadnej situácie.

Sumarizuje činnosti pre členov tímu reakcie, ktorých hlavným cieľom je zhodnotiť vzniknutú situáciu a podniknúť všetky potrebné kroky, aby nedošlo k väčším škodám a zhoršeniu vzniknutej situácie. Na základe posúdenia a vyhodnotenia rozsahu mimoriadnej situácie predseda krízového štábu rozhodne o vyhlásení, resp. nevyhlásení havarijného stavu. Ak nie je vyhlásený havarijný stav, postupuje sa podľa štandardných postupov na riešenie porúch/poruchových stavov. Ak krízový štáb rozhodne o vyhlásení havarijného stavu, ďalší postup sa riadi podľa plánov obnovy.

Plány obnovy sa aktivujú vyhlásením havarijného stavu a nadväzujú na plán reakcie.

Plány definujú pre jednotlivé havarijné tímy úlohy, kroky a postupy, ktorých náplňou je zabezpečiť kontinuitu kritických procesov banky v požadovanom čase. To znamená, ako obnoviť kritické aplikácie a systémy a pripraviť náhradné priestory pre kľúčových zamestnancov banky, ako zabezpečiť nevyhnutné vybavenie, aby mohli byť kritické procesy vykonávané na definovanej minimálne akceptovateľnej úrovni. Súčasťou plánov je tzv. zvolávací strom, ktorý definuje postupnosť zvolávania jednotlivých členov havarijných tímov, ako aj reportovacia štruktúra pre členov tímov a postup eskalácie prípadných problémov a nepredvídaných stavov. Neoddeliteľnou súčasťou plánov kontinuity sú aj plány obnovy ICT prostredia – jednotlivých aplikácií a sieťovej infraštruktúry, rovnako aj priority obnovy jednotlivých systémov.

Na zabezpečenie kontinuity kritických procesov banky – v prípade, že nastane mimoriadna udalosť – je nevyhnutné, okrem pracovných miest pre kľúčových zamestnancov a príslušných priestorov, zabezpečiť aj fungovanie tých ICT komponentov, ktoré podporujú funkčnosť kritických procesov, systémov a aplikácií. V rámci schválenej stratégie sú opísané viaceré konkrétne možnosti obnovy ICT prostredia, ktoré sú v jednotlivých plánoch následne konkretizované a rozpracované do potrebných detailov.

Vzhľadom na zvolenú stratégiu obnovy (Aktiv – Aktiv) sa väčšina plánov obnovy ICT týkala postupov na presun virtuálnych serverov do nezasiahnutej lokality a presmerovanie komunikácie a sieťovej konektivity cez lokalitu, ktorá nebola mimoriadnou udalosťou postihnutá.

4. Riadiace dokumenty BCM

Primárnym cieľom tejto etapy bolo vypracovanie metodiky pre tvorbu plánov kontinuity činností. Navrhnutá metodika špecifikuje požiadavky na riadenie procesov súvisiacich s plánovaním kontinuity, ako aj základné požiadavky na riadenie kontinuity. Obsahom metodiky sú najmä:

- základné požiadavky na obsah plánov kontinuity
- zodpovednosti pri tvorbe plánov kontinuity činností
- požiadavky na údržbu, revíziu a testovanie plánov kontinuity
- požiadavky na školenia o systéme kontinuity obchodných činností
- metodika na analýzu dopadov

Cieľom bolo tiež posúdenie existujúcich interných predpisov a identifikácia chýbajúcich dokumentov vyžadovaných regulačným orgánom (NBS), materskou spoločnosťou a auditom na riadenie procesu BCM. Všetky relevantné oblasti procesu BCM boli v prostredí banky podchytené v preskúmavaných dokumentoch, a tak nebolo potrebné vytvárať nové dokumenty. Z posúdenia existujúcich predpisov vzišli návrhy a odporúčania na ich úpravu a doplnenie (napr. riešenie bezpečnostných incidentov), aby v plnej miere pokrývali proces BCM v zhode s požiadavkami medzinárodných noriem upravujúcich túto problematiku v rámci špecifických podmienok banky.

5. Údržba plánov, tréningové programy a audit

V poslednej etape projektu bol navrhnutý typový plán revízie a údržby plánov kontinuity a plánov obnovy IT. Cieľom tohto kroku je udržiavať navrhnuté plány v stave, ktorý zaručí ich použiteľnosť v prípade, že nastane mimoriadna udalosť. Súčasťou tejto etapy bolo predovšetkým defi novanie procesov a zodpovedností za údržbu plánov BCM banky v súlade s jej strategickými cieľmi a zmenovým konaním (zmeny obchodných procesov, IT infraštruktúry, vonkajšie vplyvy, analýzy rizík, právne predpisy a pod.).

Ako súčasť tejto etapy bol vytvorený aj typový tréningový program pre jednotlivé skupiny zamestnancov banky (výkonný manažment, kľúčoví zamestnanci, zamestnanci podporných útvarov). Hlavným cieľom tréningového programu je zabezpečiť pripravenosť cieľových skupín zamestnancov na prípadné mimoriadne situácie a minimalizovať tak riziko neadekvátnej alebo neskorej reakcie.

„Banka prešla v posledných rokoch značnými zmenami v organizačnej aj technologickej oblasti, preto bol nutný nezainteresovaný pohľad na všetky interné procesy, ktoré ovplyvňujú dostupnosť poskytovaných služieb. Realizácia projektu BCM bola strategicky správnou voľbou, nakoľko výsledky mali zásadný vplyv na zmeny v havarijnom plánovaní našej spoločnosti," hovorí Peter Vrbovský, IT Security Officer UniCredit Bank Slovakia, a. s.

„Zavedením BCM v UniCredit Bank je zabezpečená nepretržitá činnosť kritických procesov, a to aj v prípade vzniku neočakávanej udalosti, prípadne havárie. Okrem tohto hlavného prínosu môžeme identifikovať aj iné benefity, ktoré projekt banke priniesol. Napríklad identifikáciu všetkých činností banky kritických z pohľadu poskytovania služieb zákazníkom alebo zvýšenie odolnosti banky voči hrozbám," vraví Peter Ferianček, konzultant analytickej bezpečnosti TEMPEST, a. s.

Špecifiká projektu a problémové miesta

Špecifikom realizovaného projektu BCM bolo, že mu predchádzal projekt „Identifikácia, klasifikácia a vlastníctvo informačných aktív banky". V rámci spomínaného projektu boli získavané aj údaje, ktoré boli následne využité pri tvorbe plánov kontinuity obchodných činností – predovšetkým podklady pre analýzu dopadov (BIA) – viac informácií sa nachádza v časti opisujúcej túto etapu (1. Analýza dopadov a analýza [ohodnotenie] rizík).

V priebehu projektu riešiteľský tím narazil aj na viaceré komplikácie, ktoré mali vplyv na priebeh jednotlivých etáp a napokon aj na samotný priebeh projektu. K týmto skutočnostiam patrili predovšetkým príprava banky na prechod na euro a veľké množstvo externých a interných auditov prebiehajúcich v čase realizácie projektu. Uvádzané skutočnosti sa prejavili predovšetkým v etapách, kde sa vyžadovala významná súčinnosť od zamestnancov banky, čo malo vzhľadom na uvádzané objektívne skutočnosti vplyv na termíny, ktoré záviseli od spätnej väzby riešiteľského tímu banky, prípadne od schválenia jednotlivých rozhodujúcich výstupov vedením banky. Uvádzané komplikácie nemali nakoniec vplyv na úspešné ukončenie projektu, prejavili sa len na časových sklzoch vybraných etáp.

Záver

Všetky etapy projektu a jednotlivé výstupy boli vypracované v zhode s požiadavkami noriem pre oblasť riadenia kontinuity činností a oblasť informačnej bezpečnosti:

- BS 25999-1 – Manažment kontinuity činností – Kódex praxe
- BS 25999-2 – Manažment kontinuity činností – Požiadavky
- ISO/IEC 27001:2005 – Systém manažérstva informačnej bezpečnosti (ďalej len ISO 27001)
- ISO/IEC 27002:2005 (ISO/IEC 17799:2005) – Kódex praxe manažérstva informačnej bezpečnosti (ďalej len ISO 27002)

Plány kontinuity navrhnuté a implementované spoločnosťou TEMPEST umožnili v primeranom čase efektívne splniť všetky stanovené ciele projektu. Riešenie je prínosom pre banku i jej zákazníkov a slúži ako kľúčový materiál pre obnovu obchodných činností v prípade havarijnej udalosti.

Tempest
IT makes sense

UniCredit Bank