

# Outsourcing DR v praxi

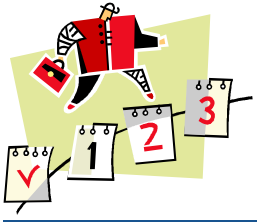


Martin Rus, 01.04.2008



# Profil společnosti

- **Factoring KB, a.s.:**
    - Na trhu od roku 1997
    - Finanční skupina Komerční banky a nadnárodně vlastněna společností Societé Générale
  
  - **Předmět podnikání:**
    - odkup
    - správa
    - financování
    - inkaso
    - převzetí rizika (zajištění) krátkodobých pohledávek (zpravidla do 90 dnů), vzniklých na základě dodávek zboží a služeb.
  
  - **Počet zaměstnanců: cca 60**
-



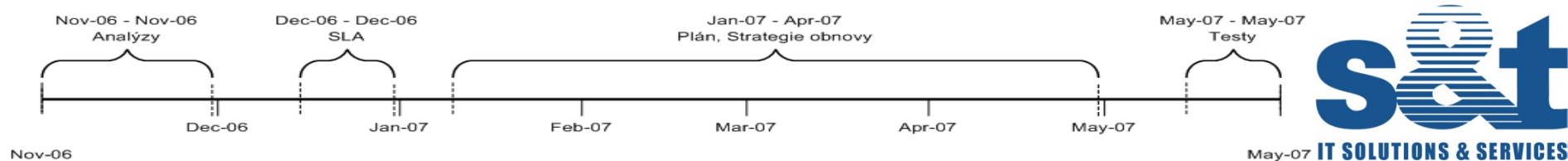
# Záměr/výstupy/cíle

- Schopnost řízeně čelit haváriím a obnovit kritické subsystémy do 48 hodin mimo prostory primární lokality:
    - Včetně 15 pracovních pozic pro klíčové role v rámci kritických obchodních procesů společnosti
  - Dodavatel určí preventivní opatření a navrhne optimální strategii obnovy
  - Plány reakce a obnovy po výskytu havárie:
    - Jak identifikovat, že se jedná o havárii,
    - Jak ustavit krizové řízení a zajistit řízenou odezvu,
    - Jak technicky obnovit jednotlivé informační systémy.
  - Veškeré procedurální postupy, technické procedury a operativní řízení prověřeno praktickým testem
-



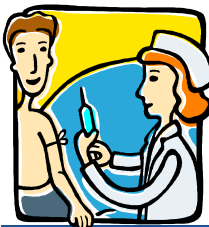
# Vstupní podmínky

- Interně provedená analýza rizik a BIA – RTO 48 hodin
    - Jeden havarijný scénář
  
  - Existující kontrakt na serverovou infrastrukturu
  
  - Kritické subsystémy:
    - Podpůrné: LAN, Internet, Domain/AD, Workstation
    - Aplikační: Email, Faktor.
  
  - Požadavky klienta na strategii obnovy:
    - Cenově efektivní strategie obnovy s ohledem na specifikovaný RTO
    - Integrace procesů a postupů třetích stran – Arbes a NTServis
    - Data v době míru výhradně v držení FKB
    - Maximální možné využití existujícího záložního HW klienta
-



# Projekt

- **Fáze I: Analýza stávajícího stavu**
  - Zmapování vazeb infrastruktury,
  - Identifikace preventivních opatření a návrh na jejich implementaci
  - Určení variant strategie obnovy s ohledem na RTO a výběr vítězné varianty
  
- **Fáze II: Aktualizace SLA na serverovou infrastrukturu**
  - Snímek interface předání havarijního centra v případě havárie
  - Dodatečný HW a nové služby, identifikované v předchozí fázi
  
- **Fáze III: Vypracování havarijního plánu**
  - Role, zodpovědnosti, definice scénářů a procesy reakce, obnovy IT/IS
  - Proces údržby a testování havarijní dokumentace
  - Integrace existující dokumentace třetích stran
  
- **Fáze IV: Komplexní test obnovy**
  - Reálný přechod provozu do prostor náhradního centra
  - Závěrečná zpráva a vyhodnocení testu



# Řešení

## ➤ Prevence:

- Data – zálohy, obnova,
- Internetová konektivita,
- HW z kontraktu,
- LAN SW,
- Firewall – NTServis,
- MX záznamy,
- Hesla,
- Pracovní stanice,
- Instalační sady.

## ➤ Reakce:

- Vyhlášení havárie,
- Svolání HT,
- Obnova HW vrstvy,
- Obnova O/S vrstvy,
- Obnova sítě,
- Obnova dat ze záloh,
- Obnova aplikací,
- Akceptační testy.



---

## Výsledky

- Efektivně dosažené RTO 32 hodin
  
  - Obsazení HT:
    - GCC 3x, Arbes 2x, NTServis 1x, FKB 1x
  
  - Veškeré subsystemy plně funkční
  
  - Akceptace kritérií z pohledu uživatele
-



# Výhody a přínos řešení pro klienta

- Minimalizace nákladů díky využití existujícího SLA,
  - Schopnost řízeně reagovat na havárii,
  - Diskuze business – IT a sladění požadavků,
  - Naplnění požadavku auditora,
  - Jasná zpráva o připravenosti směrem k business = větší spokojenost business,
  - Rizika odstraněna preventivními opatřeními.
-



# Questions



**Martin.rus@gcc.cz**

