

Obnova po havárii

Disaster recovery

Úvod do problematiky, základní pojmy, doporučení

Aleš Padrta
CESNET, z. s. p. o.

- Úvodní slovo
- Základní pojmy
- Životní cyklus DRP/BCP
 - Analýza
 - Návrh
 - Implementace
 - Provozní aspekty
- Metriky úspěchu
- Shrnutí

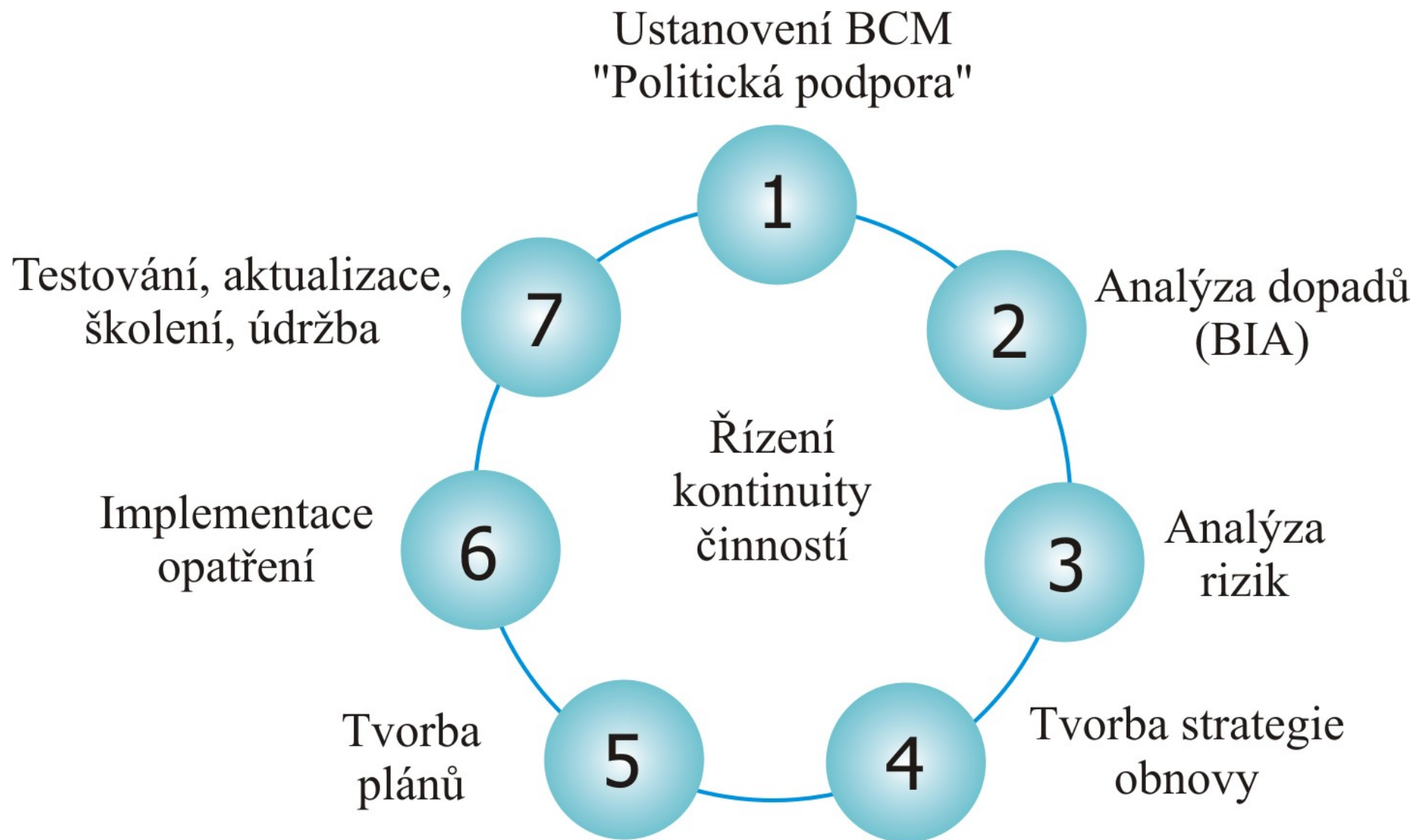
- Informační systémy
 - Poskytují klíčovou podporu
 - Nutná podmínka fungování
 - Nejsou nezničitelné
- Výskyt mimořádných událostí (katastrof, havárií)
 - Přírodní (povodně, požáry, vichřice, ...)
 - Lidský zásah (omyl, sabotáž, malware, teroristi, ...)
 - Vnější prostředí (výpadek el. energie, tel. spojení, ...)
 - Nutnost záchranných / likvidačních prací
- Jaké budou důsledky
 - Funkčnost IS/IT?
 - Funkčnost organizace?

- Business Continuity Management
 - Řízení zachování kontinuity činností
 - Zájem na nepřerušném fungování organizace
 - Některé procesy nelze přerušit
 - Ani v případě výskytu mimořádné události
 - Péče o pacienty, výdej jídel v menze
- Business Continuity Planning
 - Plány pro zachování kontinuity činností
 - Náhradní nouzová řešení
 - Karta u postele, zapisování na papír

- Disaster Recovery Planning
 - Plány pro obnovu činnosti po mimořádné události
 - Preventivní opatření
 - Zmírnění následků
 - Ulehčení obnovy
 - Reakce na mimořádnou událost
 - Obnova kritických systémů v nouzovém režimu
 - Obnova podpůrných systémů v nouzovém režimu
 - Celková obnova na úroveň původního stavu
 - Týká se
 - HW / SW
 - Dat
 - Pracovníků

- Business Continuity vs. Disaster Recovery
 - Nutnost podpory vedení
 - Dodání potřebných informací
 - Prosazení potřebných změn
 - Alokace zdrojů
 - Jinak lze pouze lokálně v rámci IT oddělení
 - Navzájem se doplňují
 - Business Continuity
 - Obecnější, zaměřeno na alternativní řešení
 - Disaster Recovery
 - Konkrétnější, zaměřeno na obnovu
 - Vytvářeny společně

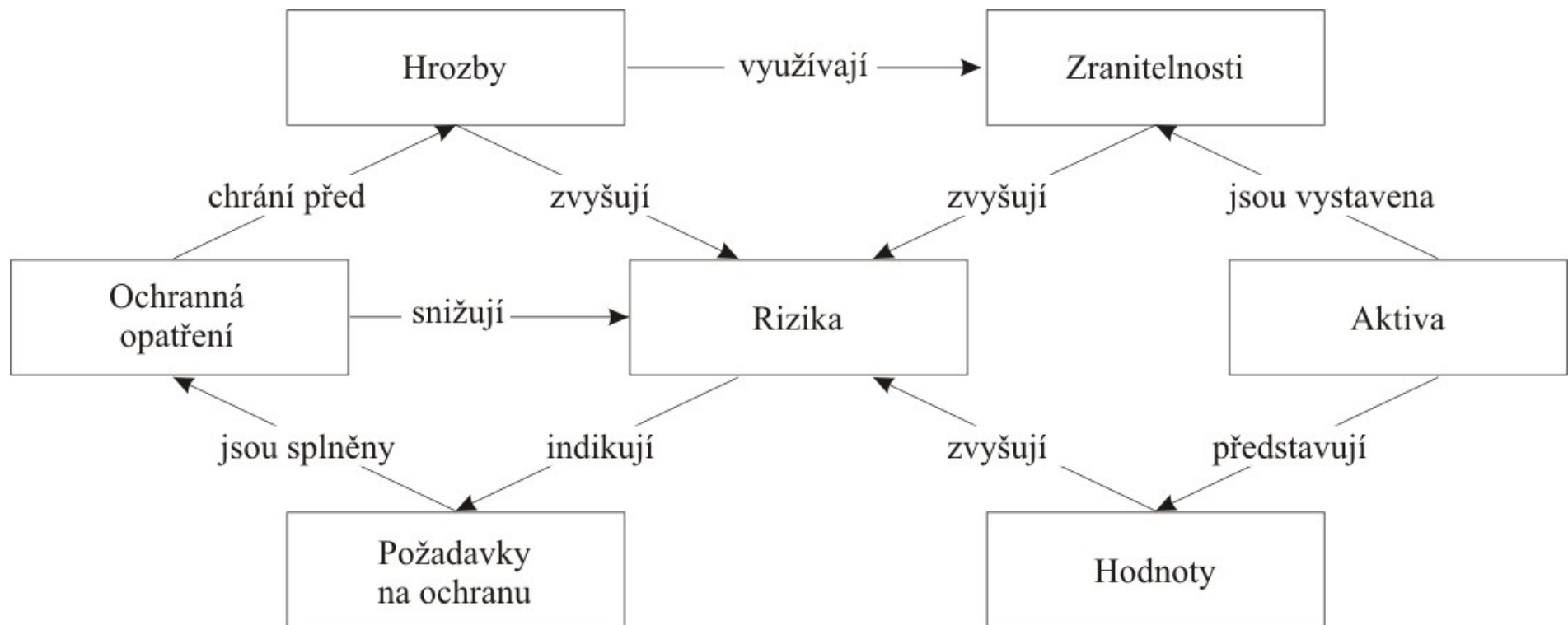
Životní cyklus DRP/BCP



- Analýza dopadů mimořádné události
- Co se stane s organizací když
 - Dojde ke ztrátě dat
 - Dojde k úniku dat
 - Dojde k neoprávněné modifikaci dat
 - Dojde k výpadku el. energie
 - IS nepůjde 5m, 10m, 15m, 1h .. 72h
 - ...
- Zjištění kritických procesů + systémů
 - Přidělení priority
 - Finanční vyčíslení škod

Analýza rizik

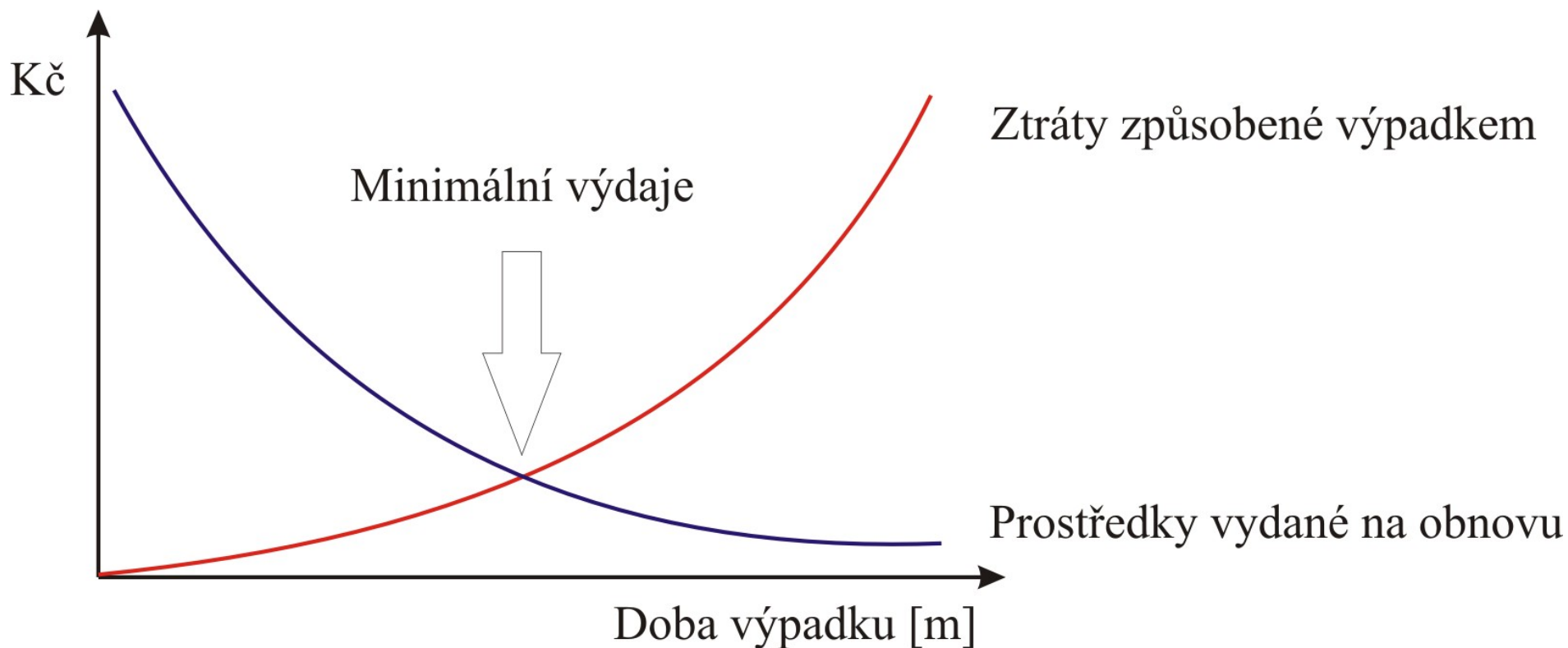
- Vyhodnocení konkrétních rizik
- Pravděpodobnost realizace konkrétních hrozeb



- Všechna rizika jsou vyloučena nebo se s nimi počítá

- Přístupy
 - Přerušování provozu
 - Přemístění provozu
 - Přenesení na třetí stranu
 - Pojištění
- Výběr strategie pro jednotlivé systémy
 - Cold-site
 - Warm-site
 - Hot-site
 - Mirrored site
- Odlišná doba výpadku a cena

- Trvání doby výpadku
 - Delší → vyšší ztráty
 - Kratší → vyšší náklady



- Definice cílů
 - Co a v jakém rozsahu má fungovat
- Reakce na události
 - Definice mimořádných událostí
 - Definice kontaktních osob - pro hlášení
 - Postup řešení mimořádné události
 - Specifikace plánu obnovy (DRP)
- Definice
 - Odpovědnosti (kdo dohlíží na plán)
 - Povinností (kdo se realizace plánu účastní)
 - Kompetencí (kdo má jaké pravomoci)

- Dílčí dokumenty
 - Jednotlivé systémy
- Definice cílů
 - Co a do jaké doby je potřeba obnovit
- Postupy a návody
 - Co a jak je potřeba udělat
- Definice
 - Odpovědnosti (kdo dohlíží na plán)
 - Povinností (kdo se realizace plánu účastní)
 - Kompetencí (kdo má jaké pravomoci)
- Dostupnost (i v případě MU)

- Cíl
 - Minimalizovat případné dopady MU
 - Ulehčit obnovu
- Monitorování
 - Provozní parametry
 - Proces zálohování
 - Prvky ochrany (IPS, FW, AV)
- Automatická reakce
 - Notifikace - zaslání e-mailu / SMS / spuštění alarmu
 - Spuštění generátoru při výpadku proudu
 - Vyhodnocení kumulativních problémů

- Primární zájem
 - Minimalizovat škody vzniklé při havárii
 - Minimalizovat narušení chodu společnosti
- Okamžitý zásah (první reakce)
 - Aktivity pro oddálení dopadů MU
 - Převedení na záložní zdroj
 - Vypnutí nedůležitých serverů šetří UPS
 - Větrání okno/dveře při výpadku klimatizace
 - Ochrana zdraví a života pracovníků
 - Evakuace / přesun do krytu

- Obnova kritických procesů
 - Důležité pro chod organizace
 - Postup podle havarijních plánů
 - Přesun do náhradních prostor
 - Jak se tam dostat, jídlo pro zaměstnance
 - Dodání náhradního HW do určité doby
 - Smlouvy s dodavateli HW
- Zotavení z MU
 - Obnova všech podpůrných činností
 - Nekritické systémy
 - Komfort + vyšší produktivita
 - Stále nouzový režim

- Obnova na úroveň původního stavu
 - Rekonstrukce budov a vybavení
 - Přejít z nouzového do standardního režimu
- Zjištění celkového rozsahu škod
 - Ztráty na živé síle
 - Zničený majetek
 - Ztráta produktivity
 - Přerušování výroby (činnosti)
 - Smluvní pokuty
 - Poškození značky / prestiže
 - Ztráta dat

- Aktualizace
 - Neaktuální plán je k ničemu
 - Z ostrých nasazení / prováděných testů
- Testování plánu
 - Pravidelně
 - Plánování scénářů testů
 - Poučení, optimalizace
- Školení
 - Nutné
 - Nepoučený pracovník zmatkuje
 - Snižuje dobu výpadku

- Dostupnost systému
 - Procento času bez neplánovaných výpadků
 - Např. 5 devítek spolehlivosti 99.999%
- Střední doba opravy
 - Jak dlouho trvá činnost systému obnovit
 - 1x 60 minut vs. 60 x 1 minuta
- Počet postižených uživatelů
 - Potenciálně vs. reálně
 - Souvisí s denní a roční dobou

- Jak přežít mimořádnou událost?
 - Podpora vedení
 - Optimální investice
 - Monitoring provozu
 - Příprava plánů a jejich aktualizace
 - Realizace plánů
 - Školení pracovníků
 - Pravidelné testování
- Bezpečnost je nekončící proces

Dotazy

???