Komplexní strategie zabezpečení dat

Petr Dvořák

Hotel Jalta, Praha
16. května 2023

Část I.

STRATEGIE V KONTEXTU ORGANIZACE

Komplexní strategie zabezpečení dat

- **Proč?**
  - Proč vlastně potřebujeme vysoce dostupná data a aplikace?
  - Proč zálohujeme?
  - Proč využíváme právě tyto postupy pro právě tyto situace?

- **Jak jsme na tom dnes?**
  - Jak řešíme vysokou dostupnost našich aplikací a našich dat?
  - Jak řešíme zálohování dat?
  - Jaké produkty v této souvislosti využíváme?

Kontinuita podnikání a její řízení

- Proč se zabývat kontinuitou podnikání?
  - Kontinuita podnikání přispívá ke zvýšení odolnosti organizace.
  - Tím snižuje riziko neočekávaných budoucích nákladů nebo výpadku příjmů.

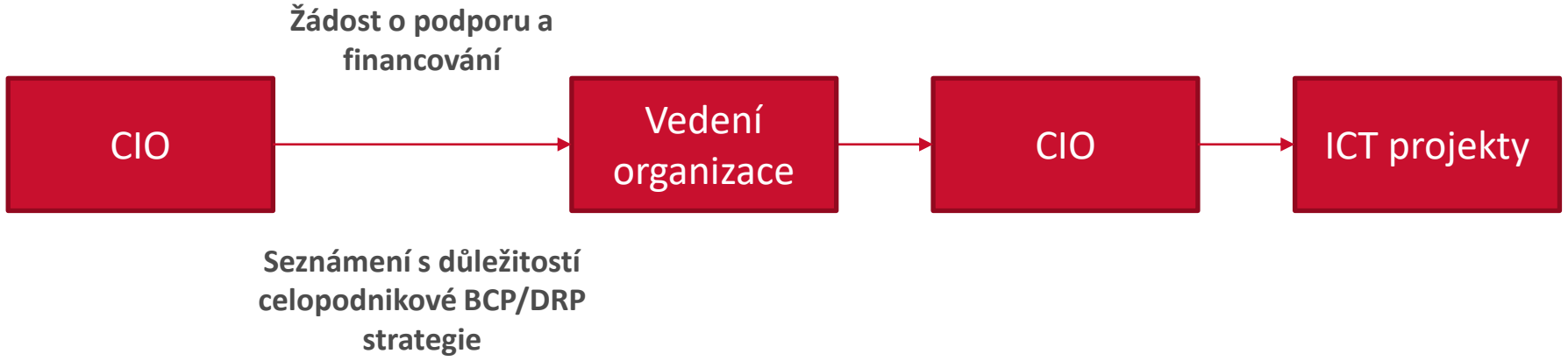
- Proč právě nyní?
  - Podpora kritických procesů organizace ze strany IT je vyšší než v minulosti.
  - Jsou využívány nové technologie a objevují se nové zranitelnosti.

- Jak k řízení kontinuity podnikání přistoupit?
  - Existují metodiky, jak postupovat, např. norma ISO 22301 – Systém managementu kontinuity podnikání (BCMS)

Role vedení organizace v BCP/DRP

BCP/DRP uvědomělá organizace

Tradiční organizace



Východiska pro návrh strategie a opatření

- 8.2 Analýza dopadů na podnikání a posuzování rizik

  - 8.2.2 Analýza dopadů na podnikání
    - Identifikace činností podporujících „business“
    - Posouzení dopadů v případě jejich nefunkčnosti
    - Stanovení časových rámců pro obnovu činností

  } Recover Point Objective (RPO)
  Recover Time Objective (RTO)

  - 8.2.3 Posuzování rizik
    - Identifikace rizik
    - Analýza rizik
    - Vyhodnocení rizik

} Rizika a jejich ohodnocení

Vznik BCP/DRP plánu

1. Závazek vedení podporovat vznik a realizaci BCP/DRP
2. Provedení analýzy rizik
3. Provedení analýzy dopadů na podnikání
4. Vypracování BCP/DRP strategie
5. Stanovení priorit realizace BCP/DRP strategie
6. Návrh konkrétních opatření (dílčích plánů)
7. Realizace těchto opatření
8. Testování těchto opatření a jejich revize

Nejslabší místa BCP/DRP v organizacích

- BC/DR plány nepostihují všechny souvislosti.
  - Analyzujme detailně všechny související procesy, činnosti a zdroje.
- BC/DR plán je dokončen a není dále aktualizován.
  - Využijme metodiku PDCA (Plan, Do, Check, Act) a aktualizujme plány.
- BC/DR plány nejsou dostatečně testovány.
  - Každý plán je nutné revidovat a testovat odpovídajícím způsobem.

Typické chyby při přípravě politik zajištění dostupnosti

1. Využití metody „švýcarského nože“
   - Lze všechny požadavky na zajištění dostupnosti vyřešit jedním nástrojem?

2. Volba nástroje nevhodného pro řešení daného požadavku
   - Lze rychle obnovit provoz např. s využitím klasického systému zálohování dat?

3. Přílišná volnost při definici pravidel zabezpečení
   - Lze si udržet kontrolu, pokud je každý systém zabezpečení jinak?

Best practices při návrhu politik zajištění dostupnosti

1. Pracujme s různými třídami zajištění dostupnosti
   - Podle kritičnosti aplikací a systémů pro běh organizace
   - Podle definovaných parametrů obnovy (RTO, RPO)
   - Podle charakteru uložených dat
   - Podle regulatorních požadavků

2. Definujme odpovídající politiky zajištění dostupnosti

3. Využívejme optimální nástroje pro dosažení daných parametrů obnovy

4. Udržme však rozumný/kontrolovatelný počet jak nástrojů, tak politik

5. Zvažme, zdali jsme schopni výše uvedené efektivně zrealizovat vlastními silami

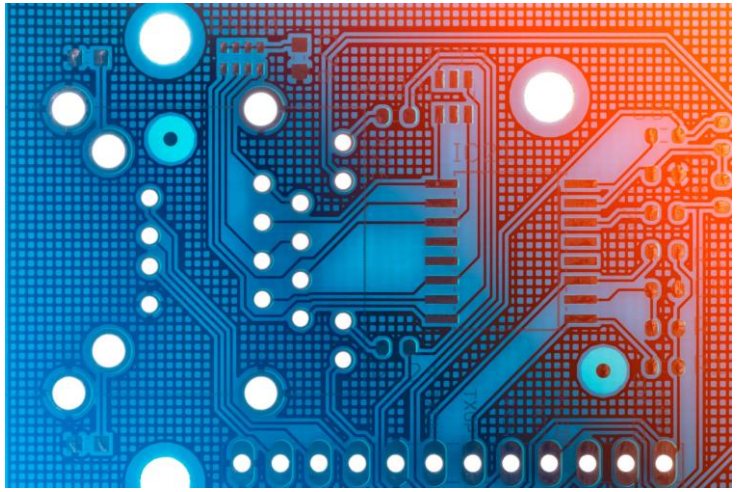
GAPP SYSTEM

Část II.

STRATEGIE V KONTEXTU TECHNOLOGIÍ

Zálohování a technologie v roce 2023

- Zálohované platformy a systémy
  - **Tradiční**
    - Bare metal OS
    - Databáze, aplikace
    - NAS systémy
  - **Moderní**
    - Hypervisory
    - K8s
    - Objektová úložiště
    - Veřejné cloudy
  - **Hybridní prostředí**
    - Any-to-any přístup
- Technologie pro efektivní zálohování dat



Funkce klasického zálohování na konci 20. století

- Obnova z fyzické chyby
  - Ztráta lokality -> obnova ze záloh (z pásky)
  - Ztráta serveru -> obnova ze záloh (z pásky)
  - Vadný pevný disk -> obnova ze záloh (z pásky), příp. RAID
- Obnova z logické chyby
  - Poškození dat v souborovém systému -> obnova ze záloh (z pásky)
  - Poškození integrity dat v databázi -> obnova ze záloh (z pásky)
  - Návrat k předchozím verzím souborů -> obnova ze záloh (z pásky)

Zálohování dnes

- Obnova z fyzické chyby
  - Ztráta lokality -> automatický failover (HA, SRM, …)
  - Ztráta serveru -> automatický failover (HA, SRM, …)
  - Vadný pevný disk -> RAID svazky
- Obnova z logické chyby
  - Poškození dat v souborovém systému -> předchozí verze, snapshoty (VSS)
  - Poškození integrity dat v databázi -> snapshoty (rollback)
  - Návrat k předchozím verzím souborů -> předchozí verze, snapshoty (VSS)

- **Klasické zálohování se stalo záchranou poslední instance – nástrojem, ke kterému se upíráme pokud vše ostatní selže.**

GAPP SYSTEM

Co si představujeme pod termínem zálohování dat?

- **Zálohování dat v širším pojetí** = ucelená strategie vypořádání se s rizikem nedostupnosti provozovaných systémů aplikací, případně s rizikem ztráty nebo poškození dat

- **Zálohování dat v užším pojetí** = řešení poslední záchrany, když všechny ostatní nástroje selžou

Jak poskládat optimální strategii zajištění dostupnosti

GAPP SYSTEM

Výběr vhodného nástroje podle typu chyby

	Typický vznik chyby	Rozsah projevu chyby	Jak dosáhnout nízkého RTO?	Jak dosáhnout nízkého RPO?
Fyzická chyba	Ztráta DC Pád serveru	Nefunkční systém bez ztráty dat Kompletní ztráta dat	Synchronní zrcadlení Transparentní failover Geograficky distribuované řešení	Synchronní zrcadlení
Logická chyba	Chyba v SW Smazání dat Poškození dat	Většinou selektivní – soubor, adresář, část databáze, souborový systém	Přímo přístupná zálohovaná data Automatizace obnovy	Kontinuální zálohování
Kombinovaná chyba	Kombinace různých chyb Záměrný útok	Kompletní ztráta dat	Přímo přístupná zálohovaná data Automatizace obnovy	Kontinuální zálohování

GAPP SYSTEM

Zařízení pro uložení zálohovaných dat

- 20. století
  - Samostatné páskové mechaniky (DAT, DLT, AIT, LTO, IBM TS - Jaguar, STK T10000)
  - Páskové knihovny
  - Pásková sila
- 21. století
  - Optimalizované diskové systémy (s deduplikací dat)
  - Appliance based zálohování (zálohovací server a úložiště v jednom)
  - Páskové knihovny a sila pro archivní data a dlouhodobě udržované zálohy (LTO)
  - Cloudová úložiště

Model přenosu zálohovaných dat

- Klasické modely zálohování dat
  - Model klient-server-úložiště
  - Model klient-server/klient-proxy-úložiště
  - Model kontinuálního zálohování
- Moderní modely zálohování dat
  - Distribuovaný model zálohování dat
  - Deduplikace dat v procesu zálohování (na cíli, na zdroji)

Efektivní přenos dat
mezi servery
a úložištěm
zálohovaných dat

Část III.

JAK ZAČÍT SNADNO A RYCHLE

Zjednodušený přístup k volbě nástrojů

Aplikace	Komponenty	Závislosti	RTO	RPO
Aplikace 1	vSphere servery Virtuální server ABC1 SQL databáze DEF1 Web server GHI1	DNS Active Directory Load balancer	1 hodina	max. jednotky minut
Aplikace 2	vSphere servery Virtuální server ABC2 SQL databáze DEF2	DNS	1 den	max. jednotky hodin
Aplikace 3	…			
Aplikace 4	…			
Aplikace 5	…			

Jaké nástroje zvolit?

- Kritéria pro volbu vhodného nástroje
  - Dle RTO/PRO
  - Dle požadované míry automatizace
  - Dle geografických charakteristik prostředí
  - Dle objemu dat

- Příklady
  - RTO = 1 hodina -> vyžaduje **replikaci dat, snapshoty** a automatizaci
  - RTO = 1 den -> řešitelné klasickým zálohováním podle rozsahu
  - RPO = 0 -> vyžaduje **synchronní zrcadlení dat**
  - RPO max. minuty -> vyžaduje nějakou formu **replikace dat a snapshotů**

Část III.

DISKOVÁ POLE, REPLIKACE A SNAPSHOTY

Uložení dat na diskových polích

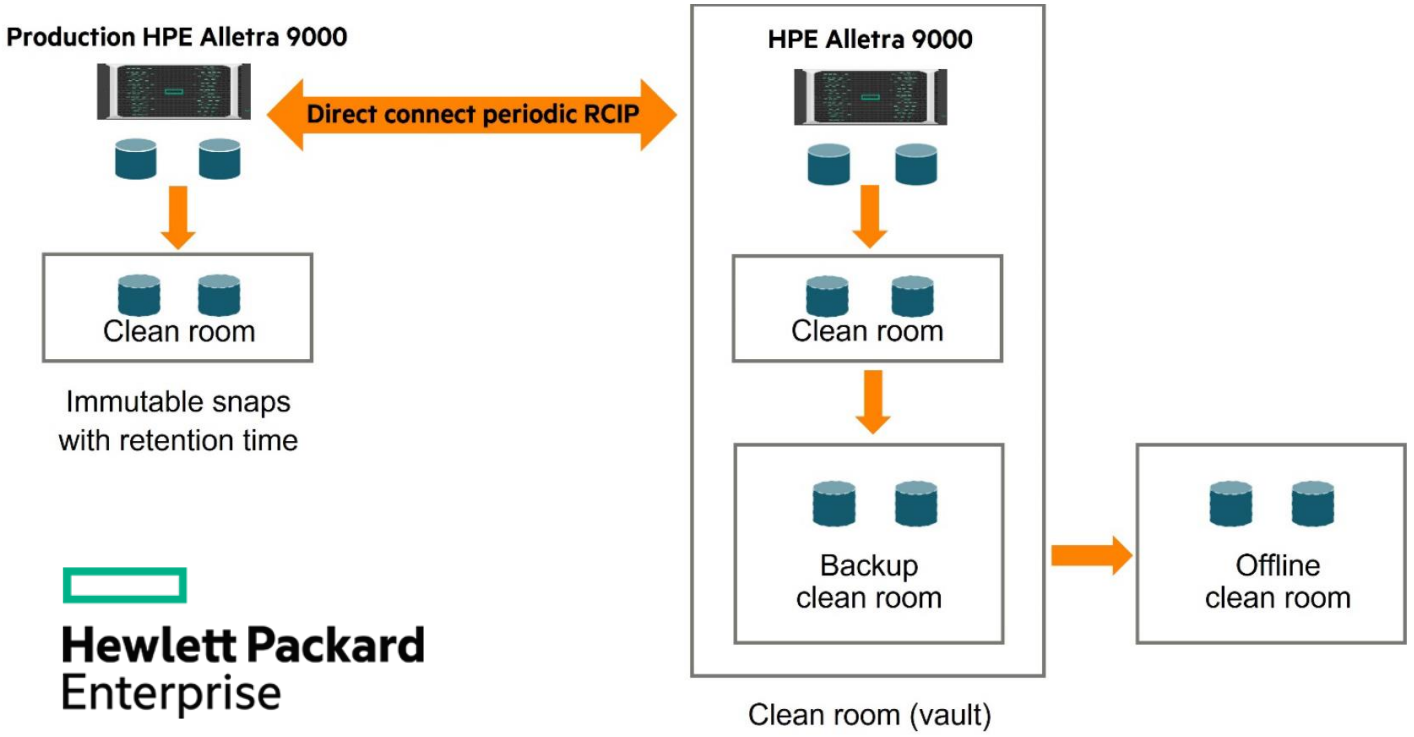
- Základní charakteristika
  - Svazky jsou přístupné serverům na blokové úrovni (přes FC, iSCSI, SAS, …)
  - Souborový systém je spravován serverem
  - V případě napadení serveru jsou zašifrovány postupně všechny k němu připojené svazky

- Nejběžnější dostupné funkce zabezpečení dat
  - **Zrcadlení a replikace** – synchronní a asynchronní
  - **Automatizovaný failover** mezi diskovými poli
  - **Snapshoty** (časové snímky) a klony

Zrcadlení a replikace proti ransomware neochrání!

HPE Virtual Lock

- Optimalizované zabezpečení proti výmazu snapshotů na diskových polích HPE
- Každý Virtual Lock snapshot má definovanou min. dobu retence
- Po tuto dobu není možné snapshot odstranit nebo změnit



Pokračování po přestávce …

Petr Dvořák
petr.dvorak@gapp.cz
+420 602 150 352