Kapitola 11

Zálohování

Po prostudování kapitoly budete umět:

- popsat smysl, důvod a účel tvorby zálohovacích systémů;
- vysvětlit rozdíly mezi zálohováním a uložením (dlouhodobým uložením) dat;
- vysvětlit architekturu RAID a účel využívání systémů RAID;
- uvést technologické prostředky používané při zálohování a ukládání dat;
- uvést základní požadavky při zabezpečení uložených citlivých dat;
- popsat proces při řízení kontinuity business procesů.

Klíčová slova:

RAID, zálohování, ukládaní, BCP, DRP havarijní plány.

11.1 Úvod

Většinou problematiku zálohování dat vnímáme jako ad hoc vytváření kopií dat na samostatný datový nosič pro případ ztráty v původním úložišti. Tento přístup lze aplikovat při správě dat na osobním počítači.

V případě informačních systémů a tím více podnikových informačních systémů musí být řešení záloh komplexní a systém záloh musí zejména zajistit

- aktuálnost záložních dat
- operativnost a dostupnost při práci se zálohami
- zabezpečení integrity a autentičnosti zálohovaných dat (v případě citlivých dat i důvěrnost)
- oprávnění přístupu

Zálohování dat musí být řešeno proaktivně a systémy zálohování musí být nedílnou součástí procesů v informačních systémech.

Zálohování dat je úzce propojeno se systémy ukládání (dlouhodobého ukládání) dat. Z tohoto pohledu je také třeba při návrhu systému zálohu tak přistupovat. Zejména u velkých informačních systémů může způsobit kolaps, neboť zpracovávané informace mohou být ztraceny:

- neúmyslnou nebo úmyslnou chybou člověka – člověk může soubory omylem smazat, přepsat, vyvolat chybu programu pro manipulaci s uloženými daty,
- chybou operačního systému – operační systém může svojí chybou způsobit přepsání některé důležité části média,
- přírodní pohromou – povodeň,
- škodlivým SW,
- zničením médií.

11.2 Architektura záložních systémů, návrh RAID

Zálohování na FTP server Zálohování na FTP (File Transfer Protocol) server poskytuje bezpečný způsob ukládání, vzhledem k možnosti uložení dat na zcela oddělené místo od zdrojových dat. Tento

způsob zálohování má však nízkou úroveň zabezpečení ukládaných dat, vzhledem k hrozbám manipulace s těmito daty během přenosu.

Online zálohování. Jedná se o metodu nahrávání dat přes internet do externího úložiště s pomocí zálohovacího softwaru od poskytovatele online služby. Soubory jsou kdykoliv k dispozici a můžeme je opět obnovit a použít.

Hlavní **výhodou** je uložení dat v jiné lokalitě, čímž je zajištěna vyšší ochrana dat proti možnému zničení záloh v důsledku požáru, povodní a jiných živelných pohrom. situací. **Nevýhody** spočívají v nutnost vysokorychlostní komunikace a delší doba uložení velkých objemů dat. připojení k internetu a delší doba nahrávání většího objemu dat. Další nevýhodou je možnost neoprávněného přístupu k datům třetí osobou., čemuž je nutné se bránit zašifrováním přenášených dat.

Software – základní podmínkou při návrhu systému zálohovaní je možnost pravidelného zálohování, tj. nutné zajistit v pravidelných intervalech ukládání záložní kopie.

Technologie RAID. Pro vytvoření záloh lze použít i RAID, což je zkratka z anglického Redundant Array of Independent Disks, (vícenásobné diskové pole nezávislých disků). Jedná se o metodu zabezpečení dat proti selhání pevného disku, na kterém jsou ukládána data. Metoda spočívá v ukládání dat na více nezávislých discích, které jsou propojeny tak, že ukládaná data jsou v případě selhání jednoho z nich zachována.

11.3 Systém zálohování dat

Způsoby zálohování a výběr vhodného typu vytváření záloh je závislá na mnoha aspektech.

Volba systému zálohování musí vycházet z výsledků analýzy, a to v některých případech i provedené analýzy rizik. Zvolený systém zálohování, který je často spojen i se systémem ukládání dat, takže při volbě způsobu, metody a systému zálohování je třeba zvážit:

- Objem zálohovaných dat.
- Charakter zálohovaných dat (citlivá, publikovatelná, systémová aj.).
- Frekvence a aktualizace zálohovaných dar.
- Offline nebo online zálohování.

Po vymezení požadavků na zálohování je třeba zajistit příslušný SW, HW, který bude schopen zálohovat požadovaná data. V případě zálohování dat lze využít:

Technologické prostředky

Páskové mechaniky. Pro zálohování velkého množství dat v informačních systémech lze použít páskové mechaniky. Tyto prostředky jsou též využívané a doporučované pro dlouhodobé ukládání dat. Provedené testy prokázaly, že digitální záznam na páskovém médiu vydrží minimálně 20 let.

REV mechaniky. REV mechanika je zálohovací systém, který využívá k zálohování výměnné pevné disky umístěné ve speciálních kazetách. Disky jsou vybaveny dvouúrovňovou ECC kontrolou chyb. Provedené testy prokázaly minimální dobu, po kterou jsou REV mechaniky schopny uchovat data na 30 let.

Zálohování a dlouhodobé uložení citlivých dat

Zálohování a dlouhodobé ukládání citlivých dat vyžaduje realizaci zabezpečeného úložiště, kde je třeba zaručit zachování integrity dat a jejich důvěrnosti a dostupnosti.

Nastavená bezpečnostní opatření ve vztahu k ochraně dat musí podléhat požadavkům stanoveným v bezpečnostních normách ČSN ISO/IES řady 27000, v případě technologického řešení pak normě ČSN ISO/IEC 15408. Tyto požadavky musí být podloženy výsledky zpracované analýzy rizik a dokumentovány vnitřními směrnicemi.

V případě dlouhodobého ukládání dat, musí být data převáděna do odpovídajících formátů.

Například elektronické dokumenty se do úložiště ukládají ve formátu PDF/A, který umožňuje integraci dat při ověřování integrity využívající elektronické podpisy.

Vzhledem ke kontinuální kontrole integrity elektronického dokumentu musí v úložišti integrovány funkcionality automatizované kontroly integrity.

Celý systémový přístup, resp. mechanismy zajištění bezpečnosti ukládaných dat musí zaručit, že v případě uložení dat do tohoto úložiště nemůže dojít k jejich ohrožení či poškození (k narušení integrity nebo k úplnému zničení).

11.4 Nastavení kontinuity procesů podnikového informačního systému

Při zabezpečení provozu informačního systému je důležitým aspektem postihnout i případy nestandardních situací. Je nutné počítat s možnými havarijními situacemi, kdy podnikový informační systém může zajišťovat pouze částečný provoz nebo být úplně mimo provoz, čímž jsou narušeny i business procesy podniku. Vzhledem k tomu, že jedním z nejdůležitějších parametrů zpracovávaných da je jejich dostupnost, je třeba mít připraveny procesy, zajistí kontinuitu informačních technologií.

BCP (Business Continuity Plan – plán kontinuity činností). Pro případ jakékoliv havárie musí mít podnik vypracovaný řídící proces, který v případě identifikace nestandardní situace, vyhodnotí možné dopady a aktivuje takové postupy a opatření, které umožní zajistit kontinuitu a obnovu klíčových procesů a činností podniku na minimální úroveň činností, které zajistí kontinuální zajištění business aktivit.

Pro jednotný přístup k řešení této problematiky je třeba vycházet z doporučení bezpečnostních norem ČSN ISO/IEC řady 27000.

DRP (Disaster Recovery Plan – plán obnovy po havárii). Lze říci, že DRP je podmnožinou BCP, neboť zpracované procesy směřují přímo k obnově činnosti technologických prostředků. Jedná se opravu, či výměnu technologických komponent – HW i SW i využití náhradních zdrojů. Zde je nutné zdůraznit, že nelze na úkor rychlé obnovy technologického parku snížit úroveň ochrany zpracovávaných informací. Z tohoto důvodu jsou proces DRP posuzovány v rámci analýzy rizik.

11.5 Havarijní plány

Havarijní plán musí postihnout celé spektrum činností (od organizační struktury havarijního výboru až po činnosti realizované v rámci DRP). Hlavním cílem zpracovaného havarijního plánu je, na základě zjištěných skutečností, nastavit priority činnosti, které je třeba řešit k zajištění minimalizace ztrát. Z tohoto důvodu jsou v rámci zpracování havarijního plánu připraveny různé scénáře, které mohou pokrýt případy s největší pravděpodobností výskytu. Bezprostředně na havarijní plán navazuje plán obnovy.

V kapitole je rozebrán smysl, důvod a účel tvorby zálohovacích systémů. Je zde uvedena architektura zálohovacích systémů. Jsou zde nastíněny rozdíly mezi zálohováním a uložením (dlouhodobým uložením) dat a uvedeny technologické prostředky používané při zálohování a ukládání dat. Samostatnou část tvoří realizace požadavků při zabezpečení uložených citlivých dat. Je zde vysvětlena architektura RAID a účel využívání systémů RAID. Závěrečnou část kapitoly tvoří popis způsobů řízení kontinuity business procesů v nestandardních situacích.

1. Popište architekturu využívaných záložních systémů.
2. Co znamená pojem RAID?
3. Vysvětlete rozdíly mezi DRP, BCP a havarijním plánem.
4. Co je třeba zajistit při uložení citlivých dat?

Literatura k tématu:

[1] SMEJKAL, V., RAIS, K. *Řízení rizik ve firmách a jiných organizacích.* 4., aktualizované a rozšířené vydání. Praha: GRADA, 2013, 488 str., ISBN 978-80-247-4644-9.