

**Česká zemědělská univerzita v Praze**

**Provozně ekonomická fakulta**

**Katedra Informačních technologií**



**Bakalářská práce**

**Zálohování a archivace dat**

**Jan Močko**

© 2021 ČZU v Praze

# ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

## ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Jan Močko

Informatika

Název práce

**Zálohování a archivace dat**

Název anglicky

**Data backup and archivation**

---

### Cíle práce

Cílem této práce je navrhnout efektivního řešení zálohy a archivace dat na základě daných kritérií pro cílovou skupinu.

Dílčím cílem je porovnání všech možností, zhodnocení výhod, nevýhod a možných příležitostí, ze kterých mohou společnosti benefitovat při správném využití.

### Metodika

Metodika bakalářské práce spočívá v nastudování odborné tištěné literatury a ověřených internetových zdrojů o archivaci a zálohování dat. Analýza problematiky a následné poznatky jsou zpracovávány do praktické části vymyšlení strategie pro společnost dle možných požadavků, včetně závěrečné SWOT analýzy u vytvořených řešení.

**Doporučený rozsah práce**

35-45s.

**Klíčová slova**

raid, úložiště, cloud, archivace, zálohování, NAS, komprese, duplikace, šifrování, ztráta

---


**Doporučené zdroje informací**

B LITTLE, David. CHAPPA, David. Implementing Backup and Recovery: The Readiness Guide for the Enterprise 1st Edition. New York: Wiley, 2003. ISBN 978-0471227144.

Internetové zdroje.

KŘÍŽ, Libor. Komprimační a archivační programy. COMPUTER PRESS, 2002. ISBN 80-7226-757-4

PECINOVSKÝ, Josef. Archivace a komprimace dat. Grada, 2003. ISBN 80-2470-659-8.



---

**Předběžný termín obhajoby**

2021/22 LS – PEF

**Vedoucí práce**

Ing. Martin Havránek, Ph.D.

**Garantující pracoviště**

Katedra informačních technologií

---

Elektronicky schváleno dne 13. 8. 2021

**doc. Ing. Jiří Vaněk, Ph.D.**

Vedoucí katedry

---

Elektronicky schváleno dne 5. 10. 2021

**Ing. Martin Pelikán, Ph.D.**

Děkan

V Praze dne 29. 12. 2021

## **Čestné prohlášení**

Prohlašuji, že svou bakalářskou práci "Zálohování a Archivace dat" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu použitých zdrojů na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 15.3. 2022

---

## **Poděkování**

Rád bych touto cestou poděkoval vedoucímu své bakalářské práce, panu Ing. Martinu Havránkovi Ph.D. za odborné vedení a cenné rady, které mi během zpracovávání bakalářské práce poskytoval. Mé poděkování patří taktéž panu Oliveru Friesovi za spolupráci při získávání informací pro zpracování praktické části. V neposlední řadě děkuji mým blízkým, kteří mi pomohli s gramatickou korekturou práce.

## Obsah

1.	Úvod.....	11
2.	Cíle práce a metodika .....	12
2.1.	Cíle práce .....	12
2.2.	Metodika .....	12
3.	Zálohování.....	13
3.1.	Proč zálohovat .....	13
3.2.	Co zálohovat .....	14
3.2.1.	Záloha disku.....	14
3.2.2.	Záloha oddílu .....	14
3.2.3.	Záloha systému .....	14
3.2.4.	Záloha adresářů .....	15
3.2.5.	Záloha Outlooku .....	15
3.2.6.	Záloha partition .....	15
3.3.	Plánování zálohy dat .....	16
3.4.	Ztráta dat a jejich příčiny.....	16
3.5.	Úložná média .....	18
3.5.1.	Magnetické pásky .....	18
3.5.2.	Pevné disky.....	19
3.5.3.	NAS.....	20
3.5.4.	Optický disk .....	20
3.5.5.	Disketa.....	21

3.5.6.	Další paměťová média (USB flash, Paměťové karty) .....	21
3.5.7.	Vzdálená zálohovací služba – Cloud.....	22
3.6.	Architektury síťového ukládání dat .....	23
3.6.1.	DAS.....	23
3.6.2.	NAS.....	24
3.6.3.	SAN.....	24
3.7.	Úložný cluster .....	25
3.8.	Historie clusterů.....	25
3.9.	Typy zálohování .....	26
3.9.1.	Plná záloha.....	26
3.9.2.	Inkrementální – Přírůstková záloha .....	27
3.9.3.	Diferenciální – rozdílová záloha.....	27
3.10.	RAID pole .....	28
3.10.1.	JBOD.....	29
3.10.2.	RAID 0 .....	29
3.10.3.	RAID 1 .....	30
3.10.4.	RAID 5 .....	30
3.10.5.	RAID 6 .....	31
3.11.	Rotace záloh .....	32
3.11.1.	Round robin (Schéma s jednou páskou každý den).....	32
3.11.2.	Grandfather-father-son .....	33
3.11.3.	Tower of hanoi .....	34

4.	Archivace.....	35
5.	Vlastní zpracování .....	36
5.1.	Specifikace .....	37
5.2.	Prerekvizity zálohování .....	37
5.3.	Zálohování v korporátním prostředí.....	41
5.3.1.	Požadavky (korporát).....	42
5.3.1.1.	Finanční náročnost .....	42
5.3.1.2.	Výkonnost a velikost úložiště.....	42
5.3.1.3.	Zabezpečení .....	43
5.3.2.	Návrh řešení (korporát).....	43
5.4.	Střední firma / Malá společnost .....	52
5.4.1.	Požadavky (Střední/Malá společnost) .....	53
5.4.1.1.	Finanční náročnost .....	53
5.4.1.2.	Výkonnost a velikost úložiště.....	53
5.4.1.3.	Požadavky na zabezpečení.....	54
5.4.2.	Návrh řešení (Střední/Malá společnost) .....	54
5.5.	Domácnost.....	59
5.5.1.	Požadavky (Domácnost).....	59
5.5.1.1.	Finanční náročnost (Domácnost).....	59
5.5.1.2.	Výkonnost a velikost úložiště (Domácnost).....	59
5.5.2.	Návrh řešení (Domácnost).....	60
6.	Závěr .....	61



<b>7.</b>	<b>Seznam použitých zdrojů .....</b>	<b>67</b>
<b>8.</b>	<b>Zdroje sběru dat .....</b>	<b>68</b>
<b>9.</b>	<b>Obrázky .....</b>	<b>69</b>
<b>10.</b>	<b>Seznam tabulek .....</b>	<b>69</b>

# Zálohování a archivace dat

---

## Data backup and archiving

### Souhrn

Tato bakalářská práce se věnuje tématu zálohování a archivace dat. V první, teoretické části pojednává o rozlišení zálohování dat od archivace, o typech a metodách zálohování dat, o médiích nebo službách, které k záloze můžeme používat, příčiny ztráty dat, kdy a jak komprimovat data a dle jakých kritérií bychom měli rozhodovat při výběru zálohování pro různé cílové skupiny (např. Malá/střední firma, domácnost apod.) Dále se bude věnovat pohledům na postupy při vybírání strategie zálohování pro malou/střední firmu. Druhá část se bude věnovat vymyšlení strategie zálohování pro malou/střední firmu v soukromém sektoru. Vytvoření více možných řešení a porovnávání dle SWOT analýzy. V závěrečné rozpravě je pojednáno o jednotlivých silných a slabých bodech řešení a doporučení v jakých situacích vybrat jednotlivá řešení.

**Klíčová slova:** Raid, Úložiště, Cloudová úložiště, Archivace, Zálohování, NAS, Komprese, Duplikace, Šifrování, ztráta

### Summary

This bachelor thesis deals with the topic of data backup and archiving. The first, theoretical part deals with possible solutions of data backup from archiving, the types and methods of data backup, the media or services we can use for backuping our files, the causes of data loss, when and how to compress data and according to our expectations we had to decide on backup for various target groups (eg small / medium business, household, etc.) They will also respect the views on the procedures for selecting a backup strategy for a small / medium business. The second part will focus on devising a backup strategy for a small / medium business in the private sector. Creating more possible solutions and comparisons according to SWOT analysis. The final part of thesis discusses the individual strengths and weaknesses of the solution and the recommendation to select individual solutions in most situations.

**Key words:** RAID, Storage, Cloud, Archivation, Backup, NAS, Compression, Duplication, Decryption, Loss

# 1. Úvod

Žijeme v době, kdy jsme obklopeni technologiemi na denním pořádku. Téměř všechna zařízení sbírají data. Některá zařízení sbírají data absolutně zanedbatelná a nepotřebují jej uchovávat, naopak některá jsou velmi důležitá a s nadsázkou řečeno na nich závisí něčí životy. [20]

Ukládání dat na interní úložiště je naprosto běžná záležitost téměř veškerých zařízení. Úložiště nám způsobuje to, že každý den nemusíme například znovu vytvářet soubory, které jsme již jednou vytvořili. [20]

Představte si však, že jste pracovník top managementu a závisí na Vás chod společnosti z finančního hlediska. Pracujete půl roku na velmi důležitém projektu, který Vám může zajistit podepsání smlouvy s velmi významným zastupitelem na trhu. Vše je téměř dokončeno, když však z ničeho nic nenastartujete Váš pracovní laptop a po analýze firemního IT pracovníka zjistíte, že se jedná o disk, který vypověděl službu a data na kterých jste pracoval/a jsou pryč. Deadline se blíží, ale již nikdy nestihneme dát dohromady půl roční práci za dva týdny a hrozí nám úpadek firmy a vyhazov. [20]

Kdyby však byla v této firmě zajištěna forma automatického nebo případně manuálního zálohování dat, tak by scénář místo depresivní situace probíhal ze začátku podobně jako v prvním scénáři, ale po zjištění závady pevného disku by Vám technik disk vyměnil a po obnovení dat byste mohli spokojeně pokračovat dál ve své práci. [20]

Zálohování dat v dnešní digitální době nemusí vždy být žádná vysoce nákladná záležitost. K dispozici existuje mnoho různých metod a médií, jak a na která lze zálohovat, případně archivovat data. Přičemž každá metoda a každé médium má různé výhody a nevýhody. Výběr by měl být tudíž učiněn s rozvahou a strategií: “Proč, kdy, jak a (za kolik)”. Tyto otázky jsou také využity ve zpracování praktické části této práce, berme je tedy jako řečenou “Svatou trojici (čtveřici)”. [20]

Zálohování není však jen zdaleka záležitost pracovního prostředí. Zálohování dat je určitou jistotou, že svá data neztratíme. A to dle našich preferencí... ať už dočasně, nebo v nedohledném horizontu... při nedohledném horizontu a delšího časového úseku s nečastým využíváním dat však budeme mluvit spíše o archivaci. [20]

## **2. Cíle práce a metodika**

### **2.1. Cíle práce**

Hlavním cílem této práce je navrhnout efektivní řešení zálohy a archivace dat na základě daných kritérií pro cílovou skupinu. Dílčím cílem je porovnání všech možností, zhodnocení výhod, nevýhod a možných příležitostí, ze kterých mohou společnosti benefitovat při správném využití.

### **2.2. Metodika**

Metodika bakalářské práce spočívá v nastudování odborné tištěné literatury a ověřených internetových zdrojů o archivaci a zálohování dat. Analýza problematiky a následné poznatky jsou zpracovávány do praktické části vymyšlení strategie pro společnost dle stanovených požadavků, včetně závěrečné SWOT analýzy u vytvořených řešení.

### 3. Zálohování

Zálohování je proces vytváření kopie dat, které máme uložené například na pevném disku svého počítače. Pro uskutečnění tohoto procesu je zpravidla potřeba druhé médium nebo služba, kam se naše data odesílají, aby byly v bezpečí a nezůstaly pouze originálem, který při poškození může navždy zmizet. Po uskutečnění zálohy dat si můžeme kdykoliv vcelku svižně obnovit naše data nejen na našem zařízení. Tuto zálohu lze u různých médií přenášet mezi zařízeními a nemusíme být závislí jen na našem hardwaru, například v případě poškození. [20]

V případě zálohy u masivnějšího množství dat se může používat specializovaný software. Existuje více různých softwarů tohoto typu závislých na operačním systému, který tento proces zajišťují. Software však není jediná pomůcka zálohování, důraz je kladen také na specializovaný hardware, který je používán převážně u většího množství dat a není běžnou součástí domácího desktopu. Tento hardware zpravidla funguje automatizovaně či poloautomaticky. [20]

V moderní době je často využíváno více a více komplexnějších způsobů zálohování disků. Nejedná se tudíž, s úsměvem řečeno, o kopírování dat na flash disky. Jedná se o efektivní zálohování mnoha počítačů, které jsou propojené napříč počítačovou sítí nebo naopak na tyto počítače můžeme data zálohovat. Toto propojení se nazývá úložný cluster. [20]

#### 3.1. Proč zálohovat

Důvody se zdají být prosté-záchrana dat při ztrátě. Argumentů je však více. Díky tomu, že správně nastavíme systém zálohování získáme:

- Odstranění nebezpečí ztráty dat.
- Data díky zálohování získávají svoji repliku na více perifériích a nejsou uložena jen na jednom místě. Díky tomuto stavu jsme schopni data obnovit zpět v případě, že dojde k poškození.
- Komfort a časovou úsporu díky ztrátě povinnosti tvorby manuální zálohy.
- Soubory je možné tímto způsobem verzovat (jsou zpětně dostupné v čase, v jednotlivých verzích).

## **3.2. Co zálohovat**

### **3.2.1. Záloha disku**

Záloha disku znamená, že celý disk a jeho obsah je zálohován společně s instalovaným operačním systémem, aplikacemi a všemi daty. Tento typ provedené zálohy také zajišťuje provedení zaváděcího záznamu skryté části operačního systému. Po následných obnovách je tedy operační systém schopný znovu plně fungovat. [1]

### **3.2.2. Záloha oddílu**

Zálohováním oddílu disku se označuje provedení zálohy všech dat v určitém oddílu. Záloha tohoto typu také provádí zaváděcí záznam, s provedením zálohy skryté části operačního systému. Po obnově je tedy znovu schopný fungovat. [7]

### **3.2.3. Záloha systému**

Záloha systému představuje provádění záloh systému, který je plně funkční a je poté možno provést jeho obnovu do původního stavu. Většinou se dají tyto zálohy provádět pomocí softwarových nástrojů. Tyto nástroje poté vytvoří zálohy samotného systému tím způsobem, že využitím sektorové metody zazálohuje celý diskový oddíl, kterého je systém součástí. Tato záloha provede nejen zálohu systému, ale také zálohu veškerých dat, které se zrovna na tomto diskovém oddíle nacházela. Tímto způsobem je možné vypalovat I CD/DVD nebo ukládat tyto zálohy na jiné disky, či oddíly anebo dokonce na síťová úložiště [1]

Tento typ softwaru také navíc také umožňuje znovu přivést systém k životu obnovou zálohy systému na čistý disk pomocí bootovacího média. [1]

Je důležité mít na paměti, že by mělo být provedeno oddělení místa pro uložení operačního systému a pracovních dat. V případě možné havárie a následném přeinstalování systému lze tímto ošetřením ochránit svá data před ztrátou. V případě, že se v zařízení nachází vícero diskových jednotek, je vhodné vyhradit jeden jen pro operační systém a systémové soubory. Pokud se v zařízení nachází pouze jeden, je možné řešit tuto situaci rozdělením disku na více oddílů. [1]

### **3.2.4. Záloha adresářů**

Existuje spousta řešení, jak přistoupit k zálohování adresářů. Jedním z příkladů je prosté kopírování obsahu plánovanou synchronizací, zálohování adresáře s komprimací obsahu a další.

Některá softwarová řešení umožňují vytvářet zálohy, ve kterých je možné provést nastavení komprimací dat, díky kterému jsou následně soubory méně náročnější pro zvolené úložiště. [1]

Zálohy je možné taktéž vypalovat na CD a DVD. Mezi oblíbenější varianty však patří ukládání dat na lokální a externí disky nebo ukládat do síťových úložišť. [2]

### **3.2.5. Záloha Outlooku**

Pod pojmem zálohování Outlooku si ve většině případů každý představí samotnou archivaci zpráv do záložního souboru Outlooku a následné překopírování záložních souborů do nového adresáře. Tento způsob zálohování je vhodné používat v případě, že se jedná dlouhodobou archivaci emailových zpráv. Nevýhoda této metody je taková, že ty zprávy, které nebyly uloženy do zálohovacího archivu nebudou zálohovány. V případě přesunutí všech zpráv do záložního archivu, bude s nimi další práce příliš obtížná. [1]

#### **Jak vyřešit tento problém**

- Je možné používat dalšího emailového alternativního klienta. Tento klient by měl mít podporu záloh emailových zpráv.
- Pro řešení těchto potíží je taktéž možné používat různé nástroje pro zálohování Outlooku.

### **3.2.6. Záloha partition**

Tento typ zálohy spočívá v označení souborů nebo balíčku souborů, které budou mít k sobě vytvořenou svoji partition kopii. Z té jsou potom zálohy vytvářeny, včetně zálohování operačního systému, který je funkční a je zároveň obsahem této zálohy a dalších dat. Tuto zálohu lze taktéž nazvat jako „obraz diskového oddílu“. [1]

### 3.3. Plánování zálohy dat

Plánování záloh dat se řeší v takzvaném zálohovacím plánu. Tento plán pojednává o tom, jakým způsobem a v jakém časovém horizontu k datům přistupuje za účelem provádění záloh. Zálohovací plán většinou stojí na předem určených požadavcích, které určují jak často a co by mělo být zálohováno. Dalším aspektem, který je zde řešen je popsání dostupného objemu dat, které je potřeba s největší pravděpodobností zálohovat, bez omezení důležitých aspektů IT infrastruktury. [2]

Zálohovací plány jsou v tomto případě jedním z nejdůležitějším předmětem dokumentace v oblasti ochrany dat před samotnou ztrátou, které by mohli způsobovat problémy samotné organizaci. Tyto ztráty mohou být problematické například v oblasti reputace, ekonomickými ztrátami, nebo dokonce v oblasti porušování GDPR. [2]

**Typický obsah zálohovacího plánu** *Veškerý bodový obsah je citován z [2]*

- Způsob zálohování (technologie, metoda)
- Termíny zálohování (zálohovací okna)
- Pravidla pro manipulaci s médii (bezpečnost uložení, skartace)
- Stanovení Recovery Time Objective (RTO; jak rychle je možno data obnovit)
- Stanovení Recovery Point Objective (RPO; jak staré mohou být zálohy)
- Definice odpovědností
- Testování záloh (ověření obnovitelnosti a čitelnosti)

### 3.4. Ztráta dat a jejich příčiny

Již na příkladu v úvodu bylo popsáno, jak může dojít ke ztrátě dat. Někdy však může zkolabovat aplikace, či počítač a zbyl nám například pouze poškozený dokument. V některých případech si této skutečnosti nemusíme ani všimnout. Mezi nejčastější projevy, které současně se ztrátou dat nastávají jsou tyto: [3]

- Soubor je poškozený (nelze otevřít)
- Nelze spustit počítač (Často s hláškou Missing Operating System atd.)
- Při pokusu o přístup se systém „zasekne“



- Adresář neobsahuje relevantní cestu
- Z počítače se ozývají neobvyklé zvuky
- Počítač nevidí pevný disk
- Soubory, či složky jsou nepřístupné

V každém případě lze konstatovat, že ztráta dat nastává v momentě, kdy se nemůžeme dostat k původním souborům.

Existuje spousta příčin ztráty dat. Je tedy v mnoha případech velmi těžké jednoznačně označit, která z nich by mohla tuto ztrátu způsobit. Často může nastat řetězová reakce a příčin může být mnohem více než jen jedna. Je však důležité podotknout, že samotnému zjišťování příčin je možné předejít samotným pravidelným zálohováním dat. [4]

Jak už bylo výše zmíněno, příčin může být spousta. Může se jednat o fyzické příčiny, mezi kterými mohou být např. zadřená ložiska disku, poškození samotné plotny pro záznam na disku nebo vadné sektory. Zpravidla se zde jedná o mechanické závady.

Existují však případy, kdy selhání může být způsobeno softwarově. Mezi takové příčiny patří třeba pád systému, infikace viry nebo poškození samotného systému souborů. Tyto situace jsou většinou následkem lidských chyb nebo softwarů, který byl lidmi nainstalován. Je zde taky důležité podotknout, že se může jednat o neočekávané přírodní vlivy. Tyto situace však spadají zpravidla pod fyzická poškození. Mezi taková patří třeba ještě požáry, setkání s vodou nebo zásahy elektrickým proudem. [4]

#### **Fyzikální**     *Veškerý bodový obsah je citován z [4]*

- vadný sektor na disku
- zadřená ložiska, vadný motor
- poškozené záznamové plotny disku
- pád, náraz, otřesy, časté změny teploty (hlavně u notebooků)
- utržené čtecí hlavy
- nadměrná teplota nebo prašnost
- přepětí, elektrostatický výboj, výpadek napájení
- vadná elektronika

- výrobní vada
- zásah elektrickým proudem
- požár
- povodeň, vniknutí kapaliny

**Softwarové** *Veškerý bodový obsah je citován z [4]*

- poškození souborového systému
- pád operačního systému
- smazání, přepsání, formátování dat
- nákaza virem
- chyba nebo kolaps operačního systému nebo aplikace
- přepsaná servisní data

Zmíněným příčinám zdaleka není konec. Existuje mnoho příčin selhání a lze konstatovat, že každé takovéto selhání je něčím specifické a unikání, protože jej předchází různé scénáře. V nejlepším případě dojde k rozpoznání příčin a při správném procesu záchrany, mohou být data obnovena včas. [4]

## **3.5. Úložná média**

### **3.5.1. Magnetické pásky**

Magnetická páska, ač velmi archaické, tak stále velmi oblíbené a výhodné zařízení v oblasti zálohování dat. Jedná se o pevné médium, které je sestaveno z magnetické vrstvy na plastické pásce. Stejně, jaké jsou známy u starých audiokazet a videokazet. Používá se často v různých datových úložištích a mainframech.

Nejsilnější stránkou Magnetických pásek je spolehlivá dlouhá životnost, cena a velikost úložiště. Využívají se však spíše pro archivaci, protože sice poskytnou velké úložiště, ale mnohem pomalejší čtení a zápis.

Na trhu se vyskytují pouze dva výrobci – Fujifilm a Sony. A i při této nízké konkurenci se dostává páskám mnoho prostoru pro vývoj. Do konce roku 2030 bychom mohli očekávat

Magnetické pásky s velikostí úložiště až 400TB na jednotku. V současnosti se pohybujeme okolo 12 TB na pásku. [5]

### **3.5.2. Pevné disky**

Pevné disky patří mezi nejznámější médium, se kterým se může běžný uživatel setkat. Slouží k ukládání dat a následnému zálohování v počítači, notebooku a dalších zařízeních. Existuje více variant Pevných disků. [6]

Interní disky, které jsou při používání součástí počítače a nachází se ve skříní „na pevno“. Zpravidla jej nevyjímáme, protože mimo uložená data a aplikace často nese i operační systém v případě, že se jedná o jediný disk, který zařízení využívá. [6]

Externí pevné disky jsou užitečné k ukládání dat, které nemusí být nutně neustále k dispozici. Dále jsou užitečné jako zálohovací médium. Mezi data, která běžný uživatel zpravidla ukládá, patří například fotky, filmy, hudba a důležité dokumenty. Konektivita je řešena většinou přes USB port. [6]

Pevné disky dále dělíme na dvě kategorie. Jedná se však o velmi důležitý parametr. První a starší typy pevných disků jsou tzv. HDD (Hard disk drives), druhou kategorií jsou SSD (Solid state drives).

HDD má fyzické točící se disky, kde jsou data uložena magneticky. HDD v sobě obsahuje rameno s vícero „hlavicemi“, které dokážou číst a zapisovat data na disk. Oproti novějším SSD jsou HDD starším řešením a patří mezi levnější média. Jsou užitečná pro data, které není potřeba číst velmi rychle, protože oproti SSD je jejich čtení mnohem pomalejší. U velikostí 3.5 palce se zpravidla jedná o 7200 otáček za minutu. U menších 2.5 palcových, které jsou většinou používané u laptopů, je rychlost otáček 5200 za minutu.

SSD nemá žádné mechanicky hýbající se součásti. V SSD jsou data ukládána v integrovaných obvodech. Tento rozdíl má mnoho důsledků, hlavně v oblasti velikosti a výkonu. Díky absenci rotujícího disku se mohou SSD mnohonásobně zmenšit až do velikosti žvýkačky (známo jako M.2 form factor) nebo dokonce do tak malého rozměru jako je poštovní známka. Díky velikosti jsou

vhodné zejména pro menší laptopy a 2v1 zařízení. SSD disky dramaticky zkracují přístupovou dobu, protože uživatelé nemusí čekat na spuštění rotace disku.

SSD disky jsou dražší než HDD v přepočtu na kapacitu úložiště (v gigabajtech (GB) a terabajtech (TB)), ale rozdíl se zmenšuje, protože ceny SSD klesají rychlejším tempem než ceny HDD rok od roku. [6]

### **3.5.3. NAS**

Network-attached storage (NAS) je vyhrazené úložiště souborů, které umožňuje více uživatelům a heterogenním klientským zařízením získávat data z centralizované diskové kapacity. Uživatelé v místní síti (LAN) přistupují ke sdílenému úložišti prostřednictvím standardního ethernetového připojení. [7]

Zařízení NAS obvykle nemají klávesnici ani displej a jsou konfigurována a spravována pomocí nástroje založeného na prohlížeči. Každý NAS je umístěn v LAN jako nezávislý síťový uzel definovaný svou vlastní jedinečnou adresou internetového protokolu (IP). [7]

NAS vyniká snadným přístupem, vysokou kapacitou a nízkou cenou. Zařízení konsolidují úložiště na jednom místě a podporují cloudovou vrstvu a úkoly, jako je archivace a zálohování. [7]

NAS a úložné sítě (SAN) jsou dva hlavní typy síťových úložišť. NAS zpracovává nestrukturovaná data, jako je zvuk, video, webové stránky, textové soubory a dokumenty Microsoft Office. SAN jsou určeny především pro blokové ukládání uvnitř databází, známé také jako strukturovaná data. [7]

### **3.5.4. Optický disk**

Optický disk je primárně používán jako přenosné a sekundární úložné zařízení. Dokáže uložit více dat než předchozí generace magnetických paměťových médií a má relativně delší životnost. Kompaktní disky (CD), digitální univerzální/video disky (DVD) a Blu-ray disky jsou v současnosti nejběžněji používanými formami optických disků. Tyto disky se obecně používají k:

- Distribuci softwaru zákazníkům

- Ukládání velkého množství dat, jako je hudba, obrázky a videa
- Přenosu dat do různých počítačů nebo zařízení
- Zálohování dat z místního počítače

### **3.5.5. Disketa**

Diskety jsou v dnešní době již historickou záležitostí. Pro záznam je zde použita magnetická vrstva. Tato vrstva se nachází na obou stranách samotného disku. Čtení a záznam dat je proveden zařízením, které je nazýváno mechanika nebo jednotka obsahuje dvě hlavy, které se dají přirovnat těm, které jsou u magnetofonů. Tato ramena poté provádějí pohyb kolmo ke směru otáčení, čímž je způsobem zápis nebo čtení dat, která jsou uložena ve stopách. Stopy zde představují soustředěné kruhy. [8]

Původ disket započal ve skunkworks IBM pro ukládání dat v San Jose v Kalifornii. V roce 1967 začal malý tým inženýrů pod vedením Davida L. Nobleho pracovat na vývoji spolehlivého a levného systému pro načítání instrukcí a instalaci aktualizací softwaru do sálových počítačů. Velké stroje již byly vybaveny pevnými disky, které také vynalezli inženýři IBM, ale lidé používali papírové děrné štítky pro zadávání dat a programování softwaru. Tým nejprve uvažoval o použití magnetické pásky, ale pak v projektu s kódovým názvem „Minnow“ přešel na použití flexibilního mylarového disku potaženého magnetickým materiálem, který by bylo možné vložit štěrbinou do mechanismu diskové jednotky a otočit na vřetenu. [9]

„Netušil jsem, jak důležitým a rozšířeným objevem se disketa stane“ - Warren L. Dalziel, hlavní vynálezce disketové jednotky. [9]

### **3.5.6. Další paměťová média (USB flash, Paměťové karty)**

USB flash disk je zařízení používané pro ukládání dat, které obsahuje flash paměť a integrované rozhraní USB (Universal Serial Bus). Většina USB flash disků je vyjímatelná a přepisovatelná. Fyzicky jsou malé, odolné a spolehlivé. Čím větší je jejich úložný prostor, tím rychleji mají tendenci pracovat. USB flash disky jsou mechanicky velmi odolné, protože neobsahují žádné pohyblivé části. Napájení k provozu získávají ze zařízení, ke kterému jsou připojeny (obvykle počítač) přes port USB. [10]

Paměťová karta (memory stick) je typ přenosného paměťového zařízení flash, které se obvykle používá s kapesními zařízeními. Paměťové karty poprvé představila společnost Sony ve svých fotoaparátech, videokamerách a dalším vybavení pro digitální fotografii. [11]

Paměťové karty byly uvedeny na trh společností Sony v roce 1998. V roce 2010 Sony oznámila, že přidá podporu pro SD karty do nových gadgetů, což naznačuje, že Paměťové karty budou postupně vyřazeny ve prospěch SD, který byl široce přijat jinými výrobci. [11]

### **3.5.7. Vzdálená zálohovací služba – Cloud**

Cloud je virtuální prostor, který existuje na internetu. Je to úložný prostor, kam mohou lidé umístit svá data, jako je software, aplikace a soubory. Zjednodušeně tedy můžeme říct, že cloud je virtuální úložný prostor na internetu. [12]

Spousta lidí si zaměňuje cloud s internetem. Cloud je však pouze jedna část internetu a ne celá. [12]

Technologie cloud computingu umožňuje lidem využívat digitální zdroje uložené ve virtuálním prostoru prostřednictvím sítí – často satelitních sítí. Umožňuje lidem sdílet informace a aplikace přes internet bez omezení jejich fyzické polohy. [12]

Existuje mnoho cloudových služeb. Mezi ty neznámější patří:

- Microsoft OneDrive
- Google Drive
- iCloud
- Dropbox

Ukládání dat na cloud dovoluje IT oddělením řešit tři nejdůležitější požadavky.

#### **Celková cena**

U cloudových úložišť není třeba řešit žádný nákup hardwaru, nebo nadměrné nevyužití úložišť. Lze přidávat nebo odebírat kapacity na zažádání, v rychlosti změnit výkonnost, záměry

využití a platit pouze za to co bude využito. Méně využívaná data lze zařadit do kategorií dat pro která budou využívána úložiště s nižším výkonem a nižšími náklady. [19]

### **Rychlost Deploymentu**

V případě, že vývojový tým je připraven spustit novou verzi dat, stav infrastruktury by nikdy neměl být brzdícím faktorem. Cloudová úložiště dovolují IT pracovníkům v rychlosti uzpůsobit velikosti úložiště v případech potřeby. Není pak třeba se zatěžovat řešením problémů kam ukládat. [19]

### **Information Management**

Centralizované úložiště dává mnoho prostoru vytvářet a pracovat s novými uživatelskými scénáři. S užíváním životního cyklu cloudového úložiště lze vytvářet automatizace v rámci hodnocení a uzamykání dat v podpoře tzv. „compliance“ pravidel. [19]

## **3.6. Architektury síťového ukládání dat**

### **3.6.1. DAS**

DAS, dlouze direct Attached Storage patří mezi externí úložiště dat. DAS je možné připojit napřímo k vlastním serverům nebo pracovním stanicím použitím existujících komunikačních protokolů. Mezi takové komunikační protokoly patří například Advanced Technology Attachment (ATA), Serial Advanced Technology Attachment (SATA), eSATA, Small Computer System Interface (SCSI), Serial Attached SCSI (SAS) a Fibre Channel. [22]

Díky těmto protokolům se zařízení v síti nechovají jako síťová zařízení, ale jako součásti samotného počítače. Lze konstatovat, že expanduje kapacitu stanic nebo serverů při zachování vysokých datových propustností a s nízkou přístupovou dobou. Typickým chováním je sdružování jednotlivých uložišť dat, jako například u pevných disků s použitím jednoho nebo více kontrolerů. Jako rozhraní pro propojení serverů, nebo pracovních stanicí se zde používá host bus adapter. (HBA). [22]

Princip DAS je v zásadě přímočarý. Systémy DAS se staly převládajícími kvůli rostoucím požadavkům na efektivní řešení úložiště IT. Rozdíl mezi DAS a NAS (Network Attached Storage) spočívá v tom, že zařízení DAS se připojuje přímo k serveru bez připojení k síti. DAS vytváří datové ostrovy, protože data nelze sdílet s jinými servery. [13]

### **3.6.2. NAS**

Síťové úložiště (NAS) je vyhrazený server, také označovaný jako zařízení, které se používá k ukládání a sdílení souborů. NAS je pevný disk připojený k síti, používaný pro ukládání a přístupný prostřednictvím přidělené síťové adresy. Funguje jako server pro sdílení souborů, ale neumožňuje další služby (jako jsou e-maily nebo ověřování). Umožňuje přidání více úložného prostoru do dostupných sítí, i když je systém během údržby vypnutý. [14]

NAS je kompletní systém určený pro těžké síťové systémy, které mohou zpracovávat miliony transakcí za minutu. NAS poskytuje široce podporovaný úložný systém pro jakoukoli organizaci vyžadující spolehlivý síťový systém. [14]

### **3.6.3. SAN**

Storage area network (SAN) je dedikovaná datová síť, která je prostředkem pro připojování externích přístrojů k serveru (disková pole, páskové knihovny a jiná zálohovací zařízení). Důvodem vzniku SAN byla konsolidace dat a zabezpečení, na které jsou poslední dobou zvyšovány nároky. Pořizovací náklady SAN začínají na vysokých částkách, je tedy jasné, že tato zařízení jsou předmětem používání primárně ve větších společnostech s velkou potřebou dostupnosti jejich produktů a služeb a rychlou odezvou (bankovníctví, automobilový průmysl a média). SAN se však díky klesající pořizovací ceně začala používat i v menších společnostech. SAN zařízení postupně nahrazují DAS. [21]

SAN zpřístupňuje síť úložných zařízení více serverům. Zařízení SAN se serverům jeví jako připojené jednotky, což eliminuje tradiční úzká místa v síti. SAN se někdy také označují (byť redundantně) jako úložiště SAN, síť SAN, síťová SAN atd. [15]



### 3.7. Úložný cluster

Úložný cluster zajišťuje přístup k diskové kapacitě. Tato disková kapacita se dále rozkládá mezi vyšší počet zařízení abychom dosáhli co nejvyššího toku dat, taktéž nazývaného jako paralelizace toku dat. Tok dat však není jediným cílem, který má cluster zajišťovat. Tím druhým je zajištění vyšší spolehlivosti toku dat. Pro zajištění fungování níže uvedených služeb je potřeba používat speciální souborové systémy. Mezi tyto služby patří například distribuovaný mechanismus zamykání souborů, pokrytí výpadků, správné rozložení zátěže anebo pokrytí výpadků. Zálohování jako takové probíhá zpravidla ve dvou základních režimech.

- 1) V režimu Online, při kterém jde o tvorby záloh, zatímco je naše zařízení běžně využíváno, tudíž musí dbát na uživatelskou přívětivost.
- 2) V režimu Offline, kdy je zařízení nepoužíváno a je možné s ním ať už fyzicky nebo softwarově manipulovat. Ve většině případů je pro tento způsob tvoření záloh využíváno speciální médium.

### 3.8. Historie clusterů

Počátky počítačových clusterů jsou spojovány s historií prvních počítačových sítí. Počítačové clustery byly víceméně jeden z hlavních důvodů proč se spustil rozvoj sítí.

Rozsáhlou historii počítačových clusterů shrnul dle více zdrojů nejlépe Greg Pfister tehdejší pracovník IBM v jeho práci “In Search of Clusters” kde pojednává například o vzniku a původu prvních clusterů. Konkrétněji zmiňuje, že clustery nebyly vynalezeny výrobci, ale odběrateli, kteří se nedokázali uspokojit s nízkým úložištěm pro jejich práci.

Komerčně se tohoto vynálezu však chopila společnost Datapoint roku 1977. Tento produkt se nazýval ARCnet, který však samotné clustrování jako takové neposunul k rozvoji. K němu došlo až s příchodem VAXclusteru pro operační systém VAX/VMS od společnosti DEC. Na trhu se dále objevily clustrové systémy Tandem Himalaya a IBM S/390 Parallel sysplex. Ty se však oproti konkurenci, která svá zařízení představila koncem sedmdesátých let, objevily až na začátku devadesátých let.

Tyto produkty však nejen podporovaly paralelní výpočetní výkon, ale dokázaly učinit systémy souborů a periferní zařízení schopné ke sdílení. Paralelní výpočty při udržitelnosti spolehlivosti dat a jedinečnosti byly hlavním a úspěšným cílem těchto vynálezů.

Na obrázku VAX 11/780

Datum představení: 1978

Rozměry: 152.4 x 121.92 x 30 cm

Cena: \$120.000 - \$150.000



VAX 11/780 [1]

### 3.9. Typy zálohování

Existují 3 hlavní typy záloh. Diferenciální, inkrementální nebo plné zálohy je možné pro potřebu zálohování požívat. Nutností je provádět pravidelné a časté zálohování. Je však důležité zmínit, že používání každodenních plných záloh je velmi nepraktické, obzvlášť v případech, kdy společnosti disponují větším množstvím podnikových dat. Velká část uživatelů proto provádí přírůstkové nebo diferenciální zálohy po většinu pracovních dnů. [16]

#### 3.9.1. Plná záloha

Úplná metoda zálohování funguje na principu zálohování všech vybraných souborů, aniž by se bral ohled, zda došlo k jejich změně. Nazývá se též jako „zálohování kopírováním“. Na zálohovacím médiu může být poté uloženo více verzí těchto záloh za určitou dobu, přitom ale není vyloučeno, že většina souborů bude duplicitní s ostatními verzemi. Pro běžného uživatele při malém objemu dat může dostačovat, ale pro řešení zálohování ve firmách již nedostačuje. [18]

### **3.9.2. Inkrementální – Přírůstková záloha**

Další metodou zálohování je takzvaná inkrementální záloha. U tohoto typu záloh incremental jsou zálohovány pouze soubory, u kterých je přidána vlastnost „Archive“, přičemž tento atribut je u nich po zálohování odstraněn. Tímto způsobem se zálohují pouze soubory, u kterých byly provedeny změny. [16]

Zálohy tohoto typu jsou méně náročné na úložiště dat, kvůli nízké velikosti, a taktéž jsou prováděny v mnohem kratším čase. Dají se používat efektivně například při zálohování během pracovního týdne. Tento typ záloh však není dostatečný pro obnovu celého stavu. Je potřeba vlastnit všechny přírůstkové zálohy. [16]

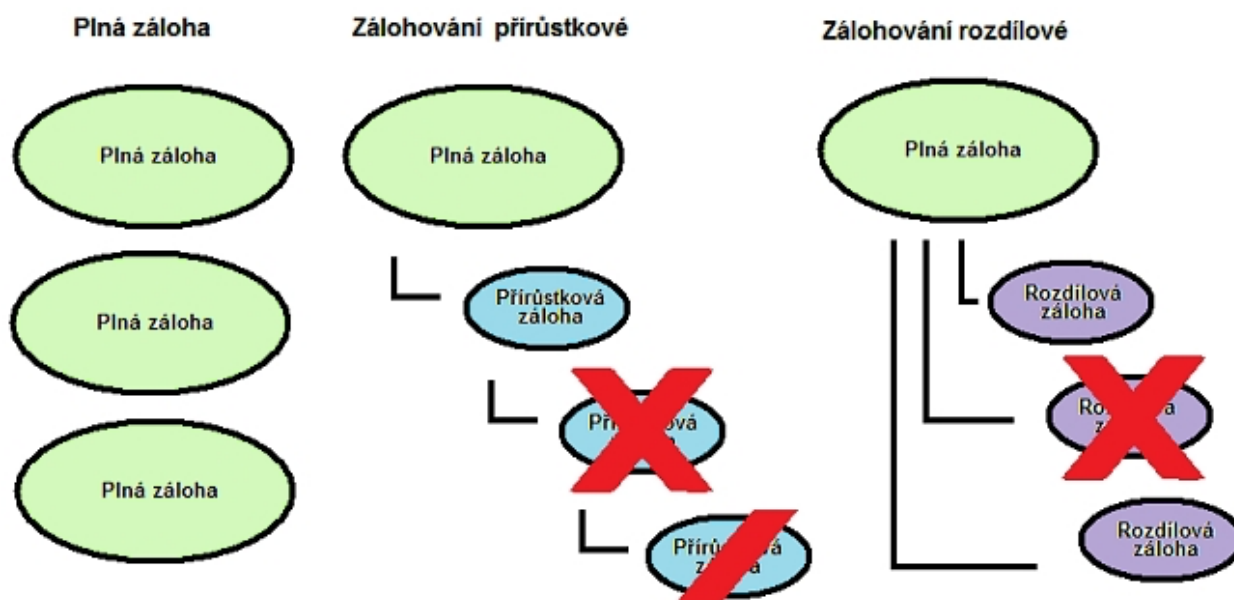
V nejhorších případech může nastat havárie diskových polí nebo dokonce serveru. Pro obnovení dat je nutné nahrát úplnou zálohu a poté postupně projít a přidat všechny do té doby vytvořené přírůstkové zálohy. [23]

Dá se tedy konstatovat, že přírůstkové zálohy jsou možným řešením pro tvorbu rychlých a menších velikostí, ale v případě obnovy je tento proces pomalejší. [16]

### **3.9.3. Diferenciální – rozdílová záloha**

Rozdílové zálohy jsou typem, u kterého dochází k zálohování právě těch souborů, u kterých dojde k nastavení atributu „Archive“, po provedení zálohy není tento atribut odstraněn. Tímto způsobem jsou pak zálohovány soubory, u kterých byly provedeny změny, nebo byly označeny atributem „Archive“. [16]

Zálohy tohoto typu jsou stejně jako u inkrementálních záloh časově nenáročné, jsou tedy stejně jako inkrementální zálohy možným řešením pro vytváření záloh během pracovních dní. Z těchto rozdílových záloh není možné samostatně obnovovat do původního stavu. [16]



Porovnání typů záloh [2]

Při havárii serverů, či diskových polí je nejdříve nutné provést obnovu poslední nejaktuálnější plné zálohy, poté je možné obnovit nejaktuálnější možnou rozdílovou zálohu, která byla provedena po záloze plné. Rozdílové zálohy jsou tedy z hlediska vytváření stejně časově nenáročné jako ty inkrementální. Čas obnovy je však v tomto případě mnohem nižší, protože není potřeba načítat všechny přírůstkové zálohy a postačí načtení jedné aktuální zálohy diferencíální. Záleží však na velikosti rozdílu mezi diferencíální a plnou zálohou. [16]

První den po provedení plné zálohy je časová náročnost na zálohování u inkrementálního i diferencíálního typu shodná, v průběhu následujících dnů narůstá čas pro zálohování diferencíální metodou, čas na obnovu se však relativně zkracuje. [16]

### 3.10. RAID pole

Jedná se používání vyššího množství levných disků, které jsou na sobě nezávislé. Mimo zkratku se jedná o Redundant Array of Independent / Inexpensive discs. Toto řešení se však

nevztahuje na metodu ochrany dat z hlediska zálohování jako prevence před smazáním dat. Jedná se o řešení, které chrání zařízení, před selháním disků na základě fyzických vlastností.

Tato metoda spočívá v ukládání dat specifickým způsobem na několikero disků, které mezi sebou nemají žádnou závislost. Data jsou tedy chráněna i před selháním jednoho ze samotných disků. Jednou z výhod Raidu je například vyšší výkonnost diskového subsystému. [17]

Číslo u RAID označuje úroveň zabezpečení, která je zde aplikována. Konkrétněji označuje počet diskových polí, které je zde používáno (RAID 0, RAID 1, RAID 5, RAID 6). RAID pole je primárně využíváno převážně v prostředí serverových řešení. RAID není možné považovat za samotné řešení zálohy dat. [17]

### **3.10.1. JBOD**

Jedná se o podobné řešení jako RAID. JBOD je řešení, ve kterém se používá znovu větší počet disků. Tyto disky jsou dále „řetězeny“ do samostatného a jedinečného logického celku. Občas se JBOD označuje taktéž jako RAID 0. [17]

JBOD funguje následovně. Disky jsou naplňovány postupně. V momentě kdy dojde k zaplnění jednoho z disků následuje ukládání na dalším disku. Nejedná se o řešení, které zahrnuje redundanci dat. Toto řešení je vhodné pouze v případě rozšiřování externích úložišť zařízení. [17]

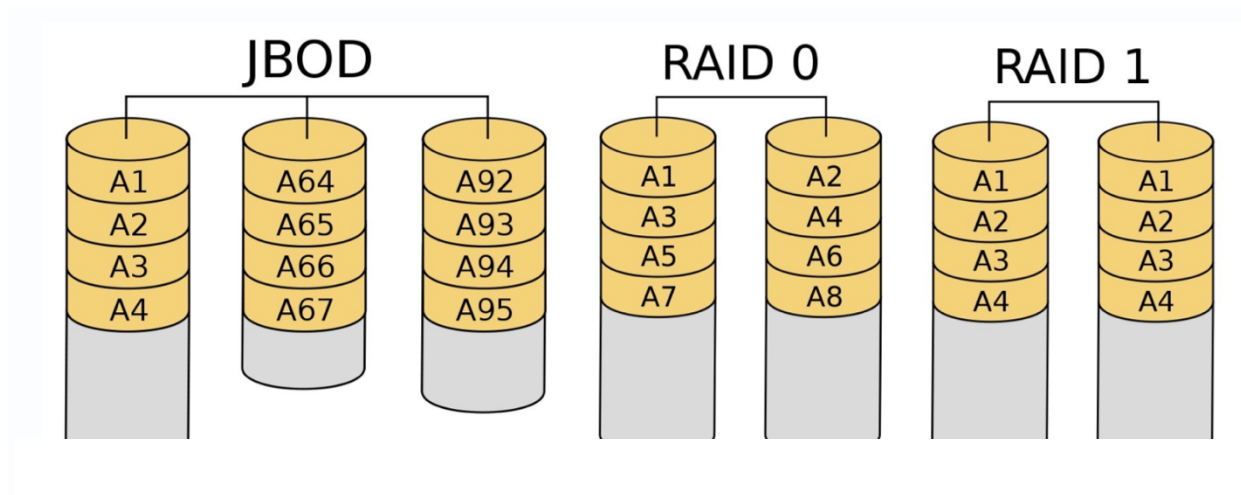
### **3.10.2. RAID 0**

RAID 0 je řešení, které nepředstavuje RAID jako takový, kvůli stejnému chování jako u JBOD. Tento typ RAIDu nevytváří redundantní data. Tento typ samotný nabízí dva nebo více disků, které jsou využívány střídavě v ukládání určitých bloků dat. Každý soubor se tedy rozděluje mezi vícero disků. Je tedy jasné, že v případě odstavení jednoho z disků dochází ve většině případů ke ztrátě veškerých dat. [17]

RAID 0 je sice nespolehlivé řešení, ale nabízí naopak vyšší výkon úložiště. Díky tomu, že jsou data ukládána střídavým způsobem, dochází k mnohem rychlejšímu zápisu a čtení. Jedná se zde o vylepšení v řádu desítek procent. Stejně jako u JBODu lze tímto způsobem rozšířit kapacitu úložiště. [17]

RAID 0 je tedy dobrým řešením pro data, které nejsou nijak kritická nebo jako určitá dočasná náhrada vyrovnávacích pamětí. Není však vhodné RAID 0 používat pro důležitá a produkční data. V těchto případech je ideální sáhnout po řešeních, které poskytují alespoň nějakou redundanci dat. [17]

### 3.10.3. RAID 1



*Raid 0 [3]*

Řešení RAID 1 je způsob duplikování dat / zrcadlení. Data jsou zrcadlena z jednoho disku na druhý. Tímto způsobem se jedná o redundantní řešení. Zpravidla se v tomto schématu používají dvě diskové jednotky. Je však možné toto řešení rozšířit. S vyšším počtem disků se navyšuje ochrana před selháním a následnou ztrátou. Jedním z hlavních důvodů používání RAIDu 1 je nižší nákladnost při používání dvou disků. [17]

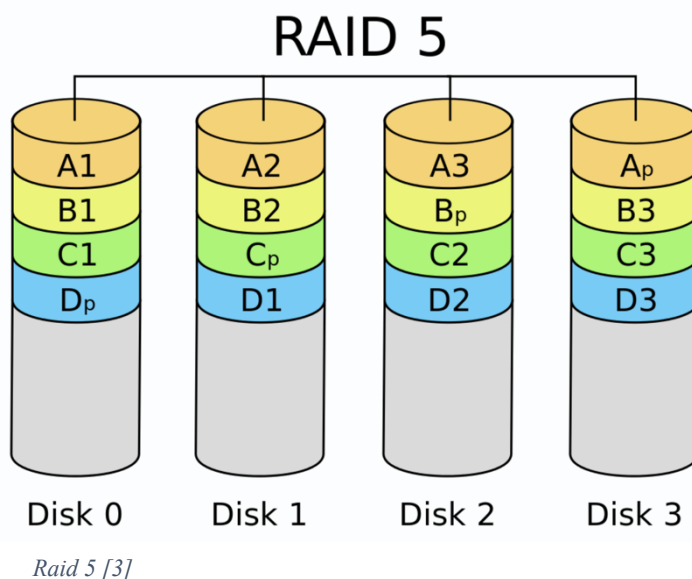
Co se týče rychlosti, tak v případě čtení je u RAIDu 1 rychlejší než při používání jednoho disku. V zápisu zde oproti RAIDu 0 zaostává, protože jsou data zapisovány vícekrát. Ve výkonnosti je tedy horší než RAID 0, ale na druhou stranu nabízí bezpečnost dat vytvářením kopií. [17]

### 3.10.4. RAID 5

Při používání RAID 5 je podmínkou použití minimálního počtu 3 diskových jednotek. Data jsou ukládány v blocích a jsou rozdělovány střídavě na dva a více disků. Dále je navíc vytvářena parita nebo jinak řečeno samoopravný kód. V případě poškození tato parita dokáže provádět

obnovu původních dat. Samoopravný kód se umísťuje taktéž střídavým způsobem mezi jednotlivými disky. [17]

Díky této distribuci parit je odstraňována nedokonalost nepoužívaného RAID 3 a 4, které používali distribuci parit pouze na jeden disk. Tento disk byl následně jako důsledkem vytíženější a vznikala zde tendence selhání oproti ostatním jednotkám. [17]



Výhody RAIDu 5 jsou například vyšší rychlosti u čtení. Data jsou zde rozdělené do bloků a usnadňují tím přístup. Kapacita je zde nižší pouze o jediný disk při používání 4 disků v případě stejných kapacit (RAID 5, který obsahuje čtyři 3TB disky poskytuje kapacitu RAIDu 9TB). [17]

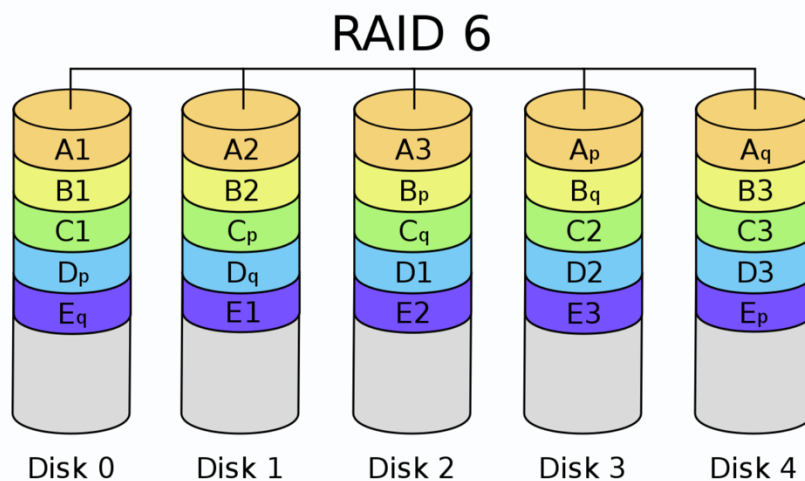
Jednou z nevýhod je například nižší rychlost u zápisů. Je zde totiž nutné dopočítávat a vytvářet samoopravné kódy. Další nevýhodou je taktéž výpadek jednoho disku. [17]

### 3.10.5. RAID 6

RAID 6 je jistým následníkem RAIDu 5. Fungují podobně, až na rozdíl ve vytváření samoopravného kódu. Zde jsou totiž vypočítávány rovnou dvě parity. [17]

Toto schéma je uspořádáno s použitím minimálně čtyř disků, přičemž jsou minimálně dva z nich použity pro rozdělování a zápis dat v blocích. Zbylé dva jsou používány pro uchování samoopravných kódů. Díky využití dvou parit, dokáže RAID 6 tolerovat selhání dvou disků. [17]

V případě čtení z hlediska rychlosti je zde možné srovnat RAID 6 s RAIDem 5. V oblasti zápisu se však jedná o znovu pomalejší řešení z důvodu výpočtu dvou parit. Jedná se tedy o řešení, které je oproti RAID 5 horší z hlediska cena/kapacita. Jedná se však o spolehlivější řešení v případě výpadku disku. [17]



*Raid 6 [3]*

### 3.11. Rotace záloh

Při provádění zálohy dat existuje mnoho důležitých bodů, které je nutno dodržovat. Jedním z těchto klíčových prvků, je nastavení rotačních schématů tak, aby byla provedena a následně zaručena ochrana minimálně pro jeden den zpět. To nejefektivnější schéma rotací, je přesně takové, které využívá více kombinací, zaručuje dlouhé a rozsáhlé kopie podnikových dat. [16]

#### 3.11.1. Round robin (Schéma s jednou páskou každý den)

To nejjednodušší řešení schématu rotací pásek vznikne v momentě, kdy je vyhrazen každý den v týdnu čas pro jednu jedinou pásku. Pásky jsou označené jako dny v týdnu. V každém dni je provedena záloha na určenou pásku. Tato záloha je plného typu, která je proveda u všech dat pro které je nastaveno zálohování. Tento způsob rotace nastavuje možnou zpětnou obnovu maximálně



jeden týden zpátky. Schéma je možné využívat v malých podnicích, které by využívaly interní nebo externí typy páskových mechanik, nebo přes použití network attached storage s nastavenou VDL. Tato VDL by následně sloužila jako primární úložiště dat. Toto řešení není zrovna efektivní, ale je vhodné do míst, kde je potřeba provádět plné zálohy každý den s dotačujícím jedním týdnem obnovy. [16]

### 3.11.2. Grandfather-father-son

Další řešení rotací je běžnější z hlediska využitelnosti. Jedná se o metodu „Grandfather-Father-Son“. Tato metoda, nebo schéma využívá rozdělení na denní (Son), týdenní (Father), a měsíční (Grandfather) sety médií. Čtyři sety médií jsou používány a označeny pro zálohu prováděnou každý den pracovního týdne (např. pondělí až čtvrtek). Na tyto sety médií jsou prováděny inkrementální zálohy, které se přepisují následující týden znovu stejným způsobem. Dalším typem jsou týdny, pro které je používáno 5 media setů. Tyto skupiny jsou pak nazvány jako Week 1, Week 2, atd. (Father). [16]



GFS [4]

Na těchto setech jsou prováděny v každém týdnu zálohy typu full backup, sety médií ve schématu Son zde nejsou používány a pro tuto skupinu se nastavuje expirační lhůta na dobu jednoho měsíce. Dále je prováděn znovu přepis těchto setů. Poslední set médií „Děda“ neboli

„Grandfather“ je složen z používání 3 setů médií. (tento set je možné tvořit jak samotnou jedinou páskou, nebo i více páskami).

Tyto sety jsou označeny jako „Month 1, Month 2, Month 3, atd.. Tyto sety jsou přepisovány po počtu pásek, které jsou zde využity. Každý set médií v tomto schématu představuje skupinu pásek, nebo používání samostatné pásky. Řešení kolik pásek zde používat závisí čistě na velikosti dat, které jsou zde zálohována. Počet všech média setů čítá dvanáct jednotek. Je vhodné z důvodu opotřebování médií, tato média obměňovat v rozumných časových intervalech. Obměny je také vhodné provádět v případě provádění archivací pásek. [16]

### **3.11.3. Tower of hanoi**

Hanojská věž, tedy konkrétně samotné schéma vzniklo v Číně původně na základně logické hry s tímto názvem. V této hře je úkolem přesunout pět kotoučů z kotlíku do dalšího s použitím nejmenšího možného počtu tahů. Hráč této hry se nikdy nesmí ocitnout ve stavu, kdy drží v ruce více než jeden kotouč. Navíc nikdy nesmí umístit větší kotouč na ten menší. Existuje důkaz, že nejmenší možný počet tahů je 31 tahů. [16]

Tato metoda je používáno pro zálohování na 5 různých setů médií. Schémat Tower of Hanoi je tedy prováděn tímto způsobem:

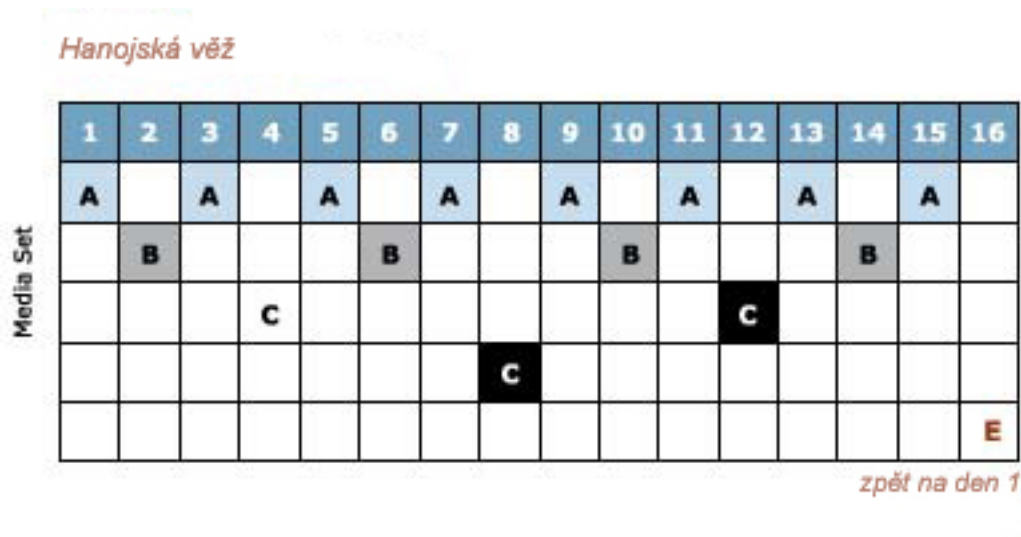
- Media set A je používán každý den
- Media set B je používán každý čtvrtý den
- Media set C je používán každý osmý den
- Media sety D a E jsou používány každý šestnáctý den ve střídavém pořadí

Zálohování v tomto schématu má svůj začátek u media setu „A“. Čtvrtý den je prováděna další záloha, ale tentokrát na set „B“. Tento den se neprovádí záloha na set „A“. Tento proces se provádí každou čtvrtou zálohu. Následně na set „C“ je prováděn každou osmou zálohu. V ty dny se neprovádí zálohy na A nebo B.

Zálohy na sety „D“ a „E“ jsou nastaveny tak, že se střídají a jsou prováděny každou šestnáctou zálohu. V tyto dny neprobíhají zálohy na „A“, „B“ anebo „C“. [16]

Výhodou tohoto řešení je také možnost navýšení počtu přidáním nového setu médií. Tímto je možné získat vyšší historii zálohy s nižším časem přepisu. Často používaná media obsahují zálohy, které jsou aktuálnější. Naopak ty méně mají více historických dat v případě potřeb obnovy. [16]

Jedná se o schéma, které je potřeba provádět pomocí softwarových nástrojů automaticky dle rozvrhového plánu. Není jednoduché tyto zálohy spravovat manuálně. Stejně jako v předchozích případech, je vhodné po čase obnovovat sety médií za účelem údržby nebo archivace. [16]



*Hanojská věž [4]*

Při samotném navrhování řešení při použití Tower of Hanoi schématu, je důležité vycházet z nastavených rovnic pro výpočet pásek, které by následně umožňovaly bezpečnost záloh, archivaci dat a řešení Disaster recovery. [16]

V dnešní době však existuje více zálohovacích schémat při využívání primárních a sekundárních úložišť. Tato řešení cílí především na vyšší bezpečnost dat. [16]

## 4. Archivace

Smyslem archivace je uchování a zajištění dlouhodobé dostupnosti digitálních dat v časovém horizontu od několika měsíců až po desítky let. Data se ukládají na nosiče s dlouhou životností a dobrým bezztrátovým uchováním informace. [20]

Takovými nosiči bývají nejčastěji magnetické pásky a vybrané pevné disky. Archivace dat je znatelně levnější než zálohování, protože u zálohovacích médií jsou vývojáři nuceni držet krok s technologickým vývojem v oblasti rychlosti přístupu k datům a velikostí úložného prostoru, zatímco pro účely archivace postačí vlastnit starší a pomalejší úložná média. [20]

Archivace může být také řešena například cloudovým řešením, které je možné získat v nižších cenových relacích. Data v režimu archivace jsou však přístupné v mnohem nižších rychlostech.

## **5. Vlastní zpracování**

Praktická část této bakalářské práce se zaměřuje na přístup a postup při plánování zálohovací strategie pro subjekty dle velikosti a požadavků. Kromě samotného návrhu zálohovacího řešení pro 4 subjekty, které nějakým způsobem využívají informační technologie k výkonu práce, zmíněné níže je pozornost zaměřena nejprve na prerekvizity v oblasti zabezpečení infrastruktury, protože tím je možné předejít ztrátě dat možnými útoky.

Část samotného zálohování je dále rozdělena na 4 části dle subjektů. Bude se jednat o korporátní prostředí, u kterého byly poskytnuty informace o tom, jak přistupovat při zabezpečení dat od specialisty kybernetické bezpečnosti Olivera Friese, dále o středně velkou společnost, menší firmu, u které jsou využity poznatky ze společnosti SABO IT. V závěru krátce zhodnotím, jak přistupovat k zálohování v domácnosti. Výstupem práce je návrh a doporučení čím se řídit pro návrh optimálního řešení.

V rámci samotného procesu návrhu strategie bude cílem pokusit se navrhnout dokonalou strategii zálohování pro vybrané subjekty. Výběry budou probíhat ve většině případů vícekritériální analýzou variant. Sběr dat pro vytvoření modelů byl prováděn shromažďováním informací z webových portálů jednotlivých poskytovatelů, či fór při nedostatečném množství dat.

## 5.1. Specifikace

V této části se zaměříme na 4 různé subjekty, které jsou rozděleny dle náročnosti na zabezpečení, velikost infrastruktury, množství dat, finančních možností a dalších podbodů. Kapacity jsou rozdělené v tabulce níže.

Subjekt	Zabezpečení	Velikost infrastruktury	Finanční možnosti
korporát	Maximální	Velká	Vyšší (Avšak nemusí být pravidlem)
Střední/malá firma	Střední / Vysoké	Střední	Dle činnosti (Adekvátní uvolněné peníze)
Domácnost	Nižší / Základní	Žádná	Minimální

*Tabulka Subjektů [1]*

## 5.2. Prerekvizity zálohování

Hlavním cílem je navrhnutí řešení zálohování pro určité subjekty. Kromě zálohování je však nejdříve třeba zaměřit pozornost na zabezpečení infrastruktury subjektů jako takové. Zálohování dat sice zachrání před ztrátou dat, ale v případě, že existuje špatně řešené zabezpečení, nastavení politik apod. (podrobněji níže), tak kromě možného úniku dat, je možné o data přicházet opakovaně. Následně by probíhala obnova ze záloh, která by byla znovu napadnutelná útočníky jak z venku, tak zevnitř.

Na začátek jsou rozepsány jednotlivé kroky zabezpečení a nastavení. Následně proběhne rozřazení potřeb dle subjektu.

- Zmapování sítě
  - o Hlavním cílem je zde vyhledání možných slabín, které jsou již známé.
  - o Detaily se často řeší se síťovým architektem, který má několik důležitých úkolů. Mezi ty nejhlavnější patří:

- Oddělení sítě klientů (jednotlivý klienti, admin účty)
  - Segmentace sítě (Segmenty sítě jsou pak jednotlivé zóny, které lze samostatně řídit, sledovat a chránit.
  - Kontrola komunikace backendu s frontendem (pokud existuje)
- Nutnost pro korporát, doporučení pro střední společnost, v malé společnosti dle zaměření a domácnosti neaplikovat
- Řešení dostatečně silných hesel
  - V minulosti platilo, že se za silné heslo považovala jakákoliv kombinace 8 písmen, kde byla splněna podmínka – Alespoň jedno velké písmeno, jedna číslice a jeden speciální znak.
  - V dnešní době to tak není a je doporučováno používat generátor hesel, který je třeba i správce hesel zároveň. Takovým generátorem je například software zvaný keepass
  - Dalšími alternativami je možnost používání tzv. dvoufaktorového ověřování, kdy kromě hesla je vyžadováno potvrzení např. skrze aplikaci nebo SMS zprávu.
  - Jednou ze zajímavých možností je využití PKI karet, které jsou nositelem certifikátu, který je jedinečný a dá se přes něj přihlašovat například k intranetovým aplikacím apod.
  - Nutnost pro korporát, střední společnost, malou firmu a doporučení pro domácnost
- Antispam techniky
  - Filtrování klíčových slov, či frází u známých typů spam emailů. (Například „Zdědil jsi neskutečné jmění po tvém strýčkovi“
  - Blacklisting známých IP adres, které by mohly způsobovat potíže
  - Antiphishing analýza – Zasílání pochybných emailů zaměstnancům, které jsou monitorovatelné. Jedná se o průzkum reakce na spam email na základě, kterého může v případě slabých výsledků proběhnout školení na toto téma.
  - Antispam techniky jsou důležité, tudíž je doporučeno je používat u všech 3 velikostech společností. V domácnosti je je možné zavést, avšak není tak nutné, protože je možné různé filtry nastavit u jednotlivých emailových stránek.
- Nastavení proxy serverů
  - Zajišťuje šifrování přenosu mezi sítěmi nebo protokoly
  - Odděluje uživatele od finální cesty, kterou vyhledávají

- Je možné nastavit například, že se nelze připojit na určitou adresu mimo firemní síť.
  - Jednou z možností, jak se připojit vzdáleně je při použití VPN (Virtual Private network), která slouží jako simulace firemní sítě.
  - Mezi VPN software patří například Pulse Secure nebo Zscaler
- Důležité pro korporáty a střední firmy, menší firmy nemusí být takovým lákadlem a není potřeba tento druh zabezpečení nastavovat pro malou společnost a domácnosti
- Odebírání administrátorských práv
  - Ponechání pouze nutně potřebným
  - Je však také možnost odebrat všem a v případě potřeby lze zažádat o nastavení dočasných administrátorských práv s udáním důvodu.
    - Tyto práva lze udělovat Automatizovaně nebo manuálně například přes Active Directory
- Vytvoření Hierarchie uživatelů v Active Directory
  - Nastavení práv uživatelů
  - Rozdělení na skupiny
  - Skupinové emaily
  - Přístupy na vzdálené úložiště
  - Správa v AD je v dnešní době samozřejmost u větších a častá u středních firem. Pro menší subjekty může být zbytečná, protože zde ještě funguje běžná verbální komunikace v případě omezení nebo potřeb. V domácnostech se nevyužívá
- Zabezpečení přístupu na server (Použití PAM)
  - Implementace PAM (Privelege access manager) řešení
  - Nepoužívají se uživatelé s plnými oprávněními
  - Rozdělení tzv. privileged účtů – příklady tohoto rozdělení:
    - Standart user accounts – limitovaná práva ve formě spouštění pouze základních programů, stahování pouze z firemního softwarového centra
    - Guest user accounts – Je více limitován, než standart user
    - Domain administrative accounts – omezen na pohyb v doméně
    - Break glass (také jako emergency nebo firecall) – Účet s maximálními právy. Často se údaje píše do obálky, a jsou uloženy v trezoru s minimálním

přístupem. V normálních situacích se nepoužívá. Je to pouze účet pro fatální situace, které je potřeba řešit nejsilnějšími možnými nástroji.

- Dle slov odborníků se jedná o „must-have“ řešení, které by mělo být v každém korporátním prostředí. U středních a menších firem může být vylepšením, není však tak potřebné. V domácnostech se nevyužívá
- Vypnutí open SMTP protokolu
  - Díky tomu je možné vystopovat emailové servery veřejně. Je tedy důležité, aby zůstaly zakázané.
  - Nutnost u všech subjektů. Avšak domácnosti tuto záležitost zřejmě řešit nebudou.
- Nastavení DMZ
  - Jedná se o podsít' mezi veřejným internetem a privátní sítí.
  - Zajišťuje další vrstvu zabezpečení
  - Příjemné vylepšení ve větších společnostech
- Honeynet
  - V poslední době poměrně oblíbený trend
  - Návnada na hackery
    - Prostor, který se tváří zranitelně. V momentě, kdy útočník pronikne, monitoring jej zachytí a lze poté blacklistovat.
    - Falešná sít' s falešnými daty
  - Vychytávka, která se hodí do korporátního prostředí, které by mohlo být terčem útoků.
- Šifrování disků (Používání hesel před samotným přihlašovaním do operačního systému)
  - Nastavení hesel do biosu
  - Je možné u všech subjektů, avšak se běžně využívá jen u korporátních prostředí. Bývá taktéž upravováno politikami dané společnosti
- Blokace používání USB zařízení
  - Používá se převážně v prostředí, kde se zachází s velmi citlivými daty
  - Používá se zřídka, primárně ve velmi kontrolovaném prostředí, hlavně však v korporátech.
- Laps (Local administrator password solution)
  - Management hesel lokálních účtů přes Active Directory a jsou chráněné ACL



- Zablokování původního domain administrátorského účtu sysID 500 – každý původní doménový admin má sysID 500
- Mělo by být používáno u všech společností, kde funguje určitá infrastruktura. V domácnosti ne.
- SIEM (Security Information and Event management)
  - Vhodný pro záznam strukturovaných logů
  - Důležitý pro identifikaci chyb
  - Velice účinná záležitost. Avšak hodí se k větším systémům, které se v menších společnostech nevyskytují. Tudíž se využívá hlavně v korporátech a středních společnostech
- NSX
  - Virtuální síť, u které lze naprogramovat její vzhled a je následně monitorována a autonomní
  - Vychytávka, která je výjimečná i v korporátech, je však „nice to have“.
- DLP (Data loss prevent)
  - Umožňuje markování dat dle důležitosti a tajnosti na různých úrovních jako např.
    - Confidential
    - Private
  - Záležitost, která záleží na politikách společnosti. Tudíž spíše zde záleží na požadavcích společnosti.
- GDPR
  - GDPR je třeba zohlednit při vytváření prekvizit pro zálohování, je zde potřeba navázat na rozdělení tajnosti jednotlivých dat. V případě, že není možné vymyslet ideální variantu řešení pomocí tajnosti, je třeba jako záruku vyžádat podpis o svolení zpracování dat

### 5.3. Zálohování v korporátním prostředí

Dle výše uvedených informací je zřetelné, že spousta zabezpečovacích technik se využívá primárně v korporátech. Tudíž je společnost většinou dobře chráněna před vnějšími i vnitřními vlivy, které by mohly způsobovat potíže a možnou ztrátu dat. Jiným problémem je zde množství, velikost a náročnost na čtení a ukládání dat.

## **5.3.1. Požadavky (korporát)**

### **5.3.1.1. Finanční náročnost**

Ačkoliv se jedná o velkou společnost s velkými obraty, finanční oddělení se snaží vždy na všem ušetřit a chovat se ekonomicky správně. Je tedy očekávané, že úměrně k velikosti společnosti bude potřeba velké úložiště, které se bude chovat dynamicky dle aktuálních potřeb, a nebude se zbytečně přeplácat.

Dále je třeba si uvědomit, zda chce společnost používat média na zálohování dat jen k ukládání kopií, nebo jako místo, kde se s daty dá pracovat a je možné je ihned používat například v týmu. Jednou z výhod přístupu, kdy se s daty pracuje přímo na úložišti je nižší náročnost na hardwarové vybavení počítačů jednotlivých zaměstnanců. Není potřeba aby počítače, notebooky a další zařízení disponovali lokálními disky s vysokou kapacitou na ukládání dat, protože uživatelé s daty budou pracovat jen vzdáleně.

Nevýhodou zde může být požadavek na přístup k internetu u konkrétního uživatele, dostupnost úložiště, nebo připojení k firemní síti. Poslední z nevýhod však lze řešit přes VPN, které je zmíněno výše jako jedna z doporučených prerekvizit.

### **5.3.1.2. Výkonnost a velikost úložiště**

Nejdůležitějším faktorem u velkých společností je množství dat. Objevuje se jich zde spousta a je potřeba k těmto datům přistupovat různými způsoby. Je třeba přemýšlet ekonomicky a řídit se tím co je zmíněno v kapitole výše.

Je zde právě zmíněno chování úložiště, které by se mělo chovat dynamicky. Tudíž pro data, která jsou využívána často a je potřeba s nimi pracovat frekventovaně je dobré mít na výkonnějším úložišti. Naopak pro data, která jsou používána zřídka kdy není potřeba je pravidelně používat, je možné zřídit úložiště, které není tak výkonné, ale zároveň ani finančně náročné

### **5.3.1.3. Zabezpečení**

V rámci zabezpečení je zde potřeba zmínit více konkrétních bodů, v prerekvizitách je zmíněno mnoho bodů zabezpečení, které jsou potřeba aby naše data nebyla jednoduše napadnutelná. Tudíž po softwarové a síťové stránce napadnutelnosti máme vše zajištěno.

Jedním z dalších hlavních požadavků je hardwarové zabezpečení. V rámci infrastruktury subjektu se zde vyskytují serverovny, které jsou srdcem dat. Těchto serveroven je víc a jsou oddělené v jiných budovách. Většinou by měli být tyto místnosti chráněné před případným fyzickým zničením ať už zaviněným, nebo nezaviněným. Tudíž se jedná o ventilovanou místnost s dvojitými podlahami, které chrání zařízení před přehřátím, nebo dokonce možným vzplanutím. Servery jsou uzamčené v klecích a samotná serverovna má omezený přístup například na biometrické bázi (Ověřování obličeje, otisky prstu, či dlaně) nebo v podobě čipových karet a hesel.

### **5.3.2. Návrh řešení (korporát)**

U korporátního prostředí se držím vzhledem k množství a důležitosti dat strategií 3-2-1. Tedy metodou, která nám zajistí, že se data nachází na třech místech. Konkrétně se jedná o jeden originál s dvěma kopiemi, přičemž v ideálním případě je jedna ze záloh na vzdáleném úložišti. Buď mimo pracoviště na jiné pobočce, centrále nebo na cloudu.

U strategie 3-2-1 se dodržují následující pravidla:

- Tři kopie dat, které tvoří dvojitou ochranu před ztrátou dat nebo selháním úložiště. Jedná se o stupeň více než by bylo třeba, ale je možné, že při ztrátě dat může dojít k problému i v záloze první. Proto je vhodné vytvářet zálohu druhou a předejít možným nepříjemnostem.
- Použití dvou rozlišných typů úložišť nám eliminuje možnost podlehnoutí určitého média ke specifickým poruchám pro dané médium. Osobně bych se v tomto případě přikláněl ke kombinaci serverových řešení onsite a cloudy.
- Jedna kopie offsite, která odstraňuje riziko poničení v případě přírodních katastrof a jsou vhodné pro obnovu a krizové řízení v případě problémů

Strategie 3-2-1 je dle expertů na bezpečnost a státních úřadů jako efektivní a osvědčené řešení. Chrání před incidenty i většími a nebezpečnějšími hrozbami jako je například ransomware a zajišťuje možnost zálohy a obnovy dat

Ve výše vybrané tabulce jsou vidět možnosti, jak postupovat při řešení. Dále je bráno v úvahu, že se pracuje se strategií 3-2-1. Jako hlavní zálohovací médium je tedy vybrán sever.

STRATEGIE	3-2-1 STRATEGIE	Strategie jedné zálohy	Bez záloh
1. místo uložení	Lokálně	Lokálně	Lokálně
2. místo uložení	Lokální server	Další úložiště	-
3. místo uložení	Cloud / Offsite server	-	-
výhody	Dvojitá ochrana, možnost využívat více funkcí a dobře segmentovat	Jednoduché na správu, finančně nenáročné	Bez nákladů
nevýhody	Finanční náročnost	Nedostatečně vysoká úroveň zabezpečení	Vystavení fatálním rizikům
Příležitosti	Díky propojení těchto dvou úložišť je možná nadstandartní správa úložišť a usnadnění práce	Jednoduchost a lehké nastavení procesů zálohování	-

Tabulka strategií [2]

Zálohy serverů je nejsnadnější řešit tzv. „server backup solutions“ ty mívají formu softwaru, který je navržen tak aby pomohl zálohovat data ze serverů na další lokální server, cloudový server, nebo hybridní server. V dnešní době se hybridní systémy velmi rozšířily, protože nabízí optimalizaci zdrojů (která je dle požadavků výše zmíněna jako stěžejní pro korporátní prostředí), podporu jednoduchého duplikování napříč regiony a nabízí taktéž rychlejší obnovu.

Takovéto typy softwaru a řešení nabízí například následující společnosti:

- Carbonite server
- Retrospect
- Veeam
- A další

### **Výběr SW nástroje**

Pro rozhodování byl sestaven model vícekritériální analýzy za účelem rozhodnutí využití nejvhodnějšího softwaru. Konkrétně se jednalo o metodu bodovací s vahami, přičemž váhy byly přiděleny autorem dle předmluvy výše. Kvalitativní ohodnocení byla převedena na kvantitativní obodováním jednotlivých variant a všechna kritéria byla taktéž převedena na maximalizační z důvodu jednotnosti a možnosti následujícího výpočtu.

Bylo porovnáváno 9 různých softwarových řešení v 8 kritériích. Kritéria byla rozdělena na dvě skupiny, kritéria hlavní a kritéria vedlejší dle jejich vah. Tabulky jsou rozděleny na dvě z důvodu přehlednosti. Výsledky jsou však počítány ze všech 8 kritérií. Data byla sbírána z více zdrojů informací. Jednalo se o webové portály samotných poskytovatelů, recenzních fór a blogů, zdroje jsou uvedeny na konci práce.

### **Mezi hlavní kritéria patří:**

- a) Cena s **váhou 0,25** (Červeně označené položky představují cenu odhadnutou na základě recenzí, protože určité společnosti neposkytují možnost výpočtu cen)
- b) Vhodnost softwaru pro velkou společnost s velkým počtem zařízení z hlediska kapacit a rychlosti s **váhou 0,3**
- c) Spolehlivost, tudíž míra spokojenosti s dostupností aplikace např. z důvodu výpadků, či údržeb a chyb s **váhou 0,12**
- d) Možnosti nastavení v aplikaci, míra možností, které aplikace poskytuje s **váhou 0,12**

Softwarový nástroj	cena v USD/měsíc	Vhodnost pro velké společnosti	Spolehlivost	Možnosti nastavení
Acronis	10	3	8	8
Rubrik	1	10	9	7
Veeam	8	10	10	10
Cohesity	3	10	8	5
Commvault	5	9	8	6
Spectrum	5	7	8	7
Veritas backup exec	1	8	9	8
Unitrends	5	9	8	7
Barracuda backup	5	6	8	5
Kritérium	Max	Max	Max	Max
Váhy	0,25	0,3	0,12	0,12

*Tabulka VAV Software [3]*

Tato tabulka představuje polovinu všech hodnocených kritérií, finální výsledky jsou zobrazeny níže. Řádky ideální varianty jsou vyznačené sytě zeleně. Druhá nejlepší varianta je vyznačena světlejší zelenou barvou a třetí je zvýrazněna nejsvětlejší zelenou barvou v tabulce.

**Mezi vedlejší kritéria patří:**

- a) UX/UI z hlediska přívětivosti aplikace pro uživatele pro snadné používání a efektivitu práce s **váhou 0,09**
- b) Technická podpora jako míra kvality řešení podpory a zpětné vazby od poskytovatele v případném řešení potíží s aplikací. Toto kritérium je ohodnoceno **váhou 0,04**
- c) Podporovaná média, protože některé služby podporují používání například jen a pouze virtuálních strojů, cloudů apod. Podporovaná média disponují **váhou 0,05**
- d) Bonusové vlastnosti představují další bonusové vlastnosti aplikace jako například migrační nástroje a podobné. Jedná se o vlastnosti, které se již nevztahují na problematiku zálohování. Poslední kritérium, protože je pro nás nejméně podstatné v korporátním prostředí, které rádo disponuje vlastním řešením je ohodnoceno **váhou 0,03**

Softwarový nástroj	UX/UI	Technická podpora	Podporovaná média	bonusové vlastnosti
Acronis	9	8	8	8
Rubrik	5	10	8	10
Veeam	9	8	9	3
Cohesity	9	6	7	0
Commvault	8	6	6	6
Spectrum	7	9	4	6
Veritas backup exec	9	8	9	5
Unitrends	8	8	7	7
Barracuda backup	7	6	7	2
Kritérium	Max	Max	Max	Max
Váhy	0,09	0,04	0,05	0,03

## Finální výsledek

V porovnávání variant se na prvním místě umístil poskytovatel Veeam s řešením veeam advanced backup. Dle analýzy je možné konstatovat, že se jedná o téměř ideální variantu, protože z 10 možných bodů se na škále umístil s 9,07 body.

Veeam splňoval preferovaná kritéria nejlépe a je vybrán jako softwarová část řešení. Výsledek řešení a získané body jsou dostupné v tabulce níže.

Softwarový nástroj	Metoda bodovací s váhami
Acronis	7,09
Rubrik	6,72
Veeam	9,07
Cohesity	6,71
Commvault	7,07
Spectrum	6,52
Veritas backup exec	6,42
Unitrends	7,35
Barracuda backup	5,89
Kritérium	MAX

Tabulka VAV Software 3 [5]

## Výběr média

Výběr média bude taktéž proveden ve dvou různých scénářích. V prvním případě se jedná o výběr prostředí jako takového. Celkové řešení zálohování tohoto subjektu se řídí 3-2-1 strategií, tudíž prvním vybraným prostředím je to fyzické v podobě lokálního serveru. Pro druhé prostředí je možné zvolit cloudové, či virtuální.

Virtuální řešení je velmi atraktivní z hlediska výkonu, jedná se však o velmi nákladnou investici, která však nemá zas tak vysokou nákladnost z hlediska údržby. Je však nákladná, protože virtuální stroje jsou komponentou fyzických zařízení, která jsou potřeba buď pořídit fyzicky in-house, což je v rozporu s 3-2-1 strategií, kdy je cílem vyhnout se možné ztrátě dat v případě



přírodních katastrof, nebo pronájmem, který může být nákladný jak z pořizovacího hlediska, tak i z toho údržbového.

Naopak cloud nám poskytuje flexibilní řešení, které nemusí být tak výkonné, ale naopak poskytuje možnost úprav velikosti a výkonnosti úložiště v krátkém čase a splňuje podmínku 3-2-1 strategie. Cloudová řešení mívají zpravidla nízké základní pořizovací náklady, ale vyšší operativní ve smyslu údržby a nastavení. Vzhledem k výše zmíněnému přístupu je zde zvoleno jako druhé prostředí, to cloudové.

Druhá fáze rozhodování se týká poskytovatelů. Ta je provedena dvakrát. Nejdříve pro fyzické prostředí a následně pro cloudové. Protože byl vybrán jako nástroj veeam, je pro jednotlivá prostředí vybráno několik poskytovatelů, se kterými veeam umí pracovat. U fyzických prostředí nabízí možnosti Windows server, Linux, IBM AIX a Oracle solaris.

V tomto případě je provedena opět vícekritériální analýza variant. Zde je kladen důraz na bezpečnost, která je zde u všech možných prostředí na kvalitní úrovni. Dále se jedná o náročnost nastavení, která je uzpůsobena právě díky používání SW nástrojů od Veeam. Dále je však potřeba zajistit personál, který bude zodpovědný za chod HW ve společnosti. Velkou položkou je však spolehlivost, která usnadní práci osobám, které budou nastavovat chody zařízení. Výkon je zde jako druhotný, avšak všichni poskytovatelé disponují dostatečnými schopnostmi.

Posledním a možná tím nejtěžejnějším, avšak s nízkou vahou, protože se jedná o bonusovou funkci, která není významným požadavkem, ale velmi přínosným je vlastnost, která přinesla MS windows serverům jejich prvenství v níže vyznačené tabulce. Jedná se o propojení s cloudem, díky kterému dochází k jednoduššímu řízení toku dat.

OS	Bezpečnost	Náročnost nastavení	Náklady na personál	Spolehlivost	Výkon	Bonusové funkce	Metoda bodovací s váhami
MS W server	8	9	10	10	6	10	8,8
Linux	7	10	7	10	7	0	7,7
IBM AIX	9	4	6	7	10	0	6,75
Oracle solaris	9	3	6	7	10	0	6,55
Kritérium	Max	Max	Max	Max	Max	Max	
Váha	0,3	0,2	0,2	0,15	0,1	0,05	

Tabulka VAV OS [6]

Pro fyzické prostředí je zvolen MS windows server ve verzi 2016, který nám poskytuje možnost propojování s druhým prostředím, a to cloudem. Veeam znovu nabízí několik poskytovatelů, kteří jsou podporováni v samotném nástroji. Mezi ně patří Google cloud, AWS a MS Azure. Jednotlivá kritéria v tomto modelu jsou srozumitelná a není potřeba jej vypisovat. Bonusové kritérium označovalo například zmíněné přímé propojení s cloudem

Pro cloud byla taktéž provedena analýza variant, kde hlavní kritérium tvořila cena a bezpečnost, dále se rozhodovalo dle vlastností, které poskytovatelé nabízejí. MS Azure nabízí rozřazení dat z hlediska důležitosti (tiering), což je jedna z výše zmíněných preferencí, které chceme u korporátního prostředí používat. Podobné vlastnosti nabízí však i zbytek konkurence.

Řazení konkurence však není tak velké a je třeba jej hlídat ručně. V azure funguje toto řazení automaticky dle přístupu k souborům. Bezpečnost je hlavním kritériem s váhou 0,2, ta lze u subjektů shrnout velmi rychle. Google cloud je sice zajímavý, ale z hlediska zabezpečení a celkové bezpečnosti je snadným terčem v případě možných útoků. V tomto kritériu tedy nezazáří. AWS poskytuje vestavěné šifrování, které se dá brát jako velké plus. Avšak Azure kromě zabudovaného šifrování poskytuje taktéž používání tzv. MFA Autentizaci. Zbytek kritérií a jejich ohodnocení je dostupný v tabulce níže.

Dle vícekritériální analýzy variant byl vybrán pro řešení cloudu MS Azure. Nyní tedy máme vybrané 3 komponenty a stěžejní součásti zálohování. Fyzické prostředí v MS serveru, Cloudové prostředí Azure a softwarové řešení Veeam. Po propojení těchto prostředí prostřednictvím veeam je potřeba věnovat pozornost níže zmíněným bodům.

Poskytovatel	Cena	Zabezpečení	Tiering	Propojení s onsite	Automatizace	Monitoring	Konfigurace	Výsledek
Azure	10	10	10	10	0	3	5	<b>8,07</b>
AWS	6	8	8	7	10	10	10	<b>7,8</b>
GCP	8	4	5	6	0	0	4	<b>4,79</b>
Kritérium	Max	Max	Max	Max	Max	Max	Max	
Váha	0,3	0,2	0,15	0,1	0,1	0,09	0,06	

Tabulka VAV Cloud [7]

Ve veeamu si nastavíme:

- Jaké typy souborů chceme zálohovat
  - o V každém případě je třeba ukládat kopie dat jednotlivých zařízení
  - o Outlookové soubory
  - o Zálohy systémů
- Kam a odkud tyto soubory budeme zálohovat
  - o První zálohu na lokální server (server ve vlastnictví) je potřeba pro něj mít zaměstnance, který jej spravuje a zodpovídá za něj. V našem případě se jedná MS server 2019. Byl vybrán metodou VAV.
  - o Druhou provádět na cloud od vybraného poskytovatele. V tomto případě byl dle kritérií vybrán MS Azure

- Plánování a automatizace zálohování
  - o Používání diferenciální zálohy každých 7 dní
  - o Aktualizace dat cloudu každý den v reálném čase
- Řízení životního cyklu záloh
  - o Každá diference bude existovat 6 měsíců od doby vytvoření zálohy, která ji přepsala a je aktuálnější. Poté v rámci serveru archivována. Na cloudu po 30 dnech spadnou nepřístupovaná data do levnější kategorie úložiště. Po 6 měsících přejdou stejně jako na serveru do stavu archivace. Využijeme zde řazení, které nám Azure nabízí a zároveň zde dojde k racionálnímu finančnímu řešení. Tento proces však lze pomocí nastavení ve Veeamu a na samotných prostředích upravit dle potřeb společnosti
- Segmentace záloh
  - o Rozdělení na kritická a citlivá data a ostatní dle priorit
  - o Po 30 dnech neotevření v azure propadne do levnější kategorie, která nemá takový výkon.
- Komprese dat
  - o Data, obrázky a média je dobré komprimovat automaticky pro lepší využití úložiště, a tak je zde potřeba identifikovat často používaná a nepoužívaná data
- Nastavení typu zálohy (plnou, diferenciální nebo inkrementální zálohu)
  - o Dle zjištění v rešeršní části je zde diferenciální záloha ideální volbou. Všechna zařízení ji disponují.

## 5.4. Střední firma / Malá společnost

V menší firmě je stále důležité dbát na ochranu dat a nepodcenit zálohy. Je potřeba uvědomit si která data jsou pro nás kritická. Je časté, že tento typ společností většinou nemá vybudovanou infrastrukturu, která by měla být zabezpečena takovým způsobem jako u korporátu. Je zde však potřeba zvážit všechna možná rizika, která mohou nastat.

## **5.4.1. Požadavky (Střední/Malá společnost)**

Zde je důležité přemýšlet s nastavením „keep it low“. Je hledána zlatá střední cesta jako prevence před ztrátou a zároveň jít cestou, která není finančně náročná. Není tedy požadavkem, aby se řešení muselo chovat dynamicky jako u korporátu. Není zde tedy takové množství dat abych musel diverzifikovat na takové úrovni.

Častým řešením v tomto typu společností je používání míst, kde se dá s daty pracovat na přímo a v případě potřeby je možné jej uložit na lokální úložiště. Po finanční stránce by bylo ušetřeno současně i na hardwaru. Bylo by však vhodné poskytnout zaměstnancům vhodné externí úložiště pro vytvoření záloh pro nejdůležitější data. Zde si to oproti korporátnímu prostředí můžeme dovolit, protože nejsou zakázána usb úložiště v samotných operačních systémech.

### **5.4.1.1. Finanční náročnost**

Jak už bylo zmíněno výše, je potřeba vybrat nízkonákladové řešení, které však bude možné řídit s určitou mírou flexibility. Finance v těchto společnostech nejsou malé, avšak je potřeba s nimi zacházet šetrně a s rozvahou.

V některých případech je vhodné vybrat řešení, které bude multifunkční a je možné jej využít pro jiné funkce. Například využití nástrojů i pro migraci softwarových systému apod. Tímto způsobem je možné ušetřit finance z dlouhodobějšího hlediska.

### **5.4.1.2. Výkonnost a velikost úložiště**

Výkonnost zde není tak stěžejní, ačkoliv záleží na typu společnosti. Zde je ale odpověď jasná. Velikost úložiště není potřeba enormní, a proto je dobré i z ekonomického hlediska vybrat cloudová řešení. Zajistí spoustu potřebného místa, které je výkonné a po stránce dostupnosti se v dnešní cloudové době najde velká konkurence mnoha společností.

Je však velmi vhodné sledovat i další možnosti využití vybraných nástrojů nebo úložiště, předpokladem je fakt, že menší společnosti nemají za potřebné vytvářet vlastní nástroje například pro migraci systémů apod.

### 5.4.1.3. Požadavky na zabezpečení

Bezpečnost je vždy velmi důležitý aspekt, je tedy potřeba brát v úvahu bezpečnost na vysokou váhu. Rozhodně však není potřeba nastavovat bezpečnosti jako nejvyšší prioritu. To však znovu závisí na oboru společnosti a zaměření.

### 5.4.2. Návrh řešení (Střední/Malá společnost)

V tomto prostředí není využita 3-2-1 strategie, ale pouze používání kombinace lokálního úložiště s cloudy. Malým vylepšením je poskytnutí malého externího disku v kapacitě cca do 50 GB. Za který si každý zodpovídá sám a je na konkrétních osobách, jak jej využijí. Je však důležité *Tabulka VAV SW malá firma [5]* podotknout, že ačkoliv toto rozhodnutí zní velmi drsně, je reálné jej uskutečnit.

#### Výběr softwarového nástroje

Kandidáti pro výběr zůstávají stejní, bylo však odstraněno kritérium „Vhodnost pro velikost společnosti“, které představovalo schopnost pojmout vyšší kapacity úložišť a spravovaných zařízení. Tudiž bylo potřeba přebodovat jednotlivá kritéria.

#### Hlavní kritéria

Nejvyšší prioritu v tomto případě má znovu cenové ohodnocení. Nyní však na druhém místě s ohodnocením 0,17 byly bonusové funkce, které představují další sadu nabízených možností využití softwaru. Třetí místo obsadila spolehlivost a poté následovaly možnosti nastavení. Tabulka byla znovu rozdělena na dvě poloviny z důvodu přehlednosti a jednoduchosti. Další kritéria jsou zmíněna v sekci vedlejší kritéria.

V hlavních kritériích silně dominuje Acronis, ten má v nabídce spoustu podpůrných funkcí, které přidaly potřebné body. Je však nutné sledovat metodu VAV jako subjektivní hodnocení, které

je však podloženo daty. V některých případech je ale třeba brát v úvahu, že modely s kardinálním typem informací tvořené například více osobami se mohou lišit i po čerpání ze stejných zdrojů dat.

Softwarový nástroj	cena v USD/měsíc	bonusové vlastnosti	Spolehlivost	Možnosti nastavení
Acronis	10	8	8	8
Rubrik	1	10	9	7
Veeam	8	3	10	10
Cohesity	3	0	8	5
Commvault	5	6	8	6
Spectrum	5	6	8	7
Veritas backup exec	1	5	9	8
Unitrends	5	7	8	7
Barracuda backup	5	2	8	5
Kritérium	Max	Max	Max	Max
Váhy	0,32	0,17	0,15	0,12

Tabulka VAV SW malá firma 1 [8]

### Vedlejší kritéria

Vedlejší kritéria v tomto případě jsou pouze 3. Mají však i tak vysokou váhu s celkovou hodnotou 0,24 a stále celkem vysokým dopadem na finální hodnocení. Mezi tato kritéria patří UX/UI, technická podpora a podporovaná média.

V tomto řešení nejvíce narostlo kritérium technická podpora, která je potřebná z důvodu chybějících specialistů ve společnosti, protože si většinou subjekty tohoto typu tyto zaměstnance nenajímají.

Softwarový nástroj	UX/UI	Technická podpora	Podporovaná média
Acronis	9	8	8
Rubrik	5	10	8
Veeam	9	8	9
Cohesity	9	6	7
Commvault	8	6	6
Spectrum	7	9	4
Veritas backup exec	9	8	9
Unitrends	8	8	7
Barracuda backup	7	6	7
Kritérium	Max	Max	Max
Váhy	0,09	0,1	0,05

Tabulka VAV SW malá firma 2 [9]

### Tabulka výsledků

Softwarový nástroj	Metoda bodovací s váhami
Acronis	8,73
Rubrik	6,06
Veeam	7,83
Cohesity	4,52
Commvault	6,16
Spectrum	6,39
Veritas backup exec	5,54
Unitrends	6,7
Barracuda backup	5,32

Tabulka VAV SW malá firma 3 [10]

Jako nástroj zde byl vybrán Acronis cyber protect ve verzi advanced pro střední společnost a menší firmu. Jedná se ideální nástroj, který lze taktéž používat v režimu hybridních úložišť a nabízí vše co je pro takovou společnost potřeba. Dále lze vybrat specifickou verzi dle výběru úložiště.

### Výběr úložiště

Acronis nabízí možnost ukládat zálohy na síťová úložná zařízení, externí HDD a SSD, páskové jednotky, na cloud poskytovaný Acronisem nebo při použití produktu Acronis cyber Infrastructure lze ukládat na libovolné úložiště. Pro používání dodatkové služby samotná



společnost neposkytuje kalkulačku cen a cena tohoto řešení nebyla nikde dostupná. Proto v rámci vícekritériální analýzy dostane ohodnocení symbolickou jedničkou. Externí disky jsou již využívány, proto nebudou součástí rozhodování.

V rámci tohoto modelu VAV byla nejdůležitějším kritériem cena, dále v důležitosti na stejné úrovni byla spolehlivost a možnost sdílení v rámci prostředí mezi uživateli. Bezpečnost, jak již byla zmiňována výše není hlavním pilířem rozhodování, avšak zůstala s poměrně vysokou váhou před posledním kritériem nazvaným přístup k datům, které specifikuje čas, za jaký jsme schopni dostat zálohu k dispozici.

Cloud i síťová řešení poskytují dobrou přístupnost v čase naproti velmi pomalému řešení páskových jednotek. To by bylo vhodnější spíše pro archivaci vzhledem k ceně, která je velmi nízká. V tomto případě však vybíráme pouze jedno prostředí. V případě, že by bylo ve zvažování možné řešení archivace dalším médiem, došlo by ke zvolení magnetických pásek.

Prostředí	Bezpečnost	Přístup k datům	Cena/kapacita	Spolehlivost	Sdílení	Výsledek
Síťová zařízení	10	10	3	7	10	6,6
Cloud	5	10	8	10	8	8,05
Páskové jednotky	10	0	10	10	0	7,5
Kritérium	Max	Max	Max	Max	Max	Max
Váhy	0,15	0,05	0,4	0,2	0,2	

*Tabulka VAV prostředí malá firma [11]*

Jako nejlepší řešení v rámci nasbíraných dat vyšel cloud, který bude poskytnut přímo od Acronisu, protože není využita služba, díky které jsme schopni vybrat cloudového poskytovatele sami. Vícekritériální analýza varianta tudíž zde nebude prováděna pro výběr poskytovatele.

## Konfigurace v Acronisu

- Nastavení úrovní souborů, které budou podrobeny zálohování
- Nastavení času zálohování
- Zálohování zařízení s Windows, MacOS, Linux, Microsoft 365, Google Workspace, Hyper-V, VMware a dalších
- Flexibilní obnovu s možností obnovování jak malých souborů, tak i celých systémů
- Migrace
- Archivování
- Používání inkrementálních a diferenciálních záloh
- Rozšířenou podporu záloh pro MS SQL a Exchange clustery, MySQL, Oracle DB, a SAP S4HANA
- Ochrana dat a vytváření reportů, skenování prostředí klientů pro zajištění správné ochrany
- Používání virtuálních strojů pro procesy zálohování

## Konkrétní nastavení v Acronisu

- Jaké typy souborů chceme zálohovat
  - Zde bychom si rozřadili zařízení, která chceme zálohovat.
  - Zálohovaná tedy jsou zařízení typu desktop, notebooky a servery, které jsou vlastnictvím společnosti
- Kam a odkud tyto soubory budeme zálohovat
  - Zálohy budou ukládány na cloudová úložiště, případně je možné využít schopnosti Acronisu ukládat zálohy na externí disky, které byly poskytnuty zaměstnancům
- Plánování a automatizace zálohování
  - Zálohování by mělo probíhat na pravidelné bázi
  - Vybraný cyklus zálohování by měl probíhat v čase, kdy jsou zařízení dostupná, ale nejsou plně využívána, tudíž by bylo vhodné vytvářet zálohy každý týden v pátek v čase oběda.
- Řízení životního cyklu záloh

- Acronis poskytuje taktéž přesun záloh do archivačního režimu, tudíž je vhodné nastavit 2 měsíce jako dobu po kterou budou data zálohována a následně přejdou do stavu archivace
- Komprese dat
  - Data ve stavu archivace by bylo vhodné komprimovat
- Nastavení typu zálohy (diferenciální nebo inkrementální zálohu)
  - Zde by bylo znovu vhodné používat diferenciální zálohu

## **5.5. Domácnost**

### **5.5.1. Požadavky (Domácnost)**

Domácnost je samozřejmě prostředí, které si řídí každý sám. Je třeba dbát na náročnost nastavení a uživatelskou přívětivost společně s cenovým řešením. Není zde však požadováno používat softwarové nástroje. V případě, že existují k dispozici nástroje ve verzi zdarma nebo ve velmi levné nabídce, bylo by výhodné jej využívat. Je důležité u výběru nástroje taktéž dbát na to, aby vybraný software dokázal podporovat starší zařízení.

#### **5.5.1.1. Finanční náročnost (Domácnost)**

Finanční náročnost domácnosti je velmi omezená, nepotřebujeme mít vlastní server na kterém je možné řídit zálohy. Je potřeba zvolit spolehlivé řešení, které je co nejlevnější.

Existuje spousta řešení, která jsou cenově dostupná na této úrovni, nebo dokonce zdarma. Někdy je však vhodné nešetřit přehnaným způsobem, protože každá desetikoruna může v tomto případě způsobit značný rozdíl v efektivitě návrhu zálohování.

#### **5.5.1.2. Výkonnost a velikost úložiště (Domácnost)**

Zde je důležité se rozhodnout co vyžadujeme, je vhodné zde zvážit možnosti sdílení dat. To je taktéž důležitým pilířem řešení pro domácnost. Není však zapotřebí sdílet kompletní data předdefinovaná v nástrojích. Výkonnost v domácnosti nesmí být zanedbána, ačkoliv není tak

důležitá. Velikost potřeb záleží vždy na domácnosti, naštěstí v dnešní době existuje mnoho řešení pro domácnosti, které splňují výše popsané požadavky.

## 5.5.2. Návrh řešení (Domácnost)

### Výběr softwarového nástroje

Softwarový nástroj by v domácnosti měl být intuitivní, nenákladný a jednoduchý na obsluhu. Drahá řešení tudíž nejsou součástí výběru. Kritéria tedy v tomto případě byla jasná. Cena představuje, zda je možné pořídit si sw zdarma, či za přijatelnou cenu. V tomto případě odpovídá hodnota 6 ceně cca okolo tisíce korun českých za doživotní licenci na více zařízení. Hodnota 10 odpovídá freeware verzi softwaru. UX reprezentuje přívětivost a intuitivitu aplikace. Nastavení popisuje možnosti předvoleb a nabízených nástrojů a v posledním případě možnosti médií představují jaká média lze přes toto řešení používat a spravovat

Nástroj	Cena	UX	Nastavení	Možnosti médií	Výsledek
AomeITech	10	6	6	4	6,8
Ashampoo	7	7	8	7	7,2
EaseUS	6	8	10	8	7,8
MiniTool	10	6	7	6	7,4
Kritérium	Max	Max	Max	Max	Max
Váha	0,3	0,3	0,2	0,2	

Tabulka VAV domácnost [12]

V tomto případě, v modelu vícekritériální analýzy variant byl zvolen software zvaný EaseUS, který zajišťuje možnosti lokálních záloh, cloudových záloh, výběru mezi plnou, diferenciální a inkrementální zálohou, zálohování outlooku, klonování disků, klonování systému, transfer systémů na jiné zařízení, obnovu, a provádění plánovaných záloh.

### Výběr média

Protože byl zvolen nástroj, který je schopen pracovat s více úložišti, konkrétně lokálními a vzdálenými, je vhodné vybrat dvě různá média. Pro lokální úložiště se možnosti výběru zdají velké,

avšak v cenové relaci, která vyhovuje požadavkům je možné konstatovat, že nejvhodnějším řešením je zde Externí disk. Používání je jednoduché, náklady na pořízení jsou poměrně nízké a spolehlivost je taktéž vysoká. Jiné řešení zde nepřichází v úvahu, protože například spravování NAS úložiště v domácnosti není jednoduché a rozhodně není levnější než externí disky. Externí disk zde poslouží jako úložiště pro veškerá data.

V rámci nastavení ve zvoleném nástroji je vhodné zvolit diferenciální zálohu, která bude následně dostupná z našeho externího disku. Z toho důvodu je vhodné vybrat disk o kapacitě minimálně 2TB v případě, že data, která uchováváme mají vyšší kapacitu. V domácím prostředí není předpokládáno, že bude tato kapacita převršena.

Dále je možné naplnit taktéž další ze zmiňovaných požadavků. A to konkrétně možnosti sdílení mezi členy domácnosti. To však není potřeba pro všechna data. V případě vyššího přenosu dat je možné čerpat přepojením externího disku. Rychlejší řešení je rozhodně výběr cloudového úložiště. Cloudová úložiště v dnešní době poskytují úložiště zdarma. Velikost úložiště v tomto případě je jediným a rozhodujícím kritériem, které rozhodlo z výběru služeb.

Mezi varianty patřil například Mega, Google cloud, Media fire a další. Nejvyšší úložiště však nabízí Blomp. Zde je totiž k dispozici 200 gigabajtů úložiště zdarma, které je dostupné v prohlížeči a mobilní aplikaci.

Na cloudové úložiště budou ukládána data, která chtějí lidé v domácnosti sdílet mezi sebou. Jedná se o nejlepší řešení z hlediska kapacity. V kombinaci s externím diskem tvoří kvalitní kompromisní dvojici pro vytvoření fungujících záloh v domácnosti.

## **6. Závěr**

V rámci problematiky zálohování existuje mnoho různých postupů, řešení a pohledů. Je však důležité si vždy nastavit priority, které jsou hlavním pilířem směru, kterým se vydáváte. V rámci práce byl popsán jen zlomek možných pohledů na tuto problematiku vzhledem ke kapacitní omezenosti práce. Byla navržena tři různá řešení, pro tři různé subjekty s vícero různými požadavky, která by měla naplnit potřeby subjektů a zajistit pokojnou správu dat a zabezpečení.

V rámci řešení bylo taktéž navrženo, jak by měly subjekty přistupovat k otázce bezpečnosti, jelikož je úzce spjata s problematikou zálohování. Bez zabezpečení infrastruktury se subjekty vystavují riziku ztráty dat i přes existující řešení zálohování.

K řešení požadavků byla využívána vícekritériální analýza variant s metodou bodovací. Všechna kritéria byla ohodnocena na škále od 1-10, kdy vyšší znamená lepší. Byl zde využíván kardinální typ informace, tudíž rozdíly mezi jednotlivými variantami nemusí být úměrné, ale představují hodnoty, které pro nás jsou stále přijatelné a které již nikoliv. Data pro kritéria byla sbírána z webů poskytovatelů, fór, či blogů, které jsou uvedeny pod citacemi.

### **SWOT analýza řešení pro korporátní prostředí**

V korporátním prostředí došlo k výběru softwaru Veeam backup, které poskytuje kvalitní uživatelské rozhraní, přehlednost mezi vysokým množstvím zařízení, a automatizaci záloh za velmi rozumnou cenu. Prostředí jsou využívána dvě, fyzický server, který poskytuje kvalitní zázemí pro vytváření záloh a cloudový poskytovatel azure s rozumným ceníkem a rozřazování zálohování dat dle důležitosti.

Řešení bylo navrženo pro uspokojení požadavků. Každé řešení má však svá pro a proti, níže je vyobrazeno několik nejpodstatnějších bodů v rámci SWOT analýzy

#### **Silné stránky**

- Používání azure má výhody v tom, že je integrováno s Office 365, je tedy možné používat pro správu souborů a dokumentů, které byly vytvořeny v tomto prostředí již od vzniku souborů a pracovat s nimi přímo v cloudu.
- Je možné flexibilně nastavit výdaje dle využívání cloudových služeb.
- Lze kvalitně strukturalizovat data.
- Všechna zařízení ve společnosti je možné spravovat v reálném čase.
- Automatizované zálohy
- Možnost správy více propojených zařízení a virtuálních strojů.
- Je možné provádět obnovy v rozsahu od celých instancí/VM až po samotné soubory

## **Slabé stránky**

- Je třeba používat silné internetové připojení při využívání cloudových služeb.
- Toto řešení lze použít jenom v případě, že korporace neoperuje v oblastech, kde není Azure podporován. V případě, že ano, tak je třeba zvolit jiné řešení.
- Je třeba chvíli strávit nad pochopením samotného nástroje a uživatelského rozhraní.

## **Příležitosti**

- Velmi nízká míra výpadků. V odhadu jednou za 8 let
- Nízká pořizovací cena, může být flexibilní dle potřeb
- Ochrana proti přírodním katastrofám
- Kvalitní podpora aplikace
- Výkonný a spolehlivý nástroj
- Možnost napojení cloudového řešení s lokálním serverem

## **Zranitelnosti**

- Je možné, že po největším DDOS útoku, který AZURE ustál, může být terčem dalších útoků.
- Ne všechny služby jsou dostupné ve všech regionech.
- Azure poskytuje velké množství služeb pro IaaS nebo PaaS, ale ne všechny tyto služby jsou dostupné ve všech oblastech, což může být pro podniky problém a odrazovat je od nasazení v Azure.
- Řešení nezahrnuje efektivní řešení pro migrace
- Neexistující podpora u Veeam Backup na MacOS, neexistuje možná instalace.

## **SWOT analýza řešení pro malou/střední společnost**

V malé/střední firmě byly nastavené požadavky s vysokou preferencí ceny řešení a možností využití vybraného řešení pro více funkcí. Na základě kritérií byl zvolen zálohovací software od Acronisu, který podporuje zálohování na připojený externí disk, který by v tomto případě byl přidělen zaměstnancům společnosti.

Dále bylo řešení doplněno o zálohování na cloud poskytovaný přímo od poskytovatele softwarového řešení. Celkově tento „ekosystém“ zajišťuje funkční a jednotné prostředí pro efektivní zálohování a archivace dat. Nejdůležitější body jsou zmíněny níže ve SWOT analýze.

### **Silné stránky**

- Možnost nastavení notifikací
- Efektivní propojení cloudu se samotným nástrojem
- Jednoduché na správu všech záloh
- Jednoduchá instalace a konfigurace
- Rychlá obnova
- Možnost využívání kapacity externích disků

### **Slabé stránky**

- Je třeba používat silné internetové připojení při využívání cloudových služeb.
- Toto řešení lze použít jenom v případě, že korporace neoperuje v oblastech, kde není Azure podporován.
- V případě, že ano, tak je třeba zvolit jiné řešení.
- Je třeba chvíli strávit nad pochopením samotného nástroje a uživatelského rozhraní.

### **Příležitosti**

- Díky nízké náročnosti procesu zálohování je možné tyto zálohy provádět v běžném procesu bez potíží s výkonem.
- Toto řešení nabízí taktéž další funkce jako např. migrace systémů.
- Ochrana před přírodními katastrofami díky využití offside úložiště.
- Jedná se o nízkonákladové řešení.

### **Zranitelnosti**

- Vysoká míra aktualizací kvůli špatným analýzám a identifikacím bugů.
- Existuje mnoho přeprodejců, kteří poskytují tyto služby formou pronájmu s dlouhou dobou trvání smluv



## **SWOT analýza řešení pro domácnost**

Domácnost je prostředí, kde není potřeba vymýšlet žádné technické vymoženosti, protože existují uživatelsky nenáročná a nenákladná řešení. Tím je například vybrané používání softwaru EaseUS, který je placen jednorázově za nízkou cenu, je jednoduchý na používání a ve spojení s používáním externího disku bohatě naplní požadavky domácnosti.

Tento výběr byl doplněn o používání vysokokapacitního cloudového řešení od Blomp, které je dostupné zdarma, pro sdílení dat pro osobní potřeby. Stejně jako v předchozích případech, jsou níže zmíněné jednotlivé body, které jsou pro toto řešení nejpodstatnější ve SWOT analýze celého řešení.

### **Silné stránky**

- Jednoduché nastavení a instalace, které je vhodné i pro netechnicky zdatné uživatele
- Vysoká kapacita úložiště

### **Slabé stránky**

- Chybějící automatizace zálohování na úložiště offsite.

### **Příležitosti**

- Nízká nákladnost řešení.
- Možnost funkce sdílení dat v domácnosti a lehkého přesouvání dat ze zařízení na zařízení.
- Poskytuje jednoduchou a zabezpečenou ochranu dat.

### **Zranitelnosti**

- Řešení vyžaduje interakci s člověkem pro ideální fungování.
- Nechrání všechna data před přírodní katastrofou

SWOT analýza byla provedena formou brainstormingu s kolegy v SABO IT, kteří byli seznámeni s problematikou mé bakalářské práce a během půl hodiny byly vzneseny některé připomínky a hodnocení, které byly dále přepracovány do jednotlivých bodů v samotné SWOT analýze

V řešení bylo cílem dospět k takzvanému řešení dokonalé strategie zálohování. To lze však dle výše uvedených postupů vyvrátit. Vždy totiž existuje přijatelná kompromisní varianta, nikdy však ideální. Každé řešení má své klady a zápory a nikdy nelze vybrat univerzální řešení pro všechny potřeby a požadavky. Proto je trh s nabídkou ať už softwarových nástrojů, prostředí, či poskytovatelů, tak velký a nabídek existuje mnoho.

Bakalářská práce však přes absenci dokonalé strategie zálohování obsahuje strukturované řešení problematiky s komplexním, ale přesto standardizovaným postupem. U všech subjektů byla zvolena kompromisní varianta, která splňuje požadavky samotných subjektů.

## 7. Seznam použitých zdrojů

### Knižní zdroje

[18] PECINOVSKÝ, Josef. Archivace a komprimace dat. Praha: Grada Publishing a.s., 2003, ISBN 80-247-0659-8.

[21] BIGELOW, Stephen, J. Mistrovství v počítačových sítích, 2004. 992 s., ISBN: 80-251-0178-9

[22] NORTH CUTT, S. Bezpečnost sítí. CP Books. 2005. ISBN: 80-251-0697-7

[23] KŘÍŽ, Libor. Komprimační a archivační programy. 1. vydání. Praha: Computer Press, 2002. 115 s. ISBN 80-7226-757-4.

### Internetové zdroje

[1] Zálohování a obnova [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.acronis.cz/kb/zalohovani/>

[2] Zálohovací plány, Acronis [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.bluepartners.cz/slovník-it-pojmu/zalohovaci-plany/>

[3] Příčiny ztráty dat [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.zachrana-dat.cz/cz/zachrana-dat-priciny-ztraty-dat.html>

[4] Příčiny ztráty dat [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.recoverycentrum.cz/priciny-ztraty-dat/>

[5] Kilián, Karel. *Zálohovací pásky mají stále co říct*, [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.zive.cz/clanky/zalohovaci-pasky-maji-stale-co-rici-fujifilm-chysta-novinku-s-kapacitou-400-tb/sc-3-a-204757/default.aspx>

[6] SSD vs HDD, Intel [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.intel.in/content/www/in/en/products/docs/memory-storage/solid-state-drives/ssd-vs-hdd.html>

[7] Network Attached Storage [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://searchstorage.techtarget.com/definition/network-attached-storage>

[8] Diskety [online]. 2021 [cit. 2021-09-31]. Dostupné z <http://it.pedf.cuni.cz/~bobr/ucspoc/hwfd.htm>

[9] The Floppy Disk, IBM [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.ibm.com/ibm/history/ibm100/us/en/icons/floppy/>

[10] USB Flash Drive [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.techopedia.com/definition/2322/usb-flash-drive>

[11] Memory stick [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.techopedia.com/definition/5303/memory-stick>

[12] What is cloud technology and how does it work [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://dynamixsolutions.com/what-is-cloud-technology-and-how-does-it-work/>

[13] Direct Attached Storage [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.techopedia.com/definition/1073/direct-attached-storage-das>

[14] Network Attached Storage [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.techopedia.com/definition/26197/network-attached-storage-nas>

[15] Storage Area Network [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.techopedia.com/definition/1116/storage-area-network-san>

[16] Definice rotace záloh StorageCZ [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.3s.cz/cs/odborna-sekce/detail/id/46-definice-a-rotace-zaloh>

[17] RAID disková pole, jaké jsou základní typy a v čem se liší. 2021 [online]. 2021 [cit. 2021-09-31]. Dostupné z <https://www.master.cz/blog/raid-diskova-pole-jake-jsou-zakladni-typy-a-v-cem-se-lisi/>

[19] What is cloud storage [Online]. 2021 [cit. 2021-27-31]. Dostupné z <https://aws.amazon.com/what-is-cloud-storage/>

[20] Autor

## 8. Zdroje sběru dat

[1] <https://linuxtechlab.com/cloud-backup-roundup-azure-vs-aws-vs-gcp/>

[2] <https://cloud.google.com/storage/pricing#europe>

[3] <https://docs.microsoft.com/en-us/answers/questions/269229/windows-server-backup-options-full-vs-bare-metal-r.html>

[4] [https://acloudguru.com/videos/cloud-provider-comparisons/cloud-provider-comparisons-aws-vs-azure-vs-gcp-storage?utm\\_campaign=11244863417&utm\\_source=google&utm\\_medium=cpc&utm\\_content=469352928666&utm\\_term=&adgroupid=115625160932&gclid=CjwKCAiA866PBhAYEiwANkIneJnsCutV9mq43n-p-fFKctkXqgrJBESMcTLM2a\\_Tv7ISZOmho62xoCqnYQAvD\\_BwE](https://acloudguru.com/videos/cloud-provider-comparisons/cloud-provider-comparisons-aws-vs-azure-vs-gcp-storage?utm_campaign=11244863417&utm_source=google&utm_medium=cpc&utm_content=469352928666&utm_term=&adgroupid=115625160932&gclid=CjwKCAiA866PBhAYEiwANkIneJnsCutV9mq43n-p-fFKctkXqgrJBESMcTLM2a_Tv7ISZOmho62xoCqnYQAvD_BwE)

[5] <https://sourceforge.net/software/product/IBM-Spectrum-Protect/>

[6] <https://geekflare.com/enterprise-data-backup-solution/>

- [7] <https://www.unitrends.com/backup-cost-calculator>
- [8] <https://sourceforge.net/software/product/Commvault-Complete-Data-Protection/>
- [9] <https://sourceforge.net/software/product/Cohesity/>
- [10] <https://www.veeam.com/cz/smb-vmware-hyper-v-essentials.html?ad=in-text-link#pricing-block>
- [11] <https://sourceforge.net/software/product/Veeam-Backup-Replication/>
- [12] <https://sourceforge.net/software/backup/for-enterprise/?page=2>
- [13] <https://www.peerspot.com/landing/report-product-rubrik>
- [14] <https://sourceforge.net/software/product/Acronis-Cyber-Backup-Cloud/>
- [15] <https://sourceforge.net/software/backup/for-enterprise>
- [16] <https://dealna.com/article/post/7635/What-is-a-storage-server-and-how-does-it-work>

## 9. Obrázky

- [1] <https://www.computerhistory.org/revolution/mainframe-computers/7/182/736>
- [2] <https://www.acronis.cz/kb/diferencialni-zaloha/>
- [3] <https://www.3s.cz/cs/odborna-sekce/detail/id/46-definice-a-rotace-zaloh>
- [4] <https://www.master.cz/blog/raid-diskova-pole-jake-jsou-zakladni-typy-a-v-cem-se-lisi/>

## 10. Seznam tabulek

- [1] Tabulka Subjektů
- [2] Tabulka strategií
- [3] Tabulka VAV Software 1
- [4] Tabulka VAV Software 2
- [5] Tabulka VAV Software 3
- [6] Tabulka VAV OS
- [7] Tabulka VAV cloud

- [8] Tabulka VAV SW malá firma 1
- [9] Tabulka VAV SW malá firma 2
- [10] Tabulka VAV SW malá firma 3
- [11] Tabulka VAV SW prostředí malá firma
- [12] Tabulka VAV domácnost