

Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií



Bakalářská práce

Zálohování a ochrana dat

Martin Valeš

© 2016 ČZU v Praze

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

Martin Valeš

Provoz a ekonomika

Název práce

Zálohování a ochrana dat

Název anglicky

Data protection and backup

Cíle práce

Cílem této práce je seznámit čtenáře se základními pojmy v oblasti zálohování dat, dále popis správného postupu zálohování důležitých dat pro běžné uživatele a informovat je o možnostech zálohování. Uvést hlavní výhody a nevýhody různých typů zálohování, srovnání placených a neplacených zálohovacích programů včetně Cloud Computing serverů. Praktická část je věnována zkoumání konkrétních zálohovacích softwarů v praxi.

Metodika

Práce je zpracována na základě prostudování odborné literatury, která se zabývá danou problematikou. Dále praktického zkoumání a posuzování různých typů zálohovacích softwarů pomocí objektivních srovnávacích metod.

Doporučený rozsah práce

40

Klíčová slova

zálohování, zálohovací software, úložiště, data, obnova dat, ztráta dat

Doporučené zdroje informací

DOSEDĚL, T. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. 190 s. ISBN 80-251-0106-1

LEBER, J. Windows NT: zálohování a obnova dat: příručka pro správce systémů. Praha: Computer Press, 1998. 282 s. ISBN 80-7226-123-1

LEIXNER, M. PC – zálohování a archivace dat: Nestůjte za dveřmi. Praha: Grada Publishing, 1993. 394 s. ISBN 80-85424-73-8

Pecinovský, Josef. 2003. Metody a možnosti zálohování počítačových dat. 1. vydání. Praha : Grada Publishing, 2003. str. 116. ISBN 80-247-0659-8.

Předběžný termín obhajoby

2015/16 LS – PEF

Vedoucí práce

Ing. Tomáš Vokoun

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 28. 10. 2015

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 10. 11. 2015

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 21. 12. 2015

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Zálohování a ochrana 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 8. 3. 2016

Poděkování

Rád bych touto cestou poděkoval svému vedoucímu bakalářské práce panu Ing. Tomáši Vokounovi za vedení mé práce a konzultace spojené s problematikou zálohování. Dále bych rád poděkoval IT pracovníkům z firmy Lom Praha, s. p., za konzultace a cenné rady spojené s tématem bakalářské práce.

Zálohování a ochrana dat

Souhrn

Bakalářská práce se zabývá problematikou zálohování a ochranou dat v domácím prostředí. Práce je rozdělena na dvě části. První část je věnovaná teorii, budou zde vysvětleny základní pojmy ochrany dat a procesu zálohování, jako jsou základní typy záloh, média a způsoby zálohování.

V druhé části budou hodnoceny zálohovací softwary a cloudová úložiště podle různých kritérií. Aplikace pro testování budou hodnoceny v operačním systému Windows 7 Home Premium. Na závěr budou navrženy možné varianty postupu zálohování a poukázáno na ekonomické úspory dosažené zálohováním dat.

Klíčová slova: zálohování, zálohovací software, úložiště, data, obnova dat, ztráta dat, cloud, pevný disk, zabezpečení, komprimace, šifrování

Data Protection and Backup

Summary

The upcoming pages of this bachelor paper are dedicated to the issue of data backup and data protection in the environment of a household. The first part is focused on theory and explanation of the basic concept of data protection and data backup. Those concepts include basic types of backup, media and forms of backup application.

The second part aims for reviewing backup software and cloud storages by different criteria. Applications used in reviews will be running on the Windows 7 Home Premium operating system. At the end of the paper, there will be presented variations of backup procedures and possible economic savings achieved by data backup.

Keywords: backup, backup software, storage, data, data recovery, data loss, cloud, hard disk, security, compression, encryption

Obsah

1	Úvod.....	12
2	Cíl práce a metodika	13
2.1	Cíl práce.....	13
2.2	Metodika	13
3	Teoretická východiska	14
3.1	Ochrana dat	14
3.1.1	Důvody ochrany dat.....	14
3.1.2	Základní způsoby ochrany dat	15
3.1.3	Pokročilé metody ochrany dat	22
3.2	Zálohování	25
3.2.1	Důvody zálohování	25
3.2.2	Typy záloh	27
3.2.3	Zálohovací cyklus	29
3.2.4	Způsoby zálohování dle použití nástrojů	30
3.2.5	Média pro zálohování	31
3.3	RAID.....	35
3.4	Komprimace dat.....	36
4	Vlastní práce	38
4.1	Srovnání zálohovacích softwarů.....	38
4.1.1	Freeware aplikace	40
4.1.2	Placené (komerční) aplikace	45
4.1.3	Celkové srovnání	50
4.2	Hodnocená cloudová úložiště	52
4.2.1	Srovnání cloudů	54
4.3	Návrh postupu zálohování	56
4.4	Ekonomická úspora.....	57
5	Závěr	60
6	Seznam použité literatury	61
7	Přílohy.....	64

7.1	Příloha A	64
7.2	Příloha B	70

Seznam obrázků

Obrázek 1 - princip fungování firewallu, zdroj: [http://www.ebrahma.com/wp-content/uploads/2015/04/Firewall-%E2%80%93-Basic-concepts.jpg]	19
Obrázek 2 - Nejčastější příčiny ztráty dat, zdroj: [http://www.itbiz.cz/tiskove-zpravy/firmy-stale-podcenuji-zalohovani-dat-tento-risk-pro-ne-muze-byt-likvidacni]	27
Obrázek 3 - - systém inkrementálních záloh, zdroj: [http://sysinfotools.com/blog/wp-content/uploads/2013/07/incremental-backup.png]	28
Obrázek 4 - systém diferenciálních záloh, zdroj: [http://www.leo-backup.com/images2/Differential-backup.jpg]	29
Obrázek 5 - Průřez strukturou CD, zdroj: [http://notebook.cz/clanky/technologie/2009/vyvoj-optickych-medii-1-cd].....	32
Obrázek 6 - Acronis True Image (úvodní obrazovka), zdroj: vlastní tvorba.....	64
Obrázek 7 - Acronis True Image (tabulka pro vložení šifrovacího klíče), zdroj: [vlastní tvorba].....	65
Obrázek 8 - Acronis True Image (nastavení rozvrhu záloh), zdroj: [vlastní tvorba].....	65
Obrázek 9 - Acronis True Image (výběr typu zálohy), zdroj: [vlastní tvorba].....	66
Obrázek 10 - Acronis True Image (nastavení úrovně komprese), zdroj: [vlastní tvorba] ...	66
Obrázek 11 - Acronis True Image (spuštění zálohovacího procesu), zdroj: [vlastní tvorba]	67
Obrázek 12 - Acronis True Image (výběr typu zálohování), zdroj: [vlastní tvorba]	68
Obrázek 13 - Acronis True Image (výběr konkrétní složky pro zálohování), zdroj: [vlastní tvorba].....	68
Obrázek 14 - Acronis True Image (výběr cíle zálohy Acronis Cloud), zdroj: [vlastní tvorba].....	69
Obrázek 15 - Cobian Backup 11 (úvodní obrazovka), zdroj: [vlastní tvorba]	70
Obrázek 16 - Cobian Backup 11 (výběr typu zálohy), zdroj: [vlastní tvorba]	71

Obrázek 17 - Cobian Backup 11 (výběr zdroje zálohy), zdroj: [vlastní tvorba]	71
Obrázek 18 - Cobian Backup 11 (výběr cíle pro vytvoření zálohy), zdroj: [vlastní tvorba]	72
Obrázek 19 - Cobian Backup 11 (nastavení rozvrhu záloh), zdroj: [vlastní tvorba]	72
Obrázek 20 - Cobian Backup 11 (nastavení komprese a šifrování), zdroj: [vlastní tvorba]	73
Obrázek 21 - Cobian Backup 11 (spuštění zálohovacího procesu), zdroj: [vlastní tvorba]	73
Obrázek 22 - Cobian Backup 11 (výběr cíle zálohy- cloud), zdroj: [vlastní tvorba]	74

Seznam tabulek

Tabulka 1 - Přehled 25 celosvětově nejpoužívanějších hesel, zdroj: [http://www.zive.cz/bleskovky/25-nejpouzivanejsich-hesel-minuleho-roku-uzivatele-jsou-nepoucitelni/sc-4-a-181099/default.aspx].....	16
Tabulka 2-Kriteriální tabulka, zdroj: [autor]	39
Tabulka 3 - hodnocení Cobian Backup 11 (Gravity), zdroj: [autor]	40
Tabulka 4 - hodnocení 7Backup, zdroj: [autor]	42
Tabulka 5 - hodnocení SyncBackFree V7.5.19, zdroj: [autor]0.....	43
Tabulka 6- Hodnocení Windows Zálohování, zdroj: [autor].....	44
Tabulka 7- přehled hodnoceného komerčního softwaru, zdroj: [http://www.sw.centrum.cz/zalohovani-a-obnova-dat/] zdroj: [http://cs24.inshop.cz/inshop/shop.asp?kat=20097534-1-B88]	45
Tabulka 8 - hodnocení Acronis True Image 2016, zdroj: [autor].....	46
Tabulka 9 - hodnocení Norton Ghost 15.0, zdroj: [autor]	47
Tabulka 10 - hodnocení Backup4all Professional, zdroj: [autor]	48
Tabulka 11 - hodnocení O&O DiskImage Professional Edition, zdroj: [autor]	49
Tabulka 12- Celkové srovnání hodnocených zálohovacích softwarů, zdroj: [autor]	51
Tabulka 13- možnosti rozšíření Google Drive, zdroj: [https://support.google.com/drive/answer/2375123?hl=cs]	53
Tabulka 14- možnosti rozšíření MEGA.....	53
Tabulka 15- Výchozí tabulka hodnocení cloudových úložišť	55
Tabulka 16- bodově ohodnocená tabulka hodnocení cloudových úložišť.....	55
Tabulka 17 - ekonomická náročnost varianty A, zdroj: [http://www.czc.cz/verbatim-store-n-go-usb-3-0-500gb-black/87544/produkt]	

.....	57
Tabulka 18 - ekonomická náročnost varianty B,	
zdroj: [http://www.czc.cz/verbatim-store-n-go-usb-3-0-500gb-black/87544/produkt].....	57
Tabulka 19 - Modelový příklad nákladů na záchranu dat č. 1,	
zdroj: [http://www.datahelp.cz/cenik-zachrany-dat/harddisk/]	
.....	58
Tabulka 20 - Modelový příklad nákladů na záchranu dat č. 2,	
zdroj: [http://www.datahelp.cz/cenik-zachrany-dat/harddisk/]	59

Seznam grafů

Graf 1 - Celkové srovnání hodnocených zálohovacích softwarů, zdroj: [autor]	51
Graf 2 -Grafické znázornění bodového hodnocení kritérií, zdroj: [autor].....	56

1 Úvod

V dnešní době neustále stoupá využívání informačních technologií, každý den používáme různé informační technologie, jako jsou počítače, mobilní zařízení, tablety atd. a ukládáme do nich svá cenná data. Vzhledem k tomu, že data jsou to nejcennější, co se může v počítači nebo jiných zařízeních nacházet, tak je velmi důležité vysvětlit si, jak správně svá data chránit proti zneužití cizími osobami, jak je zálohovat a tím je chránit proti náhlé ztrátě, v jakém intervalu provádět zálohy a na jaká média. Protože by pro mnoho běžných uživatelů mohlo být zálohování velmi složité, tak si v praktické části ukážeme několik zálohovacích softwarů a ty budeme posuzovat podle určitých kritérií, dále bude srovnáno několik cloudových úložišť a navrhnuty možné varianty pro provádění zálohování za využití určitého softwaru a médií pro ukládání.

2 Cíl práce a metodika

2.1 Cíl práce

Cílem této práce je vysvětlení základních pojmů v oblasti zálohování a ochrany dat, dále popis správného postupu zálohování důležitých dat pro běžné uživatele a informovat je o možnostech zálohování. Uvést hlavní výhody a nevýhody různých typů záloh, srovnání placených a neplacených zálohovacích programů včetně Cloud Computing serverů, konkrétně cloudových úložišť. Praktická část je věnována zkoumání konkrétních zálohovacích softwarů v praxi a hodnocení cloudů.

2.2 Metodika

Zálohovací programy a cloudová úložiště budou v praktické části hodnoceny na základě provedené vícekritériální analýze variant. Jednotlivé váhy kritérií u zálohovacího softwaru budou uděleny metodou alokace 100 bodů. Váhy u cloudových úložišť budou sestaveny na základě metody bodovací. Aplikace byly posuzovány dle následujících kritérií, kterými jsou složitost instalace, uživatelské prostředí, jazykové rozhraní a nadstandartní nástroje aplikace, podpora plné, inkrementální a diferenciální zálohy, dále jestli daná aplikace disponuje možností rozvrhu záloh, zálohování na servery FTP, možnost komprimace záloh, tvorba více zálohovacích úloh (tzv. multizálohování), zálohování na základě typu souboru, možnost šifrování záloh, dále zda je přítomna logovací tabulka pro ověření úspěšnosti zálohování a poslední kritérium obnova ze zálohy.

Pro posuzování cloudových úložišť byly vybrány následující kritéria, jako je bezplatný úložný prostor, maximální velikost nahraného souboru, dostupnost na jiných platformách (Windows, MAC, iOS, Android) a poslední kritérium je zda úložiště poskytuje desktopovou aplikaci pro synchronizaci. Váha kritérií byla stanovena metodou pořadí.

3 Teoretická východiska

3.1 Ochrana dat

To nejcennější, co máme ve svém počítači, mobilním telefonu nebo v jiném zařízení jsou data. U dat může dojít k jejich poškození, ztrátě nebo zneužití neoprávněnou osobou.

Proto by se každý uživatel měl zaměřit na ochranu svých dat a informací, které má ve svém zařízení, ale zároveň by se měl též zaměřit na ochranu soukromí, neboť tento faktor též ohrožuje bezpečnost dat.

3.1.1 Důvody ochrany dat

V prvé řadě bychom měli chránit svá data z hlediska důvěrnosti, dále bychom je měli chránit proti neoprávněné změně nebo neúmyslnému či úmyslnému zničení. (Doseděl, 2004)

K poškození nebo smazání dat může dojít například při poruše hardware, živelné pohromě nebo i při zásahu bleskem. Příčin může být několik, nicméně nelze opomenout ochranu dat před cizími osobami. (Doseděl, 2004)

V mnoha případech jsou počítače v domácnostech vystaveny většímu riziku než firemní počítače, protože jejich uživatelé ve většině případů nedodržují obecné zásady bezpečnosti na internetu. Navštěvují jakékoliv webové stránky, které mohou být infikované, dále otevírají přílohy z neznámých emailů, zveřejňují na internetu příliš citlivé informace, jako jsou například rodná čísla, adresa bydliště nebo i přístupové údaje. (Doseděl, 2004)

Svá data bychom měli chránit v následujících bodech:

1. **Fyzická ochrana dat** = měli bychom omezit přístup k diskům, kde ukládáme svá data před cizími osobami
2. **Logický přístup k datům** = chránit svá data i prostřednictvím hesla u operačního systému, aby bylo zamezeno přístupu neoprávněné osobě k datům, pokud se již k nim fyzicky dostane
3. **Ochrana dat v uložišti** = naše data by měla být chráněna vhodnými metodami i proti jejich přečtení, je vhodné zajistit nemožnost přečtení disku na jiném počítači

4. **Bezpečné přenášení dat v počítačové síti**

5. **Ochrana dat proti zničení** = ať už se jedná o úmyslné nebo neúmyslné zničení, či došlo k jejich ztrátě vlivem živelné pohromy (Doseděl, 2004 str. 48)

3.1.2 **Základní způsoby ochrany dat**

Uživatelské účty

Jedním ze základních způsobů ochrany našich dat, je již zabezpečení svého účtu v operačním systému Windows. Svůj účet bychom měli chránit silným heslem, dále omezit pravomoc ostatním uživatelům počítače, kteří by mohli případně i nechtěně smazat naše data.

V případě více uživatelů na jednom počítači, můžeme jejich pravomoc omezit zvolením typu účtu.

Například ve Windows 7 existují dva typy účtů:

1. Standardní uživatel
2. Správce

• **Standardní uživatel**

V tomto typu účtu může uživatel využívat téměř všechny software, ale v nastavení může provádět pouze takové změny, které neovlivní jiné uživatele nebo zabezpečení počítače. Tento typ účtu má například zabránit odstranění systémových souborů či instalaci nových software bez vědomí správce.

• **Správce**

Tito uživatelé mají úplný přístup k nastavení počítače a mohou provádět jakékoliv změny.

Dalším nástrojem pro ochranu uživatelských účtů je systémový nástroj operačního systému Windows “Řízení uživatelských účtů”, který upozorňuje uživatele na činnosti, které smí provádět pouze správce a mohou mít vliv na celkový chod systému. Toto upozorňování se dá nastavit ve čtyřech úrovních, od intenzivního, kdy je uživatel upozorněn na veškeré pokusy změn v operačním systému, až po naprosté omezení oznámení (tato možnost se však vzhledem k bezpečnostním rizikům nedoporučuje).

Silná hesla

Častá chyba běžných uživatelů je volba jednoduchého nebo lehce předvídatelného hesla. Pro takzvané crackery, kteří se prolomením hesel zabývají, pak v takovém případě není problém heslo rychle a snadno zjistit a následně odcizit nebo zneužít Vaše data, neboť používají databáze nejčastěji používaných hesel a jejich kombinací. (Bezpečný internet)

Tabulka 1 - Přehled 25 celosvětově nejpoužívanějších hesel

password	trustno1	passw0rd	monkey	master
123456	dragon	shadow	1234567	sunshine
12345678	baseball	123123	letmein	ashley
qwerty	111111	654321	qazwsx	football
abc123	iloveyou	superman	michael	bailey

Zdroj: Živě.cz, vlastní tvorba

Lidé by se měli ke svým heslům stavit stejně jako k ostatním cennostem a přikládat jim stejnou váhu. Volba silného hesla je naprosto nezbytná.

Silné heslo by mělo obsahovat minimálně 8 znaků při kombinaci velkých a malých písmen s číslicemi a speciálními znaky. Heslo by mělo být pro uživatele snadno zapamatovatelné, nicméně by nemělo být snadno předpověditelné pro ostatní osoby, které například dotyčného znají. (Horák, 2006)

Dále bezpečné heslo by se nemělo používat vícekrát než jednou, protože pokud budeme toto heslo používat na více místech, tak při zdařilém útoku získá útočník heslo pro všechny ostatní účty a v případě, že toto heslo používáte v místech, kde dochází k finančním tokům, riskujete materiální ztrátu.

Bohužel i mimo zabezpečení uživatelského účtu ve Windows lidé nepoužívají bezpečná hesla, jak pro přístupová například do emailové schránky, tak i možnosti pro obnovu těchto hesel. Vzhledem ke zvyšujícímu se využívání sociálních sítí, kde mnoho lidí nevědomky poskytuje cenné osobní informace o svém životě, tak není vhodné používat pro obnovu hesla otázky typu “Jméno matky za svobodna nebo jméno domácího mazlíčka”, neboť tyto údaje jsou snadno dohledatelné.

Ukládání hesel

Vzhledem k tomu, že běžní uživatelé používají při práci na svém počítači více jak jeden účet, například mají účty na sociálních sítích, v internetovém bankovníctví, emailech, různých fórech nebo i na školních stránkách přichází na řadu otázka, jak si zapamatovat všechny tyto hesla, pokud se stejné heslo nemá používat více než jednou.

Samozřejmě je možné zapsat si všechna hesla na kousek papíru a ten uschovat někde v bytě, nicméně v případě, že dojde k živelné pohromě a byt vyhoří, tak přijdeme o všechna uložená hesla. Dále se můžeme stát obětí krádeže a tyto údaje mohou být i zneužity.

Další variantou by mohlo být uložení hesel například v poznámkovém bloku v počítači, ale v případě virového útoku nejsou tyto hesla nijak šifrována a jsou čitelná pro veškeré okolí.

Nejběžnější metodou ukládání hesel u běžných uživatelů je ukládání hesel přímo ve webovém prohlížeči, například v prohlížeči Mozilla Firefox, kde je přímo integrován správce hesel. Hesla, která ve webovém prohlížeči uložíme, jsou automaticky šifrována na disku a nečitelná pro okolí. Nicméně pokud by se někdo neoprávněný dostal k počítači, tak si může nechat hesla snadno zobrazit, proto je zároveň vhodné vytvořit si jedno hlavní heslo, které bude použito pro přístup do této databáze. Avšak ani tato varianta nechrání uložená hesla před výpadkem softwaru nebo hardwaru a můžeme tak snadno přijít o svá uložená hesla. (Mozilla)

• Ukládání hesel v Cloudu

Další zajímavou možností, je uložení hesel v cloudu, jedná se o moderní a v nynější době již o bezpečný způsob uložení přihlašovacích údajů, licenčních klíčů atd. Cloud pro ukládání hesel funguje na podobném principu jako ostatní cloudové služby, kdy při registraci na příslušné stránce získáte účet a tím přístup do databáze, kde budete svá hesla ukládat. Celá databáze je uložena na serverech poskytovatele, kde je šifrována a tím zabezpečena proti možnému zneužití. Zároveň ani poskytovatel služby by neměl znát naše hesla, neboť nezná naše přihlašovací údaje, pro větší jistotu si uživatel může zvolit navíc šifrovací klíč ke svému účtu. (Tuhý, 2013)

Přístup k heslům je pak závislý na konkrétní službě, hesla mohou být přístupná po přihlášení do webového rozhraní nebo mohou používat plugin (rozšíření). (Tuhý, 2013)

Hlavní výhodou tohoto řešení je, že uživateli stačí si zapamatovat jen jedno heslo a to pro přístup do Cloudu, dalšími výhodami jsou možné připojení odkudkoliv, automatické vyplňování přihlašovacích údajů, zálohování uložených hesel a další doplňkové služby, které jsou již závislé na poskytovateli a zda se jedná o bezplatnou či placenou verzi, nicméně jednou z doplňkových služeb může být zaslání hesla bezpečnější formou než emailem. (Tuhý, 2013)

S tímto způsobem ukládání hesel jsou však spojena určitá rizika, jako je například svěřování pro nás nejcitlivějších údajů (hesel) třetí straně, proto je důležité vybrat službu, která je maximálně důvěryhodná, aby nedošlo k jejich odhalení a zároveň bychom si měli zvolit maximálně bezpečné přístupové heslo nejlépe v kombinaci se šifrovacím klíčem. Dalším rizikem je potenciální nedostupnost služby, pokud nemáme vytvořenou kopii hesel na disku a dojde k výpadku služby, tak nemáme šanci dostat se k našim heslům a v případě chyby na straně poskytovatele můžeme o svá data i přijít. (Tuhý, 2013)

Firewall

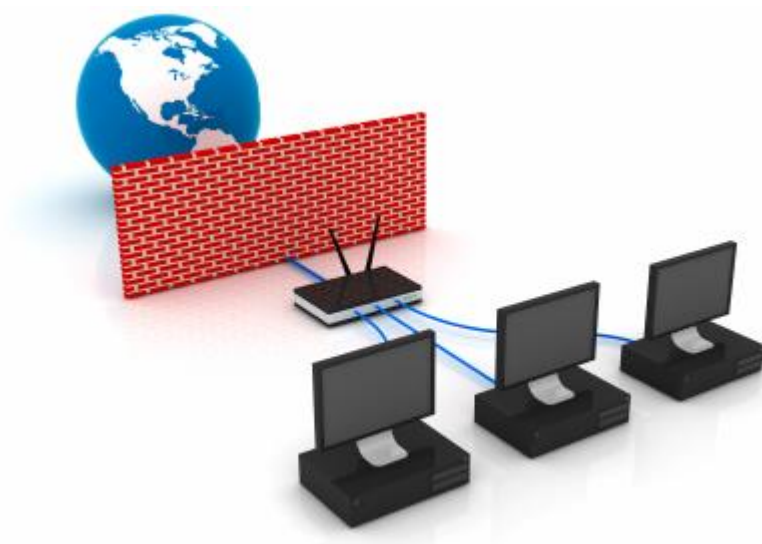
Jedná se o základní nástroj v operačním systému, který chrání data uživatelů před hrozbami z vnějšího (internetového) prostředí. (Doseděl, 2004)

Firewall znamená v překladu bezpečnostní brána, jedná se o software nebo hardware, který stojí mezi dvěma sítěmi, domácí sítí uživatelů a internetovou sítí. Zabraňuje neoprávněným průnikům do naší sítě a zároveň odesílání dat bez našeho vědomí a povolení. (Doseděl, 2004)

Jeho úkolem je tedy regulace propouštění dat mezi těmito sítěmi prostřednictvím předem definovaných pravidel, kterými jsou identifikace zdroje a cíle dat, sběr informací o stavu spojení a znalost kontrolovaných protokolů či prvků IDS. (UNET)

Firewally můžeme zařadit do kategorií na paketové filtry, stavové paketové filtry a stavové paketové filtry s kontrolou protokolů či v kombinaci s IDS a aplikační brány. (UNET)

Uživatelé mohou využít firewall přímo od poskytovatele operačního systému, například Windows Firewall od společnosti Microsoft, dále personální firewally, které bývají většinou již integrovány v komplexním balíku antivirových programů nebo si samozřejmě mohou přídavný personální firewall doinstalovat zvlášť.



Obrázek 1 - princip fungování firewallu, zdroj: [ebrahma.com]

Základní rozdělení firewallů

- **Paketové filtry:**

Firewally pracující na této úrovni přenášejí data po blocích, které se označují jako tzv. pakety. Například u paketů na bázi TCP/IP protokolů firewall rozhoduje o tom, které IP adresy pustí a které naopak tzv. odfiltruje. (UNET)

Paketové filtry bývají často součástí routerů, jejich výhodou bývá zpravidla vysoká rychlost právě díky jejich vcelku jednoduché činnosti, kdy kontrolují jen zdrojovou a cílovou adresu. Naopak jejich nevýhoda spočívá v neschopnosti upozornit administrátora na případné podezřelé aktivity. (UNET)

- **Aplikační brány:**

Všechny pakety, které nejsou přímo povoleny, jsou striktně filtrovány, v tom je hlavní rozdíl oproti paketovým filtrům. (Doseděl, 2004)

Tato varianta je daleko pokročilejší a bezpečnější než varianta paketových filtrů, na druhou stranu její nevýhodou je nižší rychlost a omezené množství služeb, které jsou podporovány. (Amenit)

V případě potřeby nové služby je nutné vytvořit novou aplikaci neboli proxy, který bude stát mezi nedůvěryhodnou a chráněnou sítí a bude kontrolovat všechny pakety pro konkrétní službu. (Amenit)

- **Stavový paketový filtr**

Tento typ filtru monitoruje komunikaci protokolů vyšší vrstvy, zejména protokoly TCP a UDP. Do naší sítě povolí pouze ty pakety, na které byl z naší strany vydán podnět. Například pokud se pokusíme navázat spojení s FTP serverem, budou poté povoleny všechny pakety v obou směrech, týkající se této relace. Na druhou stranu z naší sítě je povolen veškerý průchod paketů do internetu, neboť tento typ filtru nechrání internetovou síť proti útokům z naší sítě. (Doseděl, 2004)

Mezi hlavní výhody stavových paketových filtrů patří zejména lepší úroveň zabezpečení než u jednoduchých paketových filtrů, vysoká rychlost a snadná konfigurace. (UNET)

Naopak nevýhodou je nižší bezpečnost oproti aplikačním branám. (UNET)

Konfigurace Windows Firewall

Konfigurace brány Windows Firewall je snadná, neboť obsahuje jen 4 základní možnosti nastavení.

1) Zapnout bránu

Tato možnost je nastavená jako výchozí. Při této variantě je u většiny programů zablokována komunikace přes bránu Firewall. Pro odblokování musí být program přidán do seznamu výjimek. (Microsoft)

2) Blokování všech příchozích připojení včetně povolených programů

V této variantě dochází k blokování všech nevyžádaných pokusů o připojení k počítači. Toto nastavení se používá, pokud je zapotřebí maximálního zabezpečení, například při připojení k veřejné síti nebo při hrozícím riziku nakažení počítačovým červem.

Navzdory blokování veškerého příchozího připojení je možné navštívit většinu internetových stránek nebo odesílat či přijímat emaily. (Microsoft)

3) Upozornění na zablokování nového programu

Windows Firewall vás upozorní, pokud zablokuje nový program a zároveň nabídne možnost jeho odblokování. (Microsoft)

4) Vypnout bránu

Toto nastavení se nedoporučuje, pokud není v zařízení nainstalován jiný personální firewall. V případě absence brány firewall se zařízení stává zranitelnější proti škodlivým softwarům nebo útoku hackera. (Microsoft)

Antivirová ochrana

Antivirovou ochranou rozumíme ochranu dat proti zničení nebo zneužití před škodlivým softwarem neboli malwarem, jakou jsou viry, červy, makroviry, trojské koně, spyware, hijackery. (Horák, 2006)

V případě antivirové ochrany je nejsnazší způsob prevence prostřednictvím kvalitního antivirové a antispywarového programu, pravidelných aktualizací všech programu včetně Windows update. (Horák, 2006)

Malware

Malware je všeobecné označení škodlivého kódu, nejčastějším případem malwaru je počítačový vir, trojský kůň nebo červ. Cílem malwaru je provádění nežádoucích činností nebo poškodit uživatele. (Hoax)

Mnohé typy malwaru nesou název podle toho, jakou činnost v počítači vykonávají, příkladem může být spyware, který zasílá útočnickovi osobní údaje o uživateli, například číslo platební karty. (Kaspersky)

Antivirové programy

Antivirový program slouží jako ochrana proti virům, antivir dokáže prohledat paměť počítače i veškeré soubory, které jsou uloženy na pevném disku a nalézt přítomné viry. Antivirové programy bývají spuštěny již od spuštění počítače a chrání je nepřetržitě po celou dobu, kdy uživatel s počítačem pracuje, kontrolují veškeré spuštěné soubory a soubory, které do počítače přicházejí. (Kocman, a další, 2005)

Každý antivirový program má vlastní virovou databázi, která by měla být pravidelně aktualizována. Aktualizovaná virová databáze je nezbytná, protože antivir dokáže rozpoznat a bezpečně odstranit jen ty viry, které má ve své databázi. Dnešní antivirové programy jsou nastaveny tak, aby automaticky kontrolovaly aktuálnost své virové databáze. (Kocman, a další, 2005)

Antispywarové programy

Antispywarový program slouží jako doplněk k antivirovému programu, jeho cílem je nalezení a případné odstranění spywaru. Antispyware by měl chránit uživatele před odcizením jeho osobních údajů, dále by měl zabránit případům, kdy spyware automaticky stahuje a instaluje nežádoucí nebezpečné aplikace bez vědomí uživatele, dále by měl zabránovat spywarům měnit chování internetových prohlížečů (například odkazování na jinou stránku, než uživatel požadoval). (centrum)

Typickými příklady antispywarových programů mohou aplikace Spybot – S&D, Spyremover, Ad-Aware SE Personal nebo Spyware Blaster. (Kocman, a další, 2005)

3.1.3 Pokročilé metody ochrany dat

Duplikace

Duplikování datových nosičů je jednou z možností, jak chránit svá data. Jedná se o metodu, kdy jsou data ukládána na dva nosiče současně. Cílem této ochrany je tedy vyvarovat se riziku ztráty dat, při poruše pevného disku, neboť pravděpodobnost, že dojde k poruše obou disků zároveň je velmi malá. Toto riziko se dá ještě snížit tím, že se oba disky umístí daleko od sebe a tím se vyloučí vliv přírodních katastrof. (Doseděl, 2004)

Pokud jsou data zapisována na oba disky současně, musí být stejná i jejich úroveň zabezpečení proti všem případným nebezpečím. Dále v případě velké geografické vzdálenosti mezi oběma disky je nutné zajistit zabezpečení i pro přenosovou cestu, po které se data pohybují. (Doseděl, 2004)

Šifrování

Šifrování je základní nástroj kryptografie, jedná se o proces, kdy pomocí šifrovacího klíče a šifrovacího algoritmu vytvoříme z otevřeného textu šifrovaný text, který není možné

převést bez znalosti daného šifrovacího klíče a algoritmu zpět na otevřený text. (Kuchař, 1999)

Šifrování má za úkol změnit data do takové podoby, aby v případě, že se k nim dostane neoprávněná osoba, neměla šanci si je přečíst. (Kuchař, 1999)

Šifrovací klíč = Šifrovacím klíč představuje posloupnost jedniček a nul o určité délce, která je obvykle udávána v bitech. (Kuchař, 1999)

Šifrovací algoritmus

Algoritmus, který má za úkol utajit data jejich zašifrováním. Využívá k tomu nějaké tajemství, které nazýváme šifrovacím klíčem. Stejný šifrovací algoritmus může používat více lidí, avšak každý z nich musí mít k jeho šifrování a dešifrování vlastní jiný klíč. (Doseděl, 2004)

Šifrovací algoritmy se dělí na symetrické a asymetrické algoritmy.

- **Symetrické algoritmy**

Symetrické šifrovací algoritmy využívají pro proces šifrování i dešifrování identický šifrovací klíč, tyto typy algoritmů se používají v praxi především pro bezpečné ukládání dat na pevných discích notebooků a dále k zabezpečení například záložních medií. Využívají se zejména kvůli vyšší rychlosti oproti asymetrickým algoritmům. (Kuchař, 1999)

DES = šifrovací algoritmus, který vyvinula v sedmdesátých letech 20. století firma IBM. Šifrovací klíč má délku 56 bitů. V dnešní době se již nejedná o perspektivní algoritmus, protože již byly provedeny pokusy, které dokumentují jeho úplné zničení. (Kuchař, 1999)

3DES = Jedná se o zesílenou variantu algoritmu DES. Principem tohoto algoritmu je třikrát provedené přešifrování šifrovaných dat algoritmem DES a to první nebo druhou částí klíče. Šifrovací klíč je oproti DESu dvojnásobně dlouhý tj. obsahuje 112 bitů, nicméně oproti variantě DES je tento algoritmus z hlediska času třikrát pomalejší. (Kuchař, 1999)

AES (Advanced Encryption Standard) = Jeho původní název je Rijindael, který je odvozen po jeho tvůrcích, kterými jsou Vincent Rijmen a John Daemen. Jedná se o algoritmus vytvořený pro americkou vládu, který vznikl jako náhrada za již nevyhovující algoritmus

DES. AES je bloková šifra s šifrovacím klíčem, který může nabývat délky tří hodnot 128, 192 a 256 bitů, nicméně ve všech třech variantách má délka bloku 128 bitů a podle délky klíče se mění počet rund. (Doseděl, 2004)

IDEA = algoritmus vyznačovaný vysokou rychlostí, dále díky délce klíče 128 bitů poskytuje i dostatečnou bezpečnost. Je patentován firmou Ascom-Tech v USA a ve většině evropských zemí. (Kuchař, 1999)

BlowFish = nepatentovaný algoritmus s variabilní délkou šifrovacího klíče v rozmezí 32 - 448 bitů. Disponuje vysokým koeficientem bezpečnosti a rychlosti. (Kuchař, 1999)

- **Asymetrické algoritmy**

Algoritmy, které k procesu šifrování a dešifrování dat využívají dva různé klíče. Vygenerovaný klíč se rozdělí do dvou částí na soukromou a veřejnou část. Veřejný klíč je poskytován všem, od koho chceme přijímat šifrovaná data, soukromý klíč však musíme chránit. (Doseděl, 2004)

RSA = algoritmus sloužící k výměně klíčů a k tvorbě elektronického podpisu, RSA se řadí mezi neoficiální standardy. Bezpečnost tohoto algoritmu je založena na obtížnosti rozložení velkých čísel. Bezpečnost algoritmu je podmíněna délkou klíče. (Kuchař, 1999)

ECC = celým názvem „Eliptické kryptosystémy“, jde o algoritmy, které jsou založeny na řešení úloh diskretního logaritmu v grupách na eliptických křivkách. Jejich výhodou je velká kryptografická bezpečnost navzdory menší délce klíče například oproti RSA. Při dosažení totožné bezpečnosti jako RSA s klíčem o délce 2048 bitů mají klíče ECC délku jen 160 – 180 bitů. (Kuchař, 1999)

3.2 Zálohování

„Zálohování je proces kopírování souboru nebo adresáře na jiné místo nebo jiný druh nosiče. Původní soubor nebo adresář zůstává. Záložní kopie souboru nebo adresáře bývá později obnovena, jestliže počítačový systém postihne nějaká pohroma, jako je požár nebo krádež. Proces zálohování lze nastavit na část disku nebo celý disk“ (Leber, 1998 str. 7)

Zálohování je jedním z nejdůležitějších prvků ochrany dat, veškerá ochrana dat bez správného a pravidelného zálohování nám nedokáže naše drahocenná data ochránit, neboť tato forma chrání naše data před ztrátou, úmyslným či neúmyslným poškozením nebo smazáním tak, že se vytvoří jejich přesná kopie na záložní médium.

Zálohování by mělo probíhat v pravidelných intervalech na více zálohovacích médiích, ať už na pevný disk, optická media jako jsou DVD, CD nebo Blue-ray, ale zároveň není na škodu zálohovat data také na nějaké úložiště.

V první řadě je důležité si určit, jaká data budeme zálohovat, jak často budeme zálohovat a na jaká média. Od těchto otázek se také odvíjí i finanční náročnost zálohování. Dále bych rád podotkl, že rozhodně není správnou volbou snažit se ukládat veškerá data, protože je to velmi kapacitně náročné. Proto bychom si měli svá data rozřadit do kategorií, podle kterých budeme určovat, zda se jedná o data nahraditelná nebo nenahraditelná, data u kterých nás jejich ztráta nebude tolik bolet a na data, která mohou mít až existenční dopady, jako je například účetnictví. (Budai David, 2012)

Zálohovat bychom měli nejen data ze svého počítače a notebooku, ale také ze svých mobilních telefonů, tabletů a jiných zařízení, které běžně používáme, a kde může dojít ke ztrátě pro nás důležitých dat.

3.2.1 Důvody zálohování

Jelikož je dnešní doba plná nejrůznějších informačních technologií, které denně využíváme, ať už v práci nebo ve svém volném čase, tak bychom se měli postarat o to, aby data, se kterými každý den pracujeme nebo data, která jsou pro nás velmi důležitá, jako jsou

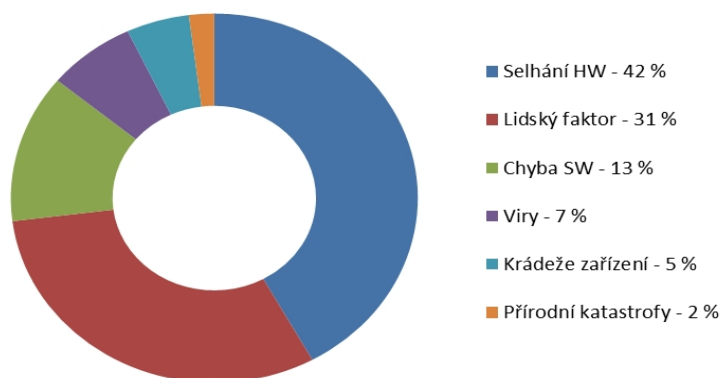
například rodinné fotografie, faktury, dokumenty atd. byly bezpečně uloženy i na jiném místě, jako záložní kopie, pro případ náhlé havárie počítače. (Pecinovský, 2003)

Sice dnes jsou počítače a podobná zařízení více kvalitní a méně poruchová, ale i tak každá věc má svou životnost a neměli bychom se spoléhat na štěstí, že se nám nic takového nemůže přihodit, protože zpravidla dojde k nějaké havárii v tu nejhorší dobu, kdy by mohl nastat. Například Vám odejde počítač ve chvíli, kdy dokončujete bakalářskou práci nebo den před odevzdáním jiného důležitého projektu. (Horák, 2006)

Uvedeme si nejčastější příčiny ztráty dat, jako je ztráta telefonu nebo notebooku, živelná pohroma, krádež, nechtěné smazání nezkušeným uživatelem. V případě krádeže má sice mnoho lidí svůj majetek pojištěn, ale data, která jsou v zařízení obsažena, již nikdy neuvidí a přitom například ztráta dat u velkého projektu daleko převyšuje hodnotu zařízení, které bylo odcizeno. V dnešní době se sice velké stolní počítače příliš nekradou, ale ukradnout notebook, tablet či mobilní telefon už tak složité není. (Pecinovský, 2003)

Například data v mobilu jsou daleko více ohrožena než data uložená v počítači, neboť ztráta telefonu je daleko běžnější než ztráta počítače, navíc telefon Vám může kdykoli nechtěně vypadnout z ruky a může tak dojít k nenávratnému mechanickému poškození a tím pádem i k nenávratné ztrátě dat. V dnešní době již však nedochází při ztrátě telefonu jen ke ztracení kontaktů, případně SMS zpráv, ale vzhledem k tomu, že mnoho z nás dnes používá telefon i jako fotoaparát, tak dochází i ke ztrátě pro nás cenných fotografií. V případě zálohy kontaktů, můžeme použít mnoho způsobů zálohy, od ručního přepsání kontaktů na papír, dále je můžeme přes software od výrobce telefonu do počítače nebo také můžeme využít možnost zálohy přes Google email nebo jakékoliv cloudové úložiště.

6 nejčastějších důvodů ztráty dat



Obrázek 2 - Nejčastější příčiny ztráty dat, zdroj: ITbiz.cz

3.2.2 Typy záloh

Různé strategie zálohování pracují odlišně s atributem Archivovat (Archive Flag), který je používán pro rozlišení, zda daný soubor byl již zálohován nebo ne. U nových a aktualizovaných souborů se tento bit automaticky nastaví na hodnotu „ON“, neboli na hodnotu, která značí, že soubor má být zálohován. (Leixner, 1993)

Atributy = jedná se o vlastnosti souboru, které jsou k dispozici v dialogovém okně vlastností. Prakticky existují čtyři typy atributů, jedná se o Systémový, Archivovat, Pouze pro čtení a skrytý.

- **Plná záloha**

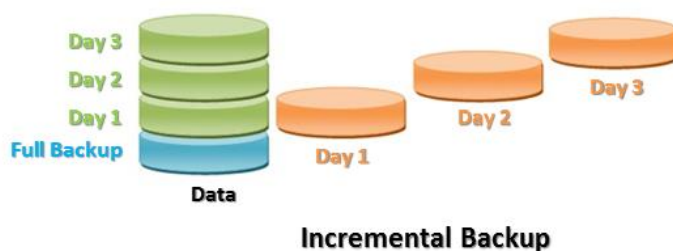
Jedná se o nejzákladnější formu zálohy, ze které poté vycházejí i ostatními typy záloh. Při plném zálohování jsou do zálohového setu uloženy všechny soubory, aniž by se bral ohled na to, zda některé soubory byly od posledního zálohování aktualizovány. Plné zálohování vlastně ignoruje stav atributu Archivovat. Po dokončení zálohy je tento atribut pro všechny zálohované soubory přepnut na hodnotu „OFF“.

Výhodou této formy zálohy je, že veškerá data jsou ukládána do jediného souboru, a proto je i tato metoda v případě potřeby obnovy dat nejrychlejší a nejsnazší. Avšak tato forma má na druhou stranu také mnoho záporů, především časová náročnost zálohy a vzhledem k tomu, že se zálohují veškerá data, tak je zde i vysoká náročnost z hlediska potřebné kapacity. Co se týká bezpečnostního rizika, tak v případě krádeže disku jsou odcizena naprosto veškerá data. (3S.CZ, 2012)

- **Inkrementální záloha**

Inkrementální neboli přírůstkové zálohování se zakládá na principu, kdy se k plné výchozí záloze postupně přidávají nové a aktualizované soubory. Jedná se vlastně o metodu částečného zálohování. Tato forma má podstatně menší časovou náročnost než u plné zálohy, proto je vhodná i pro denní zálohování. Nicméně v případě havárie diskového pole nebo serveru je nutné v první řadě obnovit plnou zálohu a poté postupně v časovém sledu od nejstarší po nejnovější obnovovat všechny inkrementální zálohy. Ačkoli se z počátku může tato forma jevit jako méně časově náročná, tak v případě obnovy je její časová náročnost větší než u plné zálohy. (3S.CZ, 2012)

Hlavní problém této metody je, že v případě poškození jedné z inkrementálních záloh jsou veškeré zálohy poškozeny a data nebude možné obnovit.

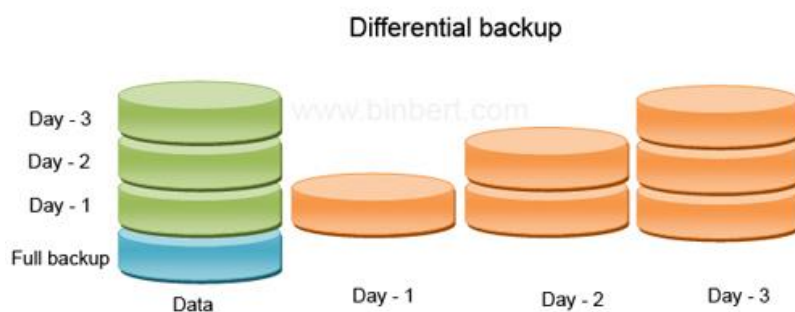


Obrázek 3 - - systém inkrementálních záloh, zdroj: [sysinfotools.com]

- **Diferenciální záloha**

Diferenciální zálohování je také metoda částečného zálohování, avšak oproti inkrementálnímu zálohování, které vytváří zálohy jen u posledních změn, tato metoda zálohuje veškeré soubory, které byly aktualizovány od výchozí plné zálohy. (Leixner, 1993)

Dalším rozdílem je, jak každá metoda přistupuje ke zpracování atributu Archivovat, kdy inkrementální metoda po zálohování nastaví atributy na „OFF“, tudíž pak při příštím zálohování nejsou tyto soubory zahrnuty v seznamu zálohování, pokud mezitím nedojde k jejich aktualizaci, naopak u diferenciálního zálohování zůstávají u souborů atributy Archivovat nastaveny na „ON“, tudíž v následujícím zálohování budou opět do této operace zahrnuty. (I v případě, že tyto soubory nebyly aktualizovány) (Leixner, 1993)



Obrázek 4 - systém diferenciálních záloh, zdroj: [leo-backup.com]

3.2.3 Zálohovací cyklus

Výběr typu zálohování

- **Volba diferenciálního typu**

Tento typ je vhodný zejména pro uživatele, který v podstatě denně pracuje se stejnými soubory, například pracuje se stejnou databází a nepotřebuje uchovávat její starší verze. Při tomto typu zálohy je také vhodné střídát dvě skupiny médií (například flash disk), které jsou rozděleny například na sudou a lichou, kdy sudá určena pro zálohy v úterý a ve čtvrtek a lichá záloha pro pondělí a středu. Plná záloha by v tomto případě mohla být tvořena například každý pátek na externí pevný disk. (Leixner, 1993)

- **Volba inkrementálního typu**

Vhodná pro uživatele, který pracuje denně s různými soubory. Tato metoda bývá také zpravidla rychlejší a efektivnější, neboť záloha probíhá jen po provedené změně.

Organizování záloh

V případě využití inkrementálního nebo diferenciálního typu zálohy, je vhodné zálohovací proces organizovat termínově jako určitý cyklus a vymežit tím, kdy se budou vytvářet plné zálohy a kdy částečné. Například zda se plné zálohy budou vytvářet vždy na konci týdne a v průběhu týdne se budou denně vytvářet částečné zálohy. (Leixner, 1993)

Intenzita tvorby záloh je podmíněna intervalem vytváření změn v datech. Například pokud uživatel provádí změnu ve svých datech jednou týdně, tak je zbytečné tvořit denní například inkrementální zálohu a bude pro něj daleko snazší vytvořit týdně jednu plnou zálohu.

Avšak je vhodné si hned na začátku určit interval pro pravidelné zálohování, bez ohledu na vybraný typ zálohy. I plná záloha by měla být vytvářena v pravidelných intervalech.

3.2.4 Způsoby zálohování dle použití nástrojů

- **Kopírováním**

Uživatel si ručně zvolí soubory, které chce zálohovat a ty pak prostřednictvím nástroje operačního systému zálohuje na zvolené médium například flash disk nebo externí HDD. Tato metoda je docela pracná a nepraktická, a proto ji uživatelé po čase začnou zpravidla opomíjet. (Pecinovský, 2003)

- **Vypalováním**

Uživatel dále může zálohovat svá data jejich vypálením na optická média (CD, DVD atd.), opět se však jedná o ruční metodu zálohy, která je z dlouhodobého hlediska nepraktická. Tento způsob je vhodné použít pro archivaci kopií důležitých souborů mimo prostředí, kde se vyskytuje originál souboru. Například uživatel vypálí pro něj důležitá data na optický disk DVD a ten následně uloží do trezoru do banky nebo třeba na chatě do skříně, avšak v tomto případě jen za předpokladu, že disk je chráněn proti přečtení neoprávněnou osobou šifrováním, aby nedošlo v případě odcizení disku k zneužití dat. Pro vypálení dat je zapotřebí specializovaný software a optická mechanika, která povoluje zápis. Uživatel může použít například některý z freeware aplikací (například ImgBurn) nebo aplikace, které vyžadují zakoupení licence, které na druhou stranu nabízejí podstatně více funkcí a některé i uživatelské prostředí v českém jazyce (například Nero). (Budai David, 2012)

- **Pomocí zálohovacího programu**

Pro zálohování existují přímo specializované programy, které nabízejí různé možnosti zálohování (plné, inkrementální, diferenciální), bývají zpravidla automatizované, neboť pracují s atributem Archivovat a tím přímo šetří uživateli práci s tvorbou zálohy a tím i jeho drahocenný čas, dále nabízejí možnost vytváření více zálohovacích úloh (tzv. multizálohování), komprimaci vytvořené zálohy a různé metody šifrování. Na internetu je nepřehledné množství těchto programů od freeware aplikací, až po placené verze. Hlavní výhodou těchto programů je automatizovaný a pro uživatele jednoduchý způsob tvorby záloh (Pecinovský, 2003)

- **Pomocí uživatelského programu**

Některé programy používané pro zpracování dat například účetnictví disponují nástrojem pro zálohování. Uživatel v tomto případě zadá příkaz programu a program se následně sám postará o vytvoření zálohy. Zálohy se v těchto programech zpravidla nespouští automaticky, nicméně pokud již dlouho záloha neproběhla, může program uživatele na tuto skutečnost upozornit. (Pecinovský, 2003)

V některých účetních softwarech, jako je například software Pohoda lze nastavit zálohování v pravidelných intervalech (denní, měsíční, před ukončením roku atd.) a zároveň tento program své zálohy komprimuje do formátu ZIP, pro snížení spotřeby místa na disku. (Stormware)

3.2.5 Média pro zálohování

Vysokou prioritu bychom měli přiřadit výběru vhodného média pro zálohování, velmi důležité je hodnocení, jak po stránce kvality a bezpečnosti média, ale také po jeho finanční náročnosti. Velmi záleží na tom, jestli na dané médium budeme ukládat denní, týdenní, měsíční nebo roční zálohy, protože při zničení média s týdenní zálohou je velmi pravděpodobné, že budeme mít stále zálohu o týden starší, proto si také můžeme pro tyto zálohy pořídit levnější médium. (Budai David, 2012)

Optická média

Historie optických disků začíná v 70 letech 20 století, kdy se začaly poprvé vyrábět kompaktní disky, které jsou známé spíše pod zkratkou CD. Kompaktní disky vznikly ve spolupráci dvou významných firem Sony a Philips. (Philips)

Dnes se již můžeme setkat s více možnostmi optických disků, jako jsou CD, DVD nebo novější optické disky Blue-ray, které nabízejí podstatně vyšší kapacitu.

Největší výhodou optických médií oproti jiným médiím je jejich nízká pořizovací cena v poměru k celkové kapacitě. (Budai David, 2012)

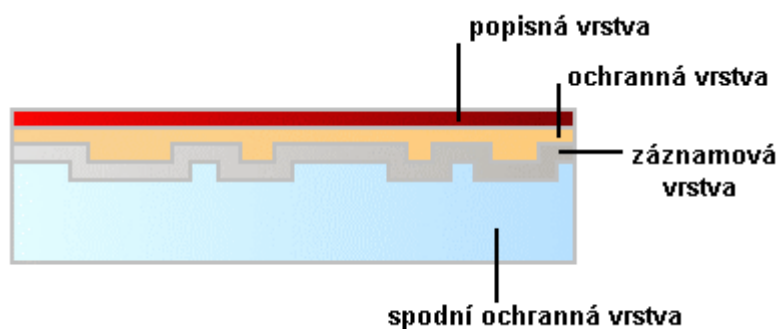
Co se týká jejich životnosti, tak dle údajů od výrobců na obalech se jejich životnost pohybuje v desítkách let. Ovšem v praxi dle zkušenosti uživatelů je jejich životnost podstatně kratší. Životnost disků nelze přímo generalizovat, neboť jejich životnost je vysoce

závislá na podmínkách skladování. Optická média jsou velmi náchylná na světlo, pokud budou vystaveny přímému světlu, dojde jejich kvalita k degradaci a tím pádem i na nich uložených datech. Dále je nutné je chránit proti mechanickému poškození poškrábáním. (Budai David, 2012)

Pokud se tedy rozhodnete zálohovat svá data na optická média, měly by být uschovány v obalech, aby byla chráněna před světlem a zároveň chráněna proti možnému poškrábání.

- **Compact disc (CD)**

Nejběžnější kapacita CD disků je 700 MB, jen výjimečně se můžete setkat s většími. Prodávají se buď disky CD-R, které jsou nepřepisovatelné, dále přepisovatelné disky CD-RW. Jejich rozměr je celosvětově daný průměrem 12cm a tloušťkou 1,2 mm, nicméně můžete také narazit na jejich zmenšenou verzi s průměrem 8 cm a kapacitou pouhých 200 MB. (Lalík, 2009)



Obrázek 5 - Průřez strukturou CD, zdroj: [notebook.cz]

Při pohledu na obrázek 5, kde je zobrazen průřez strukturou CD, můžeme vidět, že CD disky jsou náchylnější mechanickému poškození na horní straně disku, než na spodní straně skrze kterou proudí optické záření pro záznam, neboť spodní vrstva je tvořena silnou vrstvou polykarbonátu, který vytváří jeho odolnost a také ochranu proti mechanickému poškození. Naopak horní stranu disku tvoří popisná vrstva a pod ní je tenká ochranná vrstva tvořená většinou z hliníku. (Lalík, 2009)

Z hlediska zálohování jsou vhodné vzhledem k jejich malé kapacitě pro zálohování menších souborů, jako jsou například textové dokumenty, či fotografie v nižším rozlišení.

- **DVD**

Disky DVD již nabízejí příznivější kapacity. Na jednovrstvých discích je kapacita 4,7 GB, na dvouvrstvých pak 8,5 GB. K dostání jsou i oboustranné dvojevrstvé disky, které dosahují kapacity přes 17 GB, avšak jejich podpora u různých zařízení je menší, a proto je vhodné používat zejména jednovrstvé varianty.

- **Blue-ray**

Pro nedostačující kapacitu CD a DVD vznikl další typ disku pod názvem Blue-ray. Jednovrstvé disky nabízejí kapacitu 25 GB, dvouvrstvé pak 50 GB.

Tyto disky jsou vzhledem k jejich kapacitě vhodné především k zálohování objemnějších souborů. Avšak na druhou stranu je nutné podotknout, že dostupnost mechanik podporujících tento typ disku stále není moc rozšířená.

Pevný disk

- **Interní**

Pevný disk je hlavní úložiště počítače, jedná se o velmi spolehlivé médium pro záznam, které má vysokou úložnou kapacitu a přístupovou rychlost. Pro zálohování je toto řešení nejsnazší, protože zálohovaná data se ukládají přímo na pevný disk v počítači a není již třeba kupovat další externí disk či místo v cloudovém úložišti. (Pecinovský, 2003)

Výhodou tohoto řešení je rozhodně cena, protože již není třeba další investice. Naopak velkou nevýhodou je, že toto řešení neposkytuje ochranu dat v případě selhání pevného disku například přepětím nebo při virovém útoku. Další nevýhodou tohoto řešení je snižování kapacity pevného disku. (Pecinovský, 2003)

- **Externí**

Externí HDD slouží především pro rozšíření paměti interního disku, jedná se o klasický pevný disk, který je připojen k počítači externě, například prostřednictvím připojení USB nebo eSATA. Provádění záloh na externí disk bývá zpravidla lepší volbou než zálohování na flash disky a to hlavně kvůli jejich menší poruchovosti, náchylnosti k mechanickému poškození a podstatně větší kapacitě. (Koláček, 2008)

Externí disky jsou k dostání ve stejných verzích jako interní pevné disky a to ve formátech 1,8", 2,5" a 3,5". (Koláček, 2008)

Cloud computingu

Jedná se o službu, kdy společnost provádí hosting aplikace nebo sady aplikací. Hostující společnost nese náklady na hardwarové vybavení a stará se pravidelné aktualizace softwaru. Výhodou pro klienty je úspora investičních a provozních nákladů, na druhou stranu obsahuje cloud computingu i řadu nevýhod, jako je například potencionální riziku výpadku připojení k internetu a tím i nedostupnost služeb, další nevýhodou je fakt, že v případě uložení pro uživatele citlivých dat do cloudového úložiště vlastně dává svá data na server třetí osoby. (Velte, a další, 2011)

- **Cloudové úložiště**

Cloudové úložiště je úložný prostor, který je umístěn na serveru, kam si uživatel může ukládat svá data stejným způsobem jako na klasický pevný disk. (Laš, 2015)

Je poskytováno jako služba, která musí splňovat charakteristiky cloud computingu neboli musí být samoobslužná, elastická a měřitelná. (Cloud, 2016)

Výhodou cloudového úložiště může být i synchronizace dat mezi různými zařízeními. Například pokud uložíte přes počítač dokument do cloudu, je možné si ho pak stáhnout například do svého mobilního telefonu. (Laš, 2015)

NAS

Neboli síťové úložiště dat, které slouží primárně k ukládání dat a souborů a následné práci s nimi. Díky NASu si uživatel může vytvořit vlastní osobní cloud. (Budai David, 2012)

NAS je k dostání uživatelům v různých variantách podle počtu disků (jeden disk, dva disky nebo čtyři disky). Pro účely zálohování je vhodný koupit NAS s více než jedním diskem pro možnost vytvoření zrcadlového diskového pole RAID 1 nebo RAID 5. (Budai David, 2012)

Další velkou výhodou NASu je dostupnost dat odkudkoli z jakéhokoli síťového zařízení, nízká spotřeba a hlučnost, dále konfigurace oprávnění, neboť na většině NASů je možné vytvoření více uživatelských účtů s různými oprávněními. (Kejduš, 2011)

3.3 RAID

RAID (Redundant Array of Independent Disks) neboli v překladu redundantní pole nezávislých disků slouží k získání speciálních vlastností při použití více pevných disků a speciálního diskového řadiče. Tímto způsobem lze chránit svá data prostřednictvím zrcadlení pevného disku nebo lze také použít RAID pro zvýšení rychlosti. Existuje celkem 6 základních RAIDových polí. (Eagle, 2005)

- **RAID 0** = Tento typ RAID neřeší případy výpadku pevného disku, ale jeho úkolem je zvýšit výkon pevného disku tím, že data jsou ukládána na disk prokládaně v určitých blocích. Jeden disk obsahuje liché a druhý sudé bloky. Největší nevýhoda tohoto řešení je, že neposkytuje žádnou ochranu dat a v případě poruchy jednoho pevného disku je nepoužitelný i ten druhý, neboť obsahuje jen polovinu souboru. (Eagle, 2005)
- **RAID 1** = Nabízí praktické řešení ochrany dat tím, že při tomto řešení se data zapisují na oba disky současně, neboli dochází k tzv. zrcadlení. Při poruše jednoho pevného disku lze bez problému pokračovat v práci, neboť obsah disků by měl být naprosto totožný. Nevýhodou tohoto řešení by mohla být teoreticky nižší rychlost v důsledku dvojího zápisu dat, nicméně řadič lze nastavit na tzv. zpožděné zápisy a k zápisu dat dojde ve chvíli, kdy sestava není příliš zatížená. Toto řešení je vhodné zejména pro uživatele, kteří si vedou účetnictví nebo jiná operativní data. (Eagle, 2005)
- **RAID 2** = Rozděluje data v určitých blocích po bitech mezi jednotlivými pevnými disky. Tato metoda využívá Hammingova kódu pro detekci chyb při čtení. (TechTarget, 2014)
- **RAID 3** = Používá 4 disky, z nichž data rozděluje po bitech na 3 disky a na jeden disk ukládá paritní data. Sekvenční čtení a zápis dosahuje v tomto případě vyšších výkonů, nicméně na druhou stranu při náhodném čtení a zápisu dosahuje výsledků horších. V případě poruchy jednoho disku lze data obnovit z paritního. (Natarajan, 2011)

- **RAID 4** = Je odvozený typ od RAIDu 3 s rozdílem ve změně výpočtu paritní informace, zde je parita získána z paritní funkce nad bloky dat. (Kocmánek, 2003)
- **RAID 5** = Poskytuje kombinaci zvýšení výkonu sestavy a zároveň možnost ochrany dat zrcadlením pevného disku. Toto řešení ovšem vyžaduje 3 pevné disky. Při zápisu dat dochází k rozdělení paritních bitů na všechny 3 disky. Tato možnost si poradí s poruchou pouze jednoho disku. V případě selhání disku se dají data obnovit pomocí paritních bitů, které jsou uloženy na zbylých discích a dají se zároveň obnovit na nový pevný disk. Nicméně mezitím se dá diskové pole nadále používat. (Eagle, 2005)
- **RAID 6** = Je velmi podobný RAIDU 5 s tím rozdílem, že v tomto typu řešení jsou místo jednoho paritního bloku dva, dále má vyšší náročnost na výpočetní techniku, neboť potřebuje minimálně 4 pevné disky. Na druhou stranu oproti RAIDU 5 přináší výhodu v tom, že unese selhání dvou disků. (Kocmánek, 2003)

3.4 Komprimace dat

Při vytváření záloh může být vyžadováno velké množství potřebné kapacity pro uložení zálohy na disk nebo cloudové úložiště, nároky na potřebnou kapacitu můžeme snížit komprimací vytvořené zálohy. (Pecinovský, 2003)

Co je to komprimace dat?

Komprimace neboli také zabalení archivu znamená převedení souboru do archivní podoby, pomocí níž dosáhneme podstatného zmenšení velikosti původního souboru. V archivní podobě není možné se souborem běžně pracovat, pro opětovnou práci se souborem je nutné opět soubor dekomprimovat do původní podoby. (Pecinovský, 2003)

Míra komprimace dat je dána kompresním poměrem. Jedná se o poměr původní velikosti souboru s komprimovaným souborem v archivní podobě, udává se procentuálně a je možné ho vyjádřit dvěma způsoby. Při prvním způsobu dochází k poměru nové velikosti s původní velikostí vynásobené 100, kdy čím menší hodnoty je dosaženo, tím lépe. Druhý

způsob je zcela opačný a je vyžadováno dosažení co nejvyšší možné hodnoty. (Pecinovský, 2003)

Komprimování dat/záloh

Nástroj pro komprimování záloh dnes již obsahuje většina specializovaných automatických zálohovacích programů, nicméně je možné provádět komprimaci dat manuálně prostřednictvím speciálních komprimačních programů. (Morkes, 1998)

Při komprimaci záloh musí být použita bezztrátové komprese, neboť změna či ztráta jediného bitu v souboru může ve velké řadě formátů způsobit nepoužitelnost daného souboru. Například v případě ztráty znaku ve spustitelném souboru pravděpodobně nepůjde program vůbec spustit, proto je v metodách při komprimaci počítačových naprostá intolerance výpadku informací. (Morkes, 1998)

Komprimační programy

Jedná se o programy, které jsou schopné data zakódovat do takové podoby, kdy je jejich velikost menší v porovnání s velikostí před komprimací. Komprimační program musí být schopen data dekomprimovat (dekódovat) zpět do původní podoby. (Morkes, 1998)

Výhodou komprimačních programů je jejich velké rozšíření, široká použitelnost a dobré technické vlastnosti. Komprimační programy využívají pro kompresi dat různé komprimační algoritmy. Existují programy, které používají různé algoritmy na základě typu komprimovaných dat, pro dosažení optimálního výsledku. Nejvyužívanějším formátem pro komprimaci je formát ZIP, proto tento formát používá většina komprimačních programů. Typickým představitelem je nejrozšířenější aplikace WinZip. Dalším běžným formátem je formát RAR, jehož typickým představitelem je aplikace WinRAR. (Bráza, 2000)

4 Vlastní práce

4.1 Srovnání zálohovacích softwarů

Veškeré aplikace budou zkoumány v prostředí operačního systému Windows 7 Home Premium.

Hodnocení aplikací bude provedeno na základě níže uvedených 14 kritérií, které jsou ohodnoceny různými váhami podle jejich důležitosti.

Pro stanovení vah kritérií bude použita metoda alokace 100 bodů, kdy každému kritériu bude přiřazena určitá váha podle důležitosti daného kritéria v bodovém rozmezí 0- 10, kdy 10 znamená nejvíce důležité kritérium, nicméně celkový součet vah všech kritérií musí být roven 100. Čím vyšší počet bodů aplikace získá, tím je její hodnocení příznivější. Každá aplikace může získat maximálně 100 bodů.

Každé kritérium bude posuzováno samostatně a budou mu v průběhu hodnocení přisuzovány body v rozmezí 0-10, podle míry splnění, kdy úplné splnění kritéria je hodnocena bodem 10. Body budou přisuzovány dle subjektivního posouzení na základě zkušenosti s daným softwarem.

Pro srovnání aplikací a výběr kompromisní varianty bude provedena vícekritériální analýzy variant. Výpočet celkově získaných bodů určité aplikace bude získán skalárním součinem obdržených bodů a váhami kritérií.

Tabulka 2-Kriteriální tabulka

Kritéria	Popis kritéria	váha hodnocení
1.	Složitost instalace	3
2.	Uživatelské prostředí	8
3.	Jazykové rozhraní, nadstandartní nástroje aplikace	8
4.	Podpora plné zálohy	9
5.	Podpora inkrementální zálohy	7
6.	Podpora diferenciální zálohy	7
7.	Rozvrh záloh	8
8.	Zálohování přes FTP	9
9.	Komprimace záloh	7
10.	Možnost multizálohování	5
11.	Záloha na základě typu souboru	6
12.	šifrování	10
13.	Logovací tabulka pro ověření úspěšnosti zálohování	5
14.	Obnova ze zálohy	8
Bodů celkem		100

Zdroj: vlastní tvorba

- **Ad1** = složitost instalace je hodnocena podle toho, jestli průvodce instalací dané aplikace je intuitivní a daná instalace je díky tomu srozumitelná a nenáročná
- **Ad2** = zde bude hodnocen celkový grafický vzhled aplikace, její intuitivní ovládání a rozmístění prvků
- **Ad3** = zde bude hodnoceno, zda je aplikace přeložena do českého jazyka a zda její výrobce poskytuje též nápovědu v tomto jazyku
- **Ad4** = hodnocení dostupnosti možnosti provedení plné zálohy. Vzhledem k jednoduchosti obnovení, bude tento typ zálohy preferován, a proto je toto kritérium ohodnoceno více body.
- **Ad5** = hodnocení dostupnosti možnosti provedení inkrementální (přírůstkové) zálohy

- **Ad6** = hodnocení dostupnosti možnosti provedení diferenciální (rozdílové) zálohy
- **Ad7** = zde bude hodnoceno, jak aplikace umožňuje uživateli nastavit tvorby záloh z časového hlediska (například denní, týdenní, měsíční, roční zálohy atd.)
- **Ad8** = při tomto kritériu bude hodnoceno, zda aplikace umožňuje vytvářet zálohy přes FTP
- **Ad9** = zde bude hodnocena dostupnost a možnosti komprimace záloh v aplikaci pro snížení náročnosti na kapacitu
- **Ad10** = zda aplikace nabízí možnost vytváření více zálohovacích úloh
- **Ad11** = toto kritérium určuje, jestli daná aplikace umožňuje zálohování souborů na základě jejich typu (například jpg, doc, pdf)
- **Ad12** = posuzování aplikace z hlediska bezpečnosti zálohy proti jejímu odcizení (zda je záloha chráněna proti neoprávněnému přečtení prostřednictvím šifrování dat)
- **Ad13** = zde bude hodnoceno poskytování zpětné vazby aplikace uživateli o úspěšném provedení zálohy
- **Ad14** = při tomto kritériu je posuzováno, zda aplikace umožňuje obnovovat data ze zálohy přímo prostřednictvím uživatelského rozhraní nebo zda záloha musí být obnovena ručně

4.1.1 Freeware aplikace

Cobian Backup 11 (Gravity)

Tabulka 3 - hodnocení Cobian Backup 11 (Gravity)

Kritéria	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Váhy	3	8	8	9	7	7	8	9	7	5	6	10	5	8
získané body	0,4	1	1	1	1	1	0,9	1	0,6	1	0,5	0,8	1	0,5
Součin	1,2	8	8	9	7	7	7,2	9	4,2	5	3	8	5	4
Celkem	86													

Zdroj: vlastní tvorba

Jedná se o freeware nástroj pro automatické zálohování s intuitivním ovládáním a širokým spektrem nabízených funkcí.

- **Ad1** = Instalace aplikace je poměrně složitá, neboť je při ní třeba zvolení možností, které se téměř nedají zvolit intuitivně a musí k nim být buď patřičná znalost významu zvolené možnosti, nebo prostudování online návodu.
- **Ad2** = Uživatelské prostředí má přívětivý grafický vzhled, disponuje intuitivním ovládáním a rozložení prvků není chaotické.
- **Ad3** = Aplikace je celá přeložena do českého jazyka včetně průvodce instalací. Na webových stránkách výrobce je k dispozici též návod v českém jazyce. Aplikace neumožňuje provádět zálohy včetně všech ovladačů.
- **Ad4,5,6** = Aplikace disponuje možností tvorby všech tří typů záloh (plné, inkrementální i diferenciální).
- **Ad7** = Zálohy lze rozvrhnout na jednorázovou, denní, týdenní, měsíční, roční zálohu nebo lze také tvořit zálohy vždy při spuštění počítače či nastavením určitého časového intervalu prostřednictvím integrovaného časovače.
- **Ad8** = Aplikace umožňuje provádět zálohy prostřednictvím FTP.
- **Ad9** = Vytvořenou zálohu lze prostřednictvím aplikace komprimovat metodou zip nebo 7zip a tím tak snížit kapacitu zálohy.
- **Ad10** = Disponuje možností vytvoření více úloh zálohování a tím tak například zálohovat určité soubory či složky navíc samostatně na jiná média.
- **Ad11** = Aplikace umožňuje provádět zálohy na základě typů souborů, pouze po manuálním doplnění koncovek
- **Ad12** = Pro ochranu dat před zneužitím může uživatel v aplikaci využít metody šifrování AES 128bits, AES 192bits a AES 256 bits.
- **Ad13** = Aplikace disponuje logovací tabulkou pro ověření úspěšnosti provedené zálohy
- **Ad14** = Obnova ze zálohy není možná prostřednictvím uživatelského rozhraní aplikace, soubory je potřeba obnovit ručně. Aplikace provádí kopírování nebo komprimování souborů při vytváření zálohy prostřednictvím standardních metod tj. bez používání proprietárních formátů a díky tomu není k obnově ze zálohy potřeba dalších nástrojů. V případě zálohy bez komprimace stačí soubory pouze zkopírovat na určené místo.

7Backup

Tabulka 4 - hodnocení 7Backup

Kritéria	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Váhy	3	8	8	9	7	7	8	9	7	5	6	10	5	8
získané body	1	0,9	0,4	0	1	0	0	1	0,5	0	0,5	0,4	1	1
Součin	3	7,2	3,2	0	7	0	0	9	3,5	0	3	4	5	8
Celkem														52,9

Zdroj: vlastní tvorba

- **Ad1** = Jedná se o spustitelný program bez instalace.
- **Ad2** = Uživatelské prostředí má jednoduché ovládání a systematické rozmístění ovládacích prvků. Na druhou stranu po grafické stránce není příliš kvalitně propracovaný. Je možné provádět pouze zálohy souborů nebo disků, záloha včetně všech ovladačů není k dispozici.
- **Ad3** = Aplikace poskytuje české jazykové rozhraní.
- **Ad4** = Aplikace neposkytuje možnost tvorby plné zálohy.
- **Ad5** = Aplikace používá inkrementální typ záloh.
- **Ad6** = Aplikace neposkytuje možnost tvorby diferenciálního typu zálohy.
- **Ad7** = Vzhledem k jednoduchosti aplikace není možné nastavit rozvrh zálohování, každé zálohování je nutno provádět manuálně.
- **Ad8** = Aplikace umožňuje provádět zálohy přes FTP.
- **Ad9** = 7Backup nabízí 2 možnosti komprimace záloh ve formátu 7ZIP (první jednodušší možnost komprimace provádí aplikace automaticky bez dotazování uživatele, v hlavním menu aplikace je k dispozici zvolit druhou možnost komprimace „použít účinnější, ale pomalejší kompresi“)
- **Ad10** = Aplikace neumožňuje nastavit více úkolů zálohování.
- **Ad11** = V aplikaci je možné nastavit zálohování souborů na základě jejich typu, nýbrž pouze po manuálním nastavení koncovek souborů.
- **Ad12** = Pro ochranu dat před zneužitím je uživatelům k dispozici pouze jeden typ šifrování a to AES 256 bits.
- **Ad13** = Disponuje logovací tabulkou pro ověření úspěšnosti provedené zálohy

Ad14 = Obnova ze zálohy lze provést přímo prostřednictvím uživatelského rozhraní i manuálně pomocí průzkumníka Windows.

SyncBackFree V7.5.19.0

Tabulka 5 - hodnocení SyncBackFree V7.5.19.0

Kritéria	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Váhy	3	8	8	9	7	7	8	9	7	5	6	10	5	8
získané body	0,9	0,6	0,4	1	0	0	0,6	1	1	1	0,5	0,4	1	1
Součin	2,7	4,8	3,2	9	0	0	4,8	9	7	5	3	4	5	8
Celkem	65,5													

Zdroj: vlastní tvorba

- **Ad1** = Instalace aplikace probíhá v českém jazyce, nicméně během instalace se v textu objevují chyby ve formátu kódování (písmena s háčky jsou nahrazeny jinými písmeny).
- **Ad2** = Uživatelské prostředí je intuitivní formou průvodce, avšak při pokročilém nastavování záloh se již stává méně přehledným. Pro úpravu nastavení zálohování je možné zvolit ze dvou režimů a to buď režim „odborník“, který umožňuje nastavit uživateli průběh zálohování více podrobně. Další možností je režim „začátečník“, který poskytuje uživateli jen minimální zásah do nastavení.
- **Ad3** = Překlad do českého jazyka není kompletní, místy se objevují anglické texty. Návod je poskytován pouze v anglickém jazyce. Prostřednictvím této aplikace není možné zálohovat celý systém včetně ovladačů.
- **Ad4** = Aplikace disponuje možností plné zálohy.
- **Ad5** = Tento typ zálohy není aplikací poskytován.
- **Ad6** = Tento typ zálohy není aplikací poskytován.
- **Ad7** = Lze nastavit rozvrh pro pravidelné zálohování, je k dispozici denní, týdenní a měsíční nastavení.
- **Ad8** = Disponuje možností provádět zálohy prostřednictvím FTP.

- **Ad9** = Komprimace záloh ve formátu ZIP, k dispozici je široké spektrum možností intenzity komprimace v devíti úrovních, kdy první úroveň je nejnižší, ale zároveň nejrychlejší způsob komprimace zálohy.
- **Ad10** = Lze nastavit více úkolů zálohování.
- **Ad11** = Zálohování na základě typu souborů lze pouze po manuálním vložení koncovky určeného typu souborů do filtru.
- **Ad12** = Software využívá pro ochranu dat před zneužitím ZIP kódování a metodu AES 256bits.
- **Ad13** = Ověření úspěšnosti vytvořené zálohy lze ověřit v logovací tabulce.
- **Ad14** = Obnovení dat ze zálohy lze jak prostřednictvím uživatelského rozhraní aplikace, tak lze data obnovit ručně.

Windows Zálohování (Windows 7 Home Premium)

Tabulka 6- Hodnocení Windows Zálohování

Kritéria	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Váhy	3	8	8	9	7	7	8	9	7	5	6	10	5	8
získané body	1	0,9	0,6	1	0	0	1	0	0	0	0	0	1	0,5
Součin	3	7,2	4,8	9	0	0	8	0	0	0	0	0	5	4
Celkem	41,0													

Zdroj: vlastní tvorba

- **Ad1** = Výhodou této aplikace je skutečnost, že je přímo integrovaná v systému Windows.
- **Ad2** = Grafický vzhled aplikace je jednotný jako u ostatních nástrojů Windows, aplikace nabízí jednoduché uživatelské rozhraní. Nastavení zálohování je formou průvodce ve 3 snadných krocích. Uživatel určí místo, kam se bude ukládat záloha, nastaví rozvrh záloh a nakonec zvolí, co vše bude zálohovat. Pro zjednodušení si uživatel může zvolit možnost, kdy nechá rozhodnout systém o tom, co se bude zálohovat. V takovém případě jsou zálohovány datové soubory v knihovnách, na ploše a ve výchozích složkách systému, dále je automaticky vytvořena bitová kopie systému.

- **Ad3** = Aplikace je kompletně přeložena do českého jazyka včetně návodu. Jak již bylo zmíněno, software umožňuje vytvořit bitovou kopii systému tj. vytvořit zálohu včetně veškerých ovladačů. Zálohování Windows nabízí pouze základní funkce.
- **Ad4,5,6** = Aplikace umožňuje vytvářet pouze plné zálohy.
- **Ad7** = Rozvrh zálohování je k dispozici, je možné vytvářet denní, týdenní nebo měsíční zálohy.
- **Ad8** = Zálohy je možné vytvářet pouze na lokální disky/média, není možné vytvářet zálohy na servery FTP.
- **Ad9** = Prostřednictvím aplikace není možné nastavit komprimaci záloh.
- **Ad10** = Možnost vytváření více zálohovacích úloh není k dispozici.
- **Ad11** = Software neumožňuje zálohování souborů na základě jejich typu.
- **Ad12** = Šifrování není k dispozici.
- **Ad13** = Aplikace disponuje logovací tabulkou, kde uživatel může sledovat průběh procesu zálohování.
- **Ad14** = Obnova ze zálohy lze jen prostřednictvím uživatelského rozhraní systému.

4.1.2 Placené (komerční) aplikace

Tabulka 7- přehled hodnoceného komerčního softwaru

Hodnocený zálohovací software	Cena
Acronis True Image 2016	1 339 Kč
Norton Ghost 15.0 (Symantec)	845,80 Kč
Backup4all Professional	1 412 Kč
O&O DiskImage Professional Edition	1 159 Kč

Zdroj: sw.centrum, cs24.inshop.cz, vlastní tvorba

Acronis True Image 2016

Tabulka 8 - hodnocení Acronis True Image 2016

Kritéria	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Váhy	3	8	8	9	7	7	8	9	7	5	6	10	5	8
získané body	1	1	1	1	1	1	1	1	1	1	0	1	1	0,5
Součin	3	8	8	9	7	7	8	9	7	5	0	10	5	4
Celkem	90,0													

Zdroj: vlastní tvorba

Acronis True Image je jeden z nejprodávanějších zálohovacích programů v češtině, jedná se o velmi kvalitně zpracovaný software s širokým spektrem funkcí.

- **Ad1** = Instalace probíhá v českém jazyce, na konci instalace je nutné provést registraci.
- **Ad2** = Uživatelské rozhraní je velmi propracované, jak po grafické stránce, tak i po stránce systematického rozmístění ovládacích prvků. Ovládání je velmi snadné intuitivního charakteru.
- **Ad3** = Je zde velmi kvalitní překlad do českého jazyka, včetně velmi podrobného návodu pro používání aplikace. Software nabízí možnost komplexní zálohy včetně všech ovladačů, dále nabízí možnost využití vlastního cloudového úložiště s neomezenou kapacitou, uživateli tím tak odpadá starost v případě potřeby s registrací a dalšími poplatky u jiného poskytovatele. Aplikace poskytuje uživatelům další užitečné nástroje pro práci s daty, například nabízí možnost archivace souborů skrze aplikaci pro ušetření kapacity na místním disku, dále nabízí vytvoření záchranného média pro opravu systému.
- **Ad4,5,6** = Aplikace umožňuje vytvářet všechny 3 typy záloh (plnou, inkrementální i diferenciální)
- **Ad7** = Rozvrh zálohování je k dispozici, výrobce nabízí několik typů rozvrhu záloh, které jsou denní, týdenní, měsíční, dále možnost „při události“ (při přihlášení/odhlášení uživatele, vypnutí/restart počítače nebo spuštění systému se zpožděním), dále možnost Nonstop. Zálohy je však možné vytvářet i manuálně bez rozvrhu.

- **Ad8** = Zálohy je možné provádět na servery FTP.
- **Ad9** = Zálohy je možné vytvářet, jak bez komprese, tak s kompresí, kterou je možné provést ve třech typech (normální, vysoká, maximální)
- **Ad10** = Multizálohování je poskytováno, v uživatelském rozhraní lze nastavit více úkolů pro zálohování.
- **Ad11** = Program neumožňuje zálohovat souboru na základě jejich typu.
- **Ad12** = Aplikace využívá šifrovacích metod AES 128 bits, AES 192 bits, AES 256 bits.
- **Ad13** = Logovací tabulka pro ověření úspěšnosti provedené zálohy je k dispozici.
- **Ad14** = Obnova ze zálohy je možná pouze prostřednictvím uživatelského rozhraní.

Norton Ghost 15.0

Tabulka 9 - hodnocení Norton Ghost 15.0

Kritéria	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Váhy	3	8	8	9	7	7	8	9	7	5	6	10	5	8
získané body	0,9	0,6	0,8	0	1	0	1	1	1	1	1	1	1	0,5
Součin	2,7	4,8	6,4	0	7	0	8	9	7	5	6	10	5	4
Celkem														74,9

Zdroj: vlastní tvorba

Norton Ghost je komerční zálohovací software od společnosti Symantec.

- **Ad1** = Průvodce instalací je intuitivního charakteru, instalace probíhá v anglickém jazyce.
- **Ad2** = Má intuitivní ovládání, avšak menší systematičnost, ve srovnání například s aplikacemi Acronis či Cobian Backup je méně přehledný.
- **Ad3** = Uživatelské rozhraní není dostupné v české verzi. Zálohovat lze komplexně včetně ovladačů a uživatelských nastavení.
- **Ad4,5,6** = Software vytváří pouze inkrementální typ záloh. Zálohy plné nebo diferenciální nepodporuje.
- **Ad7** = V nastavení je možné nastavit rozvrh záloh buď na týdenní, měsíční nebo na možnost jednorázové zálohy.
- **Ad8** = Zálohování přes FTP není možné.

- **Ad9** = Zálohy je možné vytvářet s kompresí (standartní, střední, vysoká).
- **Ad10** = Disponuje možností multizálohování.
- **Ad11** = Aplikace umí velmi dobře zálohovat soubory na základě jejich typu. Při tvorbě zálohy stačí zadat, jaké soubory se mají zálohovat (například videa, hudba, obrázky nebo soubory na ploše, internetové prohlížeče či email schránka)
- **Ad12** = Zálohy lze šifrovat prostřednictvím metod AES 128 bits, AES 192 bits a AES 256 bits.
- **Ad13** = Aplikace obsahuje logovací tabulku pro ověření úspěšnosti provedené zálohy.
- **Ad14** = Data nelze obnovit manuálně, ale jen prostřednictvím uživatelského rozhraní.

Backup4all Professional

Tabulka 10 - hodnocení Backup4all Professional

Kritéria	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Váhy	3	8	8	9	7	7	8	9	7	5	6	10	5	8
získané body	1	0,7	0,7	1	1	1	1	1	1	1	0	1	1	1
Součin	3	5,6	5,6	9	7	7	8	9	7	5	0	10	5	8
Celkem														89,2

Zdroj: vlastní tvorba

- **Ad1** = Instalace je velmi snadná, probíhá v češtině pouze ve dvou krocích.
- **Ad2** = Vzhledově aplikace připomíná kancelářský software MS Office. Je zde systematické rozmístění ovládacích prvků, ovládání programu je intuitivní.
- **Ad3** = Software je kompletně přeložen do českého jazyka. Umožňuje komplexní zálohu včetně všech uživatelských nastavení, historie internetových prohlížečů a všech ovladačů. Dále aplikace nabízí v případě potřeby možnost oprav vytvořených záloh.
- **Ad4,5,6** = K dispozici jsou všechny tři typy záloh (plná, inkrementální i diferenciální)

- **Ad7** = Automatické zálohy lze nastavit v přítomném rozvrhu záloh, program nabízí následující možnosti (denní, týdenní, měsíční, ruční)
- **Ad8** = Prostřednictvím softwaru Backup4all je možné ukládání záloh na servery FTP.
- **Ad9** = V aplikaci je možné zálohy pro ušetření místa v úložišti komprimovat, uživatelům jsou k dispozici tři typy komprese (nízká, normální, nejlepší), dále je možné v nastavení zvolit, které typy souborů nebudou komprimovány (např. formát mp3, jpg).
- **Ad10** = Aplikace umožňuje vytvářet více úloh zálohování.
- **Ad11** = Zálohování na základě typu souboru není aplikací podporováno.
- **Ad12** = Zálohované soubory se dají prostřednictvím aplikace šifrovat a to buď metodami AES (128,192 nebo 256bits) nebo prostřednictvím ZIP2. Další možností ochrany dat je možné maskování názvů souborů v zipu.
- **Ad13** = Logovací tabulka je k dispozici.
- **Ad14** = Obnovit soubory ze záloh lze, jak prostřednictvím uživatelského rozhraní, tak i manuálně.

O&O DiskImage Professional Edition

Tabulka 11 - hodnocení O&O DiskImage Professional Edition

Kritéria	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Váhy	3	8	8	9	7	7	8	9	7	5	6	10	5	8
získané body	0,8	0,4	0,7	1	1	1	1	0	0,2	1	0	1	1	0,3
Součin	2,4	3,2	5,6	9	7	7	8	0	1,4	5	0	10	5	2,4
Celkem														66,0

Zdroj: vlastní tvorba

- **Ad1** = Instalace probíhá prostřednictvím intuitivního průvodce v anglickém jazyce.
- **Ad2** = Uživatelské rozhraní je nepřehledné, rozmístění ovládacích prvků nesystematické, nastavení záloh složité.
- **Ad3** = Program je dostupný pouze v anglickém jazyce včetně jeho návodu, aplikace umožňuje vytvářet komplexní zálohy včetně všech ovladačů, dále umožňuje vytvoření opravného disku a obnovit nechtěně smazané soubory.

- **Ad4,5,6** = K dispozici jsou všechny tři typy záloh (plná, inkrementální i diferenciální)
- **Ad7** = Lze nastavit rozvrh pravidelných záloh (denní, týdenní, při připojení zařízení či jednorázové)
- **Ad8** = Aplikace neumožňuje připojení FTP.
- **Ad9** = Z hlediska ochrany dat je možné vytvořené zálohy šifrovat, bohužel však aplikace poskytuje jen jednu možnost šifrování a to BZIP2.
- **Ad10** = Uživateli je umožněno vytvářet více zálohovacích úloh.
- **Ad11** = Provádění zálohy na základě typu souboru není k dispozici.
- **Ad12** = Zálohy je možné šifrovat prostřednictvím metod AES 128 bits, AES 192 bits a AES 256 bits.
- **Ad13** = Aplikace je opatřena logovací tabulkou pro ověření úspěšnosti provedené zálohy.
- **Ad14** = V případě potřeby obnovy dat z vytvořené zálohy, lze obnovu provést pouze prostřednictvím uživatelského rozhraní, nicméně nalezení možnosti pro obnovu je v aplikaci díky její špatné přehlednosti a nesystematičnosti velmi složitá.

4.1.3 Celkové srovnání

V celkovém srovnání dopadl nejlíp placený software Acronis True Image 2016 s celkovým počtem získaných bodů 90, na druhém místě se umístil též komerční software Backup4all Professional s celkovým výsledkem 89,2 body. S velmi dobrým hodnocením se na třetím místě umístila freeware aplikace Cobian Backup 11, která získala v celkovém součtu jen o 4,4 bodů méně než vítězná komerční aplikace Acronis. V celkovém hodnocení zůstala na posledním místě integrovaná aplikace systému Windows 7 (Windows Zálohování) se 41 body.

V tabulce číslo 12 jsou znázorněny celkové výsledky jednotlivých aplikací, které jsou seřazeny podle počtu získaných bodů od vítězné aplikace po nejhůře hodnocenou.

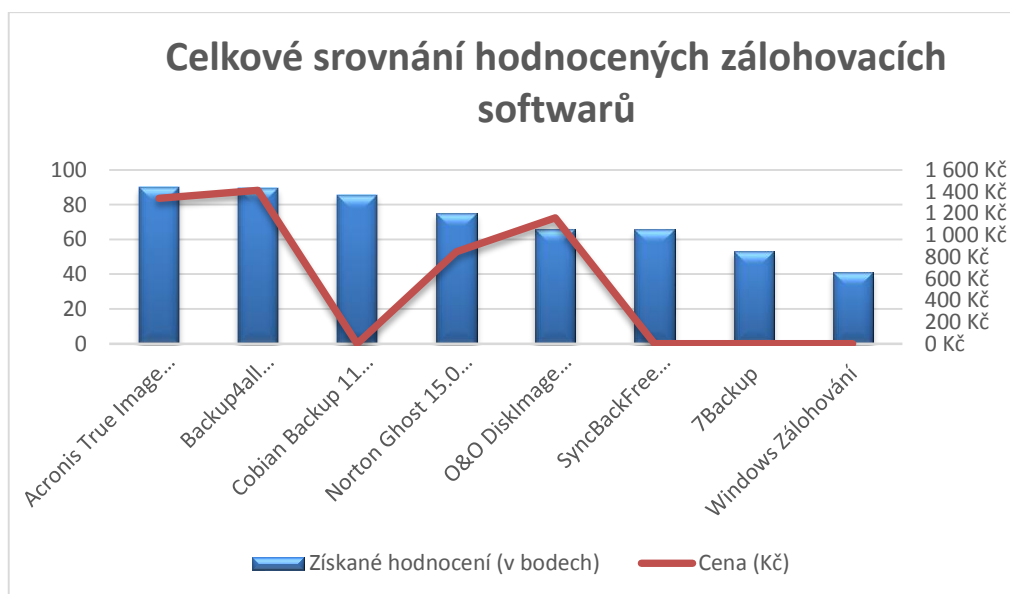
Tabulka 12- Celkové srovnání hodnocených zálohovacích softwarů

Pořadí	Hodnocená aplikace	Získané hodnocení (v bodech)	Cena (Kč)
1.	Acronis True Image 2016	90	1 339
2.	Backup4all Professional	89,2	1 412
3.	Cobian Backup 11 (Gravity)	85,6	0
4.	Norton Ghost 15.0 (Symantec)	74,9	845,80
5.	O&O DiskImage Professional Edition	66	1 159
6.	SyncBackFree V7.5.19.0	65,5	0
7.	7Backup	52,9	0
8.	Windows Zálohování	41	0

Zdroj: vlastní tvorba

Na grafu číslo 1. je zobrazeno graficky celkové bodové ohodnocení jednotlivých aplikací včetně další proměnné, kterou je cena za danou aplikaci.

Graf 1 - Celkové srovnání hodnocených zálohovacích softwarů



Zdroj: vlastní tvorba

4.2 Hodnocená cloudová úložiště

Úložiště BOX

Box nabízí pro běžné uživatele 2 typy účtů „Personal Free“ a „Personal Pro“. Ve free verzi je uživateli nabídnuto již po registraci 10 GB volného místa pro ukládání dat, při čemž je velikost nahrávaného souboru limitována velikostí pouze 250 MB. Úložiště je možné využít na platformách Windows, MAC, iOS, Android i Blackberry. Poskytovatel nabízí pouze jednu možnost rozšíření kapacity a to přechod na již zmíněný typ účtu Personal Pro, kde je úložná kapacita rozšířena na celých 100 GB při měsíční paušální platbě 8 €/ 216,52 Kč (kurz platný ke dni 28. 2. 2016), dále je zvýšena velikost pro nahrávaný soubor na 5 GB.

Úložiště Dropbox

Poskytovatel nabízí ve své free verzi Dropbox basic úložný prostor o velikosti 2 GB, kdy velikost nahrávaného souboru je limitována 10 GB, dále je k dispozici na platformách Windows, MAC, iOS, Android a Linux. Úložiště je možné rozšířit přechodem na druhý typ účtu Dropbox Pro, kde je uživateli nabídnuta kapacita 1 TB pro ukládání dat, měsíční paušál tohoto tarifu je 9,99 € / 270,379 Kč (kurz platný ke dni 28. 2. 2016).

Google Drive

Google Drive nabízí uživatelům 15 GB úložného prostoru zdarma, s možností rozšíření úložného prostoru v pěti možnostech až do maximální výše 30 TB. Společnost Google nabízí rozšíření úložné kapacity v možnostech 100 GB, 1 TB, 10 TB, 20 TB a již zmíněných 30 TB. Maximální velikost souborů je dělena dle jejich typu, uživatelé mohou prostřednictvím úložiště ukládat i vytvářet dokumenty do velikosti 50 MB, dále databáze do 2 milionů buněk, dále prezentace do 100 MB a ostatní soubory do velikosti 5 TB. Google Drive je podporován na platformách Windows, MAC, iOS a Android, u kterého bývá automaticky předinstalovaný jako výchozí cloudové úložiště pro zálohování mobilních zařízení.

Pro větší přehlednost možností rozšíření úložné kapacity a následných poplatků jsou tyto údaje převedeny do níže uvedené tabulky číslo 13.

Tabulka 13- možnosti rozšíření Google Drive

Velikost úložného prostoru	Cena / měsíčně	Cena v Kč * / měsíčně
15 GB	Free	-
100 GB	\$1.99	53,859
1 TB	\$9.99	270,379
10 TB	\$99.99	2 706,229
20 TB	\$199.99	5 412,729
30 TB	\$299.99	8 119,229

Zdroj: ceník Google drive, vlastní tvorba

* Kurz platný ke dni 28. 2. 2016

MEGA

Poskytovatel cloudového úložiště MEGA již ve své free verzi nabízí uživatelům přívětivých 50 GB úložného prostoru. Nahrávání souborů je kapacitně omezeno ve výši 10 GB. Kapacitu lze rozšířit ve čtyřech možnostech, při čemž nejnižší kapacita pro rozšíření je 200 GB a největší možnou kapacitou jsou celé 4 TB. Všechny možnosti včetně paušálních měsíčních poplatků jsou znázorněny v níže uvedené tabulce.

Tabulka 14- možnosti rozšíření MEGA

Velikost úložného prostoru	Cena / měsíčně	Cena v Kč * / měsíčně
50 GB	Free	-
200 GB	\$4.99	135,054
500 GB	\$9.99	270,379
2 TB	\$19.99	541,029
4 TB	\$29.99	811,679

Zdroj: Mega, vlastní tvorba

* Kurz platný ke dni 28. 2. 2016

OneDrive

Společnost Microsoft ve svém cloudovém úložišti nabízí uživatelům zdarma 5 GB úložného prostoru, který si uživatelé mohou rozšířit za 49,99 Kč měsíčně na 50 GB. Další rozšíření úložné kapacity je možné jen v případě zakoupení licence produktu MS Office 365, kdy uživatel automaticky získá 1 TB volného místa. Měsíční částka předplatného MS Office 365 činí 189,99 Kč. OneDrive je dostupný na platformách Windows, MAC, iOS a Android. Nahrání souborů v tomto úložišti je omezeno 10 GB.

4.2.1 Srovnání cloudů

Pro snížení ekonomické náročnosti zálohování, budou při hodnocení cloudových úložišť posuzovány pouze jejich bezplatné varianty pro individuální uživatele.

Hodnocení cloudových úložišť pro vybrání kompromisní varianty bylo provedeno též použitím vícekritériální analýzy variant, kde pro ohodnocení jednotlivých kritérií byla konkrétně použita bodovací metoda. Každé kritérium bylo ohodnoceno v rozmezí 1-10 bodů, kdy deseti body byla ohodnocena nejlepší možnost a jedním bodem ta nejméně vhodná. Výsledky budou normalizovány váhami kritérií, které byly stanoveny metodou pořadí.

Kritéria pro hodnocení úložišť seřazené dle důležitosti:

- 1.** Desktopová aplikace pro synchronizaci
- 2.** Bezplatný úložný prostor
- 3.** Maximální velikost nahraného souboru
- 4.** Dostupnost na jiných platformách (Windows, MAC, iOS, Android)

Tabulka 15- Výchozí tabulka hodnocení cloudových úložišť

Cloudové úložiště	Bezplatný úložný prostor	Maximální velikost nahraného souboru	Dostupnost na jiných platformách	Desktopová aplikace
Box	10 GB	250 MB	Ano	Ano
Dropbox	2 GB	10 GB	Ano	Ano
Google drive	15 GB	5 TB	Ano	Ano
MEGA	50 GB	10 GB	Ano	Ano
OneDrive	5 GB	10 GB	Ano	Ano

Zdroj: vlastní tvorba

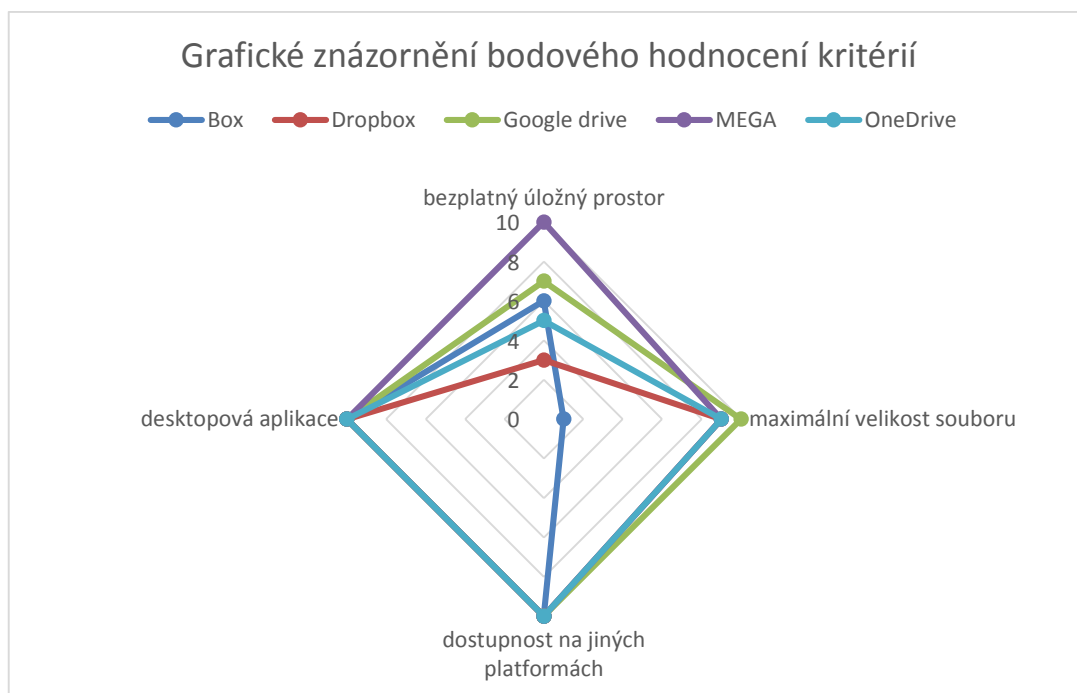
Tabulka 16- bodově ohodnocená tabulka hodnocení cloudových úložišť

Cloudové úložiště	Bezplatný úložný prostor	Maximální velikost nahraného souboru	Dostupnost na jiných platformách	Desktopová aplikace	Celkové hodnocení
Box	6	1	10	10	7
Dropbox	3	9	10	10	7,7
Google drive	7	10	10	10	9,1
MEGA	10	9	10	10	9,8
OneDrive	5	9	10	10	8,3
Váhy kritérií	0,3	0,2	0,1	0,4	-

Zdroj: vlastní tvorba

Na základě výsledků z tabulky číslo 16 byla, jako kompromisní varianta vybráno úložiště MEGA. Na druhém místě se umístilo úložiště od společnosti Google „Google drive“, které získalo 9,1 bodů. Jako poslední v hodnocení skončilo cloudové úložiště Box se sedmi získanými body.

Graf 2 -Grafické znázornění bodového hodnocení kritérií



Zdroj: vlastní tvorba

Na grafu číslo 2 jsou graficky znázorněna bodová ohodnocení jednotlivých kritérií u hodnocených cloudových úložišť.

4.3 Návrh postupu zálohování

Varianta A

Tato varianta je vhodná pro uživatele, pro které je cena dat velmi vysoká, dále preferují, co nejjednodušší možnost tvorby záloh a s ní spojené činnosti, jako jsou registrace u různých poskytovatelů cloudových úložišť, výrobců zálohovacích softwarů, snadné nastavení procesu zálohování a případně snadné obnově dat.

Na základě výsledků hodnocení zálohovacích softwarů, bude v této variantě doporučen uživateli zálohovací software Acronis True Image 2016 a jako zálohovací médium externí pevný disk. Na základě náročnosti obnovení bude zvolen typ plné zálohy, kdy výchozí rozvrh bude 1x týdně (interval zálohování je závislý na individuálním uživateli a jeho intenzitě práce s daty).

Přesný návod zálohování v této variantě je zobrazen v příloze A.

Ekonomická náročnost varianty:

Tabulka 17 - ekonomická náročnost varianty A

Předmět	Cena (vč. 21% DPH)
Acronis True Image 2016	1 339 Kč **
Externí HDD Verbatim 500 GB	1 279 Kč
Celkem	2 618 Kč

Zdroj: CZC, vlastní tvorba

**Data z tabulky číslo 7

Varianta B

Tato varianta je vhodná pro uživatele, kteří volí kompromis mezi náklady a komfortem spojený s tvorbou záloh. V této variantě bude použita freeware aplikace Cobian Backup 11 Gravity, která se umístila na třetím místě v celkovém srovnání zálohovacího softwaru. Jako zálohovací médium bude použit též externí pevný disk jako ve variantě A, avšak jako cloudové úložiště bude použit cloud MEGA, který vyšel jako vítěz ve srovnání cloudových úložišť.

Ekonomická náročnost varianty:

Tabulka 18 - ekonomická náročnost varianty B

Předmět	Cena (vč. 21% DPH)
Cobian Backup 11 Gravity	zdarma
Externí HDD Verbatim 500 GB	1 279 Kč
Celkem	1 279 Kč

Zdroj: CZC, vlastní tvorba

Postup zálohování v této variantě viz příloha B.

4.4 Ekonomická úspora

Nyní si ukážeme, že i při výběru dražší varianty A dochází k ekonomické úspoře vynaložených nákladů na případnou obnovu dat. Pokud bychom si vybrali pro obnovu dat

specializovanou firmu, která se obnovou dat zabývá například v případě selhání pevného disku, se náklady na obnovu mohou vyšplhat až na částku převyšující 10 tisíc.

Pro ukázkou je zvolena společnost DATAHELP, která na svých webových stránkách uvádí konkrétní zkušenosti s obnovou dat různým zákazníkům i s výší nákladů, které byla spojena s obnovou dat (při čemž ne vždy se podařilo zachránit všechna data z pevného disku).

Příklad č. 1

V příkladu číslo 1. uživateli spadl disk na zem, tím došlo k mechanickému poškození disku. V tomto případě se podařilo zachránit 98% uložených dat, avšak oprava trvala jeden týden a uživatel neměl po celou dobu svá data k dispozici. Celkové náklady na záchranu dat se vyšplhaly na částku 10 890 Kč včetně 21% DPH. Rozdíl uspořené nákladů oproti variantě A činí 8 272 Kč a při srovnání s variantou B je celková úspora nákladů ve výši 9 611 Kč.

Tabulka 19 - Modelový příklad nákladů na záchranu dat č. 1

Hardwarová chyba	
Závada:	vadné čtecí hlavy, částečně poškozená plotna.
Příčina:	pád na zem za chodu disku.
Doba realizace:	týden
Cena:	10 890 Kč včetně DPH
Úspěšnost záchrany:	98 % - zbytek dat nebylo možno zachránit z důvodu poškození plotny

Zdroj: Helpdesk, vlastní tvorba

Příklad č. 2

V příkladu číslo 2 došlo též k chybě hardwaru, nicméně úspěšnost záchrany dat se pohybuje mezi 70-100%. Tento typ závady může nastat výrobní vadou, stářím média či mechanickým poškozením. Celkově vynaložené náklady se v tomto případě pohybují mezi 5000-12000 Kč bez DPH a doba realizace opravy je v rozmezí jednoho až dvou týdnů. Ve srovnání s náklady varianty A se úspora pohybuje v rozmezí 3 432 – 11 902 Kč a ve srovnání s náklady u varianty B se dokonce úspora pohybuje v rozmezí 4 771 – 13 241 Kč.

Tabulka 20 - Modelový příklad nákladů na záchranu dat č. 2

Hardwarová chyba	
Závada:	poškození ploten (částečná), nebo poškození některé ze čtecích hlav
Příčina:	výrobní vada, stáří média, mechanický otřes
Doba realizace:	1 den – 2 týdny
Cena:	5 000 – 12 000 Kč bez DPH
Úspěšnost záchrany:	70 % - 100 %

Zdroj: Helpdesk, vlastní tvorba

Ve výše uvedených dvou příkladech je vidět, jak vysoké náklady mohou nastat v případě nutnosti obnovy specializovanou firmou. Dále je tu velké riziko ztráty určité části dat a v neposlední řadě je velmi důležité zmínit, že ačkoli se jedná o specializovanou firmu, tak i v tomto případě se vaše soukromá a v mnoha případech nijak nechráněná data dostávají do rukou třetích osob a může tak dojít k jejich zneužití.

Všem těmto rizikům se přitom dá velmi lehce předejít a to pravidelným zálohováním.

5 Závěr

V první části této práce, bylo objasněno téma základních a pokročilých možností ochrany dat, dále byly objasněny základní termíny v problematice zálohování.

V druhé části byly prakticky srovnávány aplikace pro automatické zálohování v prostředí Windows, konkrétně byly testovány v operačním systému Windows 7 Home Premium. K určení kompromisní varianty mezi jednotlivými aplikacemi byla použita vícekriteriální analýza variant, kde jednotlivá kritéria byla ohodnocena prostřednictvím metody alokace 100 bodů. Ve srovnání aplikací vyšla jako vítězná aplikace Acronis True Image 2016, na druhém místě byla aplikace Back4all Professional a na třetím místě se umístila freeware aplikace Cobian Backup 11. Z výsledků bylo patrné, že až na aplikaci Cobian Backup 11 lépe dopadl placený software než freeware, který byl v porovnání s placenými aplikacemi převážně jednoduchý a obsahoval jen základní nástroje.

Po dokončení srovnávání zálohovacího softwaru, byly posuzovány cloudová úložiště, konkrétně zkoumání bylo zaměřeno na bezplatné verze, aby byla zmírněna ekonomická náročnost. Cloudy byly hodnoceny též na základě vícekriteriální analýzy variant, kde pro hodnocení jednotlivých kritérií bylo použito metody bodovací, při čemž váhy kritérií byly stanoveny metodou pořadí. Z hodnocených cloudových úložišť dopadlo nejlépe od poskytovatele MEGA, které nabízelo největší úložný prostor oproti ostatním, dále dle hodnocení velikosti kapacity nahrávaného souboru se sice umístilo na druhém místě, ale dále disponovalo dostupností na jiných platformách i desktopovou aplikací. Na druhém místě se umístilo úložiště od společnosti Google „Google drive“.

Poté byly navrhnuty dvě varianty zálohování, samozřejmě v oblasti zálohování existuje velké množství postupů a strategií, avšak tato práce byla zaměřena na domácí prostředí, a proto tyto varianty byly zpracovány tak, aby byly pro uživatele jak efektivní, tak snadné na nastavení.

V závěru práce bylo poukázáno na ekonomické hledisko úspory nákladů, neboť v případě absence pravidelných záloh a následné nutnosti obnovy dat specializovanou firmou dochází k velmi vysokým nákladům, kterým by se pravidelným zálohováním lehce předešlo.

6 Seznam použité literatury

- 3S.CZ. 2012.** Definice a rotace záloh. *3S.CZ.* [Online] 27. Únor 2012. [Citace: 27. Prosinec 2015.] <http://www.storage.cz/cs/odborna-sekce/detail/id/46-definice-a-rotace-zaloh>.
- Acronis.** Acronis True Image 2016 - 1 Computer. [Online] [Citace: 24. Únor 2016.] <http://shop.backup-store.cz/true-image-2016-1computer.html?webSyncID=5ea4e62e-c08b-6b61-49a8-e29647da29a2&sessionGUID=356a7241-8e72-7ae4-6a7a-75212dd6ca02>.
- Amenit.** antivirové centrum. [Online] [Citace: 24. Prosinec 2014.] <http://www.antivirovecentrum.cz/firewally.aspx>.
- Bezpečný internet.** Hesla. *Bezpečný internet.* [Online] [Citace: 10. Únor 2016.]
- Bráza, Jiří. 2000.** *WinZip, WinRAR a další komprimační programy.* Praha : Grada Publishing, 2000. ISBN 80-247-9005-X.
- Budai David, Janů Stanislav, Dědiček Dominik. 2012.** *Bible vypalování a zálohování.* Brno : Extra Publishing, s.r.o., 2012. ISSN 1802-1220, MK ČR E 17010.
- centrum, Antivirové.** Antispyware. *antivirovecentrum.* [Online] Amenit s.r.o. [Citace: 26. Únor 2016.] <http://www.antivirovecentrum.cz/antispyware.aspx>.
- Cloud. 2016.** CLOUD COMPUTING: CO TY POJMY ZNAMENAJÍ? *Cloud.* [Online] 2016. [Citace: 1. Březen 2016.] <http://www.cloud.cz/cloud/158-cloud-computingco-ty-pojmy-znamenaji.html>.
- Doseděl, Tomáš. 2004.** *Počítačová bezpečnost a ochrana dat.* Brno : Computer Press, 2004. ISBN 80-251-0106-1.
- Eagle. 2005.** Pořídíte si RAID 1 (zrcadlení). *Svět Hardware.* [Online] 12. Leden 2005. [Citace: 14. Leden 2016.] <http://www.svethardware.cz/poridte-si-raid-1-zrcadleni/11180>.
- Hoax.** Malware. *Hoax.* [Online] [Citace: 26. únor 2016.] <http://www.hoax.cz/malware/>.
- Horák, Jaroslav. 2006.** *Havárie počítače.* Brno : Computer Press, a.s., 2006. ISBN 978-80-251-1451-3.
- Kaspersky.** Získejte více informací o malwaru a způsobech ochrany proti němu. [Online] Kaspersky Lab. [Citace: 26. Únor 2016.] <http://www.kaspersky.com/cz/internet-security-center/internet-safety/what-is-malware-and-how-to-protect-against-it>.
- Kejduš, Radek. 2011.** Úvod do NAS serverů – Váš domácí cloud. *PC tuning.* [Online] 9. Květen 2011. [Citace: 7. Únor 2016.] <http://pctuning.tyden.cz/software/zalohovani-zachrana-dat/20780-uvod-do-nas-serveru-vas-domaci-cloud?start=4>.

- Kocman, Rostislav a Lohniský, Jakub. 2005.** *Jak se bránit virům, spamu, dialerům a spyware.* Brno : CP Books, a.s., 2005. ISBN 80-251-0793-0.
- Kocmánek, Vít. 2003.** Přehled všech režimů RAID - rychlejší a bezpečnější ukládání dat . *Živě.* [Online] 2. Duben 2003. [Citace: 27. Únor 2016.] <http://www.zive.cz/clanky/prehled-vsech-rezimu-raid---rychlejsi-a-bezpecnejsi-ukladani-dat/raid-10-2-3-4-5/sc-3-a-111138-ch-27726/default.aspx>.
- Kolářek, Michal. 2008.** Externí pevné disky a boxy obecně. *Svět hardware.* [Online] 5. Srpen 2008. [Citace: 7. Únor 2016.] <http://www.svethardware.cz/externi-pevne-disky-a-boxy-obecne/23856>.
- Kuchař, Michal. 1999.** *Bezpečná síť.* Praha : Grada Publishing, 1999. ISBN 80-7169-886-5.
- Lalík, Aleš. 2009.** Vývoj optických médií 1 - CD. *Notebook.* [Online] 22. Červenec 2009. [Citace: 27. Prosinec 2015.] <http://notebook.cz/clanky/technologie/2009/vyvoj-opticky-ch-medii-1-cd>.
- Laš, Jan. 2015.** Téma – Cloudová úložiště. *Android CHÁPU TO.* [Online] 30. Leden 2015. [Citace: 21. únor 2016.] <http://android.chaputo.cz/tema-cloudova-uloziste/#obecne-funkce-cloudovych-ulozist>.
- Leber, Josef. 1998.** *Windows NT Zálohování a obnova dat.* Praha : Computer Press, 1998. ISBN 80-7226-123-1.
- Leixner, Miroslav. 1993.** *PC - zálohování a archivace dat.* Praha : Grada, a.s., 1993. ISBN 80-85424-73-8.
- Microsoft.** Principy nastavení Windows Firewallu. *Microsoft.* [Online] [Citace: 25. Prosinec 2015.] <http://windows.microsoft.com/cs-cz/windows/understanding-firewall-settings#1TC=windows-7>.
- Morkes, David. 1998.** *Komprimační a archivační programy.* Brno : Computer Press, 1998. ISBN 80-7226-089-8.
- Mozilla.** správce hesel. [Online] [Citace: 25. Prosinec 2015.] https://support.mozilla.org/cs/kb/spravce-hesel-zapamatovani-mazani-ci-zmena-ulozeny#w_ochrana-hesel.
- Natarajan, Ramesh. 2011.** RAID 2, RAID 3, RAID 4, RAID 6 Explained with Diagram. *The Geek Stuff.* [Online] 21. Listopad 2011. [Citace: 14. Leden 2016.] <http://www.thegeekstuff.com/2011/11/raid2-raid3-raid4-raid6/>.

Pecinovský, Josef. 2003. *Archivace a komprimace dat*. Praha : Grada Publishing a.s., 2003. ISBN 80-247-0659-8.

Philips. The history of the CD - The beginning. *Philips Research*. [Online] [Citace: 26. Prosinec 2015.] <http://www.research.philips.com/technologies/projects/cd/>.

Stormware. Zálohování dat. *Stormware*. [Online] [Citace: 28. Prosinec 2015.] http://www.stormware.cz/prirucka-pohoda-online/Zakladni_dovednosti/Zalohovani_dat/.

TechTarget. 2014. RAID 2 Definition. *Techtarget*. [Online] Prosinec 2014. [Citace: 14. Leden 2016.] <http://searchstorage.techtarget.com/definition/RAID-2-redundant-array-of-independent-disks>.

Tuhý, Radan. 2013. ukládáme hesla do cloudu. *Svět hardware*. [Online] 21. Březen 2013. [Citace: 25. Prosinec 2015.]

UNET. co je to firewall. *Unet*. [Online] [Citace: 24. Prosinec 2015.] <https://www.unet.cz/blog/2015/09/10/co-je-to-firewall/>.

Velte, T., Anthony, Velte, J., Toby a Elsenpeter, Robert. 2011. *Cloud Computing: Praktický průvodce*. Brno : Computer Press, a.s., 2011. ISBN 978-80-251-3333-0.

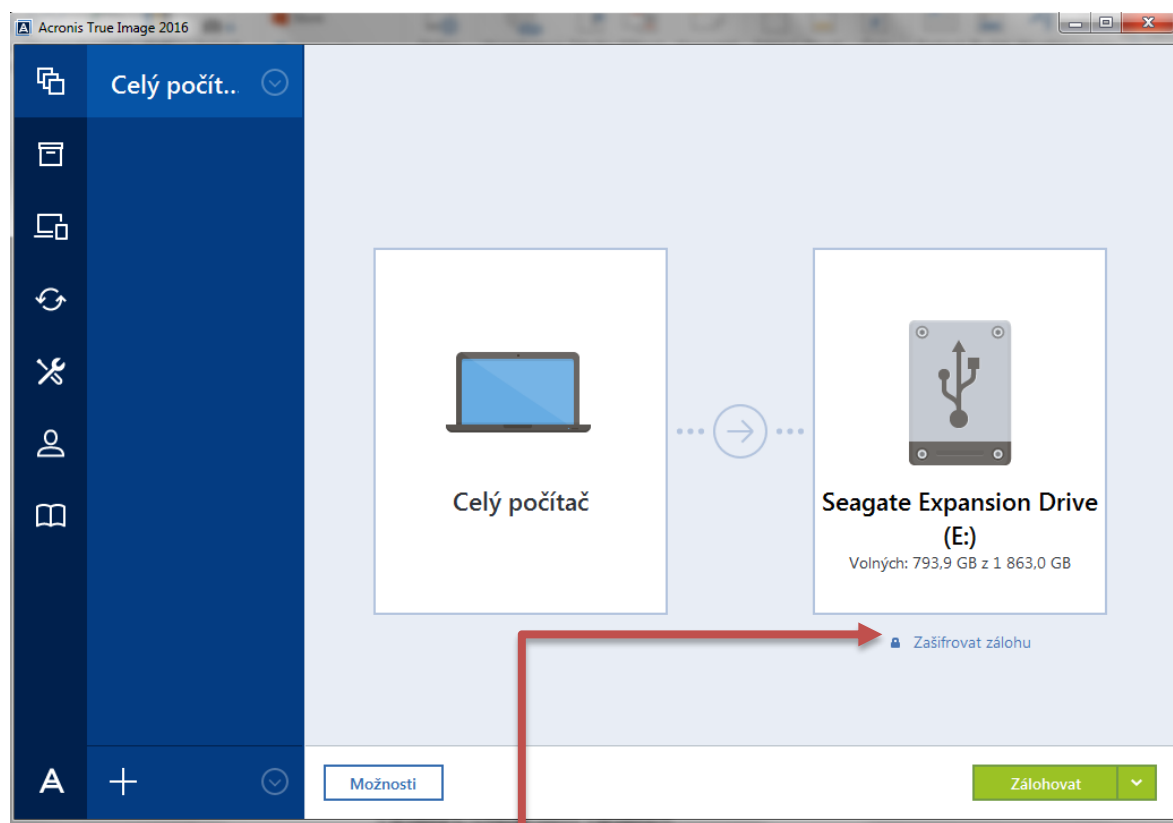
7 Přílohy

7.1 Příloha A

Návod pro variantu A

1. Krok

V prvním kroku zvolíme, co budeme zálohovat a kam se záloha bude vytvářet. V našem případě se bude jednat o zálohu celého počítače a záloha se bude vytvářet na externí pevný disk.

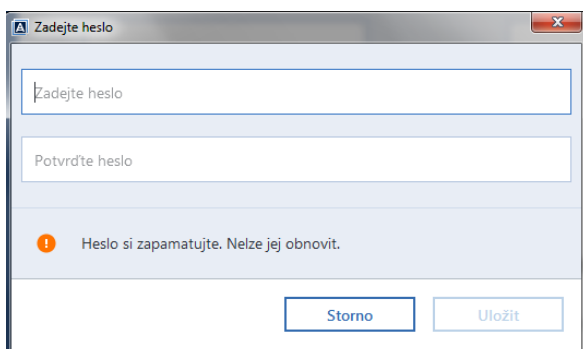


Obrázek 6 - Acronis True Image (úvodní obrazovka), zdroj: vlastní tvorba

2. Krok

V druhém kroku zvolíme možnost „zašifrovat zálohu“, abychom v případě odcizení pevného disku zamezili přístup k záloze neoprávněným osobám. V případě zvolení této možnosti jsou data automaticky šifrována algoritmem AES 256 bits.

Po zvolení této možnosti se uživateli objeví následující tabulka s požadavkem na zadání hesla (šifrovacího klíče)

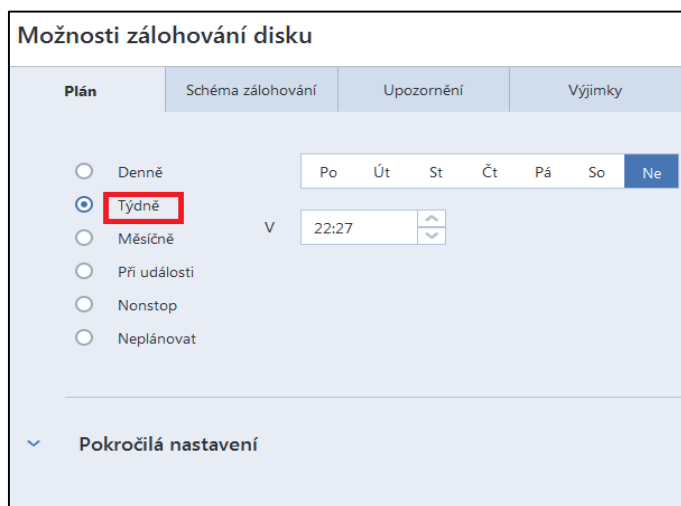


Obrázek 7 - Acronis True Image (tabulka pro vložení šifrovacího klíče), zdroj: [vlastní tvorba]

Šifrovací klíč je nutné si dobře zapamatovat, protože nelze obnovit a v případě ztráty je záloha nepoužitelná.

3. Krok

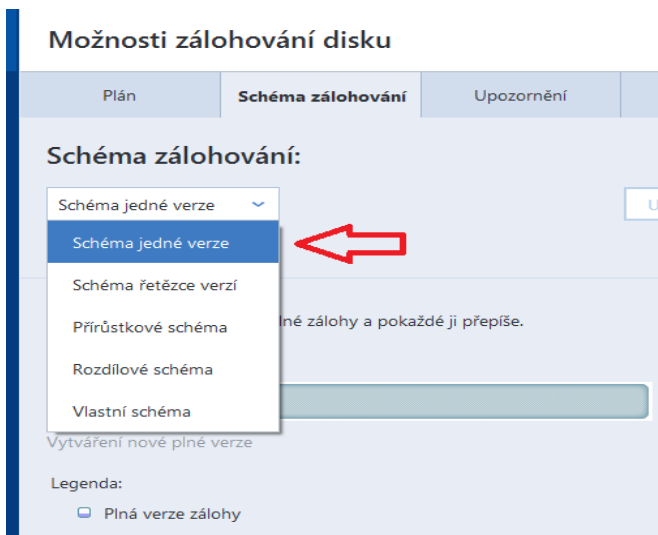
Ve třetím kroku zvolíme na úvodní obrazovce položku „MOŽNOSTI“ a nastavíme pravidelný automatický rozvrh záloh. V našem případě zvolíme možnost tvorby týdenních záloh například v neděli. (Tento krok je skutečně závislý na intenzitě práci s daty, některému uživateli bude stačit tvořit zálohu jednou měsíčně a některému jednou týdně)



Obrázek 8 - Acronis True Image (nastavení rozvrhu záloh), zdroj: [vlastní tvorba]

4. Krok

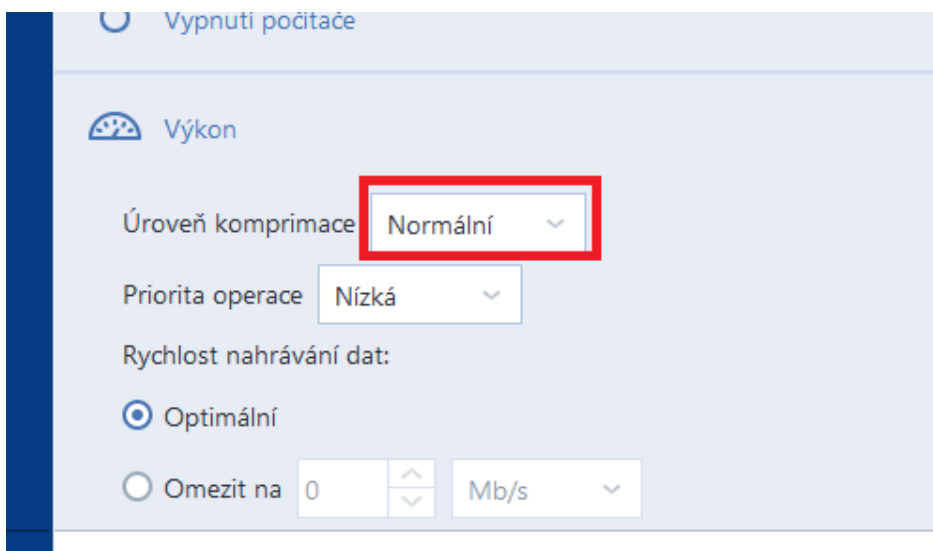
Ve čtvrtém kroku zvolíme schéma zálohování, kde vybereme možnost „Schéma jedné verze“.



Obrázek 9 - Acronis True Image (výběr typu zálohy), zdroj: [vlastní tvorba]

5. Krok

V pátém kroku v možnostech na kartě „pokročilé“ nastavíme možnost komprimace na úroveň „Normální“, pro dosažení kompromisu mezi velikostí zálohy a délkou tvorby zálohy.



Obrázek 10 - Acronis True Image (nastavení úrovně komprese), zdroj: [vlastní tvorba]

6. Krok

V šestém posledním kroku již na úvodní stránce zvolíme možnost „ZÁLOHOVAT“



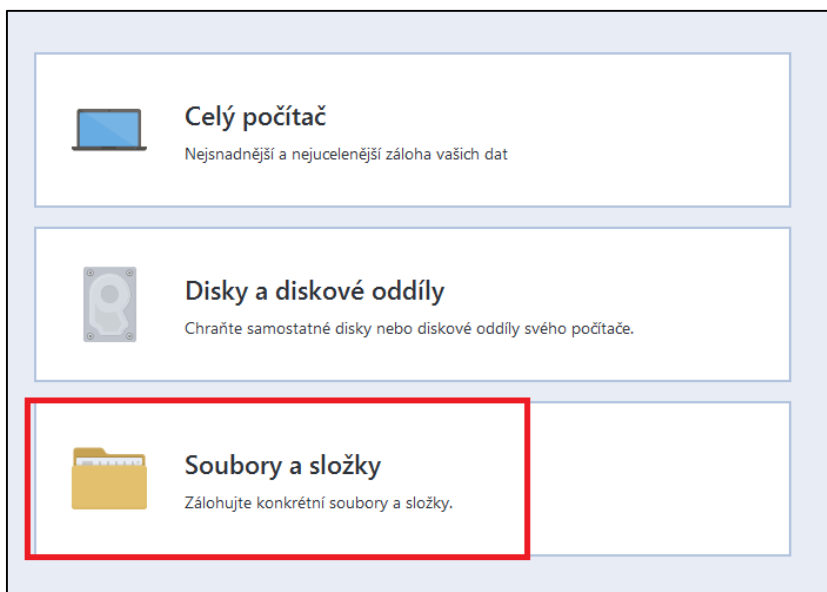
Obrázek 11 - Acronis True Image (spuštění zálohovacího procesu), zdroj: [vlastní tvorba]

Tímto jsme vytvořili celkovou zálohu počítače na externí pevný disk. Nicméně pro ochranu dat je důležité mít data zálohována na jiném místě než je originál dat, aby například v případě krádeže či živelné pohromy nedošlo i ke ztrátě zálohy, proto je vhodné využít cloudového úložiště, které přímo poskytuje společnost Acronis s neomezenou kapacitou a na toto úložiště vytvořit opět zálohu celého disku (ale tato možnost by byla velmi časově náročná a také náročná na přenos dat, neboť komplexní zálohy mají velkou náročnost na úložný prostor). Uživatel tedy může provést zálohu jen určitých (nenahraditelných) souborů na cloudové úložiště, my si například vybereme v počítači složky dokumenty, fotky a videa, které samostatně zálohujeme. Díky možnosti multizálohování je možné tuto zálohu též zautomatizovat.

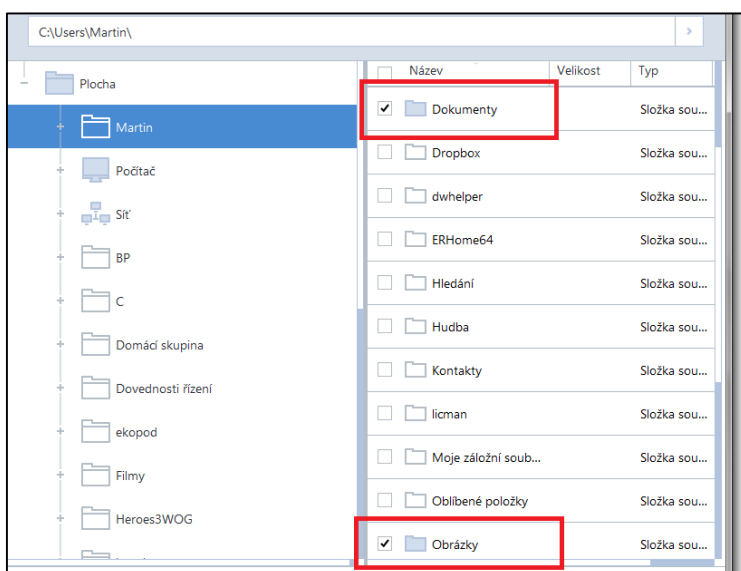
Postup provedení zálohy je totožný, až na výběr toho, co budeme zálohovat a kam budeme zálohu vytvářet. Změny si ukážeme v následujících krocích.

1. Krok

V prvním kroku vybere namísto zálohy celého počítače možnost „Soubory a složky“.



Obrázek 12 - Acronis True Image (výběr typu zálohování), zdroj: [vlastní tvorba]



Obrázek 13 - Acronis True Image (výběr konkrétní složky pro zálohování), zdroj: [vlastní tvorba]

2. Krok

Ve druhém kroku vybereme, jako úložiště možnost „Acronis Cloud“.



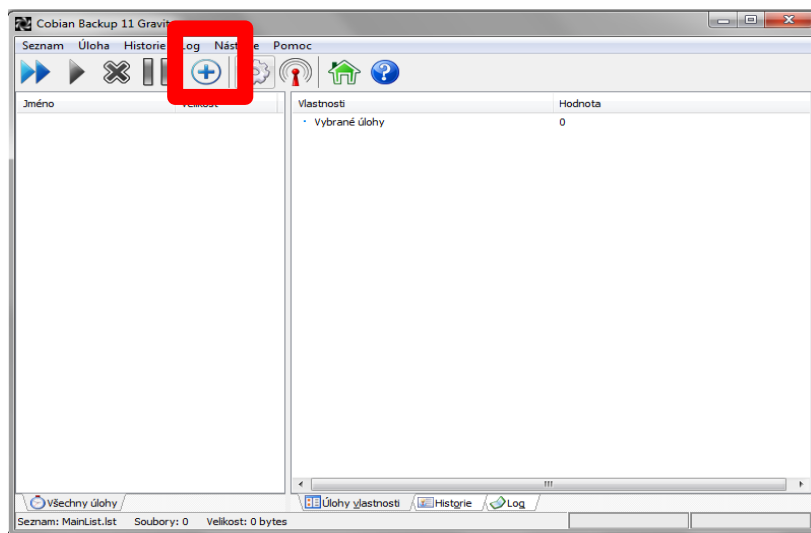
Obrázek 14 - Acronis True Image (výběr cíle zálohy Acronis Cloud), zdroj: [vlastní tvorba]

7.2 Příloha B

Návod pro variantu A

1. Krok

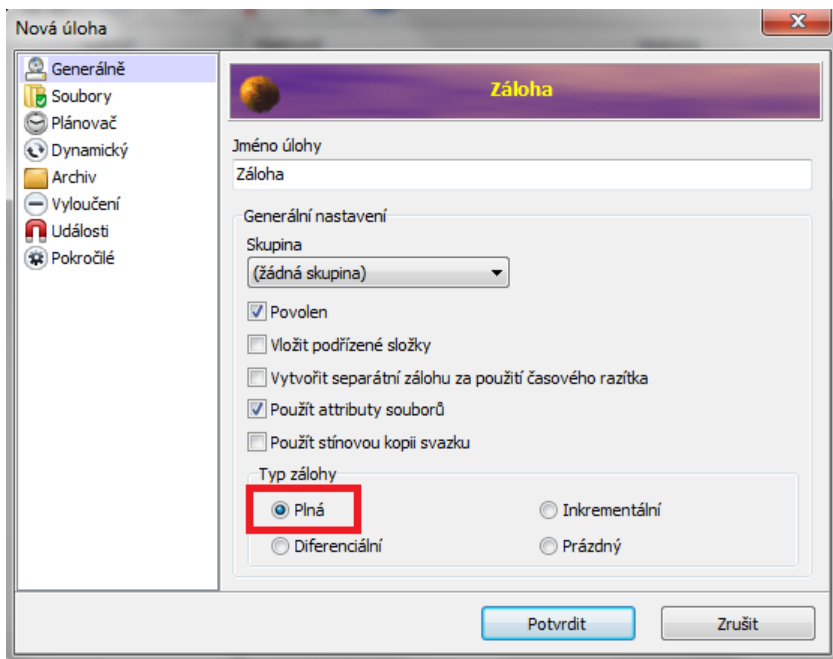
V prvním kroku zvolíme možnost vytvořit novou úlohu zálohování, tato možnost je v uživatelském rozhraní znázorněna symbolem plus.



Obrázek 15 - Cobian Backup 11 (úvodní obrazovka), zdroj: [vlastní tvorba]

2. Krok

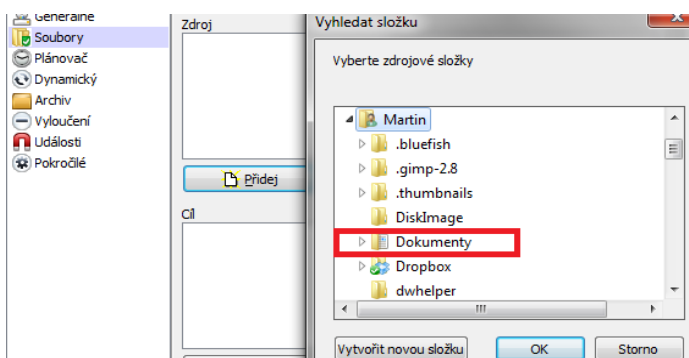
Ve druhém kroku si zvolíme typ zálohy „plná záloha“ a pojmenujeme zálohovací úlohu například „Záloha“, abychom v případě tvorby více zálohovacích úloh dokázali rozeznat úlohy mezi sebou, kdybychom potřebovali nějakou editovat.



Obrázek 16 - Cobian Backup 11 (výběr typu zálohy), zdroj: [vlastní tvorba]

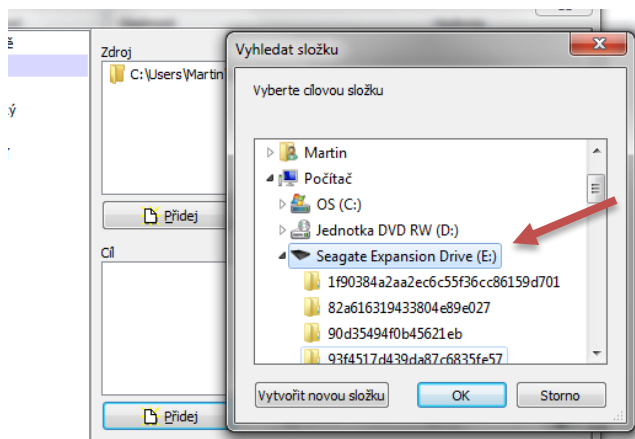
3. Krok

Ve třetím kroku vybereme zdroj zálohy, neboli soubory či složky, které chceme zálohovat. V našem případě budeme volit například složku „Dokumenty“.



Obrázek 17 - Cobian Backup 11 (výběr zdroje zálohy), zdroj: [vlastní tvorba]

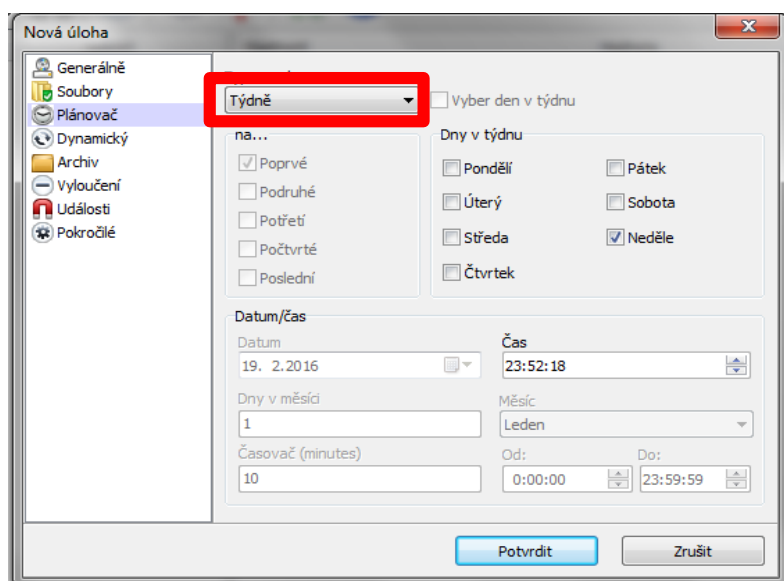
Dále vybereme cíl, kam budeme vytvářet zálohu. V našem případě volíme externí pevný disk.



Obrázek 18 - Cobian Backup 11 (výběr cíle pro vytvoření zálohy), zdroj: [vlastní tvorba]

4. Krok

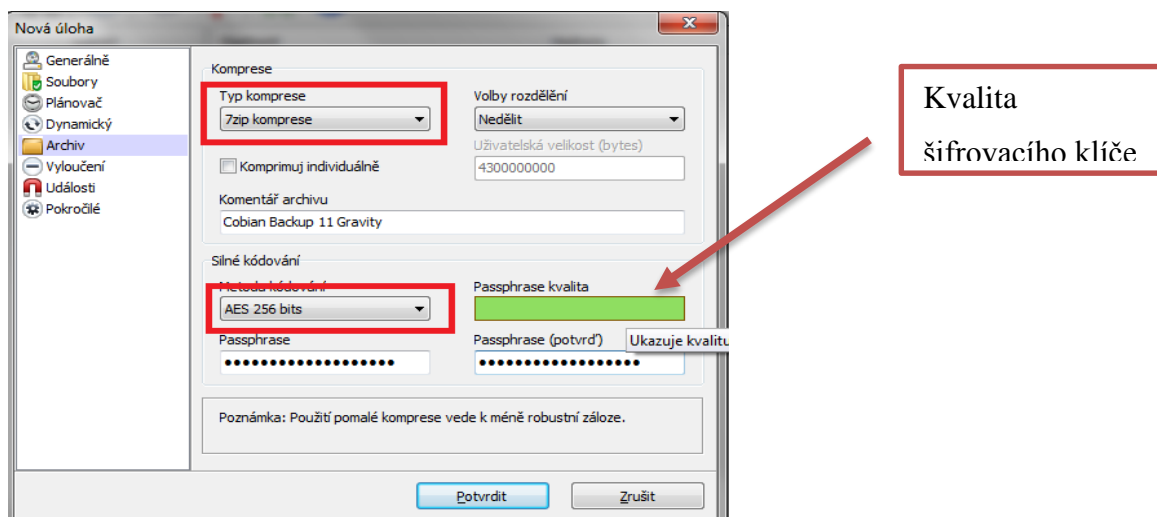
Ve čtvrtém kroku nastavíme rozvrh plánování záloh. Opět zvolíme možnost týdenního zálohování v neděli jako v předešlé variantě.



Obrázek 19 - Cobian Backup 11 (nastavení rozvrhu záloh), zdroj: [vlastní tvorba]

5. Krok

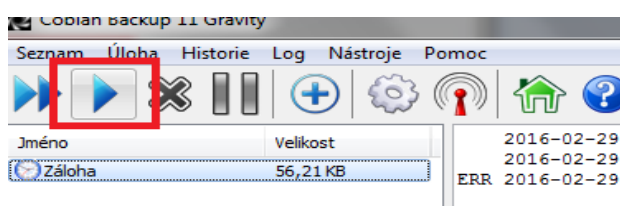
V pátém kroku zvolíme typ komprese „7zip komprese“ a nastavíme metodu kódování na „AES 256 bits“ a následně si zvolíme vlastní šifrovací klíč. Při volení šifrovacího klíče aplikace automaticky upozorňuje na kvalitu klíče. Šifrovací algoritmus AES 256 bits volíme vzhledem k jeho vyšší úrovni bezpečnosti.



Obrázek 20 - Cobian Backup 11 (nastavení komprese a šifrování), zdroj: [vlastní tvorba]

6. Krok

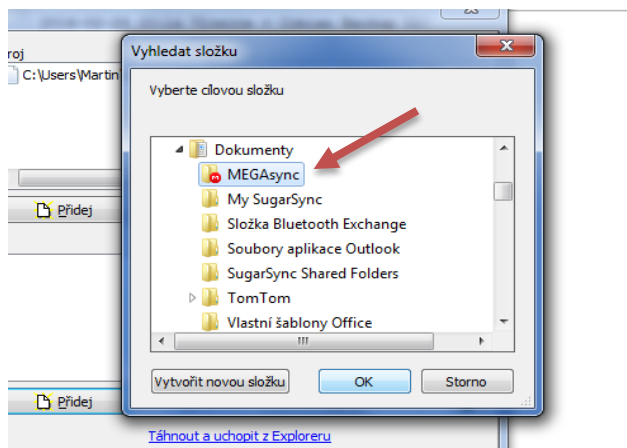
V šestém posledním kroku již spustíme proces zálohování, v uživatelském rozhraní je tento nástroj spuštění procesu zálohy zobrazen jako tlačítko „play“



Obrázek 21 - Cobian Backup 11 (spuštění zálohovacího procesu), zdroj: [vlastní tvorba]

I v tomto případě je však dobré mít data zálohována daleko od původních dat, a proto použijeme možnost vytvoření další zálohovací úlohy a zálohu vytvoříme na cloudové úložiště MEGA. Nejjednodušším způsobem, jak provést zálohu na zmíněný cloud v tomto případě je provést zálohu do složky MEGAsync, kterou uživatel automaticky získá po nainstalování klienta pro synchronizace s cloudem MEGA. Výchozí umístění této složky je C:\Users\UŽIVATEL\Documents\MEGAsync . Data vložená do této složky jsou okamžitě synchronizována s vaším cloudovým úložištěm.

Jediná změna, která v tomto případě nastává, je změna cílové složky, ostatní kroky pro nastavení zálohy zůstávají stejné. Změnu si ukážeme na následujícím obrázku.



Obrázek 22 - Cobian Backup 11 (výběr cíle zálohy- cloud), zdroj: [vlastní tvorba]