



VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ

FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY

INSTITUTE OF INFORMATICS

ZÁLOHOVÁNÍ DAT A DATOVÁ ÚLOŽIŠTĚ

DATA BACKUP AND DATA STORAGE

BAKALÁŘSKÁ PRÁCE

BACHELOR'S THESIS

AUTOR PRÁCE

AUTHOR

Klára Rudy

VEDOUCÍ PRÁCE

SUPERVISOR

Ing. Jiří Kříž, Ph.D.

BRNO 2023

Zadání bakalářské práce

Ústav: Ústav informatiky
Studentka: **Klára Rudy**
Vedoucí práce: **Ing. Jiří Kříž, Ph.D.**
Akademický rok: 2022/23
Studijní program: Manažerská informatika

Garant studijního programu Vám v souladu se zákonem č. 111/1998 Sb., o vysokých školách ve znění pozdějších předpisů a se Studijním a zkušebním řádem VUT v Brně zadává bakalářskou práci s názvem:

Zálohování dat a datová úložiště

Charakteristika problematiky úkolu:

Úvod
Cíle práce, metody a postupy zpracování
Teoretická východiska práce
Analýza současného stavu
Vlastní návrhy řešení
Závěr
Seznam použité literatury
Přílohy

Cíle, kterých má být dosaženo:

Cílem práce je analýza současného stavu datového úložiště a způsobu ukládání dat ve společnosti a následné vylepšení bezpečnosti a efektivity.

Základní literární prameny:

CUBR, L. Dlouhodobá ochrana digitálních dokumentů. Praha: Národní knihovna České republiky, 2010. ISBN 978-80-7050-588-5

DEMBOWSKI, K. Mistrovství v hardware. 1.vyd. Brno: Computer Press, 2009. ISBN 978-80-251-2310-2

NELSON, S. Pro data backup and recovery. New York: Distributed to the book trade worldwide by Springer Science+Business Media, 2011. ISBN 978-1-4302-2663-5.

PECINOVSKÝ, J. Archivace a komprimace dat. Praha: Grada Publishing a.s., 2003. ISBN 80-24-0659-8

Termín odevzdání bakalářské práce je stanoven časovým plánem akademického roku 2022/23

V Brně dne 5.2.2023

L. S.

Ing. Jiří Kříž, Ph.D.
garant

doc. Ing. Vojtěch Bartoš, Ph.D.
děkan

Abstrakt

Bakalářská práce se zabývá problematikou týkající se zálohování dat a datovými úložišti. Teoretická část nastiňuje způsob, jakým počítače čtou data. Následně je popsána historie datových úložišť, od děrných štítků po cloud. Část zabývající se zálohováním popisuje jednotlivé druhy zálohování spolu s doporučenými postupy. Praktická část práce analyzuje společnost Krako-Welding, s. r. o., jejíž výsledkem je návrh pro vylepšení praktik pro zacházení s uloženými daty.

Klíčová slova

data, soubory, zálohování, datová úložiště, datová bezpečnost

Abstract

The bachelor's thesis deals with the problematics pertaining to data backup and data storage. The theoretical section describes how computers interpret data. The history of data storage is then described, starting with punched cards and ending with the cloud. The section concerning data backup describes different types of backups along with suggested practices. The practical section of the thesis covers the analysis of the company Krako-Welding, s.r.o., the result of which is a proposal for improving practices for handling stored data.

Keywords

data, files, backup, data storage, data security

Bibliografická citace

RUDY, Klára. *Zálohování dat a datová úložiště* [online]. Brno, 2023 [cit. 2023-04-28]. Dostupné z: <https://www.vutbr.cz/studenti/zav-prace/detail/152364>. Bakalářská práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Ing. Jiří Kříž, Ph.D.

Čestné prohlášení

Prohlašuji, že předložená bakalářská práce je původní a zpracovala jsem ji samostatně. Prohlašuji, že citace použitých pramenů je úplná, že jsem ve své práci neporušila autorská práva (ve smyslu zákona č. 121/2000 Sb., o právu autorském a o právech souvisejících s právem autorským).

V Brně dne 28. 4. 2023

Klára Rudy

autor

Poděkování

Ráda bych poděkovala panu Ing. Jiřímu Křížovi, Ph.D. za vedení a konzultaci mé bakalářské práce. Dále bych chtěla poděkovat panu Michalovi Krakovskému a paní Jitce Krakovské, spolu s ostatními zaměstnanci Krako-Welding, s. r. o., za jejich vstřícný přístup a panu Kalandrovi za poskytnutí informací pro vypracování praktické části bakalářské práce.

Obsah

Úvod.....	9
Cíl práce, metody a postupy zpracování	10
1. Teoretická východiska práce	11
1.1. Data a soubory.....	11
1.1.1. Základní informace	11
1.1.2. Souborový systém	11
1.1.3. NTFS.....	13
1.2. Datová úložiště.....	16
1.2.1. Děrný štítek.....	16
1.2.2. Magnetická páska	17
1.2.3. HDD Pevný disk	19
1.2.4. Floppy disk Disketa	21
1.2.5. CD Kompaktní disk	22
1.2.6. SSD Polovodičový disk	25
1.2.7. USB flash disk	27
1.3. Cloud	29
1.3.1. Historie internetu a cloudu.....	29
1.3.2. Cloudová architektura	30
1.4. Implementace datových úložišť	33
1.4.1. Identifikace potřeb	33
1.4.2. Datová bezpečnost	35
1.5. Zálohování dat.....	38
1.5.1. Typy záloh	38
1.5.2. Zálohovací strategie.....	40
1.5.3. Obnova dat.....	41
2. Analýza současného stavu	43
2.1. Informace o společnosti	43
2.2. Popis budovy.....	44
2.2.1. Vybavení místností	45
2.3. Síťová infrastruktura	45
2.3.1. Hardware.....	47
2.4. Zacházení s daty	48
2.4.1. Ukládání dat.....	48
2.4.2. Zálohování	48
2.4.3. E-mail a webové stránky.....	48
2.5. Bezpečnost a hrozby	49
2.5.1. Vnitřní hrozby.....	49
2.5.2. Vnější hrozby	50
3. Vlastní návrhy řešení	51
3.1. Zálohování.....	51
3.2. Ukládání dat	53
3.3. Bezpečnostní postupy.....	53
3.4. Zhodnocení vlastního návrhu.....	54
Závěr.....	56
Seznam použité literatury	57
Přílohy.....	59
Seznam obrázků.....	59
Seznam tabulek.....	59

Úvod

Dnešní době se přezdívá informační věk. V životě téměř každého člověka hrají zásadní roli technologie, které rapidně rostou ve své výkonnosti a sofistikovanosti a data začínají být tou nejcennější věcí, kterou jedinec i organizace může vlastnit. Data mohou být chápány jako souhrn poznatků, které v celku poskytují konkrétní informace. Co původně začalo jako malé množství instrukcí pro ovládání stroje, se postupem času přeměnilo na zdroj vše různých informací s multimiliardovou tržní hodnotou.

Data jsou kvůli jejich cennosti žádaná jak pro organizace, tak pro útočníky, kteří se jejich odcizením chtějí obohatit. Každoročně se množství počítačové kriminality zvyšuje, proto je obzvláště důležité, aby se firmy i jedinci aktivně zajímali o datovou bezpečnost a uplatňovali preventivní opatření. Navigování kyberprostorem může být přirovnáno k řízení auta. Pokud jsou dodržována pravidla silničního provozu, snižuje se riziko, že se jedinec stane účastníkem autonehody. Toto riziko není možné úplně eliminovat, avšak pokud jsou použity bezpečnostní pásy a funkční airbagy, značně se sníží dopad, jaký nehoda může mít. Tyto stejné principy platí i v datové bezpečnosti, kde způsob interakce s kyberprostorem rozhoduje o výši rizika nehody, a zálohy slouží jako bezpečnostní pás v případě napadení kyberútočníky.

Teoretická část této práce se zabývá vývojem a charakteristikami datových úložišť, zálohováním dat a datovou bezpečností. Získané poznatky byly aplikovány při vypracování praktické části, která spočívá v analýze konkrétní společnosti. Během analýzy byly zhodnoceny bezpečnostní postupy společnosti, způsob zacházení s daty, hardwarová výbava a zálohovací strategie. Výsledkem analýzy byl návrh vlastního řešení pro zlepšení současného stavu.

Cíl práce, metody a postupy zpracování

Cílem práce je provést analýzu současného stavu datových úložišť a způsobu ukládání dat ve společnosti a navrhnout následného vylepšení bezpečnosti a efektivity.

Teoretická východiska práce by měla seznámit čtenáře s problematikou dat a nastínit, jak dnešní technologie data interpretují. Dále se práce zabývá historií vývoje datových úložišť a poskytnout přehled o výhodách a nevýhodách jednotlivých úložišť. Následně práce pojednává o bezpečnostních praktikách, zálohování dat a problematice s ní spojené.

Praktická část práce se zabývá analýzou konkrétní firmy s ohledem na datovou bezpečnost, zacházení s daty a způsoby zálohování. Na základě analýzy a teoretických poznatků je následně vytvořen vlastní návrh, který by měl řešit problémy, které byly identifikovány během analýzy, v co nejvíce přijatelnější míře pro snadnou integraci.

1. Teoretická východiska práce

1.1.Data a soubory

1.1.1. Základní informace

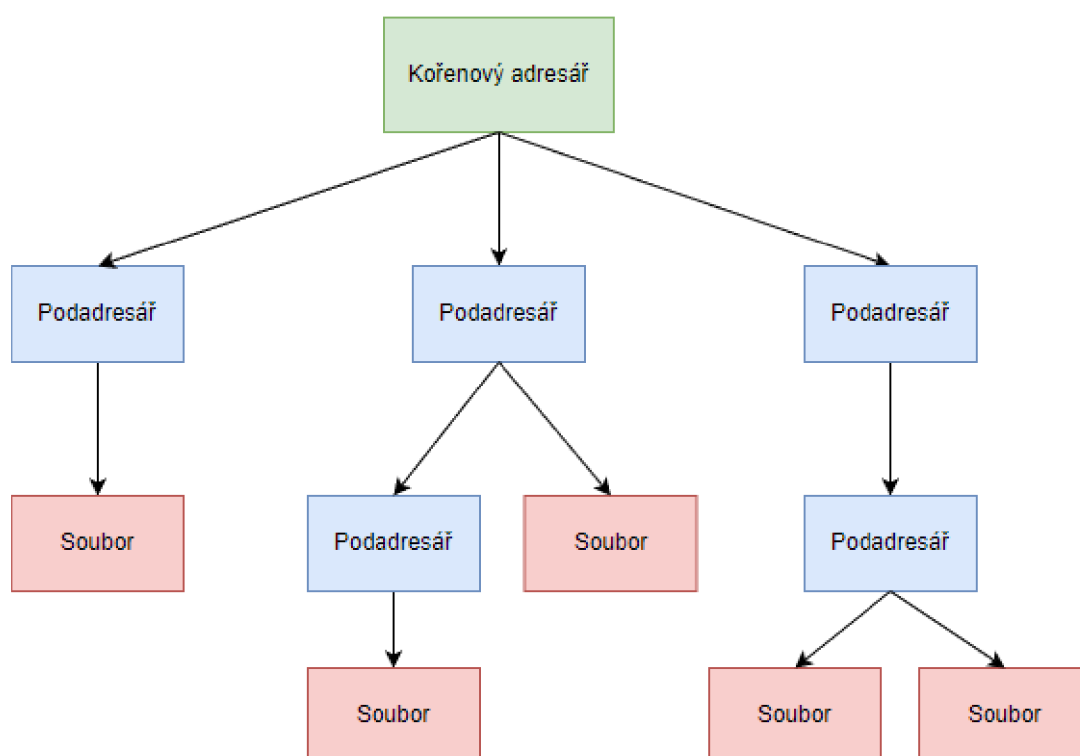
Matematická informatika je vědecký obor, zabývající se zpracováním a přenosem informací softwarového charakteru. Hlavním subjektem tohoto oboru jsou data a programy. Počítačový program lze definovat jako sadu instrukcí napsané programovacím jazykem, který zpracovává data formou shromažďování, správy či analýzou. Data mají podobu formalizovaného seskupení faktů, které jsou zaznamenány pomocí symbolů, jmenovitě písmena abecedy, čísla a speciální znaky, jako jsou lomítka, plus, minus a mnoho dalších. Z dat je možné následně získat informace, které mají pro konečného uživatele přínos. Aby data mohla být zpracována, musí je být možné skladovat a ukládat. Reálná data mohou být například sepsána na papíře a uložena v archivu, aby tato data však bylo možné interpretovat, musí být zapsána standardizovanou formou, která je pro čtenáře pochopitelná a musí být známo, kde se nachází. Digitální data fungují na stejném principu, ale místo člověka je musí být schopen pochopit počítač. Stejně jako člověk rozumí slovům, počítač chápe uspořádané sekvence 1 a 0 prostřednictvím binárního kódu. Pokud chceme v počítači uchovat data, která nám mají poskytnout informaci „A,” binární kód je vidí jako „01000001”. Obdobně jako lidé mají fyzická úložiště, jako jsou archivy, nebo i knihy, počítače mají paměťová média, jinými slovy datová úložiště. [1, 2]

1.1.2. Souborový systém

Jednotka	Rovná se
1 Bit	Binární hodnota
8 Bitů	1 Bajt
1024 Bajtů	1 Kilobajt
1024 Kilobajtů	1 Megabajt
1024 Megabajtů	1 Gigabajt
1024 Gigabajtů	1 Terabajt
1024 Terabajtů	1 Petabajt
1024 Petabajtů	1 Exabajt
1024 Exabajtů	1 Zettabajt
1024 Zettabajtů	1 Yottabajt
1024 Yottabajtů	1 Brontobajt

Obrázek 1 Tabulka jednotek [Vlastní zpracování]

Počítač data ukládá v podobě bitů. Každý bit reprezentuje jednu binární hodnotu, což znamená, že výše uvedené písmeno „A”, které je zapsáno jako „01000001”, má 8 bitů. Je zřejmé, že se jedná o velmi malou jednotku, kdybychom chtěli data číst na úrovni bitů, pohybovali bychom se v milionových hodnotách, proto byly zavedeny jednotky, jako jsou bajt, megabajt a gigabajt. V důsledku neustálého růstu objemu dat se vytvářejí nové a větší jednotky. V tabulce jsou aktuálně používané jednotky. [2, 3]



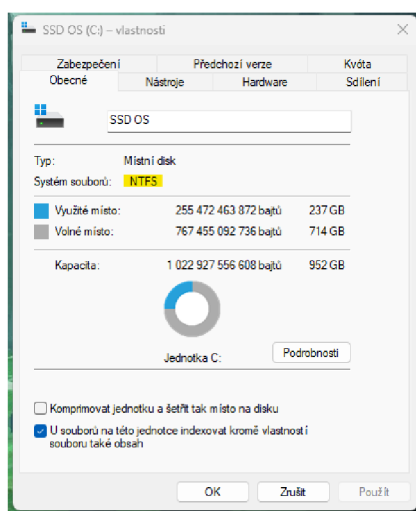
Obrázek 2 Stromová hierarchie [Vlastní zpracování]

Data se na paměťová média ukládají jako datové soubory, které mohou mít podobu textu nebo binárního souboru. Aby však počítač chápal, co to soubor je, potřebuje příručku v podobě souborového systému. Souborový systém odpovídá za funkce datového úložiště, jako jsou rozdělení souborů do uspořádaných skupin a zvolení místa na disku, kde se budou nacházet. Skupinám souborů se říká adresáře. Souborový systém tyto adresáře používá k organizaci souborů pomocí hierarchie, která má stromovou strukturu. Na nejvyšší pozici stojí kořenový adresář, který se postupně dělí na podadresáře, které postupně vedou až k danému souboru. Jednotlivé části adresáře spolu navzájem souvisejí. Programy pomocí těchto adresářů jsou schopny najít data, která

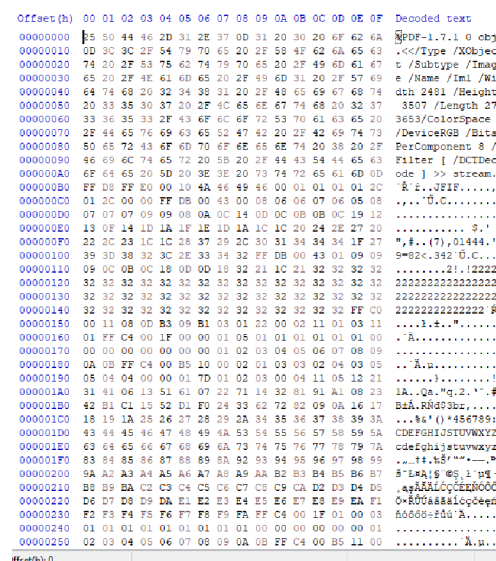
potřebují k provedení svého kódu. Příkladem může být software pro úpravu videí, který jednotlivé soubory, které k úpravě používá, ukládá do složky „Assets”. V této složce se nachází soubor „projekt.mp4”, který má následující adresář „C:\Users\Jmeno_Uživatele\Program\Project_Files\Assets\projekt.mp4”. V této hierarchii je kořenem stromu „C:\”, což je jméno disku, na kterém se soubor nachází, „\Users\Jmeno_Uživatele\Program\Project_Files\Assets\” jsou pod adresáři a souborem je „projekt.mp4”. Program je schopen soubor najít pomocí tohoto konkrétního adresáře, pokud se změní název jednotlivých složek, nebo bude soubor přesunut jinam, program ho nebude schopen najít a dojde k chybě. Adresáře jsou také důvod, proč je možné mít více souborů se stejným názvem, s výjimkou souborů ve stejné složce. V dnešní době existuje mnoho souborových systémů, jako je například APFS (Apple File System) anebo NTFS (New Technology File System), který používá většina nových počítačů s operačním systémem Windows. [4, 5]

1.1.3. NTFS

New Technology File System, neboli NTFS, byl poprvé představen Microsoftem v roce 1993 spolu s operačním systémem Windows NT 3.1 jako následovník jejich původního systému FAT (File Allocation Table) z roku 1977. NTFS je 64bitovým souborovým systémem užívaným v mnoha verzích operačního systému Windows (NT, 2000, Xp, Vista, 7, 8, 10, 11), je také kompatibilní s Linus a MacOS, v případě Mac však poskytuje pouze podporu pro čtení. [4, 6]



Obrázek 4 Snímek systému souborů [Vlastní zpracování]



Obrázek 3 Snímek MTF tabulky [Vlastní zpracování]

Aby disk mohl souborový systém používat, musí nejdříve podstoupit formátování, což je proces konfigurace paměťového média pro daný systém. Při formátování pevného disku, což je komponent, který používá většina stolních počítačů jako své hlavní úložiště, je disk rozdělen na několik oddílů, které přímo odpovídají jejich rozdělení na fyzickém disku. Častou mylnou představou je, že jsou veškerá data na disku následně smazána, to však není zcela pravdou, jelikož se jedná o fyzické paměťové médium, data na disku zůstanou do té doby, dokud nejsou přepsána novými daty. Co se však stane, je, že se smaže nebo přepíše původní souborový systém, spolu se všemi adresáři, což má za následek zpřístupnění starých dat. Posledním krokem formátování je vygenerování nového souborového systému, který se v případě NTFS skládá z několika systémových souborů, jako je Master File Table (MFT). MFT je tabulka, která obsahuje veškeré informace o jednotlivých souborech, jako jsou název, datový typ, obsah, v kterém oddílu se nachází a jeho přesné umístění. Soubory jsou ukládány na oddíly v podobě svazků, což jsou nejmenší jednotky, pomocí které může NTFS přiřadit souboru místo na disku, což znamená, že i když by měl soubor velikost pouze 1 bit, bude uložen ve formě svazku, který má přidělenou velikost 7 MB - 512 MB. Na níže uvedené tabulce jsou uvedeny svazky, které NTFS podporuje. [4, 6, 7]

Svazky	Windows NT 3.51	Windows NT 4.0	Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows Vista, Windows Server 2003, Windows XP, Windows 2000
7 MB–512 MB	512 bytes	4 KB	4 KB
512 MB–1 GB	1 KB	4 KB	4 KB
1 GB–2 GB	2 KB	4 KB	4 KB
2 GB–2 TB	4 KB	4 KB	4 KB
2 TB–16 TB	Není podporováno	Není podporováno	4 KB
16TB–32 TB	Není podporováno	Není podporováno	8 KB
32TB–64 TB	Není podporováno	Není podporováno	16 KB
64TB–128 TB	Není podporováno	Není podporováno	32 KB
128TB–256 TB	Není podporováno	Není podporováno	64 KB
> 256 TB	Není podporováno	Není podporováno	Není podporováno

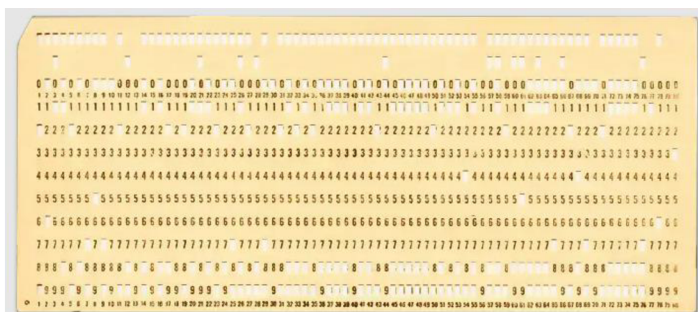
Obrázek 5 Tabulka svazků [Vlastní zpracování]

NTFS je dnes standardem hned z několika důvodů. Hlavní důvod spočívá v tom, že je schopen podporovat velká úložiště dat a zároveň nezabírá moc místa, díky integrované kompresi dat, což snižuje velikost dat a pomáhá zrychlit jejich přesun. Tento systém je také bezpečný, poskytuje prostředky pro šifrování jednotlivých dat nebo celého disku, dále umožňuje správci systému omezit přístup k zvoleným datům, úrovně přístupu jsou: číst, psát, číst a spustit, upravit a plná kontrola. Další výhodou je, že je systém velmi spolehlivý díky svému logování, to znamená, že si systém vede záznam všech změn, které se na disku provedly. Tento záznam pomáhá v situacích, kdy dojde ke katastrofám ve spojitosti s úložišti, jako jsou selhání systémů nebo výpadek proudu. Logování pomáhá zabránit poškození úložiště a také při jeho následné obnově. Systém má však i pár nevýhod. NTFS je vybudovaný specificky pro operační systém Windows, má tedy omezenou kompatibilitu s ostatními OS, jmenovitě Mac a Android. Systém také není schopen podporovat starší zařízení, jako jsou televize, digitální kamery a přehrávače médií. [4, 7]

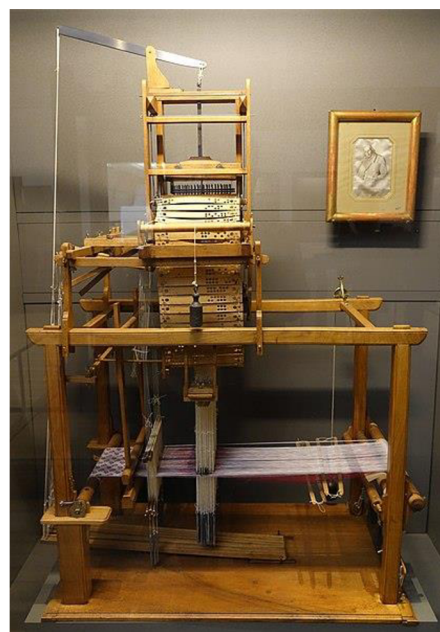
1.2. Datová úložiště

1.2.1. Děrný štítek

Za první datové úložiště se mohou považovat děrné štítky. Jednalo se o tuhý kus papíru, do kterého se podle názvu vytvářely otvory, seřazené ve sloupcích a řádcích. Každý z těchto otvorů představoval kus dat, jmenovitě čísla nebo písmena, z dnešního pohledu tyto otvory můžeme považovat za bity. Data se z karet četla od horního levého rohu vertikálně, odshora dolů. Klasické děrné štítky měly 80 sloupců a 12 řádků, což vychází na 960 bitů, což lze převést na 120 bajtů. Pro představu, jak je tato hodnota malá, obrázek uvedený výše má 1,08 MB, což vychází na 1 138 830 bajtů, pokud bychom chtěli uchovat informace o obrázku čistě v děrných štítcích, potřebovali bychom necelých 9 491 jednotlivých štítků. [8]



Obrázek 6 Děrný štítek [8]



Obrázek 7 Jacquardův tkací stroj [9]

Děrné štítky byly široce používány ve 20. století, avšak jejich kořeny lze vysledovat až v roce 1725, kdy Basile Bouchon a jeho asistenti Jean-Baptiste Falcon a Jacques Vaucanson vytvořili tkací stroj, který pomocí děrných štítků opakovaně vytvořil vzory za asistence pracovníků. Tento proces se dá považovat jako první případ programování. V roce 1804 Joseph Marie Jacquard tento koncept vylepšil, a vytvořil automatický tkací stroj, který byl schopen vzít informace z několika na sebe navazujících děrných štítků.

Umístění otvorů v děrných štítcích určovala, které svislé nitě se zvednou, aby umožnily horizontálním nitím projít pod nimi a vytvořit vzor. [10]

Mezi roky 1880 a 1890 začal děrné štítky používat Herman Hollerith v USA pro účely sčítání lidu. Později založil firmu IBM, která mimo jiné stroje prodávala i děrné štítky, které v 50. letech tvořily až 20 % veškerého zisku firmy. Od toho momentu se štítky rychle rozšířily do dalších sektorů, od podnikatelských až po vládní a vědecké, kde byly standardem až do 60. let, kdy začaly být postupně nahrazovány, do 80. letch byly stále používány pro uchovávání dat a počítačových programů v podobně binárního formátu. Konec éry děrných štítků nastal začátkem 90. let. [11]

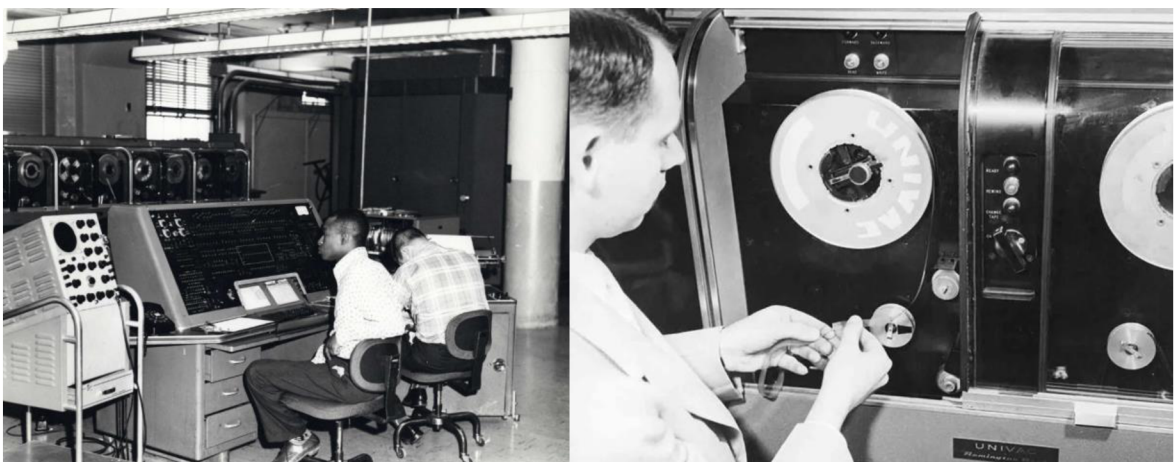
1.2.2. Magnetická páska

Následníkem děrných štítků byly magnetické pásky, které byly vyvinuty v Německu v roce 1928 Fritzem Pfleumerem za účelem nahrávání zvuku. První magnetická páska měla podobu velmi tenkého papíru, který byl pokryt práškovým oxidem železa pomocí laku, později se z papíru přešlo na fólii. Jak naznačuje název, magnetické pásky fungují na principu magnetické energie, konkrétně převádějí elektrické zvukové signály na magnetickou energii. Tyto signály se otisknou na pásku, která se pohybuje po magnetických hlavách, následně magnetické částice pulsy signálu zarovnávají do vzorů, a tím způsobí produkci zvuku, později se stejným způsobem zaznamenávaly bity. Nahrávání záznamu na magnetické pásky muselo být provedeno za ideálních podmínek, jelikož jakékoliv rušení při nahrávání mohlo způsobit poškození dat, jedná se například o silná magnetická pole. Přesnost reprodukce byla závislá na rychlosti, kterou se páska pohybovala, pokud došlo ke změně rychlosti, nastalo zkreslení výšky zvuku. [12]



Obrázek 8 Pfleumer a první magnetická páska [12]

I přesto, že magnetické pásky byly široce používány v rozhlasovém a nahrávacím průmyslu, začaly se používat pro účely zaznamenávání dat až od roku 1951, kdy byl na trh uveden první komerčně vyráběný digitální počítač UNIVAC I (Universal Automatic Computer I), který vyvinul tým inženýrů pod vedením Johna Prespera Eckerta a Johna Mauchlyho. Podíleli se také na vytvoření ENIAC (Electronic Numeric Integrator and Computer), který byl určen pro vojenské využití v laboratořích pro balistický výzkum. Během vývoje se John Mauchly setkal s několika úředníky Úřadu pro sčítání lidu, ohledně možného vývoje obdobného zařízení pro nevojenské účely a po dokončení vývoje EINACU byl tým schopen zajistit potřebné legislativní schválení k vývoji UNIVACU I pro účely sčítání lidu. Na rozdíl od svého předchůdce UNIVAC používal magnetické pásky jako primární vstupní a výstupní zařízení pro ukládání dat a programů. V této době však bylo stále standardem používat děrné štítky, což zpočátku způsobovalo malé množství prodejů, jelikož společnosti na nich uchovávaly velké množství dat. Aby byl přechod na novou technologii snesitelnější, byla k UNIVACU vytvořena dodatečná zařízení, která nejen, že uměla zpracovávat data z děrných štítků, ale také je převádět na magnetické pásky. [13, 14]



Obrázek 9 UNIVAC I [13]

Obrázek 10 Magnetická páska pro UNIVAC I [15]

Magnetické pásky byly obrovským průlomem v oblasti ukládání dat. S neustále rostoucím objemem dat byly magnetické pásky ideální volbou pro dlouhodobé zálohování a archivaci dat, první magnetické pásky měly přibližně 1,1 MB, což bylo značným vylepšením oproti 120 bajtům na děrných štítcích, jejich skladování bylo také méně náročné. Jednou z velkých nevýhod byla rychlost, nejen při zaznamenávání dat, ale také při přístupu k nim. Data jsou stále i v dnešní době na páskách zaznamenána

sekvenčně, není možné si najít přesný bod, který potřebujeme, je potřeba data procházet postupně, což značně ztěžuje také aktualizaci dat. Právě tato omezení vedla k vyvinutí pevných disků, které magnetické pásky nahradily. Na rozdíl od děrných štítků, které jsou dnes už jen vzpomínkou, magnetické pásky mají stále své využití i v dnešní době. Jsou používány zejména pro zálohování a archivaci, jejich velkou výhodou je dlouhá životnost, magnetické pásky mohou vydržet až desítky let. Také jsou méně náchylné na ztrátu dat, na rozdíl od moderních disků, u kterých je hrozbou selhání softwaru. Magnetické pásky jsou také cenově výhodnější, koupě nového úložiště na magnetické páse je mnohem levnější než nákup ekvivalentu na pevném disku. Moderní komerční magnetické pásky mohou obsahovat 15 TB dat, avšak na této technologii se stále pracuje, v roce 2020 IBM a Fujifilm představily magnetickou pásku s kapacitou úložiště 580 TB. [15, 16, 17]

1.2.3. HDD | Pevný disk

Magnetické pásky byly obrovským průlomem ve světě výpočetní techniky. V roce 1953, pouhé dva roky po zavedení magnetických pásek, se však objevila potřeba technologie, která je schopna nejen uchovávat velké množství dat, ale také umožňuje rychlý přístup ke konkrétním datům, proto byl v roce 1956 vyvinut první komerční pevný disk IBM 350. Vývoj vedl Reynold Johnson pod záštitou firmy IBM, tento disk byl součástí sálového počítače RAMAC (Random Access Method of Accounting And Control), který byl uveden na trh o rok později. Pevný disk pro RAMAC se skládal z 50 jednotlivých disků a pro provoz vyžadoval celou místnost, jeho kapacita byla necelých 5 MB. [18, 19]



Obrázek 11 RAMAC [19]

Od roku 1960 se požadavky na kapacitu úložiště začaly značně zvyšovat, každá jednotka RAMACu vážila přes tunu a musela být transportována pomocí vysokozdvihných vozíků, proto bylo nezbytné, aby se pevné disky začaly zmenšovat. V roce 1962 IBM představilo 1316 Disk Pack. Každá z těchto jednotek se mohla umístit do čtecích zařízení. Každá jednotka vážila cca 4,5 kg s kapacitou přibližně 2 MB, ale její hlavní výhodou bylo, že se daly měnit, tím pádem se jednalo o první externí pevné disky. Začátkem 70. let se objevilo nové využití počítačů, tentokrát ne pro vědecké či podnikatelské účely, ale pro osobní využití. Tyto nově vzniklé počítače zpočátku používaly zejména diskety, jinak floppy disky, které však brzy IBM opět nahradila pevnými disky, při uvedení prvního osobního počítače s pevným diskem na trh. Koncem 80. let se cena pevných disků snížila natolik, že se staly standardním komponentem osobních počítačů. [20, 21]



Obrázek 12 HDD [22]

Stejně jako magnetické pásky, tak i pevné disky používají magnetické prvky, konkrétně disky, které se nazývají plotny, mají magnetický povrch, který na sobě ukládá data v podobě magnetických vzorů. Samotné disky jsou zpravidla z tvrdých materiálů, jako jsou sklo, keramika nebo hliník. Tento disk se otáčí na ose a od středu až po okraj se nad ním pohybuje čtecí a zapisovací hlava, která je schopna zmagnetizovat pomocí elektrického proudu konkrétní místa. Díky magnetizaci jsou data uložena i po vypnutí proudu, proto se na pevné disky instalují zejména operační systémy. Plotna je rozdělena na miliardy malých oblastí, každá z těchto oblastí může být individuálně zmagnetizována, aby uchovala hodnotu 1, nebo demagnetizována pro hodnotu 0. Aby v datech nebyl zmatek, bity jsou ukládány v uspořádaných kruhových drahách, kterým se říká stopy, každá z těchto stop je dále rozdělena na sektory. Pevný disk si v jedné části

uchovává mapu sektorů, která obsahuje informace o tom, které sektory jsou již používány, a které jsou stále volné, tato mapa se u každého operačního systému nazývá jinak, Windows používá NTFS (New Technology File System), Mac má APFS (Apple File System) a Linux může používat různé variace FAT (File Allocation Table), které nazývají VFAT (Variant of FAT). Zápis dat se odvíjí od této mapy, když počítač zapisuje nová, či přepisuje stará data, podívá se na mapu a pošle pokyn zapisovací hlavě, která se následně přesune na zadané místo a zapíše data, tato akce probíhá stejným způsobem pro čtení dat, pouze obráceně. [5, 23, 24]

V současnosti jsou pevné disky stále standardním vybavením osobních počítačů, pro velké množství uživatelů jsou ideálním prostředkem pro dlouhodobé uchovávání dat. Mnoho počítačových sestav začíná používat spolu s pevnými disky také SSD disky, avšak kvůli specializaci každého disku na jinou oblast je nepravděpodobné, že by v blízké době SSD kompletně nahradily tradiční pevné disky.

1.2.4. Floppy disk | Disketa

Diskety byly typem diskového úložiště, jednalo se o tenký pružný disk z plastu, který byl pokryt oxidem železa z obou stran. Jelikož diskety byly náchylné na poškození prachem, byly uzavřeny v hranatém plastovém pouzdru podšitým látkou, která odstraňovala prach při točení disku na ose. Diskety byly v mnoha ohledech podobné HDD, data na disketě byla zaznamenána pomocí stop, které měly kruhový vzor a které se dále dělily na sektory. Těsně nad diskem se také pohybovala čtecí a zapisovací hlava. Čtecí otvor byl chráněn pohyblivou krytkou a uvnitř samotného krytu byla také papírová vložka. [25, 26]



Obrázek 14 Disketa [26]



Obrázek 13 První disketa Minnow [27]

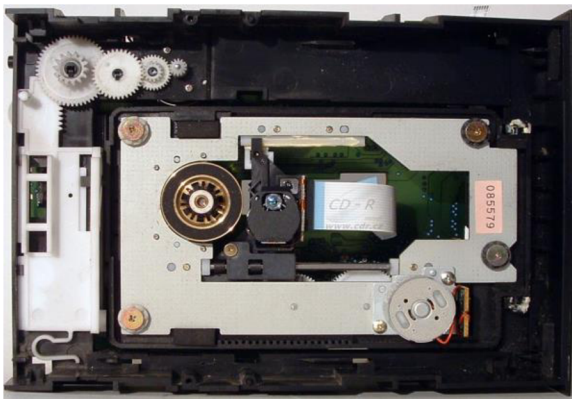
Diskety byly vynalezeny v roce 1967 v IBM laboratoři malým týmem s Davidem L. Noblem ve vedení. Jejich cílem bylo vyvinout levný a spolehlivý způsob, jak zadávat nové instrukce a instalovat softwarové aktualizace do sálových počítačů, které již v této době používaly pevné disky. Do tohoto momentu se pro vstup dat a softwarového programování používaly děrné štítky. V roce 1971 byla představena 80 kB disketa 23 FD, které se přezdívalo Minnow a měla nástroje pouze pro čtení, avšak byla schopna nahradit až 3 000 děrných štítků, v roce 1983 IBM představil novou generaci disket, které měly až 1,44 MB. Spolu s příchodem disket také vzrostla popularita osobních počítačů, které používaly diskety jako úložiště až do pozdních 80. let. Největší přínos však tyto nosiče neměly jako úložiště pro osobní počítače, ale jako způsob, jak distribuovat software. Doposud si veškeré programy na osobních počítačích musel navrhnout uživatel sám, diskety umožnily stvoření softwarového průmyslu a sdílení programů. Diskety dále umožnily snadný přenos dat, tím pádem uživatelé nebyli závislí pouze na jednom konkrétním počítači. Dominovaly na softwarovém trhu až do 90. let, od roku 2000 začaly být postupně nahrazovány CD a USB flash disky. Stopy disket v oblasti IT můžeme vidět dodnes, aplikace Total commander používá disketu jako svou ikonu, a mnoho produktů, jako jsou například Microsoft Office, je dodnes stále používá jako symbol pro uložení dat. [23, 26, 27]

1.2.5. CD | Kompaktní disk

Počátky CD, jinak kompaktních disků, můžeme najít již v roce 1966, kdy James Rusell chtěl nahradit gramofonové desky novou technologií, a nechal si vydat patent na zařízení, které kombinovalo lasery, digitální nahrávky a optické disky. Tento patent později Sony a Philips odkoupili a v roce 1979 představily výsledek své spolupráce – Digitální audio kompaktní disk, který byl o 3 roky později uveden do prodeje. CD mělo úložiště přibližně 700 MB, což posluchačům poskytlo necelých 80 minut audio nahrávek, kterým se postupem času začalo říkat audio soubory, což s sebou neslo úvahu, že by se na CD daly nahrát další typy souborů, a brzy vznikly další verze, které se řídily podle Rainbow books, což byla sbírka standardů pro každou verzi kompaktních disků. V rámci datových úložišť je však nejdůležitější verzí CD-ROM (Compact Disk Read Only Memory), CD-R (Compact Disk Recordable) a CD-RW (Compact Disk ReWritable). CD-ROM byl vydán v roce 1985 pod Yellow Book standardem a fungoval jako optické datové úložiště, které bylo hlavně používané pro distribuci software a

video her. Aby uživatelé byli schopni zaznamenávat svá vlastní data, byly v roce 1992 vytvořeny CD-R disky podle Yellow Book standardu, tyto disky umožňovaly takzvané „vypalování“, což mělo nevýhodu, že vypálená data byla již permanentní, bez možnosti přepisu. CD-RW vyšel v roce 1997 v rámci Orange Book standardu a uživatelům poskytl možnost data nahrávat a následně i mazat. V této době již přichází na trh DVD s daleko větším úložištěm. [23, 29, 30]

Jak naznačuje název, CD je tenký disk, vyrobený z polykarbonátového plastu, který je



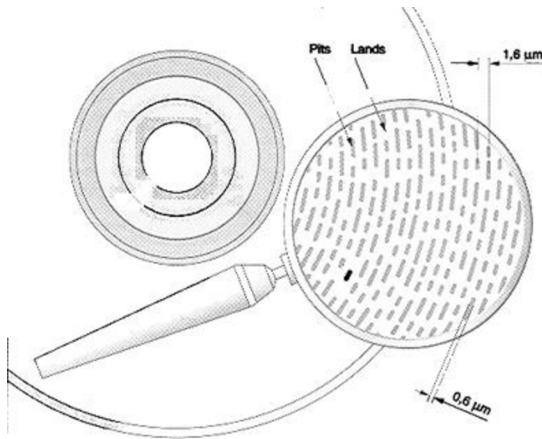
Obrázek 15 Mechanická čtečka disků [31]



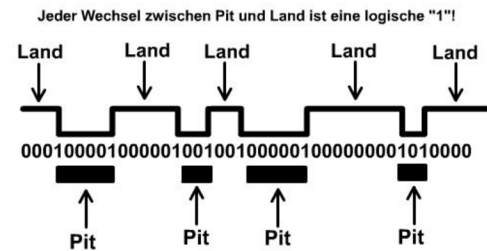
Obrázek 16 Kompaktní disk [32]

pokryt tenkou vrstvou hliníku. Pro nepřepisovatelné disky se do této vrstvy vtisknou mikroskopické hrbolky, které jsou uspořádány do jedné nepřetržité spirály dat. Těmto jamkám se říká „pits“ a místa mezi nimi jsou „lands.“ Pro čtení disku se používá polovodičový infračervený laser, který se zaměří na jednu stopu disku, při otáčení disku tento laser měří rozdíly v tom, jak se světlo odráží od jednotlivých pitů a landů. Avšak to neznamená, že pit značí 1 a land 0. Binární hodnoty jsou zaznamenány jako změna mezi pitem a landem. Změna značí 1, a pokud k žádné změně nedojde, znamená to 0. Aby na disky mohli ukládat data uživatelé, vznikla nová metoda zapisování, která používala fotocitlivé barvivo. Principem bylo, že se na disk vtiskla prázdná spirála, na kterou se nanoslo barvivo, až poté byla na disk přidána hliníková vrstva. Na takto vyrobeném disku se pomocí zapisovacího laseru měnila barva na spirále, čímž se vytvořil trvalý vzor, tento proces je známý jako vypalování CD. Problémem bylo, že barva měla životnost přibližně 5 let, poté začala blednout, což vedlo ke ztrátě a poškození dat. S příchodem CD-RW přišla další inovace, která umožnila data nejen na disk zapisovat, ale také mazat. Místo barviva se začala používat kovová slitina, tuto

slitinu laser zahřál, čímž změnil její odrazivost. V tomto případě jsou 1 a 0 zaznamenány jako odrazlivé a neodrazlivé oblasti. [32, 33]



Obrázek 18 Schéma datové vrstvy CD [34]

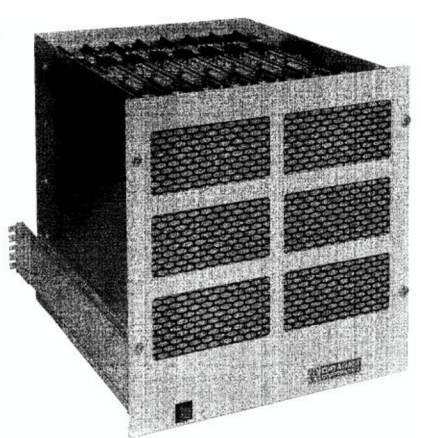


Obrázek 17 Schéma zapisování binárních hodnot [34]

CD disk se stal velmi úspěšným, brzy po vydání se stal standardem pro distribuci hudby a netrvalo dlouho a ve všech ohledech nahradil diskety. CD byl standardem až do roku 2007, avšak již v 90. letech začal být postupně nahrazován DVD (Digital Video Disc | Digital Versatile Disc), který používá laser s kratší vlnovou délkou, díky tomu se na disk dá umístit větší hustota dat. Průměrný DVD má 4,7 GB, později přišly dvouvrstvé DVD, které měly až 8,5 GB. CD bylo zcela nahrazeno Blu-ray diskem v roce 2008. Změna spočívala v použití jiného laseru, v tomto případě modrého, který je až dvakrát menší než červený laser u DVD. Díky větší hustotě dat má jedna vrstva Blu-ray disku až 25 GB úložiště, je možné použít až 4 vrstvy zároveň, což uživateli poskytne 128 GB. V současné době klesá obliba optických disků, nové notebooky a počítače často již nemají mechaniku pro jejich čtení, z velké části jsou nahrazeny USB flash disky, co se týče sdílení a zálohování dat. Blu-ray disky jsou stále populární volbou pro distribuci filmů a video her, pro distribuci fyzických kopií hudby se stále používají CD. [35]

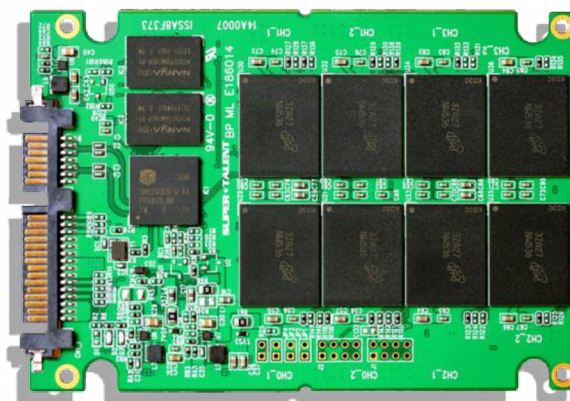
1.2.6. SSD | Polovodičový disk

První pokusy o vytvoření SSD disků začaly v 70. letech, v této době polovodičová technologie byla stále ve svých prvních stádiích a tyto první disky byly příliš drahé pro běžné užití, byly instalovány pouze do superpočítačů. Jako první SSD disk v historii se uvádí Bulk Core, vyrobený firmou Dataram v roce 1976. Tento disk poskytoval 2 MB paměti a údajně nabízel rychlost až 10 000krát vyšší než pevné disky ve své době i přesto, že místo dnešní polovodičové paměti používal jádrovou, a hlavně bez jakýchkoliv pohyblivých částí. Další velký průlom nastal v roce 1980, kdy inženýr Fujio Masuoka vynalezl nový druh paměti „flash“, která byla v roce 1987 součástí prvního komerčního SSD disku svého druhu. Tato paměť byla důležitým krokem vpřed nejen pro SSD disky, ale také pro budoucí USB flash disky. SSD disky se začaly ve větším měřítku rozšiřovat v 90. letech, kdy na trh vstoupil SanDisk se svým 20 MB SSD diskem, v této době se SSD disky používaly hlavně u velkých serverových aplikací. Běžným komponentem se staly až v roce 2006, kdy Samsung představil první SSD disk pro spotřebitelský trh, který byl určen jako náhrada za pevné disky v notebookech. Díky jeho kompaktní velikosti notebooky mohly značně zredukovat svou velikost bez obětování výkonnosti. V dnešní době jsou SSD disky standardním vybavením notebooků a počítačů a je velký předpoklad, že během pár let by SSD mohly zcela nahradit pevné disky. Jejich průměrná paměť je 250-500 GB, jsou běžně používány i disky s například 2 TB úložišti. Největší dostupné komerční SSD disky mají až 15 TB. [36, 37]



Obrázek 19 První SSD disk Bulk Core [37]

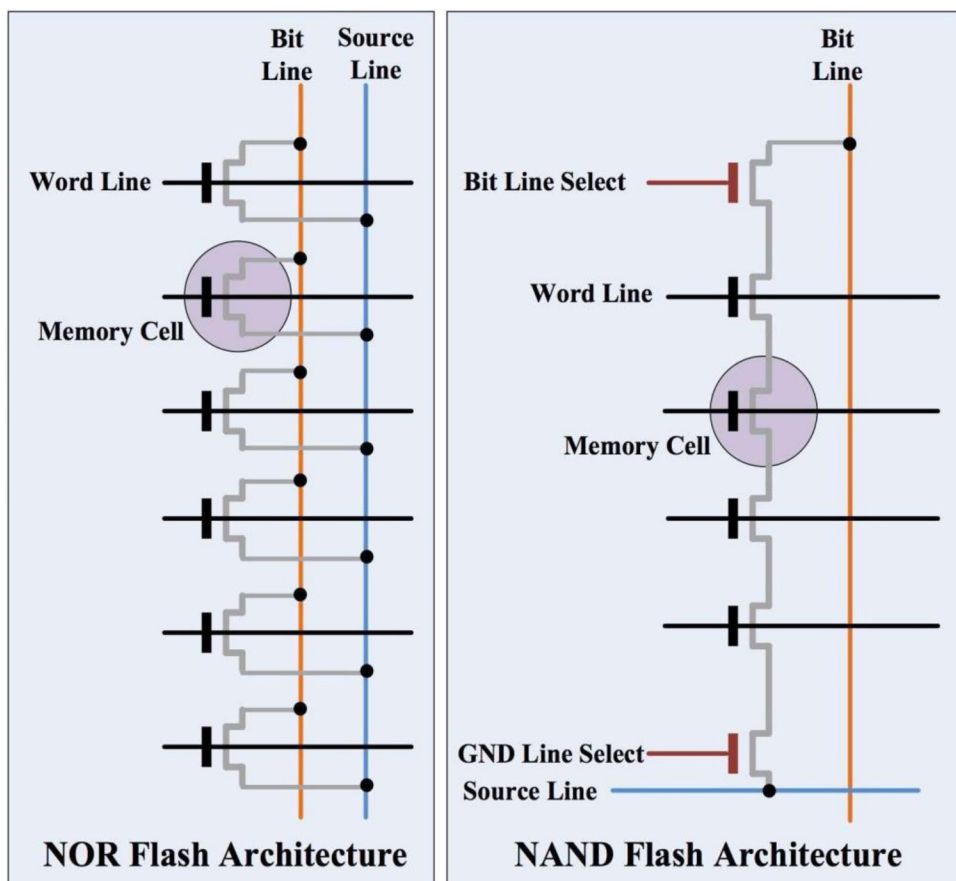
Zkratka SSD vychází z anglického názvu Solid-state drive, z čehož vyplývá, že nemají žádné pohyblivé části, což je kontrastem k pevným diskům. SSD nepoužívají žádné fyzické disky, ale veškerá data jsou uložena pomocí flash paměti. Podobně jako mechanická paměťová média, SSD disky svá data mají také uspořádané v daném schématu, a tím jsou programovatelné bloky, které se skládají z několika paměťových buněk. Pro zapisování dat do bloků se používá elektrický obvod. Proud protéká tranzistorem, který funguje jako vypínač – pokud transistor povolí průtok proudu, data se uloží jako 1, pokud se toku zabráňuje, ukládají se jako 0. Stejným způsobem funguje i paměť RAM, avšak ta po vypnutí zdroje vymaže všechna uložená data. Aby došlo k jejich trvalému uložení, má každá buňka flash-paměti floating gate, který data uchovává i po vypnutí proudu. Rozeznáváme dva základní typy flash-paměti, NOR a NAND. [23, 38]



Obrázek 20 SSD disk [39]

NOR je optimalizovaný pro rychlé hledání dat v libovolném pořadí. Tato vlastnost je zajištěna horizontálním rozmístěním buněk, každá buňka má jeden konec zapojený ke zdrojové lince a druhý k bitové lince. Tento typ paměti poskytuje zvýšenou bezpečnost dat a obvykle se používá pro čtení a provádění kódu. NOR je také schopen data číst na úrovni bajtů. Nevýhodou NOR paměti je, že si musí pamatovat pozici každé individuální buňky, což má za následek, že musí mít komplexní obvody. Z toho důvodu je velikost paměti často omezená a zapisování nových hodnot je zpravidla pomalejší než u NAND paměti, která je optimalizována pro ukládání velké hustoty dat na úkor rychlého přístupu. Buňky NAND jsou zapojeny v sérii, kde jsou propojeny samy na sebe. To znamená, že jsou obvody jednodušší, ale přístup k datům je možný pouze v blocích a sekvenci, což je důvodem pomalejšího čtení dat. [40]

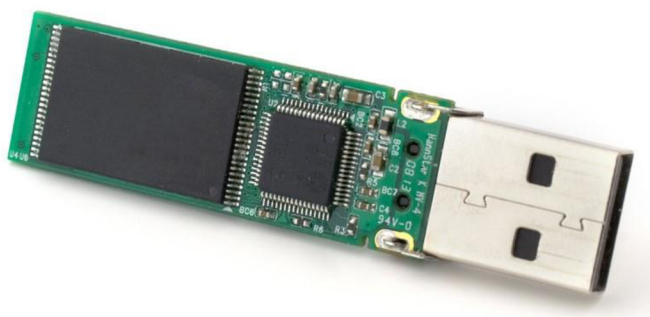
Paměť NAND je z velké části preferována před NOR, díky své velké hustotě dat, rychlému zápisu a nižší spotřebě energie. Velkou výhodou typu NOR je jeho spolehlivost. NAND je náchylnější na bit-flipping, což může být jednak náhodná chyba, ale také cílený kybernetický útok. Principem bit-flippingu je, že se hodnoty bitů změní na opačné, tím dojde k poškození dat. Další nevýhodou NAND je vyšší výskyt vadných bloků, které jsou často přítomny již při výrobě. Posledním bodem je životnost dat, NOR může dosáhnout až 20 let životnosti, zatímco NAND má životnost cca 10 let. Další důležitou součástí SSD disku je controller, který ukládá požadavky do mezipaměti za účelem zlepšení životnosti disku a zrychlení zápisu a čtení. Tato mezipaměť je obzvláště důležitá pro podnikové aplikace a datové servery. [40]



Obrázek 21 Schéma NOR a NAND [40]

1.2.7. USB flash disk

Poslední kapitola v tomto oddílu se zabývá univerzální sériovou sběrnici, které se často přezdívá USB, lidově „fleška“. Informace o původu USB se často liší. Některé zdroje uvádějí, že jejich počátky nastaly již v 80. letech. Popularita USB disků značně vzrostla v polovině 90. let, kdy se řešilo, jak rychle a pohodlně přenášet data mezi různými počítači. Za vynálezce prvního USB disku se nejčastěji uvádějí dvě osoby – Fujio Masuoka, který v 80. letech vytvořil druh paměti flash a Dov Moran, který spolu s Amir Banem a Oronem Ogdanem pracoval pro M-Systems a v roce 1999 podali žádost o patent „Architecture for a Universal Serial Bus-Based PC Flash Disk“. O rok později byl tento patent udělen a ve stejném roce IBM začalo prodávat 8 MB USB disky pod názvem „DiskOnKey“. Odpověď na to, kdo skutečně vynalezl první USB flash disk, asi nenajdeme. Pravdou ovšem zůstává, že popularita těchto malých přenosných zařízení byla i je značná. Dnes, 23 let od prvního vstupu na trh, jsou USB stále oblíbenou levnou alternativou pro zálohování a přenos dat. [41]



Obrázek 22 USB Flash Disk [42]

Jak naznačuje anglický název „Flash disk“, USB používají stejnou flash paměť jako SSD disky, inovace spočívá v jejich malé velikosti a na samotném USB plugu. USB plug prošel několika generacemi, které zpravidla zvyšovaly rychlost přenosu dat. Různé generace USB od sebe můžeme rozpoznat na první pohled podle barvy. První generace USB 1.0 vyšla v roce 1996 a při plné rychlosti dosahovala 12 Mbps, její barva byla bílá. V roce 2000 byla představena verze 2.0, tato generace měla černou barvu a byla 4 000x rychlejší než předchozí s 480 Mbps. Dalším krokem vpřed byla třetí generace 3.0, která má modrou barvu a vyšla v roce 2008. Tato generace nejen, že zvýšila rychlost přenosu na 5 Gbps, ale hlavně měla plně duplexní režim, který umožňuje současně přenášet a přijímat data. Tato generace dostala další 2 verze - 3.1 v roce 2013 a 3.2 v roce 2017, obě tyto verze zvýšily rychlost přenosu o 5 a 10 Gbps. [43]

1.3.Cloud

1.3.1. Historie internetu a cloudu

Cloudové úložiště je služba, která uživatelům umožňuje ukládat a sdílet soubory na virtuálním úložišti poskytovatele. Cloud umožňuje přístup k datům odkudkoliv a kdykoliv, a je tudíž velmi populární pro týmovou spolupráci. Mnoho lidí se domnívá, že cloudová úložiště jsou záležitostí 21. století, počátky cloudu můžeme najít již v 60. letech 20. století.

Historie cloudu je úzce spjata s vývojem internetu, jelikož původním účelem internetu bylo vytvořit způsob pro sdílení informací mezi vládními vědeckými pracovníky. V roce 1963 DARPA (Defence Advanced Research Projects Agency), což je vládní agentura amerického Ministerstva obrany, financovala univerzitu MIT s úkolem uskutečnění projektu MAC. Cílem projektu bylo zpřístupnit programy z jednoho počítače několika uživatelům z různých míst, tento projekt se stal základem moderních počítačových sítí a následně také základem pro cloud. V roce 1969 byl spuštěn ARPANET – počítačová síť, která propojovala 4 americké univerzity: University of California Los Angeles, Stanford Central Research Institute, University of California Santa Barbara a University of Utah. Vývoj ARPANETu v následujících 20 letech zaznamenal raketový vzestup. Nejen, že se k této síti připojovalo stále více uživatelů, ale také díky ní vznikly virtuální stroje, vzdálené přihlášení, přenos souborů a e-mail. Na základě struktury ARPANETu byl vytvořen internet, který byl spuštěn 1. ledna 1983, ARPANET byl aktivní dalších 7 let až do roku 1990, kdy byl oficiálně vypnut. [44]

Internet, jak ho známe dnes, byl veřejnosti zpřístupněn v 90. letech a netrvalo dlouho a zprovoznily se první služby využívající cloudových prvků. První komerční program pro vzdálené sdílení dat byl spuštěn v roce 1994 americkou telekomunikační firmou AT&T. Nesl název PersonaLink Services a zprostředkoval vzdálenou komunikaci a také uživatelům umožnil ukládat své soubory online. Dalším významným programem byl Salesforce v roce 1999. Salesforce na rozdíl od PersonaLink byl webovou službou a nevyžadoval instalaci dedikovaného programu, a právě tento program z velké části ovlivnil cloudové služby, jak je známe dnes. [44]

První moderní cloudová úložiště začala vznikat od roku 2006, kdy Amazon představil svůj Amazon Web Services, který společně poskytoval možnost své pracovní stanice propojit pomocí internetu a virtualizace. Brzy začaly své služby poskytovat další společnosti, jako např. OneDrive firmy Microsoft v roce 2007 a Dropbox v roce 2008, který používá AWS jako poskytovatele úložiště. V roce 2011 byl spuštěn iCloud od Apple a o rok později byl zprovozněn Google Drive. [45]

1.3.2. Cloudová architektura

V předcházející kapitole bylo zmíněno, že cloudové úložiště je způsob ukládání dat, který spočívá v tom, že jsou data pomocí internetu uložena na virtuálním stroji, ten je nainstalován na vzdáleném fyzickém serveru, který zpravidla zpracovává poskytovatel třetí strany. Cloud je úzce spojen s internetem, který pouze zpracovává požadavky a poskytuje odpovědi, cloud navíc také spouští programy a ukládá data.

Rozlišujeme čtyři hlavní typy cloudových úložišť dle poskytovatele

- Soukromý cloud
- Veřejný cloud
- Hybridní cloud
- Multicloud

Princip soukromého cloudu spočívá v tom, že veškeré hardwarové a softwarové zdroje jsou určeny a zpřístupněny pouze jedné konkrétní organizaci. Tento typ využívají zejména státní a finanční instituce nebo velké firmy, které si celou cloudovou infrastrukturu buď vybudují samy, nebo si ji nechají sestavit na zakázku. Soukromé cloudy jsou zpravidla provozovány na lokálních datových centrech zákazníka. Výhodou je, že se infrastruktura úložiště dá sestavit přesně dle specifikací zákazníka, což s sebou nese vysokou míru flexibility. Druhou velkou výhodou je bezpečnost, jelikož veškerá data jsou pod správou samotné organizace. Je zde sníženo riziko odcizení citlivých dat a důvěrných dokumentů. Soukromý cloud také umožňuje společně splňovat předpisy jejich dané země. Evropské společnosti jsou povinny dodržovat směrnice GDPR, pokud však používají cloudové služby od amerických dodavatelů, může dojít k porušení těchto předpisů, v důsledku rozdílných nároků na zacházení s daty. Jsou zde však také nevýhody. Soukromé cloudy si zpravidla spravují organizace samy, což znamená, že

část svých zdrojů musí věnovat údržbě, aktualizaci, pořízení vlastního hardwaru a vytvoření vlastního softwaru. Vytvoření toho cloudu je také časově náročné a je zde riziko, že bude ve výsledku dražší a méně stabilní než alternativy dostupné od společností, které se soustředí na poskytování těchto služeb. Tento typ cloudu má vysokou vstupní cenu a je pro mnohé z firem nedostupným řešením. [45]

Veřejný cloud je pro většinu uživatelů tím nejznámějším. Tento typ úložiště poskytuje své služby široké veřejnosti, firmám a dalším uživatelům zdarma v případě malého objemu dat, v opačném případě je nutné za službu zaplatit. Veškerá odpovědnost spojená s údržbou a hostingem spadá na poskytovatele, který musí mimo jiné také zajistit rychlý přístup k datům. Veřejné cloudy své služby dělí mezi několik uživatelů zároveň, kteří společně užívají fyzické zdroje poskytovatele. Aby nedocházelo k překrývání mezi uživateli, každému je přiděleno jedno samoobslužné rozhraní, které je logicky odděleno od ostatních. Výhodou veřejného cloudu je nízká vstupní cena, kterou si mohou firmy evidovat jako daňově uznatelný náklad. Uživatelé se nemusejí starat o údržbu, jelikož veškerá odpovědnost je na straně poskytovatele. To však s sebou přináší i specifická rizika. Prvním je závislost na internetovém připojení. Výpadek anebo oprava na obou stranách vede k dočasnému pozastavení služeb, které mohou bránit běžnému provozu. V potaz musí být brána také bezpečnost. V dnešní době jsou cloudová úložiště dobře zabezpečena proti kyberútokům, bohužel žádná data s internetovým přístupem nejsou 100 % v bezpečí. Dalším potenciálním problémem je, že samotný poskytovatel může mít k datům přístup. Běžnou praxí zůstává, že jsou stejná data ukládána na několika různých serverech, což může způsobit nesoulad v předpisech, pokud se jedná o zákonem regulovaná data. Tento typ cloudu je využíván zejména jedinci a malými až středně velkými firmami. Současnými největšími poskytovateli veřejných cloudů jsou Amazon, Google, IBM a Microsoft. [45]

Hybridní cloud kombinuje služby veřejných a soukromých cloudů. Hybridní architektura využívá část hardwarové vybavy soukromé firmy. Tato vymezená část se transformuje na infrastrukturu pro provoz soukromého cloudu. Nově vytvořená infrastruktura je následně napojena na prostředí veřejného cloudu. Tento přístup často vede k lepší optimalizaci zdrojů a nákladů. Také pomáhá odstranit problémy spojené s regulací veřejných cloudů, jelikož si firma důvěrná data ukládá na svém vlastním

cloudu, zatímco výrobní data mohou využívat služby veřejného cloudu. Hybridní cloudy jsou dnes čím dál oblíbenější. [45]

Posledním z uvedených úložišť je multicloud. Multicloud využívá několik různých veřejných cloudových úložišť ve stejnou dobu a na rozdíl od hybridních cloudů nemá svou vlastní soukromou architekturu. Hlavní výhodou multicloudu je redundance. V případě výpadku jednoho z cloudů je organizace chráněna před pozastavením svého provozu, což je také výhodné, pokud jsou data v procesu migrace z jednoho cloudového úložiště na nové při změně poskytovatele. Multicloud má komplexní strukturu. Každý poskytovatel má své vlastní procesy a různé podmínky a při velkém množství jednotlivých úložišť se správa stává obtížnou. Komplexnost může mít také vliv na výkon úložišť. Je nutné jednotlivé cloudy mezi sebou vhodně propojit, aby se omezila zpožděná odezva a zajistila maximální spolehlivost. S větším počtem úložišť také roste náchylnost pro kybernetické útoky. V praxi se multicloud často používá v hybridní podobě. [45]

1.4. Implementace datových úložišť

1.4.1. Identifikace potřeb

Pro správnou implementaci datových úložišť je potřeba provést analýzu potřeb a dostupných zdrojů. Na základě této analýzy se vytvoří plán, který zahrnuje veškeré informace pro samotné zavedení úložiště a následnou údržbu a správu.

Jako první je potřeba identifikovat, jaké druhy dat společnost ukládá, jejich hodnotu a důležitost. Firemní data jsou souhrnné informace, popisující nejen samotnou firmu, ale také její procesy. Firmy sbírají velké množství dat, např. o svých zákaznících. Tento druh dat obsahuje zejména jejich osobní data spolu s nákupními zvyky, na základě těchto informací se mohou vytvořit zákaznické skupiny. Data o zaměstnancích spolu s osobními údaji obsahují informace o pracovním výkonu. Analytická data mohou být různá, jelikož se odvíjejí od předmětu podnikání a podnikatelských procesů. Pro společnosti, které provozují e-shop, mohou být těmito daty návštěvnost webu a SEO. Hlavním účelem analytických dat je poskytnout podklady pro zlepšení firemních procesů. Z toho důvodu jdou často analytická a marketingová data ruku v ruce, jelikož na základě analytických dat se dají získat data marketingová, která zahrnují informace například o konkurenci, trhu, na kterém se firma pohybuje a efektivnosti reklam. Dalšími typy jsou data o účetnictví, zásobách, obchodních partnerech a produktech. Zvláštním případem jsou produkční data, která jsou potřebná pro fungování firemních procesů. Každý druh dat má jinou funkci a také jiné nároky na ukládání. Jednotlivé typy dat můžeme rozdělit na hot, warm a cold data, na základě tohoto rozlišení se rozhoduje, jak budou skladována, což vede k druhému bodu, a tím je umístění úložiště.

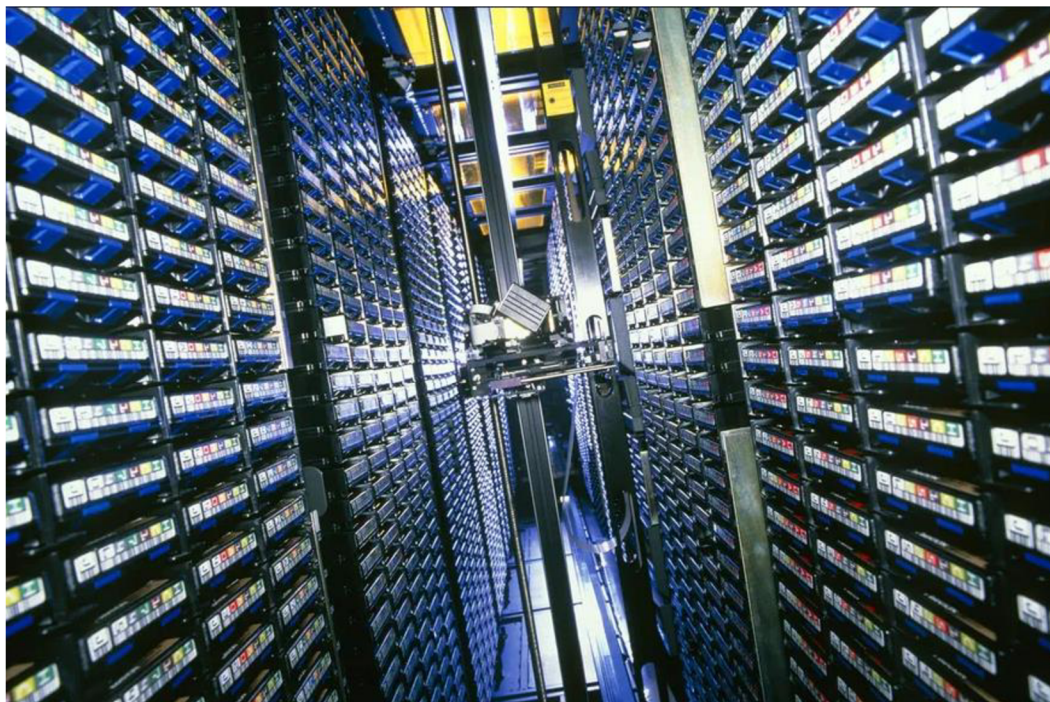
Kolik fyzického místa datové úložiště zabere, se může značně lišit. Některá úložiště jsou součástí vybavení, jako jsou SSD a HDD disky, jsou však způsoby skladování, které vyžadují dedikované místnosti, konkrétně servery a magnetické pásky. Hlavním rozhodovacím faktorem, mimo finance a dostupné prostory, je druh dat, který byl uveden výše jako hot, warm a cold data. Za hot data označujeme data, která musí být vždy rychle a spolehlivě dostupná, jedná se například o produkční data. Hot data jsou zpravidla nainstalována na úložištích, které jsou buď přímo komponentem počítače, jako jsou lokální HDD a SSD disky. Existují také hot cloud storage služby, které

nabízejí rychlejší odezvu než klasická cloudová úložiště, běžnou praxí je pro tyto cloudové služby ukládání kopií na lokální disk, aby v případě výpadku byl k datům stále přístup. Právým opakem jsou cold data, která mají archivní charakter. Tato data jsou používána zřídka a nevyžadují rychlý přístup, jsou ukládána na pomalých médiích, jako jsou externí pevné disky a magnetické pásky, existují už také cloudové alternativy. Cold storage má často podobu místnosti, která je určena pouze pro účel skladování fyzických médií. Zde mohou být uloženy pevné disky, a to na serveru, nebo volně v regálech. Jelikož se jedná o fyzická média, tyto místnosti, kterým se někdy přezdívá serverovny, by měly dodržovat řadu podmínek, aby nedošlo k předčasnému poškození zařízení. Jak naznačuje samotný název „cold storage“, skladovací místnost by měla být chladná, mezi 15-20 °C, s přibližnou vlhkostí 40-50 %. Dále by místnost měla být dobře odvětraná s co nejmenším množstvím prachu, tato podmínka je velmi důležitá pro skladování magnetických pásek, které jsou citlivé na fyzické poškození. Tato úložná média by měla být skladována ve vertikální poloze, s minimem slunečního svitu. Posledním datovým typem jsou warm data, která v běžném provozu firmy používají jen zřídka, ale na druhou stranu se pravidelně aktualizují. Jedná se například o analytická a zákaznická data. Tato data se často ukládají na lokálních HDD discích a cloudových úložištích, což znamená, že mají podobné nároky na skladování jako hot data. [46, 47]

Pro úspěšnou implementaci datových úložišť je klíčové vytvořit tým, který odpovídá za uskutečnění a údržbu. Tento tým by měl být ideálně samostatnou jednotkou, která ve firmě nezastává jiné funkce. Nedoporučuje se, obzvláště ve velkých firmách, aby například správce sítě byl zároveň správcem datových úložišť. Důvodem není pouze větší pracovní zátěž, ale je zde riziko, že zaměstnanci, kteří již mají jinou funkci, by mohli využít své pozice jako správce k usnadnění přístupu, například, že jejich zařízení nepotřebují hesla, což může vést ke vzniku bezpečnostního incidentu.

1.4.2. Datová bezpečnost

Data jsou cenným majetkem firem, což znamená, že jsou velkým lákadlem pro kybernetické útoky. Počet útoků prudce roste, spolu se zvyšující se mírou digitalizace, z tohoto důvodu je obzvlášť důležité dbát na zabezpečení dat. Integrity360, což je jedna z



Obrázek 23 Cold Storage magnetických pásek [15]

největších firem specializujících se na kybernetickou bezpečnost, uvedla, že počet kybernetických útoků v roce 2022 vzrostl o 424 % oproti roku 2021, z čehož 43 % incidentů vzešlo z firem samotných, ať už úmyslně, nebo neúmyslně. [48]

K zabezpečení se přistupuje podle úrovně důvěrnosti, tyto úrovně jsou: veřejné, vnitřní, důvěrné a vysoce důvěrné. Veřejná data jsou například volné pracovní pozice, novinky a události. Interní data nejsou veřejně dostupná, jejich prolomení by mělo malé následky, jedná se například o příručky pro zaměstnance nebo dokumenty týkající se firemní politiky. Důvěrná data jsou určena pouze pro specifikované skupiny uživatelů, jako jsou například marketingové materiály, kontaktní informace a finanční záznamy. Vysoce důvěrná data jsou přístupná pouze malému počtu jednotlivců, může se jednat o nezveřejněná data o výzkumu. To znamená, že veřejná a interní data mohou být uložena na cloudových úložištích, ale důvěrná a vysoce důvěrná data by měla být ideálně

uložena na offline fyzických úložištích s omezeným přístupem, aby se co nejvíce zabránilo neoprávněnému přístupu.

Základem veškeré ochrany je stanovení zásad bezpečnosti a zaučování zaměstnanců. S pojmem kyberútok si mnoho lidí vybaví malware, ransomware, viry, sql injection a mnoho dalších. Nejběžnější útoky však spoléhají na sociální inženýrství. Dá se říct, že jednou z největších slabin systému jsou hlavně lidské články, čehož si kyberzločinci jsou velice vědomi. Nejčastějšími typy těchto útoků jsou phishing, vishing a smishing. Jedná se o podvodnou techniku, kdy útočník kontaktuje oběť pomocí E-mailu, telefonního hovoru nebo SMS zprávy. Typická phishing kampaň buď spoléhá na impulzivní reakci nebo zvědavost cílového příjemce. Zpráva zpravidla pojednává například o nezaplacené platbě nebo slevových kuponech, pro vyvolání impulzivní reakce se zdůrazňuje, že pokud oběť nebude reagovat okamžitě, bude to mít následky, zpráva následně příjemce navede ke kliknutí na odkaz, který má za cíl buď ukradnout informace pomocí duplikované webové stránky nebo k infikování zařízení. Aby se tomuto riziku předešlo, firmy by měly své zaměstnance proškolit, jak efektivně rozpoznat falešné zprávy a jaké dodržovat standardy bezpečnosti. Nejzákladnějším krokem pro zabezpečení zařízení zaměstnanců a datových úložišť je použití hesel. Existuje mnoho technik, jak hesla prolomit, jednou z nich je brute force attack, který pomocí algoritmu typuje heslo pomocí kombinací, uvádí se, že tyto algoritmy jsou schopny zjistit slovo ze slovníku během jedné sekundy, proto je důležité používat dlouhá a komplexní hesla. Doporučené kroky při vytváření hesel jsou používat velká a malá písmena, čísla a symboly o délce alespoň 8-12 znaků. Hesla by neměla obsahovat žádné informace, které by se daly vyvodit z údajů o uživateli, jako jsou jména či datum narození. Pro vytvoření unikátních a silných hesel dnes existuje mnoho aplikací a služeb, které generují silná hesla a uchovávají je v takzvaném trezoru, ke kterému se uživatelé dostanou pomocí jednoho hlavního hesla nebo biometrických dat. Pro zvýšenou bezpečnost se čím dál více používá dvoufaktorové ověření, které po zadání hesla dále vyžaduje potvrzení ve formě bezpečnostní otázky, kódu nebo potvrzení přihlášení z druhého zařízení.

V poslední době se v mnoha firmách začal používat přístup „Bring your own device“, který spočívá v tom, že zaměstnanci k práci používají svá vlastní zařízení, pomocí kterých se připojují k firemnímu serveru a internetovému připojení. Na první pohled se

tento přístup může zdát výhodný, zaměstnanci jsou se svými vlastními zařízeními lépe seznámeni a společnost může ušetřit na nákladech za hardware, BYOD je však velkým bezpečnostním rizikem. Hlavní hrozbou je, že se zaměstnanci mohou připojit k serveru s potenciálně infikovaným zařízením. Zařízení, která nejsou pod správou společnosti, nemusejí splňovat bezpečnostní standardy, jako jsou pravidelné aktualizace systému, antivirová ochrana, firewallové omezení a šifrování. Tato zařízení mohou být hrozbou i poté, co se uvedou mimo provoz, proto je nutné zajistit, aby se data v nich obsažená nedala znovu obnovit, což platí hlavně pro externí úložiště.

Pro maximální bezpečnost však nestačí pouze zaškolený personál. Mezi základní prvky bezpečnosti patří šifrování dat, díky kterému mohou být nečitelná i v případě, že se dostanou do neoprávněných rukou. Šifrování data zakóduje a aby se stala opět čitelnými, je potřeba poskytnout jeden až dva dešifrovací klíče. Data by měla být zašifrovaná hlavně při přenosu a během dlouhodobého stavu klidu v cold storage. V neposlední řadě je velkou slabinou Wi-Fi připojení. Wi-Fi je jednoduchý způsob, jak na pracovišti šířit internetové připojení, bohužel právě tato jednoduchost s sebou nese také mnoho slabin, které zpravidla plynou ze slabé bezpečnostní konfigurace. Doporučené praktiky pro zabezpečení Wi-Fi signálu jsou zavedení silného hesla, přejmenování sítě, jelikož mnoho routerů má za výchozí jméno název modelu, pravidelné aktualizace, zavedení firewallu a VPN.

1.5.Zálohování dat

1.5.1. Typy záloh

Data jsou velmi cenná a je velice nutné je dobře zabezpečit, jelikož jejich odcizení či znepřístupnění může vážně ovlivnit chod společnosti. V dnešní době je vysoká pravděpodobnost, že se firma stane obětí kybernetického útoku. Nejlepší způsob, jak omezit dopad útoku, je udržování záloh. Ztráta dat však nemusí být pouze následkem útoku, ale také je častou příčinou poškození nebo ztráta hardwaru, chyby v softwaru, mylné zacházení s daty a náhodné zkratky. Zálohování dat pomáhá minimalizovat dopad těchto událostí, pomocí vytváření a ukládání kopií dat, které umožňují v případě ztráty jejich obnovu do naposledy uloženého stavu. Rozlišují se čtyři základní typy zálohování – úplná, rozdílová, inkrementální a zrcadlová. [49, 50]

Úplná záloha je nejstarším typem. Principem je, že se vytvoří 1:1 kopie zvolených dat, může se jednat o jednotlivé soubory nebo o kopii celého disku. Hlavní výhodou je, že díky úplným zálohám jsou data zachována ve své kompletní formě, díky čemuž je následná obnova velmi jednoduchá. Má to však i své nevýhody, nejen, že je tento přístup časově náročný, ale také vyžaduje velké množství dostupných úložišť, i po kompresi dat. Pokud je záloha uložena na fyzickém médiu, je také vystavena riziku poškození, proti kterému se lze chránit vytvořením více než jedné kopie, což přispívá k nárokům na úložiště. [50]

Rozdílová záloha byla vytvořena jako rozšíření zálohy úplné a jejím hlavním účelem je zrychlit vytváření záloh. Po vytvoření úplné zálohy se vytváří pouze kopie souborů, které se od vytvoření zálohy změnily. Tímto způsobem se pokračuje až do další úplné zálohy, která tyto změny zakomponuje. Rozdílový přístup je oproti úplným zálohám mnohem rychlejší, jelikož se ukládá menší počet dat, nevýhodou však je, že se počet uložených dat neustále zvyšuje a dochází ke značné redundanci. [50]

Inkrementální zálohy jsou ve svém fungování podobné rozdílovým datům, také zálohují pouze ta data, která byla změněna od poslední zálohy. Jsou však jiná tím, že jako poslední zálohu nepočítají pouze zálohu úplnou, tento typ je schopen detekovat sám sebe i rozdílové zálohy. Díky tomu je tento přístup rychlejší než rozdílové zálohy a vyžaduje méně místa na úložišti, jelikož nevytváří duplicitní soubory. Tento proces se

provádí do další úplné zálohy a je zpravidla prováděn automaticky pomocí specializovaných programů. [50]

Posledním a nejnovějším typem je zrcadlení. Nejedná se o pravou formu zálohování, které data zpravidla chrání před úplnou ztrátou dat, zrcadlení se používá jako rychlé řešení při náhodném zkratu disku. Na rozdíl od klasických záloh, které se vytvářejí pravidelně v daných časových úsecích, zrcadlení vytváří a synchronizuje kopie dat v reálném čase na jiném úložišti pomocí zrcadlového softwaru. Zrcadlení se používá formou hot swapping, kdy z minuty na minutu přestane fungovat používaný disk, je možné ho ihned vyměnit za disk se zrcadlovou zálohou a vrátit se přesně do bodu, ve kterém došlo k výpadku. V případě klasické zálohy by se nejdříve musela zkopírovat na disk náhradní, což podle objemu dat může trvat déle než 48 hodin, a chyběla by ta nejnovější data. Zrcadlení by se však nemělo považovat za skutečnou zálohu, právě kvůli synchronizaci, jelikož v případě napadení hlavního disku malwarem je okamžitě infikovaná i zrcadlová kopie. Další nevýhodou jsou nároky na úložiště, jelikož podobně jak u úplné zálohy se kopírují data 1:1. Zrcadlový software také může omezit výkonnost počítače, z důsledku dvojitého ukládání. [51]

Při volbě vhodné metody zálohování je potřeba stanovit dvě metriky – RTO a RPO. RTO (Recovery Time Objective) vyjadřuje maximální prodlevu mezi zpřístupněním a obnovou dat, než dojde k závažným následkům kvůli pozastavení firemních procesů. Délka RTO se mezi jednotlivými společnostmi liší, jelikož má na ni vliv několik činitelů zároveň, jako jsou náklady na obnovení dat a možný ušlý zisk v důsledku pozastavení činnosti. Také je třeba mít na paměti, na jakém úložném médiu se záloha nachází, obnova z fyzických médií je zpravidla značně rychlejší než z cloudových úložišť. Mnoho společností neutrpí ztráty, pokud bude muset obětovat pár hodin na obnovu dat, ovšem pokud firma poskytuje například hostovací služby, rapidní obnova je při výpadku klíčová, proto je v těchto případech doporučeno zrcadlení dat. [48]

RPO (Recovery Point Objective) značí, jak dlouhý časový úsek dat, jinak řečeno, jaké množství dat, si může firma dovolit ztratit. Pokud firma zálohuje data každé dva dny, RTO bude mít hodnotu 48 hodin. Hlavním rozhodovacím faktorem je, jak je náročné nebo nákladná ztracená data získat znovu a také kolik nových dat nebude zaznamenáno v důsledku pozastavení chodu. [52]

1.5.2. Zálohovací strategie

Sestavení strategie pro zálohování často spadá na jednoho manažera, který je odpovědný nejen za nastavení zálohovacího systému, ale také za jeho údržbu, testování a bezpečnost. Tato osoba nese i odpovědnost za sestavení plánu obnovy v případě nouze.

Chybou mnohých firem je, že veškerá svá data ukládají na jednom místě, což má za následek jejich zranitelnost. Velmi vhodným způsobem je od sebe zálohy oddělovat podle jejich typu a pro kriticky důležitá data vést více záloh najednou. Spolehlivou strategií pro zálohování dat je takzvaná Strategie 3-2-1: ta spočívá v tom, že nejefektivnější způsob zálohování je vytvoření několika záloh na různých místech a médiích. Číslo 3 znamená, že by měly existovat 3 kopie dat. 2 kopie by měly být v prostorách firmy, ale na různých úložných médiích a 1 kopie na fyzickém úložišti mimo firmu. Mít zálohy poblíž místa dění je pohodlný a rychlý způsob, jak data obnovit v případě nouze. Kopie mimo pracovní prostory zajišťuje zachování dat v případě, že jsou data poškozena kvůli události na pracovišti, jako jsou požáry, zaplavení či jiná fyzická poškození. Strategie 3-2-1 se připisuje fotografovi Petrovi Kroghovi, který tento způsob ukládání dat užíval z důvodu dříve omezené kapacity datových úložišť. [53]

Důležitou složkou pro zavedení zálohového systému je stanovení potřeb organizace, tedy jaká data bude potřeba zálohovat, která jsou nejdůležitější spolu s RTO a RPO metrikami. Na základě těchto požadavků se může zvolit vhodné paměťové médium. Běžnou volbou jsou fyzická média, z kterých jsou na výběr pevné disky, blu-ray disky, USB flash disky a magnetické pásky. Magnetické pásky jsou jedním z nejméně populárních médií pro běžné zálohování dat i přesto, že poskytují velké množství úložiště, mají značnou nevýhodu v oblasti rychlosti a uživatelské přívětivosti, jelikož na rozdíl od externích pevných disků a USB, které lze jednoduše propojit s jakýmkoliv počítačem, magnetické pásky vyžadují speciální zařízení pro zapisování a čtení dat, mají však své využití jako spolehlivé offline úložiště v rámci strategie 3-2-1. Blu-ray a USB flash disky jsou vhodnou volbou pro sekundární zálohy, jejich nevýhodou, obzvlášť pro USB, je jejich relativně malá velikost, což s nezodpovědným zacházením může vést ke ztrátě nebo krádeži, mají však poměrně omezená úložiště, což znamená, že nejsou vhodné pro velké organizace. Pro mnoho firem jsou proto externí pevné disky

ideální volbou jako primární zálohové médium, díky jejich velkému úložišti a všestrannosti. Cloudová úložiště jsou dnes obzvláště populárním prostředkem pro vytváření záloh pro malé i velké firmy, díky jejich snadné přístupnosti a jsou efektivním způsobem, jak ukládat data mimo prostory firmy. Nevýhodou cloudových úložišť je však pomalá obnova dat a bezpečnostní rizika spojená s jeho onlinovým charakterem.

Dalším důležitým aspektem zálohovací strategie je zajištění aktuálnosti dat. Málokterá firma by se chtěla ocitnout v pozici, že ztratí svá data a jejich nejaktuálnější záloha je vytvořena před rokem. Doporučenou prodlevou pro úplné zálohy je 24-48 hodin, a pravidelnými inkrementálními zálohami každých pár hodin v případě, že společnost má velký proud dat, hlavní je však data zálohovat pravidelně. Vytváření záloh je však časově náročné, obzvláště pokud se provádí manuálně. Z toho důvodu je vhodné investovat do softwaru, který může proces automatizovat, případně zálohování outsourcovat externí firmě. Zálohovací softwary jsou často cloudové anebo součástí podnikového informačního systému, jsou však i poskytovatelé, kteří nabízejí backup-as-a-service, což je software specializovaný pouze pro vytváření záloh. Outsourcing externím firmám je cenově výhodný a zákazníkům poskytuje přístup k nejmodernějším metodám zálohování.

1.5.3. Obnova dat

Obnova dat je proces získání dat, která se stala nepřístupnými, jako jsou omylem smazané nebo poškozené soubory. Je mnoho způsobů, jak může dojít k poškození dat, nejčastěji však plynou z lidských chyb. Na poškození dat se však může podílet mnoho externích nebo nepředpokladatelných vlivů, jako jsou malware, nekompatibilní software, chyby v operačním systému a náhodné poškození souborů. Soubory se stávají poškozenými nejčastěji během ukládání, k poškození může dojít, pokud spadne operační systém během ukládání, nebo pokud se na pevném nebo SSD disku vyskytnou vadné sektory, tomuto typu se říká logické chyby. Data uložená na fyzických médiích jsou také vystavena rizikům, jako jsou výpadky elektřiny, elektrické zkraty, selhání hardwaru a různé incidenty, jako jsou povodně nebo požáry. Jedním z nejčastějších důvodů pro poškozená data je také odpojení USB a pevných disků bez vysunutí. Za ideálních podmínek se mohou chybějící data obnovit pomocí záloh, v tomto případě obnova spočívá pouze v kopírování dat ze zálohy zpět na původní místo. Mohou však

nastat situace, kdy je obnova dat možná pouze z poškozených fyzických médií. Jiným případem jsou firmy, které jsou na trhu už desítky let. U těchto firem se dá očekávat, že mají stará data uložená na zastaralých médiích a potřebují k nim přístup. Může se jednat o spojení s jinou společností, která vyžaduje přehled starých dokumentů, změnu archivních místností anebo stará data mohou obsahovat důkazy v případě soudních sporů.

Fyzická úložiště jsou náchylná na vnější poškození. Pevné disky trpí zejména mechanickými poruchami, jako jsou selhání motoru, zhroucení hlavy, což je způsobeno dotykem čtecí a zapisovací hlavy na disku. CD, DVD a Blu-ray disky mohou být poškrábány, nebo v případě CD-R mohlo dojít k vyblednutí barviva. Magnetické pásky jsou náchylné na mnoho různých poškození, jako jsou oxidace, prach, vlhkost, vysoké teploty a silná magnetická pole. Prvním krokem k obnově dat je oprava daného úložiště. Oprava fyzických úložišť je náročná a zpravidla není možná bez pomoci specializovaných firem, ať už se jedná o odstranění nánosů na magnetických páskách nebo leštění disků. Obnova dat probíhá využitím obnovovacích softwarů, které používají různé algoritmy a metody skenování úložišť, zpravidla však platí, že aby bylo možné opravit data, je nejdříve potřeba získat co největší množství informací z metadat, což jsou data poskytující informace o jiných datech. V případě fyzicky poškozených médií často použití softwaru není možné, jelikož by mohlo vést k dalšímu poškození. V těchto případech je nejdříve nutné vytvořit obraz disku, což je replika všech dat, která se na úložišti nacházela. Tato replika se provádí postupným kopírováním jednotlivých sektorů. Nejjednoduššími daty obnovení jsou ztracená a omylem smazaná data. Jak bylo naznačeno v první kapitole, tato data nejsou skutečně odstraněna, dokud nejsou přepsána novými daty. U NTSF jsou smazaná data a jejich adresáře označeny za „nepoužitá“, v tomto případě je program schopen taková data najít pomocí deterministických a heuristických algoritmů a následně obnovit, smazaná data je také možné najít pomocí příkazového řádku. [29, 49, 54]

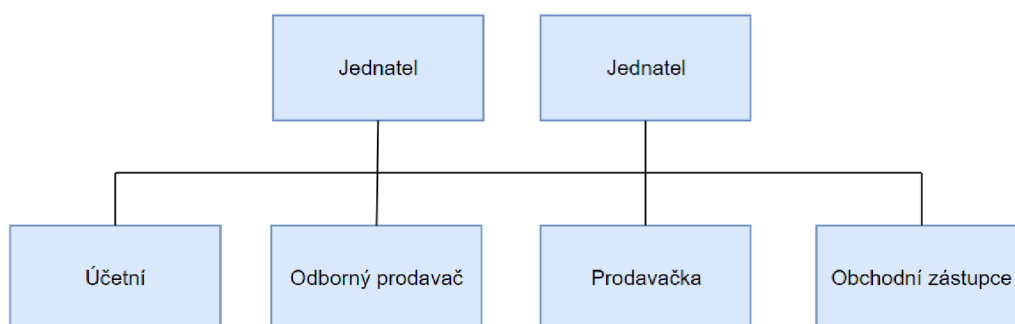
2. Analýza současného stavu

Pro praktickou část své bakalářské práce jsem si zvolila firmu Krako-Welding, s.r.o, kde jsem vykonávala svou praxi. Cílem této části je provést analýzu současného stavu společnosti ohledně zacházení s daty a datovou bezpečností. Výsledkem této analýzy bude zhodnocení kladů a záporů, spolu s vlastním návrhem na řešení nedostatků.

2.1. Informace o společnosti

Jak již bylo zmíněno, subjektem je firma Krako-Welding, s.r.o. Jedná se o rodinnou firmu malého charakteru, která byla založena v roce 1994. Firma se specializuje na prodej, rozvoz a servis svařovací techniky, zejména:

- Svářecí stroje MIG/MAG
- Inventory MMA
- Inventory TIG
- Svařovací materiály
- Svařovací dráty
- Elektory i speciály
- Regulační a autogenní techniku
- Nářadí
- Brusivo
- Ochranné a pracovní pomůcky



Obrázek 24 Organizační struktura společnosti [Vlastní zpracování]

Firma má sídliště v Novém Malíně s pobočkami v Bruntále a Jeseníku. S ohledem na velikost firmy je její struktura jednoduchá. Společnost má dva jednatele, z nichž jeden zastává funkci ředitele společnosti a druhý má pozici vedoucího prodejny. Všichni zaměstnanci mají přímou komunikaci s jednatelem, což má za důsledek nepřítomnost manažerských funkcí.

2.2. Popis budovy

Hlavní sídlo společnosti se nachází v Novém Malíně, nedaleko obecního úřadu. Toto místo zahrnuje dvě budovy – prodejnu a sklad.

Prodejna se dělí na čtyři oblasti:

- Kanceláře
- Malý sklad
- Prodejní prostory
- Archiv



Obrázek 25 Fotografie budovy [Vlastní zpracování]

Prodejna se nachází v budově s vyvýšeným stavebním základem. Hlavní vchod vede do prodejny, která má otevřený půdorys. Přimo naproti dveřím se nachází pult s kasou a zbytek prostoru zabírají regály se zbožím. Po pravé straně je k prostorám prodejny připojen sklad, který uchovává zejména zboží malé a střední velikosti. Na levé straně se nachází vchod do kanceláří, kde jsou veškeré pracovní stanice, spolu s malou kuchyňkou, toaletami a velkým kulatým stolem. Kancelář má také druhé patro, kde se

nachází serverovna. Dveře vedoucí do kancelářských prostor jsou uzamykatelné a dostanou se tam pouze pracovníci. Jelikož k serverovně přímo vedou pouze schody bez dalších zábran, mohou se do ní dostat všichni pracovníci. Poslední místností je archiv, kde se skladují dokumenty. Tato místnost je zamknuta a mají k ní přístup pouze jednatelé. Firma také vlastní halu, která je používána jako sklad pro velké zboží a garáž pro firemní vozidla.

2.2.1. Vybavení místností

Archiv

- 1x NAS zálohovací server

Prodejna

- 1x Elektronická kasa
- 1x Počítačová sestava
- 1x Access Point

Kancelář

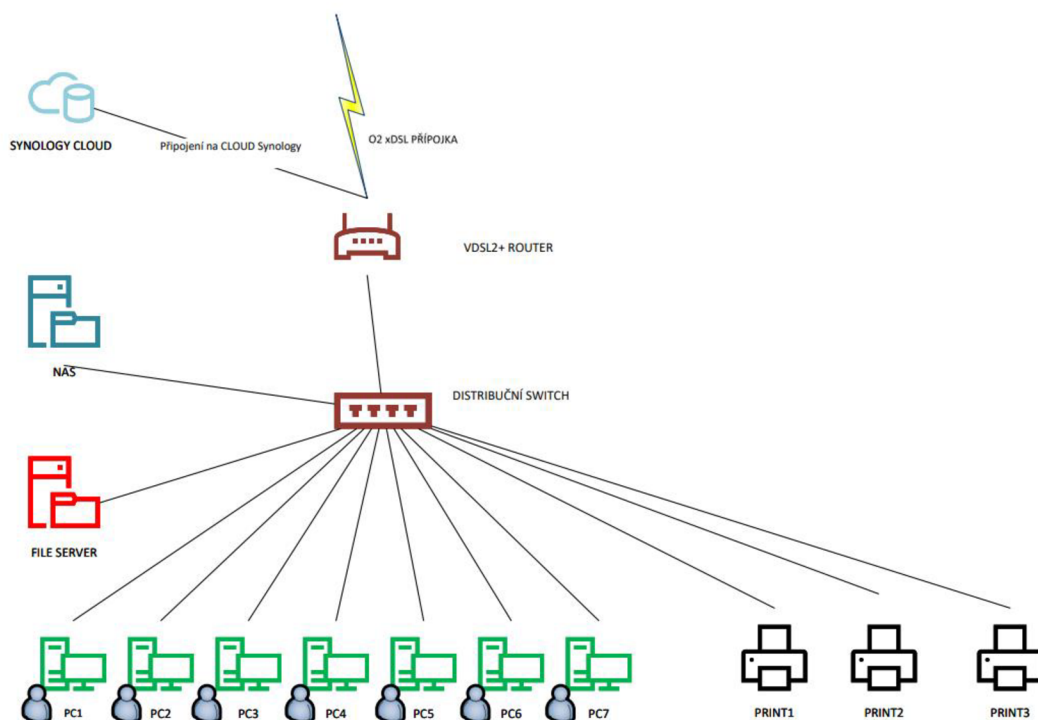
- 3x Laserové tiskárny
- 6x Počítačových sestav
- 1x Access point

Serverovna

- 1x Server
- 1x Router
- 1x Switch

2.3.Sít'ová infrastruktura

Pracovní stanice, tiskárny, server a záložní server jsou připojeny pomocí strukturované kabeláže do distribučního switchu. Tento switch je vybaven 24x 1Gb/s porty, 4x SPF porty a jeho přepínací kapacita je 56Gbs. Celá lokální síť je připojena na router, který vyjednává požadavky internetu. Router využívá konfiguraci DHCP, jedná se o protokol přidělující jednotlivým prvkům sítě IP adresy. Nastavení firewall stanovuje pravidla komunikace do a z internetu, čímž chrání uživatele před DDoS útoky. Na routeru je také zavedena soukromá VPN, která umožňuje zašifrované připojení uživatelů k internetu.



Obrázek 26 Schéma počítačové sítě [Vlastní zpracování]

Počítačová síť je ve společnosti rozdělena formou VXLAN, což je rozšířením VLAN. VLAN již sám o sobě poskytuje výhody oproti LAN zapojení, jelikož zajišťuje vyšší bezpečnost, díky menšímu počtu potřebných prvků v síti, lepší výkon a také snadnější správu ze strany zprostředkovatele. VXLAN k tomuto základu přidává zvýšenou flexibilitu a škálovatelnost segmentů. VXLAN využívá tunelování, čímž se eliminuje potřeba užívat Spanning tree protokol, který má za úkol blokovat redundantní cesty, čímž však způsobuje, že síť používá pouze polovinu svých dostupných cest. Díky odstranění tohoto protokolu je síť schopna využít všechny své dostupné cesty, čímž se maximalizuje její výkonnost. Výkonnost sítě je pro firmu důležitá, jelikož se k serveru

připojují pomocí vzdálené polohy za využití individuálních účtů a pouštějí jednotlivě instance IS Money S3.

2.3.1. Hardware

Na serveru jsou vedeny vzdálené plochy a je na něm nainstalovaná aplikace IS Money S3.

- Procesor: Intel Xeon E 2224G
- RAM: 8 GB
- Grafická karta: Intel UHD Graphics P630
- Pevný disk: 1TB HDD

Pro účely zálohování se v serverovně nachází server NAS.

Parametry:

- Procesor: Intel Celeron
- RAM: 2 GB
- Pevný disk: 1TB SSD

Každá pracovní stanice je vybavena stolním počítačem od společnosti DELL pro kancelářské účely, spolu se standardními monitory a ostatním příslušenstvím. Zaměstnanci mají možnost si vyměnit příslušenství, jako jsou například klávesnice, za své vlastní.

Parametry:

- Procesor: Intel Xeon E5-1603
- RAM: 16 GB
- Grafická karta: GeForce GTX 1050
- Pevný disk: 240 GB SSD

- OS: Windows 10 Pro

Kancelář je také vybavena třemi laserovými tiskárnami, které jsou do sítě propojeny přes rozhraní LAN a jsou dostupné pro všechny počítače v síti, za předpokladu, že má nainstalované potřebné ovladače a nastavenou IP adresu tiskárny.

Model:

- HP Color Laser MFP 179fnw

2.4.Zacházení s daty

2.4.1. Ukládání dat

Každá pracovní stanice se připojuje ke vzdálené ploše, kde využívá dvou disků, a to místního C, kde je nainstalovaný operační systém spolu s dalšími aplikacemi. Druhým diskem je E. Tento disk je společný pro všechny pracovníky a nejsou na něm zavedeny bariéry mezi jednotlivými zaměstnanci.

2.4.2. Zálohování

Zálohování probíhá ve firmě pomocí zálohovacího NAS serveru, na který jsou zálohy vytvářeny za využití agenta Active Backup For Business. Daný agent je nainstalován na každé pracovní stanici i na serveru. Zálohy serveru se vytváří 2x denně a to ve 3:00 a 17:00, první vytvořená záloha v měsíci má podobu Úplné zálohy, každá další záloha je inkrementální. Jsou zálohovány i jednotlivé pracovní stanice, avšak ty jsou na rozdíl od serveru zálohovány pouze 1x denně.

Zálohy jsou lokálně šifrované a NAS je připojen přes router ke službám C2 Cloud Synology, kde jsou data zkomprimována a ukládána. Společnost si pronajímá prostor o velikosti 1 TB a při jeho zaplnění je vždy odstraněna nejstarší záloha.

2.4.3. E-mail a webové stránky

Webové stránky mají podobu e-shopu a spolu s e-mailovými službami jsou uskutečněny na serveru Active24, který spravuje externí zprostředkovatel. Společnost si pronajímá e-

mailové schránky o velikosti 5 GB a jsou přístupné z aplikace Outlook nebo z mailových aplikací na mobilních telefonech zaměstnanců.

2.5. Bezpečnost a hrozby

Data jsou jedním z nejcennějších aktiv, které firma vlastní, proto je obzvláště důležité uplatňovat postupy, které minimalizují výskyt bezpečnostních incidentů a jejich dopad. Firma uchovává velká data:

- Účetní data
- Data o zaměstnancích
- Zákaznická data
- Firemní kontakty
- Zálohy

Data je nutné zabezpečit před několika hrozbami, které se dají rozdělit na vnitřní a vnější.

2.5.1. Vnitřní hrozby

Často se uvádí, že největší hrozbou jakéhokoliv systému je lidské selhání a řekla bych, že je toto tvrzení oprávněné. Z technického pohledu je firma poměrně dobře chráněna, avšak má do určité míry laxní přístup k bezpečnosti z pohledu zaměstnanců. Firma má přátelskou, až rodinnou, pracovní kulturu, což má vliv na to, jak se staví k omezování svých zaměstnanců. Mnoho zaměstnanců své firemní E-maily používá i pro osobní účely, což má za následek zvýšenou pravděpodobnost, že se stanou obětí podvodných spam akcí a phishingových E-mailů. Další velkou slabinou je nedbalost k omezení internetového přístupu prostřednictvím firewall. Zaměstnanci mají plný přístup k internetu a mohou využívat jakékoliv sociální sítě, či jiné pochybné webové stránky.

Společnost nemá své vlastní dedikované IT pracovníky, proto veškerou technickou podporu získávají od externí firmy, která zpracovává vše od počítačové sítě po server. Tato slabina se naplno projevila minulý rok, kdy servery této externí společnosti byly

napadnuty ransomware, který zašifroval nejen veškeré zálohy uložené na serveru, ale také znepřístupnil všechny pracovní stanice, které měly neustále otevřený vzdálený přístup.

2.5.2. Vnější hrozby

Firma je dobře zabezpečena proti fyzickým hrozbám, jako je například krádež, které je zabráněno pomocí bezpečnostních zámků, alarmu a kamer umístěných po venkovních i vnitřních prostorech. Díky vyvýšenému půdorysu je malá pravděpodobnost, že by majetek firmy byl poškozen povodní a všichni zaměstnanci jsou důkladně a pravidelně školeni, jak zacházet s nebezpečným zbožím a jak se chovat v případě požáru. K vnějším hrozbám také patří chyby operačního systému, únik dat v rámci aplikací a také incidenty vyplývající z bezdrátového propojení stanic.

3. Vlastní návrhy řešení

Na základě analýzy společnosti následně vytvořím návrh, který by za využití mých teoretických poznatků mohl vylepšit datovou bezpečnost společnosti. Podle mého názoru společnost akceptovala bezpečnostní rizika pod domněnkou, že jako malá firma je nepravděpodobné, že by se mohl vyskytnout bezpečnostní incident z vnější strany, bohužel se však opak stal pravdou. Můj návrh zahrnuje změny v zálohování a zpřísnění bezpečnostních postupů.

3.1. Zálohování

Prvním krokem pro zvýšení bezpečnosti je dle mého názoru důkladnější systém zálohování. Současný způsob zálohování je adekvátní, má však nevýhodu toho, že se jedná o pouze jednu instanci zálohy, která je vedena na externím cloudovém úložišti. Domnívám se, že by bylo vhodné, kdyby firma začala aplikovat strategii 3-2-1. Tedy 3 kopie, 2 v prostorách firmy, 1 na úložišti na jiném místě.

Společnost používá své současné NAS zařízení, jako zálohovací server, který posílá data na cloudové úložiště C2 Cloud Synology. Výhodou NAS je, že je možné zařízení konfigurovat pro více účelů. Bylo by užitečné, kdyby se zařízení používalo také jako fyzické úložiště záloh. Toho lze dosáhnout instalací HDD disku do volného slotu na zařízení. Daný disk by spolu s cloudovým úložištěm pokryl požadavky 3-2-1 strategie, týkající se uchovávání záloh v prostorách společnosti.

V tabulce jsou uvedeny možné HDD úložiště, které by odpovídaly potřebám společnosti.

Tabulka 1 NAS HDD disky [Vlastní zpracování, ceny dle Alza.cz 18. 3. 2023]

Výrobce	Western digital	Seagate	Western digital
Model	Red Plus 1TB	SkyHawk 1TB	Blue 1TB
Rychlost přenosu	150 Mb/s	180 Mb/s	150 Mb/s
Vyrovňovací paměť	64 MB	64 MB	64 MB
Rozhraní	SATA III	SATA III	SATA III
Cena s DPH	1 358 Kč	1 019 Kč	949 Kč

Nejlepší volbou HDD disku je dle mého úsudku WD Red Plus, díky jeho rychlosti zapisování a vysoké spolehlivosti.

Pro zálohu, která bude uchovávána mimo prostory společnosti, navrhuji dvě varianty – externí disk a cloudové úložiště. V obou variantách je zálohovací plán stejný, první pracovní den měsíce by byla vytvořena úplná záloha, a následně by se každý pátek vytvářely inkrementální zálohy serveru i pracovních stanic.

V případě externích disků jsou dvě možnosti, a to HDD a SSD disky. Oba dva typy disků mají své výhody i nevýhody. HDD disky jsou náchylné na fyzické poškození, kvůli jejich mechanickým součástkám, nabízí však mnohem větší kapacitu za nižší cenu. SSD disky se vyznačují obzvláště svou rychlostí a odolností vůči poškození, díky tomu, že nemají žádné pohyblivé součástky. Mohou však trpět na bitflipping a jsou ve vyšší cenové kategorii. Externí disk by uchovávali jednatelé ve svém bydlišti. Na níže uvedených tabulkách jsou možné nabídky.

Tabulka 2 Externí SSD a HDD disky [Vlastní zpracování, ceny dle Alza.cz 18. 3. 2023]

Výrobce	SanDisk	Samsung	Western digital	Verbatim
Model	Extreme Portable SSD V2	Portable SSD T7	Elements Portable	Store 'n' Go
Kapacita	1 TB	1 TB	1 TB	1 TB
Šifrování	AES 256-bit hardwarové	AES 256-bit hardwarové	AES 256-bit Softwarové	AES 256-bit hardwarové
USB rozhraní	3.2	3.2	3.0	3.0
Cena s DPH	2 699 Kč	2 277 Kč	1 449 Kč	1 324 Kč

Cloudová úložiště jsou dnes čím dál více populární volbou pro uchovávání záloh, díky jejich snadné integraci. Zvolila jsem 4 možné poskytovatele, kteří odpovídají požadavkům společnosti.

První volbou je Google Workspace, s tarifem Business Standard, tento tarif uživatelům poskytuje 2TB úložiště, vlastní zabezpečené emaily, zabezpečení zpráv spolu s dalšími aplikace Google jako jsou například Google Docs.

OneDrive pro firmy plán 2 nejlépe odpovídá požadavkům firmy, co se týče funkcí. Tento tarif zahrnuje 1 TB úložiště s funkcemi pro sdílení a zabezpečení souborů.

V případě DropBox Business požadavkům nejlépe odpovídá tarif Professional, který poskytuje 3 TB úložiště, elektronické podpisy, funkce pro sdílení a obnovení souborů.

Tabulka 3 Cloudová úložiště [Vlastní zpracování]

Úložiště	Google Workspace	OneDrive	Dropbox
Plán	2 TB	1 TB	3 TB
Šifrování	256-bit AES	256-bit AES	256-bit AES
Cena bez DPH za 1 uživatele	11,50 €/měsíc	9,40 €/měsíc	19,99 €/měsíc

Na základě nabídky a požadavků firmy jsem usoudila, že nejlepší variantou pro úložiště mimo prostory je externí SSD disk od společnosti Samsung. Firma již využívá cloudové úložiště, pro uchovávání záloh, a bylo by nevhodné využívat dvě stejné služby. Externí disk je také bezpečnější díky jeho fyzickému charakteru.

3.2. Ukládání dat

Pro ukládání dat bych zavedla pár změn, které by mohly pozitivně ovlivnit jejich bezpečnost. Veškeré soubory na serveru jsou přístupné všem zaměstnancům, mým názorem je, že by bylo užitečné, kdyby se na serveru vytvořil nový logický oddíl, který by byl určen pro jednotlivé zaměstnance. Každý by měl na serveru své vlastní místo, kde si může ukládat data, ke kterým má přístup pouze přesně určený jedinec. Dále by bylo vhodné, kdyby obzvláště citlivá data, jako jsou například informace o zákaznících, byla při ukládání zašifrována.

3.3. Bezpečnostní postupy

V oblasti bezpečnostních postupů jsem identifikovala pár nedostatků, které by bylo vhodné změnit. V první řadě bych zpřísnila omezení firewall na všech pracovních stanicích. Znepřístupnila bych jmenovitě:

- Sociální sítě
- Webové stránky, na které mohou uživatelé nahrávat vlastní obsah (různé fileshare stránky, blogy a pirátské stránky)
- Webové stránky s nezabezpečenou doménou
- Webové stránky s online hrami

Dále bych zavedla povinné školení ohledně bezpečnosti pro všechny zaměstnance, tato školení by měla obzvláště zahrnovat, jak efektivně rozpoznat phishingové E-maily, sociální inženýrství, vytváření hesel a autentifikaci. Také bych zaměstnancům znepřístupnila možnost užívat pracovní E-maily pro osobní účely, jelikož se tím zvyšuje pravděpodobnost, že se stanou obětí spam akcí a jiných podvodných E-mailů. Kurz kyberbezpečnosti bude poskytnut online formou od společnosti Pumpedu s. r. o.

Do serverovny by měli mít přístup pouze jednatelé a správce serveru. Navrhuji buď server přesunout do archivu, který je zabezpečen zámkem anebo nainstalovat bezpečnostní ohradu na schodiště vedoucí k serverovně.

Jako poslední bych zvažila snížit závislost společnosti na externí služby v oblasti IT, prvním krokem by mohlo být vytváření záloh. Zvolila bych jednoho zaměstnance, který by po důkladném proškolení zodpovídal za veškeré zálohy, které společnost provozuje. Následně by tento zaměstnanec mohl být zaškolen ve správě a konfiguraci serverového systému.

3.4. Zhodnocení vlastního návrhu

Návrh na zakoupení nových datových úložišť firmu chrání před hrozbami plynoucími z používání jediné zálohy, zvyšují integritu dat a jejich fyzický charakter pokrývá nedostatky vyplývající z používání cloudového úložiště.

Změny v bezpečnostních postupech a způsobu ukládání dat řeší bezpečnostní rizika vytvořené lidským faktorem. Zaškolení zaměstnanců v oblasti bezpečnosti je řešeno v podobě online kurzu. O zaškolení zaměstnance, který bude zodpovídat za správu záloh, se postará externí společnost, která Krako-Weding poskytuje IT služby.

Jelikož společnost již vlastní NAS úložiště, náklady na hardware jsou poměrně nízké, jelikož se jedná o rozšíření již existující struktury. Nejdražší položkou je vybudování bezpečnostní ohrady schodiště, tato cena je odhad, který zahrnuje ohradu, dveře a cenu za montáž. Ceny jsou uvedeny s DPH.

Tabulka 4 Cenová kalkulace [Vlastní zpracování]

Položka	Cena
Hardware	3 635 Kč
Vzdělávací kurz	8 349 Kč
Bezpečnostní ohrada schodiště	Odhad 70 000 Kč
Celkem	82 406 Kč

Závěr

Cílem mé bakalářské práce bylo seznámit čtenáře s problematikou datových úložišť, zálohování dat a kybernetickou bezpečností. Práce nastínila, jak moderní počítače interpretují a organizují data. Dále se zabývala historií vývoje nejdůležitějších datových úložišť, jejich charakteristikami a způsobem, jakým jsou data na tyto fyzická úložiště zapsána. Práce se také zabývala zálohováním, bezpečností, doporučenými postupy a strategiemi.

Tyto poznatky sloužili jako podklad pro analýzu konkrétní společnosti v této oblasti, z které vyplynulo:

- Dobré technické provedení z pohledu počítačové sítě, využitých zálohovacích technologií a hardware
- Závislost na externí společnosti pro správu serveru, síťové infrastruktury, zálohování
- Nedostatečné bezpečnostní postupy

Na základě analýzy byl proveden vlastní návrh pro zlepšení současného stavu:

- Zavedení zálohovací strategie 3-2-1
- Zvýšení nezávislosti na externí společnosti zaučením zaměstnance, který by zodpovídal, za veškeré zálohovací záležitosti
- Zpřísnění bezpečnostních opatření

Vlastní návrh byl navržen způsobem, který je pro společnost ekonomicky přijatelný a umožnil snadnou implementaci.

Seznam použité literatury

1. VAUGHAN, Jack. What is Data? [online]. [cit. 2023-01-30]. Dostupné z: <https://www.techtarget.com/searchdatamanagement/definition/data>
2. ARCHIVED: What are bits, bytes, and other units of measure for digital information?. University Information Technology Services [online]. [cit. 2023-01-30]. Dostupné z: <https://kb.iu.edu/d/ackw>
3. Bits & Bytes Conversion Table. Portland Computing Class [online]. [cit. 2023-01-30]. Dostupné z: <https://mrribaux.weebly.com/bits--bytes.html>
4. VAN WETTEN, Ariën. What Is NTFS and How Does It Work?. Datto [online]. [cit. 2023-01-30]. Dostupné z: <https://www.datto.com/blog/what-is-ntfs-and-how-does-it-work>
5. NTFS File and Folder Permissions Reporting Tool. FileCloud [online]. [cit. 2023-01-30]. Dostupné z: <https://www.filecloud.com/blog/2017/03/it-admin-guide-to-ntfs-file-and-folder-permissions/#.Y9gMOqjMK3A>
6. LUTKEVICH, Ben. NTFS (NT File System). TechTarget [online]. [cit. 2023-01-30]. Dostupné z: <https://www.techtarget.com/searchwindowsserver/definition/NTFS>
7. Default cluster size for NTFS, FAT, and exFAT [online]. [cit. 2023-01-30]. Dostupné z: <https://support.microsoft.com/en-us/topic/default-cluster-size-for-ntfs-fat-and-exfat-9772e6f1-e31a-00d7-e18f-73169155af95>
8. Punch Card. Computer Hope [online]. 05/02/2021 [cit. 2023-01-30]. Dostupné z: <https://www.computerhope.com/jargon/p/punccard.htm>
9. Miniwark. *Modèle réduit de métier à tisser Jacquard, 1810* [online]. 18- [cit. 2023-04-22]. Dostupné z: https://commons.wikimedia.org/wiki/File:Modèle_réduit_de_métier_à_tisser_Jacquard_1810.jpg
10. 1801: PUNCHED CARDS CONTROL JACQUARD LOOM. Computer History Museum [online]. [cit. 2023-01-30]. Dostupné z: <https://www.computerhistory.org/storageengine/punched-cards-control-jacquard-loom/>
11. IBM [online]. [cit. 2023-01-30]. Dostupné z: <https://www.ibm.com/ibm/history/ibm100/us/en/icons/punchcard/>
12. Abby. Magnetic Tape Explained – Everything You Need To Know [online]. 6/12/2022 [cit. 2023-01-30]. Dostupné z: <https://history-computer.com/magnetic-tape/>
13. United States Consensus Bureau [online]. [cit. 2023-01-30]. Dostupné z: https://www.census.gov/history/www/innovations/technology/univac_i.html
14. SWAINE, Michael R. a Paul A. UNIVAC Computer: Universal Automatic Computer. Britannica [online]. [cit. 2023-01-30]. Dostupné z: <https://www.britannica.com/technology/UNIVAC>
15. IEEE Spectrum [online]. [cit. 2023-01-30]. Dostupné z: <https://spectrum.ieee.org/why-the-future-of-data-storage-is-still-magnetic-tape>
16. BRAIN, Marshall. How Tape Recorders Work. Howstuffworks [online]. [cit. 2023-01-30]. Dostupné z: <https://electronics.howstuffworks.com/gadgets/audio-music/cassette.htm>
17. MELLOR, Chris. IBM and Fujifilm demo 580TB tape. Yes it's a record. Blocks & Files [online]. 16/12/2020 [cit. 2023-01-30]. Dostupné z: <https://blocksandfiles.com/2020/12/16/ibm-and-fujifilm-580tb-tape-capacity-record/>
18. The History of External Hard Drives and Portable Backup Systems. Record Nations [online]. [cit. 2023-01-30]. Dostupné z: <https://www.recordnations.com/articles/external-hard-drive/>
19. RAMAC: The First Magnetic Hard Disk. IBM [online]. [cit. 2023-01-30]. Dostupné z: <https://www.ibm.com/ibm/history/ibm100/us/en/icons/ramac/transform/>
20. IBM [online]. [cit. 2023-01-30]. Dostupné z: https://www.ibm.com/ibm/history/exhibits/storage/storage_1311.html
21. WOODFORD, Chris. Hard drives. Explain that stuff [online]. 9/11/2021 [cit. 2023-01-30]. Dostupné z: <https://www.explainthatstuff.com/harddrive.html>
22. COUGHLIN, Tom. *We Need A Boost In HDD Areal Density!* [online]. 18-9-2022 [cit. 2023-04-22]. Dostupné z: <https://www.forbes.com/sites/tomcoughlin/2022/09/18/we-need-a-boost-in-hdd-areal-density/?sh=41804a125f63>
23. DEMBOWSKI, K. *Mistrovství v hardware*. 1. vyd. Brno: Computer Press, 2009. ISBN 978-80-251-2310-2
24. BROWN, Gary. How Floppy Disk Drives Work [online]. [cit. 2023-01-30]. Dostupné z: <https://computer.howstuffworks.com/floppy-disk-drive2.htm>
25. Floppy disk. Computer Hope [online]. 11/10/2021 [cit. 2023-01-30]. Dostupné z: <https://www.computerhope.com/jargon/f/floppydi.htm>
26. The FLOppy Disk. IBM [online]. [cit. 2023-01-30]. Dostupné z: <https://www.ibm.com/ibm/history/ibm100/us/en/icons/floppy/transform/>
27. 1971: FLOPPY DISK LOADS MAINFRAME COMPUTER DATA [online]. [cit. 2023-01-30]. Dostupné z: <https://www.computerhistory.org/storageengine/floppy-disk-loads-mainframe-computer-data/>
28. Personal computer. Britannica [online]. [cit. 2023-01-30]. Dostupné z: <https://www.britannica.com/technology/personal-computer>
29. PECINOVSKÝ, J. *Archivace a komprimace dat*. Praha: Grada Publishing a.s., 2003. ISBN 80-24-0659-8

30. Compact Disc Rainbow Books. Museum of obsolete data [online]. [cit. 2023-01-30]. Dostupné z: <https://obsoletemedia.org/audio/compact-disc-rainbow-books/>
31. Co se ukrývá uvnitř a specifikace [online]. 18/7/2003 [cit. 2023-01-30]. Dostupné z: <https://diit.cz/clanek/co-se-ukryva-uvnitř-a-specifikace>
32. SULLIVAN, Erin. Compact disc. Tech Target [online]. [cit. 2023-01-30]. Dostupné z: <https://www.techtarget.com/searchstorage/definition/compact-disc>
33. BRAIN, Marshall. How CDs Work. Howstuffworks [online]. 12/7/2021 [cit. 2023-01-30]. Dostupné z: <https://electronics.howstuffworks.com/cd.htm#pt1>
34. Der physikalische Aufbau: Pits und Lands [online]. [cit. 2023-01-30]. Dostupné z: https://referate.mezdata.de/sj2003/cd_thomas-ley/ausarbeitung/aufbau2.html
35. TIŠNOVSKÝ, Pavel. Vývoj optických pamětí: od DVD k Blu-ray. *Root* [online]. 11-9-2008 [cit. 2023-04-29]. Dostupné z: <https://www.root.cz/clanky/vyvoj-opticky-pameti-od-dvd-k-blu-ray/>
36. GOLDENBAUM, Jeff. New AMD Opteron-Based ProLiant Servers. Dataram [online]. 22/8/2012 [cit. 2023-01-30]. Dostupné z: <http://www.dataram.com/blog/>
37. The Development and History of Solid State Drives (SSDs). Symmetry electronics [online]. 10/9/2014 [cit. 2023-01-30]. Dostupné z: <https://www.symmetryelectronics.com/blog/the-development-and-history-of-solid-state-drives/>
38. HOPKINS, Jessica. Introduction to Flash Memory. Total Phase [online]. 27/8/2021 [cit. 2023-01-30]. Dostupné z: <https://www.totalphase.com/blog/2021/10/what-is-flash-memory-introduction-types-examples-applications/>
39. TOKAR, Les. Super Talent DuraDrive AT7 SSD Review (1TB) – In Vehicle Infotainment (IVI) System SSDs. *The SSD Review* [online]. [cit. 2023-04-22]. Dostupné z: <https://www.thesdreview.com/our-reviews/super-talent-duradrive-at7-ssd-review-1tb-vehicle-infotainment-ivi-system-ssds/>
40. ARAVINDAN, Avinash. Flash 101: NAND Flash vs NOR Flash. *Embedded* [online]. 23-7-2018 [cit. 2023-04-29]. Dostupné z: <https://www.embedded.com/flash-101-nand-flash-vs-nor-flash/>
41. CHAMPION, Leo. The History of USB Flash Drives [online]. [cit. 2023-01-30]. Dostupné z: <https://www.techwalla.com/articles/the-history-of-usb-flash-drives>
42. WHITENER, Patrick. What's Inside: USB Flash Drive Components. *USB Memory Direct* [online]. 17-4-2021 [cit. 2023-04-22]. Dostupné z: <https://www.usbmemorydirect.com/blog/whats-inside-usb-flash-drive-components/>
43. What's the Difference Between USB 1.0, 2.0 and 3.0?. *Every USB* [online]. [cit. 2023-01-30]. Dostupné z: <https://www.everyusb.com/difference-usb-1-2-3-generations>
44. A Brief History of the Internet [online]. [cit. 2023-01-30]. Dostupné z: https://www.usg.edu/galileo/skills/unit07/internet07_02.phtml
45. FARRIS, Chelsey. History of Cloud Storage [online]. 5/12/2019 [cit. 2023-01-30]. Dostupné z: <https://capacity.com/cloud-storage/history-of-cloud-storage/>
46. CUBR, L. Dlouhodobá ochrana digitálních dokumentů. Praha: Národní knihovna České republiky, 2010. ISBN 978-80-7050-588-5
47. N, Doug. Recommended Server Room Temperature and Humidity. *PageLines* [online]. 11/2/2021 [cit. 2023-01-30]. Dostupné z: <https://www.poweradmin.com/blog/recommended-server-room-temperature-and-humidity/>
48. OLNEY, Matthew. 2022 in 22 Cyber Security Statistics [online]. 13/12/2022 [cit. 2023-01-30]. Dostupné z: <https://insights.integrity360.com/2022-in-22-cyber-security-statistics>
49. NELSON, S. Pro data backup and recovery. New York: Distributed to the book trade worldwide by Springer Science+Business Media, 2011. ISBN 978-1-4302-2663-5.
50. WALLEN, Dave. Types of Backup: Understanding Full, Differential, and Incremental Backup. *Spanning* [online]. 31/3/2020 [cit. 2023-01-30]. Dostupné z: <https://spanning.com/blog/types-of-backup-understanding-full-differential-incremental-backup/>
51. What is data mirroring?. *ManageEngine* [online]. [cit. 2023-01-30]. Dostupné z: <https://www.manageengine.com/device-control/data-mirroring.html>
52. Paul. RPO vs. RTO: Key differences explained with examples, tips. *TechTarget* [online]. [cit. 2023-01-30]. Dostupné z: <https://www.techtarget.com/searchstorage/feature/What-is-the-difference-between-RPO-and-RTO-from-a-backup-perspective>
53. What is a 3-2-1 Backup Strategy?. *Seagate* [online]. [cit. 2023-01-30]. Dostupné z: <https://www.seagate.com/blog/what-is-a-3-2-1-backup-strategy/>
54. VERMA, Mansi. DATA ERASURE. *Stellar* [online]. [cit. 2023-01-30]. Dostupné z: <https://www.stellarinfo.com/article/is-your-data-ever-really-gone.php>

Přílohy

Seznam obrázků

OBRÁZEK 1 TABULKA JEDNOTEK [VLASTNÍ ZPRACOVÁNÍ]	11
OBRÁZEK 2 STROMOVÁ HIERARCHIE [VLASTNÍ ZPRACOVÁNÍ]	12
OBRÁZEK 3 SNÍMEK MTF TABULKY [VLASTNÍ ZPRACOVÁNÍ].....	13
OBRÁZEK 4 SNÍMEK SYSTÉMU SOUBORŮ [VLASTNÍ ZPRACOVÁNÍ]	13
OBRÁZEK 5 TABULKA SVAZKŮ [VLASTNÍ ZPRACOVÁNÍ].....	14
OBRÁZEK 6 DĚRNÝ ŠTÍTEK [8]	16
OBRÁZEK 7 JACQUARDŮV TKACÍ STROJ [9]	16
OBRÁZEK 8 PFLEUMER A PRVNÍ MAGNETICKÁ PÁSKA [12].....	17
OBRÁZEK 9 UNIVAC 1 [13]	18
OBRÁZEK 10 MAGNETICKÁ PÁSKA PRO UNIVAC 1 [15]	18
OBRÁZEK 11 RAMAC [19].....	19
OBRÁZEK 12 HDD [22].....	20
OBRÁZEK 13 PRVNÍ DISKETA MINNOW [27]	21
OBRÁZEK 14 DISKETA [26]	21
OBRÁZEK 15 MECHANICKÁ ČTEČKA DISKŮ [31]	23
OBRÁZEK 16 KOMPAKTNÍ DISK [32].....	23
OBRÁZEK 17 SCHÉMA ZAPISOVÁNÍ BINÁRNÍCH HODNOT [34]	24
OBRÁZEK 18 SCHÉMA DATOVÉ VRSTVY CD [34]	24
OBRÁZEK 19 PRVNÍ SSD DISK BULK CORE [37].....	25
OBRÁZEK 20 SSD DISK [39]	26
OBRÁZEK 21 SCHÉMA NOR A NAND [40]	27
OBRÁZEK 22 USB FLASH DISK [42].....	28
OBRÁZEK 23 COLD STORAGE MAGNETICKÝCH PÁSEK [15]	35
OBRÁZEK 24 ORGANIZAČNÍ STRUKTURA SPOLEČNOSTI [VLASTNÍ ZPRACOVÁNÍ]	43
OBRÁZEK 25 FOTOGRAFIE BUDOVY [VLASTNÍ ZPRACOVÁNÍ].....	44
OBRÁZEK 26 SCHÉMA POČÍTAČOVÉ SÍTĚ [VLASTNÍ ZPRACOVÁNÍ]	46

Seznam tabulek

TABULKA 1 NAS HDD DISKY [VLASTNÍ ZPRACOVÁNÍ, CENY DLE ALZA.CZ 18. 3. 2023].....	51
TABULKA 2 EXTERNÍ SSD A HDD DISKY [VLASTNÍ ZPRACOVÁNÍ, CENY DLE ALZA.CZ 18. 3. 2023]	52
TABULKA 3 CLOUDOVÁ ÚLOŽIŠTĚ [VLASTNÍ ZPRACOVÁNÍ].....	53
TABULKA 4 CENOVÁ KALKULACE [VLASTNÍ ZPRACOVÁNÍ]	55