VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH SPOLEHLIVÉ DATOVÉ INFRASTRUKTURY VE SPOLEČNOSTI S VÍCE POBOČKAMI

DESIGN A RELIABLE DATA INFRASTRUCTURE IN A MULTI-BRANCH COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. Filip Dočekal
AUTHOR

VEDOUCÍ PRÁCE — Ing. Viktor Ondrák, Ph.D.
SUPERVISOR

BRNO 2020

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Filip Dočekal**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Viktor Ondrák, Ph.D.**
Akademický rok:	2019/20

Ředitel ústavu 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 diplomovou práci s názvem:

Návrh spolehlivé datové infrastruktury ve společnosti s více pobočkami

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:

Navrhnout spolehlivou datovou infrastrukturu.

Základní literární prameny:

ČSN ISO/IEC 27001:2006 Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací – Požadavky. Český normalizační institut, 2006.

ČSN ISO/IEC 27002:2005 Informační technologie – Bezpečnostní techniky – Soubor postupů pro řízení bezpečnosti informací. Český normalizační institut, 2005.

DE GUISE, Preston. Data Protection: Ensuring Data Availability. Apple Academic Press, 2017. ISBN 9781482244151.

MORGAN, Richard a Ruth BOARDMAN. Data protection strategy: implementing data protection compliance. 2nd ed. London: Sweet & Maxwell/Thomson Reuters, 2012. ISBN 978-0414026742.

POŽÁR, Josef. Základy teorie informační bezpečnosti. Praha: Vydavatelství PA ČR, 2007. ISBN 978-80-7251-250-8.

TAYLOR, Andy. Information security management principles. Second edition. Swindon, UK: BCS, the Chartered Institute for IT, 2013. ISBN 9781780171753.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2019/20

V Brně dne 29.2.2020

L. S.

doc. RNDr. Bedřich Půža, CSc. ředitel	doc. Ing. et Ing. Stanislav Škapa, Ph.D. děkan

Abstrakt

Diplomová práce je zaměřena na funkční návrh spolehlivé datové infrastruktury ve společnosti s více pobočkami. Diplomová práce analyzuje současný stav datové infrastruktury a na základě analýzy je zrealizováno vlastní řešení. Řešení musí být funkční a odpovídat požadavkům dohodnutým s investorem.

Klíčová slova

Návrh, datová infrastruktura, uložiště, ukládání dat

Abstract

The master’s thesis is focused on a functional suggestion of a data infrastructure in a company with more branches. It analyses the present condition of the data infrastructure and it is based on an analysis and there is an own solution implemented. The solution must be functional, and it must match the requirements discussed with the investor.

Key words

Suggestion, data infrastructure, storage, saving of data

Bibliografická citace

DOČEKAL, Filip. *Návrh spolehlivé datové infrastruktury ve společnosti s více pobočkami* [online]. Brno, 2020 [cit. 2020-05-16]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/125425. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Viktor Ondrák.

Čestné prohlášení

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

V Brně dne 16. května 2020

……..

podpis studenta

Poděkování

Moje poděkování patří především Ing. Viktorovi Ondrákovi, Ph.D. za vedení mé diplomové práce. Děkuji za jeho odborné rady a pomoc při řešení problémů. Dále bych chtěl poděkovat rodině a přátelům, kteří mě při tvorbě práce podporovali.

OBSAH

ÚVOD

Diplomová práce je zaměřená na téma návrh spolehlivé datové infrastruktury ve společnosti s více pobočkami. Zajištění spolehlivé datové infrastruktury je pro společnosti velmi důležité. Díky kvalitní datové infrastruktuře se zvýší produktivita práce a efektivita celé firmy. Trendem dnešní doby je sdílet si mezi pobočkami společnostmi svá data, u kterých je potřeba zajistit kvalitní dostupnost dat a zároveň zajistit bezpečnost sdílených dat.

Společnost, pro kterou jsem se rozhodl realizovat diplomovou práci na téma návrh spolehlivé datové infrastruktury společnosti s více pobočkami, se nyní potýká s velmi nekvalitním zabezpečením a absencí zálohování dat. Taktéž se zaměstnanci potýkají s nulovou dostupností dat mezi svými pobočkami firmy.

CÍLE PRÁCE

Hlavním cílem této práce je návrh plně funkčního řešení, které zajistí spolehlivou datovou infrastrukturu mezi pobočkami firmy s možností jednoduchého budoucího rozšíření. První část se týká analýzy současného stavu a na základě toho se vytvoří funkční řešení, které bude odpovídat požadavkům investora.

Diplomová práce se zabývá analýzou současného stavu. Zde je popsána stávající situace spojená s dostupností dat a její nedostatky. Další část se zabývá teoretickými východisky, která jsou nutná pro návrh kvalitní a spolehlivé datové infrastruktury. Poslední část se týká realizace návrhů, popsání jejich výhod a finančního zhodnocení celého projektu.

1 ANALÝZA SOUČASNÉHO STAVU

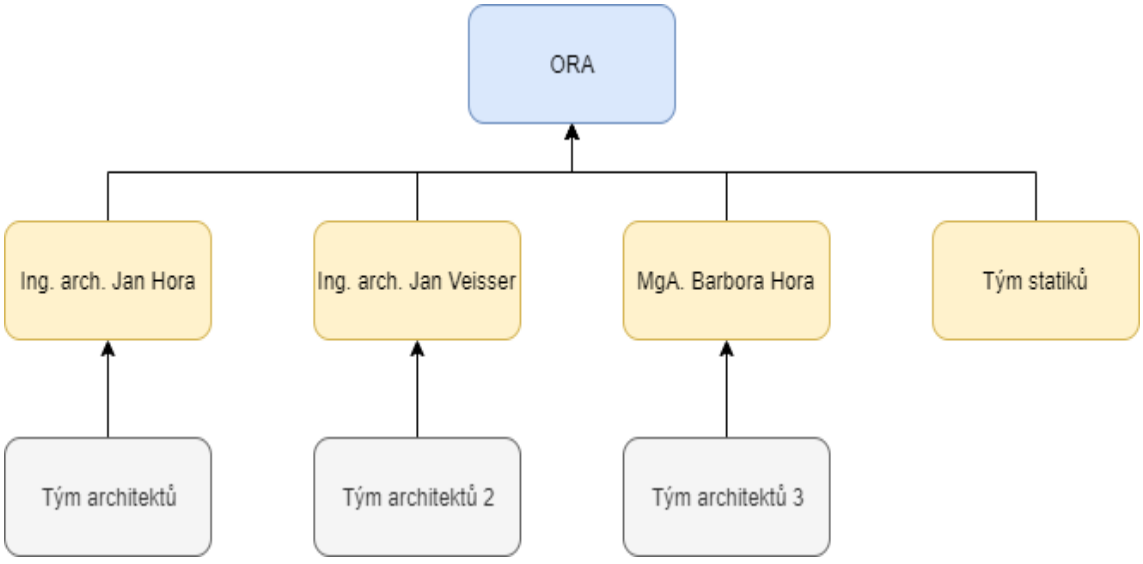
Tato kapitola se zabývá popisem společnosti, pro kterou bude projekt realizován. V této kapitole je zhodnocena stávající infrastruktura a požadavky investora na vytvoření nové spolehlivé datové infrastruktury mezi více pobočkami firmy.

1.1 Popis firmy

Sdružení ORA je zkratkou pro Originální Regionální Architekturu. ORA vznikla v roce 2014 třemi znojemskými architekty. Momentálně každý architekt pracuje jako OSVČ. Architektonický ateliér má sídlo ve Znojmě. Hlavním tématem, kterým se toto sdružení architektů zabývá je maloměsto a jeho kontext.

ORA se v roce 2017 rozrostla do Kutné Hory, kde sídlí 3 architekti. Na pobočce ve Znojmě, která sídlí na adrese Rooseveltova 836/6 pak sídlí 13 architektů, kteří pracují na společných projektech.

Společně s architekty pracuje i tým statiků pod firmou STATIKA 3 STRUCTURE s.r.o., které sídlí v druhém patře na znojemské pobočce. Tým statiků má přístup do aktuálních projektů sdružení ORA, se kterými tyto projekty konzultuje a provádí úpravy.



Obrázek 1: Organizační struktura ORA

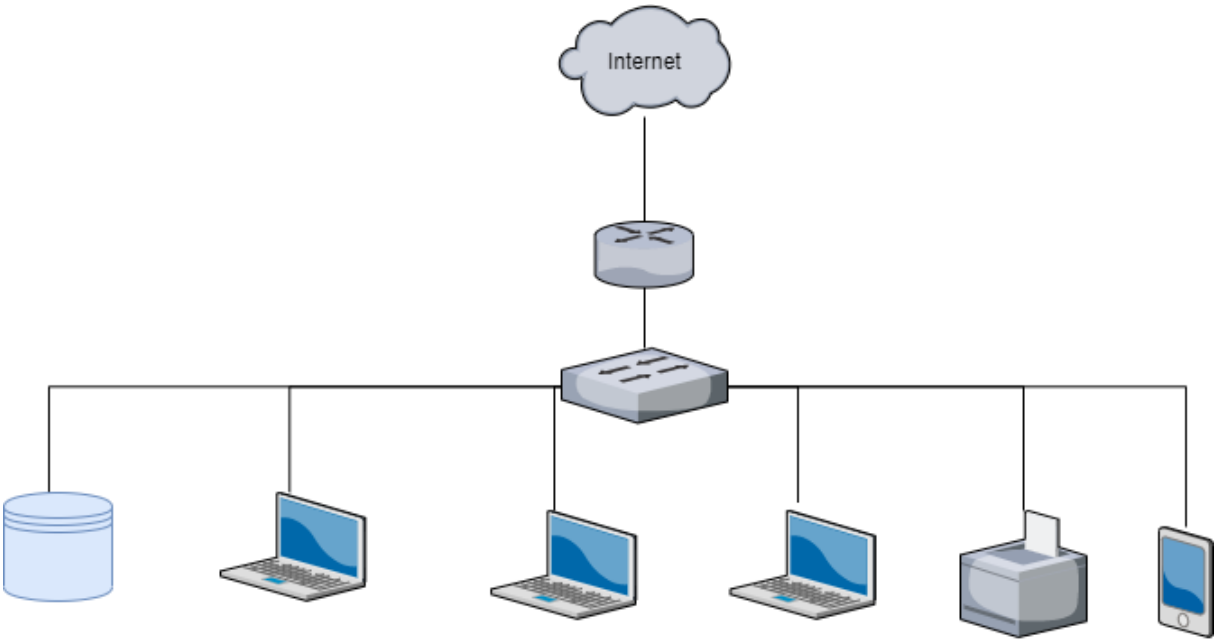
(Zdroj: Vlastní zpracování)

1.2 Analýza současného stavu sítě

Tato kapitola se zabývá současným stavem sítě na pobočce Znojmo a na pobočce Kutná Hora.

1.2.1 ICT ve sdružení ORA

ICT neboli informační a komunikační technologie je nedílnou součástí každé firmy. Výjimku netvoří ani sdružení architektů ORA. Sdružení využívá vnitřní síť LAN zejména pro přístup do síťového uložiště, kde jsou uloženy veškerá firemní data, jako projekty, na kterých se právě pracuje, archiv a jiná firemní data. Počítačová síť se pak využívá pro komunikaci se síťovou tiskárnou, přes kterou se provádí tisk a skenování. Uživatelé se do počítačové sítě mohou připojit buď přes drátovou nebo bezdrátovou komunikaci. Bezdrátovou komunikaci ve vnitřní síti sdružení zajišťují přístupové body od společnosti Ubiquiti. Komunikační uzly v rámci LAN sítě jsou propojeny hvězdicovou topologií. Přístup do internetu, tedy WAN síť, pak pracovníci využívají zejména pro přístup do mailové schránky a pro vyhledávání potřebných informací na internetu.



Obrázek 2: Struktura sítě na znojemské pobočce

(Zdroj: Vlastní zpracování)

1.2.2 Současný stav pobočky Znojmo

Na pobočce ve Znojmě je v současné době NAS od společnosti Synology verze DS218j. Na toto zařízení se připojuje cca 6 uživatelů současně. Veškerá firemní data jsou uložena na tomto zařízení a nikam se nezálohují. Největším problémem je tedy absence jakéhokoliv zálohování a v případě napadení virem nebo smazáním dat některým z uživatelů dojde k nenávratné ztrátě dat. Na zařízení je vytvořeno pole RAID 1, které tak pouze ochrání data v případě selhání jednoho ze dvou HDD. Toto síťové uložiště je nevyhovující pro firemní prostředí.

Na pobočce nejsou zavedena žádná pravidla přístupu a každý uživatel může přistoupit do kterékoliv složky a upravovat či mazat data na síťovém uložišti.

Pobočka ve Znojmě trpí také nedostatkem kapacity síťového uložiště. V Synology jsou nainstalovány disky o kapacitě 2 TB. Vzhledem k velikosti souborů a počtu zaměstnanců na této pobočce je kapacita nevyhovující. Na uložišti jsou umístěny data od založení sdružení.

Tabulka 1: Parametry síťového uložiště ve Znojmě

(Zdroj: Vlastní zpracování dle: 2)

Synology DS218j	
Počet disků	2
Kapacita disků [TB]	2
RAID	1
CPU	Marvell Armada 385 88F6820 1,3GHz
RAM [MB]	512
Počet GLAN	1

Nevyhovující pro jakékoliv přenosy mimo interní síť je také internetová konektivita. V současné době je konektivita zajištěna společností PODA a.s. Průměrná rychlost z více měření je popsána v následující tabulce.

Tabulka 2:Internetová konektivita pobočka Znojmo

(Zdroj: Vlastní zpracování)

Internetová konektivita	
Download [Mbps]	15
Upload [Mbps]	2

1.2.3 Současný stav pobočky Kutná Hora

Na pobočce v Kutné Hoře pracují tři zaměstnanci, kteří nemají přístup na žádné síťové uložiště a veškerá data si předávají na externím HDD. Sdílení dat mezi pobočkami Znojmo – Kutná Hora nyní funguje také přes externí disk. Z důvodu neefektivity sdílení dat mezi pobočkami musí být zhruba 20 % projektů, které firma za rok navrhne, odmítáno.

Průměrná internetová konektivita na pobočce v Kutné Hoře je zohledněna v následující tabulce. Uvedené hodnoty jsou zprůměrovány z více měření.

Tabulka 3: Internetová konektivita pobočka Kutná Hora

(Zdroj: Vlastní zpracování)

Internetová konektivita	
Download [Mbps]	30
Upload [Mbps]	8

1.3 Analýza a klasifikace dat

Tato kapitola se zabývá analýzou dat. Analýza a klasifikace dat je důležitá pro vytvoření spolehlivé datové infrastruktury dle potřeb vedoucích pracovníků sdružení.

1.3.1 Struktura dat

Sdružení ORA nyní uchovává interní data, která se týkají vzniku sdružení, obsahují cenové nabídky, přijaté a vydané faktury. Tyto soubory jsou většinou ve formátu .pdf nebo .doc. Jedná

se o malé soubory, které se často neaktualizují. Většina dokumentů vznikla na pobočce ve Znojmě.

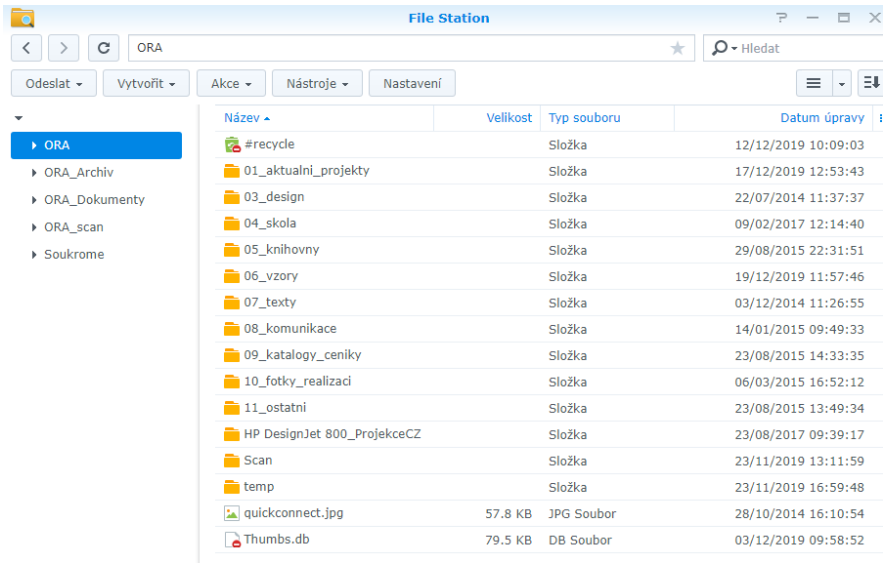
Další část dokumentů, které se denně aktualizují, se týká práce na projektech. Vytváření kvalitní dostupnosti dat mezi pobočkami bude záviset právě na velikosti a typu dat, které se týkají projektů. Je tedy nutné zanalyzovat typ dat a jejich velikost. Tyto údaje zobrazuje následující tabulka. Data týkající se projektů vznikají na obou místech, tedy na pobočce ve Znojmě i na pobočce v Kutné Hoře. Některé data vznikají i externě mimo tyto pobočky a následně se přenáší pomocí externího HDD do jednotlivých poboček, kde se s nimi dále pracuje.

Tabulka 4: Analýza dat projektů

(Zdroj: Vlastní zpracování)

Velikost projektu [GB]	5,5
Velikost souboru v projektu [MB]	350
Celkem rozpracovaných projektů [ks]	20
Současně otevřených projektů [ks]	6
Počet projektů za rok [ks]	40

V současné struktuře se nachází také archivní data, kde jsou staré projekty. Do těchto projektů se nahlíží jen zřídka a to na obou pobočkách. Tyto data jsou uložena ve složce „ORA_archiv“. Ve složce „ORA“ jsou aktuální projekty a podklady potřebné k jejich realizaci. Ve složce „Soukrome“ jsou soukromé složky všech uživatelů, kteří mají přístup na síťové uložiště. Do složky „ORA_scan“ se pak ukládají naskenované dokumenty ze síťové tiskárny umístěné na pobočce ve Znojmě.



Obrázek 3: Současná struktura dat

(Zdroj: Vlastní zpracování)

1.3.2 Ochrana dat

Momentálně jsou data na síťovém uložišti Synology přístupná všem pracovníkům sdružení. Architekt, který má mít přístup pouze ke svým rozpracovaným projektům, může prohlížet cenové nabídky nebo přijaté a vydané faktury. Takto nastavené oprávnění ke složkám je nepřípustné a může tak dojít k úniku citlivých informací. Únik citlivých informací společnosti může poškodit dobré jméno sdružení nebo umožnit konkurenčním firmám pracovat s interními daty sdružení ORA.

1.4 SWOT analýza současného stavu dostupnosti

Silné stránky

- Data nejsou přístupná z vnější sítě – eliminace napadení firemních dat
- Jednoduché používání systému
- Velmi levný způsob sdílení dat

Slabé stránky

- Vysoká hrozba ztráty dat
- Absence zálohování
- Slabé zabezpečení
- Jednoduché vynesení firemních dat třetí straně

Příležitosti

- Vytvoření vzdáleného přístupu VPN
- Možnost vytvoření veřejného cloudu
- Jednoduché rozšíření systému

Hrozby

- Ztráta nebo odcizení dat při přenášení na externím HDD
- Fyzické zničení uložiště
- Fyzické zničení disků v uložišti

1.5 Požadavky vedoucích pracovníků

Vedoucí pracovníci si přejí, aby:

- se využila kapacita stávajících zdrojů,
- došlo k rozšíření kapacity na vhodnou velikost,
- pracovníci mohli sdílet projekty mezi pobočkami,
- byla zajištěna bezpečnost dat,
- každý pracovník měl přístup pouze do předem definovaných složek,
- byla garantována kvalitní dostupnost dat mezi pobočkami i uvnitř každé pobočky.

1.6 Shrnutí analýzy

Po osobních setkáních s vedoucími pracovníky jsem provedl analýzu stávajícího stavu sítě, dostupnosti dat a zkonzultovali jsme nedostatky v oblasti bezpečnosti, zálohování i dostupnosti dat. Analýza prokázala absenci jakéhokoliv zabezpečení a na nutnost implementace zálohování a vytvoření kvalitní dostupnosti dat mezi pobočkou Znojmo a Kutná Hora pro zvýšení efektivity práce.

Na pobočce ve Znojmě si pracovníci ukládají veškerá firemní data na síťové uložiště Synology. Z analýzy vyplývá, že toto zařízení je nevyhovující pro práci více uživatelů a svým výkonem je absolutně nevyhovující do firemního prostředí. Veškerá data jsou uložena pouze na tomto zařízení a neexistuje tak žádná záloha těchto dat. V případě ztráty dat firma přijde o veškerá svá data a rozpracované projekty. Zařízení umožňuje pouze připojení dvou disků, lze tedy vytvořit nejvíce RAID 1, který je odolný vůči výpadku jednoho ze dvou disků. Dalším problémem je

také absence řízení přístupů k datům. Každý uživatel může prohlížet i citlivá firemní data. Zvyšuje se tak riziko vynesení těchto dat mimo pobočku. Společnost chce zajistit dostupnost dat mezi pobočkami Znojmo a Kutná Hora. Z měření rychlosti internetového připojení na pobočce ve Znojmě vyplývá, že rychlost je nevyhovující a je potřeba zajistit vyšší rychlost internetového připojení. Na pobočce v Kutné Hoře je absence jakéhokoliv síťového uložiště a data jsou předávána mezi pracovníky na externím disku. Tato metoda je velice neefektivní a nevhodná do firemního prostředí. Mezi pobočkami je nutné zajistit dostupnost dat, vytvořit plán záloh a vytvořit systém pro řízení přístupu k firemním datům.

Vedoucí pracovníci sdružení ORA kladou velký důraz na dostupnost dat mezi pobočkami, neboť v současné době musí odmítat zhruba 20 % projektů a nebrání se tak dražšímu finančnímu řešení. Po konzultacích jsou seznámení i s nutností zálohování a zabezpečení firemních dat.

2 TEORETICKÁ VÝCHODISKA PRÁCE

V teoretické části jsou vysvětleny základní pojmy důležité pro pochopení návrhu spolehlivé datové infrastruktury ve společnosti s více pobočkami. Tato část je nezbytná pro vytvoření reálného návrhu spolehlivé datové infrastruktury.

Teoretická část se zabývá způsobem ukládáním dat, poté umístěním a následně dostupností dat. Poté následuje důležitá kapitola s názvem řízení přístupu, kde jsou blíže popsány pojmy jako autentizace, autorizace a audit. V závěru práce je popsána teorie zabývající se řízením a ošetřením rizik.

2.1 Ukládání dat

Veškeré datové soubory, které jsou nutné uchovat, je potřeba uložit. Ukládání dat se provádí na záznamové médium. Existuje mnoho typů úložných médií, kde každé má svoje výhody či nevýhody. Uchování dat je možné provádět například na disketu, CD-ROM, HDD, USB flash disk apod.

2.1.1 Optická paměťová zařízení

Mezi optické paměťové zařízení řadíme například CD, DVD, Blu – Ray disky. Na CD lze uložit cca 700 MB dat, na DVD pak zhruba 4,7 GB. Blu – Ray disk pak umožní uložit data o velikosti 25 GB až 128 GB v závislosti na použité technologii. Ukládání na tyto média je však v současnosti vytlačeno jinými úložnými médii (Zdroj: 5).

2.1.2 HDD

Ukládání dat na HDD – hard disk drive je v současnosti jedno z nejuniverzálnějších a cenově nejvýhodnějších způsobů ukládání dat. Na tyto disky lze ukládat velké objemy dat. Typicky jsou tyto média o velikosti stovek GB či jednotek TB. Typicky se nachází v osobních počítačích, serverech, ve spotřební elektronice nebo také v přenosném formátu pod označením externí disk. Výhodou HDD je rychlost čtení a zápisu dat, relativně nízká cena, spolehlivá technologie nebo relativně malá velikost paměťového média. Nevýhodou HDD jsou pohyblivé části zařízení, které jsou náchylné na poškození. Na rozdíl od disků zvané SSD mají vyšší spotřebu elektrické energie a mají také nižší rychlost čtení a zápisu (Zdroj: 6).

2.1.3 SSD

SSD – solid state drive jsou podobně jako klasické HDD schopny pojmout velké množství dat. Na rozdíl od HDD však využívají flash paměť, což jim dává výhodu v rychlejším přístupu k datům než klasický pevný disk. Díky využití flash paměti nemají žádné pohyblivé části, proto jsou odolnější vůči otřesům, mají nižší elektrickou spotřebu a také nižší hlučnost. SSD jsou například v chytrých telefonech, noteboocích, ale i výkonnějších datových uložištích. Jejich nevýhodou je vyšší cena oproti HDD a omezený počet zápisů (Zdroj: 6).

2.2 Umístění dat

Data mohou být uložena na lokálním zařízení, na sdíleném uložišti, na které přistupují jednotliví uživatelé dle nastaveného oprávnění nebo na cloudovém uložišti.

2.2.1 Lokální uložiště

Ukládání dat na lokální zařízení je nejjednodušším způsobem, kdy se data ukládají na zařízení, na kterém uživatel pracuje. Nejčastěji například na disk umístěný v počítači. Výhodou je, že data má uživatel ve svojí správě. Data jsou přístupná i bez přístupu do internetu nebo do lokální sítě. Nevýhodou je, že data nejsou žádným způsobem zálohována a nejdou jednoduše sdílet mezi jednotlivými uživateli (Zdroj: 9).

2.2.2 Sdílené uložiště

Ukládání dat na sdílené uložiště je typ ukládání na specializované uložiště, které má přidělenou vlastní IP adresu a mohou k nim přistupovat klienti z počítačů či mobilních zařízení. Toto uložiště je přístupné z lokální sítě (LAN), ale po přidělení veřejné IP adresy se lze na zařízení připojit prakticky odkudkoliv. Na sdíleném uložišti je nutné nakonfigurovat přístupová práva jednotlivých uživatelů. Výhodou sdíleného uložiště je jednoduchá správa uložených dat. Nevýhodou je zakoupení vlastního hardware a v případě hrozby, jako mohou být například živelné katastrofy, odcizení hardware nebo napadení virem, dojde ke ztrátě dat (Zdroj: 8, s. 56).

2.2.3 Cloudové uložiště

Slovo „cloud“ lze přeložit jako oblak a v oblasti informačních technologií označuje výpočetní prostředky ležící mimo vnitřní síťovou infrastrukturu domácnosti či firmy. Americká organizace NIST označila cloud jako. „model, který umožní pohodlný a všudypřítomný přístup

ke sdíleným výpočetním zdrojům, které lze poskytnout rychle a s minimálním úsilím“ (Zdroj: 7).

Využívání cloudových služeb se stává trendem v oboru informačních technologií. Cloudové technologie poskytují velkou výhodu při způsobu ukládání dat, a to bezstarostnost a vysokou dostupnost dat. K datům se dá přistupovat odkudkoliv, pokud je k dispozici internetová konektivita. Mezi hlavní výhodu patří škálovatelnost, tedy v podstatě neomezeně velký datový prostor a výpočetní výkon. Velikou výhodou je také přenesení odpovědnosti za případnou nedostupnost nebo ztrátu dat poskytovateli cloudové služby. S využíváním je ovšem spjata řada nevýhod. Zejména poskytnutí dat třetí straně, platby za poskytnutou kapacitu a omezená rychlost. Data jsou uložena mimo lokální síť a jsou dostupná pouze tak rychle, jak rychlé je internetové připojení (Zdroj: 5).

Modely Cloudu

Veřejný cloud – je služba poskytovaná široké veřejnosti. U veřejného cloudu je infrastruktura vlastněna jeho provozovatelem a k poskytovaným službám přistupují zákazníci po síti prostřednictvím klientského rozhraní. Výhodou je poměrně nízká cena. Nevýhodou pak omezená možnost přizpůsobení si služby dle vlastních potřeb. Veřejný cloud poskytuje například Microsoft Azure, Dropbox, Google Drive (Zdroj: 8, s. 241).

Privátní cloud – cloud je v tomto případě provozovaný firmou nebo organizací. Službu poskytuje firma sama sobě nebo ji společnosti poskytuje třetí strana. Výpočetní infrastruktura může být umístěna v místě organizace nebo mimo ni. Výhodou tohoto modelu je vysoká škálovatelnost, samoobslužnost a automatizovaná správa. Privátní cloud eliminuje nevýhody veřejného cloudu, jeho cena je však řádově mnohem vyšší (Zdroj: 8, s. 244).

Hybridní cloud – tento typ cloudového řešení vznikl spojením veřejného a privátního cloudu. Tento typ umožňuje rozdělit výpočetní prostředky. Jedna skupina pracuje s modelem veřejného cloudu, druhá skupina s modelem privátního neboli soukromého cloudu. Tento model je vhodné využít například v případě, pokud společnost vyžaduje mít přístupná pouze z určitých míst a některá data odkudkoliv. Využitím může být sdílení dat mezi pobočkami, ale zároveň uchování dat pouze v některé pobočce firmy (Zdroj: 8, s. 244).

Komunitní cloud – u tohoto typu sdílí jednu infrastrukturu skupina uživatelů, která má stejné zájmy, cíle nebo požadavky (Zdroj: 8, s. 242).

Bezpečnostní hrozby v cloudu

Využití cloudového uložiště je stále častěji využívaná varianta a objevují se tak nové druhy hrozeb.

Hrozby mohou být následující:

- klonování a rychlé sdružování prostředků,
- pohyblivost dat,
- nešifrovaná data,
- prostředí veřejných cloudů je sdíleno různými nájemci,
- kontrola a dostupnost,
- způsob jakým útočníci zneužívají cloud (Zdroj: 4, s. 244).

2.3 Dostupnost dat

Dostupnost dat je schopnost přistupovat ke svým datum v očekávané kvalitě. Z pohledu poskytovatele služeb jde o poskytování dat s minimálním výpadkem a v očekávané kvalitě, která se nejčastěji stanovuje SLA smlouvou (Zdroj: 10, s. 11).

Narušení dostupnosti se označuje jako nedostupnost nebo nežádoucí zničení. Dostupnost je obvykle vyjádřena jako procento v daném časovém úseku. (Zdroj: 11).

Tabulka 5: Dostupnost dat

(Zdroj: Vlastní zpracování dle: 11)

Dostupnost [%]	Doba výpadku
90	36,5 hodin
95	18,25 hodin
98	7,3 hodin
99	3,65 hodin
99,5	1,83 hodin
99,8	17,52 hodin
99,9	8,76 hodin

99,99	52,6 minut
99,999	5,26 minut
99,9999	31,5 sekund

I když je obvyklé uvádět dostupnost dat v procentech, je vhodné využívat ukazatele, které vyjadřují dobu obnovení systému ku množství dat, o které může uživatel přijít (Zdroj: 11).

RTO – Recovery Time Object **–** Doba obnovení systému. Za jak dlouho po výpadku budou data dostupná (Zdroj: 11).

RPO –Recovery Point Objective – Jaké množství dat může být ztraceno od vymezeného okamžiku (Zdroj: 11).

RT – Recovery Time – čas potřebný k obnově (Zdroj: 11).

Dostupnost dat je měřena následovně:

- **Data nejsou dostupná** – Pokud uživatel nemůže přistupovat ke svým datům, je služba nedostupná. Situace je způsobena chybou na straně uživatelské stanice, internetovou konektivitou nebo napadením služby hackerem (Zdroj: 10, s.11).
- **Systém pracuje velmi pomalu** – Data jsou dostupná s velkým zpožděním. Uživatel vzdává čekání a považuje data za nedostupná (Zdroj: 10, s.11).
- **Systém má časté problémy** – Uživatel si vybere systém, který nesplňuje jeho požadavky a má časté výpadky (Zdroj: 10, s.11).

Dostupnost dat se dá zajistit redundancí v místě primárního uložení, například vytvořením RAID pole nebo na sekundárním uložišti, kde není přístup uživatelů. Jedná se například o zálohu s následnou možností obnovení na primární uložiště. Je důležité zanalyzovat, proti jakým incidentům je potřeba čelit. Může to být například selhání HW nebo SW, havárie úložného média, nedostupnost sítě, uživatelské smazání dat apod (Zdroj: 10, s.11).

2.3.1 Zálohování dat

Zálohování dat je nedílnou součástí všech firem i domácností. Zálohování je proces, při kterém se ukládají data z provozních médií na zálohovací média. Pokud budou data ztracena nebo poškozena, je možné je obnovit ze zálohy. Data mohou být smazána neúmyslně uživatelem

nebo mohou být napadeny viry. Důležitá data je tedy potřeba ochránit před jejich ztrátou. Proto je důležité dělat pravidelně zálohy svých dat (Zdroj: 3, s. 2).

Rizika ztráty dat:

- porucha hardware,
- softwarové útoky,
- lidský faktor,
- živelné pohromy (Zdroj: 4, s. 325).

Lidský faktor představuje nejvyšší míru rizika. Nejčastější důvody ztráty dat jsou způsobeny například neúmyslným smazáním dat uživatelem, chyba obsluhy, chyba aplikace, ztráta integrity dat atd (Zdroj: 4, s 325).

Vzniklé škody mohou být následujícího charakteru:

- přímá ztráta,
- ztráty lidských zdrojů – znovupořízení dat,
- ztráta konkurenceschopnosti,
- ohrožení existence organizace. (Zdroj: 4, s. 325).

Faktory, které ovlivní způsob zálohování:

- požadavky na objem dat,
- čas potřebný pro zálohování,
- čas potřebný pro obnovu záloh,
- stav sítě, serverů, databází, apod (Zdroj: 4, s 325).

Zálohování dat můžeme dělit na:

- průběžné zálohování, kde se veškerá data okamžitě zrcadlí do jiné jednotky, jakmile dojde k jejich změně
- trvalá archivace – data se v pravidelných intervalech zálohují pokaždé na nové médium a tato média jsou následně archivována. Často vyplývá ze zákona uchovávat určitá data po nějakou dobu.
- Cyklické zálohování – data se v pravidelných cyklech ukládají na několik médií, které se střídají (Zdroj: 4, s. 329).

Úplná záloha

Tento typ zálohy kopíruje všechny vybraná data na záložní médium a označí je jako zálohované. Označení provádí zálohovací program, který všem souborům vynuluje nastavení archivačního atributu. Tento typ zálohy se též nazývá jako normální záloha a je nejjednodušší variantou. Obnova dat je velmi snadná (Zdroj: 4, s. 330).

Přírůstková záloha

Metoda se též nazývá inkrementální záloha a dovoluje zálohovat pouze soubory změněné od poslední normální (úplné) zálohy nebo zálohy inkrementální. Přírůstková metoda také označuje soubory jako zálohované a nastaví jim archivační atribut. Metoda pracuje s menším objemem dat, je proto mnohem rychlejší. Nevýhodou je však obtížnější obnova dat, protože musíme mít k dispozici nejen všechny přírůstkové zálohy, ale také plnou zálohu, což může být mnohdy komplikací (Zdroj: 4, s. 330).

Rozdílová záloha

Rozdílová záloha se nazývá diferenciální a používá se pro zálohování souborů změněných od poslední normální nebo inkrementální zálohy. Liší se v tom, že pro obnovu potřebujeme poslední úplnou zálohu, poslední přírůstkovou zálohu a všechny rozdílové zálohy od poslední úplné nebo inkrementální zálohy (Zdroj: 4, s. 330).

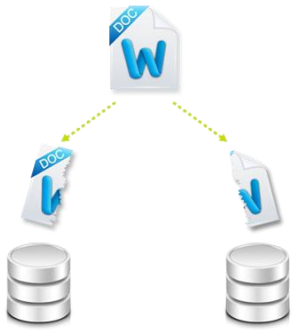
2.3.2 Disková pole RAID

RAID je zkratka anglického Redundant Array Independent Disks. Je to metoda, která slouží k ukládání dat na více disků. Vytvoření RAID snižuje chybovost a zvyšuje výkonnost. Existuje několik typů RAID, z nichž všechny jsou postaveny na stejných principech. Jedná se buď o zrcadlení (opakování zápisu na jinou jednotku), dělení (rozdělení dat na více jednotek) nebo paritě (Zdroj: 1, s. 513).

RAID 0

RAID 0 se často označuje jako stripping (dělení). Tento typ dělí data na bloky a ty umisťuje na více jednotek. To zvyšuje výkonnost, protože se zvyšuje šance, že požadovaná data se budou nacházet na jiných jednotkách. To znamená, že ke čtení dat může docházet najednou z více jednotek. Obecně tedy platí, že čím více jednotek se používá, tím vyšší je výkon. RAID 0 však

neumožňuje selhání žádného z disků, dokonce možnost selhání zvyšuje, protože se data ukládají na více jednotek, které mohou selhat a znepřístupnit tak data (Zdroj: 1, s. 514).

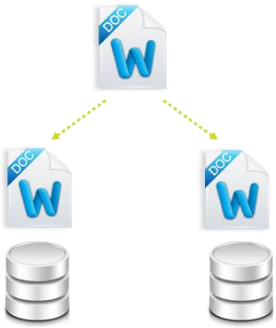


Obrázek 4: RAID 0

(Zdroj: 2)

RAID 1

Typ RAID 1 se často označuje jako „mirroring“ – zrcadlení. Stejná data jsou ukládána na jinou jednotku. Tím se zvyšuje odolnost vůči chybám, protože stejná data jsou uložena na jiné jednotce. Výkon zápisu je nízký, neboť data jsou ukládána na více jednotek současně. Čtení je rychlejší jak zápis, protože je možné číst z více jednotek současně. K implementaci RAID 1 je nutné mít alespoň dvě jednotky (Zdroj: 1, s. 514).



Obrázek 5: RAID 1

(Zdroj: 2)

RAID 5

Tento typ poskytuje jak toleranci při závadě, tak zajišťuje vyšší výkon pro čtení. K jeho realizaci jsou zapotřebí alespoň tři disky. Typ RAID 5 umožňuje selhání jedné jednotky.

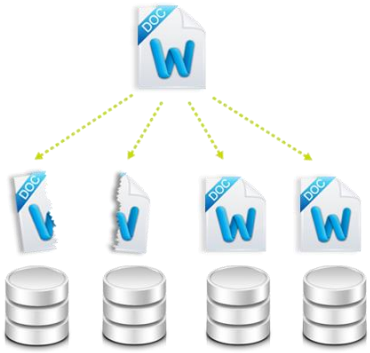
V případě selhání jednotky se data rekonstruují pomocí parity na ostatních discích. Toto diskové pole je vhodné využít tam, kde je kapacita důležitější než výkon (Zdroj: 2).

Obrázek 6: RAID 5

(Zdroj: 2)

RAID 6

RAID 6 je velmi podobný RAID 5, avšak poskytuje jinou úroveň proužkování a umožňuje selhání dvou jednotek. K jeho realizaci jsou však zapotřebí alespoň čtyři disky. RAID 6 je díky zvýšené toleranci proti selhání disku méně výkonný než RAID 5 (Zdroj: 2).

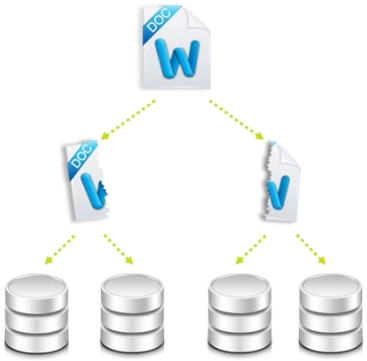


Obrázek 7: RAID 6

(Zdroj: 2)

RAID 10

RAID 10 je kombinací typu RAID 1 a RAID 0. Nabízí všechny výkonnostní výhody dělení a také odolnost vůči chybám díky zrcadlení disků. K implementaci se vyžadují čtyři jednotky. RAID 10 unese několik závad, avšak za předpokladu, že k závadám nedojde ve stejné podskupině. Typ RAID 10 se hodí tam, kde jsou časté požadavky na čtení, zápis dat a vyžadujeme vysokou ochranu vůči selhání některé z jednotek. (Zdroj: 1, s. 516)



Obrázek 8: RAID 10

(Zdroj: 2)

2.4 Řízení přístupu

Řízení přístupů k IS/ICT popisuje norma ČSN ISO/IEC 27001 a lze jej rozdělit na:

- řízení přístupu uživatelů pomocí přístupových práv,
- řízení přístupu k síti a k síťovým službám,
- řízení přístupu k operačnímu systému,
- řízení přístupu k aplikacím,
- řízení dálkového přístupu (Zdroj: 4, s. 116).

Základními principy k řízení přístupu jsou autentizace a autorizace a audit. Autentizace je ověření identity entity nebo zprávy. Součástí tohoto procesu je i proces identifikace. Identifikace označuje rozpoznání entity. Proces autorizace zahrnuje ověření oprávnění pro vstup do nějakého systému nebo aplikace. Pro proces autorizace je nutná úspěšná autentizace (Zdroj: 4, s. 116).

2.4.1 Autentizace

Autentizace je pojem v oblasti řízení bezpečnosti a znamená ověření identity nějakého subjektu. Autentizace zjišťuje, zda je subjekt ten, za který se vydává.

Existují tři základní způsoby autentizace a to:

- **dle toho, co subjekt má** – například identifikační karta, klíč, platební karta, token,
- **dle toho, co zná** – například pin, heslo,
- **dle toho, čím je** – do této skupiny patří biometrické údaje – oční sítnice, otisk prstu (Zdroj:11).

Autentizace pomocí hesla

Silné stránky

- nevyžaduje speciální HW nebo SW při přihlášení uživatele,
- uživatel se může přihlásit odkudkoliv,
- ochranu hesel zesilují kryptografické systémy,
- jednoduché a levné používání,
- pohodlný, rychlý, snadno zapamatovatelný způsob,
- automatické generování hesel,
- bezpečnostní příručka,
- používání delších hesel,
- kombinace alfanumerických znaků,
- kombinace s jinou autentizační metodou (Zdroj: 13).

Slabé stránky

- uživatelé si musí pamatovat své heslo,
- jsou kladeny vysoké nároky na paměť uživatele,
- systém je závislý na uživateli (nejslabší složkou systému je lidský faktor),
- používání mnoha hesel,
- slabá forma ochrany,
- odchycení hesla speciálním software,
- uhádnutí, prolomení ochrany,
- většina uživatelů používá do všech systémů stejná hesla,
- velká šance na prolomení hesla,
- krádež identity (Zdroj: 13).

Autentizace pomocí tokenu

Silné stránky

- rychlá zjistitelnost ztráty tokenu,
- úspěšná autentizace je podmíněna použitím tokenu,
- informaci nelze tak snadno šířit jako heslo,
- nelze snadno zkopírovat,

- žádné úpravy na straně klienta,
- obtížné kopírování,
- bezpečně uložené informace,
- při opakované špatné autentizaci lze zablokovat přístup,
- při pokusu o násilné vniknutí do tokenu některé zařízení sami zničí informaci (Zdroj: 13).

Slabé stránky

- fyzická ztráta, zničení,
- mechanické poškození,
- autentizace není možná pokud uživatel nemá token u sebe,
- potřeba token fyzicky vlastnit,
- softwarové chyby,
- v případě poruchy uživatel nemůže provést autentizaci (Zdroj: 13).

Autentizace pomocí biometriky

Silné stránky

- vysoce bezpečný způsob ověření,
- vysoká spolehlivost,
- využití více faktorové autentizace,
- nízká míra oklamání systému,
- informace nemůže být ukradnuta, zničena,
- prosazuje se ve veřejném sektoru,
- uživatel si nemusí pamatovat žádné informace,
- biometrické ověření není tajné (na rozdíl od hesla) (Zdroj: 13).

Slabé stránky

- některé charakteristiky podléhají změnám – hlas, podpis apod.,
- stoprocentní ověření není možné,
- tato metoda se stále vyvíjí – přesnost, rychlost,
- nutnost neustálé údržby přístupového systému,
- nemožnost registrace všech osob,

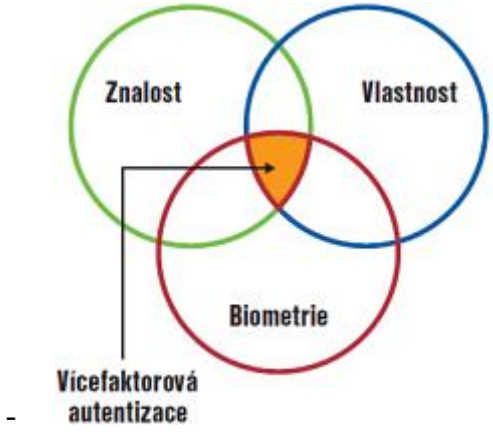
- odpor některých uživatelů – nechtějí se podrobit měření biometrických znaků, ukládání dat do systému,
- biometrická data nejsou tajná,
- mohou výrazně narušit soukromí uživatele,
- nedostatečná legislativní úprava,
- obsahují mnoho citlivých informací (Zdroj: 13).

Každá tato metoda má své výhody či nevýhody. Autentizace patří mezi bezpečnostní opatření, které zabraňuje přístupu pod falešnou identitou. Pokud chceme zvýšit míru důvěry autentizace, lze kombinovat více jejich faktorů (Zdroj: 11).

Jedno faktorová autentizace – k ověření dojde pouze podle něčeho, co uživatel má – například uživatelské jméno a heslo (Zdroj: 11).

Dvou faktorová autentizace – znamená, že dojde ještě navíc k označení podle toho, co uživatel má, například mobilní zařízení, na které dojde potvrzovací SMS. Typicky u přístupu do internetového bankovnictví (Zdroj: 11).

Tří faktorová autentizace – ověřuje navíc i něco, co je spojené s člověkem, tedy nějaké biometrické prvky (Zdroj: 11).



Obrázek 9: Více faktorová autentizace

(Zdroj: 12)

2.4.2 Autorizace

Autorizace znamená povolení k nějaké operaci, zda může subjekt nějakou činnost nebo operaci provést. V procesu kontroly navazuje na autentizaci. Autorizace patří mezi bezpečnostní opatření a zajišťuje ochranu před neoprávněným přístupem. V informatice je nedílnou součástí

k řízení přístupových oprávnění k datům, souborům apod. V informatice je autorizace většinou automatizovaná a provádí ji operační systém nebo specializovaný software na základě seznamu pro řízení přístupu. Rozsah oprávnění je obvykle vyjádřen v nějakém dokumentu, který definuje rozsah pravomocí, povolení a přístupů (Zdroj: 11).

2.4.3 Účtování

Účtování je procesem po autentizaci a autorizaci. Proces účtování se týká evidence a sledování uživatelských činností v počítačové síti a následně jejich zápis. Tyto informace slouží například pro podávání různých zpráv. Tyto zprávy mohou zahrnovat čas strávený v síti, použité síťové služby, analýzu kapacity, alokaci síťových nákladů. Dá se tedy evidovat počet paketů, bajtů apod. Servery, které pracují s AAA protokolem jsou například RADIUS server, KERBEROS server, TACASC server (Zdroj: 4, s. 116).

2.5 Technologie zabezpečení přístupu

Tato kapitola se zabývá technologií zabezpečení přístupu. V této kapitole bude popsána technologie VPN, VLAN a šifrování dat.

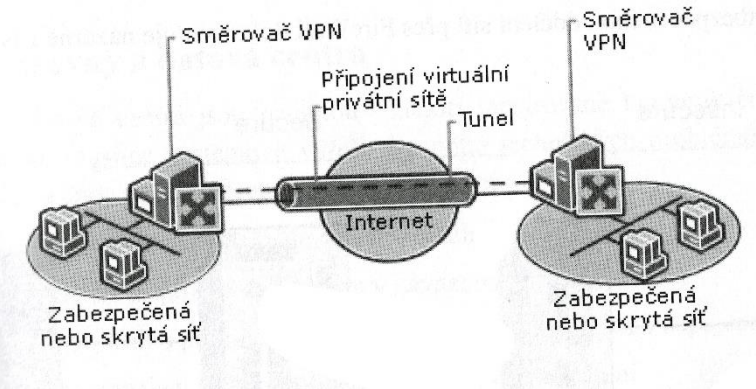
2.5.1 VPN

Internet byl od počátku navržen jako nebezpečný, neboť IPv4 neobsahuje žádný mechanismus, kterým by bylo možné zajistit komunikaci proti odposlechu nebo záměně. Postupem se do internetových technologií a protokolů zavádějí způsoby, jakým tohoto zabezpečení dosáhnout, jedním z těchto principů je například VPN tunel (Zdroj: 21).

VPN (Virtual Private Network) neboli virtuální privátní síť lze implementovat ve dvou typech. Prvním typem je „Client to site“, což je implementace VPN serveru, který umožňuje přístup do vnitřní sítě uživatelům v internetu. Na uživatelské stanice je nutné nainstalovat softwarového klienta. Pokud se uživatel připojí odkudkoliv z internetu do VPN sítě, ocitnou se v místní firemní síti, jako by byli připojeni uvnitř firemní sítě a mohou přistupovat k firemním datům, sdíleným diskům apod (Zdroj: 14, s. 232).

Druhým typem je implementace „Site to site“. Tento typ umožňuje propojení celých sítí. Například propojit firmu v lokalitě A s firmou v lokalitě B. Data, která se mezi sítěmi přenáší jsou automaticky šifrována, avšak stále posílána nezabezpečeným internetem. Implementací tohoto typu VPN připojení tak lze například sdílet firemní data mezi vzdálenými lokalitami (Zdroj: 4, s. 284).

Tento typ připojení VPN charakterizují vlastnosti jako zapouzdření, ověřování a šifrování. Připojení propojuje dvě části privátních sítí. Server VPN poskytuje směrované připojení k síti, ve které je server připojen. VPN klient se ověří VPN serveru a z důvodu vzájemného ověření dojde i k k tomu, že se odpovídající směrovač ověří volajícímu směrovači (VPN serveru) (Zdroj: 15, s. 16).



Obrázek 10: VPN tunel

(Zdroj: 15, s. 17)

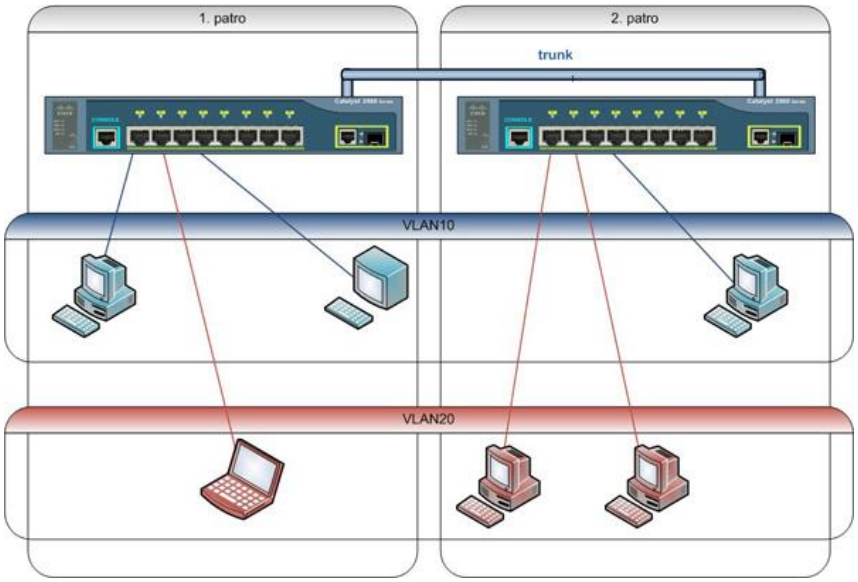
2.5.2 VLAN

VPN umožňuje zabezpečené připojení přes veřejnou síť, VLAN neboli virtuální LAN síť, umožňuje logicky oddělit vnitřní síť nezávisle na fyzickém uspořádání, neboť dojde k oddělení komunikace a každá VLAN může mít přístup do své části sítě (Zdroj: 16).

Vytváření VLAN probíhá podle organizační struktury, kdy pracuje jedno oddělení společně a využívají stejné zdroje jako jsou tiskárny, datové servery apod. Dalším typem je oddělení podle služeb. Do VLAN je vhodné seskupit uživatele, kteří využívají stejné zdroje, jako je například účetnictví, různé databáze apod. Pro zařazení do VLAN se nejčastěji používá metoda statická a dynamická. Dále existuje metoda přiřazení do VLAN pomocí protokolu nebo podle autentizace (Zdroj: 16).

Statická metoda je metodou, kde každý z portů je ručně nakonfigurován do určité VLAN. Je to nejrychlejší a nejpoužívanější řešení, neboť je tato metoda jednoduchá z hlediska správy (Zdroj: 17, s. 269).

Dynamická metoda využívá fyzické adresy zařízení. Je nutné tedy udržovat tabulku MAC adres pro každé zařízení a k němu přiřazená VLAN. Výhodou tohoto typu je to, že pokud se zařízení přepojí do jiného portu, bude stále ve správné VLAN (Zdroj: 17, s. 269).



Obrázek 11: Zařazení koncových zařízení do VLAN

(Zdroj: 16)

2.5.3 Šifrování dat

Šifrování dat považují odborníci na kybernetickou bezpečnost za nejspolehlivější řešení. Moderní šifrovací nástroje používají aktivně tři metody zabezpečení dat pomocí kryptovacích algoritmů. Jedná se o souborové šifrování dat, celodiskové šifrování a šifrování virtuálního disku (Zdroj: 18).

Souborové šifrování dat pracuje na principu zabezpečení určité části disku, například profilu uživatele, určitých adresářů nebo souborů. Metoda funguje na principu, pokud má uživatel šifrovací klíč, pak má přístup k datům. Ve srovnání s celodiskovým šifrováním jsou kladeny menší požadavky na hardwarové prostředky. V tomto případě jsou chráněna pouze data, která chce uživatel chránit (Zdroj: 18).

Celodiskové šifrování zabezpečuje celý pevný disk nebo jeho logickou jednotku. Výhodou je, že uživatel neovlivňuje, zda se soubor uloží šifrovaně či nikoliv. Celodiskové šifrování zašifruje celý disk včetně jeho prázdného místa. Díky tomuto typu šifrování není možné bez znalosti klíče přečíst například strukturu disku. Nevýhodou je vyšší nárok na hardwarové prostředky.

Mezi software, které umožňují šifrování celého disku patří například BitLocker, TrueCrypt, WinMagic a jiné (Zdroj: 18).

Šifrování virtuálního disku využívá alokování určitého místa na disku, které se v systému připojí jako fyzický disk. Uživatel do tohoto disku může jednoduše ukládat data, která potřebuje šifrovat. Výhodou je, že tato metoda stojí mezi metodou souborového šifrování a celodiskového šifrování. Kapacita virtuálního disku roste podle potřeb uživatele a klade tak menší důraz na hardware, protože nedochází k šifrování celé jednotky. S diskem může pracovat více uživatelů, které je však nutné předem definovat (Zdroj: 18).

2.6 Řízení rizik

Riziko znamená vystavení se nepříznivým okolnostem. Tento pojem lze definovat také jako pravděpodobnost či možnost vzniku ztráty, odchýlení skutečných a očekávaných výsledků, nebezpečí negativní odchylky od cíle a jiné. Řízením rizik se zabývá norma ISO 27 000 (Zdroj: 21, s. 47).

Analýza rizik zahrnuje kroky:

1) identifikace aktiv – vymezení popisovaného subjektu, aktiva,
2) stanovení hodnoty aktiv – určení hodnoty a jejich význam pro subjekt. Ohodnocení dopadu ztráty, změny nebo poškození aktiva,
3) identifikace hrozeb a slabin – určení druhů událostí a akcí, které mohou negativně ovlivnit hodnotu aktiv,
4) stanovení závažnosti hrozeb a míry zranitelnosti – určení pravděpodobnosti výskytu hrozby s míry zranitelnosti subjektu vůči vzniklé hrozbě (Zdroj: 20, s. 51).

Identifikace aktiv lze nejlépe popsat tabulkou. K hodnocení je třeba využít stupnici hodnoticích kritérií, například 1-5, kde 5 je nejdůležitější aktivum (Zdroj: 4, s. 267).

Identifikace hrozeb a zranitelnosti vytváří tabulku s uvedením pravděpodobnosti hrozeb a zranitelnosti. K hodnocení je třeba využít stupnici hodnotících kritérií na škále 1-5, kde 5 je nejpravděpodobnější hrozba (Zdroj: 4, s. 267).

Stanovení závažnosti hrozeb a míry zranitelnosti k této části lze přistupovat maticovou metodou. Tato analýza využívá matice aktiv hrozeb a zranitelností (Zdroj: 4, s. 267).

Postup zahrnuje následující kroky:

1) vytvoření matice zranitelnosti spojením tabulek identifikace aktiv a tabulky hrozeb a zranitelností,
2) posouzení zranitelnosti aktiv a doplnění do matice,
3) výpočet míry rizika vztahem R= T*A*V, kde R – míra rizika, T – pravděpodobnost vzniku, A – hodnota aktiva, V – zranitelnost aktiva,
4) stanovením hranic rizika (nízká, střední, vysoká) (Zdroj: 4, s. 267).

Po procesu analýzy rizik je nutné rizika vyhodnotit a vybrat optimální opatření ke snížení rizika. Poslední fází je rozhodovací fáze, ve které je nutné zvolit vhodný způsob zvládání rizika, například transferem, pojištěním, vyhnutím se rizika, podstoupením apod (Zdroj: 21).

Obrázek 12: Řízení rizik

(Zdroj: 21)

2.6.1 Ošetření rizik

Cílem ochrany rizik je vytvořit balíček ochranných opatření některých nebo všech IT systémů. Mezi základní rozlišení patří preventivní bezpečnostní opatření, detekce a reakce a podpůrná opatření. Bezpečnostní opatření informačních systémů se dělí na oblasti řízení a správy bezpečnosti, bezpečnosti provozního prostředí a na technologickou bezpečnost (Zdroj: 4, s. 100).

Norma ČSN ISO/IEC 27002:2005 popisuje řízení bezpečnosti informací, která je východiskem pro vytvoření bezpečnostních opatření. Norma obsahuje opatření rozdělená do 11 kategorií a to:

- A.5 – bezpečnostní politika,
- A.6 – organizace bezpečnosti,

- A.7 – řízení aktiv,
- A.8 – bezpečnost lidských zdrojů,
- A.9 – fyzická bezpečnost a bezpečnost prostředí,
- A.10 – řízení komunikací a řízení provozu,
- A.11 – řízení přístupu,
- A.12 – akvizice, vývoj a údržba informačního systému,
- A.13 – zvládání bezpečnostních incidentů,
- A.14 – řízení kontinuity činností organizace,
- A.15 – soulad s požadavky (Zdroj: 4, s. 104).

Strategie ošetření rizik

U každého rizika je nutné zvolit strategii, jakou postupovat k jeho ošetření. Riziko lze:

- **podstoupit** – to znamená, že se riziko nebude žádným způsobem ošetřovat, protože pravděpodobnost nebo dopad rizika je akceptovatelná,
- **zmírnit** – tato metoda se zabývá snížením rizika pomocí různých opatření, abychom odstranili příčinu nebo ji zmírnili na přijatelnou úroveň,
- **vyhnout se** – riziku znamená, že se neuskuteční jeho záměr, tedy se riziko vůbec nepodstoupí. Například se neuskuteční velmi rizikový projekt (Zdroj: 11).

2.6.2 Metoda RIPRAN

Metoda RIPRAN slouží k analýze a procesu řízení projektových rizik. Proces by se dal označit jako vazba vstup na výstup, kdy vstup je začátek procesu a výstup je výsledek s určitým cílem. Proces metody RIPRAN zahrnuje tyto kroky:

1) příprava analýzy rizik,
2) identifikace rizik,
3) kvantifikace rizik,
4) zpětná vazba na rizika,
5) celkové zhodnocení rizik (Zdroj: 19).

Metoda RIPRAN se zapisuje do tabulky, kde se popíšou jednotlivé hrozby, které se následně ohodnotí, následně se popíše scénář a dopad. Na základě ohodnocení se určí celková hodnota

rizika a na ni se naváže vhodné opatření. Cílem metody RIPRAN je na základě informovanosti připravit opatření, která sníží hodnotu jednotlivých rizik na akceptovatelnou úroveň (Zdroj: 19).

Tabulka 6: Popis tabulky RIPRAN

(Zdroj: Vlastní zpracování)

Zkratka	Popis
MP	Malá pravděpodobnost
SP	Střední pravděpodobnost
VP	Velká pravděpodobnost
MD	Malý dopad
SD	Střední dopad
VD	Velký dopad
MHD	Malá hodnota rizika
SHD	Střední hodnota rizika
VHD	Velká hodnota rizika

Následující tabulka vychází ze vzorce, kde celkový dopad = pravděpodobnost hrozby * pravděpodobnost scénáře.

Tabulka 7: RIPRAN celkový dopad

(Zdroj: Vlastní zpracování)

	MP	**SP**	**VP**
MP	MD	MD	SD
SP	MD	SD	VD
VP	SD	VD	VD

Tabulka celkové hrozby rizika vychází ze vzorce, kde celkové hodnocení rizika = Celková pravděpodobnost * Celkový dopad.

Tabulka 8: RIPRAN celková hodnota rizika

(Zdroj: Vlastní zpracování)

	MD	**SD**	**VD**
MP	MHR	MHR	SHR
SP	MHR	SHR	VHR
VP	SHR	VHR	VHR

3 VLASTNÍ NÁVRHY ŘEŠENÍ

Tato kapitola se zabývá návrhem řešení, které vyplývá z analýzy současného stavu a opírá se o teoretickou část. V kapitole vlastního návrhu řešení je popsán funkční návrh řešení včetně jejich ekonomického zhodnocení a výhod či nevýhod zavedení projektu. Součástí vlastního návrhu je i časový harmonogram projektu a popsání rizik metodou RIPRAN.

3.1 Specifikace požadavků

Pro zajištění vysoké dostupnosti dat je nutné nejdříve specifikovat požadavky. Tato kapitola se týká kapacity uložiště a možnosti zálohování.

3.1.1 Kapacita uložiště

Z analýzy vyplynulo, že kapacita uložiště, které je v momentálně umístěné na pobočce ve Znojmě je nevyhovující. Každý projekt má průměrně 5,5 GB a za rok se zpracuje zhruba 40 projektů. Vzhledem ke zvyšujícím se nárokům na kapacitu a možnému rozšíření firemních kapacit navrhuji zvýšit kapacitu uložiště na velikost 8 TB. Tato kapacita by měla mít dostatečnou rezervu pro případy zvýšeného nároku na kapacitu uložiště v následujících letech.

3.1.2 Zálohování firemních dat

Z analýzy současného stavu popsaného v 1. kapitole, je zřejmé, že v současné době nejsou data žádným způsobem zálohována.

Data mohou být zálohována úplnou zálohou, přírůstkovou nebo rozdílovou. Vzhledem k povaze a objemu firemních dat doporučuji kombinaci úplné zálohy a zálohy přírůstkové – inkrementální.

První den v týdnu doporučuji udělat zálohu úplnou a každý následující den udělat pouze přírůstkovou zálohu. Přírůstková záloha je velmi rychlá, neboť zálohuje pouze soubory změněné od poslední úplné nebo inkrementální zálohy. Nevýhodou je, že společnost musí mít k dispozici jak veškeré zálohy úplné, tak inkrementální.

Zálohování dat doporučuji provádět vždy po skončení pracovní doby. Pracovní doba končí v 18:00, doporučuji nastavit zálohování dat na 03:00.

3.2 Umístění uložiště dat

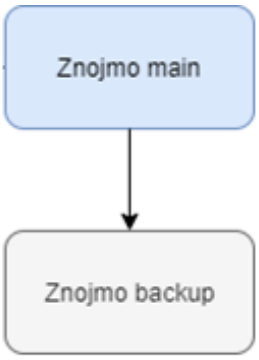
Z důvodu současné nevyhovující situace v umístění dat, kdy jsou data umístěna pouze na pobočce ve Znojmě a není tak zajištěna žádná dostupnost s pobočkou v Kutné Hoře, je nutné implementovat vhodný návrh řešení pro zlepšení stávající situace. Prvním krokem k zajištění vysoké dostupnosti dat mezi pobočkami Znojmo a Kutnou Horou je zvolení způsobu, jak a kde budou data ukládána. Možností je více. Data mohou být uložena pouze na jedné z poboček a následně k nim využívat vzdálený přístup. Druhou variantou je umístit lokální uložiště na pobočku ve Znojmě i v Kutné Hoře a data vzájemně replikovat. Dalším vhodným řešením je umístit data do cloudu, tedy na pobočkách nebude žádné lokální uložiště. Vhodným řešením je i kombinace předchozích variant, tedy využívat cloudové i lokální uložiště.

3.2.1 Varianta 1: Lokální uložiště na jedné z poboček

Z analýzy provedené ve sdružení ORA vyplývá, že práce s firemními daty a jejich dostupnost je nedostatečná a je potřeba učinit zásadní kroky ke zlepšení stávající situace. Tato kapitola se zabývá návrhem řešení, ve kterém budou data umístěny na lokální síti sdružení, a to pouze na jedné z poboček.

Vzhledem k tomu, že na pobočce ve Znojmě je mnohem více zaměstnanců než v Kutné Hoře, je vhodné umístit zařízení na pobočku ve Znojmě, neboť zde bude nejvíce uživatelů přistupovat přes lokální síť.

Data je nutné pravidelně zálohovat na jiné zařízení. Kvůli rychlosti záloh je vhodné umístit zálohovací zařízení také na pobočku ve Znojmě. To s sebou však nese nevýhodu zejména v bezpečnosti. Pokud bude napadena firemní síť na pobočce ve Znojmě, útočník se může jednoduše dostat také na zálohovací zařízení.



Obrázek 13: Lokální umístění dat na znojemské pobočce

(Zdroj: Vlastní zpracování)

Výhody:

- nízké pořizovací náklady,
- jednoduchá implementace,
- v případě výpadku uložiště lze data jednoduše obnovit,
- jednoduché rozšíření systému.

Nevýhody:

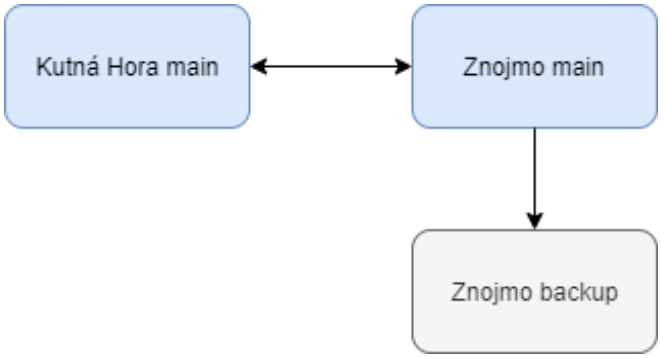
- zálohovací zařízení je ve stejné síti jako firemní uložiště – nízká bezpečnost,
- uživatelé z Kutné Hory musí na zařízení přistupovat vzdáleně – dostupnost závisí na internetové konektivitě,
- při výpadku internetové konektivity na pobočce jsou data mimo pobočku nedostupná,
- nutnost fyzicky kontrolovat zálohovaná data,
- pravidelná výměna HW.

3.2.2 Varianta 2: Lokální uložiště na více pobočkách se vzájemnou replikací

Zajištění vhodné dostupnosti dat bude dosaženo umístěním síťového uložiště na každé pobočce. Uživatelé tedy svá data budou mít přímo na své pobočce, a tak tedy není nutné k nim přistupovat z internetové sítě. Samozřejmě je nutné zajištění replikace dat mezi pobočkami, aby na každé pobočce byla vždy aktuální data. Tímto krokem se docílí toho, že každý pracovník na konkrétní pobočce bude přistupovat ke svému projektu z lokální sítě a rychlost přístupu je tak omezena pouze na síťovou infrastrukturu na každé pobočce. Uživatel bude využívat internetovou

konektivitu v případě, že se bude připojovat do lokálního uložiště mimo firemní síť. Je nutné připojovat se pomocí VPN tunelu nebo pomocí cloudové služby.

Lokální uložiště umístěné na obou pobočkách budou fungovat na principu replikace dat mezi pobočkami. Pokud by však došlo ke smazání, přepsání dat nebo napadením některého ze zařízení, dojde k replikaci těchto poškozených dat na obě zařízení a následně tak dojde ke znehodnocení firemních dat. Proto je nutné umístit alespoň na jednu z poboček zařízení, na kterou se budou provádět pravidelné zálohy pro případ zavirování, smazání dat. Propojení těchto uložišť ukazuje následující obrázek.



Obrázek 14: Lokální umístění dat se vzájemnou replikací mezi pobočkami

(Zdroj: Vlastní zpracování)

Výhody:

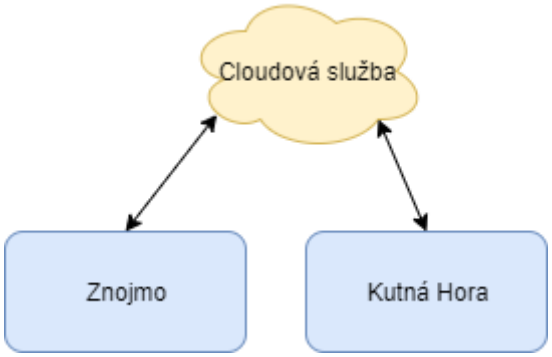
- relativně nízká pořizovací cena,
- zajištění vysoké dostupnosti dat,
- možnost přistupovat k datům mimo firemní síť,
- rychlá implementace,
- při práci na pobočce není nutné využívat internetovou konektivitu pro přístup k datům.

Nevýhody:

- zakoupení vlastního HW,
- v případě přepsání dat na jedné pobočce se data replikují na druhou a dojde tak ke znehodnocení dat,
- nutnost pravidelně měnit HDD v zařízeních,
- fyzické kontrolování zálohovaných dat.

3.2.3 Varianta 3: Cloudové uložiště

Další možností umístění dat je využití cloudových služeb. Data budou umístěna pouze v cloudové službě a uživatelé budou přistupovat přes internetovou konektivitu přímo na cloudovou službu. Grafické znázornění přístupu dat mezi jednotlivými pobočkami je znázorněno na následujícím obrázku.



Obrázek 15: Umístění uložiště v cloudu

(Zdroj: Vlastní zpracování)

Výhody:

- využívání cizích zdrojů – není nutné kupovat vlastní HW,
- jednoduchá změna kapacity služeb,
- vysoká rychlost nasazení,
- vysoká bezpečnost.

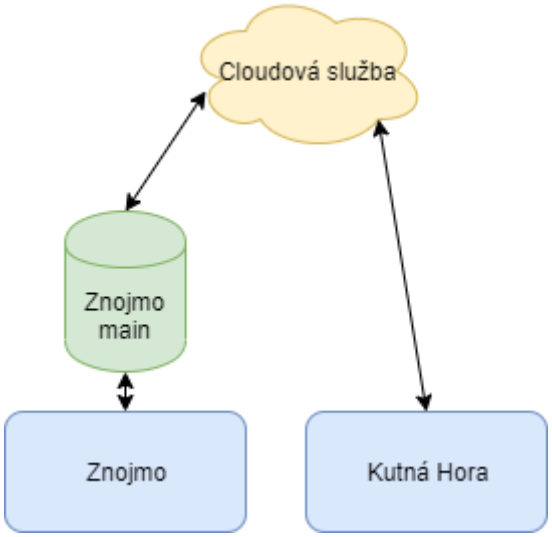
Nevýhody:

- poskytovatel cloudu nemůže dobře garantovat dostupnost dat – přístup přes internetovou konektivitu,
- data jsou umístěna u třetí strany,

- není definováno místo, kde jsou data uložena,
- limity poskytovaných služeb dle poskytovatele,
- vyšší cena (záleží na SLA smlouvě).

3.2.4 Varianta 4: Hybridní uložiště

Další možnou variantou umístění dat je hybridní uložiště. Tento typ kombinuje cloudové i lokální uložiště. Navrhuji lokální uložiště umístit na pobočce ve Znojmě, neboť zde pracuje největší množství pracovníků a je zde kladen největší důraz na rychlou dostupnost dat. Zajištění dostupnosti pracovníkům na pobočce v Kutné Hoře bude zajištěno cloudovými službami nebo přístupem přes VPN na lokální uložiště umístěné na pobočce ve Znojmě. Umístění uložišť je graficky znázorněno na následujícím obrázku.



Obrázek 16: Umístění dat na lokálním i cloudovém uložišti

(Zdroj: Vlastní zpracování)

Výhody:

- na pobočce ve Znojmě je zajištěn přístup k datům z lokální sítě i při výpadku internetové konektivity,
- možnost přístupu mimo firemní síť,
- zajištění vysoké dostupnosti dat,
- vysoká bezpečnost.

Nevýhody:

- vysoké pořizovací náklady,
- pravidelná výměna zakoupeného HW,
- dostupnost mimo lokální síť ve Znojmě závisí na internetové konektivitě,
- školení IT techniků.

3.2.5 Návrh umístění uložiště

Předchozí kapitoly nastínily čtyři možnosti umístění uložiště, a to lokální uložiště umístěné na jednu z poboček, lokální uložiště na více pobočkách, cloudové uložiště a hybridní uložiště, které bude využívat jak lokální uložiště, tak cloudové služby.

Uložiště doporučuji díky převažujícím výhodám využít lokální, aby byla zajištěna vysoká dostupnost dat i při výpadku internetové konektivity. Vzhledem k rozšiřujícím se lidským zdrojům na pobočce v Kutné Hoře je nejvhodnější variantou implementovat lokální uložiště na obě pobočky a data vzájemně replikovat. Vhodným způsobem umístění dat je tedy varianta 2, která je popsána v kapitole 3.2.2. Z důvodu replikace je nutností nastavit pravidelné zálohování na zálohovací zařízení, které bude umístěno na pobočce ve Znojmě.

3.3 Výběr úložného zařízení

Kapitola výběr úložného zařízení se týká výběru vhodných zařízení, které budou umístěny na jednotlivých pobočkách sdružení.

3.3.1 Specifikace požadavků

Zařízení musí být dostatečně rychlé pro připojení více uživatelů současně. Na pobočce ve Znojmě sídlí 13 architektů, proto musí být výkon zařízení uzpůsoben vyššímu počtu uživatelů. Důležitou vlastností, které musí zařízení splňovat je také dostatečná přenosová rychlost v lokální síti.

Zařízení by mělo podporovat replikaci dat přes veřejný cloud a umožnit nastavení pravidelné zálohy firemních dat skrze vhodný software zařízení.

Dalším kritériem pro výběr zařízení je také odolnost vůči selhání některému z disku. Diskové pole musí být uzpůsobeno pro rychlé čtení i zápis.

3.3.2 Kritéria výběru

Pro zajištění rychlého čtení a zápisu dat je nutné zvolit zařízení, které má slot pro čtyři disky. Díky tomu je možné vytvořit RAID 10. Tento typ RAID je vhodný zejména díky rychlosti čtení a zajišťuje ochranu proti selhání některého z disku.

Je vhodné využít zařízení, které má dva gigabitové síťové porty. Díky tomuto počtu je možné na zařízení vytvořit linkovou agregaci a rozložit tak síťovou zátěž mezi dva porty zařízení. Vznikne tak vyšší propustnost a zároveň zařízení bude fungovat i při výpadku jedné z linek.

Zařízení musí mít dostatečný výkon pro připojení více uživatelů současně, proto je nutné vybrat zařízení ve vhodné cenové relaci a s vhodnými hardwarovými parametry.

3.3.3 Dostupné varianty

Řešení dostupnosti mezi pobočkami lze řešit více způsoby. Na každou pobočku může být implementován datový server například na operačním systému Windows Server. V úvahu přichází také síťová uložiště, která jsou vhodná do firemního prostředí. Společnosti, které se zabývají těmito uložišti jsou například Synology, QNAP, Zyxel nebo Asustor. Tyto zařízení umožňují spolehlivou replikaci dat přes veřejný cloud.

Tabulka 9: Porovnání dostupných variant uložišť

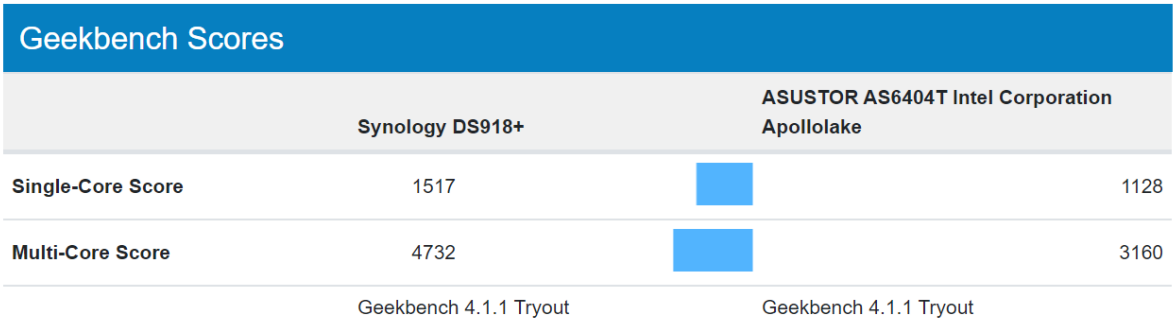
(Vlastní zpracování dle: 22)

Typ zařízení	Synology DS918+	QNAP TS – 932X – 2G	Asustor AS6404T	Dell PowerEdge R240
Produktové číslo	DS918+	TS932X-2G	AS6404T	S20-R240-02
Procesor	Intel Celeron J3455 quad-core 1,5	Alpine AL-324 1,7 GHz	Intel Celeron J3455 quad-core 1,5 GHz	Intel Xeon E-224
Paměť [GB]	4, rozšíření až na 8	2	4, rozšíření až na 8	16
Počet disků [ks]	4	9	4	2
Počet GLAN	2	2	2	2

Pořizovací cena [Kč bez DPH]	12 500	15 000	12 000	30 000 + Licence Windows Server

Varianta s využitím Windows Server je pro tak malý subjekt neefektivní, neboť je nutné zakoupit server na každou pobočku a k němu také vhodnou licenci Windows Server. Vzhledem k ceně samotného zařízení a drahé licenci doporučuji výběr z variant Synology, QNAP a Asustor.

Konfigurace u zařízení QNAP má možnost připojení 9 disků. Vytvoření takového RAID pole je již zbytečné a nákladné. Ve výběru tedy zůstává Synology a Asustor. Obě zařízení mají stejné parametry za téměř totožnou cenu. Vítězným produktem se podle benchmarku na portálu Geekbench.com stalo zařízení Synology. Výsledky testu ukazuje následující obrázek. Vzhledem k tomu, že Synology je známou firmou na trhu s těmito zařízeními a má kvalitní podporu, doporučuji implementaci dostupnosti dat na zařízeních od společnosti Synology.



Obrázek 17: Porovnání Synology a Asustor

(Zdroj: 25)

Za každé zařízení je vhodné umístit záložní zdroj, který slouží k bezpečnému vypnutí zařízení při výpadku elektrické energie a také jako ochrana proti přepětí.

3.3.4 Výběr disku do uložiště

Vybrané zařízení podporuje SATA disky. Je nutné vybrat vhodný typ disku, který je určen pro nepřetržitý provoz. Celková kapacita uložiště musí odpovídat 8 TB. V případě implementace RAID 10 při využití 4 disků je nutné, aby kapacita jednotlivého disku byla 4 TB. Vhodné je vybrat disk s co největší MTBF, tedy střední dobou mezi poruchami. V úvahu připadají výrobci Seagate a Western Digital.

Tabulka 10: Porovnání dostupných variant disků

(Zdroj: Vlastní zpracování dle: 22)

Typ zařízení	WD RED pro 4 TB	Seagate Iron Wolf Pro 4 TB
Produktové číslo	WD4003FFBX	ST400NE001
Velikost	3,5"	3,5"
Rozhraní	SATA III	SATA III
Otáčky [ot. /min]	7200	7200
MTBF [hodin]	1 000 000	1 200 000
Cache paměť [MB]	256	128
Záruka [let]	5	5
Pořizovací cena [Kč bez DPH]	4 400	3 900

Do zařízení doporučuji zakoupit disky od společnosti Western Digital. Produkt této značky má sice o 200 000 hodin menší střední dobu mezi poruchami, má však větší cache paměť. Disky doporučuji pravidelně měnit před uplynutím záruční lhůty.

3.4 Komunikace mezi pobočkami

Aby docházelo k replikaci uložiště ve Znojmě a v Kutné Hoře, je nutné zajistit komunikaci mezi těmito pobočkami. Komunikace lze zajistit pomocí veřejného cloudu Synology za využití Quick Connect ID a následně připojení přes aplikaci, která se jmenuje Cloud Station. Využití veřejného cloudu však není bezpečné, neboť data jsou replikována za pomocí cloudové služby třetí strany.

Druhým a bezpečnějším řešením je zajistit VPN tunel typu site – to site a propojit si tak vzájemně oboje firemní zařízení. K využití VPN tunelu není potřebné využívat cloudovou službu třetí strany a je tak zajištěna vyšší bezpečnost replikace dat. Nevýhodou tohoto řešení je, že obě pobočky musí mít zřízenou veřejnou IP adresu.

Návrh řešení

Z důvodu zajištění vyšší bezpečnosti doporučuji využít VPN tunel. Data tak nebudou poskytována třetí straně a není nutné spoléhat se na funkčnost cloudové služby společnosti

Synology. Doporučuji tak vytvořit VPN tunel s šifrováním L2TP s využitím IPsec. Drobnou nevýhodou je zřízení veřejné IP adresy na každou pobočku, zvýší se tak měsíční náklady (v řádu desítek korun) na internetovou konektivitu.

3.4.1 Internetová konektivita

Pro zajištění spolehlivé a rychlé replikace dat mezi pobočkami je nutné zlepšit internetovou konektivitu na pobočkách. Společně s novou internetovou konektivitou je nutné zajistit také veřejnou IP adresu, která je nutná pro propojení obou firemních sítí pomocí VPN tunelu.

Specifikace požadavků

Současná internetová konektivita na obou pobočkách je v současné době nevyhovující. Nutností je zajistit pro každou pobočku garantovanou symetrickou linku, která bude podložena SLA smlouvou. Vhodné je vybrat poskytovatele internetové konektivity, který je schopný zajistit dohled 24/7 a mít hotline linku pro firemní zákazníky pro případ rychlého řešení problémů s konektivitou.

Rychlost připojení je vhodné mít na obou pobočkách alespoň 50/50 Mbit/s. Pro kvalitní dostupnost dat doporučuji také zajištění záložní internetové konektivity.

Internetová konektivita Znojmo

Do objektu není přiveden optický kabel, z toho důvodu je nutné využít bezdrátové připojení. V úvahu připadají poskytovatelé Starnet, Videon a PODA.

Společnost PODA a.s. je schopná na rozdíl od své konkurence garantovat rychlost připojení. Připojení je symetrické a v ceně je již veřejná IP adresa, která je nutná pro připojení se do firemního uložiště mimo pobočku.

Tabulka 11: Internetová konektivita PODA

(Zdroj: Vlastní zpracování dle: 23)

Rychlost připojení [Mbit/s]	Cena bez DPH [Kč]
30 / 30	2 900
40 / 40	3 500
50 / 50	4 200

80 / 80	5 300
100 / 100	6 200

Z dostupných variant doporučuji kapacitu linky 50 Mbit/s. Cena linky je vyšší, avšak bude využívána pro připojení všech uživatelů mimo firemní síť. Vzhledem k rychlé replikaci dat mezi pobočkami a zajištění kvalitní dostupnosti dat, je vhodné vybrat alespoň tuto variantu. Důležité je, aby stejná rychlost byla zajištěna i na pobočce v Kutné Hoře.

Vzhledem k zajištění vysoké dostupnosti dat doporučuji využít i záložní internetovou konektivitu. Společnost Videon nabízí záložní konektivitu na bezdrátovém pásmu 5 GHz s rychlostí připojení 10 Mbit/s za 175 Kč měsíčně.

Internetová konektivita Kutná Hora

Na pobočce v Kutné Hoře je také nutné zajistit garantovanou linku. Ze společností, které jsou toho schopny dosáhnout je to pouze firma JON. Cenovou nabídku na poskytování jejich služeb popisuje následující tabulka.

Tabulka 12: Internetová konektivita JON

(Zdroj: Vlastní zpracování dle: 24)

Rychlost připojení [Mbit/s]	Cena bez DPH [Kč]
50 / 50	2 090
75 / 75	3 360
100 / 100	4 900
150 / 150	5 430
Záložní linka 20 / 2	388

Pobočka ve Znojmě má doporučenou rychlost linky 50 / 50 Mbit. Tuto kapacitu linky doporučuji využít i od společnosti JON pro pobočku v Kutné Hoře. Na obou pobočkách tak bude zajištěna stejná symetrická a garantovaná linka.

Výhodou internetové konektivity v Kutné Hoře je také zajištění záložního xDSL připojení o kapacitě linky 20 / 2 Mbit za 388 Kč bez DPH měsíčně.

3.5 Přístup k datům mimo firemní síť

Přístup k datům mimo pobočky je možný dvěma způsoby. Buď lze na každou stanici nainstalovat aplikaci Synology Cloud Station, kde bude probíhat replikace dat stejně jako mezi zařízeními Synology. Velká nevýhoda je však v tom, že se do uživatelské stanice nahrají veškeré soubory, které chceme replikovat. Pokud bychom chtěli replikovat například složku ORA, je tato možnost nereálná, protože složka s aktuálními projekty má velkou kapacitu. Tak velký objem dat není reálné replikovat s každou uživatelskou stanicí. Přístup přes Synology Cloud Station probíhá přes veřejný cloud společnosti Synology. Vzniká tak bezpečnostní riziko slabého zabezpečení a odcizení tak citlivých dat.

Další možností je použití VPN, kde se vytvoří tunel mezi klientem a mezi zařízením na pobočce. Vytvoření VPN je z důvodu bezpečnosti vhodnější. Lze využít L2TP šifrování s IPsec, které lze jednoduše nastavit na routerboardu Mikrotik. Toto zařízení je umístěné na každé z poboček.

Přístup k datům mimo firemní pobočku omezuje internetová konektivita. Ta musí být dostatečně rychlá jak na straně firemních poboček, tak na straně uživatele.

Návrh řešení

Aplikace Synology Cloud Station, přes kterou je možné replikovat data do svého zařízení, není vyhovující k použití. Na uživatelské stanici musí probíhat replikace všech vybraných složek, a data jsou tedy uložena jak na uložišti, tak i na uživatelské stanici. Vhodným řešením je využití VPN tunelu.

Na každé firemní pobočce je routerboard Mikrotik. Díky tomu je jednoduché vytvořit VPN tunel pomocí L2TP šifrování s využitím IPsec. Tím se zajistí bezpečné připojení do lokální sítě a přístup k firemním datům tak, jako by byl uživatel přímo uvnitř lokální sítě. Nevýhodou je využití internetové konektivity, která musí být dostatečná jak na straně firemní pobočky, tak na straně klienta. Pro vytvoření VPN tunelu je nutné mít veřejnou IP adresu, kterou je potřeba zřídit společně s kvalitním internetovým připojením.

3.6 Autentizace, autorizace

Kapitola se zabývá vytvořením uživatelských skupin, oprávnění přístupů ke složkám a způsobem ověření uživatelů.

3.6.1 Uživatelské skupiny

Pro zabezpečení firemních dat je nutné vytvořit vhodné uživatelské skupiny pro jednoduchou správu uživatelských oprávnění. Nutností je zabezpečit, aby každá uživatelská skupina měla přístup pouze do své části uložiště a nemohla tak přistupovat do jiných složek sdružení. Vhodným způsobem je vytvoření matice, která jasně definuje, kam má který uživatel přístup a jaká má oprávnění.

Návrh uživatelských skupin:

- „architekt“ – uživatelská skupina pro pracovníky sdružení,
- „majitel“ – skupina vytvořená pro vlastníky sdružení,
- „vedouci“ – uživatelská skupina pro manažery jednotlivých projektů.
- „externista“ – uživatelská skupina pro tým statiků

Složka ORA: Do této složky mají přístup všichni uživatelé. V této složce jsou aktuálně rozpracované projekty a podklady k jejich zpracování.

Složka ORA_archiv: Do složky, kde jsou uchovány staré projekty mají přístup pouze vedoucí týmu architektů a vlastníci sdružení.

Složka ORA_soukrome: Ve složce je vytvořena podsložka se jménem jednotlivého uživatele. Každý uživatel má přístup pouze do své složky, kde si může ukládat data potřebné pro zpracování projektů. Vedoucí projektu by měl mít možnost data číst, ale nikoliv je upravovat.

Složka ORA_scan: Složka slouží k prohlížení naskenovaných souborů ze síťové tiskárny na pobočce ve Znojmě. Přístup je povolen pro všechny uživatele. Každý uživatel může data číst, ale nikoliv je mazat, upravovat nebo do složky vkládat vlastní data.

Složka ORA_dokumenty: Složka obsahuje citlivá data týkající se cenových nabídek, vydaných či přijatých faktur a dokumenty týkající se založení firmy. Přístup do této složky je omezen pouze pro majitele sdružení.

Tabulka 13: Matice přístupů do složek

(Zdroj: Vlastní zpracování)

	ORA	ORA_archiv	ORA_Soukrome	ORA_Scan	ORA_Dokumenty
Architekt	R/W	-	R/W	R	-
Externista	-	-	R/W	R	-
Majitel	R/W	R/W	R/W	R	R/W
Vedouci	R/W	R/W	R/W	R	-

Tabulka 14: Legenda k matici přístupů do složek

(Zdroj: Vlastní zpracování)

Zkratka	Vysvětlení
R	složka pouze pro čtení
R/W	složka pro čtení a zápis
-	bez přístupu

3.6.2 Ověření uživatelů

Autentizace uživatelů bude zajištěna způsobem „dle toho, co subjekt zná“. Přihlášení bude tedy probíhat pod unikátním uživatelským jménem. Autentizace bude systémem zajištěna pomocí hesla. Výhodou tohoto způsobu je snadné měnění hesel v určitém intervalu (například jeden krát měsíčně) z důvodu bezpečnosti. Tento systém přihlášení je závislý na uživateli, který je nejslabším článkem celého systému. Uživatel si nemusí pamatovat heslo. Pokud si uživatel heslo například někde napíše, může tak dojít jednoduše k jeho zneužití. Je důležité generovat složitá hesla a pravidelně je měnit.

3.7 Implementace projektu

Kapitola implementace projektu popisuje nastavení zařízení Synology na jednotlivých pobočkách a nastavení VPN tunelu.

3.7.1 Nastavení zařízení Synology

Projekt bude postaven na zařízeních od společnosti Synology ve verzi 918+ s disky od společnosti Western Digital o kapacitě 4 TB.

Tabulka 15: Použité zařízení a jeho konfigurace

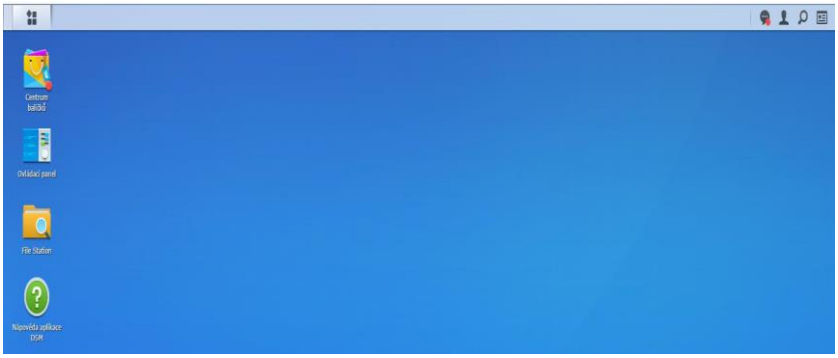
(Zdroj: Vlastní zpracování)

	Kutná Hora main	Znojmo main	Znojmo backup
Typ zařízení	Synology DS918+	Synology DS918+	Synology DS918+
Produktové číslo	DS918+	DS918+	DS918+
Počet disků	4	4	4
Kapacita disku	4TB	4TB	4TB
Typ RAID	RAID 10	RAID 10	RAID 10
Celková kapacita	8TB	8TB	8TB

Po fyzické montáži disků a aktualizaci operačního systému se lze pomocí webového rozhraní přihlásit na zařízení Synology.

Obrázek 18: Zařízení Synology

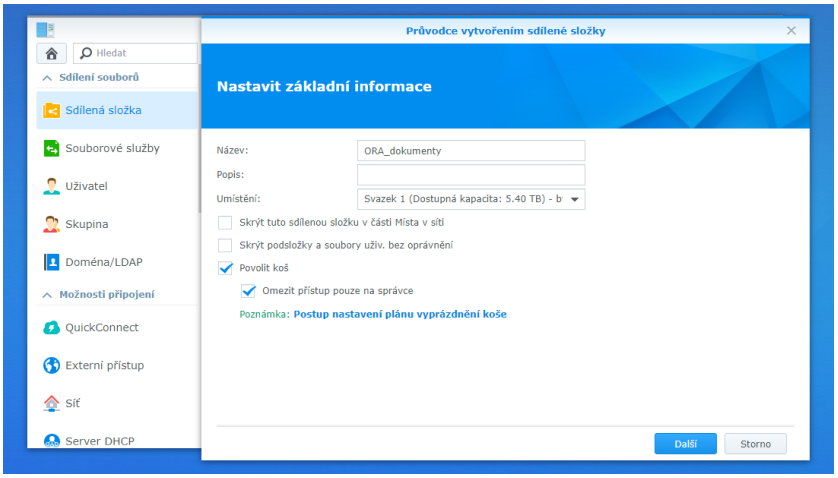
(Zdroj: 2)



Obrázek 19: Prostředí Synology

(Zdroj: Vlastní zpracování)

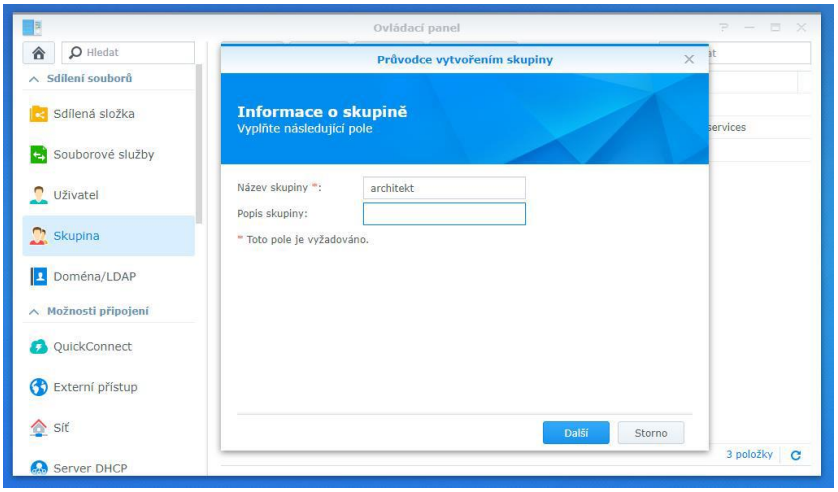
Vzhledem k tomu, že současná struktura dat je vhodná i pro implementaci nového řešení, není nutné vytvářet novou strukturu dat. Prvním krokem je tedy již vytvoření sdílených složek. Sdílené složky je nutné vytvořit na zařízení Znojmo main i Kutná Hora main.



Obrázek 20: Vytvoření nové sdílené složky

(Zdroj: Vlastní zpracování)

Dalším krokem je vytvoření uživatelských skupin. Tyto skupiny jsou na obou pobočkách také totožné. Způsob jejich vytvoření ukazuje následující obrázek.

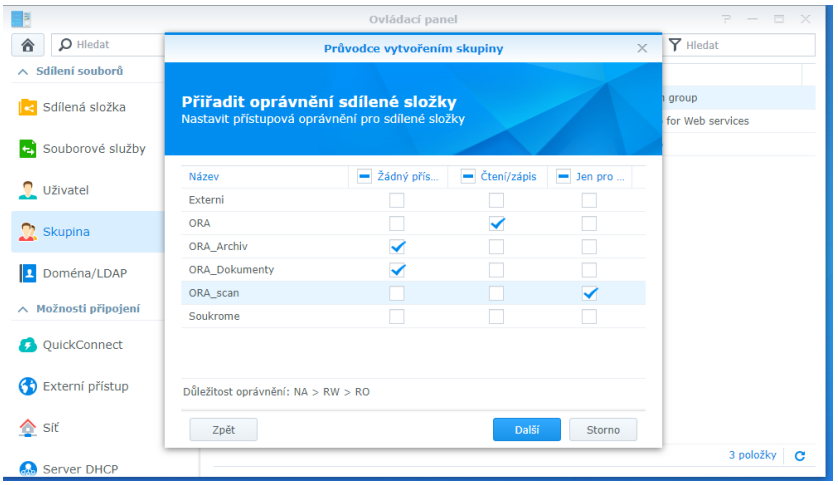


Obrázek 21: Vytvoření uživatelských skupin

(Zdroj: Vlastní zpracování)

Stejným způsobem, jakým se vytváří uživatelské skupiny, se vytváří jednotliví uživatelé, kteří se následně se přiřadí do vhodné skupiny. Uživatelská hesla musí být dostatečně silná, k jejich vytváření doporučuji využít generátor hesel.

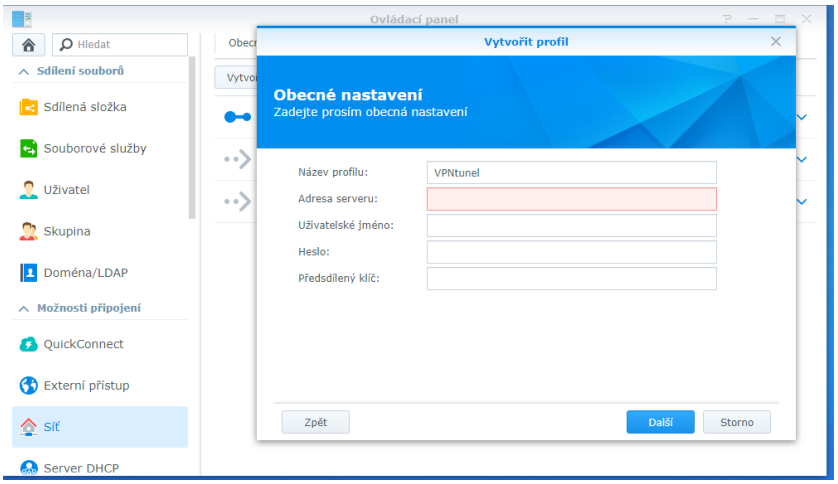
Po vytvoření uživatelských skupin a přiřazení jednotlivých uživatelů je nutné nastavit oprávnění uživatelských skupin do jednotlivých složek. Oprávnění jednotlivých skupin jsou popsána v kapitole o uživatelských skupinách.



Obrázek 22: Nastavení oprávnění ke složkám

(Zdroj: Vlastní zpracování)

Pro replikaci dat je možné vytvořit spojení mezi pobočkami za pomocí veřejného cloudu společnosti Synology a využít tak jejich „Quick Connect ID“. Vzhledem k tomu, že je na obou pobočkách veřejná IP adresa, je lepším řešením vytvořit VPN tunel. Vytvoření VPN tunelu je popsáno v další kapitole. Následující obrázek ukazuje připojení k VPN v zařízení Synology.

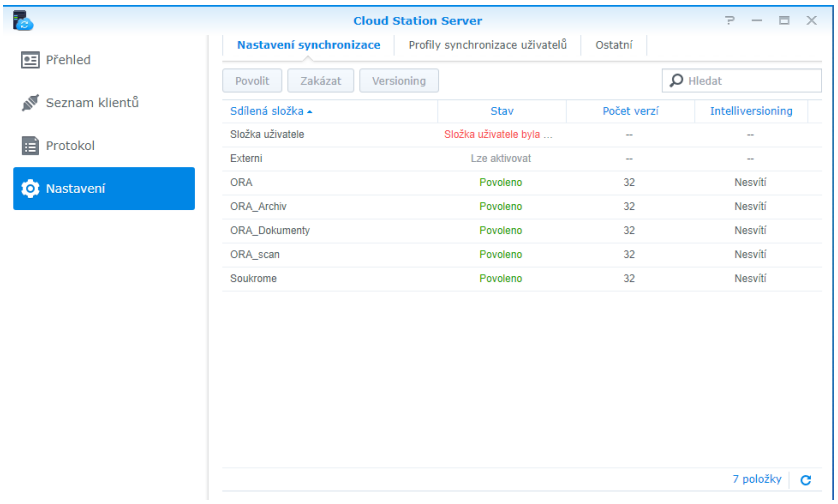


Obrázek 23: Připojení do VPN

(Zdroj: Vlastní zpracování)

Nastavení replikace Znojmo main

Pro zajištění replikace dat mezi pobočkami Znojmo a Kutná Hora je nutné nainstalovat na zařízení aplikaci Synology Cloud Station Server. Replikace uložišť bude probíhat v reálném čase. V aplikaci je nutné pouze zvolit sdílené složky, které se mají replikovat. Další nastavení se provádí na druhém zařízení, a to na zařízení umístěném v Kutné Hoře.

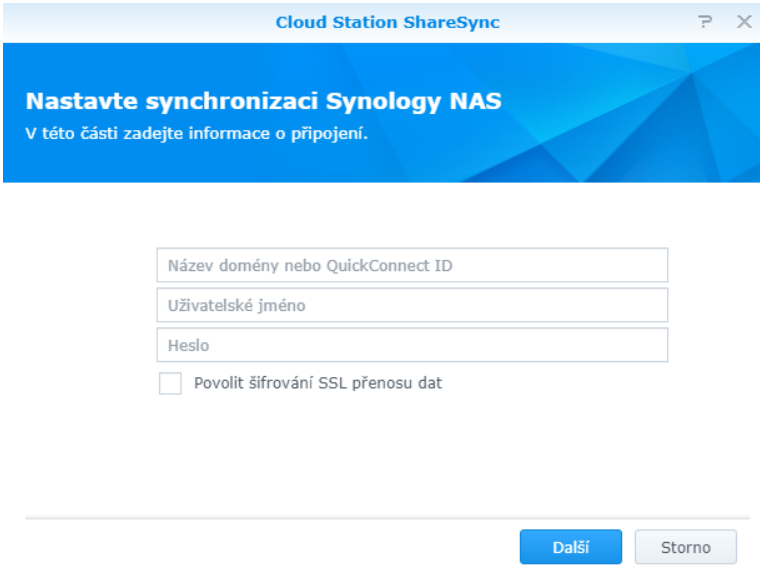


Obrázek 24: Výběr replikovaných složek

(Zdroj: Vlastní zpracování)

Nastavení replikace Kutná Hora main

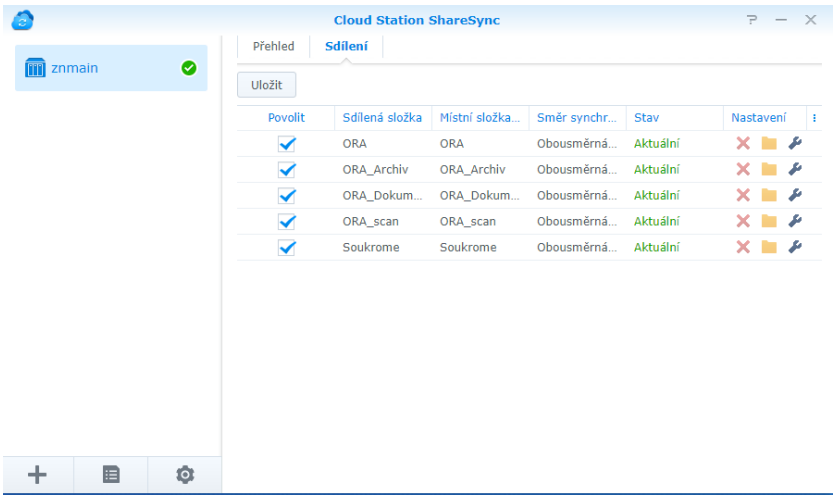
Pro nastavení replikace dat mezi pobočkami je nutné na zařízení Kutná Hora main nainstalovat aplikaci Synology Cloud Station, přes kterou lze jednoduše provádět replikaci mezi pobočkami. Připojení na zařízení ve Znojmě ukazuje následující obrázek.



Obrázek 25: Připojení přes Synology Cloud Station

(Zdroj: Vlastní zpracování)

Po úspěšné autentizaci dojde k propojení se zařízením umístěném ve Znojmě. V následujícím kroku se zvolí složky, které chceme replikovat mezi jednotlivými pobočkami. Po nastavení dojde k prvotní migraci dat z pobočky ve Znojmě na pobočku do Kutné Hory. Po úspěšné migraci všech dat jsou zařízení připravena k používání.



Obrázek 26: Nastavení replikovaných složek

(Zdroj: Vlastní zpracování)

Prvotní replikace firemních dat

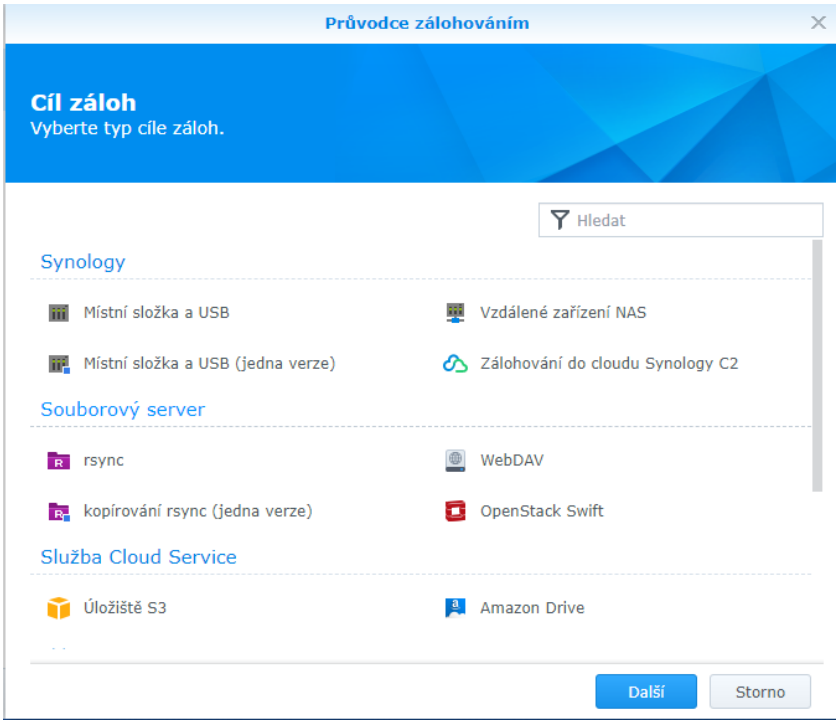
Současná kapacita firemních dat je o velikosti 2 TB. Pokud by se data migrovala na jedno uložiště pobočky a následně by se data replikovala na druhou pobočku, celý proces by byl velmi

zdlouhavý. Z toho důvodu je vhodné provést prvotní replikaci na jedné z poboček a až poté umístit zařízení na druhou pobočku. Dojde k výrazné úspoře času trvání celého projektu.

Nastavení zálohování dat

Na pobočce ve Znojmě je umístěno zařízení Znojmo backup, které slouží k záloze firemních dat. Způsob zálohování je nastaven na kombinaci úplné a přírůstkové zálohy. První den v týdnu, tedy v pondělí se udělá úplná záloha firemních dat a následně se každý den provede záloha přírůstková. Zálohování dat probíhá vždy po konci pracovní doby kvůli vytížení síťové konektivity i jednotlivých zařízení na pobočce ve Znojmě. Spuštění záloh doporučuji stanovit na 3:00. Záloha se provádí skrze aplikaci Hyper Backup. Jednotlivé zálohy je nutné pravidelně kontrolovat fyzickým připojením na toto uložiště. Aplikace umí při chybné záloze dat odeslat notifikační e-mail, ovšem neumí zkontrolovat, zda je záloha čitelná.

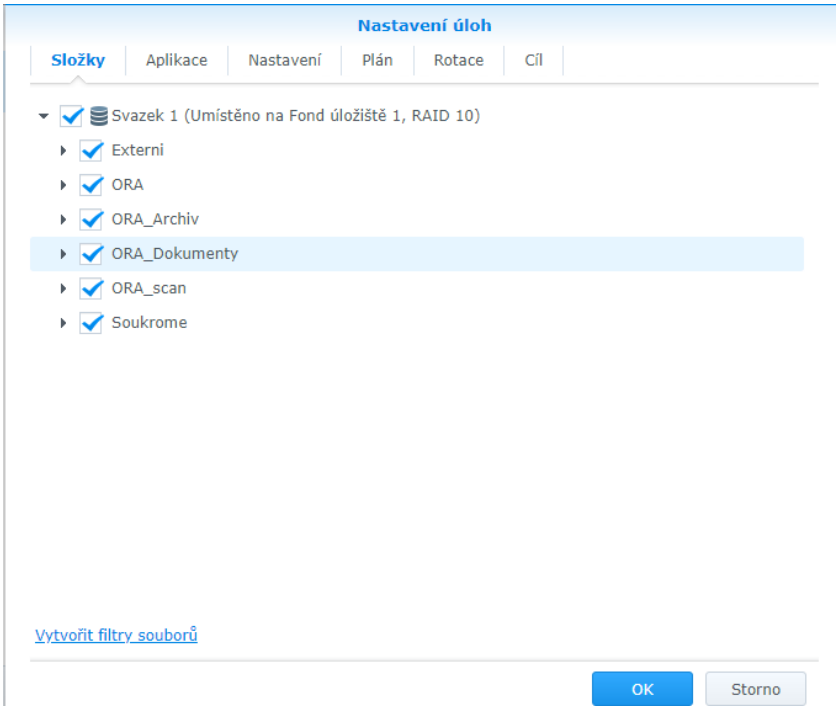
Zálohování dat se nastavuje na zařízení Znojmo main přes aplikaci Hyper Backup. Průvodce zálohování pomocí této aplikace znázorňuje následující obrázek.



Obrázek 27: Průvodce zálohováním Hyper Backup

(Zdroj: Vlastní zpracování)

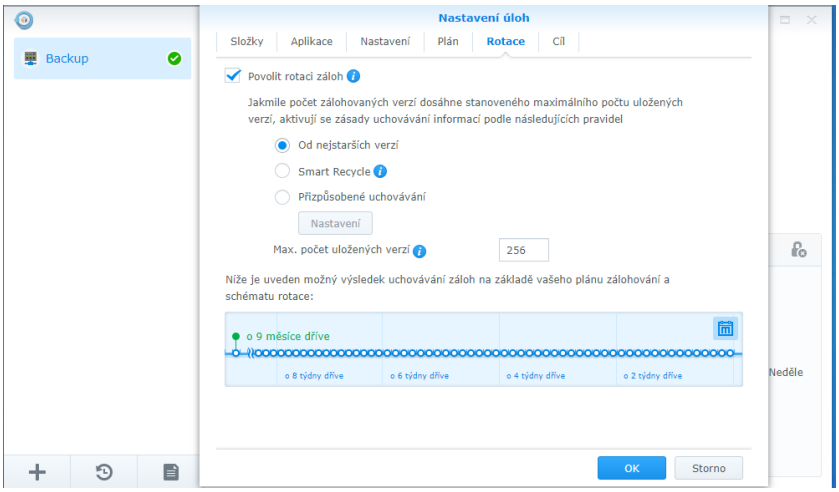
V dalším kroku je nutné nastavit složky, které chceme zálohovat. V tomto případě dochází k záloze celého svazku, tedy všech složek.



Obrázek 28: Výběr zálohovaného svazku

(Zdroj: Vlastní zpracování)

Aplikace Hyper Backup umí aktivovat zásadu o uchování informací dle různých pravidel. V tomto případě je aktivována zásada o smazání nejstarších verzí. Jakmile dojde k vyčerpání kapacity disků, aktivuje se tato zásada a nejstarší záloha bude smazána.



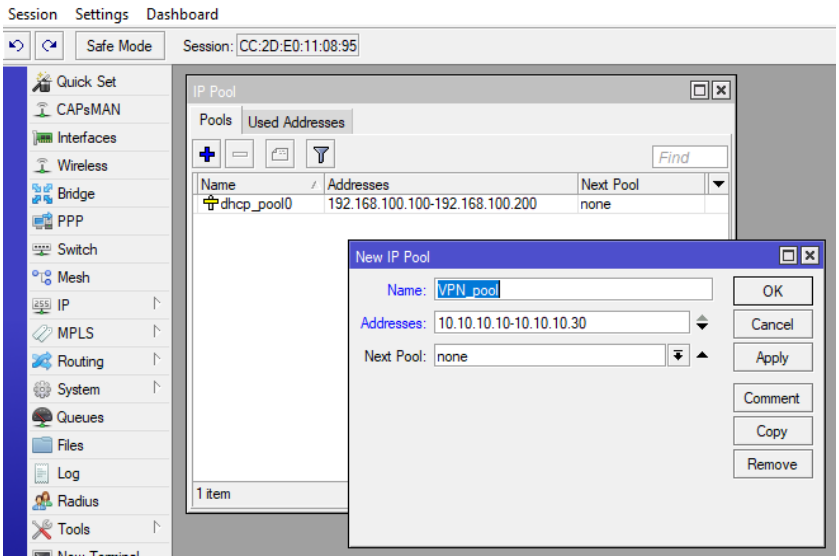
Obrázek 29: Rotace záloh v aplikaci Hyper Backup

(Zdroj: Vlastní zpracování)

3.7.2 Nastavení VPN tunelu

Tato část se týká nastavení VPN tunelu pomocí L2TP šifrování s využitím IPsec. Před samotným nastavením VPN doporučuji vytvořit si zálohu současné konfigurace zařízení a následně provést upgrade firmware na nejnovější verzi.

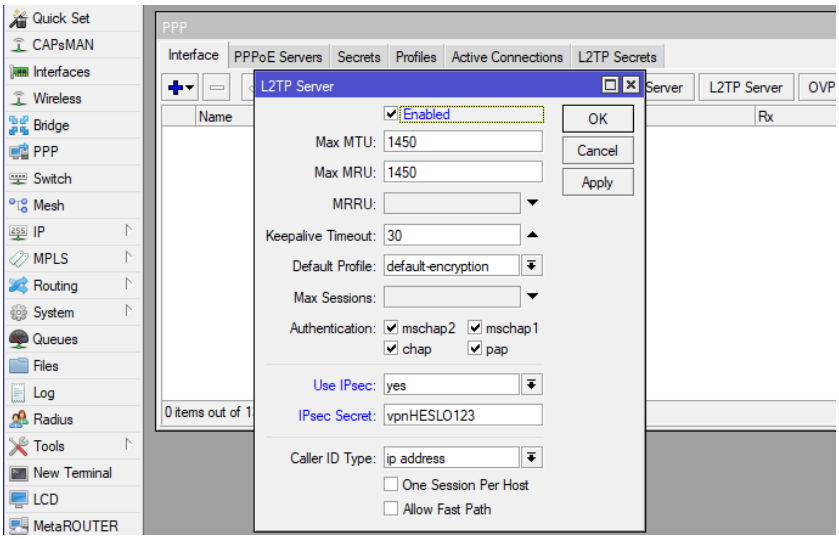
Při samotném vytvoření VPN tunelu je prvním krokem vytvoření VPN IP pool. Pool pojmenuji jako VPN_pool a rozsah adres je 10.10.10.10 – 10.10.10.30.



Obrázek 30: Vytvoření VPN pool

(Zdroj: Vlastní zpracování)

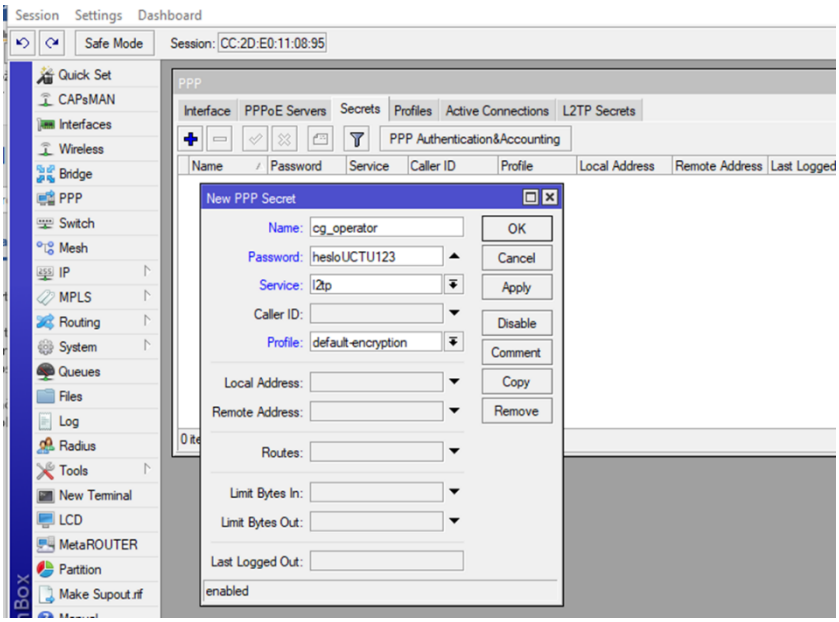
Dalším krokem je zapnutí L2TP serveru včetně povolení IPsec. Do pole „IPsec Secret“ se píše heslo, kterým se šifruje komunikace.



Obrázek 31: Povolení L2TP serveru

(Zdroj: Vlastní zpracování)

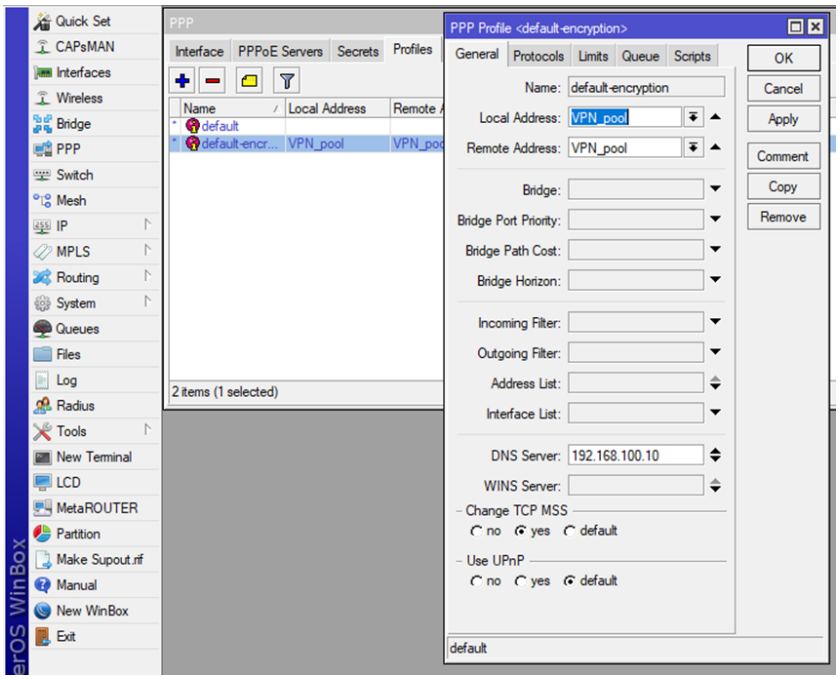
Dalším krokem je vytvoření uživatele v záložce „Secrets“ Uživatelské heslo doporučuji vytvořit dostatečně silné, nejlépe pomocí generátoru hesel.



Obrázek 32: Vytvoření VPN uživatele

(Zdroj: Vlastní zpracování)

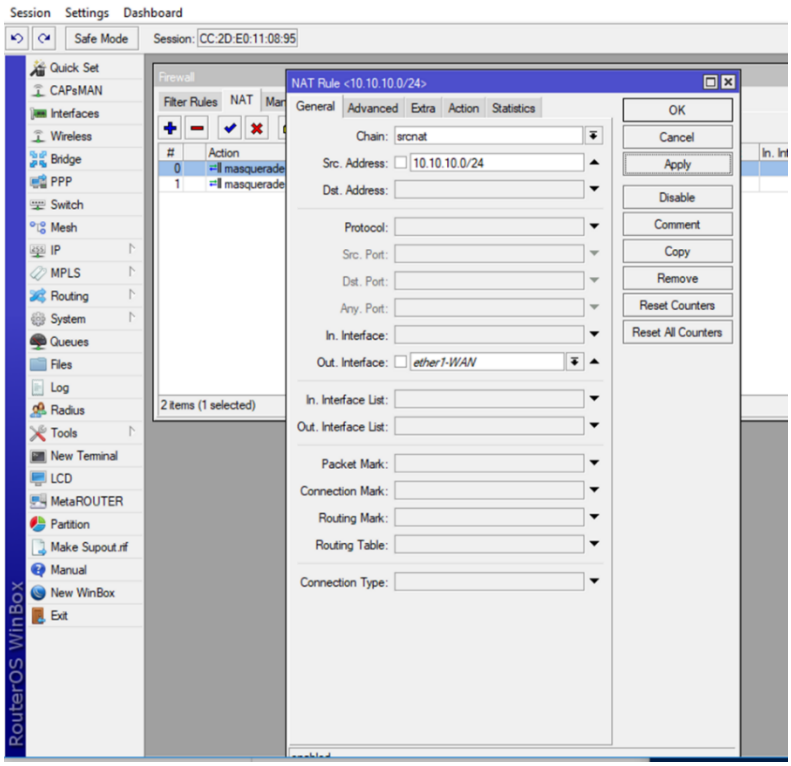
Po vytvoření uživatele je nutné přiřadit VPN_pool uživatelskému profilu. V tomto případě je profil pod názvem default-encryption. V tomto kroku je potřebné nastavit také DNS server.



Obrázek 33: Přiřazení VPN poolu uživatelskému profilu

(Zdroj: Vlastní zpracování)

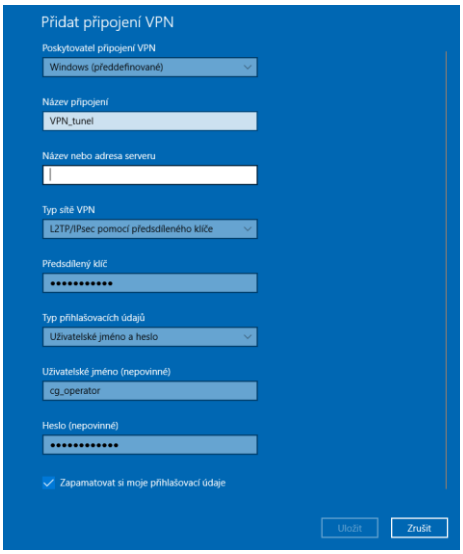
Pro připojení VPN uživatelů do internetu se musí povolit jejich IP rozsah. V záložce „NAT“ se vytvoří nový „srcnat“, kde se do „Src. Address“ vloží VPN IP rozsah.



Obrázek 34: Povolení VPN uživatelům přístup do internetu

(Zdroj: Vlastní zpracování)

VPN tunel je vytvořený. Nyní je potřeba nastavit všem zaměstnancům účty, vygenerovat hesla a nastavit jim VPN připojení na jejich koncovém zařízení. Následující obrázek ukazuje způsob připojení uživatele do firemní sítě na operačním systému Windows 10.



Obrázek 35: Připojení do VPN na Windows 10

(Zdroj: Vlastní zpracování)

3.8 Řízení projektu nasazení

Kapitola se týká řízení projektu. V této kapitole jsou popsány přínosy projektu, pomocí metody WBS rozdělení projektu na dílčí úkoly a časový harmonogram projektu. V závěru kapitoly je analýza rizik.

3.8.1 Kvantifikace sil

Kvantifikace sil určuje, zda je projekt pro firmu přínosný nebo nikoliv. Síly působící pro změnu jsem ohodnotil na stupnici 1 až 5 a síly působící proti změně na stupnici -1 až -5.

Tabulka 16: Kvantifikace sil

(Zdroj: Vlastní zpracování)

Síly působící ve prospěch změny		Síly působící proti změně	
Zajištění dostupnosti mezi pobočkami	5	Počáteční náklady na implementaci	-5
Zefektivnění práce	5	Složitější obsluha systému (Nutnost platit IT správce)	-3
Přístup k datům i mimo firemní prostředí	4	Z důvodu připojení do internetové sítě hrozí vnější útoky	-3

Možnost rychlého rozšíření systému	2	Ztráta důvěry v bezpečné uložení dat	-1
Zajištění záloh firemních dat	4		
Celkem ve prospěch změny	**20**	**Celkem proti změně**	**-12**

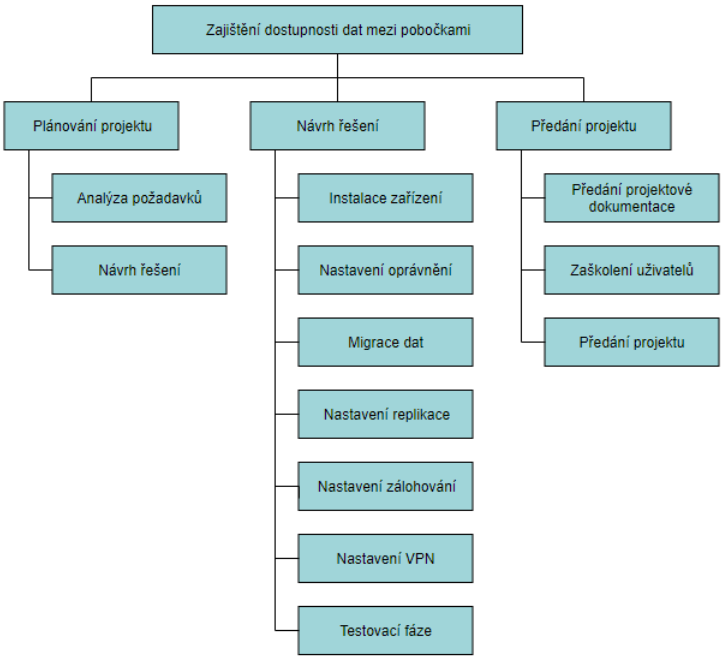
Z tabulky jasně vyplývá, že síly převažují ve prospěch změny a firmě zajištění vysoké dostupnosti dat mezi pobočkami Znojmo a Kutná Hora pomůže a zefektivní práci. Jednotlivé síly, které působí proti změně je možné eliminovat vhodnými opatřeními, které jsou popsány v následujících kapitolách týkajících se analýzy rizik.

3.8.2 Přínosy projektu

Spolehlivá a vysoká dostupnost dat ve společnosti zajistí, že uživatelé budou mít v reálném čase aktuální data jak na pobočce ve Znojmě, tak v Kutné Hoře. Velmi se tak zvýší efektivita práce, neboť na projektu může zároveň pracovat zaměstnanec v Kutné Hoře i Znojmě bez nutnosti přeposílání projektu na některé online uložiště a bez nutnosti přenášet informace na externím HDD. Dalším velkým přínosem je také to, že zákazníci budou mít přístup k firemním datům i mimo firemní prostředí. Mohou tak pracovat na „home office“ a mít firemní data stále u sebe.

3.8.3 WBS

Work breakdown structure (WBS) obsahuje rozklad dílčích částí projektů. Projekt zajištění dostupnosti dat mezi pobočkami a jeho jednotlivé činnosti zobrazuje následující obrázek.



Obrázek 36: WBS struktura

(Zdroj: Vlastní zpracování)

3.8.4 Přidělení odpovědností projektu

Kapitola se týká přidělení odpovědností k jednotlivým činnostem projektu. Do projektu budou zasahovat čtyři subjekty, a to majitel IT firmy, IT technik, majitelé sdružení ORA a ORA architekti.

Tabulka 17: Matice odpovědnosti projektu

(Zdroj: Vlastní zpracování)

	Majitel IT firmy	IT technik	Majitelé ORA	ORA architekt
Analýza požadavků	A	R	C	C
Návrh řešení	A	C	C	I
Instalace zařízení	C / I	R / A	I	
Nastavení oprávnění	I	R / A	C	
Migrace dat	C/ I	R / A		
Nastavení replikace	C / I	R / A		
Prvotní replikace dat	C / I	R / A	I	

Nastavení zálohování	C / I	R / A	I	
Testovací fáze	C / I	R / A	C	C
Nastavení VPN	C / I	R / A	I	I
Předání projektové dokumentace	A	R	C	
Zaškolení uživatelů	A	R	I	I
Předání projektu	A	R	I	I

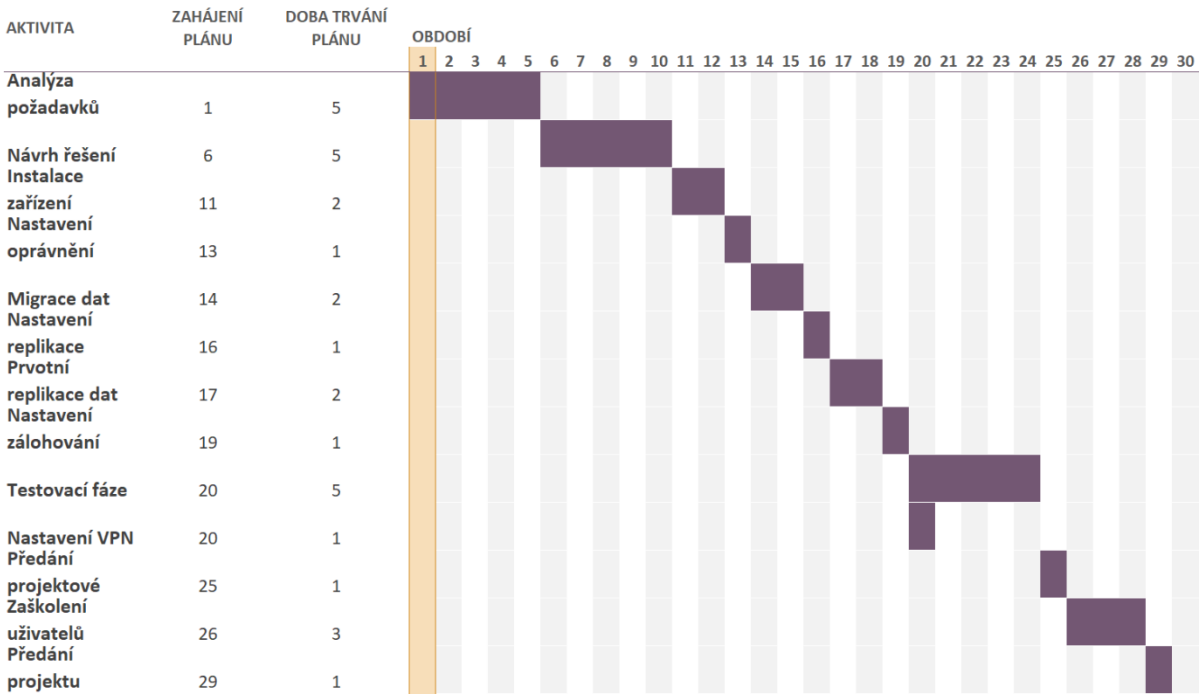
Legenda k matici:

- R – ti, kteří vykonávají práci
- A – ti, kteří zodpovídají za výsledek
- C – ti, kteří poskytují konzultace
- I – ti, kteří jsou informování

3.8.5 Časový harmonogram projektu

Zavedení projektu, založeném na lokálním uložišti umístěném na každé z poboček se vzájemnou replikací, pomocí Ganttova diagramu popisuje následující tabulka.

Z Ganttova diagramu lze vyčíst, že v projektu je spousta na sebe navazujících činností. Souběžně s ostatními činnostmi probíhá pouze testovací fáze. Ostatní fáze projektu začínají po skončení předchozí fáze. Prodlení v každé části projektu prodlouží celkovou dobu trvání projektu, je tedy potřebné striktně dodržet každou část, aby projekt proběhl za plánovaných 29 dní.



Obrázek 37: Ganttův diagram

(Zdroj: Vlastní zpracování)

3.8.6 Rizika řešení

Hodnocení rizik projektu je vyjádřeno pomocí metody RIPRAN, která je znázorněna v následující tabulce.

Tabulka 18: Metoda RIPRAN

(Zdroj: Vlastní zpracování)

ID	Hrozba	PST hrozby	ID	Scénář	PST scénáře	Celková PST	Dopad	Hodnota rizika	ID	Opatření
1	Zničení zařízení přírodním živlem	MP	1.1	Zatopení způsobené povodněmi	MP	MP	SD	MHR	1.1.1	Instalace čidla proti povodním
									1.1.2	Přesunout serverovnu do vyššího patra budovy
			1.2	Vyhoření serverovny	SP	MP	SD	MHR	1.2.1	Instalace kouřového čidla
			1.3	Přepětí elektrické sítě	SP	MP	SD	MHR	1.3.1	Před síťové uložiště umístit kvalitní záložní zdroj UPS

			1.4	Vysoká teplota v serverovně	SP	MP	SD	MHR	1.4.1	Hlídání teploty v serverovně
2	Napadení uložiště ransomware	VP	2.1	Uživatel otevře mailovou přílohu s virem	VP	VP	VD	VHR	2.1.1	Proškolení uživatelů v oblasti kyberbezpečnosti
									2.1.2	Pořídit kvalitní mail server
			2.2	Uživatel vloží do firemní sítě vlastní zavirované zařízení	VP	VP	VD	VHR	2.2.1	Použití USB, RJ45 blokátorů (NISS)
									2.2.2	Firemní směrnice o používání vlastních zařízení
									2.2.3	Proškolení uživatelů v oblasti kyberbezpečnosti
3	Smazání dat uživatelem	VP	3.1.	Uživatel smaže firemní data	VP	VP	SD	VHR	3.1.1	Zachovávat kopie na uložišti
									3.1.2	Pravidelná záloha dat na zálohovací zařízení
									3.1.3	Správně nastavit politiku o právech a přístupech uživatelů k datům
4	Nečitelná záloha dat	MP	4.1	V případě nutnosti obnovy nebudou data čitelná	SP	MP	VD	SHR	4.1.1	Pravidelně kontrolovat čitelnost záloh proškoleným technikem
5	Poškození diskového pole	SP	5.1	Poškození HW jednotlivých disků	SP	SP	SD	SHR	5.1.1	Pravidelná výměna disků na konci záruční doby
6	Fyzická krádež uložiště	SP	6.1	Fyzické vniknutí do serverovny	SP	SP	VD	VHR	6.1.1	Uzamčení serverové místnosti

									6.1.2	Instalace kamerového systému
									6.1.3	Instalace zabezpečovacího systému
									6.1.4	Vstup pouze povolaným technikům, autentizace kódem
7	Zneužití dat třetí stranou	VP	7.1	Zaměstnanec vynese firemní data	VP	VP	VD	VHR	7.1.1	Nastavení firemní politiky o firemních datech
			7.2	Napadení firemní sítě útokem zvenčí	SP	VP	VD	VHR	7.2.1	Instalace kvalitního firewallu
									7.2.2	Proškolení IT techniků v oblasti kyberbezpečnosti
									7.2.3	Kvalitní a jednotné antivirové řešení

Z metody RIPRAN plyne, že největšími problémy při využití ukládání dat na lokální uložiště je napadení ransomware, smazání uživatelských dat uživatelem, nečitelná záloha dat a zneužití firemních dat třetí stranou. V metodě RIPRAN je zavedeno i opatření, které sníží tyto rizika. V případě napadení uložiště ransomware nebo pokud dojde ke zneužití dat třetí stranou se lze bránit kvalitním firewallem, správným nastavením firemní politiky a pravidelně školit své zaměstnance a IT techniky v oblasti kyberbezpečnosti.

3.9 Zhodnocení projektu

Tato kapitola se týká celkového zhodnocení projektu. Jsou zde popsány náklady na projekt, jsou kvantifikovány přínosy projektu a následně je projekt zhodnocen jako celek.

3.9.1 Ekonomické zhodnocení nákladů

Následující tabulka popisuje ekonomické vyjádření projektu zajištění dostupnosti dat ve společnosti ORA pomocí lokálních síťových uložišť se vzájemnou replikací. V ceně jsou zahrnuty samotné zařízení včetně odhadu práce.

Tabulka 19: Ekonomické zhodnocení projektu

(Zdroj: Vlastní zpracování)

Položka	Počet ks	Cena / ks	Cena celkem
Synology DS918+	3	12 554	37 662
HHD WD Red pro 4 TB	12	4 400	31 200
Záložní zdroj	3	6 000	18 000
Odhad práce	40	600	24 000
Cena celkem bez DPH			**132 300 Kč**
Cena včetně DPH (21 %)			**160 083 Kč**

V této částce není uvedena internetová konektivita pro jednotlivé pobočky, kde platba probíhá měsíčně. Měsíční platby shrnuje následující tabulka.

Tabulka 20: Ekonomické zhodnocení internetové konektivity

(Zdroj: Vlastní zpracování)

Pobočka	Položka	Cena měsíčně
Znojmo	Hlavní konektivita PODA 50/50 Mbit	4 200
Znojmo	Záložní konektivita Videon 10/2Mbit	175
Kutná Hora	Hlavní konektivita JON 50/50 Mbit	2 090
Kutná Hora	Záložní konektivita JON 20/2Mbit	388
Cena celkem bez DPH		**6 853 Kč**
Cena celkem s DPH (21 %)		**8 292 Kč**

3.9.2 Ekonomické zhodnocení přínosů

Společnost v současném stavu vytvoří zhruba 40 projektů za rok. Největším problémem byla dostupnost dat, kdy si pracovníci museli předávat projekty na externím HDD a pobočky neměly aktuální data. Díky zajištění vysoké dostupnosti dat se zvýší efektivita práce. V následující tabulce budu uvažovat zvýšení výkonnosti o 20 %. Toto procentní vyčíslení v současném stavu musí společnost odmítat z kapacitních důvodů, neboť je nedostatečná dostupnost dat, jak je již uvedeno v analýze současného stavu v kapitole 1.2.

Tabulka 21: Ekonomické zhodnocení přínosů projektu

(Zdroj: Vlastní zpracování)

	Současný stav	**Stav po implementaci projektu**
Prodejní cena projektu bez DPH	400 000 Kč	400 000 Kč
Počet projektů	40 ks	48 ks
Roční obrat celkem bez DPH	16 000 000	19 200 000

Z tabulky vyplývá, že po zavedení projektu a zvýší efektivita práce o 20 %. Tím se zvýší počet vypracovaných projektů o 12 ks. Při ceně 400 000 za jeden projekt se zvýší celkový roční obrat společnosti o 3 200 000 Kč. Vzhledem k jednorázové investici ve výši 132 300 Kč a zvýšení měsíční platby za internetovou konektivitu o 6 853 Kč, tedy 82 236 Kč ročně, je projekt ziskový a firmě přinese zvýšení celkového obratu, tedy i zisku.

3.9.3 Celkové zhodnocení řešení

Nastavení dostupnosti dat mezi pobočkami firmy s využitím prvků od společnosti Synology bylo dostáhnuto za pomoci umístění lokálního uložiště na obě firemní pobočky. Tyto data se budou následně replikovat v reálném čase pomocí vytvořeného VPN tunelu. Tento způsob je poměrně levný, avšak má v sobě řadu nevýhod, které jsou zmíněny v analýze rizik. V současné době probíhá velké množství ransomware útoků. Pokud dojde k napadení jednoho ze zařízení, data se automaticky replikují i na druhé uložiště a dojde tak k zašifrování všech firemních dat. Tomuto problému se dá bránit kvalitním firewallem a zejména pravidelnými zálohami. Tyto zálohy probíhají na zařízení umístěné ve Znojmě. Další nevýhodou oproti cloudovému řešení

je také nutnost zakoupit vlastní hardware, který je nutné pravidelně měnit při uplynutí záruční lhůty.

Zajištěním vysoké dostupnosti dat dojde k navýšení efektivity práce. S poměrně nízkými náklady tak lze předpokládat významné navýšení obratu, neboť v analýze současného stavu se zjistilo, že sdružení ORA musí odmítat 20 % projektů ročně. Díky zajištění kvalitní dostupnosti dat mezi pobočkami dokážou zaměstnanci naprojektovat o 8 projektů ročně více. Celkový obraz společnosti se tak zvýší odhadem o 3 200 000 Kč.

ZÁVĚR

Cílem diplomové práce bylo navrhnout spolehlivou datovou infrastrukturu ve společnosti s více pobočkami pro sdružení ORA. Návrh řešení plynul z analýzy současného stavu datové infrastruktury a požadavků investora.

V návrhu řešení jsem čerpal z analýzy současného stavu. Další část práce se týkala teoretických východisek. Na základě teoretické části jsem vypracoval vlastní návrh řešení přímo pro sdružení ORA. Návrh zajištění dostupnosti dat pro sdružení byl vytvořen z důvodu velmi nízké a nevyhovující dostupnosti dat.

Návrh řešení byl již konzultován s majiteli sdružení. Majitelé tak mají přehled o použitých prvcích v datové infrastruktuře, jsou seznámeni s časovým harmonogramem projektu, a znají přínosovou i nákladovou stránku celého nového řešení. Při konzultaci a představení návrhu řešení byly projednány také rizika nové datové infastruktury a následně byly představeny ošetření, jak tyto rizika eliminovat nebo snížit na přijatelnou úroveň.

Po konzultaci a zohlednění všech aspektů jsou majitelé sdružení ORA nakloněni k realizaci projektu návrhu spolehlivé datové infrastruktury pro jejich společnost s pobočkami ve Znojmě a Kutné Hoře.

-

SEZNAM POUŽITÝCH ZDROJŮ

1. GILFILLAN, Ian. Myslíme v MySQL 4. Praha: Grada, 2003. Knihovna programátora (Grada). ISBN 80-247-0661-1.

2. Synology [online]. 2020 [cit. 2020-04-14]. Dostupné z: www.synology.com

3. NELSON, Steven. Pro data backup and recovery. New York: Distributed to the book trade worldwide by Springer Science+Business Media, c2011. Expert's voice in data management. ISBN 9781430226628.

4. ONDRÁK, Viktor, Petr SEDLÁK a Vladimír MAZÁLEK. Problematika ISMS v manažerské informatice. Brno: Akademické nakladatelství CERM, 2013. ISBN 978-80-7204-872-4.

5. Svět Hardware: Zálohování a archivace dat: jaké jsou možnosti? [online]. 2016 [cit. 2020-04-14]. Dostupné z: https://www.svethardware.cz/zalohovani-a-archivace-dat-jake-jsou-moznosti/43212-2

6. Computer Science: Storage Devices [online]. [cit. 2020-04-14]. Dostupné z: https://www.computerscience.gcse.guru/theory/storage-devices

7. MELL, Peter; GRANCE, Timothy. The NIST Definition of Cloud Computing [online]. Geithersburg: U.S. Department of Commerce, September 2011 [cit. 13. 11. 2016]. Dostupné z: http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

8. LACKO, Ľuboslav. Osobní cloud pro domácí podnikání a malé firmy. Brno: Computer Press, 2012. ISBN 978-80-251-3744-4.

9. 22hlav: Způsoby ukládání dat [online]. 2018 [cit. 2020-04-14]. Dostupné z: https://www.22hlav.cz/zpusoby-ukladani-dat

10. SCHMIDT, Klaus. High availability and disaster recovery: concepts, design, implementation. London: Springer, c2006. ISBN 3540244603.

11. Management Mania [online]. 2020 [cit. 2020-04-14]. Dostupné z: https://managementmania.com/

12. System Online: Bezpečnostní politika hesel a vícefaktorová autentizace [online]. 2016 [cit. 2020-04-14]. Dostupné z: https://www.systemonline.cz/it-security/bezpecnostni-politika-hesel-a-vicefaktorova-autentizace.htm

13. KNOPOVÁ, Martina. Bezpečnost dat v informačních systémech. Ikaros [online]. 2011, ročník 15, číslo 6 [cit. 2020-04-14]. Dostupné z: http://ikaros.cz/node/13714

14. KUROSE, James F. a Keith W. ROSS. Počítačové sítě. Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

15. JORDÁN, Vilém a Viktor ONDRÁK. Infrastruktura komunikačních systémů III: integrovaná podniková infrastruktura. Brno: CERM, Akademické nakladatelství, 2015. ISBN 978-80-214-5241-1.

16. Samuraj: VLAN - Virtual Local Area Network [online]. 2007 [cit. 2020-04-14]. Dostupné z: https://www.samuraj-cz.com/clanek/vlan-virtual-local-area-network/

17. PRICE, Ron. CompTIA Server+ Certification Guide: A comprehensive, end-to-end study guide for the SK0-004 certification, along with mock exams. Packt Publishing, 2019. ISBN 978-1-78953-791-8.

18. Programujte: Jak se liší metody šifrování dat? [online]. 2018 [cit. 2020-04-14]. Dostupné z: http://programujte.com/clanek/2018042009-jak-se-lisi-metody-sifrovani-dat/

19. RIPRAN: Metoda pro analýzu projektových rizik [online]. [cit. 2020-04-14]. Dostupné z: https://ripran.cz/

20. RAIS, Karel a Radek DOSKOČIL. Risk management: studijní text pro kombinovanou formu studia. Brno: Akademické nakladatelství CERM, 2007. ISBN 978-80-214-3510-0.

21. SEDLÁK, Petr. Vysoké učení technické v Brně, Fakulta podnikatelská, Kolejní 2906/4, Brno. SAE. [cit. 2020-04-10] Přednáška.

22. TS Bohemia. Https://www.tsbohemia.cz/ [online]. 2020 [cit. 2020-04-27]. Dostupné z: https://www.tsbohemia.cz/

23 PODA [online]. 2020 [cit. 2020-05-05]. Dostupné z: https://www.poda.cz/

24 JON [online]. 2020 [cit. 2020-05-05]. Dostupné z: https://www.jon.cz/

25 Geekbench Browser: Synology DS918+ vs ASUSTOR AS6404T Intel Corporation Apollolake [online]. 2020 [cit. 2020-05-09]. Dostupné z: https://browser.geekbench.com/v4/cpu/compare/11985417?baseline=11985559

SEZNAM POUŽITÝCH ZKRATEK A SYMBOLŮ

GB – Gigabyte

HDD – Hard disk drive

HW – Hardware

ICT – Information and Communication Technologies

LAN – Local Area Network

MAC – Media Access Control

MB – Megabyte

Mbps – Megabite per second

NAS – Network Attached Storage

NIST – National Institute of Standards and Technology

RPO – Recovery Point Objective

RT – Recovery Time

RTO – Recovery Time Object

SLA – Service – Level agreement

SSD – Solid State Drive

SW – Software

TB – Terabyte

VLAN – Virtual Local Network

VPN – Virtual Private Tunel

WAN – Wide Area Network

SEZNAM OBRÁZKŮ

SEZNAM TABULEK