VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
FACULTY OF BUSINESS AND MANAGEMENT

ÚSTAV INFORMATIKY
INSTITUTE OF INFORMATICS

NÁVRH A IMPLEMENTACE PLÁNU ZÁLOHOVÁNÍ DAT SPOLEČNOSTI
DATA BACKUP PROPOSAL AND IMPLEMENTATION FOR THE COMPANY

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. Ondřej Hriadeľ
AUTHOR

VEDOUCÍ PRÁCE — Ing. Jiří Kříž, Ph.D.
SUPERVISOR

BRNO 2019

VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ
FAKULTA PODNIKATELSKÁ

Zadání diplomové práce

Ústav:	Ústav informatiky
Student:	**Bc. Ondřej Hriadeľ**
Studijní program:	Systémové inženýrství a informatika
Studijní obor:	Informační management
Vedoucí práce:	**Ing. Jiří Kříž, Ph.D.**
Akademický rok:	2018/19

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 a implementace plánu zálohování dat společnosti

Charakteristika problematiky úkolu:

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

Cíle, kterých má být dosaženo:

Cílem diplomové práce je návrh a implementace plánu zálohování pro konkrétní společnost. Důvodem ke zlepšení stavu zálohování dat v této společnosti je nekompletní a nedostatečný plán práce s daty.

Základní literární prameny:

BAROT, Gaurav, Chintan MEHTA a Amij PATEL. Hadoop Backup and Recovery solutions. Mumbai: Packt Publishing, 2015. ISBN 978-1783289042.

KOOP, Karsten, Dorian COUGIAS a E.L. HEIBERGER. The Backup Book: Disaster Recovery from Desktop to Data Center. 3rd edition. Schaser-Vartan Books, 2003. ISBN 978-0972903905.

LIU, Ling a M. Tamer ÖZSU. Encyclopedia of Database Systems. New York: Springer, 2009. ISBN 978-0-387-39940-9.

NELSON, Steven. Pro Data Backup and Recovery. New York: Apress, 2011. ISBN 978-1-4302-2-63-5.

PECINOVSKÝ, Josef. Archivace a komprimace dat : jak zálohovat data, jak komprimovat soubory WinRAR, WinZip, WinAce, Windows a nástroje komprese dat, jak archivovat data ve Windows. Praha: Grada, 2003. ISBN 80-247-0659-8.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2018/19

V Brně dne 28.2.2019

L. S.

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

Abstrakt

Tato diplomová práce je zaměřena na návrh a realizaci nového zálohovacího plánu. V úvodní části práce zmiňuji teoretická východiska ohledně problematiky zálohování a práce s daty. Následující kapitola je věnována analýze současného stavu a požadavkům investora. V poslední části navrhuji a implementuji konkrétní řešení zálohovacího plánu s maximálním ohledem na ekonomickou a kvalitativní stránku návrhu. Kromě návrhu a realizaci zálohové plánu se věnuji i návrhu směrnice o zálohování.

Abstract

This diploma thesis is focused on the development of a new backup plan and its implementation. In introductory part of the thesis I explore the theorethical backround of data backup and data management. Next part is dedicated to analysis of current state and investor requierements. Last part is aimed to implementation of new backup plan with focusing on economic and quality point of view. Besides concept and realization of backup plan the concept of the backup directive is created .

Klíčová slova

Záloha dat, ochrana dat, nastavení backup plánu, NAS úložiště, obnova dat, směrnice

Key words

Data backup, data protection, backup plan setup, NAS storage, data recovery, directive

Bibliografická citace

HRIADEĽ, Ondřej. Návrh a implementace plánu zálohování dat společnosti [online]. Brno, 2019 [cit. 2019-05-07]. Dostupné z: https://www.vutbr.cz/studenti/zav-prace/detail/120071. Diplomová práce. Vysoké učení technické v Brně, Fakulta podnikatelská, Ústav informatiky. Vedoucí práce Jiří Kříž.

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 7.května 2019

.....

podpis studenta

Poděkování

Velmi bych chtěl poděkovat vedoucímu své diplomové práce Ing. Jiřímu Křížovi, Ph.D. a oponentu práce doc. Ing. Miloši Kochovi CSc. za konstruktivní připomínky, nápady a myšlenky. Tyto postřehy a čas věnovaný této práci napomohl k jejímu vzniku.

OBSAH

ÚVOD

V dnešní době jsou jednou z nejdůležitějších firemních komodit data. Kdo má data a pracuje s nimi, dosahuje často lepších výsledků než právnické či fyzické osoby, které s daty nepracují. Přestože je tato skutečnost všeobecně známá, společnosti se o svá data nestarají. Nemají navržen plán zálohování, směrnici o zálohovaní a není tak možné zajistit obnovu dat při jejich ztrátě.

Společnost, pro kterou ve své diplomové práci právě tyto problémy pokrývám, si je vědoma důležitosti dat a je ochotna do nich investovat finanční prostředky. Jednatel společnosti si uvědomil, že při ztrátě dat dojde ke kritickým finančním ztrátám s možným koncem společnosti.

V první části této práce se věnuji teoretickým poznatkům z oblasti zálohování. Jsou zde uvedena typy úložišť, možnosti rotací záloh, formáty souborů atd. Další část práce je věnována analýze, která se zabývá HW a SW analýzou a datovou analýzou. Velmi důležitou součástí analýzy je analýza rizik, která zahrnuje kromě analýzy i návrhy opatření pro jednotlivá rizika. Tyto opatření je nutné konzultovat s jednatelem a co největší množství dodržet v průběhu realizace, aby nedošlo ke zbytečným ztrátám dat či nedodržení rozsahu projektu. Návrhová část práce je věnována návrhu zálohovacího plánu tak, aby vyhovoval požadavkům jednatele a odpovídal aktuální situaci v oblasti IT. Poté je tento návrh přenesen do reality a zprovozněn. Předposlední částí je návrh směrnice, která by měla být uzavřena mezi poskytovatelem a odběratelem. Práce je zakončena zhodnocením návrhu a realizace zálohovacího plánu.

CÍL PRÁCE, METODY A POSTUPY ZPRACOVÁNÍ

Cílem diplomové práce je návrh a implementace plánu zálohování pro konkrétní společnost. Důvodem ke zlepšení stavu zálohování dat v této společnosti je nekompletní a nedostatečný plán práce s daty. Jedním z dalších cílů je poskytnout co nejkvalitnější řešení s co nejnižšími náklady na realizaci. Dalším cílem je návrh směrnice o zálohování, aby byly jasně vytyčena práva a povinnosti obou zúčastněných stran této směrnice. Toto téma jsem si vybral, protože se této firmě starám o kompletní správu sítě a mám přehled o technologiích, struktuře firmy a jsem v přímém kontaktu s vedením společnosti.

Pří tvorbě této diplomové práce bylo využito několika metod pro získání informací potřebných k návrhu a realizaci cíle této diplomové práce. Jednatel společnosti obdržel online dotazník s otázkami ohledně aktuálního stavu zálohování ve společnosti. Po vyplnění dotazníku jsem inicioval osobní schůzku, kde jsem pomocí rozhovoru a otázek rozšířil a doplnil odpovědi z dotazníku. Cílem schůzky byla základní určení problému a domluva na základních podmínkách vzájemné komunikace a spolupráce při realizaci zálohovacího plánu.

TEORETICKÁ VÝCHODISKÁ PRÁCE

Tato část práce je věnována teoretickým východiskům z oblasti zálohování dat, druhů zálohování a datových úložišť. Tyto informace poslouží jako podklad pro analytickou a návrhovou část práce.

1.1 Zálohování dat

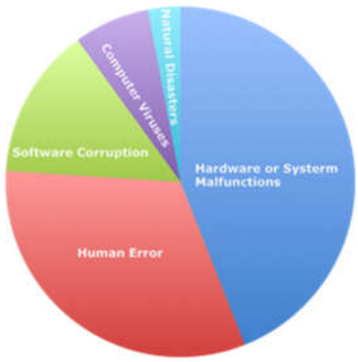
Zálohování dat znamená vytvoření kopií fyzických, virtuálních souborů nebo databází do umístění odlišného od umístění zdrojového. Tyto kopie jsou vytvořeny pro případ poruchy zařízení nebo jiné katastrofy. Zálohování slouží jako jedna ze způsobů ochrany dat. Zálohování zajišťuje obnovu dat při jejich ztrátě. V ideálním případě je vše obnoveno do původního stavu tak, že uživatel nepřijde o žádná data (1)(3).

Záložní kopie by se měly nacházet v jiném umístění než zdrojová data. Je nutné zachovat v úložišti kopií stejnou úroveň ochrany jako v úložišti zdrojovém. Důležitou součástí zálohování je pravidelná kontrola funkčnosti záloh pro nutnost jejich využití (1)(3).

1.2 Příčiny ztráty dat

Zálohovací plány jsou velmi často kritickým bodem společnosti. I přes častá upozornění odborníků nejsou zálohovací plány vytvořeny a dodržovány. Ztráta dat je v těchto případech kritická a má vysoký finanční dopad na uživatele nebo společnost (1)(2)(5).

Příčiny ztráty dat se rozdělují do 5 skupin (viz obrázek číslo 1). Systémové a hardwarové chyby a chyba lidského faktoru jsou nejčastějšími příčinami ztráty dat (5).



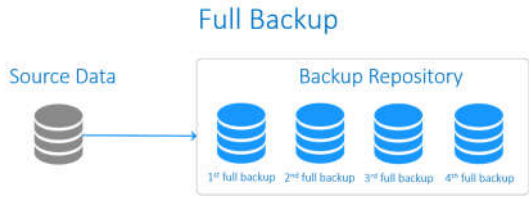
Obr. 1:Nejčastější příčiny ztráty dat (5).

1.3 Typy záloh

Zálohování dat je možné realizovat více odlišnými způsoby. V následující kapitole jsou popsány základní typy metod zálohování.

1.3.1 Úplná záloha (full backup)

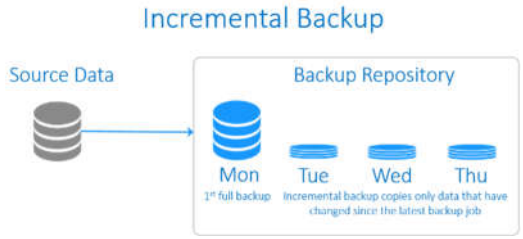
Fullbackup záloha je kompletní záloha veškerých dat uložených na médiu. Při tomto typu zálohování není využíván atribut Archive, ten slouží pro rozlišení zálohovaných a nezálohovaných dat a bude využit v dalších typech záloh. Tento typ zálohování obsahuje všechna zdrojová data. Je to ideální způsob pro vrácení dat do původního stavu. Nevýhodou tohoto typu je časová náročnost. Úplné zálohy jsou ve většině případů prvním krokem pro nastavení inkrementální či rozdílové zálohy (6)(7).



Obr. 2: Schéma plné zálohy (8).

1.3.2 Inkrementální záloha

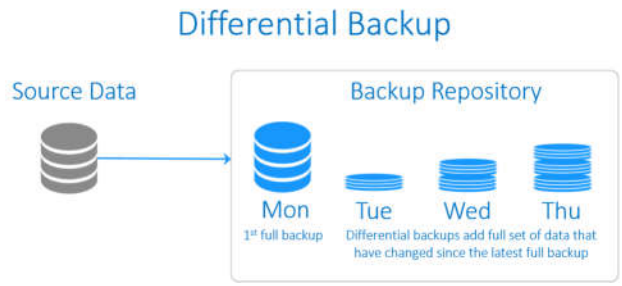
Rozdílem inkrementální zálohy a úplné zálohy je to, že se zálohují pouze data, která mají nastavený atribut Archive. Tento atribut je přidělen datům, která se od poslední zálohy změnila. Další možností je nastavení atributu archiv ručně. Inkrementální záloha není tak časově náročná jako úplná. Není možné obnovit kompletní data. Jednotlivé přírůstkové zálohy tvoří celek a při poruše jedné z nich dochází k nepoužitelnosti ostatních inkrementálních záloh. Pro obnovu tak musíme využít původní úplnou zálohu a následně všechny inkrementální (6)(7).



Obr. 3: Schéma inkrementální zálohy (8).

1.3.3 Rozdílová záloha

Tento typ zálohy zálohuje soubory, které jsou rozdílné od poslední úplné zálohy. Výhodou oproti záloze inkrementální je nezávislost jednotlivých záloh. Při nemožnosti obnovit jednu rozdílovou zálohu tak neztrácíme všechny ostatní verze záloh. Pro obnovu dat z rozdílové zálohy je nutné mít poslední úplnou zálohu a příslušnou rozdílovou (7)(8)(9).



Obr. 4: Schéma rozdílové zálohy (8).

1.3.4 Mirror záloha

Tento typ zálohy funguje na stejném principu jako záloha plná. Rozdílem oproti plné záloze je uchování verzí. Tato záloha udržuje pouze poslední verzi zálohovaných dat a vytváří přesnou kopii zdrojových dat. Výhodou tohoto typu je velmi krátká časová náročnost obnovy. Nevýhodou je nutnost zachování bezpečnostních politik a zdvojení prostoru datového úložiště (8)(10).

1.4 Zálohovací média

Kapitola zálohovací média je věnována nejpoužívanějším hardwarovým prvkům pro ukládání dat (HDD disk, SSD disk a magnetické pásky).

1.4.1 Hard disk drive

Hard disk drive je fyzický pevný disk sloužící pro ukládání dat. Funguje na principu magnetického záznamu, který je ukládán na rotující plotny disku. Tyto plotny jsou poháněny elektro motory. Standartní rychlosti otáčení ploten jsou 5400, 7200 a 10 000 otáček za minutu. Čím je tato hodnota vyšší, tím je vyšší i přenosová rychlost. Základní velikosti disků jsou 3,5“ a 2,5“. Nevýhodou tohoto typu média je náchylnost na poškození hlavně v oblasti mechanického poškození (11).

1.4.2 Solid state drive

Tento typ datového média neobsahuju žádné pohyblivé mechanické části. Data se v tomto typu disků ukládají do Flash pamětí. Výhodou je vyšší rychlost, menší spotřeba energie, tichost, a především menší náchylnost na mechanické poškození (12).

1.4.3 Magnetické pásky

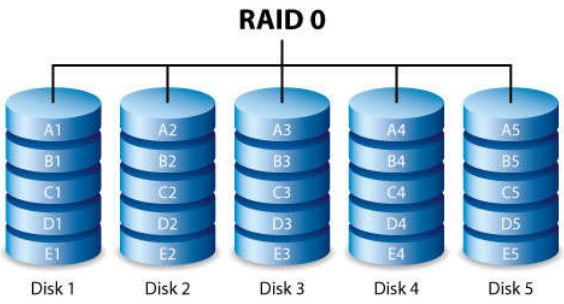
U magnetické pásky je záznamovým médiem magnetická vrstva nanesená na plastové nebo hliníkové části pásky. Výhodou magnetických pásek je nízká cena. Nevýhodou je cena zařízení využívajících magnetické pásky, tyto zařízení bývají velmi nákladné. Magnetické pásky jsou nejvyužívanější pro data, jejichž množství čítá desítky TB (13).

1.5 Diskové pole RAID (Redundant Array of Independent Disks)

Technologii RAID chápeme jako redundantní pole nezávislých disků. Jedná se o propojení více fyzických celků do jednoho logického. Cílem technologie RAID je zajištění redundance a zvýšení výkonnosti disků. Využití technologie RAID je nejčastěji u souborových serverů, datových úložišť atd (14).

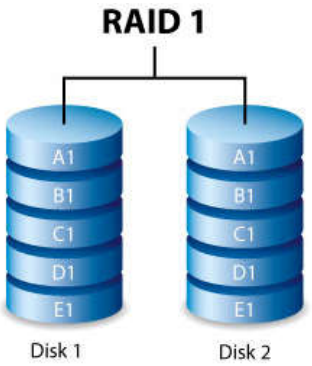
1.5.1 RAID 0

Úroveň RAID 0 je označována jako překládání. Data ukládaná v této úrovni jsou data nejdříve rozdělena na bloky a ty jsou pak rozděleny na jednotlivé disky. V praxi to znamená, že když máme v sadě 4 disky, tak se část dat zapíše na první disk, část na druhý, část na 3 a část na čtvrtý disk. Výhodou tohoto řešení je primárně rychlost řešení. Velkou nevýhodou je absence redundance. Při zničení jednoho z disků dochází k znehodnocení celého pole (14)(15)(16).



1.5.2 RAID 1

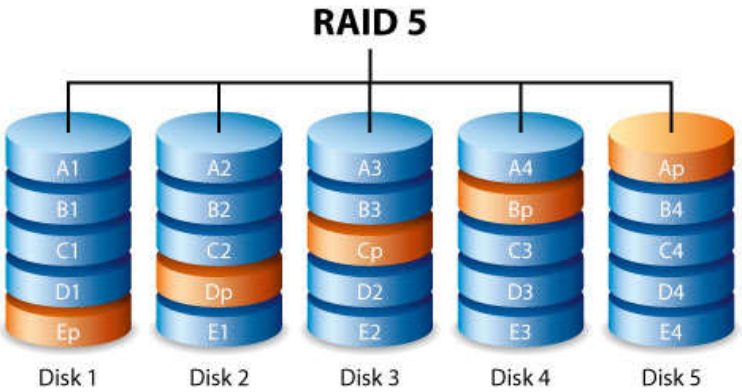
Úroveň RAID 1 je také nazývaná zrcadlení. Disky zapojené do RAID 1 jsou navzájem zrcadleny a data jsou ukládána na oba disky. Pole je schopno obnovy dat na základě rovnice n-1(n=počet disků). Pokud jsou v disku zapojeny 4 disky, tak pokud zůstane alespoň jeden funkční, tak jsme schopni data obnovit. Kapacita celého pole je rovna velikosti nejmenšího disku. Nevýhodou je pomalý zápis dat, protože se data zapisují 2x. Velkou výhodou je zde funkční redundance oproti RAID 0 (14)(15)(16).



Obr. 5: RAID 1 (16).

1.5.3 RAID 5

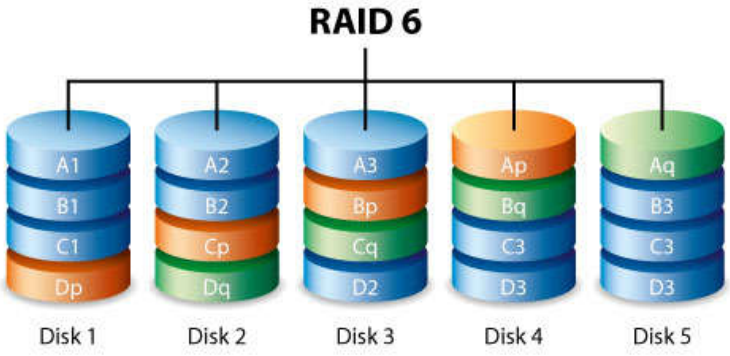
Technologie RAID 5 vyžaduje pro realizaci nejméně 3 disky. Funkčnost tohoto řešení je založena na paritních datech. Selhání jednoho disku tak nezpůsobí pád celého pole, protože paritní data se dopočítají na ostatních discích a pole funguje dál. Při selhání jednoho disku jsou tak operace směřovány na ostatní disky v poli (14)(15)(16).



Obr. 6: RAID 5 (16).

1.5.4 RAID 6

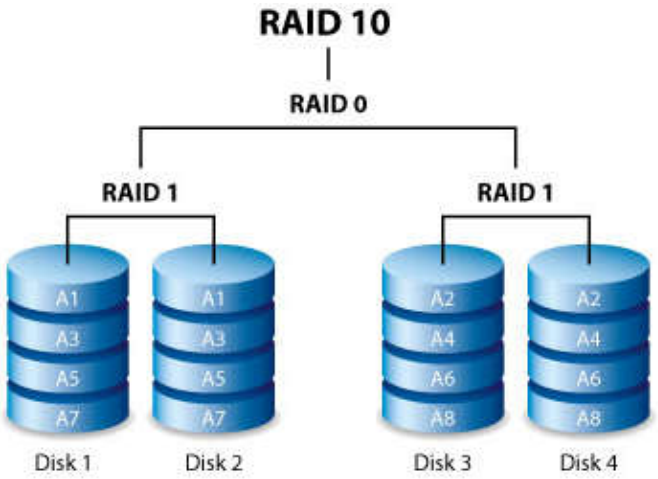
Technologie RAID 6 funguje na stejném principu jako RAID 5 s tím rozdílem, že zde funguje vícenásobná parita. Obnova dat je možná i při selhání dvou disků v poli. Nevýhodou technologie RAID 6 jsou ještě vyšší nároky na výpočetní výkon. Technologie RAID 6 je pomalejší než RAID 5 (14)(15)(16).



Obr. 7: RAID 6 (16).

1.5.5 RAID 10

Tato technologie je spojením RAID 0 a RAID 1. Minimální počet disků jsou 4. Nejdříve se vytvoří dvě RAID 1 pole a nad nimi je postaven RAID 0. Výhodou tohoto řešení je kombinace rychlosti a spolehlivosti. Nevýhodou je zdvojení počtu disků pro realizaci oproti ostatním RAID technologiím. Tato technologie přebírá nevýhody technologií RAID 0 a RAID 1 (14)(15)(16).



Obr. 8: RAID 10 (16).

1.5.6 Hot swap

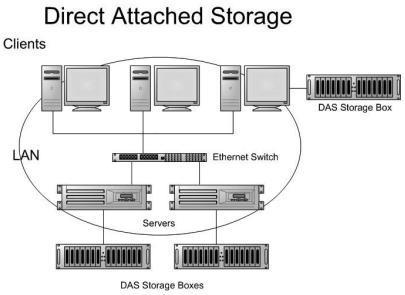
Společně s diskovým polem RAID je nutné vysvětlení pojmu Hot swap, který je pro pole velmi důležitý. Tato funkce disku zajišťuje možnost vyjmutí disku za plného provozu a nahrazení disku jiným. Nový disk musí být stejného rozhraní (nejlépe i výrobce) a musí mít stejnou nebo větší velikost (14)(15).

1.6 Datová úložiště

Cílem této kapitoly je popis 3 typů zapojení datových úložišť do firemní sítě: NAS (Network attached storage), DAS (Direct Attached Storage) a SAN (Storage Area Network). Hlavním účelem datových síťových úložišť je vzdálený přístup a možnosti zálohování vzdáleně. Dalším účelem je přesun dat mezi servery a úložišti. Z hlediska bezpečnosti je doporučeno, aby byla tato zařízena oddělena do vlastní sítě.

1.6.1 DAS (direct attached storage)

Jak napovídá název tohoto typu připojení, jedná se o přímé připojení k zařízení (např. serveru). Úložiště DAS má více typů: CD/DVD/Blueray mechaniky, všechny druhy disků, disková pole a další. Výhodou tohoto typu zařízení je vyšší přenosová rychlost, protože přenos dat není realizován přes internet. Nevýhodou je omezená dostupnost, protože úložiště typu DAS je přístupné pouze přímo ze zařízení, ke kterému je připojené.

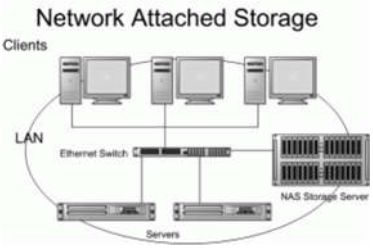


Obr. 9: DAS (17).

1.6.2 NAS (network attached storage)

Dalším způsobem pro ukládání dat je technologie NAS. Tato technologie funguje na principu úložiště připojeného do sítě. Výhodou NAS je možnost nastavení práv pro uživatele a vzdálený přístup za příznivých nákladů a efektivního řešení. V dnešní době jsou NAS koncipovány jako „malé servery“ – skládají se z jednoho či více disků, paměti

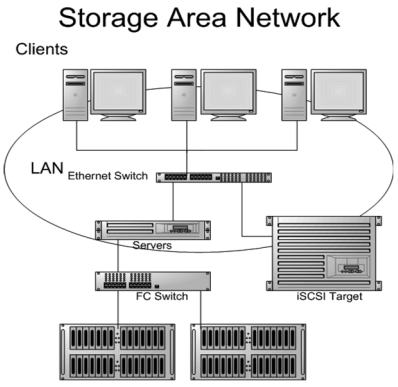
RAM, síťové karty, SW pro správu. Pokročilejší NAS servery mají možnost hotswap disků a samozřejmě řadiče RAID. Systémy NAS jsou také spolehlivým řešením pro zálohování mimo firemní síť.



Obr. 10: NAS (17).

1.6.3 SAN (storage area network)

Úložiště tohoto typu jsou vyžívána ve velkých společnostech, které zpracovávají velká množství dat. SAN je síť určená přímo pro práci s daty, Tato síť je oddělena od sítí LAN a WAN, což usnadňuje následnou obnovu dat a zkracuje reakční dobu obnovy. Výhodou SAN je lepší práce s daty, bezpečností i managementem díky nezávislosti na jednom zařízení jako je to u DAS. Další výhodou je ušetření využití hw kapacity firemních serverů, protože SAN síť funguje jako samostatný prvek. Nevýhodou jsou prvotní náklady. Potenciální nevýhodou je neznalost správce sítě, který může způsobit porušení integrity špatně nastavenou autorizací.



Obr. 11: SAN (17).

1.6.4 Zálohování pomocí FTP serveru

Další možností uložení dat je využití FTP serveru. Tento způsob funguje na principu FTP (file transfer protocol). FTP server zde vystupuje jako vzdálené úložiště dat. Dnes je již FTP nahrazeno FTP s podporou SSL/TLS šifrování nebo SFTP (secure fite transfer

protocol), který využívá SSH. Tyto metody byly zavedeny hlavně z důvodu zvýšení bezpečnosti (18).

1.7 Cloud computing

Cloud computing je koncept založený na pronajmutí výpočetního výkonu a hw techniky mimo lokální síť. Společnost Microsoft definuje cloud computing jako (19):

„Jednoduše řečeno je cloud computing doručování výpočetních služeb, jako jsou servery, úložiště, databáze, sítě, software, analytické nástroje, inteligentní funkce a další, přes internet („cloud“) a nabízí rychlejší inovace, flexibilitu prostředků a úspory z rozsahu (19).“

Hlavními výhodami cloud computingu jsou investiční náklady na nákup HW a SW oproti řešení na vlastní infrastruktuře. Často opomínaným ušetřeným nákladem je pracovník IT, který se o infrastrukturu stará. Velkou výhodou cloud computingu je variabilita. Při rozšíření technologií je výrazně jednodušší rozšířit cloudové služby než rozšiřovat vlastní infrastrukturu. Cloudová řešení jsou poskytována poskytovateli cloudových služeb, kteří dodávají požadované výpočetní prostředky. Jako příklad těchto cloudových řešení můžeme uvést Microsoft Azure, Google cloud platformy nebo například Amazon web services (19)(20).

1.7.1 Typy cloudových služeb

Cloudové služby dělíme do 3 základních skupin: infrastruktura jako služba, platforma jako služba a software jako služba (19).

1.7.1.1 Infrastruktura jako služba (Iaas)

Tato kategorie služeb je aktuálně jednou z nejvyužívanějších. V rámci Iaas dochází k nahrazení primárně serverové infrastruktury: jsou pronajímány servery, síťové prvky, úložiště atd. (19).

1.7.1.2 Platforma jako služba (Paas)

Platforma jako služba poskytuje zázemí pro vývoj, testování, distribuci aj. software. Jedná se o řešení pro vývojáře a programátory. Výhodou řešení je již nakonfigurovaná infrastruktura a uživatel nemusí provádět základní nastavení (19).

1.7.1.3 Software jako služba (Saas)

Toto řešení již dodává koncovým uživatelům konkrétní aplikační řešení. Velkou výhodou tohoto řešení je rychlá a bezproblémová implementace nových patchů nebo verzí aplikací (19).

ANALÝZA PROBLÉMU A SOUČASNÁ SITUACE

Tato část práce je věnována analýze současného stavu. První část se věnuje představení společnosti. Další částí pak analýze dat, která jsou zálohována, a HW i SW vybavením společnosti. V posledních dvou částech pak aktuálnímu stavu zálohování a požadavkům jednatele firmy.

2.1 Představení společnosti

Pro svoji diplomovou práci jsem si vybral společnost, pro kterou pracuji jako správce sítě. Firma si nepřála být jmenována. Jedná se o společnost podnikající v oblasti prodeje výživových doplňků a věcí potřebných pro fitness.

Společnost má 65 zaměstnanců, kteří pracují dohromady v 5 pobočkách. Hlavní sídlo společnosti je v Brně v ulici Tkalcovská. Tři pobočky jsou v Brně (Cimburkova ulice, Smetanova ulice, Nádražní ulice). Poslední pobočka se nachází v Praze na Kubánském náměstí.

Hierarchie společnosti je zobrazena na obrázku č.12. Společnost řídí jednatel, kterému jsou podřízení vedoucí jednotlivých oddělení (oddělení e-shopu, personální, finanční o, nákupní, sklad, stížnosti od uživatelů). Jedná se o liniovou hierarchii.

Obr. 12: Hierarchie společnosti (vlastní).

Situace v oblasti IT je složitá, protože o počítačovou síť se starají 4 subjekty. Jedna společnost je správcem účetního systému Pohoda, druhá je společnost zajišťující skladový systém, třetí oddělení e-shopu společně s externistou a posledním subjektem je společnost, která zajišťuje fungování celé sítě a propojení jednotlivých oblastí do funkčního systému.

2.2 Analýza dat

Tato část práce je věnována analýze dat, která ve společnosti vznikají.

2.2.1 Sdílená data na projekty

Společnost v průběhu čtvrtého kvartálu roku 2017 přešla z poskytovatele emailu Microsoft Exchange na služby Gsuite od společnosti Google. Sdílená data jsou ukládána zde a jsou přístupná přes aplikaci Google Drive. Původní sdílené úložiště bylo zrušeno a všechna data přesunuta na Google úložiště. Zálohování tohoto úložiště není předmětem diplomové práce, protože za uchování těchto dat zodpovídá společnost Google.

2.2.2 Data jednotlivců

Data jednotlivců vznikají ve firmě z nástrojů MS Office, konkrétně se jedná o verzi Office 365 pro firmy. Jde se o dokumenty typu doc., docx, xlxs, ppt., txt. apod. Velikost dokumentů se pohybuje od 0-10 MB. Tato data slouží pro potřeby smluv, formulářů, záznamů z porad, poznámek atd.

2.2.3 Analytické nástroje

Firma využívá software na analýzu dat a výsledků, zároveň jsou využívány i analytické nástroje a doplňky aplikace MS Excel. Tyto soubory mají velikost 0-20 MB a jedná se o dokumenty, které zajišťují možnosti analýzy provozu a fungování společnosti (např. množství objednávek atd.).

2.2.4 Data z účetních programů

Toto jsou jedny z kritických dat společnosti uchovávané pomocí MS SQL Serveru. Velikost dat je do stovky 100 GB, protože do účetního programu vstupují částečně i data ze skladového systému a e-shopu.

2.2.5 Data z e-shopu

Zálohu e-shopu a dat na e-shopu si řeší a odpovídá tým e-shopu sám a nebude předmětem této diplomové práce.

2.2.6 Data ze skladového systému

Stejně jako u e-shopu, poskytovatel skladového systému zálohuje hlavní data ze skladového systému pomocí svého vlastního cloudového řešení, a nebudou tak předmětem této práce.

2.3 Analýza HW

Tato část práce je věnována HW používanému ve společnosti. HW analýza je rozdělena do podkapitol podle typu HW.

2.3.1 Diskové pole

Společnost má nově zakoupené diskové pole od společnosti DELL. Konkrétně se jedná o typ Dell PowerVault MD3400. Diskové pole obsahuje celkem 8 disků. Jejich zapojení je zobrazeno v tabulce číslo 1.

Tab. 1: Zapojení disků v diskovém poli (vlastní).

Enclosure, Drawer	Slot:	Manufacturer:	Physical Disk Type:	Capacity (GB)	Typ zapojení
Enclosure 0	Slot 0	SAMSUNG	Seriál Attached SCSI	273,896	RAID10
Enclosure 1	Slot 1	SAMSUNG	Seriál Attached SCSI	273,896	RAID10
Enclosure 2	Slot 2	SAMSUNG	Seriál Attached SCSI	273,896	RAID10
Enclosure 3	Slot 3	SAMSUNG	Seriál Attached SCSI	273,896	RAID10
Enclosure 4	Slot 4	HGST	Seriál Attached SCSI	273,896	RAID1
Enclosure 5	Slot 5	HGST	Seriál Attached SCSI	273,896	RAID1
Enclosure 6	Slot 7	SEAGATE	Seriál Attached SCSI	1112,314	RAID5
Enclosure 7	Slot 8	SEAGATE	Seriál Attached SCSI	1112,314	RAID5
Enclosure 8	Slot 9	SEAGATE	Seriál Attached SCSI	1112,314	RAID5

2.3.2 Serverové vybavení společnosti

Společnost má 2 fyzické servery propojené do clusteru (CLST1 a CLST2). Datové úložiště je zajištěno diskovým polem od společnosti DELL. Datové úložiště je složeno z disků typu HDD i SSD, na discích SSD běží systémy jednotlivých serverů a HDD disky slouží pro uložení dat.

Fyzické servery jsou také od společnosti DELL, jedná se o typ PowerEdge R430. Výhodou těchto serverů je 1U řešení ideální do racku a také vzdálená správa pomocí iDRAC8 Enterprice.

Tab. 2: Specifikace fyzický server (vlastní).

Typ	DELL PowerEdge R430
Procesor	Intel Xenon – Skylake 6.generace
Operační paměť	V základu 16 GB, rozšířeno na 64 GB

2.3.3 Stanice

V prodejnách (Cimburkova, Nádražní, Tkalcovská a Kubánské náměstí) jsou využívány PC sestavy od společnosti DELL. Konkrétně se jedná o typ Dell OptiPlex 3050 SFF.

Tab. 3: Specifikace stanice pro prodejny (vlastní).

Procesor: **Intel Core i5 7500 Kaby Lake**
RAM: **8 GB DDR4**
Grafická karta: **Intel HD Graphics 630**
Disk: **SSD 256 GB**
Operační systém: **Windows 10 PRO**

Administrativní zaměstnanci (HR oddělení, finanční oddělení a nákupní oddělení) mají k dispozici notebooky od společnosti Lenovo. Jedná se o různé modely, které se měnily v průběhu let, vždy ale se stejnou konfigurací:

Tab. 4: Specifikace stanice pro administrativní zaměstnance (vlastní).

Procesor: **Intel Core i5 (5.,6. a 7. generace)**
RAM: **8 GB DDR4**
Grafická karta: **Integrovaná grafická karta poskytovaná výrobcem**
Disk: **SSD 256 GB**
Operační systém: **Windows 10 PRO**

Oddělení zabývající se marketingem a grafikou potřebuje výkonnější stroje. Toto oddělení má proto, stejně jako jednatel firmy, k dispozici notebooky od společnosti Apple, které jsou vhodné pro tvorbu a úpravu kreativního obsahu marketingového oddělení. Specifikace těchto zařízení je uvedena v tabulce číslo 5.

Tab. 5: Specifikace stanice pro marketingové oddělení (vlastní).

MacBook Pro 13" Retina
Procesor: **Intel Core i7 2.7 GHz**
RAM: **16 GB LPDDR3**
Grafická karta: **Intel Iris Plus Graphics 655**
Disk: **SSD 512 GB**

2.3.4 Ostatní zařízení

Kromě výše zmíněných zařízení jsou ve firmě routery od společnosti Mikrotik. Kromě routerů se ve společnosti nacházejí switche od společnosti Zyxel. Přehled zařízení Mikrotik je uveden v tabulce č.6. Přehled zařízení Zyxel v tabulce číslo 7.

Tab. 6: Přehled zařízení Mikrotik v interní sít(vlastní).

Pobočka	**Typ routeru**	**Celkový počet(ks)**
Sídlo společnosti (serverovna)	Mikrotik RB3011UiAS	1
Pobočky	Mikrotik RB951G-2HnD	4

Tab. 7: Přehled zařízení Zyxel v interní síti (vlastní).

Pobočka	**Typ Switche**	**Celkový počet(ks)**
Sídlo společnosti (serverovna)	Zyxel GS1920-48	6
Pobočky	Zyxel GS1920-24	4

Wifi připojení je zajištěno zařízeními od společnosti Unifi. Na pobočkách je umístěno vždy jedno zařízení UniFi AP-AC-LR s výjimkou prodejny v Letmu, kde jsou zařízení dvě. Ve skladu je 6 zařízení UniFi AP-AC-LR, aby byl celý sklad pokryt signálem a bylo možné využívat čtečky čárových kódů využívající WiFi připojení. Další dvě zařízení UniFi AP-AC-LR jsou umístěna v kancelářích v sídle společnosti.

Ve společnosti je využito 31 IP kamer od společnosti Hikvision, které pokrývají prostory skladu, balíren, prodejen a důležitých prostor. Všechny tyto kamery jsou sdružovány ve dvou NVR také od firmy Hikvision. Přehled kamerového systému je zobrazen v tabulce č.7.

Tab. 8: Přehled zařízení pro kamerový systém (vlastní).

Zařízení	Využití zařízení	Počet zařízení(ks)
NVR DS-7616NI-E2/A	Primárně slouží pro kamery umístěné ve skladu.	1
NVR DS-7732NI-K4	Primárně slouží ke sdružování kamer na jednotlivých pobočkách.	1
Kamera DS-2CD2055FWD-I	Online sledování provozu na pobočkách a ve skladu.	31

Ve společnosti byla nově koupena NAS Synology se dvěma 8TB disky. Minulý IT správce na NAS nastavil pouze základní funkce a nevyužil tak potenciál zařízení. Konkrétně se jedná o model Synology DS218+, kam je možné vkládat 2 SATA disky s kapacitou až 20TB dat. Základní parametry jsou uvedeny na obrázku číslo 13.

Obr. 13: Parametry HDD (34).

2.4 SW analýza

Tato část práce bude věnována SW využívanému ve společnosti. Všechny stanice, kromě stanic od společnosti Apple, mají nainstalovaný operační systém Windows 10 PRO, aby bylo možné jejich připojení do domény a využití pokročilých funkcí operačních systémů Windows a aby byla zajištěna lepší kontrola nad zařízeními.

2.4.1 MS Office + Google Apps

Pro tvorbu základních dokumentů jsou využívány aplikace MS Office a Google Apps. U společných a sdílených souborů jsou využívány Google Apps, zatímco pro dokumenty MS Office.

2.4.2 Kancelářské programy

Kromě výše zmíněných programů pro vytváření a správu dokumentů jsou využívány programy pro standardní uživatelskou přívětivost zařízení: VLC player, Adobe reader, 7-Zip, Google Chrome, Mozilla Firefox, Mozilla Thunderbird, případně další programy podle přání uživatelů. Každé klientské zařízení má nainstalovaný Eset Antivirus, zajišťující zabezpečení PC.

2.4.3 Účetní a personální programy

Ve firmě jsou využívány produkty od společnosti Stormware-Pohoda pro účetní transakce a vedení účetnictví, a Pamica pro veškerou agendu týkající se personalistiky. Program Pohoda slouží i pro synchronizaci účetnictví s pokladnami v prodejnách a kontrolu EET. Software Pohoda také kontroluje množství a převzetí zboží na jednotlivých prodejnách.

2.4.4 Serverový SW

Všechny servery mají nainstalovaný operační systém Windows server 2012R2.
Na serverech CLST1 a CLST2 je spuštěno Hyper-V, kde jsou vytvořeny 4 další virtuální servery.
Tyto virtuální servery jsou spravovány z clusterů pomocí aplikace Failover Clustering.

Úlohy virtuálních serverů:

DC1: Domain controler 1 plní tyto funkce: Active Directory, DNS server, DHCP server, ERA controler, Unifi controler, Windows Backup, Print server. Kromě těchto základních funkcí zde běží dvě aplikace sloužící k synchronizaci AD s Gsuite (Google Password Sync a Google cloud directory sync).

DC2: Domain controler 2 představuje replikaci DC1. Je nutné, aby byl zajištěn provoz Google password sync (nutnost běhu na všech DC v síti), který slouží k synchronizaci hesel s prostředím Gsuite.

Terminál: Terminálový server má využití pro připojení uživatelů mimo firemní síť. Běží zde instance Pohody a Pamici, program na prohlížení kamerových záznamů a Micrososft Power BI.

SQL1: Na SQL serveru běží program MS SQL Management Studio, který zajišťuje chod databáze pro Pohodu a Pamicu. i pro nástroj Power BI. Tento server také udržuje základní rozšíření Pohody: Mserver. Spouští se zde synchronizační skripty pro skladový systém, e-shop a Pohodu. Důležitou součástí tohoto serveru jsou naplánované úlohy, které řídí propojení databází, synchronizace jednotlivých součástí systému, exporty dat, archivaci logů atd. Kromě naplánovaných úloh je velmi důležitou součástí nastavení a provoz ODBC. Tato serverová aplikace zajišťuje přístup API z e-shopu do Pohody a spárování jednotlivých položek.

BCU1: Zálohovací server slouží jako sběrnice dat při jednotlivých zálohovacích úlohách. Některé zálohy probíhají přes FTP, proto jsou na serveru povoleny služby IIS a FTP, aby bylo možné server takto využívat.

2.5 Aktuální stav zálohování

Zálohování je v kritickém stavu. Velkým problémem je zálohování serverů, které probíhá pomocí aplikace Windows backup od společnosti Microsoft, ale pouze tak, že se servery zálohují „samy na sebe“. Jeden disk se tak zálohuje na jiný, vše v rámci serveru, takže pokud dojde ke zkratu, výpadku elektřiny nebo jiné vážné technické závadě v průběhu zálohování serveru, jsou ztracena nastavení, konfigurace serverů a také veškerá data, která jsou na serverech uložena.

Uživatelské stanice nejsou nijak zálohovány ani ošetřeny. Je pouze na uživateli, která data si sám zálohuje. Tento problém je nejkritičtější u zaměstnanců managementu. Ztráta dat z jejich zařízení může být pro firmu naprosto devastující, protože se jedná o data spojená s firemním „know-how“ a fungováním společnosti.

Data ze SQL1 serveru propojeného s účetními a personálními programy se zálohují pouze na DC1 a sama na sebe na SQL1. To je u těchto kritických dat velmi nebezpečné a rizikové řešení.

Konfigurace jednotlivých kamer, NVR, AP, AP controleru nejsou zálohovány žádným způsobem a ztráta těchto souborů může zavinit nefunkčnost celé počítačové sítě ve společnosti.

2.6 Směrnice

V rámci prvotní analýzy proběhla také kontrola směrnic a krizových plánů při ztrátě dat. U společnosti bylo zjištěno, že krizové plány nejsou vypracovány vůbec, což může mít při ztrátě dat naprosto kritický dopad na celou společnost a prodloužit tak čas obnovení systému do původního stavu.

Interní směrnice jsou ve firmě vypracovány na velké množství oblastí. Nejsou však zaměřeny na problematiku zálohování, klasifikaci a uchování dat. Tato směrnice je velmi důležitým dokumentem a slouží jako zajištění odpovědnosti v oblasti zálohování a práce s daty pro celou společnost. Směrnice o zálohování dat a určení práv a povinností zaměstnanců i poskytovatele může velmi dobře posloužit jednateli společnosti jako doplňkový nástroj pro její řízení.

2.7 Analýza rizik

V této kapitole byla vypracována analýza rizik. Tato rizika by mohla vzniknout při realizaci zálohovacího plánu. K analýze rizik byla využita skórovací metoda Jednotlivá rizika jsou rozdělena do skupin podle zaměření. V další části jsou navržena opatření, která by měla být akceptována při návrhu řešení a jeho realizaci, aby byla rizika při realizaci co nejvíce snížena.

2.7.1 Ohodnocení rizik

V následující tabulce jsou jednotlivá rizika ohodnocena na škále 1 – 10. Rizika jsou rozdělena do skupin podle profesní oblasti, které se týkají – projektová, bezpečnostní, technologická, ekonomická a právní. Pravděpodobnost vzniku rizika označíme P, dopad rizika na funkčnost systémů D. Celkovou hodnotu rizika H získáme vynásobením P x D. Údaje H zaneseme do mapy rizik (tabulka č.9). Na základě vyhodnocení této mapy navrhneme adekvátní řešení. Cílem je pokrýt především rizika, která spadají do oblasti Kritické a Významné riziko. V tabulce 10 jsou zobrazena konkrétní hodnoty sledovaných rizik. Z výsledků je zřejmé, že do kategorie Kritická rizika spadá 1 hrozba, do kategorie Významná rizika spadá 11 hrozeb, do kategorie Běžné riziko 1 hrozba a do kategorie Bezvýznamné riziko 1 hrozba. Po dohodě s jednatelem společnosti byla navržena opatření

ke snížení nebo odstranění rizika pro všechny kategorie rizik –od bezvýznamných až po kritická.

Tab. 9:Hodnotící: mapa rizik (vlastní).

Dopad	Významné riziko	Kritické riziko
	Bezvýznamné riziko	Běžné riziko
1	1 Pravděpodobnost	10

Mapu rizik je možné vyobrazit jako čtyři kvadranty o rozsahu 5x5 na základě kterých hodnotíme významnost rizika. Jak bylo zmíněno výše pro kritická rizika je nutné navrhnout a řídit se opatřeními. Po dohodě s jednatelem společnosti byla navržena opatření pro všechny druhy rizik od bezvýznamných až po kritická rizika. Analýza rizik byla konzultována s externistou, aby byla pokryta co největší oblast možnosti vzniku incidentu a zajištěna objektivnost analýzy rizik. V tabulce č.10. jsou již zobrazena konkrétní hrozby a scénáře, které mohou vznikat společně s realizací. V tabulce číslo 10 jsou také již určeny konkrétní hodnoty pro pravděpodobnost, dopad a hodnotu.

Tab. 10: Seznam rizik projektu (vlastní).

ID	Hrozba	Scénář	P	D	H	
	Projektová rizika					
1	Nedostatečná komunikace zúčastněných stran	Nefunkčnost systému, nepřipravení uživatelé, nespokojenost na obou stranách.	2	7	14	Významné riziko
2	Podcenění prvotní analýzy	Nedostatečné řešení, nefunkčnost řešení, nedodržení smluvních podmínek	4	8	32	Významné riziko
3	Špatně navržené řešení	Nedostatečné řešení, nefunkčnost řešení, nedodržení smluvních podmínek	3	8	24	Významné riziko
4	Nedodržení časového plánu	Nedodržení smluvních podmínek nefunkční systém.	5	8	40	Významné riziko
	Bezpečnostní rizika					
5	Při rekonfiguraci porušení bezpečnostních politik	Narušení systému, smazání veškerých záloh.	3	10	30	Významné riziko
6	Špatně nastavená politika přístupu uživatelů	Ztráta či únik dat a záloh.	4	10	40	Významné riziko
7	Fyzické odpojení zařízení	Nefunkčnost zálohovacího plánu->ztráta dat.	3	9	27	Významné riziko
8	**Technologická rizika**					
9	Nefunkčnost zařízení - mechanická závada	Nefunkčnost zálohovacího plánu->ztráta dat.	5	6	30	Významné riziko
10	Opotřebení zařízení stářím	Nefunkčnost zálohovacího plánu->ztráta dat.	2	6	12	Významné riziko
11	Změna technologií	Nefunkčnost zálohovacího plánu->ztráta dat.	9	9	81	Kritické riziko
12	**Ekonomická rizika**					
13	Nečekané náklady	Navýšení ceny projektu	7	4	28	Běžné riziko
14	Změna cen používaných systémů	Navýšení ceny projektu	1	4	4	Bezvýznamné riziko
17	Vývoj trhu	Nedostatek prostředků na zaplacení projektu	3	10	30	Významné riziko
18	**Právní rizika**					
19	Špatně definované smluvní podmínky	Nejasnosti, neodpovědnost za škody atd.	5	7	35	Významné riziko

2.7.2 Návrh opatření rizik

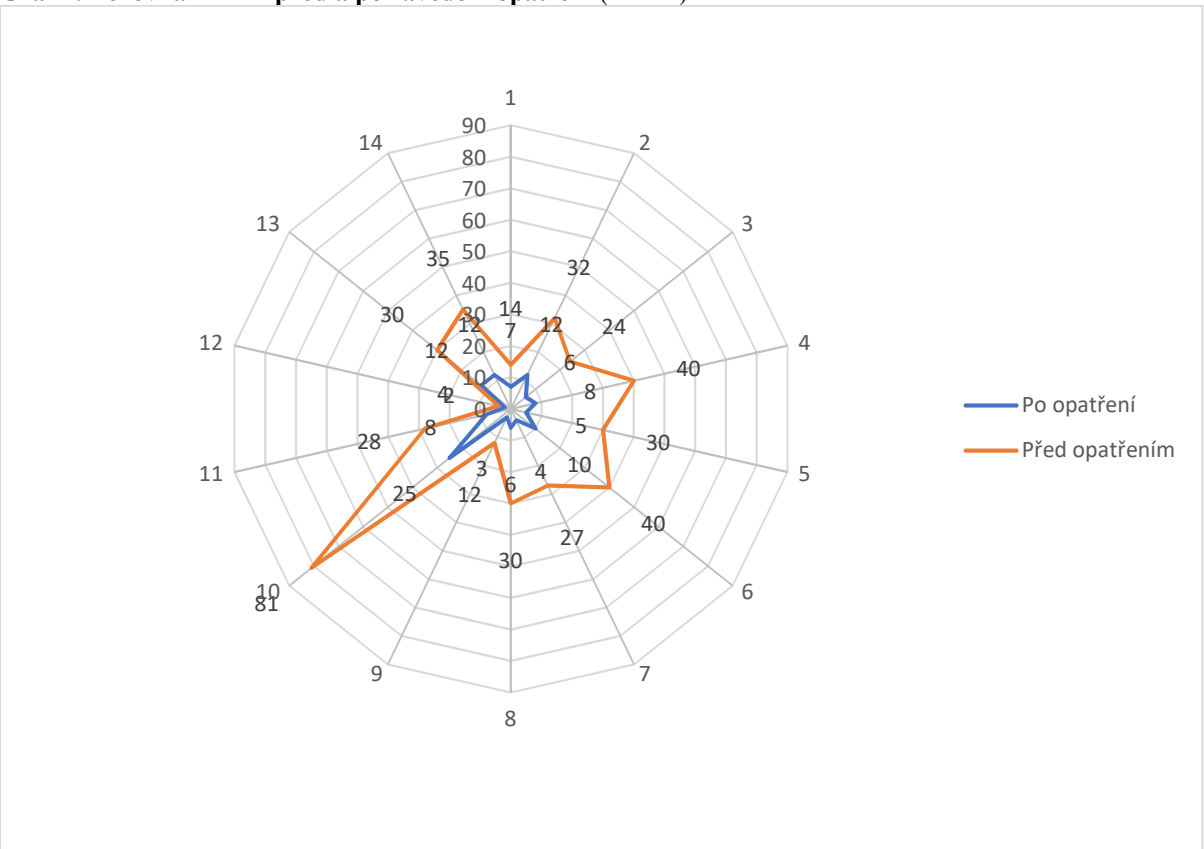
Tabulka číslo 11. vyobrazuje a navrhuje opatření pro rizika. Velmi často postačí správně nastavené kroky v první fázi projektu tzn. Kvalitní analýza, dobře nastavené smluvní podmínky a konzultace změny s externistou. Pokud společnost následující opatření zavede, měla by realizace změny proběhnout bez větších problémů. Rizika tu stále jsou, ale již v tolerovatelné míře.

Tab. 11: Seznam opatření pro rizika (vlastní).

ID	Hrozba	Opatření	P	D	H
	Projektová rizika				
1	Nedostatečná komunikace zúčastněných stran	Pravidelné porady, reporting, smluvní podmínky	1	7	7
2	Podcenění prvotní analýzy	Důkladná analýza ošetřená smluvně, nezávislý pohled externisty	2	6	12
3	Špatně navržené řešení	Konzultace s externistou, více nabídek, kvalitní analýza	1	6	6
4	Nedodržení časového plánu	Ošetření smluvních podmínek, penalizace	2	4	8
	Bezpečnostní rizika				
5	Při rekonfiguraci porušení bezpečnostních politik	Kvalitní analýza, kontrola a důkladné testování, plán změny	1	5	5
6	Špatně nastavená politika přístupu uživatelů	Testování řešení a politik, zálohy již před ostrým spuštěním	2	5	10
7	Fyzické odpojení zařízení	ISMS, fyzická bezpečnost a přístup k serverovému vybavení	1	4	4
8	**Technologická rizika**				
9	Nefunkčnost zařízení - mechanická závada	Podpora, záruka	2	3	6
10	Opotřebení zařízení stářím	Monitoring HW, smluvní povinnost	1	3	3
11	Změna technologií	Sledování aktuálních trendů, pravidelný reporting od poskytovatele	5	5	25
12	**Ekonomická rizika**				
13	Nečekané náklady	V projektu zahrnout rezervu	4	2	8
14	Změna cen používaných systémů	V projektu zahrnout cenu, dobře nastavená politika objednávek	1	2	2
17	Vývoj trhu	V projektu zahrnout rezervu	2	6	12
18	**Právní rizika**				
19	Špatně definované smluvní podmínky	Konzultace s nezávislým právníkem	3	4	12

Graf č. 1 zobrazuje jednotlivá rizika před a po zavedení opatření. Cílem tohoto grafu je porovnání hodnot před a po zavedení opatření, aby byly jasně viditelné změny, kterých bude dosaženo v případě nasazení a dodržení opatření navržených v tabulce číslo 10. Jak je možné z grafu vyčíst, tak po zavedení opatření se celková hodnota rizika zmenšila. Hodnota rizika projektu před zavedením opatření byla 427. po navržení a zavedení opatření se hodnota zmenšila na 120. Důležitou poznámkou je, že o realizaci jednotlivých opatření rozhodne jednatel na základě jeho vlastního uvážení.

Graf 1: Porovnání rizik před a po zavedení opatření (vlastní).



2.8 Shrnutí analýzy a požadavky investora

Po osobní schůzce s investorem a CEO celé společnosti jsme se shodli na několika bodech, které je potřeba akutně zajistit, aby se zlepšila práce s daty a jejich zálohování.

- Nejdůležitějším cílem je zajistit redundantní zálohování databází účetního a personálního programu.
- Dalším důležitým cílem je zajištění zálohování všech serverů společnosti.
- Akutní řešení zálohování jednotlivých uživatelský profilů, minimálně převedení a kopie části dat na server, aby nedocházelo ke zbytečným ztrátám. Nastavit zálohování dat na server pro vedoucí teamů na oblast složky Dokumenty a Plocha. Pro ostatní uživatele pak pouze složka dokumenty. Na mé doporučení se kopie na server provádí i u složek, ve kterých jsou uložena IMAP soubory z aplikace Mozilla Thunderbird.
- Vyřešení zálohování jednotlivých dat z poboček -. minimálně jednou redundantní.
- Návrh Redundance zálohování a opatření proti ransomware.
- Návrh a doplnění směrnice tak, aby vyhovovala veškerým požadavkům, které jsou nutné pro efektivnější fungování společnosti.
- Důležitým krokem, který jednatel na začátku projektu zkontroluje, bude prvotní minimalizace rizik na základě analýzy rizik provedené poskytovatelem. O nasazení jednotlivých rizik jednatel rozhodně na základě svého vlastního uvážení

Jednatel společnosti neudal konkrétní peněžní prostředky, které je ochoten do realizace investovat. Vyžaduje kvalitně provedenou práci za co nejmenší náklady. Jednotlivé kroky realizace je nutné schválit s jednatelem a na základě jeho souhlasu je realizovat. Další podmínkou realizace je zajištění nahlížení do dokumentace v průběhu celé realizace.

VLASTNÍ NÁVRH ŘEŠENÍ

V první části této práce jsou navržena jednotlivá řešení problémů se zálohováním. Další část je věnována realizaci jednotlivých nastavení. Poslední část se věnuje návrhu směrnice upravující práva a povinnosti zaměstnanců a poskytovatele IT služeb v oblasti zálohování a práce s daty.

3.1 Zálohování uživatelských stanic a dat

U zálohování dat z uživatelských účtů navrhuji zálohovat celý disk pomoci aplikace Zálohování od společnosti Microsoft. Tato záloha bude probíhat pouze jednou za týdně v pondělí v 11:00, protože většina dat se nachází v cloudovém úložišti Google drive. Na každé pobočce bude nastaven EOIP tunel, který bude sloužit k přímému propojení s vnitřní sítí a je tak možné zálohovat na BCU1 server.

Pro eliminaci ztráty kritických dat bude využita funkce Windows Serveru folder redirection. Folder redirection bude nastavena u standartních zaměstnanců pouze na složku Dokumenty, pro vedoucí týmů bude nastavena i plocha. V celé společnosti je využívána aplikace Mozilla Thunderbird, která ukládá IMAP soubory do složky C:\Users\konkretni_uzivatel\AppData\Roaming\Thunderbird\Profiles\profil_v_thunderbirdu.default. na Celou složku budou aplikována nastavení folder redirection, aby bylo zamezeno největší ztrátě, kterou představuje emailová komunikace.

3.2 Systém zálohování NAS

Hlavní NAS umístěná v sídle společnosti bude zálohována každou neděli v 15:00 na externí NAS umístěnou u jednatele doma. Hlavní NAS je v jiné části budovy než ostatní serverové vybavení. Tato centrální NAS má přes USB připojené 2 externí HDD. Na tyto HDD je zálohován obsah NAS offline uživatelem vytvořeným v zařízení NAS. Tento způsob zálohování je zaveden jako ochrana proti kryptoútoku, ransomware a jiným hrozbám. Vzhledem k tomu, že uživatel je vytvořen pouze v zařízení NAS, nemělo by při tomto druhu útoku dojít k zašifrování či ztrátě dat na externím úložišti. Záloha zajišťující ochranu proti kryptoútoku probíhá každý den ve 12:00.

3.3 Zálohování síťových prvků

Tato část práce se zabývá návrhem zálohování jednotlivých síťových prvků.

3.3.1 Routery Mikrotik

Na každé pobočce je umístěn jeden router od společnosti Mikrotik, konkrétní typy jsou uvedeny v tabulce č.5. Navrhuji, aby všechny routery byly zálohovány jednou týdně v sobotu ve 13:00. Na vše pobočkách k tomu bude využito aplikace scheduler, do které budou zadány příkazy, které má Mikrotik Router provést, a ten automaticky provede zálohu. Zálohy budou ukládány na server BCU1 do složky C:\Mikrotik_backup\Jméno_pobočky. Jednotlivé zálohy budou pojmenovány ve formátu rrrrmmdd_jmenopobocka (napr. 20190209_smetanova). Jednotlivá zařízení budou zálohována také při aktualizacích firmware, aby byly zachovány aktuální verze jednotlivých routerů při případné chybě zařízení v průběhu aktualizace.

3.3.2 Zálohování kamerového systému

Jednotlivé kamery jsou zapojeny do nahrávacích zařízení od společnosti Hikvision. Zálohování kamer ani nahrávacích zařízení není nastaveno. K tomuto budou využity zabudované nástroje od společnosti Hikvision. Kvůli velkému množství kamer jsou kamery nastaveny tak, aby byly obrazy ukládány pouze při změně pohybu. Z kamerového systému budou zálohovány pouze konfigurace jednotlivých zařízení. Operace zálohování veškerých kamerových záznamů je velmi náročná na využití úložiště, do kterého nechce jednatel společnosti investovat. Proto budou zálohovány pouze konfigurace nahrávacích serverů, a ne záznamy ze všech zařízení.

3.3.3 Zálohování Unifi zařízení

Jednotlivé AC pointy budou zálohovány pomocí AP controleru jednou za 14 dní v pátek ve 21:30. Název jednotlivých souborů generuje automaticky AP controler. O stažení souborů se postará dopsaný skript v Unifi controleru, který bude shromažďovat zálohované soubory ve složce C:\Unifi_Backup.

3.4 Zálohování databází

U zálohování databází navrhuji, aby byly zálohovány každý den v 6:00. Zálohované soubory budou uchovávány kvůli jejich velikosti pouze 14 dní. Databáze jsou zálohovány na zálohovací virtuální server. Protože se jedná o kritická data, tak databáze BI a SQL jsou zálohovány ještě na SQL1 server na jiný disk, než jsou umístěna zdrojová data. Zálohy těchto dat se ze zálohovacího serveru každý den v 7:00 přenášejí šifrovaně na NAS umístěnou u jednatele doma.

3.5 Zálohování virtuálních serverů

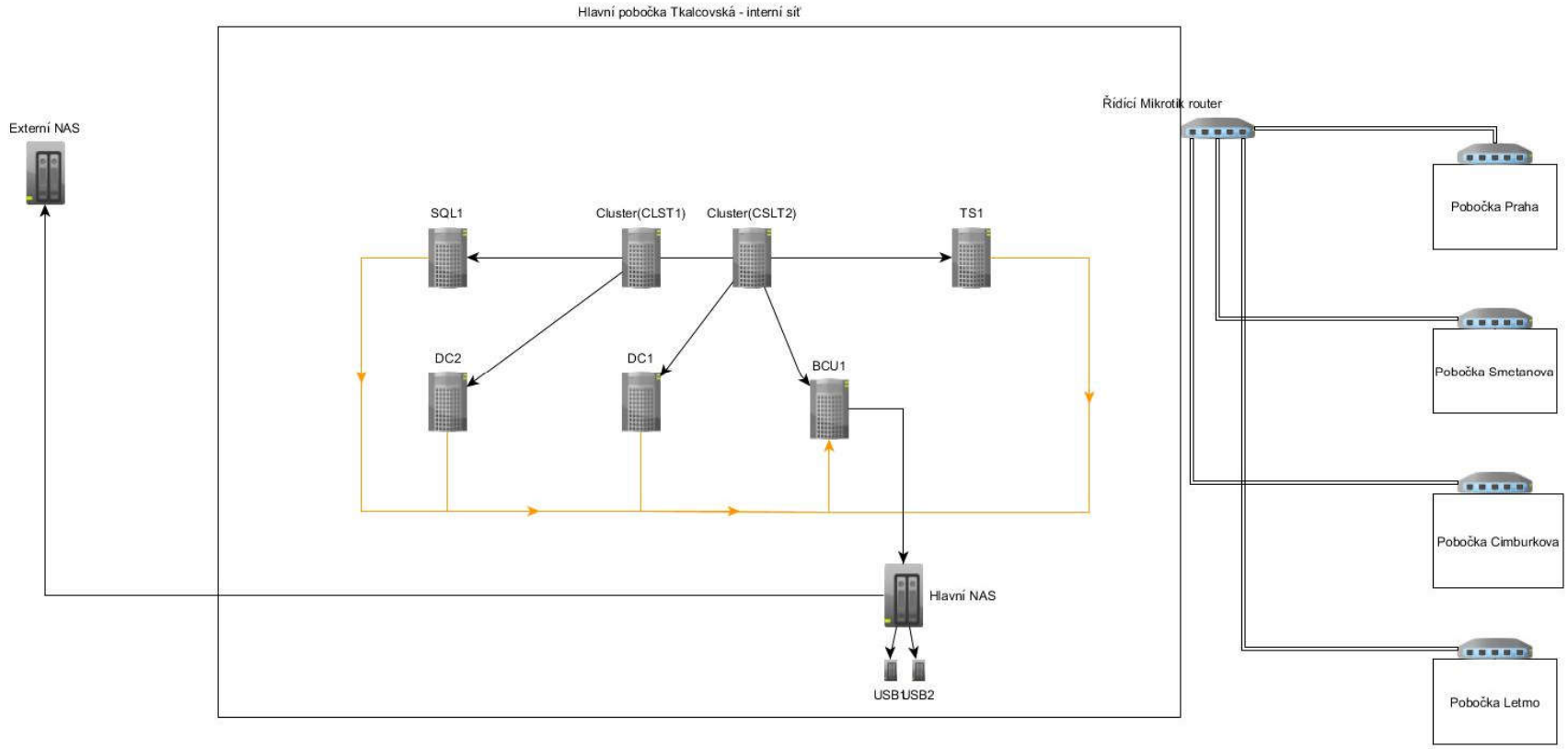
Jak je vysvětleno v kapitole 2.4.4 ve společnosti je provozováno 5 virtuálních serverů. Všechny servery se zálohují v nočních/ranních hodinách, kdy je provoz na síti minimální, aby nedošlo k narušení produktivity a snížení výkonu serverů. Všechny virtuální servery kromě BCU1 se zálohují právě na backup server. Mezi virtuálními servery jsou hodinové rozestupy tak, aby bylo využití výpočetního výkonu jak fyzických, tak virtuálních serverů rovnoměrně rozděleno. Konkrétní časy zálohování jsou uvedeny v tabulce číslo 12. Zálohování virtuálních serverů začíná až v 1:00, protože do té doby probíhají naplánované úlohy provádějící údržby databází, úpravy účetních jednotek a kontroly jednotlivých komponent systému. Serverové vybavení a konfigurace nám dovoluje zálohování fyzických serverů CLST1 a CLST2, protože při případném krátkodobém výpadku dochází k automatickému přepnutí virtuálních strojů na druhý server v clusteru a je tak zajištěna redundance. Na virtuálních serverech DC1, DC2, SQL1, TS1 a BCU1 bude pro zálohování využita aplikace Windows backup.

Tab. 12: Návrh zálohování fyzických a virtuálních serverů (vlastní).

Zařízení	Cíl zálohování	Čas zálohování	Interval zálohy
SQL1+DC2	BCU1	1:00	Každý den
DC1+TS1	BCU1	2:00	Každý den
BCU1	HNAS	3:00	Každý den
CLST1	HNAS	4:00	Každý den
CLST2	HNAS	5:00	Každý den

3.6 Finální varianta zálohování

Na obrázku číslo 14 je vyobrazena finální varianta zálohovacího plánu v kombinaci s tabulkou číslo 13 je možné mít přesné informace o tom, jak se jednotlivé části systému zálohují, kam se zálohují a jaká je přibližná doba trvání zálohy.



Obr. 14: Návrh zálohování společnosti (vlastní).

Tab. 13: Přehled zálohování jednotlivých systémů (vlastní).

Přehled zálohování					
	Zdroj zálohy	Cíl zálohy	Čas začátku zálohy	Interval zálohy	Předpokládaná doba trávní zálohování
Fyzické a virtuální servery	SQL1+DC2	BCU1	1:00	Každý den	45 minut
	DC1+TS1	BCU1	2:00	Každý den	30 minut
	BCU1	HNAS	3:00	Každý den	45 minut
	CLST1	HNAS	4:00	Každý den	20 minut
	CLST2	HNAS	5:00	Každý den	20 minut
Databáze	DB SQL+BI	SQL1	6:00	Každý den	1 h
	DB SQL+BI	ENAS	7:00	Každý den	1 h
Uživatelská zařízení	Stanice	BCU1	22:00	Každé 2 dny	15 minut
NAS	HNAS	Externí HDD	12:00	Každý den	1 h
	HNAS	ENAS	15:00	Ne každý týden	1 h
Ostatní síťová zařízení	Mikrotik zařízení	BCU1	13:00	So každý týden	5 minu
	Hikvision	BCU1	14:00	So každých 14 dni	10 minut
	Unifi	BCU1	21:30	So každých 14 dni	30 minut

Na základě této tabulky budou navržena jednotlivá zálohování. Vše je koncipováno tak, aby se zálohování navzájem nepřekrývala a bylo tak možné plně využít HW kapacitu zařízení.

3.7 Realizace návrhu zálohování

Tato část práce se věnuje konkrétní realizaci mnou navržených řešení. První část práce uvádí obecná nastavení, která je potřeba realizovat před nastavením zálohování na jednotlivých zařízeních. Další části se zabývají jednotlivými realizacemi zálohování. Poslední část obsahuje finální schéma zapojení jednotlivých komponent do zálohovacího celku. Tato část práce je rozdělena do podkapitol podle jednotlivých skupin zařízení a nastavení, která na nich bude nutné provést.

3.7.1 Mikrotik routery

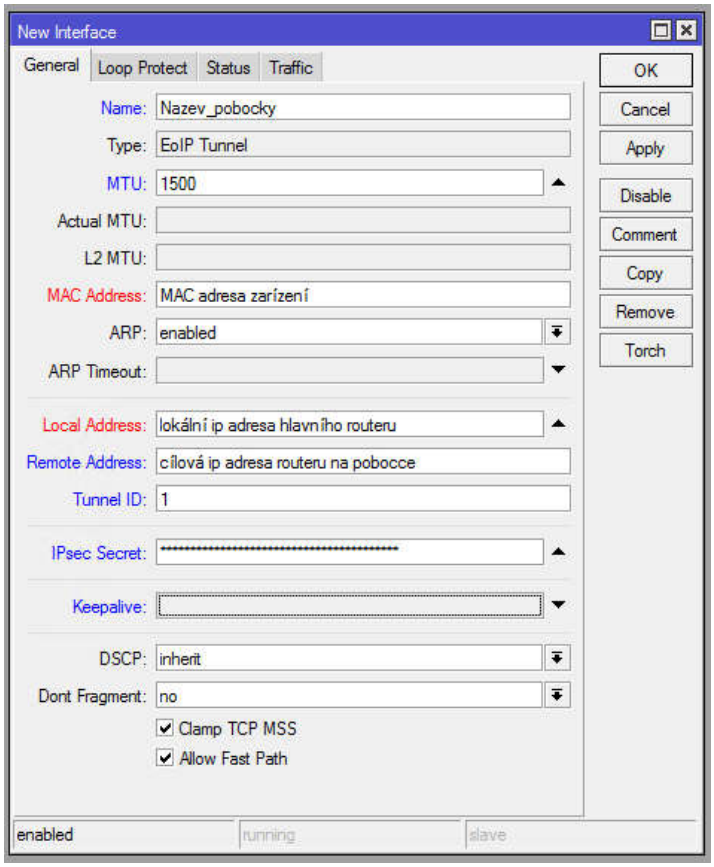
Vzhledem k tomu, že se na 3 pobočkách využívá firemní software minimálně, případně na terminálovém serveru, nebylo zde dosud realizováno žádné propojení s hlavním routerem a doménou. Zde bude nutné nastavit propojení s hlavním routerem. Aby byla zajištěna základní bezpečnost, navrhuji nastavení EOIP tunelu, který pro účely propojení hlavního routeru s pobočkami splňuje veškeré požadavky na zabezpečení a konektivitu. Uvedený typ tunelu zajistí kromě bezpečně propojení s hlavním routerem, také propojení s doménou, centrálním DHCP i DNS serverem. Nutnou podmínkou pro fungování řešení jsou statické veřejné adresy na všech zařízeních. Tato podmínka byla komunikován s jednatelem, který souhlasil se zakoupením veřejných statických adres.

Další nastavení, které je potřeba realizovat na routerech, jsou úpravy Firewallu. Vzhledem k přísně nastaveným politikám je nutné dát jednotlivým zařízením výjimky, aby se routery a zařízení navzájem viděly a bylo možné zálohovat po zabezpečené síti. S nastavením firewallu jsou spojena i nastavení NAT, aby zařízení byla vidět a byla schopná spolu komunikovat na konkrétních nestandartních portech a byla tak zvýšena bezpečnost.

3.7.1.1 Nastavení EOIP tunelu na hlavním routeru

Nastavení EOIP tunelu bude pro všechny pobočky téměř totožné. Jednotlivé EOIP tunely budou pojmenovány podle modelu Nazev_pobocky (např. Cimburkova). Technicky budou tunely odlišeny rozdílnými ID tunelů, které budou začínat číslem 1, následované 2 atd. Dále nastavujeme u zařízení hodnotu MTU na 1500, vzhledem k optickému připojení je možné tuto hodnotu nastavit a nedojde ke ztrátě propojení. Dále zadáme MAC adresu zařízení, lokální IP adresu a IP adresu cílového zařízení. Vygenerujeme dostatečně silné tajemství, které bude zajišťovat ověření tunelů. V tomto konkrétním případě jsem zvolil 40. místné náhodně vygenerované heslo obsahující velká i malá písmena, číslice i znaky. Tyto podmínky zajistí

základní zabezpečení tunelu mezi hlavním routerem a pobočkou Obecné ukázkové nastavení je možné vidět na obrázku číslo 15. Tímto způsobem jsou vytvořeny tunely pro všechny pobočky a odlišeny názvem a ID tunelu.



Obr. 15: Konfigurace EOIP tunelu na hlavním routeru (vlastní).

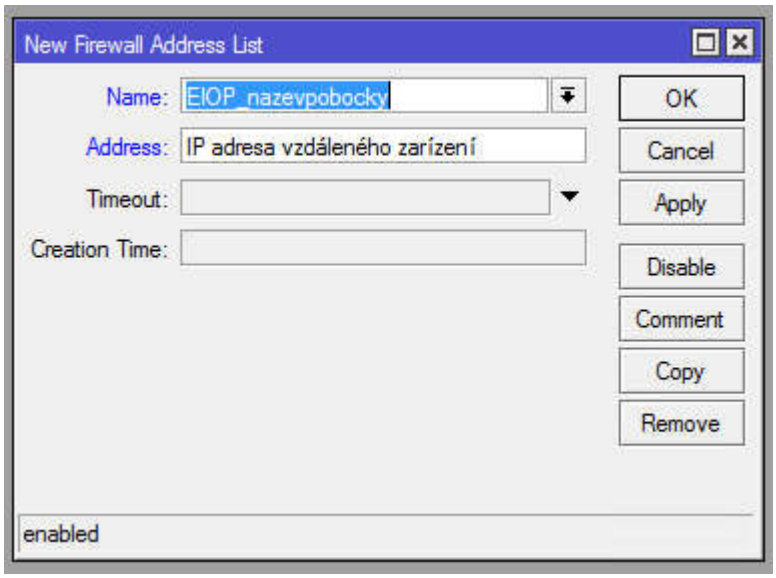
3.7.1.2 Nastavení EOIP tunelu na pobočkách

Na pobočkách provedu nastavení totožné jako na hlavním routeru. V tomto kroku je kladen důraz na to, aby bylo dobře nastaveno ID a tajemství tunelu. Je nutné zajistit korektní nastavení IP adres. Pokud budou parametry špatně nastaveny, tunel nebude fungovat a zálohovací plán tak nebude možné nastavit, protože se zařízení nespojí s doménovým řadičem.

3.7.1.3 Nastavení firewallu

Na hlavním routeru i na routerech poboček je nutné povolit komunikaci s veřejnou adresou protilehlého zařízení. IP adresy zařízení přidáme v Adress listu firewallu protilehlé IP, toto nastavení provedeme na obou stranách tunelu. Adresy nazveme podle vzorce EOIP_nazevpobocky, dalším parametrem bude nastavení vzdálené IP adresy. Toto nastavení

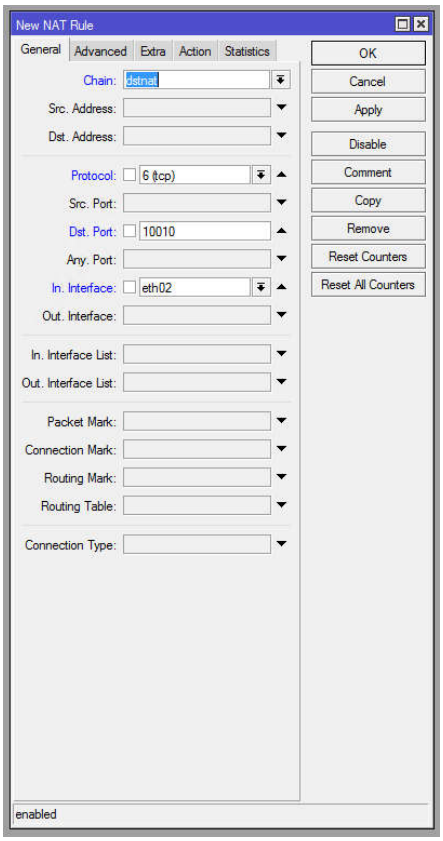
provedeme na hlavním routeru stejně jako na routerech na pobočkách. Obecné nastavení je zobrazeno na obrázku číslo 5.



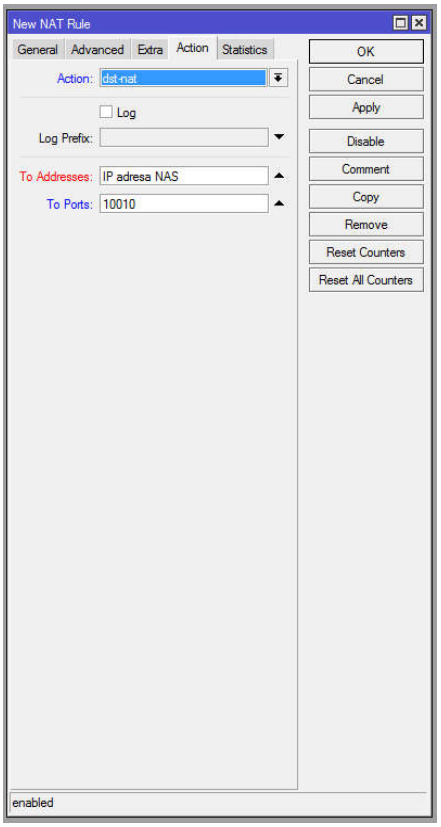
Obr. 16: Povolení EOIP tunelu na firewallu (vlastní).

3.7.1.4 Nastavení NAS

NAS Synology standardně komunikují na portu 5000. Externí NAS přesměrujeme na port 10010, který standardně není využíván pro komunikaci na úrovni služeb. Na hlavním routeru je nutné nastavit ve firewallu v záložce NAT přesměrování portu na IP adresu na NAS. Postup je uveden na obrázcích číslo 17 a číslo 18. V záložce general nastavujeme druh akce, kterou budeme provádět(chain), komunikační protokol, cílový port a interface, na kterém bude komunikace probíhat. Na záložce Action pak proběhne nastavení akce(dst-nat), cílové adresy a cílového portu. Takto budou nastavena jednotlivá zařízení v síti, v konfiguraci se bude vždy měnit IP adresa a cílový port. Tyto kroky ztěžují případnému útočníkovi dosah na vzdálenou NAS, protože port 10010 je nestandartní a jsou tak navýšena bezpečnostní opatření.



Obr. 17:Pravidlo NAT (obecné)(vlastní).

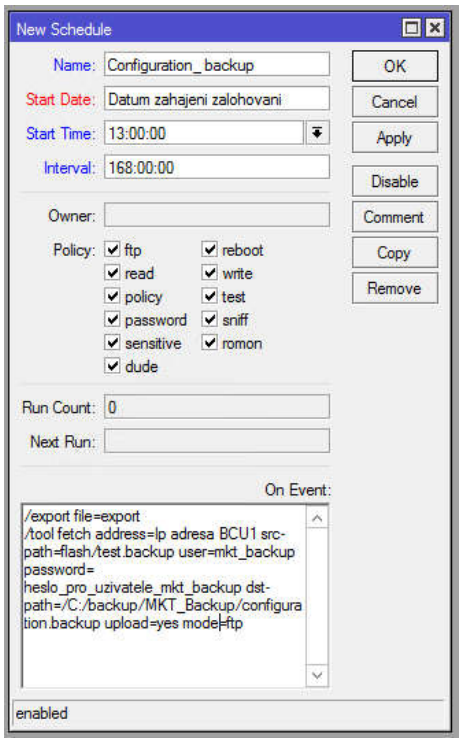


Obr. 18: Pravidlo NAT (akce)(vlastní).

3.7.1.5 Nastavení zálohování konfiguračních souborů

Celý proces zálohování by měl být maximálně automatizovaný. U externí zálohy Mikrotik routerů využiji možnosti Auto Scheduleru, který bude spouštět script starající se o zálohování. Předpokladem pro nastavení zálohování routeru je na BCU1 serveru povolená IIS s vytvořenou FTP stránkou. K FTP bude přistupovat pouze jeden určitý účet. Tento účet bude sloužit výhradně pro zálohování konfiguračních souborů a nebude mít žádná další oprávnění. Na obrázku číslo 19 je nastavení parametrů pro spuštění automatického zálohování.

U nové úlohy je nastaveno jméno, počáteční datum i čas a interval zálohování. Do oblasti On Event zadáme příkazy, které proběhnou vždy v námi udaný čas. **Příkaz: /export file=export** vytvoří export konfigurace zařízení. Zbytek příkazu zajišťuje nahrání souboru export na FTP server (BCU1). V této části příkazu je uvedeno přihlašovací jméno a heslo pro přístup na FTP, cílová IP adresa (IP adresa FTP), zapnutí FTP módu a povolené nahrání souboru.



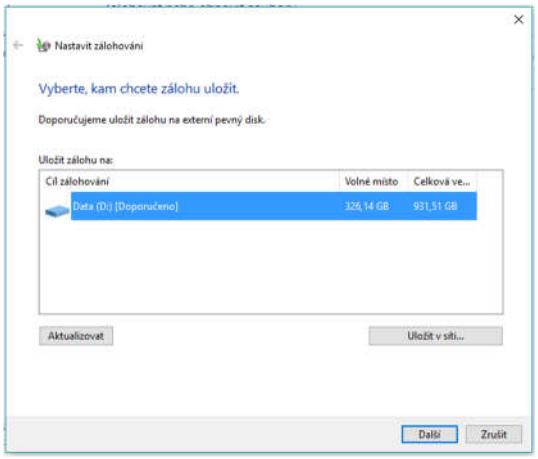
Obr. 19: Nastavení automatického zálohování zařízení Mikrotik (vlastní).

3.7.2 Nastavení zálohování uživatelských stanic

V této kapitole jsou vysvětleny postupy při nastavení zálohování uživatelských stanic a nastavení folder redirection pro nepřímou zálohu.

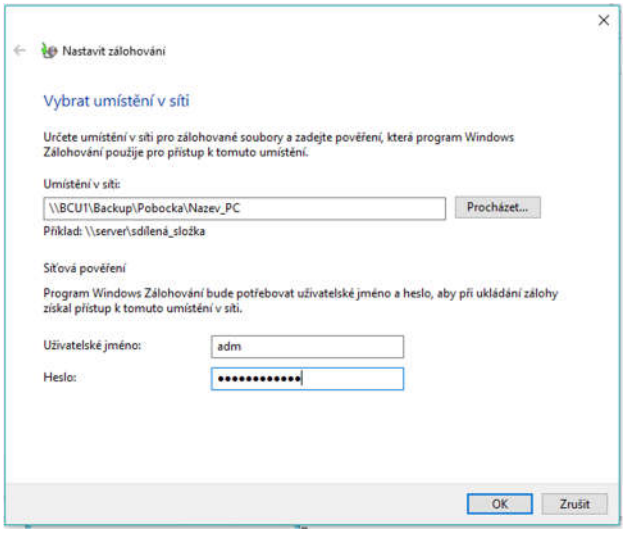
3.7.2.1 Nastavení zálohovaní na PC na pobočkách

Data z jednotlivých poboček budou zálohována na BCU1 server do složky Backup\Pobocka\Nazev_PC. Na jednotlivých pobočkách bude zálohování nastaveno administrátorem při instalaci zařízení. V prvním kroku je zvoleno nastavení zálohování (viz. obrázek číslo 20).



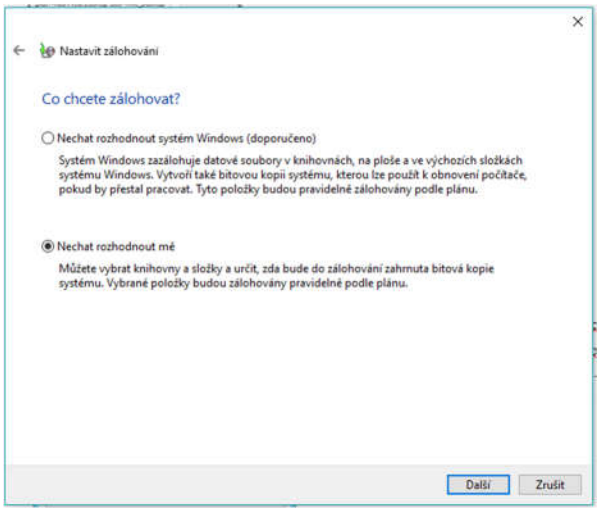
Obr. 20: Volba cíle zálohování (vlastní).

Na obrázku číslo 21 je zobrazeno umístění v sítí, které je vybráno a také zadané přihlašovací údaje administrátora, aby bylo možné provést i zálohu dat, která jsou ve složkách s omezeným přístupem.

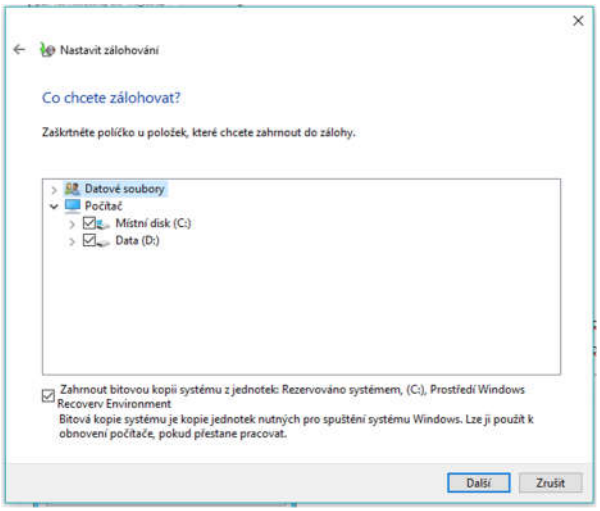


Obr. 21: Výběr a ověření přihlašování do síťového úložiště (vlastní).

Na obrázku 22 je zvolena možnost, kdy jsou zvolená data zálohována. Konkrétní výběr dat je zobrazen na obrázku číslo 23.

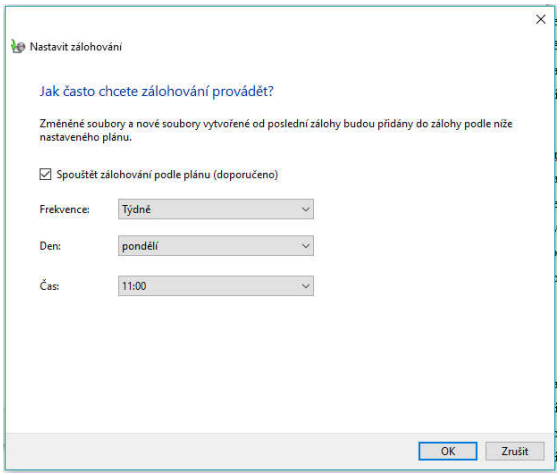


Obr. 22: Výběr možností zálohy (vlastní).



Obr. 23: Výběr zdrojových dat pro zálohu (vlastní).

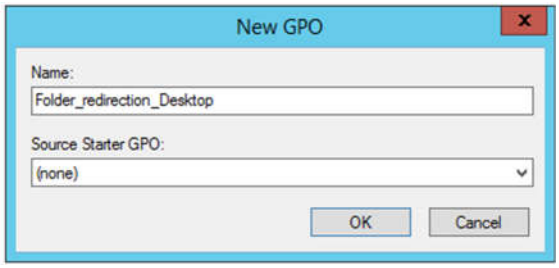
Následně je nastaven čas a frekvence zálohování na základě plánu, který byl vytvořen. V tomto případě se jedná vždy o pondělí 11:00, kdy jsou pobočky zavřeny z důvodu polední přestávky. Posledním krokem je potvrzení zálohování. Výsledný stav je zobrazen na obr. číslo 24.



Obr. 24: Nastavení časového plánu zálohování (vlastní).

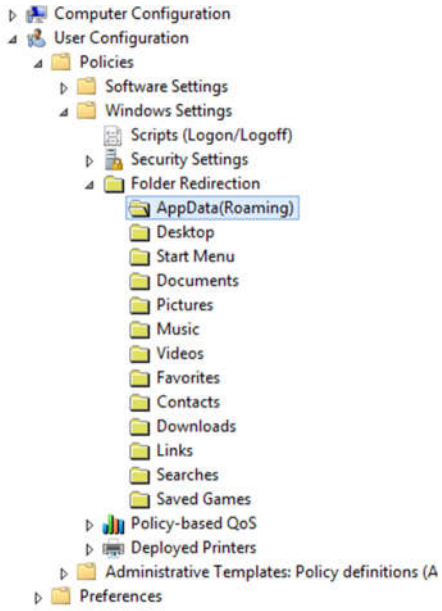
3.7.2.2 Nastavení folder redirection

Finální nastavení folder redirection předpokládá vytvoření dvou bezpečnostních skupin, jednu pro vedení společnosti, která bude zahrnovat i přesměrování plochy. Druhou pro řadové zaměstnance, ta nebude zahrnovat oblast Plochy. V prvním kroku vytvořím pod doménovou strukturou novou politiku přes Group policy management. První krok je ukázán na obrázku číslo 25.

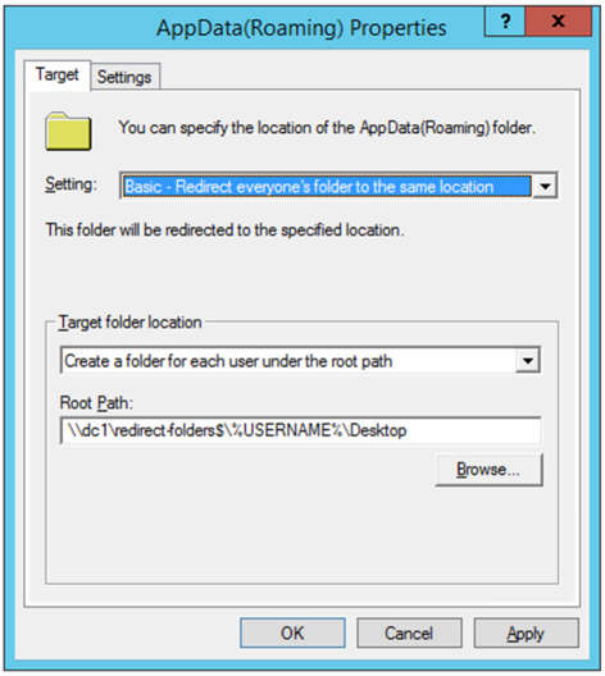


Obr. 25: Vytvoření folder redirection (vlastní).

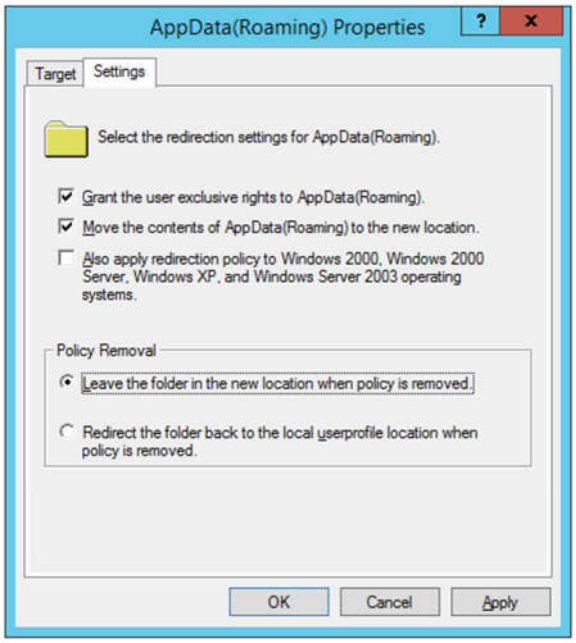
Dalším krokem je otevření možností politik a zvolení složek, které chceme přesměrovávat (obrázek č.26). U těchto složek je zvolena možnost vlastnosti. V nastavení cíle je zvolena cílová síťová složku a typ přesměrování. V tomto případě se budou data ukládat pro každého uživatele do zvláštní složky. V nastavení složky jsou zvolena a uložena další pokročilá nastavení. Kroky, které jsou příkladově provedeny na složce AppData musí být provedeny u všech složek, které se budou přesměrovávat (viz. kapitola 3.1). V posledním kroku (obrázek č.29) je kontrolováno, že politiky byly vytvořeny správně a jsou jim přiděleny skupinu, do kterých budou přidáni uživatelé, kterých se toto nastavení bude týkat.



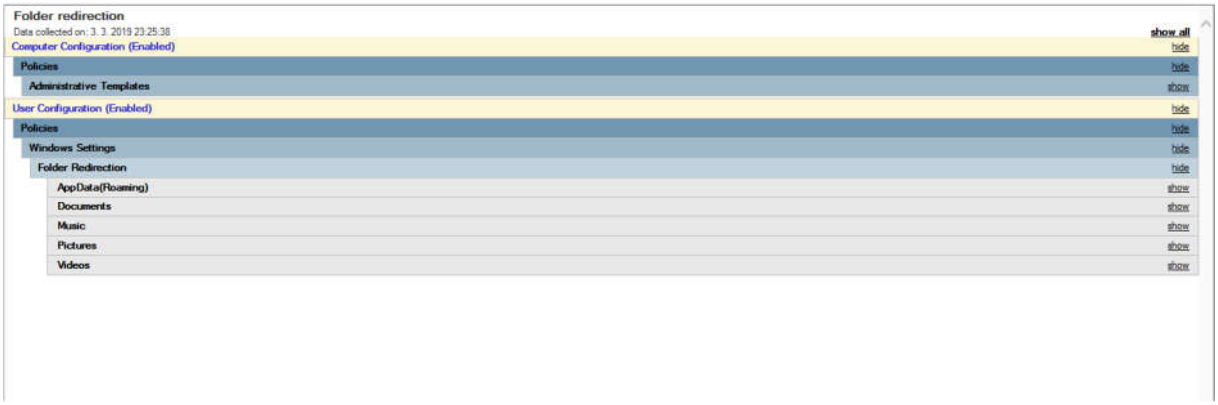
Obr. 26: Výběr cíle pro folder redirection (vlastní).



Obr. 27: Nastavení cíle folder redirection (vlastní).



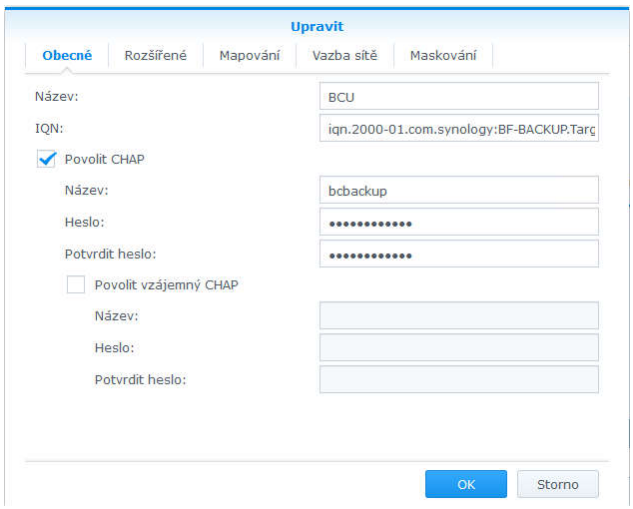
Obr. 28: Pokročilá nastavení folder redirection (vlastní).



Obr. 29: Kontrola nastavení folder redirection (vlastní).

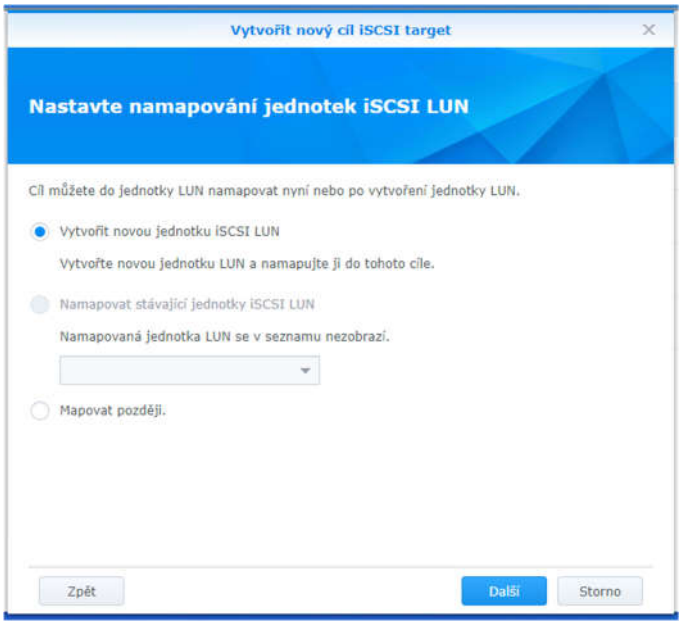
3.7.3 Zařízení NAS

U NAS zařízení bude nutné nainstalovat aplikaci Hyperbackup, která bude zajišťovat zálohování NAS. Tato aplikace je bezpečným řešením pro zálohování dvou zařízení NAS od společnosti Synology mezi sebou. Kromě nastavení vzájemného zálohování NAS je nutné nastavit Luny a Targety pro zálohování BCU1 serveru a fyzických serverů. Po přihlášení do NAS a otevřeme nastavení iSCI iniciátoru. V prvním kroku nazvu cílový target (viz. obrázek číslo 30) a zadám přihlašovací údaje, které budou využívány pro ověření targetu v iSCI iniciátoru.



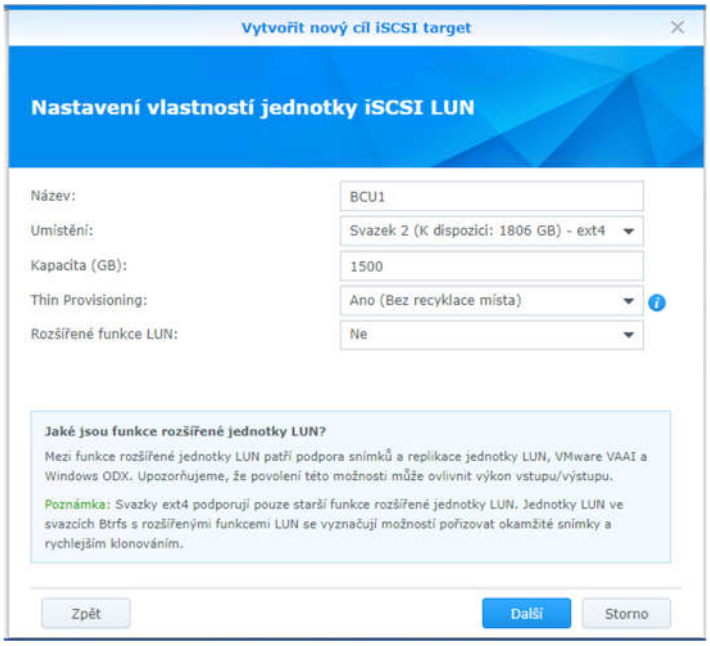
Obr. 30: Vytvoření targetu na NAS zařízení (vlastní).

V dalším kroku vyberu možnost, kam bude target umístěn. V tomto případě je zvolena první možnost, protože chceme vytvořit zároveň i nový LUN (viz. obrázek číslo 31).

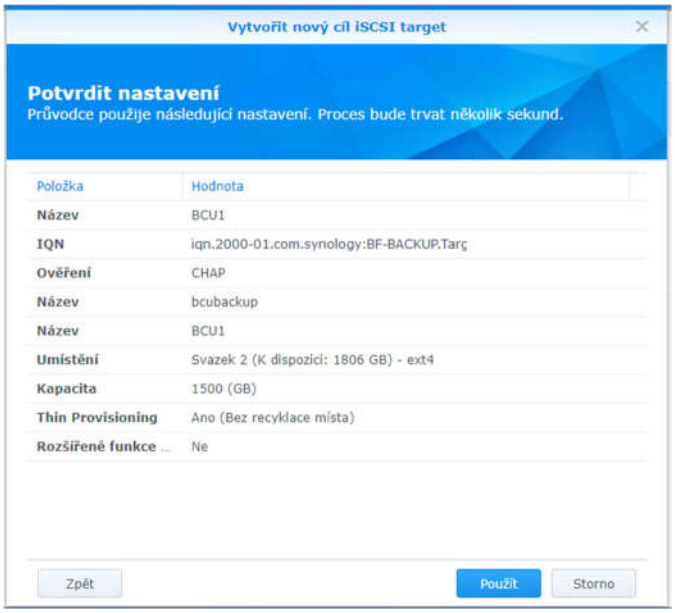


Obr. 31: Vytvoření LUNU na NAS zařízení (vlastní).

U nastavení vlastností lunu jsou zvoleny parametry: název lunu, umístění, přesnou kapacitu z umístění, která má být lunu přiřazena. V případě nutnosti jsou také zvoleny další pokročilé možnosti (např. Thin Provisioning).



Obr. 32: Nastavení parametrů LUNU (vlastní).

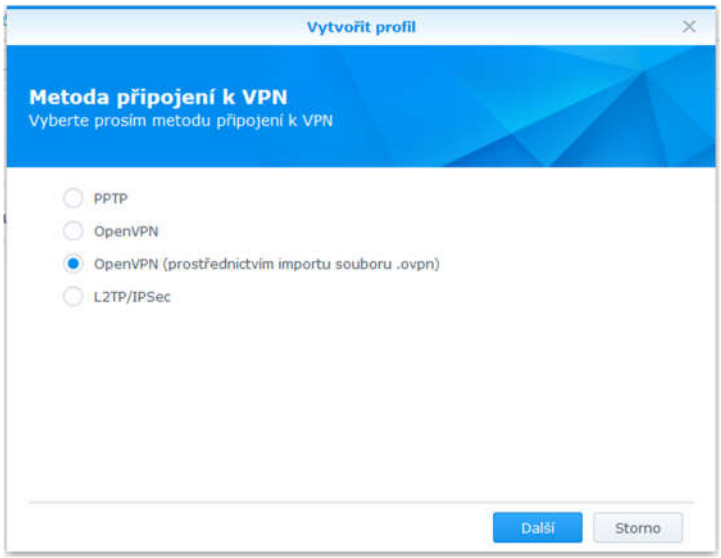


Obr. 33: Kontrola nastavení nového targetu (vlastní).

Na obrázku číslo 33 jsou po kontrole potvrzeny možnosti. Stejný postup jako postup zmíněný v kapitole 3.7.3 je aplikován i pro nastavení fyzických serverů, jedinou změnou jsou názvy a účty, kteří se budou vůči iSCI ověřovat. Jedná se zase o práci s luny a targety.

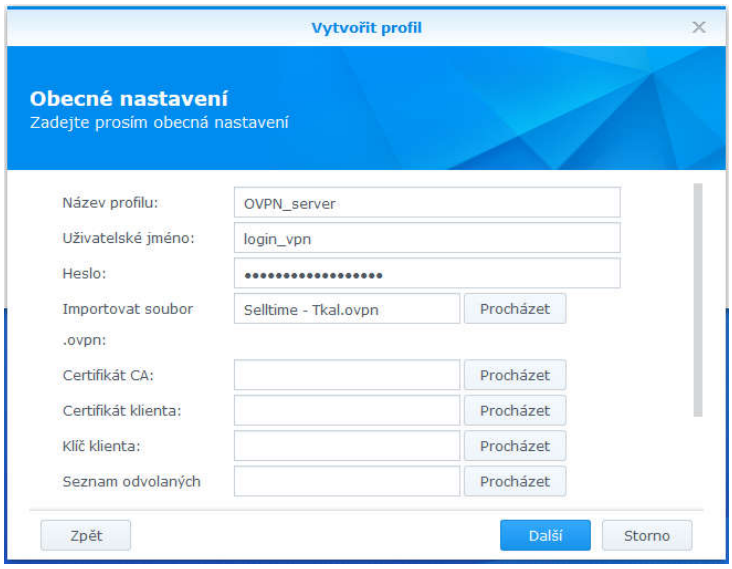
3.7.3.1 Nastavení vzájemné zálohy NAS

Před nastavením zálohování hlavní NAS na externí NAS je nutné nainstalovat na cílovou NAS doplněk Hyper backup vault, který umožňuje vzdálené zálohování na cílovém zařízení. Vzdálené propojení bude zajištěno aplikací OpenVPN. OpenVPN je realizovaná na hlavním Mikrotiku a není tak problém s připojením NAS do interní sítě.

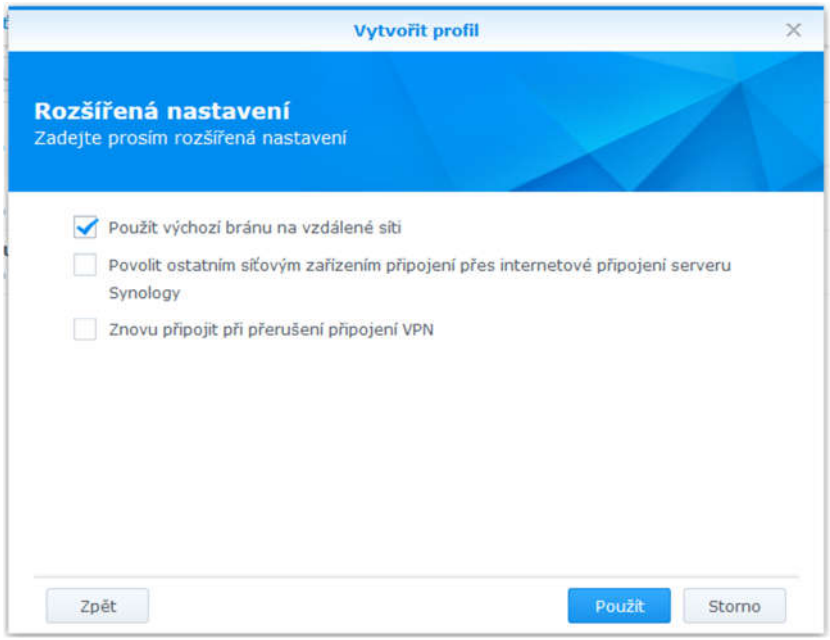


Obr. 34: Nastavení VPN na NAS zařízení (vlastní).

Na obrázku číslo 34 je vyobrazen první krok vytvoření připojení na VPN server. V tomto případě je využit konfigurační soubor, který je již nastavený. V dalším kroku jsou vyplněna jednotlivá kritéria: název připojení, login a heslo uživatele, OPVN soubor, CA certifikát a následně i klientský certifikát a klíč, případně seznam odvolaných certifikátů. To není v tomto případě není nutné (viz. obrázek číslo 35). V dalším koku je nastavena konfigurace pro připojení (viz obrázek číslo 36). Posledním krokem je potvrzení konfigurace.

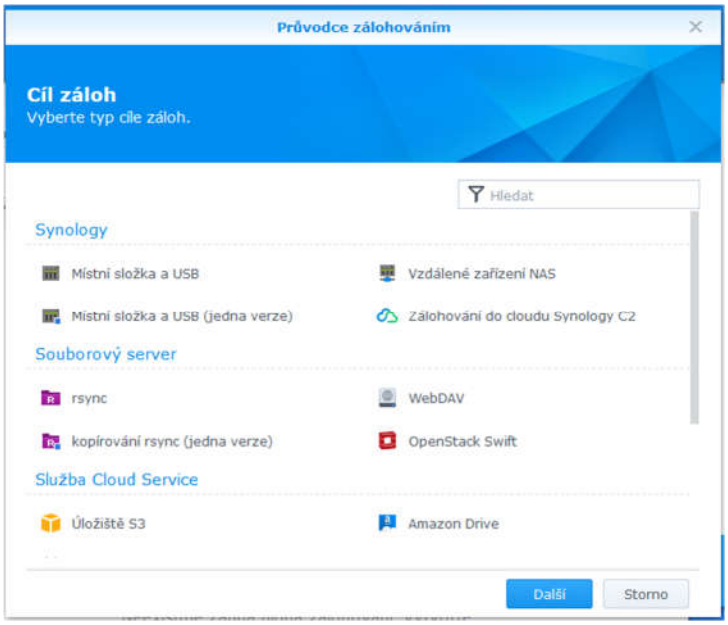


Obr. 35: Obecná nastavení OpenVPN na NAS (vlastní).



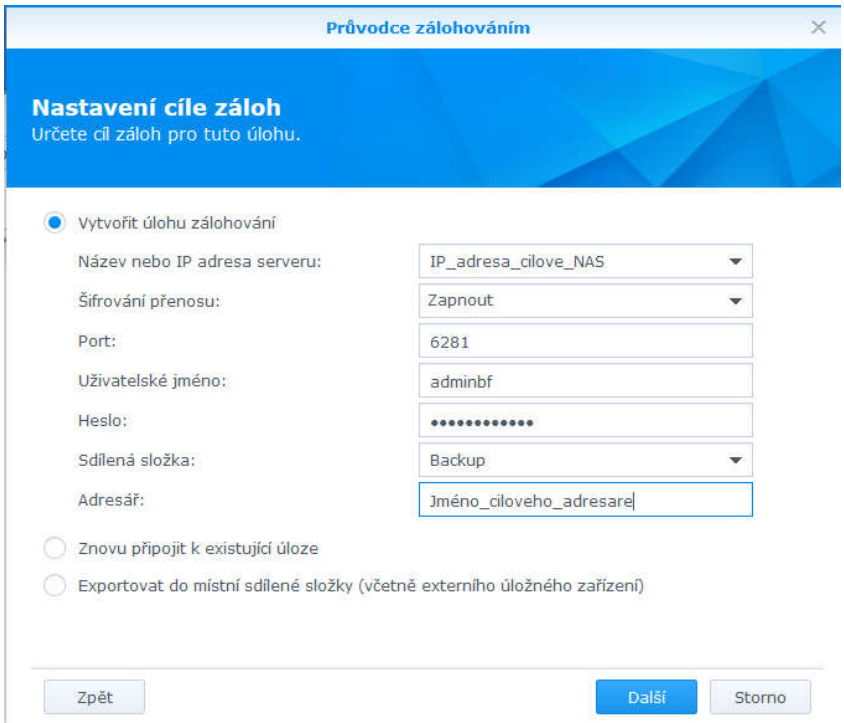
Obr. 36: Rozšířená nastavení VPN na NAS (vlastní).

Po nastavení VPN je možné nastavit externí zálohu. Jsou vybrána vzdálená zařízení NAS, jak je ukázáno na obrázku číslo 37.



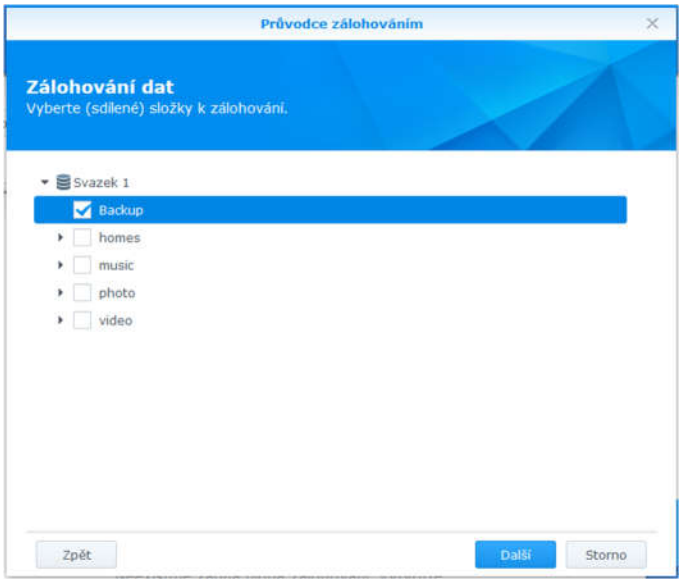
Obr. 37: Nastavení externí zálohy NAS (vlastní).

V následujícím kroku je zadána IP adresa cílové NAS, zapnuto šifrování kvůli bezpečnějšímu přenosu dat. Pro ověření je zadáno uživatelské jméno a heslo cílové NAS. Z nabídky je vybrána cílová složka. Tento krok ukáže, zda je vše dobře nastaveno, protože pokud ne, tak spolu NAS nebudou komunikovat. Je zvolen název cílové složky a potvrzen tento krok.



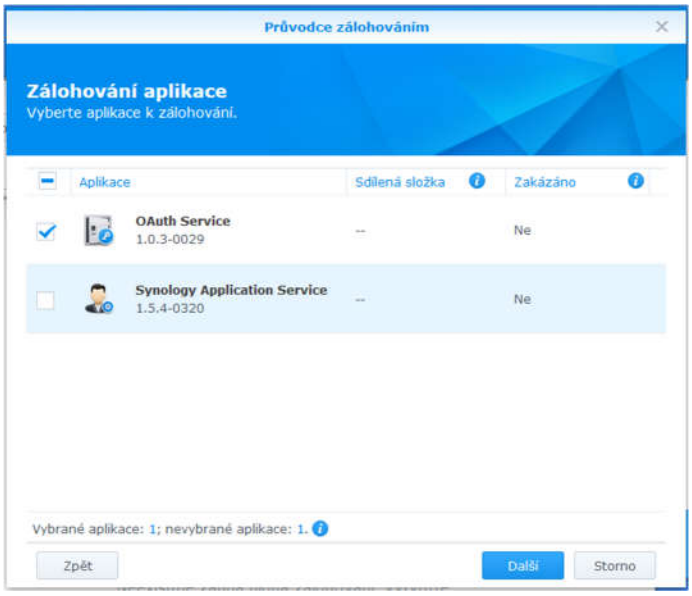
Obr. 38: Nastavení cíle zálohování (vlastní).

Na následujícím obrázku číslo 39 je vybrána sdílená složku, kterou je nutné zálohovat.



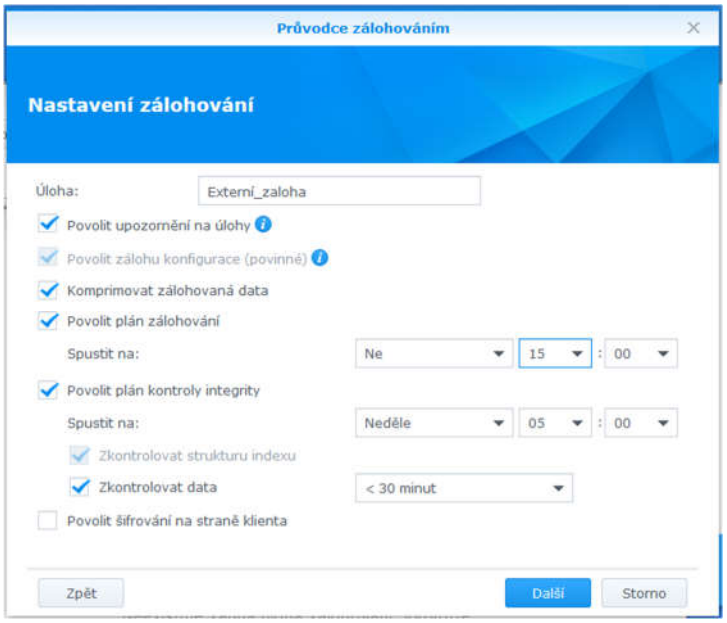
Obr. 39: Nastavení zdroje zálohy (vlastní).

Obrázek číslo 40 představuje volbu aplikací, které budou zajišťovat zálohování.

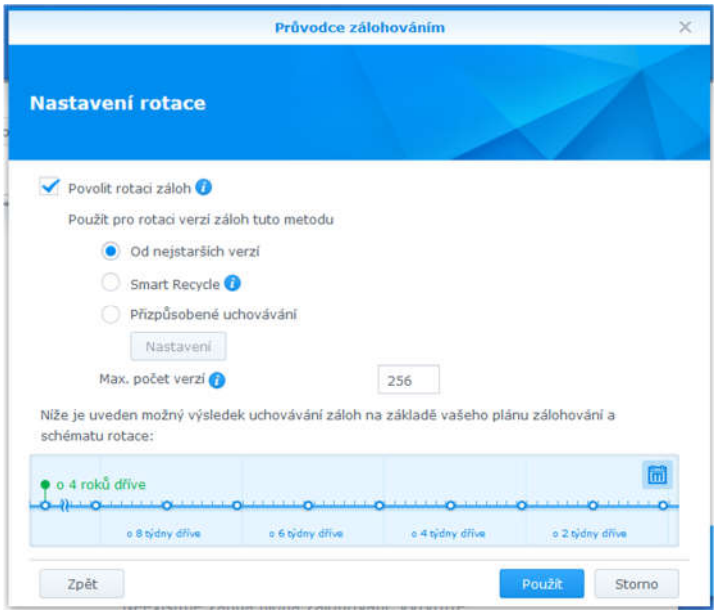


Obr. 40: Výběr aplikací zálohování (vlastní).

Obrázek číslo 41 zobrazuje již konkrétní nastavení úlohy zálohování. Úloha je nazvána Externí_záloha, je nastaven čas podle plánu na neděli na 15:00. Je zapnuta možnost kontroly integrity a také kontrola dat 30 min před zálohováním. Tyto kroky zajišťují hladký průběh externí zálohy a minimalizují ztrátu dat v průběhu zálohování. V posledním kroku je nakonfigurována rotace záloh. Tato nastavení slouží pro úsporu místa a přemazání nejstarších záloh. Velikost úložiště tak zůstává bez údržby stále stejně využitelná (obrázek číslo 42).



Obr. 41: Nastavení časů a způsobu zálohování (vlastní).



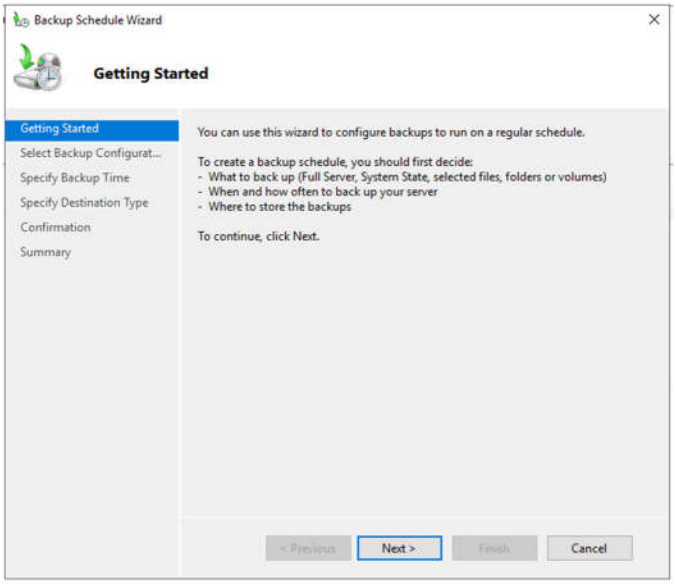
Obr. 42: Nastavení rotace záloh (vlastní).

3.7.4 Virtuální a fyzické servery

Na serverech SQL1, DC1, DC2 a TS1 bude zálohování prováděno aplikací Windows backup na BCU1 server. Tato záloha bude sloužit pro případnou obnovu kritických data. Fyzické servery budou také zajišťovány aplikací Windows backup, budou ale zálohovány do jiného úložiště než servery virtuální.

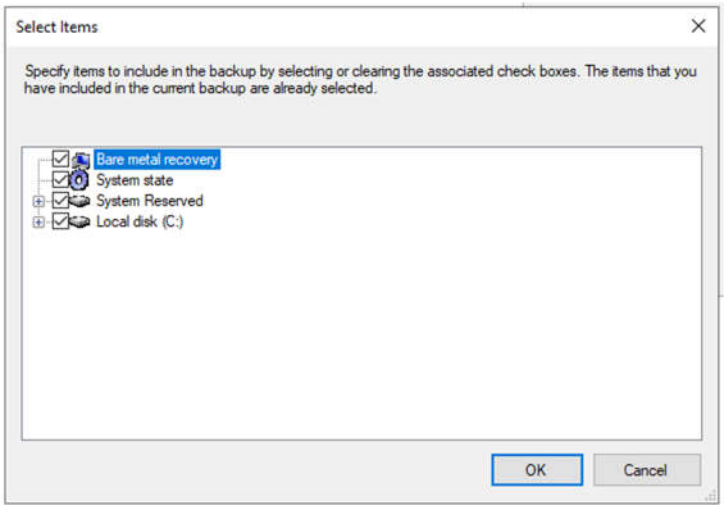
3.7.4.1 Zálohování virtuálních serverů DC1, DC2, SQL1 a TS1

V prvním kroku je spuštěna konfigurace Pravidelného zálohování (viz. obrázek číslo 43).



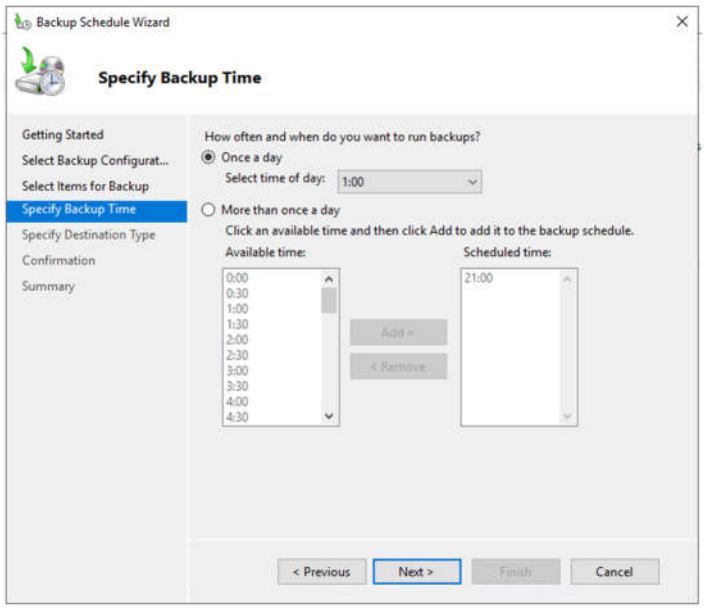
Obr. 43: Nastavení Windows backup (vlastní).

V dalším kroku je proveden výběr jednotlivých částí serveru, které je potřeba zálohovat, zde je z nabídky vybrána kompletní záloha, aby bylo možné pružně reagovat na případné chyby systému a zprovoznit servery v co nejkratším časovém úseku.



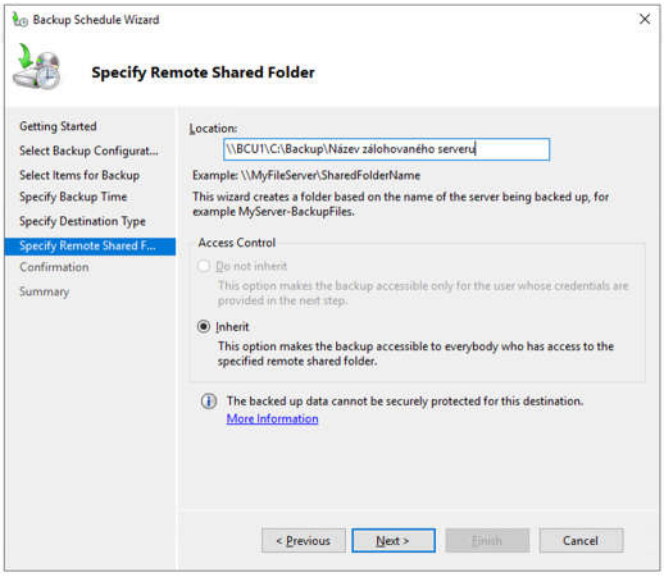
Obr. 44: Výběr zdroje pro zálohování (vlastní).

Dalším krokem je nastavení časů zálohování. Na obrázku číslo 45 je zobrazeno nastavení pro servery SQL1 a DC2, které se zálohují v 1:00. Stejné nastavení provedeme i pro servery DC1+TS1, zde čas nastavíme na 2:00.



Obr. 45: Výběr času zálohování (vlastní).

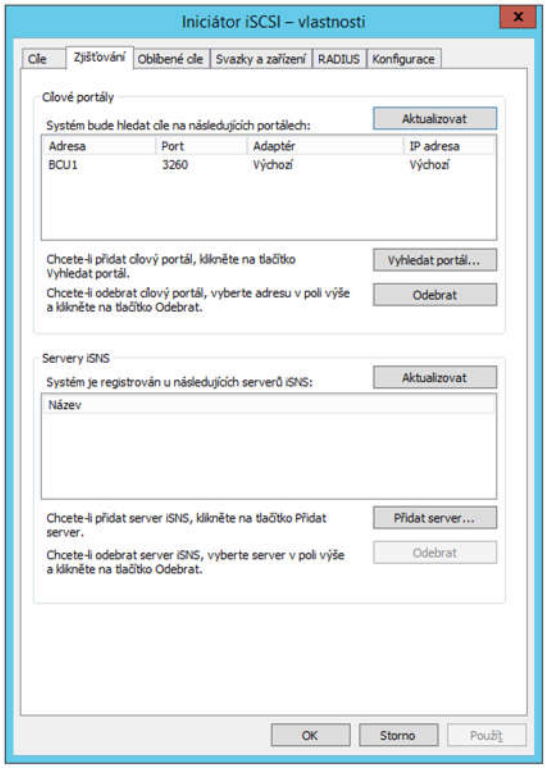
Dalším krokem je nastavení cíle zálohování. Pro jednotlivé servery jsou na BCU1 serveru vytvořeny složky s cestou \\BCU1\C:\Backup\Název_zálohovaného_serveru (např. \\BCU1\C:\Backup\DC1). Toto nastavení je možné vidět na obrázku číslo 46. Posledními kroky jsou potvrzení a souhrn nastavení. Po nastavení se provede první kompletní záloha. Poté budou zálohy probíhat v čase určeném nastavením a zálohovacím plánem.



Obr. 46: Nastavení cílové destinace zálohy (vlastní).

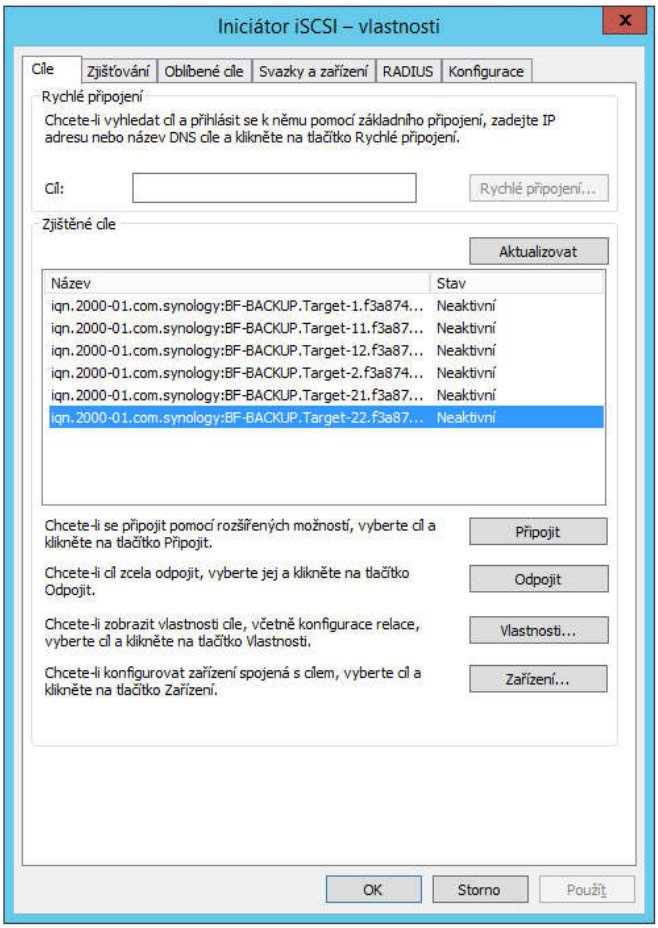
3.7.4.2 Zálohování zálohovacího serveru

Zálohovací server je zálohován hlavní NAS (HNAS). Nastavení NAS je uvedeno v kapitole 5.1.3. První nastavení bude inicializace cíle NAS nástrojem iSCI iniciátor. V záložce Zjišťování zkontrolujeme, jestli je cílový portál BCU1 dostupný.

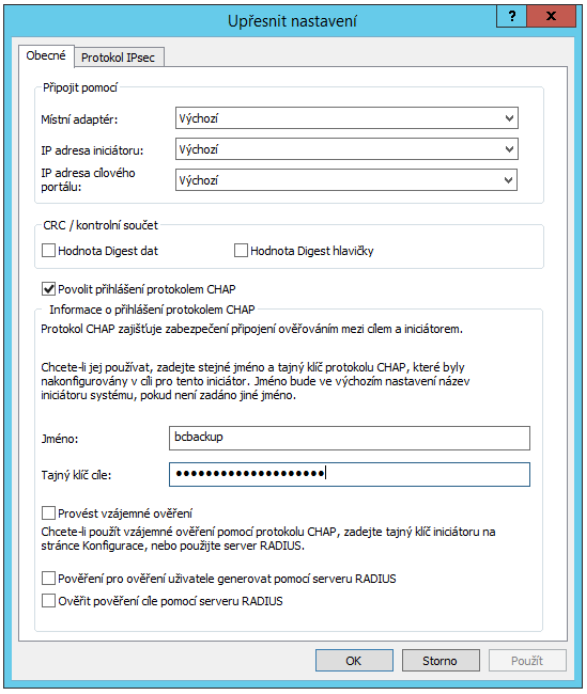


Obr. 47: Nastavení ISCI na serveru (vlastní).

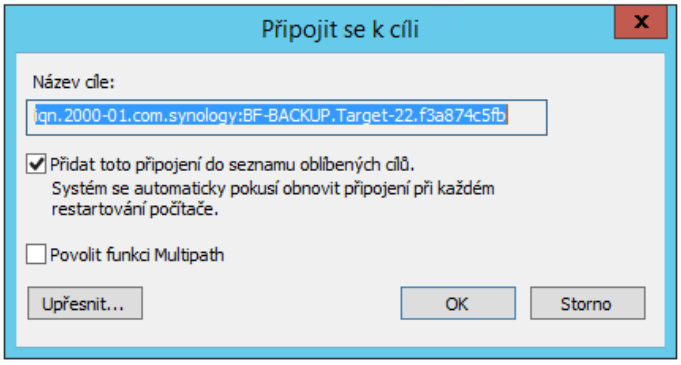
Na záložce Cíle je z nabídky vytvořený cíl (obrázek 49) vybrán konkrétní cíl. U vybraného disku je vybrána možnost připojit, následně možnost upřesnit (viz. obrázek číslo 48). V dalším okně je zvolena možnost povolit CHAP, jsou vyplněny přihlašovací jméno a heslo, které bylo vytvořeno v zařízení NAS. Disk připojen potvrzením Ok. Posledním krokem pro možnost využití disku na NAS je inicializace disku přes nástroj Správa disků systému Windows. V tomto kroku je nutné uvést disk do stavu online, disk je inicializován a je vybrána možnost, GPT nebo MBR podle toho jaký typ diskového oddílu je vyžadován.



Obr. 49: Připojení ISCI targetu (vlastní).



Obr. 48: Ověření ISCI targetu (vlastní).



Obr. 50: Potvrzení připojení k ISCI targetu (vlastní).

Po inicializaci disku je zálohování nastaveno stejným způsobem jako u ostatních virtuálních serverů. U nastavení času zálohování je hodnota změněna na 3:00. V dalším kroku je vybrána možnost Back up to a harddisk dedicated for backups. Následuje výběr správného disku, kontrola nastavení a potvrzení voleb. Protože se jedná o zálohování na disk, který se chová jako lokální, je zálohování po první celé záloze přenastaveno na přírustkové. Tak zajistím aktuálnost dat a ušetřím prostor pro data.

3.7.4.3 Zálohování fyzických serverů

Fyzické servery CLST1 a CLST2 budou zálohovány stejným způsobem jako zálohovací server. U CLST1 nastavíme čas na 4:00. U CLST2 na 5:00. Pro funkční zálohování těchto serverů je nutné splnit veškeré přechozí kroky (nastavení NAS a vytvoření Lunů a targetů + nastavení iSCI iniciátoru).

3.7.5 Unifi zařízení

Pro zálohování Unifi controleru je využit níže uvedený skript, který je upraven tak, aby odpovídal požadavkům zálohovacímu plánu. Spuštění tohoto skriptu je zajištěno přes plánovač úloh na serveru DC1. Ve skriptu jsou změněny parametry: přihlašovací jméno a heslo a čas, jak dlouho se má záloha udržovat (14 dní). V nastavení plánovače úloh se bude spouštět úloha jednou za 14 dnů v pátek ve 21:30.

Tab. 14: Skript pro zálohování Unifi zařízení (32) (vlastní).

```
#!/bin/bash -e
#
# Improved backup script for Ubiquiti UniFi controller
# original source: http://wiki.ubnt.com/UniFi#Automated_Backup
#

# must contain:
# username=<username>
# password=<password>
source ~/.unifi-backup

baseurl=https://localhost:8443
output=/root/backups/unifi
filename=`date +%Y%m%d%H%M`.unf
keep_days=14

# create output directory
mkdir -p $output

curl_cmd="curl --cookie /tmp/cookie --cookie-jar /tmp/cookie --insecure --silent --
fail"

# authenticate against unifi controller
if ! $curl_cmd --data
'{"username":"'$přihlašovací_jméno'","password":"'$přihlašovací_heslo'"}'
$baseurl/api/login > /dev/null; then
  echo Login failed
  exit 1
```

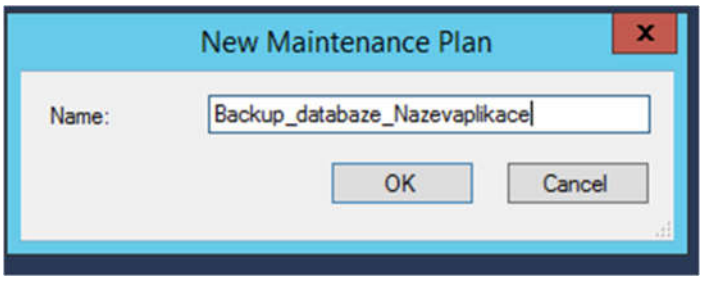
```
fi

# ask controller to do a backup, response contains the path to the backup file
path=`$curl_cmd --data 'json={"cmd":"backup","days":"-1"}'
$baseurl/api/s/default/cmd/system | sed -n 's/.*\(\/dl.*unf\).*/\1/p'`

# download the backup to the destinated output file
$curl_cmd $baseurl$path -o $output/$filename

# logout
$curl_cmd $baseurl/logout

# delete outdated backups
find $output -ctime +$keep_days -type f -delete

echo Backup successful
```

3.7.6 Zálohování Hikvision zařízení

Společnost Hikvision má vyvinutý nástroj na zálohování záznamů z kamer. Investor odmítá investovat do rozšíření úložiště. Zálohovány jsou tak pouze konfigurace jednotlivých zařízení. Tuto možnost ale nenabízí nástroj vyvinutý společností, proto je vše zálohováno ručně přes webové rozhraní kamerových serverů. Tato záloha probíhá vždy druhé úterý v měsíci při pravidelných serverových kontrolách.

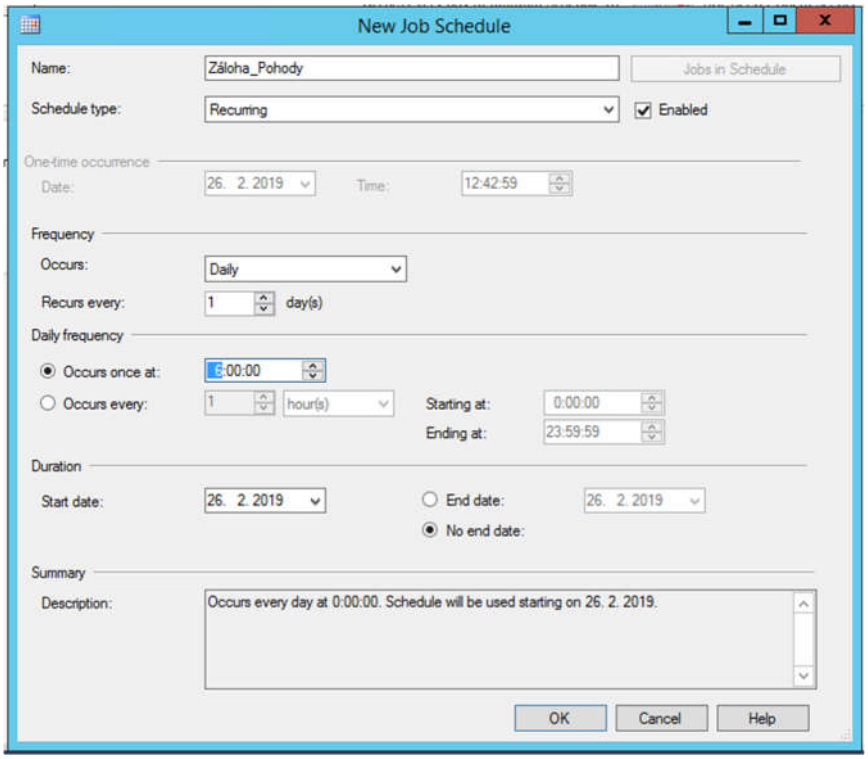
3.7.7 Zálohování databází Pohody, Pamici a Power BI

Prvním krokem bude přihlášení na SQL server. V ukázkovém příkladu se bude jednat o nastavení zálohy databáze Pohody. V serveru je otevřena záložka management, poté maintanance plan a začnu s tvorbou plánu. Jak je vidět na obrázku číslo 51, v prvním kroku je určován název plánu údržby.



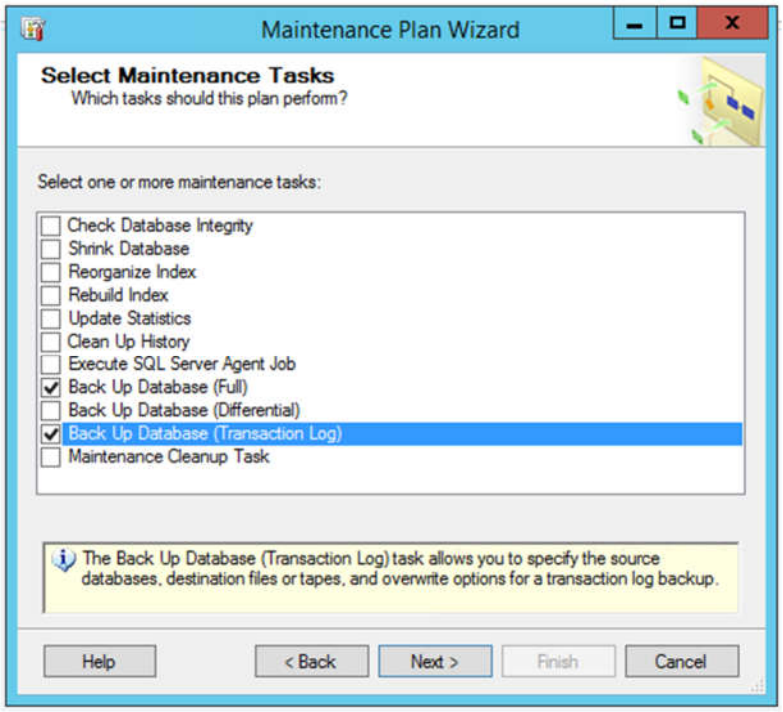
Obr. 51: Vytvoření maintanance plánu zálohy databáze (vlastní).

V dalším kroku jsou nastaveny parametr: typ úlohy, frekvenci, počátek a konec. Čas je nastaven na 6:00 dle zálohovacího plánu. Frekvenci 1x denně. Vše je uvedeno v obrázku číslo 52.



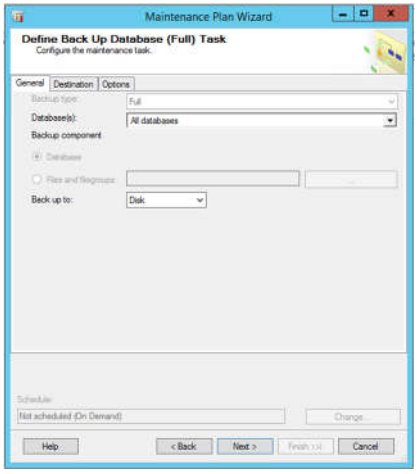
Obr. 52: nastavení času zálohování DB (vlastní).

Třetím krokem je výběr možností, které chci provádět, v tomto případě je vybrána možnost full backup a transaction backup (kvůli logování událostí). Toto nastavení je vyobrazeno na obrázku číslo 53.

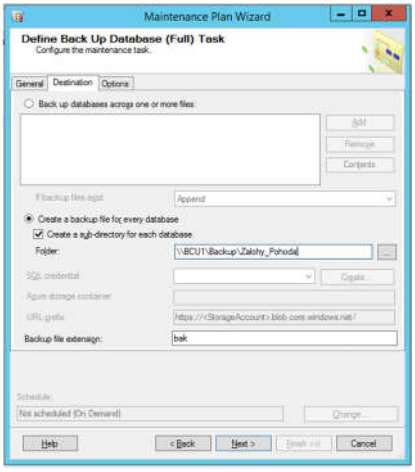


Obr. 53: Výběr typu zálohování DB (vlastní).

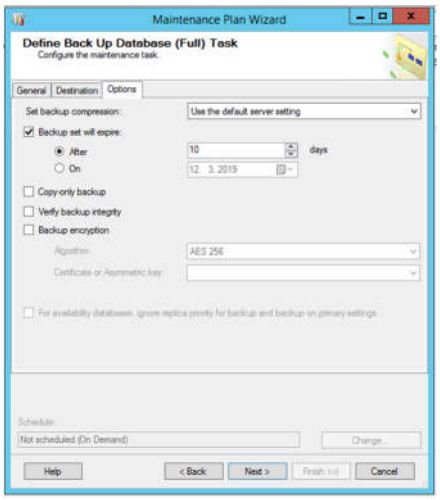
V posledních krocích jsou vybrány databáze, které budou zálohovány a možnost typů zálohovacího média. V dalším kroku je zadáno konkrétní cílové úložiště dat, v tomto případě \\BCU1\Backup\Zalohy_Pohoda\Full. Je zvolena možnost, která pro každou databázi na serveru vytvoří vlastní složku. Toto je velmi dobrá možnost při obnově pouze části dat, případně při řešení problémů Pohody, které nemusí zahrnovat všechny databáze. V posledním se kroku už jedná pouze o doplňující nastavení, zde je nejdůležitější nastavení expirace záloh, aby nedocházelo k přeplnění místa v úložišti. Po dohodě s jednatelem společnosti je doba uchování záloh nastaveno na 10 dnů. Stejné nastavení je realizováno i pro nastavení transakčního typu zálohování. Zde je změněna cesta na \\BCU1\Backup\Zalohy_Pohoda\Transakce a čas na 7:30. Data z Pamici se zálohují společně s daty z Pohody. Jedna z DB patří tak Pamice. Data z Power_BI budeme zálohovat v 7:00 stejným způsobem pouze s cestou\\BCU1\Backup\Zalohy_power_BI



Obr. 54:Základní nastavení plánu (vlastní).



Obr. 55: Nastavení cíle plánu zálohování (vlastní).



Obr. 56: Doplňující nastavení plánu (vlastní).

3.8 Doporučení pro tvorbu interních směrnic

Tato část mé diplomové práce je věnována návrhu interní směrnice upřesňující práva a povinnosti poskytovatele a objednatele služeb správy sítě. Směrnice je závěrečným krokem v zavedení zálohovacího plánu, protože když tato směrnice není vypracována není možné nijak dokládat práva a povinnosti obou stran. V případě ztráty dat není definována odpovědná osoba a objednatel je bez dat, což může mít likvidační vliv na jeho podnikatelskou činnost.

3.9 Návrh směrnice zálohování

Směrnice systému zálohování a obnovy dat ve společnosti XY.s.r.o

Objednatel: Společnost XY.s.r.o. zastoupená Michalem Novákem

Poskytovatel: Společnost YX.s.r.o poskytující služby v oblasti správy počítačové sítě zastoupená Ondřejem Hriadeľem

V tabulce číslo 14 je přehled subjektů odpovědných za umístění, úschovu a údržbu jednotlivých HW částí celého systému.

Tab. 15:Zodpovědné osoby (vlastní).

Zařízení	**Zodpovědný subjekt**
Zařízení v rámci vnitřní sítě a poboček	Společnost YX.s.r.o. zastoupená Ondřejem Hriadeľem
Externí zařízení vně sítě (NAS)	Společnost XY.s.r.o. zastoupená Michalem Novákem

Definice základních pojmů:

Uživatel – uživatelem je každý zaměstnaný subjekt, který přistupuje do lokální sítě s přihlašovacími údaji, které mu byly vydány správcem sítě.

Software – software je definován jako programové vybavení, které uživatelé společnosti XY.s.r.o využívají k výkonu práce. Případně se jedná o programové vybavení potřebné k řízení s správě sítě.

Hardware – Hardware je myšleno veškeré fyzické vybavení potřebné k realizaci sítě ve společnosti XY.s.r.o (servery, síťové prvky, kamery atd.)

Zálohování – proces vytvoření dat, která slouží k obnově systému do původního stavu.

Záloha – výsledek zálohování, data, která při ztrátě původních dat poskytnou možnost obnovení a uvedení systému do původního stavu.

Účel směrnice: Účelem směrnice je poskytnout přehled o právech a povinnostech poskytovatele a objednatele v oblasti zálohování a obnovení dat.

Obsah jednotlivých článků směrnice:

Tab. 16: Seznám článků směrnice (vlastní).

Článek I	Obecná ustanovení
Článek II	Zálohování fyzických a virtuálních serverů
Článek III	Zálohování uživatelských stanic
Článek IV	Zálohování síťových prvků
Článek V	Zálohování NAS zařízení
Článek VI	Zálohování DB
Článek VII	Shrnutí

Článek I – Obecná ustanovení

Objednatel se zavazuje, že na reklamace výsledků a podání podrobnějšího vysvětlení měsíčního reportu má 7 pracovních dní. Tyto dny jsou počítány od prvního pracovního dne následujícího měsíce a od přijetí reportu. Report je povinen zaslat poskytovatel nejpozději do prvního pracovního dne následujícího měsíce.

V případě ostatních reportů je objednatel povinen ozvat se s případnými stížnostmi do 24 h od obdržení reportu.

Odpovědnost za funkčnost a kontrolu systému zálohování nese poskytovatel. V případě nedodržení kontrol, či způsobením chyby poskytovatelovým zaviněním, je poskytovateli udělena pokuta ve výši 25 % z celkových měsíčních nákladů na služby poskytovatele.

Poskytovatel nenese odpovědnost v případě neovlivnitelných událostí nebo při pochybení a nedodržení této směrnice ze strany objednatele. V tomto případě nemá objednatel nárok na náhradu škody a práce nutné k uvedení systému do původního stavu uhradí do 20 dne dalšího měsíce na základě smlouvy o poskytování služeb.

Poskytovatel nenese odpovědnost za výpadek konektivity. Zde přechází odpovědnost na poskytovatele internetového připojení.

Poskytovatel nenese odpovědnost za mechanické porušení sítě nekompetentní osobou a následného narušení schématu sítě.

Poskytovatel se zavazuje informovat objednatele o možnosti nefunkčnosti zařízení z důvodu jeho končící životnosti. Poskytovatel bude vycházet z informací poskytnutých výrobcem zařízení.

Objednatel se zavazuje poskytnout informace o dalších krocích ohledně staří zařízení, a to do 24 h od obdržení informace o možné kolizi.

Poskytovatel nenese odpovědnost za závady způsobené výrobní chybou. Poskytovatel je povinen objednateli závadu nahlásit a udělat vše pro obnovu zálohovacího plánu.

Poskytovatel nenese odpovědnost za závady způsobené vnějšími vlivy počasí.

Poskytovatel se zavazuje zabezpečit zařízení tak, aby eliminoval riziko vzniku problému z technického, bezpečnostního hlediska i ostatních hrozeb.

Článek II – Zálohování serverů

Zálohování fyzických a virtuálních serverů je řízeno tabulkou číslo 17. Po dobu platnosti této směrnice a existence systému zálohování má poskytovatel tyto povinnosti: podle tabulky číslo 17 provádět kontroly systému zálohování podle daných intervalů a v daném rozsahu.

Tab. 17: Kontrolní mechanismus zálohování serverů (vlastní).

Předmět kontroly	Interval kontroly	Nástroj kontroly	Výstup kontroly	Odpovědná osoba
Provedení kontroly fukčnosti SW části zálohování fyzických i virtuálních serverů.	Každých 48 h počínaje platností této směrnice	Poskytovatel provede kontrolu záznamů z monitorovacího zařízení Zabbix a také kontrolu průběhu zálohování v aplikace windows Backup	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.
Provedení aktualizace zálohovacího server (stažení a instalace).	1 x měsíčně	Aktualizace operačního systému pomocí nástroje Windows update	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.
Provedení kontroly HW vybavení diskového pole a serverů.	1 x týdne	Testování výkonu HW a kontrola monitorovacího zařízení Zabbix. Dále kontrola Event manageru a HW nástrojů od společnosti DELL.	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.
Kontrola obnovení zálohy systému	1x měsíčně	V testovacím prostředí otestovat, zda je možné využít jednotlivé zálohy pro obnovení serverů do původního nastavení.	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.
Měsíční shrnutí	1x měsíčně	Vytvoření souhrnné zprávy o nečekaných událostech v rámci zálohovacího plánu (poruchy, neprovedené zálohy aj.) a o aktuálním stavu zálohování.	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.

Článek III – Zálohování uživatelských stanic

Zálohování uživatelských stanic je prováděno pomocí funkce systému Windows – Windows backup. Dalším bezpečnostním mechanismem je nastavení nástroje folder redirection, které slouží k ochraně uživatelských dat a dokumentů.

Objednatel zajistí, že všichni uživatelé počítačové sítě budou informování o skutečnosti, že zálohy probíhají jednou za 2 dny ve 22:00. Dále pak informuje uživatele, že jsou zálohovány složky Dokumenty a Obrázky. Za data uložená mimo tyto úložiště nenese poskytovatel žádnou odpovědnost.

Funkce folder redirection bude nastavena na složku Dokumenty a AppData. Objednatel je informován o těchto skutečnostech a předá tyto informace uživatelům.

Podle tabulky 18 budou prováděny kontroly funkčnosti systému zálohování uživatelských stanic.

Poskytovatel neodpovídá za nefunkční folder redirection u nově příchozích uživatelů, kteří nebudou uvedeni na seznamu poskytnutém objednatelem.

Tab. 18: Kontrolní mechanismus zálohování uživatelských stanic (vlastní).

Předmět kontroly	Interval kontroly	Nástroj kontroly	Výstup kontroly	Odpovědná sooba
Kontrola aktuálnosti seznamu pro GPO.	1x měsíčně	Kontrola bezpečností skupiny folder redirection a její aktuálnosti na základě dat poskytnutých objednatelem.	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.
Provedení kontroly fukčnosti SW části zálohování fyzických stanic.	Každých 48 h počínaje datem podepsání této směrnice	Poskytovatel provede kontrolu záznamů z monitorovacího zařízení Zabbix a také kontrolu aktuálnosti složky na BCU serveru.	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.
Měsíční shrnutí	1x měsíčně	Vytvoření souhrné zprávy o nečekaných událostech v rámci zálohovacího plánu (poruchy, neprovedené zálohy aj.) a o aktuálním stavu zálohování.	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.

Článek IV – Zálohování síťových prvků

Zálohování síťových prvků je ve většině případů automatizovanou záležitostí. Zálohování síťových prvků probíhá na základě tabulky číslo 19.

Tab. 19: Kontrolní mechanismus zálohování síťových prvků (vlastní).

Předmět kontroly	Interval kontroly	Nástroj kontroly	Výstup kontroly	Odpovědná osoba
Kontrola záloh na BCU serveru	1x měsíčně	Poskytovatel provede kontrolu aktuálnosti složky na BCU serveru a také přímo v konkrétním zařízení.	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.
Provedení kontroly funkčnosti SW části zálohování síťových prvků.	Každých 48 h počínaje datem začátkem platnosti této směrnice	Poskytovatel sleduje vývoj jednotlivých nástrojů pro síťové prvky a sleduje, zda nedochází k SW změnám v rámci zálohování, pokud ano, tak provede příslušná opatření, aby byl dodržen zálohovací plán.	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.
Měsíční shrnutí	1x měsíčně	Vytvoření souhrnné zprávy o nečekaných událostech v rámci zálohovacího plánu (poruchy, neprovedené zálohy aj.) a o aktuálním stavu zálohování.	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.

Článek V – Zálohování NAS

Poskytovatel zajistí nastavení zálohování na externí NAS mimo firemní síť.

Poskytovatel neodpovídá za ztráty způsobené neodborným zásahem do nastavení osobní jednateli NAS

Tab. 20: Kontrolní mechanismus zálohování NAS zařízení (vlastní).

Předmět kontroly	Interval kontroly	Nástroj kontroly	Výstup kontroly	Odpovědná osoba
Kontrola aktualizací operačního systému NAS a jednotlivých doplňků potřebných pro fungování zálohování.	1x měsíčně	Kontrola a provedení aktualizací.	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.
Provedení kontroly využití úložiště.	1x měsíčně	Poskytovatel provede kontrolu využití úložiště a v případě nutnosti informuje objednatele o docházející kapacitě.	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.
Měsíční shrnutí	1x měsíčně	Vytvoření souhrnné zprávy o nečekaných událostech v rámci zálohovacího plánu (poruchy, neprovedené zálohy aj.) a o aktuálním stavu zálohování.	Report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.

Článek VI - Zálohování databází

Poskytovatel se zavazuje informovat neprodleně objednatele o každém problému vzniklém při zálohování DB, protože se jedná o kritická data. Objednatel se zavazuje předat poskytovateli rozhodnutí, zdali souhlasí s navrhovanými kroky do 24 h od informování o problému**.**

Tab. 21: Kontrolní mechanismus zálohování databází (vlastní).

Předmět kontroly	**Interval kontroly**	**Nástroj kontroly**	**Výstup kontroly**	**Odpovědná osoba**
Kontrola aktualizací MS SQL serveru.	1x měsíčně	Kontrola a provedení aktualizací.	Výstupem kontroly bude report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.
Provedení kontroly využití úložiště.	1x měsíčně	Poskytovatel provede kontrolu využití úložiště a v případě nutnosti informuje objednatele o docházející kapacitě.	Výstupem kontroly bude report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.
Zajištění kontroly iSci připojení	Každých 24 h počínaje podpisem této směrnice	Poskytovatel provede kontrolu, zda je připojení s NAS aktivní a je možné virtuální server a fyzické servery zálohovat.	Výstupem kontroly bude report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.
Kontrola SW nastavení zálohování DB	1x měsíčně	Poskytovatel sleduje vývoj jednotlivých nástrojů pro MS SQL a sleduje, zda nedochází ke změnám v rámci zálohování, pokud ano, tak provede příslušná opatření, aby byl dodržen zálohovací plán bez vlivu.	Výstupem kontroly bude report poskytovaný objednateli v emailové formě.	Správce sítě ze společnosti poskytovatele služeb v oblasti správy sítě.

Článek VII – Závěrečná ustanovení

Objednatel: Společnost XY.s.r.o. zastoupená Michalem Novákem

Poskytovatel: Společnost YX.s.r.o poskytující služby v oblasti správy počítačové sítě zastoupená Ondřejem Hriadeľem

Tato směrnice byla schválena objednatelem i poskytovatelem služeb. Je vyhotovena ve dvou vyhotoveních.

Platnost směrnice je 1 rok od data podepsání.

Objednatel i poskytovatel se zavazují dodržovat veškerá práva a povinnosti uvedeny v článcích I-VII. Sankce za nedodržení těchto práv a povinností jsou definované v Článku I – obecná ustanovení.

Obsah směrnice lze měnit pouze na základě písemného dodatku schváleného oběma zúčastněnými stranami.

V Brně dne 11.3.2019

Za objednatele Michal Novák

Za poskytovatele Ondřej Hriadeľ

3.10 Zhodnocení navrhovaného řešení

Tabulka číslo 22 se týká pouze nákladů na služby poskytovatele. Společnost provedla HW renovaci, a proto jsou veškerá zařízení nakoupena. Zároveň na nich bývalý administrátor provedl základní konfiguraci. Tento administrátor špatně a nedostatečně využil potenciál zařízení. Přestože je již všechen HW nakoupen, je potřebný pro realizaci plánu, proto jsem v tabulce číslo 22 vyčíslil náklady na HW. V tabulce číslo 23 jsem poté náklady sjednotil a dostal tak výslednou cenu za realizaci zálohovacího plánu. Ceny v tabulkách 21, 22, 23 i 24 jsou platné k 6.5.2019.

Tab. 22: Nákladů na práci (32) (vlastní).

Úkon	Počet hodin	Cena za hodinu bez DPH za h	Cena s DPH za h	Koncová cena bez DPH	Koncová cena s DPH
Úvodní audit	2	700 Kč	847 Kč	1 400 Kč	1 694 Kč
Návrh řešení	3	700 Kč	847 Kč	2 100 Kč	2 541 Kč
Mikrotik setup	1,5	700 Kč	847 Kč	1 050 Kč	1 271 Kč
Server setup	4	700 Kč	847 Kč	2 800 Kč	3 388 Kč
Konfigurace ostatních síťových zařízení	8	700 Kč	847 Kč	5 600 Kč	6 776 Kč
Vytvoření směrnice	3	700 Kč	847 Kč	2 100 Kč	2 541 Kč
Testování řešení	5	700 Kč	847 Kč	3 500 Kč	4 235 Kč
Nastavení monitoringu	1	700 Kč	847 Kč	700 Kč	847 Kč
Cena celkem	27,5	700 Kč	847 Kč	19 250 Kč	23 293 Kč

Tab. 23: Náklady na HW (33) (vlastní).

Název zařízení	Počet	Cena za ks bez DPH (Kč)	Cena za ks s DPH (Kč)	Cen bez DPH za množství (Kč)	Cena s DPH za množství (Kč)
Dell PowerVault MD3400	1	154840,79	196001	154840,79	196 001
Dell PowerEdge R430	2	25384,675	32132,5	50769,35	64 265
RAM 32 GB	2	7213,49	9131	14426,98	18 262
NAS Synology DSJ218	4	1856,105	2349,5	7424,42	9398
8TB Seagate Ironwolf	3	6634,946667 Kč	8398,666667	19904,84	25196
Seagate Barracuda PRO 3,5-2TB	3	2590,41	3279	7771,23	9837
Samsung Enterprise SSD 240GB	4	1576,84	1996	6307,36	7984
Celkem	x	200097,2567	253287,6667	261444,97	330943

Tab. 24: Shrnutí nákladů na realizace

Položka	Cena bez DPH celkem	Cena s DPH celkem
Náklady na práci	19 250č	23 293
Náklady na HW	261 445	330 943
Celkem	280 695	354 236

Jak je možné vidět v tabulce číslo 24 cena za realizaci činí 280 695 Kč bez DPH. Je nutné podotknout, že HW část neslouží pouze pro účely zálohování. HW tak bude využíván i k jiným účelům a náklady se rozloží na více úkonů. Společnost má zisky v řádem jednotek až desítek milionů, proto je tato investice velmi nutná. Společně s jednatelem společnosti byl vytvořen přibližný plán nákladů při ztrátě dat. Při hodinovém výpadku jsou ztráty v řádů statisíců. Při naprosté ztrátě uživatelských dat se dostáváme na 1 milion korun. Kdyby došlo k naprosté ztrátě databáze, tak se jedná o fatální problém a společnost by nebyla schopná se z této situace vzpamatovat, protože náklady by sahali až k prvnímu dni od založení.

Tab. 25: Odhadované náklady při nefunkčnosti systému(vlastní).

Položka		Výpadek na 1h provozu
Nedostupnost serverových prostředků		130 000,00 Kč
	Mzdy	10 000,00 Kč
	Zařízení	120 000,00 Kč
Nedostupnost DB		100 000,00 Kč
Ztráta uživatelských dat		
	Mzdy	10 000,00 Kč
	Data	1 000 000,00 Kč
Ztráta DB		Nevyčíslitelné

ZÁVĚR

Cílem této diplomové práce byl návrh a realizace zálohovacího plánu společnosti a s tím spojený návrh interní směrnice o zálohování.

V první fázi diplomové práce jsem shrnul teoretické poznatky potřebné pro vypracování návrhové části diplomové práce a využití správných technologií. V analytické části jsem vyhodnotil aktuální stav zálohování a veškerých aktiv spojených s tvorbou zálohovacího plánu. V analytické části jsem také zhodnotil rizika, která mohou vzniknout při realizaci návrhu. Tato analýza sloužila jako ukazatel největších rizik, která je nutné pokrýt, aby byla realizace co nejméně riziková. Ve třetí části práce jsem se věnoval nejdříve návrhu zálohovacího plánu tak, aby splňoval požadavky investora a byla zajištěna záloha všech dat nutných pro provoz společnosti. Poté jsem návrh zálohovacího plánu otestoval a zrealizoval. Dalším krokem bylo navržení interní směrnice, která je věnována právům a povinnostem poskytovatele i odběratele služeb spojených se zálohovacím plánem. Posledním krokem bylo zhodnocení celé realizace. Kromě vyhodnocení nákladů jsem na základě poznatků od jednatele společnosti vypracoval možné finanční ztráty při nedostupnosti dat.

Cíle této diplomové práce byly naplněny, což bylo potvrzeno i spokojeností jednatele společnosti. Navržený zálohovací plán je již v provozu a v několika případech byl využit a bylo tak zabráněno ztrátě dat.

SEZNAM ZDROJŮ

(1) BOTT, Ed. Mistrovství v zabezpečení Windows 2000 a XP. Brno: Computer Press, 2004. ISBN 80-722-6878-3.

(2) BAROT, Gaurav, Chintan MEHTA a Amij PATEL. Hadoop Backup and Recovery solutions. Mumbai: Packt Publishing, 2015. ISBN 978-1783289042.

(3) ROUSE, Margaret. What is backup?. In: TechTarget [online]. 2016 [cit. 2018-03-24]. Dostupné z: http://searchdatabackup.techtarget.com/definition/backup.

(4) DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat. Brno: Computer Press, 2004. ISBN 80-251-0106-1.

(5) IMOBIE. *Imobie.com* [online]. 2019 [cit. 2019-03-24]. Dostupné z: https://www.imobie.com/support/top-5-causes-of-data-loss.htm.

(6) 3S. *3s.sk* [online]. 2012 [cit. 2018-03-06]. Dostupné z: http://www.3s.cz/sk/odborna-sekcia/detail/id/46-definicia-a-rotacie-zaloh.

(7) ACRONIS. *Acronis.com* [online] .2019 [cit. 2019-03-24]. Dostupné z: https://www.acronis.cz/kb/diferencialni-zaloha/

(8) NAKIVO. Nakivo.com[online] .2019 [cit 2019-03-24] Dostupné z: https://www.nakivo.com/blog/backup-types-explained-full-incremental-differential-synthetic-and-forever-incremental/.

(9) LIU, Ling a M. Tamer ÖZSU. Encyclopedia of Database Systems. New York: Springer, 2009. ISBN 978-0-387-39940-9.

(10) ENTERPRISE FEATURES STAFF. Backup Types: Full, Incremental, Differential. Enterprise Features [online]. 2015 [cit. 2017]. Dostupné z: http://www.enterprisefeatures.com/backup-types-full-incremental-differential/.

(11) DATA RECOVERY GROUP. Data storage history and future. Data Recovery Group [online]. 2011 [cit. 2017]. Dostupné z: http://www.datarecoverygroup.com/articles/data-storage-history-and-future.

(12) ROUSE, Margaret. SSD(solid-state drive): TechTarget [online]. 2016 [cit. 2018-03-24]. Dostupné z: https://searchstorage.techtarget.com/definition/SSD-solid-state-drive.

(13) IBM. Icons of Progress: Magnetic Tape Storage. IBM100 [online]. 2019 [cit. 2019-03-24]. Dostupné z: http://www-03.ibm.com/ibm/history/ibm100/us/en/icons/tapestorage/.

(14) NELSON, Steven. Pro Data Backup and Recovery. New York: Apress, 2011. ISBN 978-1-4302-2663-5.

(15) ROUSE, Margaret. Virtual Tape Library (VTL). Tech Target [online]. 2019 [cit. 2019-03-24]. Dostupné z: http://searchdatabackup.techtarget.com/definition/virtual-tapelibrary-VTL.

(16) LACIE. Lacie.com [online]. 2019 [cit. 2019-03-24]. Dosupné z: https://www.lacie.com/gb/en/manuals/lrm/raid/.

(17) Solutions. Apex Microsystems [online]. 2009 [cit. 2012-03-24]. Dostupné z: http://www.apexmicrosystems.com/?page_id=518

(18) KOOP, Karsten, Dorian COUGIAS a E.L. HEIBERGER. The Backup Book: Disaster Recovery from Desktop to Data Center. 3rd edition. Schaser-Vartan Books, 2003. ISBN 978-0972903905.

(19) MICROSOFT. Microsoft.com [online]. 2019 [cit 2019-03-24]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-cloud-computing/.

(20) AMAZON WEB SERVICES. Amazon.com [online]. 2019 [cit 2019-03-24]. Dostupné z: https://aws.amazon.com/what-is-cloud-computing/.

(21) PECINOVSKÝ, Josef. Archivace a komprimace dat: jak zálohovat data, jak komprimovat soubory WinRAR, WinZip, WinAce, Windows a nástroje komprese dat, jak archivovat data ve Windows. Praha: Grada, 2003. ISBN 80-247-0659-8.

(22) KLJUN, Matjaž, John MARIANI a Alan DIX. Toward understanding short-term personal information preservation: A study of backup strategies of end users. Journal of the Association for Information Science [online]. 2016, 67(12), 2947-2963 [cit. 2018-03-24]. DOI: 10.1002/asi.23526. ISSN 23301635.

(23) SOSINSKY, B. Mistrovství – počítačové sítě. 1. vyd. Brno: Computer Press, 2010. 840 s. ISBN 978-80-251-3363-7.

(24) Data Storage History and Future. Data Recovery Group [online]. 07/08/2011 [cit. 2019-05-10]. Dostupné z: http://www.datarecoverygroup.com/articles/data-storagehistory-and-future

(25) MESSMER, Hans-Peter a Klaus DEMBOWSKI. Velká kniha hardware. Brno: CP Books, 2005. ISBN 80-251-0416-8.

(26) SALEKUL ISLAM a MOHAMMAD AMANUL ISLAM. SysProp: A Web-based Data Backup, Synchronization and System Administration. International Journal of Computer Network and Information Security [online]. 2014, 6(9), 1-11 [cit. 2019-04-08]. DOI: 10.5815/ijcnis.2014.09.01. ISSN 2074-9090. Dostupné z: http://www.mecspress.org/ijcnis/ijcnis-v6-n9/IJCNIS-V6-N9-1.pdf

(27) STRICKLAND, Jonathan. Home / Tech / Computer / Internet / Cloud Computing How Cloud Computing Works. Computer.howstuffworks.com [online]. 2019 [cit. 2019-03-03]. Dostupné z: http://computer.howstuffworks.com/ cloud-computing/cloud-computing1.htm.

(28) PRESTON, W. C. Backup & Recovery: Inexpensive Backup Solutions for Open Systems. Sebastopol, CA: O´Reilly Media, Inc., 2006. First Edition. ISBN 978- 0-596-10246-3.

(29) SOMASUNDARAM, G. a A. SHRIVASTAVA. Information Storage and Management: Storing, Managing, and Protecting Digital Information. Indianapolis: Wiley Publishing, Inc., 2009. ISBN 978-0-470-29421-5

(30) MEYERS, Mike a Scott JERNIGAN. Osobní počítač: názorný průvodce hardwarem, systémem a sítěmi. Vyd. 1. Brno: CP Books, 2005. ISBN 80-251-0834-1.

(31) Improved backup script for Ubiquiti UniFi controller. Github.com [online]. 2019 [cit. 2019-05-02]. Dostupné z: https://gist.github.com/corny/3cf7af0f6cb7a00adeb3

(32) Smlouva o poskytování IT služeb v oblasti správy sítí. Brno, 2017. [cit. 2019-05-02]

(33) Export zaplacených závazků společnosti za období 01/2016-12/2019. Brno, 2017. [cit. 2019-05-02]

(34) CZC. Czc.cz [online]. 2019 [cit 2019-03-24]. Dostupné z: https://www.czc.cz/synology-diskstation-ds218/220863/produkt

SEZNAM TABULEK

SEZNAM OBRÁZKŮ

SEZNAM ZKRATEK

HR	Human resource
NTB	Notebook
DDR	Double Data Rate
HW	Hardware
SW	Software
U	Unit
GHZ	Gigahertz
AP	Access point
LR	Long ranged
NVR	Network video recorder
TB	Terabyte
MB	Megabyte
IT	Information technology
NAS	Network attached storage
HDD	Hard disk drive
AD	Active directory
DNS	Doman name system
DHCP	Dynamic host configuration protocol
CEO	Chief executive officer
USB	Universal seriál bus
IIS	Internet information server
VPN	Virtual private network
EOIP	Ethernet over IP
GPT	GUID partition table
MRB	Master boot record
DB	Database
RAM	Random Access Memory
MTU	Maximum transmission unit
ODBC	Open database connectivity