VYSOKÉ UČENÍ TECHNICKÉ V BRNĚ

BRNO UNIVERSITY OF TECHNOLOGY

FAKULTA PODNIKATELSKÁ
ÚSTAV INFORMATIKY

FACULTY OF BUSINESS AND MANAGEMENT
INSTITUTE OF INFORMATICS

ZÁLOHOVÁNÍ A ARCHIVACE DAT V PROSTŘEDÍ MALÉ FIRMY

DATA BACKUP AND ARCHIVING IN SMALL BUSINESS ENVIRONMENT

DIPLOMOVÁ PRÁCE
MASTER'S THESIS

AUTOR PRÁCE — Bc. TOMÁŠ SVITANA
AUTHOR

VEDOUCÍ PRÁCE — Ing. VIKTOR ONDRÁK, Ph.D.
SUPERVISOR

BRNO 2012

Vysoké učení technické v Brně
Fakulta podnikatelská

Akademický rok: 2011/2012
Ústav informatiky

ZADÁNÍ DIPLOMOVÉ PRÁCE

Svitana Tomáš, Bc.

Informační management (6209T015)

Ředitel ústavu Vám v souladu se zákonem č.111/1998 o vysokých školách, Studijním a zkušebním řádem VUT v Brně a Směrnicí děkana pro realizaci bakalářských a magisterských studijních programů zadává diplomovou práci s názvem:

Zálohování a archivace dat v prostředí malé firmy

v anglickém jazyce:

Data Backup and Archiving in Small Business Environment

Pokyny pro vypracování:

Úvod
Vymedzenie problému a cieľa práce
Analýza súčasného stavu
Teoretická východiska riešenia
Návrh riešenia
Zhodnotení a záver
Zoznam použitej literatúry
Prílohy

Seznam odborné literatury:

BORGHOFF, U. M., RÖDIG, P., SCHEFFCZYK, J. Long-Term Preservation of Digital Documents : Principles and Practices. 1st ed. 2006 edition. Berlin : Springer, 2006. 289 s. ISBN 978-3642070174.
BUCHANAN, S. Microsoft Data Protection Manager 2010. Birmingham : Packt Publishing, 2011. 360 s. ISBN 978-1849682022.
DE GUISE, P. Enterprise Systems Backup and Recovery: A Corporate Insurance Policy. 1 edition. Boca Raton : Auerbach Publications, 2008. 308 s. ISBN 978-1420076394.
GREGORY, P. IT Disaster Recovery Planning For Dummies. 1 edition. Hoboken : Wiley Publishing, 2007. 360 s. ISBN 978-0470039731.
NELSON, S. Pro Data Backup and Recovery. 1 edition. New York : Apress, 2010. 350 s. ISBN 978-1430226628.

Vedoucí diplomové práce: Ing. Viktor Ondrák, Ph.D.

Termín odevzdání diplomové práce je stanoven časovým plánem akademického roku 2011/2012.

L.S.

Ing. Jiří Kříž, Ph.D. Ředitel ústavu	doc. RNDr. Anna Putnová, Ph.D., MBA Děkan fakulty

V Brně, dne 20.05.2012

Abstrakt

Obsahom mojej diplomovej práce je úvodná analýza aktuálneho stavu vo vybranej firme, za ktorou nasleduje základné teoretické pozadie problematiky. Podstatnou časťou je vypracovanie vlastného návrhu systému zálohovania a archivácie dát v prostredí malej firmy, ktorý bude aplikovaný v praxi pri maximálnom ohľade na ekonomickú a kvalitatívnu stránku systému.

Abstract

Purpose of my master's thesis is an initial analysis of the current status of the selected company, which follows the basic theoretical background of the issue. Essential part of thesis is developing draft of backup and archive system in a small business environment, which will be applied in practice with respect to the maximum economic and qualitative aspects of the system.

Kľúčové slová

Záloha, dáta, obnova, plán, DPM 2012, smernica, RAID, archivácia.

Keywords

Backup, data, recovery, schedule, DPM 2012, directive, RAID, archiving.

Bibliografická citácia

SVITANA, T. *Zálohování a archivace dat v prostředí malé firmy*. Brno: Vysoké učení technické v Brně, Fakulta podnikatelská, 2012. 100 s. Vedúci bakalárskej práce Ing. Viktor Ondrák, Ph.D.

Čestné prehlásenie

Prehlasujem, že predložená diplomová práca je pôvodná a spracoval som ju samostatne. Prehlasujem, že citácia použitých prameňov je úplná, že som vo svojej práci neporušil autorské práva (v zmysle Zákona č. 121/2000 Sb., o práve autorskom a o právach súvisiacich s právom autorským).

V Brne dňa ..... …..……

Tomáš Svitana

Poďakovanie

Rád by som poďakoval vedúcemu mojej bakalárskej práce, práce Ing. Viktorovi Ondrákovi, Ph.D. za jeho prínosné rady a metodickú pomoc, ktoré ma nasmerovali k vypracovaniu tohto dokumentu.

Obsah

ÚVOD

Zálohovanie, slovo často skloňované v rôznych súvislostiach s dátami. Len málokto si však uvedomuje jeho pravú stránku. Zväčša je zamieňané s pojmom „kopírovanie dát“, ktoré je iba jedným krokom procesu zálohovania dát. S potrebou ochrany dát formou zálohovania sa stretávame aj v tom najmenšom meradle – pre osobnú potrebu. Avšak komplexnejšie riešenie vyžaduje korporátne prostredie, kde nie je priestor pre omyly a chybné konfigurácie. Práve menšia firma, často závislá na chode informačného systému alebo emailového servera, si neuvedomuje potenciálnu hrozbu, ktorú predstavuje strata dát. Samotná strata dát je iba posledným stupňom v celom reťazci zahrňujúcom obnovu dát v určenom časovom horizonte. Druhým stupňom je obnova z poslednej korektnej zálohy, pričom v prípade jej zlyhania sa dá hovoriť o strate dát.

Zálohovanie chápané ako „záchrana“ má svoju obdobu v komerčnom poistení. Spoločnosti, ktoré zažili určitý počet zlyhaní v IT (strata dát), redukujú náklady na vývoj a zlepšovanie systému záloh a presúvajú uvoľnené finančné prostriedky do komerčného poistenia dát. Táto situácia však prináša so sebou mnoho ďalších otázok. Ako príklad uvedieme otázku vyspelosti poisťovníctva v českej republike, alebo akúsi ochotu firmy akceptovať stratu dát, ktorá bude kompenzovaná finančným plnením zo strany poisťovne.

1 VYMEDZENIE PROBLÉMU A CIELE PRÁCE

Problém zálohovania a archivácie dát je stále aktuálnou témou. Vzhľadom k rastúcim dátovým objemom je potrebné hľadať nové, komplexné metódy bez zbytočnej redundancie dát.

Cieľom mojej diplomovej práce je navrhnúť ucelený systém zálohovania a archivácie dát s ohľadom na aktuálne požiadavky vybranej spoločnosti, s prihliadnutím na predpokladaný vývoj do budúcnosti v rozmedzí 2 - 3 rokov. Hlavným pilierom bude systém Microsoft Data Protection Manager (DPM) 2012. Súčasťou vypracovaného systému je aj integrácia procesov zálohovania na úrovni manažmentu spoločnosti, vypracovanie smerníc zálohovania, definície metrík procesu kontroly zálohovania, roztriedenie dát a pridelenie priorít ako aj stanovenie zodpovednosti v rámci organizačnej štruktúry.

2 ANALÝZA PROBLÉMU A SÚČASNÁ SITUÁCIA

Analyzovať problematiku zálohovania je pomerne časovo náročná práca, ktorá vyžaduje úplné preniknutie do štruktúry spoločnosti, poznanie jej silných a slabých stránok a zameranie sa na ošetrenie existenčných otázok v oblasti dát.

Popis súčasného stavu zahrňuje všetky existujúce prvky zálohovania a archivácie aktuálne k novembru 2011.

2.1 Predstavenie spoločnosti

Spomínaná problematika je poukázaná na malej spoločnosti s počtom približne dvadsať zamestnancov. Náplňou jej podnikateľskej činnosti je niekoľko odvetví. Webdesign, reklama a grafické štúdio patria do tzv. kreatívneho oddelenia. Zabezpečovanie akcií, festivalov, školení a teambuildingu je náplňou oddelenia produkcie. Obe oddelenia spája obchodné oddelenie, ktoré prináša množstvo nových príležitostí. Ako samostatný prvok funguje aj správca IT, avšak vzhľadom k „veľkosti“ nie je vhodné hovoriť o oddelení, ale o podpore chodu IT vo firme.

Na účely tejto práce budeme spoločnosť nazývať GPO, spol. s r.o.. Pre lepšiu predstavu o stave spresníme, že spoločnosť má 18 zamestnancov rozdelených do vyššie uvedených oddelení. Sídli v Brne a svojimi aktivitami pokrýva celý juhomoravský kraj a Prahu s okolím. Najvýznamnejšími klientmi sú DHL, Maersk, Amica, Autobenex a ďalší. V rámci svojej obchodnej stratégie vyniká schopnosťou i napriek nie početnému tímu realizovať projekty veľkého rozsahu. Ďalšou špecialitou je poskytovanie komplexných marketingových služieb väčším spoločnostiam.

Formou výhody pred konkurenciou je využívanie dotácií z európskej únie, najmä z programu „Operačný program ľudské zdroje a zamestnanosť“, kde hlavnou náplňou je poskytovať zamestnancom možnosť neustáleho zdokonaľovania a rozširovania znalostí formou odborných školení.

2.2 Analýza dát

Dáta sú jedným z najdôležitejších vstupov (a výstupov) firemných procesov. Ich včasné poskytnutie užívateľom ovplyvňuje produktivitu práce. Taktiež rýchle a presné získanie dát prináša pre firmu konkurenčnú výhodu.

Denne vzniká vo firme množstvo nových dát uložených na rôznych nosičoch a pomocou rôznorodých aplikácii. Dáta sú uložené v rôznych formách či už databázy, emaily, elektronické dokumenty (word, excel). Rozdielne typy ukladaných informácií majú rôznu hodnotu pre chod a fungovanie spoločnosti. Z pohľadu nákladov majú i dáta svoju cenu – cenu za uloženie a prípadne spracovanie IS, ktorá je definovaná nákladmi na ICT technológie a ľudské zdroje. S rastúcou bezpečnosťou a dostupnosťou dát narastajú aj náklady. Existuje potreba určiť (klasifikovať) jednotlivé dáta, aby nedochádzalo k umelému zaberaniu kapacity na nosičoch určených pre citlivé dáta, dátami s nízkou hodnotou. Vybudovanie efektívnej infraštruktúry na ukladanie dát znamená nájsť rovnováhu medzi splnením požiadaviek užívateľov a vynaloženými nákladmi.

2.2.1 Klasifikácia dát

Klasifikácia dát umožňuje nájsť optimálny spôsob uloženia dát, ktoré splňuje užívateľské nároky pri nasadení cenovo efektívnej technológie riešenia. Optimalizácia úrovne služieb a voľba vhodnej technológie ukladania dát umožňuje docieliť finančné úspory pri budovaní ICT[1] spoločnosti a vytvoriť tak cenovo efektívny nástroj pre zvládanie rastu objemu firemných dát. (1)

Aktuálne spoločnosť nemá spracovaný žiadny koncept klasifikácie dát, a preto sa stretáva s problémom nedostatku miesta na pevných diskoch nielen klientskych staníc ale i serverov. Pri pokuse o prečistenie úložného priestoru narazila na problém nejednotného ukladania, redundancie, kde mali rovnaké projekty rôzne pomenovanie a obe zložky obsahovali iné zloženie súborov. Tento stav značne komplikuje zálohovanie dát, hlavne dátového úložiska a spôsobuje enormný nárast kapacity potrebnej k uloženiu záloh.

[1] Skratka významu Informational and Comunication Technologies v preklade Informačné a komunikačné technológie.

Je preto nevyhnutné navrhnúť model klasifikácie dát a určiť tak priority, ktoré budú predstavovať najviac zabezpečenú oblasť z hľadiska zálohovania.

2.3 Analýza hardvérového zázemia

Pre korektný návrh zálohovacieho „mechanizmu“ je nutné detailne poznať hardvérové zázemie spoločnosti.

2.3.1 Servery

S nástupom virtualizácie fyzických serverov dochádza k redukcii priestoru potrebného na prevádzku serverov. S tým je spojené i znižovanie nákladov na energie. Firma využíva technológiu Microsoft Hyper-V.

SERVER HV

Server je fyzický stroj spoločnosti DELL, označenie R510 v konfigurácii:

- Procesor INTEL XEON E5645 (2.40GHZ),
- 32GB operačnej pamäti,
- x 500 GB SAS interný disk (systém) RAID1[2],
- 2 x 500 GB SAS interný disk RAID 1,
- Redundantný zdroj napájania.

Vzhľadom k použitej technológii Hyper-V, na kontroléri sú spustené štyri virtuálne servery:

- Server CRM[3] s IS Microsoft Dynamics CRM 2011
  virtuálny disk o veľkosti 120 GB, WIN 2008 R2,
- Server v testovacom režime TEST
  virtuálny disk o veľkosti 60 GB, WIN 2008 R2,
- Virtuálny operačný systém WIN 7
  virtuálny disk o veľkosti 80 GB, WIN 7,
- Server pre replikáciu domény DC
  virtuálny disk o veľkosti 60 GB, WIN 2008 R2.

[2] Skratka významu Redundant Array Of Independent Disks, v preklade redundantné pole nezávislých diskov.
[3] Skratka významu Customer Relationship Management, v preklade Riadenie vzťahu so zákazníkmi.

SERVER DC 2

Server spoločnosti DELL, označenie R210 v konfigurácii:

- Procesor INTEL CORE i3,
- 8GB operačnej pamäti,
- 2 x 250 GB SAS interný disk (system) RAID 1,
- WIN 2008 R2.

Na serveri bežia služby MS Exchange 2010, DHCP, DNS. Systémový disk s aktuálnou veľkosťou 160GB.

SERVER FS

Server SuperMicro v konfigurácii:

- Procesor INTEL Xeon,
- 4GB operačnej pamäti,
- 2 x 32 GB SAS interný disk (system) RAID 1,
- Pole o veľkosti 12 diskov (SATA),
- WIN 2008 R2.

Server má rolu fileserver, pričom slúži ako hlavné úložisko dát, a preto predstavuje najcitlivejšie miesto spoločnosti. Celková úložná kapacita predstavuje 4 TB.

2.3.2 Periférie

Okrem zálohovania serverov ako takých, je potrebné sa zamerať aj na uloženie (export) konfigurácie periférii typu Firewall, UPS[4], tlačiarne a iné. To je častým problémom a mnohokrát spôsobuje dlhšie výpadky služieb než obnova operačného systému servera. Samozrejme nejde o žiadne citlivé data, avšak ku príkladu konfigurácia firewall-u predstavuje prácu rádovo desiatok hodín.

2.3.3 Klientske stanice

Vzhľadom k centralizovanému systému ukladania dát na súborový server (fileserver), nie je aktuálne zavedený variant zálohovania klientskych staníc.

Typy PC používaných vo firme je možné rozčleniť do dvoch kategórií.

- Multimediálne PC
  - Ide o výkonné pc, využívané v sekcii grafiky.

[4] Skratka významu Uninterruptible power supply, v preklade neprerušiteľný zdroj napájania.

- Kancelárske PC
    - Ide o bežné PC, so základnými parametrami, ktoré postačujú pre prácu s MS Office 2010, Outlook.

Ani jedna spomínaná kategória nevyžaduje zálohovanie, nakoľko proces opravy /preinštalácie operačného systému a jeho konfigurácie je pomerne rýchly, dá sa povedať, že časovou náročnosťou zhodný s procesom obnovy systému pomocou nástroja recovery tool. Taktiež tým klesá objem zálohovaných dát.

2.4 Analýza softvérového zázemia

Dôležitým krokom k správnej implementácii systému zálohovania dát je poznanie softvérového pozadia spoločnosti. Okrem bežne používaných operačných systémov je pre nás zaujímavý aj chod databázy, prípadne emailového servera.

Väčšina podnikových informačných systémov má realizované úložisko práve formou databázy. Databázy zahrňujú najdôležitejšie informácie v spoločnosti, pričom každú minútu dochádza k modifikácii a zmenám obsahu.

2.4.1 Operačné systémy

Nevyhnutným stavebným prvkom softvérovej architektúry je operačný systém. Variantom jeho ochrany je vytváranie pravidelných záloh systému, ktoré sú použiteľné v prípade pádu systému z dôvodu zásahu operátora alebo pri zlyhaní hardvéru.

Spoločnosť GPO, spol. s r.o. využíva na všetkých svojich serveroch operačný systém Microsoft Windows Server 2008 R2 s aplikovaným servisným balíčkom SP1, čím je zaručená kompatibilita služieb medzi servermi.

Aktuálny stav zálohovania serverov je nevyhovujúci a kritický zároveň. Pre zálohovanie serverov sa využíva vstavaná funkcionalita Windows Backup s nastavením týždenného intervalu záloh, čo je rozhodne nedostačujúce. Zálohy sú smerované na jediný sieťový disk lokalizovaný v spoločnej miestnosti so servermi. Na viac je zálohovanie nastavené formou „stav systému“, ktoré v prípade výpadku hardvéru, poškodenia systémového disku predstavuje nepoužiteľný zdroj záloh. Je teda odvážne hovoriť o aktuálnom systéme zálohovania OS serverov a serverov ako celku, nakoľko žiadne neexistuje.

Klientske stanice operujú s OS Microsoft Windows 7 s nainštalovaným servisným balíčkom SP1[5]. Zálohovanie klientskych staníc z už uvedeného dôvodu nie je nastavené. S prihliadnutím na spôsob práce s dátami a vyťaženie PC to skutočne nie je potrebné.

2.4.2 Databázy

Databázy sú často kľúčovým prvkom v dátovej architektúre firmy. Ani tento prípad nie je výnimkou.

[5] Skratka významu Service pack, v preklade servisný balíček.

GPO, spol. s r.o. plne využíva interný informačný systém Microsoft Dynamics CRM 2011. Ten svojou funkcionalitou pokrýva takmer všetky oblasti činnosti spoločnosti, a preto ide rozhodne o najcitlivejšie miesto na stratu a poškodenie dát. Spoločnosť už od svojho vzniku využíva IS Dynamics CRM, ktorý bol pôvodne zakúpený vo verzii 3.0, nasledoval upgrade na verziu 4.0 a aktuálna verzia 2011.

Hlavným úložiskom dát pre MS Dynamics CRM 2011 je databáza SQL. Konkrétne produkt MS SQL SERVER 2008 R2 Enterprise s aplikovaným servisným balíčkom SP1. Databáza obsahuje údaje od roku 2003, kedy bol systém implementovaný. Dôležitým krokom pri migrácii bolo zachovanie pôvodných dát a rozšírenie funkcionality informačného systému.

Taktiež významným faktom je, že IS MS Dynamics CRM pracuje vo svojej podstate so všetkými normálnymi formami databáze, preto sa tu nevyskytujú javy typu redundancia dát, nesprávne delenie adries, nejednoznačná identifikácia a podobne.

Server CRM poskytuje ako jediný databázové služby. Stav zálohovania serveru ako takého je popísaný vyššie a ako vyplynulo nie je dostačujúci. Okrem záloh serveru je potrebné sledovať aj zálohy databázy separátne, aby ju bolo možné obnoviť na iný server bez nutnosti obnovy celého serveru.

Aktuálne nastavenie zálohovania databázy je pomerne rizikové a v prípade výpadku databázy môže viesť ku strate dát za posledných sedem dní. Tento fakt je však v súčasnej dobe, kedy majú informácie vysokú hodnotu, neprípustný. Rovnako ako u zálohovania serveru je i databáza zálohovaná jeden krát za 7 dní, a to vždy v sobotu. Je vytvorená plná záloha a následne odoslaná na sieťové úložisko. Nie je využitý princíp plnej a inkrementálnej zálohy, čo v prípade databázy rozsahu 120GB je nevyhnutnosť. Taktiež nie je vykonávaná údržba databázy na chyby a konzistenciu. I správne vykonaná záloha nemusí byť použiteľná a to v prípade, že databáza samotná je nekonzistentná.

2.4.3 Email server

Dnes najrýchlejším a relatívne nízko nákladovým spôsobom zasielania a výmeny informácií je používanie emailu. Ako i ostatné technológie, aj email má množstvo variant realizácie.

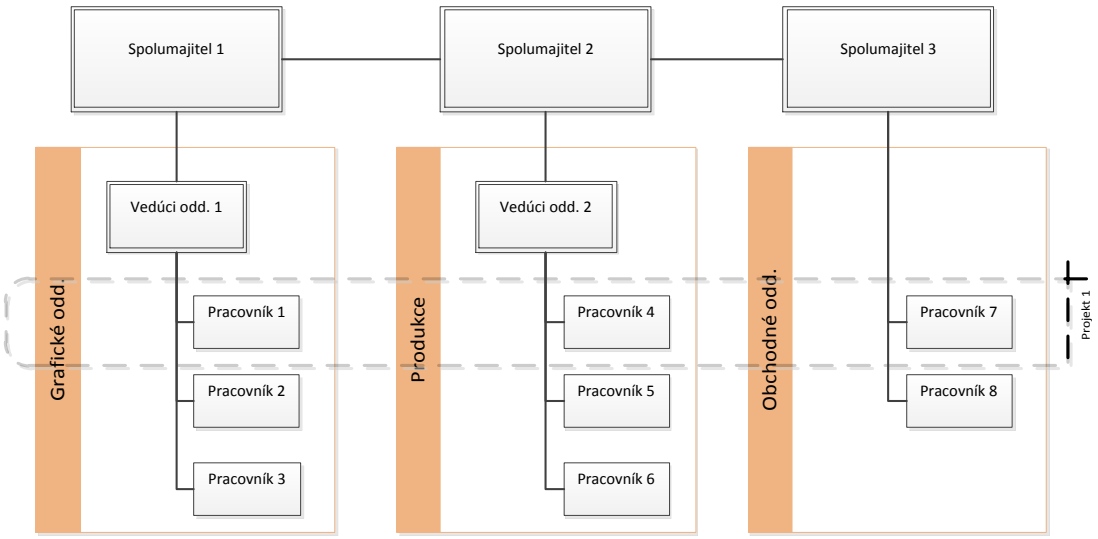
Spoločnosť GPO, spol. s r.o. využíva svoj vlastný emailový server, ktorý beží na platforme Microsoft Exchange 2010 s aplikovaným servisným balíkom SP1.

V súčasnosti veľkým problémom je objem dát uchovávaných formou emailov. Štandardná kvóta užívateľa, nastavená na 20GB už nie je dostatočná. I napriek prevedenej analýze obsahu schránok a upozornení užívateľov bolo nutné povoliť navýšenie kapacity na 25GB na schránku, čo je samozrejme dočasným riešením situácie. Pri veľkosti databázy emailových schránok 135GB je pomerne náročné zabezpečiť zálohovanie korektne.

Aktuálny stav zálohovania predstavuje okrem spomínaného „stavu systému“ v intervale jedného týždňa aj variantu kopírovania zložky emailovej databázy na externý sieťový disk. Ako sa dá očakávať, taktiež s týždňovou periodicitou.

2.5 Integrácia do organizačnej štruktúry

Moderná spoločnosť predstavuje flexibilnú organizačnú štruktúru, ktorej tvar a hierarchia často nemá žiadne stále pravidlo. Tieto parametre splňuje aj spoločnosť GPO, ktorá pružne upravuje štruktúru v závislosti od aktuálnych projektov.



Obrázok 2.1 Organizačná štruktúra

2.5.1 Smernice a manuály

V rámci úvodnej analýzy prebehla i časť kontroly smerníc a manuálov. Bola zistená skutočnosť, že spoločnosť nedisponuje žiadnym dokumentom pripomínajúcim smernicu alebo interné pokyny pre zálohovanie ako také. Tento stav je pravdepodobne dôsledkom celkového výpadku zálohovania so systémovým prístupom.

Absencia smerníc predstavuje chýbajúci nástroj manažérov na kontrolu dodržiavania postupov a plnenia pracovnej zmluvy pracovníka IT. Z toho vyplýva, že nie je možné preniesť zodpovednosť za prípadné straty dát a nedostupnosť služieb na konkrétnu osobu tzv. zhmotnenie zodpovednosti zamestnancovi. Spoločnosť nesie riziko a zodpovednosť za stratu dát sama ako celok.

2.5.2 Krízové plány

Súčasťou dokumentácie systému zálohovania musia byť po správnosti aj krízové plány, ktorých dôležitosť a existenciu oceníme až vo chvíli ich použitia.

Ani v tomto smere spoločnosť GPO, spol. s r.o. nespĺňa základné požiadavky. Nemá vypracovaný žiadny krízový manuál, ktorý by určil presný postup pri vzniku havárie, alebo inom výpadku. Chýbajúci krízový plán často vedie k neúmernému predĺženiu doby obnovy po výpadku. Dokonca môže dôjsť i k nesprávnemu postupu obnovy s prípadným poškodením existujúcej zálohy. Celý nesprávny postup môže vyústiť do neschopnosti a nemožnosti obnoviť systém do požadovaného stavu, a čo viac, môže dôjsť ku komplexnej strate dát bez akéhokoľvek variantu ich obnovenia.

3 TEORETICKÉ VÝCHODISKÁ

3.1 Úvod do zálohovania a archivácie

Majoritným zámerom teórie je vysvetlenie základných pojmov, ktoré uľahčia pochopenie a prístup k časti samotného návrhu riešenia. Nakoľko sa jedná o pomerne odbornú tému, je nutné spomenúť hlavné body, o ktoré sa väčšina systémov zálohovania a archivácie opiera. Prínosný je pohľad na systém z uhlu ľudských a technologických zdrojov.

3.1.1 Záloha verzus fault tolerance

Fault tolerance (chybová tolerancia) je v obore všeobecný názov, ktorý opisuje systémy, aplikácie a konfigurácie, ktoré môžu prežiť chybu komponentov bez povšimnutia hodného (alebo akceptovateľnej degradácie) vplyvu na užívateľov. Rozličné systémy a prostredia poskytujú slušnú paletu stupňov chybovej tolerancie. Pre lepšiu predstavu uvedieme príklady:

- Hardvérová redundancia, zahrňujúca
  - RAID (redundantné polia pomerne lacných diskov). Cieľom je zachovanie chodu systému pri výpadku aspoň jedného a v závislosti od konfigurácie aj viacerých diskov súčasne.
  - Viacero sieťových kariet (NIC). Pokiaľ dôjde k výpadku sieťovej karty serveru, alebo k zlyhaniu prepínača, server dokáže zostať pripojený do siete v redukovanej forme.
  - Hot-swap disky, operačné pamäte, procesory, periférie. Novými komponentmi môžeme nahradiť zlyhané, a to bez vypnutia systému a obmedzovania užívateľov.
- Clustering
  - LAN[6] clustering, kde iný systém pokračuje v poskytovaní aplikačného/dátového prístupu i napriek výpadku prvého systému.

[6] Skratka významu Local Area Network, v preklade lokálna sieť.

- WAN7 clustering, kde pri výpadku primárneho systému preberá plynule jeho úlohu systém umiestnený v inej geografickej lokalite, pričom všetky služby ostávajú dostupné.

- Softvérový manažment zväzkov
  - Softvérovo vytvorený RAID, ktorý poskytuje väčšiu flexibilitu než hardvérový RAID, ale zvyčajne na úkor zníženia výkonu kvôli vyšším nárokov na zaťaženie procesora. To umožňuje firmám dosiahnuť určitú úroveň redundancie bez utrácania väčšieho obnosu peňazí na diskové úložiska.
- Replikácia dát/aplikácií
  - Pre systémy s malou šírkou pásma, alebo systémy ktoré nepodporujú aktívny clustering, replikácia dát/aplikácií umožňuje rýchlejšie obnovenie služieb v inej lokalite, pokiaľ dôjde k výpadku primárneho systému.
- Snapshots
  - Slovo významu snímka systému.
  - Používa sa u systémov vyžadujúcich minimálnu stratu dát a taktiež okamžitú alebo minimálnu dobu obnovy. Taktiež slúžia správcom ako body návratu v systéme, zvyčajne po inštalácii servisného balíčka alebo záplaty.

Pre dosiahnutie systému, ktorý bude dostupný takmer 100% času (dosiahnuť čistej hodnoty 100% je nemožné) je nutné skombinovať viacero spomínaných variant súčasne.

Zálohy svojou existenciou v žiadnom prípade nenahrádzajú chybovú toleranciu. Predstavujú nižší stupeň služieb, ktorý zahŕňa oblasti ako správne pracovné postupy, kontrolované prostredie.

Na strane druhej, chybová tolerancia nedokáže poskytnúť sľúbenú úroveň dostupnosti bez správneho systému záloh, ktorý ju chráni v prípade neočakávaného zlyhania. Fault tolerance a zálohovanie predstavujú synergické procesy pre korporátne prostredie. Z praxe však vieme, že často dochádza k mylnému poňatiu. To predstavuje

[7] Skratka významu Wide Area Network, v preklade Sieť veľkého rozsahu.

myšlienku, že v prípade nasadenia Fault tolerance (napríklad RAID 1) nie je potrebné vykonávať zálohy a mať komplexný systém záloh. Na strane druhej, každý skúsenejší pracovník IT vie, že nič sa nepokazí skôr, ako RAID1 – zrkadlenie. To iste platí pre clustering a softvérové pole. (2)

3.1.2 Riziko verzus náklady

Žiadna spoločnosť, bez ohľadu na veľkosť, finančnú silu alebo znalosti zamestnancov, nedokáže úplne eliminovať riziko z prostredia informačných technológií. V prípade vynaloženia všetkých prostriedkov spoločnosti na budovanie systému záloh, fault tolerance, vysokej dostupnosti, stále nie je možné garantovať na 100% fakt, že:

- Systémy nikdy nezlyhajú,
- dáta nebudú nikdy stratené,
- zálohy nebude nikdy potreba a ak áno, obnova bude rýchla a do požadovaného bodu.

Úroveň investícií a ochrany priamo súvisí s kritickosťou systému. Pochopiť riziko verzus náklady znamená nájsť odpovede na základné otázky:

- Riziko
  - technické : Čo je rizikom zlyhania systému?
  - komerčné: Aké je riziko pre biznis v prípade nechráneného zlyhania?
- Náklady
  - technické: Aké sú náklady v čase pádu systému?
  - komerčné: Aké sú náklady straty dát daného systému?
  - fiškálne: Aké sú náklady na dosiahnutie požadovanej úrovne ochrany, aby sa zabránilo tomuto scenáru.

Je potrebné ohodnotiť dva odlišné typy rizík – technické riziko zlyhania a taktiež komerčné riziko. Veľmi často je brané do úvahy iba jedno z týchto dvoch typov rizík. Napríklad, oddelenie IT pripustí, že existuje 5%-ná možnosť zlyhania systému, ale obchodné oddelenie nemá zmapované dopady na procesy vo firme, pokiaľ dôjde k výpadku. Rovnako je potrebné vymedziť aj typy rizík u nákladov.

Spomínaných päť otázok formuje jadro akéhokoľvek rozhodnutia ohľadne ochrany systému.

Najnižšiu pravdepodobnosť výskytu, ale zároveň i ochrany, má tzv. kaskádové zlyhanie, kde dôjde k postupnému zlyhávaniu viacerých úrovní ochrany.

Na druhej strane, najväčšie riziko straty a zneužitia dát predstavujú prenosné zariadenia, či už notebooky, handheldy alebo smartfóny. Tu okrem mizivých možností na zálohovanie, predstavuje najmarkantnejšie ohrozenie citlivých dát v prípade straty alebo krádeže zariadenia.

3.1.3 Mýty o zálohovaní

Zálohovanie, ako jedna z mnohých súčastí IT je „opradená“ rôznymi nepravdami a polopravdami, s ktorými sú najčastejšie konfrontovaní užívatelia bez odbornejších znalostí. Nepredpokladáme za bežné, aby sa v manažmente malej spoločnosti vyskytol i odborník na IT, preto je nutné vysvetliť niektoré fámy o zálohovaní, na základe ktorých by mohlo vedenie spoločnosti dôjsť k nekorektným rozhodnutiam.

Technológia pások (páskové mechaniky) je na ústupe a behom krátkej doby budeme zálohovať na lacné disky.

Táto nepravda je najčastejšie rozširovaná IT novinármi bez príslušných vedomostí, vzdelania a často ide o snahu pretlačiť na trh nový komerčný produkt.

Páskové mechaniky sú stále aktuálna technológia a nepredpokladá sa je zánik. Naopak, očakávame v rámci vývoja nových technológií pokles cien. Stále ide o kvalitnú offline ochranu dát. Pokiaľ dôjde k nahradeniu pások novou technológiou, firmy sa ešte minimálne dekádu budú stretávať so starými zálohami na pásku.

Komerčný zálohovací softvér nie je tak kvalitný a dôveryhodný ako vstavaný nástroj operačného systému.

Väčšina komerčných zálohovacích nástrojov je založená práve na využívaní systémových nástrojov OS[8]. Jediným rozdielom často býva grafické užívateľské

[8] Skratka významu operačný systém.

rozhranie, jednoduchosť ovládania a prídavné funkcionality, ktoré znižujú potrebnú úroveň znalostí o zálohovaní na minimum (wizard, kliknutia).

Zálohovanie je mrhanie peňazí

Ide o pomerne nebezpečný mýtus, ktorý zväčša pretrváva iba do doby prvého zlyhania systému alebo prvej vážnejšej straty dát. Každý navrhnutý systém predstavuje hrozbu plytvania finančných prostriedkov, pokiaľ nie je správne navrhnutý. Vytváranie nepoužiteľných záloh, alebo neznalosť postupu obnovy sú najvýraznejším príkladom.

Všetky uvedené nepravdy často spôsobia výrazné skreslenie predstáv o behu zálohovacieho systému a ešte častejšie odklon finančných prostriedkov pôvodne určených na vylepšenie systému zálohovania.

3.1.4 Ľudská vrstva

Iba skutočne málo ľudí vo firme rozumie, aká je ich pozícia vo vzťahu k zálohovaniu a obnove systému. Ak položíte bežnému zamestnancovi oddelenia informačných technológií otázku, aká je jeho úloha a zodpovednosť v procese zálohovania a obnovy, nenájdu uspokojujúcu odpoveď.

Je rozhodne užitočné posúdiť organizačnú štruktúru z hľadiska zálohovacieho systému a stanoviť úlohy a zodpovednosť zamestnancov na jednotlivých úrovniach firmy. Pri priereze firemnou štruktúrou narazíme na tri pre nás zaujímavé skupiny zamestnancov :

- Technický zamestnanci,
- manažment,
- koncoví užívatelia.

Technický zamestnanci

Prevažne ide o zamestnancov oddelenia IT, ktorý prichádzajú denne do styku so zálohovacím systémom. Základným bodom je, aby práve títo zamestnanci prijali zodpovednosť za zálohy, inak systém ako taký nebude fungovať.

Prvý, kto prichádza do styku s informáciou je vždy Help Desk. Jeho pracovníci prijímajú podnety od koncových užívateľov zväčša o nefunkčnosti systému alebo jeho časti. Na tomto úseku sú zamestnanci zodpovedný za diagnózu zvyčajných problémov v procese automatickej obnovy. Ďalej musia mať základný prehľad o procese

zálohovania (najmä klientskych staníc) a taktiež vedieť rozhodnúť čo je a čo nie je možné obnoviť. V zložitejších prípadoch predávajú prípad ďalej na administrátora.

Väčšie spoločnosti vzhľadom k množstvu úloh rozdeľujú administrátorské funkcie na dve časti, a to administrátor zálohovania a systémový administrátor.

Administrátor zálohovania nesie v tomto prípade hlavnú zodpovednosť za chod a nastavenie systému záloh. Základnými bodmi jeho práce sú:

- Riešenie dotazov z help desku,
- diagnostika a riešenie problémov zálohovania,
- vysvetlenie potrebných krokov a nákladov manažmentu spoločnosti,
- školenie jeho asistentov,
- správa a sledovanie denných záloh a ich log-ov,
- správa úložného priestoru záloh, jeho monitorovanie a rozširovanie,
- vypracovávanie plánov rozšírenia systému a ich predloženie vedeniu spoločnosti,
- vytváranie dokumentácie zálohovacieho systému,
- vykonávanie testov záloh a obnovy,
- vykonávanie aktualizácii systému záloh,
- predkladanie a vysvetlenie výstupov (reportov) zo systému manažmentu.

Pokiaľ spoločnosť nevyužíva delenie administrátorských funkcií, potom všetky spomínané úlohy má v náplni systémový administrátor.

Systémový administrátor vo väčších firmách predstavuje skupinu administrátorov, kde každý má svoje špecifické zameranie. Pre nás je však dôležitejšie zamerať sa na systémového administrátora ako na jedinú osobu v prostredí menšej spoločnosti. Náplňou jeho práce je :

- Vykonávanie záloh systému podľa dokumentácie,
- vykonávanie obnovy operačného systému podľa dokumentácie,
- vykonávanie obnovy aplikácií/dát pomocou dokumentácie,
- podávanie reportov manažmentu spoločnosti o stave problému a jeho riešení.

Dokumentácia je základnou a neoddeliteľnou časťou systému zálohovania. Najmä v kritických momentoch – pri zlyhaní systému, je potreba okamžitej správnej reakcie. Akýkoľvek dopredu nepripravený postup bez predošlého overenia často vedie k neúspechu.

Manažment

Napriek mnohým otáznikom v oblasti zodpovednosti manažmentu firmy za chod systému záloh a obnovy, je nutné priznať a určiť jednotlivým predstaviteľom ich role v spomínanom systéme. Fungujúci systém zálohovania môže pracovať správne iba v prípade, ak obe sféry – manažment i IT plnia ich role synergicky.

Najčastejšie sa stretávame v praxi s modelom, kde manažment spoločnosti nenesie žiadnu zodpovednosť za systém záloh a obnovy. Tento model samozrejme nie je správny z hľadiska miery viny pri zlyhaní. Manažér by mal niesť rolu „kontrolóra“, kde na základe postupov a metrík stanovených v dokumentácií je schopný vykonať kontrolu behu systému zálohovania a pripravenosť na možné výpadky. Taktiež pomocou reportov od systémového administrátora vidí, čo sa deje a zapája sa aj pasívne do prípadnej obnovy systému, kde jeho pôsobnosť spočíva v dohľade na dodržaní postupov a času stanoveného na obnovu.

Obnovy za asistencie manažmentu firmy je možné rozdeliť na dve formy:

- „pokojné“ obnovy
  - nastávajú, ak v prípade nutnej obnovy po zlyhaní dochádza ku konzistentnému toku komunikácie na všetkých úrovniach, čo každému umožní pracovať na jeho úlohe podľa dokumentácie. Tento proces vyžaduje vzájomnú dôveru medzi zamestnancami IT, užívateľmi a manažmentom.
- „úlomkovité“ obnovy
  - sú obnovy, kde zamestnanci vykonávajúci proces obnovy sú často rušený z dôvodu udania postupu pri práci alebo sú zanesený do nepríjemne rozhorčených konverzácií s užívateľmi alebo manažmentom. To vytvára veľmi rušivé a stresujúce prostredie, v ktorom rapídne rastie pravdepodobnosť chyby pri obnove.

Úlohou manažéra je na základe správy po obnove od administrátora vyvodiť príslušné opatrenia/dôsledky, ktoré zabránia opakovaniu.

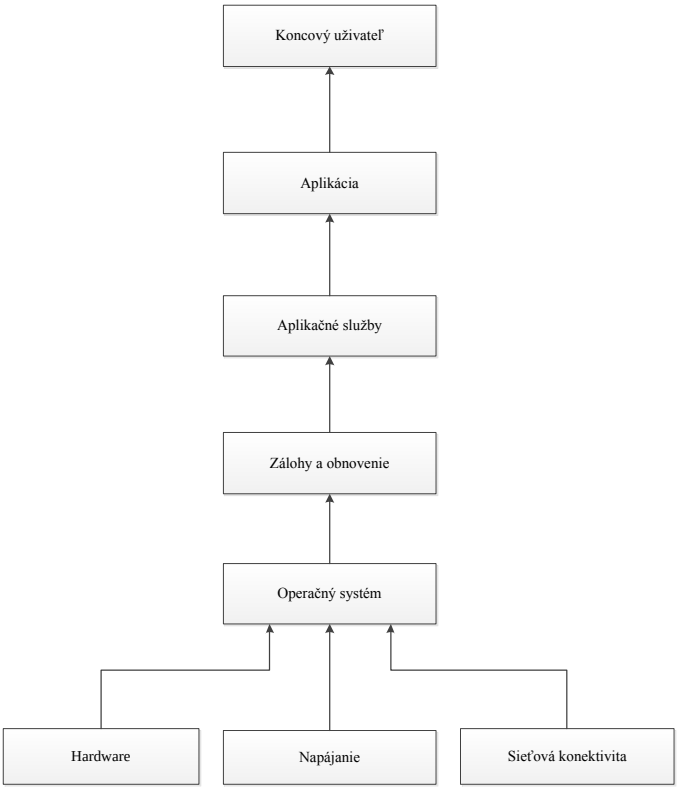
Koncoví užívatelia

Aj keď sa na prvý pohľad môže zdať, že v procese zálohovania a obnovy nemajú užívatelia svoju rolu, opak je pravdou. Ich úlohy sú síce malé, ale práve vďaka nim je možné urýchliť najmä proces obnovy. Úlohou číslo jedna je informovať helpdesk o vzniknutom probléme a jasne, zrozumiteľne ho vysvetliť. Ďalšou úlohou je pochopiť, že systém zálohovania nie je archív.

3.1.5 Technická vrstva

Ďalším krokom preniknutia do systému zálohovania po poznaní personálneho aspektu je spôsob, akým systémy ochrany spolupracujú s ostatnými prvkami v oblasti IT.

Obrázok 3.1 znázorňuje štruktúru závislosti, kde koncový užívateľ predstavuje vrchol celého procesu. Podstatou pre schopnosť užívateľa pracovať, je funkčná aplikácia. Taktiež pre správnu funkciu aplikácie musí bežať aplikačná služba v požadovanej kvalite. V týchto závislostiach strom pokračuje až na najnižšiu úroveň. Pri výpadku jednej služby dôjde k nefunkčnosti celého stromu.



Obrázok 3.1 Vrstvy služieb

3.2 Koncepty zálohovania a obnovy

Zálohovanie a zálohovací softvér môžeme zaradiť do rady skupín. Zálohovací softvér obsahuje mnoho štandardných i nadštandardných funkcionalít. Práve ich prítomnosť (či absencia) má výrazný vplyv na využitie produktu firmou. Dôležité je podotknúť, že nie všetky funkcie poskytované programom zálohovania sú pre firmu potrebné, a preto nie je vhodnou metódou výberu softvéru strohé porovnávanie funkcionalít na základe produktových listov. Základný balík funkcionalít, ako napríklad adekvátna ochrana zálohovacieho servera samotného, môžeme nájsť v každom vyspelejšom softvéri na zálohovanie a obnovu. Taktiež je dobré mať na pamäti, že softvér označovaný ako najlepší/najpoužívanejší nemusí byť ideálny pre nasadenie do nami požadovaného prostredia. Dôležitým krokom k poznaniu a výberu softvéru je:

- Zodpovedať otázky vyššie položené.
- Preniknúť skrz „príťažlivé“ užívateľské rozhranie až na úroveň základných funkcionalít.

- Zamerať sa predovšetkým na funkcionality pre nás potrebné, neprikladať význam „bonusovým“ funkciám, ktoré nie sú v našom prostredí použiteľné.

Základné názvoslovie

V rámci diskusie o zálohovaní, je žiaduce rozkľúčovať základné výrazy a pojmy.

Server : Zálohovací server alebo „master“ server, ktorý je zodpovedný za plánovanie záloh, konfiguráciu, manažment úložiska, indexovanie záloh a iné.

Klient : Akýkoľvek „hostiteľ“ (host), ktorý je chránený serverom (zálohovacím). Zvyčajne to zahrňuje mnoho, ak nie všetky, stroje, ktoré za normálnych okolností nazývame serverom – súborový server, emailový server, doménový server. Tie sú v terminológií zálohovania a obnovy chápané ako host-y.

Média server – úložisko: Stroj, ktorý je umiestnený v štruktúre medzi klientom a serverom. Ukladá zálohy, ktoré inicializuje server.

3.2.1 Topológia zálohovania

V procese rozhodovania o použití tej ktorej zálohovacej topológie máme k dispozícií dva typy, a to centralizovanú a decentralizovanú. Vo všeobecnosti centralizovaná topológia je predurčená na použitie v prostredí pevných pracovných skupín alebo na podnikovej úrovni, pričom decentralizovaná topológia je odporúčaná pre domáce alebo SOHO[9] riešenia.

Decentralizované zálohovanie

Decentralizované prostredie predstavuje zálohovanie každého host-a na zálohovacie zariadenia (zvyčajne pásky), ktoré má priamo pripojené. Pokiaľ je host zahrnutý v komerčnom prostredí, potom zvyčajne každý host je zároveň i master server, ktorý je separovaný od zvyšku zálohovacieho prostredia. Tento model zálohovania nájdeme v malých až stredných firmách, ktoré „vyrástli“ z jedného až dvoch serverov na pomerne objemné rozmery 20 – 30 serverov. V tomto prostredí je zálohovanie často chápané ako úkon po nákupe, čo vedie k potrebe samostatného úložiska pripojeného separátne k novému serveru.

Príkladom decentralizovanej topológie zálohovania je Obrázok 3.2. V praxi, decentralizované zálohy nie sú správnym rozhodnutím pre väčšinu firiem, keďže

[9] Skratka významu Small Office Home Office, v preklade prostredie malej alebo domácej kancelárie.

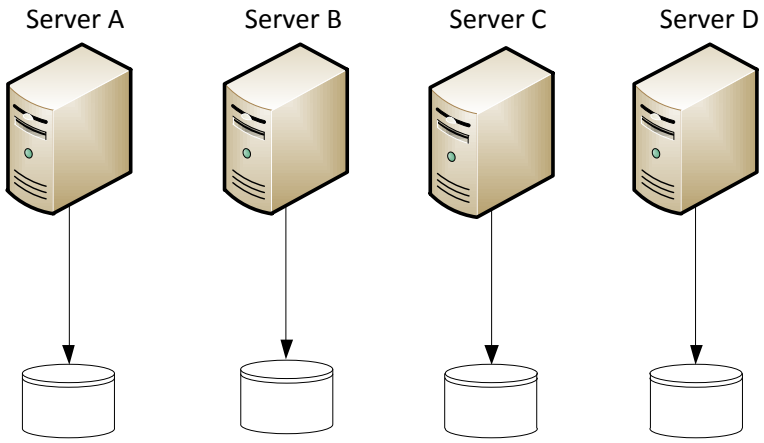
spôsobujú vyššie zaťaženie administrátora a môžu viesť ku strate dát vzhľadom k vyššej potrebe manuálnych zásahov pri konfigurácii a správe systému. Taktiež spôsobujú znateľný nárast objemu a potreby zálohovacích médií.

Kľúčové vlastnosti v podobe výhod sú:

- Každý individuálny host môže mať jednoduchšiu konfiguráciu,
- Nevznikajú závislosti medzi host-mi, výpadok lokálneho úložiska ohrozí iba konkrétny server (host).

Nevýhody:

- Potreba zálohovacieho média pre každý host navršuje cenu riešenia, čo vedie ku obstaraniu lacných nekvalitných zariadení, aby udržali náklady na nízkej úrovni.
- Zvyšujúce sa nároky na osobu operátora/administrátora s nárastom počtu host-ov a objemu dát, taktiež vplyv na rýchlosť obnovy.
- I napriek tomu, že konfigurácia jednotlivých host-ov vyzerá jednoduchá, ich komplexná správa je omnoho zložitejšia.
- Chýba centralizovaná funkcionalita reportov a správ.
- Chýba centralizovaný manažment a konfigurácia.
- Pri použití komerčného zálohovacieho riešenia je cena za jednotlivý host vyššia než pri kúpe multi-licenčného balíčka.
- Najväčším rizikom je postup v čase a používanie rôznych komerčných nástrojov (nie jednotných).



Obrázok 3.2 Topológia decentralizovaného zálohovania

Centralizované zálohovanie

V prostredí centralizovaného zálohovania, viaceré host-y sú zálohované pomocou centrálneho „master“ servera, alebo master servera a slave servera.

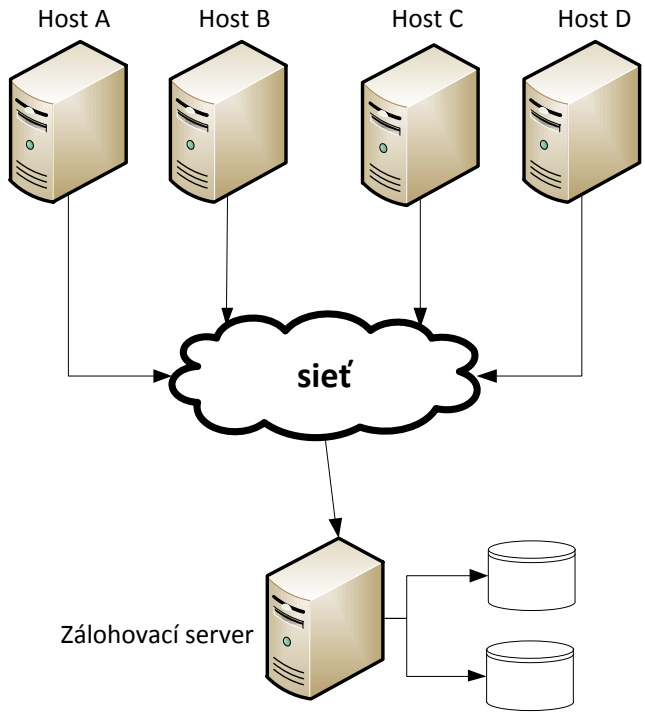
Jednoduché prostredie centralizovaného zálohovania zobrazené na Obrázok 3.3 predstavuje stav, kde je jediný server s pripojeným úložiskom zodpovedný za zálohy. Všetky ostatné host-y poskytujú dáta zálohovaciemu serveru, ktorý je zodpovedný za ich zápis a obnovu z úložného média. Jedná sa o pomerne jednoduchý princíp, pričom zložitejšie systémy s požiadavkou na zvýšenú bezpečnosť a dostupnosť využívajú dva a viac zálohovacích serverov, ktoré sa vzájomne replikujú.

Rovnako, ako pri decentralizovanom zálohovaní, aj centralizované má svoje svetlé a tmavé stránky ako napríklad výhody:

- Za pomoci centralizácie úložiská môžu byť efektívnejšie využívané, čo znižuje potrebu zásahu operátora/administrátora, urýchľuje proces obnovy dát a znižuje náklady na hardvér.
- Celková konfigurácia zálohovacieho prostredia sa stáva jednoduchšia a prehľadnejšia.
- Ochrana zálohovacieho prostredia samotného sa taktiež stáva jednoduchšia, pretože postačuje ochrániť jeden server zálohovania a menší počet úložísk zabezpečiť proti výpadku elektrického prúdu.
- Reporty, alerty, analýza nárastu objemu dát, výstrahy a iné notifikačné a reportovacie funkcionality.
- Náklady na licencie sa znižujú v porovnaní s decentralizovaným prístupom.

Nevýhody:

- Pri výpadku serveru zálohovania dôjde v podstate k výpadku celého systému záloh a obnovy. Opatrením je existencia redundantného serveru zálohovania, ktorý pri výpadku primáru automaticky preberá jeho úlohu.
- Implementácia systému centralizovaného zálohovania vyžaduje vyššie počiatočné investície ako aj viac času na prípravu a systémový prístup.



Obrázok 3.3 Topológia centralizovaného zálohovania

Pre zhrnutie zopakujme, že centralizované zálohovacie prostredie je najvhodnejšou štruktúrou pre firemné prostredie i napriek nižším nákladom decentralizovaného systému pri implementácii. Investované prostriedky sú omnoho efektívnejšie využívané hlavne pri pridávaní nových zariadení do systému centralizovaného zálohovania.

3.2.2 Úrovne zálohovania

V závislosti od použitého softvérového produktu, môžu byť podporované viaceré úrovne zálohovania. Úroveň zálohovania predstavuje objem dát alebo počet súborov, ktorý je zálohovaný ako časť konkrétnej operácie.

Je dobré poznamenať, že napriek štandardne existujúcim a používaným pomenovaniam jednotlivých úrovní aplikujú niektoré softvérové spoločnosti vlastné štandardy pomenovávania.

Plná úroveň (full level)

Plná záloha je jednoduchou zálohou „všetkého“, čo daný host obsahuje. Je možné vylúčiť súbory zo zálohy na základe ich definovania pri vytváraní úloh. Plná záloha transferuje všetky data z host-a na zálohovacie médium. Zároveň poskytuje

najjednoduchší variant obnovy pre prostredie firmy, pretože záloha obsahuje jediný kompaktný súbor, bez nutnosti dohrávania bodu v čase.

Zatiaľ čo takmer všetky spoločnosti používajú plnú zálohu ako časť ich zálohovacieho plánu, tie sú aplikovateľné na dennej báze iba pre spoločnosti, kde platí nasledujúce:

- Nie je vyžadovaná 24/7 dostupnosť.
- Úplná záloha pojme minimum miesta na médiu.
- Administrátor zálohovania/systému nemusí byť denne k dispozícii, a preto primárnym cieľom je minimalizovať objem média pre úspešnú obnovu.

Samozrejme, kľúčovou podmienkou pre plnú zálohu je, aby časové okno bolo dostatočné veľké pre načítanie všetkých systémových dát každú noc. Typicky je táto konfigurácia bežne akceptovaná v podmienkach malých firiem s menším počtom host-ov. S nárastom objemu dát a počtu host-ov sa plné zálohy vykonávajú v rámci jedného týždňa. Výhodami plných záloh je:

- Obnova z plnej zálohy zahrňuje konsolidované načítanie dát z jedného úložiska.
- Medzi jednotlivými plnými zálohami v čase neexistujú prepojenia, tzn. strata jednodennej zálohy neovplyvní obnovenie dát zo staršej zálohy (predošlý deň).

Nevýhodami zasa:

- Najviac využíva dostupné miesto na úložisku, preto je najnákladnejšia.
- Plné zálohy trvajú značne viac, než zálohy ostatných úrovní.
- Bez správneho postupu a minimalizácie objemu systémových dát host-a sa neúmerne zvyšuje objem zálohovaných dát, ktorý sa zvyčajne presúva po sieti.

Inkrementálna úroveň (incremental level)

Inkrementálna záloha sa zameriava na súbory a položky, ktoré sa zmenili od poslednej zálohy. Výsledkom je značne menší objem zálohovaných dát a skrátenie času potrebného na vykonanie zálohy.

Pre mnoho zálohovacích produktov zameraných na skupinu domácich užívateľov a SOHO, umožňuje vykonávať inkrementálne zálohy iba nad súbormi operačného systému a nie napríklad nad databázami. Komerčné riešenia odstraňujú toto obmedzenie. Najmä v korporátnom prostredí dochádza k výraznému zníženiu objemov dátových prenosov. Napríklad databáza SQL o veľkosti 2TB zaznamená počas dňa zmenu iba na 5% dát. Za použitia plnej zálohy by sa vytvoril obraz databázy o veľkosti 2TB, pričom použitím inkrementálnej zálohy sa prenesú iba zmenené súbory, čo je 102,4 GB.

Pre väčšinu firiem, inkrementálna úroveň záloh predstavuje dennú rutinu, pričom plná záloha sa vykonáva raz za týždeň. To umožňuje vytvoriť časový plán záloh, aby server mal dostatok času vykonať zálohy všetkých host-ov. Tabuľka 3.1 ukazuje ako môže vyzerať jednoduchý plán zálohovania.

Tabuľka 3.1 Príklad časového harmonogramu zálohovania

Pondelok	Utorok	Streda	Štvrtok	Piatok	Sobota	Nedeľa
Inkrement.	Inkrement.	Inkrement.	Inkrement.	Plná	Inkrement.	Inkrement.
23:00	23:00	23:00	23:00	21:00	23:00	23:00

Prevláda názor, že inkrementálne zálohy nie sú potrebné cez víkend, kedy nik nepracuje. Ide však o mylný názor, nakoľko sa dnes bežne vyskytujú mimoriadne zmeny a potreby práce nadčas a cez víkend. Preto platí základné pravidlo, že vždy je lepšie zálohovať trochu viac než o niečo menej!

Hoci inkrementálna úroveň záloh predstavuje variantu zmenšenia objemu prenášaných dát a časového okna potrebného k zálohe, vyžaduje taktiež viac námahy a času pri nasadení do komplexného systému zálohovania a obnovy. Preto je na mieste opatrnosť pri implementovaní tejto úrovne a hlavnú úlohu hrajú správne nastavenia úrovne plného zálohovania, ktorá by mala byť v čo možno najkratšom intervale. Ku príkladu nastavenie plného zálohovania na dobu 30 dní a inkrementálnej zálohy na dennej báze nie je práve najrýchlejšie z hľadiska obnovy dát, pretože inkrementálne zálohy by sa museli obnovovať deň po dni. Nespornými výhodami inkrementálnej úrovne zálohovania je:

- Nízke zaťaženie siete vzhľadom k menšiemu toku dát.

- Interval medzi jednotlivými zálohami môže byť nastavený na pomerne krátky čas.
- Pri použití s databázovými systémami je inkrementálna záloha najrýchlejším a lacnejším riešením.

Nevýhody inkrementálne úrovne

- Obnovy systému, kde intervaly medzi plnými zálohami predstavujú veľké časové okno sú zložité.
- Platí postup obnovy, kde prvým krokom je použitie plnej zálohy a následne sa nahrávajú inkrementálne zálohy.

Diferenčná úroveň (differential level)

Diferenčná záloha zachytáva všetky zmeny, pokrývajúce často aj obdobie niekoľkých dní od poslednej plnej zálohy. Poznáme dva základné typy – jednoduchú diferenčnú zálohu a viac úrovňovú diferenčnú zálohu. Zatiaľ čo podpora diferenčnej zálohy na súboroch operačného systému je vynikajúca, s databázami je to o poznanie horšie. Napríklad rozdielom medzi inkrementálnou a diferenčnou zálohou databázy je často spôsob nakladania s transakčnými protokolmi (transactional logs), kde jedna metóda ich ponecháva a druhá vymazáva.

Diferenčná úroveň oproti inkrementálnej predstavuje výhodu hlavne pri obnove dát, pričom silne závisí na korektnej konfigurácii systému zálohovania a obnovy. Ideálne je vysvetliť si princíp na mesačnej časovej schéme zálohovania za použitia kombinácie všetkých spomínaných úrovní. Vzhľadom k časovej a dátovej náročnosti je vhodné používať plnú zálohu čo najmenej. Bežne používaným modelom je vykonanie plnej zálohy na začiatku mesiaca, počas pracovného týždňa denne vykonávať inkrementálne zálohy a každú nedeľu spustiť diferenčnú zálohu. Týmto sa vyhneme zdĺhavému procesu obnovy dát pomocou inkrementálnej úrovne, kde sa vždy použije posledná diferenčná záloha a na ňu sa budú nabaľovať inkrementálne zálohy.

Konsolidovaná úroveň (consolidated level)

Malá časť komerčných zálohovacích nástrojov ponúka funkcionalitu konsolidovaných záloh, známych tiež pod pojmom „umelé plné zálohy“, ktoré majú pomerne špecifické využitie.

Konsolidované zálohy používajú nasledujúcu stratégiu:

1. Vykoná sa plná záloha pri zavedení systému alebo počas veľmi zriedkavej odstávky systému.
2. Po stanovenú dobu sa vykonávajú inkrementálne/diferenčné zálohy.
3. Po ubehnutí stanovenej doby je spustená konsolidovaná záloha, kde predošle vytvorená plná záloha a inkrementálne/diferenčné zálohy sa zlúčia a dôjde tak k vytvoreniu „syntetickej“ plnej zálohy.

Výhodou úrovne je odbúranie potreby častej plnej zálohy. Nevýhodou naopak slabá podpora v súčasných OS.

3.2.3 Dostupnosť dát

Dostupnosť dát užívateľovi je ovplyvnená typom vykonanej zálohy. U firiem má požadovaná úroveň dostupnosti dát silný vplyv na voľbu metód zálohovania.

Offline

Offline záloha nazývaná aj studená záloha je stav, kedy je zálohovaný host nedostupný užívateľom počas celej doby trvania procesu zálohovania. Samozrejmým efektom je výpadok aplikácií, ktorý trvá až do ukončenia zálohovania. V dnešnej dobe to predstavuje marginálnu nevýhodu, ktorú väčšina firiem nie je ochotná a schopná akceptovať ako daň za nižšie náklady na zálohovací systém. Je vhodné poznamenať, že offline zálohy môžu spôsobiť problémy aplikáciám bežiacim na zálohovanom host-e. Týka sa to prevažne databázových aplikácií, kde sa do vyrovnávacej pamäte zariadenia ukladajú často používané dáta, čím sa znižuje doba odozvy systému. Táto pamäť je po offline zálohe (vypnutím alebo reštartom servera) vyprázdnená a chod aplikácie sa tým z hľadiska užívateľa spomalí do doby opätovného naplnenia vyrovnávacej pamäti. Výhodami offline zálohovania je:

- Triviálny postup obnovenia systému.

Prevažujú však nevýhody:

- Nedostupnosť systému a aplikácií počas celej doby zálohovania.
- Vyprázdnenie vyrovnávacej pamäti servera.
- Metóda je použiteľná iba u menších dátových objemoch.

Online

Online záloha je stav, kedy host zostáva kompletne dostupný počas celého procesu zálohovania. Samozrejme sa online záloha prejaví na zaťažení zálohovaného zariadenia. V praxi to znamená, že server bude dostupný, avšak jeho odozvy budú pomalšie. Veľkosť vplyvu na výkon systému záleží od konfigurácie systému, dostupnom mieste, počtu aplikácií bežiacich na pozadí a počtu požiadaviek na server od užívateľov.

U databázy je pokles výkonu spôsobený vytváraním väčšieho počtu transakčných protokolov. Bežná záloha operačného systému je vykonávaná s ohľadom na možné riziko, ktoré predstavujú zmeny systému počas zálohovania. Najpoužívanejší

operačný systém Windows využívajúci súborový systém NTFS umožňuje zabrániť prepisu pri zálohe dá,t a to formou uzamknutia používaných súborov, kde na dobu ukončenia práce so súborom je znemožnený zápis zmien. Na druhej strane sú systémy založené na jadre UNIX a Linux, ktoré neumožňujú rezervované uzamykanie súborov.

Nakoľko dnes bežne vyžadovaným štandardom vo firemnom prostredí je dostupnosť systému 24/7, online zálohy predstavujú jediný akceptovateľný variant zálohovania systému. Hlásenia systému typu „Systém je aktuálne nedostupný“ znamenajú pre zákazníka nepriamy výraz pre „Naše metódy sú zastarané a nespoľahlivé, prejdite prosím ku konkurencii.“. Určite to nie je cieľom žiadnej modernej firmy, a práve preto offline spôsob zálohovania sa dnes využíva skutočne iba okrajovo.

Aj online zálohovanie má svoje nevýhody, konkrétne:

- Zložitejšie na konfiguráciu a správu (otázne).
- Potreba skúseného užívateľa pri online zálohovaní databáz.

Výhody:

- Zálohovanie prebieha bez výpadku služieb.
- Vyrovnávacia pamäť databázových systémov nie je ovplyvnená.
- Zvyšuje percento dostupnosti systémov.

Zálohovanie pomocou snímok systému (snapshots)

Snapshot je záloha typu „bod v čase“, ktorá umožňuje okamžitú obnovu systému do určeného bodu inicializácie zálohy. Rozdiel medzi snímkou systému a bežnou zálohou je, že snímka poskytuje rovnakú zálohu v čase pre všetky súbory, bez ohľadu na čas, kedy bola záloha vykonaná. Bežná metóda zálohovania (online) uchováva systémové súbory v rôznom čase, v závislosti na postupe zálohy systémom. Snapshot sa typicky využíva v prostredí, kde je vysoká potreba okamžitej obnovy systémov bez znateľného alebo s minimálnym výpadkom.

Snapshots je možné deliť na 2 skupiny – offline (cold) a online(hot). Princíp je rovnaký ako u bežných online/offline záloh. Rozdielom je však doba trvania u offline bežných záloh a snímok. Pri offline snímku sa pohybuje rádovo v rozmedzí sekúnd než minút. Typickým je príklad dátových centier po celom svete, kde pri nastavení klasickej

online zálohy na konkrétny deň a čas môže vplyvom časového posunu dôjsť k obmedzeniu užívateľov iného časového pásma.

Druhým spôsobom využitia snímok systému a v podstate ich primárny vznik spolu s virtuálnymi systémami je zameraný na správu systémov. Pred každým závažnejším zásahom do systému, napríklad inštalácia servisného balíčku, sa vytvorí snapshot, ktorý je použiteľný pre prípad problémov po inštalácií. Ide o tzv. náhradu „bodu obnovenia systému“ v rámci virtuálneho variantu. Výhody zálohovania pomocou snímok systému (snapshot):

- Rýchlejšia obnova systémov.
- Rýchlejší proces tvorby snímku.
- Možnosť okamžitej migrácie na iné hostiteľské zariadenie.

Nevýhody

- Zvyčajne vyžaduje prídavné diskové pole alebo zväčšenie kapacity.
- Musí byť dodržaná rovnaká výkonnosť diskového poľa.
- Zvýšenie zaťaženia hostiteľského servera – vedie k zníženiu výkonu všetkých virtuálnych jednotiek hostiteľa.
- Zložitá správa snímok naprieč viacerými hostiteľmi.

3.2.4 Stratégia uchovávania záloh

Spôsob, akým zálohovací nástroj spravuje uchovávanie záloh, priamo ovplyvňuje funkcionalitu záloh a dobu ich použitia. Ako bolo spomínané, účelom záloh je umožniť obnovu dát v čase potreby. Stratégia uchovávania záloh má priamy dopad na kvalitu zálohovacieho nástroja. Rozoznávame dva typy stratégií uchovávania – jednoduchý model a model na základe závislosti.

Uchovávanie záloh na základe závislosti

Na základe použitia tohto modelu, sú medzi jednotlivými zálohami vytvárané väzby. To nám zaručuje obnoviteľnosť zálohovaných dát. Uvedieme jednoduchý príklad. Podľa skôr spomínaných pravidiel je zálohovanie nastavené podľa Tabuľka 3.1. Závislosti vytvorené na základe zvoleného modelu uchovávania záloh spájajú do reťazca poslednú plnú zálohu s nadväzujúcimi inkrementálnymi zálohami. K prerušeniu

reťazca dochádza v bode novej plnej zálohy. Práve bod prerušenia je u tohto modelu najdôležitejším faktom.

V prípade zlyhania inkrementálnej alebo plnej zálohy ju systém nezapočítava do doby uchovania zálohy nastavenej administrátorom.

Výhody použitého modelu:

- Zálohy, ktoré sú v rámci doby uchovania odstránené iba v prípade ak neexistuje priama závislosť, ktorá by spôsobila nemožnosť obnovenia.
- Je garantovaná korektná celková obnova systému v rámci stanovenej doby uchovania.

Nevýhody

- Môže mať vyššie nároky na veľkosť úložiska.

Jednoduchý model uchovávania záloh

Jedná sa o najrozšírenejší model kontroly uchovávania záloh bežnými komerčnými zálohovacími produktmi. V tomto prípade je doba uschovania záloh presne nastavená a nezaručuje možnosť korektnej obnovy. Najlepšou metódou ukážky je uviesť príklad. Administrátor nastavil v systéme zálohovania jednoduchý model uchovávania dát na dobu 42 dní. Výsledkom je, že všetky zálohy, bez ohľadu na obnoviteľnosť a úroveň, staršie ako 42 dní budú vymazané. Samozrejme absolútne nie je zaručená obnoviteľnosť systému, keďže môže dôjsť k stavu, kde plná záloha za posledných 50 dní nebola úspešná, ale systém ju i napriek tomu spolu s inkrementálnymi zálohami vymaže. Zálohy sú potom nepoužiteľné. Situáciu graficky popisuje Tabuľka 3.2. Výhody jednoduchého modelu:

- Bez akýchkoľvek výhod.

Nevýhody:

- Bez garancie možnosti obnovy zo záloh.

Tabuľka 3.2 Jednoduchý model uchovávania záloh

42	41	40	39	38	37	36	35	34	33	32	32	30	29	28
I	I	I	I	F !	I	I	I	I	I	I	F !	I	I	I

I= Inkrementálna záloha, F!= Plná záloha - neúspešná

3.2.5 Záloha databázy

Zálohy zahŕňajú viac než iba ochranu súborového systému. Pre mnoho firiem je najkritickejším systémom práve databáza, ktorá vyžaduje vyššiu pozornosť než záloha súborového systému. Vzhľadom k citlivosti databáz na zálohovanie a potreby absolútne správnej konfigurácie. Základné kroky popíšeme v tejto sekcii.

Najrozšírenejším modelom zálohovania databáz je práve plná záloha. Tá však svojou dátovou náročnosťou nie je vykonateľná v denných cykloch a nepokrýva všetky možnosti a nutnosti databázy. Komplexný systém zálohovania databázy pokrýva tri kroky:

- Nastavenie plnej zálohy.
- Nastavenie diferenčnej zálohy.
- Nastavenie zálohy transakčného protokolu.

Jediným krokom, ktorý sme zatiaľ neanalyzovali je záloha transakčného logu. Databázy pri zmene dát vytvárajú transakčné protokoly, kde ja zaznamenaná zmena s uvedením dátumu, času a typu zmeny. Nevýhodou transakčných záznamov je ich objem pri väčších databázových systémoch. Často sa integruje systém, kde transakčné protokoly sú ukladané na záznamové médium/pevný disk mimo systémového disku. Výrazne sa tým urýchľuje indexovanie databázy a celková odozva. Zálohovanie transakčných log-ov zároveň rieši otázku narastania objemu databázy ich vplyvom. Po vykonaní zálohy sa transakčné protokoly vymažú.

Z hľadiska časového harmonogramu záloh databázy platí nastavenie spomínané v kapitole 3.2.2, kde sa plná záloha vykonáva raz týždenne, nasledujú denné diferenčné zálohy. Keďže u databázových systémov dochádza veľmi často k zmenám na dátach (zápis, editácia, mazanie), kľúčovým prvkom je nastavenie hodinovej zálohy transakčných protokolov. Tým je umožnená obnova do bodu poslednej celej hodiny, pričom vzniká strata dát maximálne v rozmedzí 59 minút. Samozrejme väčšie spoločnosti neakceptujú ani túto minimálnu stratu. U nich sa to rieši formou zrkadlenia databázy, kde pri výpadku hlavnej databázy automaticky preberá funkciu záložná databáza umiestnená na inom serveri.

3.2.6 Bezpečnosť a ochrana

Rovnako, ako je nevyhnutné sa presvedčiť, že neexistuje nezálohovaný a nezabezpečený host, je nutné sa presvedčiť aj o zaistení ochrany samotného zálohovacieho servera.

Ochrana záloh

Dôležitým článkom v reťazci zálohovania je ochrana záloh samotných. Komerčný *zálohovací softvér* často obsahuje vstavané nástroje typu klonovanie alebo duplikácia, ktoré zabezpečujú ukladanie záloh okrem primárneho zálohovacieho servera aj na iné vybrané úložisko, zvyčajne umiestnené mimo priestory serverov.

Z hardvérového hľadiska existujú rôzne riešenia pre ochranu pásiek a pevných diskov. Najpoužívanejším je už spomínané diskové pole RAID, režim 5, 6 alebo 10. Rovnaká technológia je použiteľná i pre páskové jednotky.

Nesmieme zabúdať na *fyzickú ochranu záloh*. To znamená, že všetky zariadenia a úložiská musia byť umiestnené v zabezpečenom uzamykateľnom priestore chráneným pred možnými vplyvmi vandalizmu a prírodných živlov.

Zabezpečenie zálohovacieho servera

Server, ako jediný prvok riadiaci zálohy, má obrovskú a jedinečnú úlohu, ktorá v prípade výpadku serveru nebude nahradená. Preto je nutné dbať na zvýšené zabezpečenie zálohovacieho serveru.

Hardvérové hrozby v podobe výpadku komponentov servera sú často riešené za behu vymeniteľnými časťami, ktoré neovplyvnia chod servera (hot plug). Extra pozornosť sa zameriava na ochranu úložiska, ktoré ako bolo spomínané zväčša využíva diskové/páskové pole RAID/RAIT. Okrem tejto ochrany je u citlivých dát používané zrkadlenie alebo už opomínaný clustering.

Softvérové hrozby ako napadnutie útočníkom, vírusy a pod. musia byť odbúrané inštaláciou kvalitného firewall-u a na zváženie je i používanie antivírusového enterprise riešenia.

F*yzická ochrana* je zabezpečovaná rovnako ako u ochrany záloh. Táto úroveň ochrany sa implementuje ako celok pre všetky zariadenia nachádzajúce sa v chránenej

oblasti. Prvkami sú protipožiarna, proti živelná ochrana, tepelná regulácia a odvetrávanie.

Samostatnou kapitolou vzťahujúcou sa na všetky zariadenia vyžadujúce elektrickú energiu je zabezpečenie proti jej výpadku. Riešením je inštalácia neprerušiteľného zdroja napájania UPS o potrebnej sile.

3.3 Zálohovanie serverov

Typicky, zálohovacie operácie vykonávané na firemných serveroch, sú kľúčovým komponentom korporátnych zálohovacích systémov. Zároveň sú to základné stavebné prvky IT zázemia spoločnosti a jedna z hlavných úloh jeho zamestnancov.

Pri procese výberu vhodného riešenia zálohovania serverov je potrebné zodpovedať všetky nasledujúce otázky a vymedziť si tak hlavné funkcionality, ktoré budú požadované.

- Aké sú role servera?
- Vyžaduje server špeciálny prístup zálohovania z dôvodu databázy alebo inej aplikácie?
- Kedy (časovo) môže prebiehať záloha servera?
- Kedy (časovo) nesmie prebiehať záloha servera?
- Aký typ záloh je nutné na serveri vykonávať?
- Obsahuje server špecifickú funkcionalitu, ktorá môže spôsobiť komplikácie pri zálohovaní?
- Ovplyvní zálohovanie serveru jeho dostupnosť?
- Ovplyvní zálohovanie serveru dostupnosť iného zariadenia?
- Pokiaľ dôjde k zlyhaniu procesu zálohovania, má ten byť reštartovaný okamžite alebo počkať do najbližšieho plánovaného spustenia?
- Existuje bod (v čase), počas ktorého zálohy výslovne nesmú bežať?
- Kto je správcom servera?
- Kto je autorizovaný k podávaniu návrhov na zmenu a modifikáciu systému zálohovania?
- Kto má byť notifikovaný o prípadných problémoch pri zálohovaní?
- Aké sú priority jednotlivých serverov spoločnosti?

Po zodpovedaní všetkých otázok nastáva priestor na výber konkrétneho zálohovacieho riešenia od poskytovateľov, prípadne vyvinúť vlastný softvér.

3.4 Zálohovanie klientskych staníc a prenosných zariadení

Napriek tomu, že zálohovanie klientskych staníc je typicky považované za príliš nevyhovujúce, nákladné a plné rôznych chýb, rôzne spoločnosti boli donútené reguláciami vlády, aby ho zaviedli a zabránili tak hrozbe straty dát. Ak sa rozhodujeme o nezálohovaní klientskych staníc a prenosných zariadení, berieme v úvahu odpovede na nasledujúce otázky.

- Je možné v pracovnom prostredí užívateľom ukladať dáta do lokálneho PC?
  - Ak áno, je možné použiť automatickú replikačnú procedúru ku kopírovaniu lokálnych dát na server?
  - Ak nie, je možné použiť automatickú replikačnú procedúru, odporúča sa zamedziť užívateľom možnosť lokálneho ukladania dát? V inom prípade sa musí realizovať zálohovanie klientskych staníc.
- Ak prostredie neumožňuje užívateľom ukladať dáta lokálne.
  - Je spomínané správanie testované?
  - Je dostupný nástroj rýchlej obnovy systému?
  - Sú definované pravidlá a postupy pre jednotlivé kategórie problémov užívateľa?

Ak na základe zodpovedania hore uvedených otázok dôjdeme k záveru, že je nutné integrovať klientske stanice do systému zálohovania, musíme odpovedať na ďalšie dotazy. Tie nás navedú na to správne riešenie.

- Bude proces zálohovania automatizovaný?
- Bol proces zálohovania otestovaný, aby sa overil jeho dopad na výkonnosť užívateľa?
- Je zakázaná možnosť užívateľa prerušiť proces zálohovania?
- Bude mať užívateľ možnosť obnovy systému a prístupu k zálohám?
- Ako budú vykonávané zálohy prenosných zariadení, ktoré sú mimo internú firemnú sieť?
- Ak sa plánuje zálohovanie klientskych staníc cez noc, boli užívatelia oboznámení, že nemajú vypínať počítače po ukončení práce?

- Ako bude zálohovací systém spracovávať potenciálne veľký výskyt chybových hlásení od zariadení mimo dosah alebo vypnutých?

Hlavným problémom záloh iniciovaných užívateľmi je ľudský faktor. Výskyt chýb je u tohto typu vysoký. Užívatelia často zabúdajú na rutinné operácie, ktoré majú vykonať. Je nutné proces zálohy klientskych staníc automatizovať v čo najväčšej možnej miere, ideálne úplne. (3)

3.5 Softvér

Dominantným riadiacim prvkom je spomínaný zálohovací server. Sám o sebe však potrebnou funkcionalitou nedisponuje. Potrebné služby bude zabezpečovať softvér od spoločnosti Microsoft, ktorý je vyvinutý za účelom použitia v prostredí malej a strednej firmy. Každý komerčný zálohovací softvér obsahuje základnú funkcionalitu, ktorá je viac menej totožná u všetkých produktov. Zaujímavé z pohľadu administrátora sú doplnky, ktoré uľahčujú a automatizujú prácu so zálohovaním a obnovou systému.

V tomto riešení bude použitý produkt Microsoft Data Protection Manager vo verzii 2012, ktorá oproti verzii 2010 prináša rozšírenú funkcionalitu a opravu zabezpečenia prístupu.

Ďalším softvérovým nástrojom je komerčný produkt MirrorFolder, ktorý je primárne určený na online replikáciu súborového servera.

3.5.1 Data protection manager 2012

DPM 2012 (v skratke Microsoft Data Protection Manager 2012) poskytuje rozsiahle možnosti zálohovania prostredia Microsoft. Princíp jeho fungovania je založený na využívaní technológie Volume Shadow Copy Service, čo je služba serverov Microsoft 2008 a novšie. S nástupom virtuálnych technológií prišla otázka, ako tieto virtuálne stroje zálohovať. I túto otázku rieši spomínaný produkt. Zálohovanie technológie Hyper-V, ako aj zálohovanie SQL databázy, Exchange servera a Sharepoint servera sú súčasťami vybavenia. Nespornou výhodou je možnosť zálohy fyzického servera a jeho následné prevedenie na virtuálny server. Technológia ukladania záloh umožňuje používať klasické pevné disky (diskové polia), páskové knižnice alebo ich kombinácie. Štruktúra ukladania záloh môže byť D2D, D2T, D2D2T, čím sa minimalizuje riziko straty záloh.

Zálohovanie Hyper-V prostredia umožňuje nielen zálohovať jednotlivé virtuálne servery a ich inicializačnú knižnicu, ale nástrojom migrácie je možné preniesť virtuálny server na iného hostiteľa za jeho behu (tzv. dynamická migrácia virtuálnych serverov). Okrem obnovy servera ako kompaktného celku disponuje softvér funkciou ITL (Item Level Recovery), čo znamená obnovu na úrovni jednotlivých položiek. Ide o významný krok, kedy nie je potrebné obnoviť celý server na získanie konkrétnych dát.

Zálohovanie SQL databázy je integrovaná ako základná funkcionalita. Umožňuje zálohovať až tisíc databáz na jediný DPM server. Pracuje so vstavanými nástrojmi databázy na zálohy a obnovu. Existuje taktiež variant obnovy databázy priamo koncovým užívateľom s príslušnou rolou. Zálohovanie databázy pomocou DPM servera prináša aj proces automatizácie, kde každá nová pridaná databáza je automaticky zahrnutá do procesu zálohovania s nastaveniami zhodnými pre celú vybranú skupinu.

Zálohovanie Exchange servera vo verzii 2003 až 2010. Podporuje zálohovanie a obnovu štruktúry vysokej dostupnosti DAG.

DPM 2012 má okrem spomínaných výhod aj radu nevýhod, ktoré zväčša administrátor odhalí až v praxi. Jednou z nich je nemožnosť vytvárania záloh na externé zariadenia pripojené cez USB. Systém podporuje iba interné pevné disky alebo pripojené páskové knižnice. (4)

3.6 Archivácia

Zálohy dát a dátové archívy sú často zamieňané pojmy. Mnoho ľudí nepozná rozdiel medzi týmito dvoma pokročilými technikami ukladania dát, a preto sa mylne domnievajú, že v prípade potreby je možné použiť úložisko záloh ako úložisko pre archívne dáta, čo rozhodne nie je dobrý nápad.

Položme si preto otázku, na ktorú málo ľudí pozná odpoveď. Aký je teda základný rozdiel medzi úložiskom záloh a úložiskom archívu? Vysvetlenie je jednoduché. Zálohy dát sú primárne určené k obnove po pohromách a zlyhaniach, zatiaľ čo dátové archívy slúžia na „zisťovanie“ údajov a informácií. Záloha dát je určená na obnovu a zotavenie zo stratených alebo poškodených súborov. Takže v prípade kedy užívateľ náhodne vymaže potrebné dáta, alebo poškodí operačný systém, použije sa záloha a dáta sa obnovia. Na strane druhej ani vytváranie verzií súborov nie je považované za archiváciu. (5)

Určite jednou z vecí, ktoré nad zálohami nie je možné (alebo nechceme) vykonať je použiť ich ako zdroj pre rýchle vyhľadávanie potrebných informácií. To je práve účel a cieľ dátovej archivácie. Všeobecne je možné systémy archivácie dát popísať ako úložiska, kde sú dáta ukladané na dlhšiu dobu za účelom ich použitia pri analýzach, štatistikách a najmä ako podpora rozhodovania manažmentu firmy. Nevyhnutnosťou pre rýchlosť archívu je kvalitné indexovanie, ktoré prináša radu výhod vo vyhľadávaní konkrétnych dát, informácií.

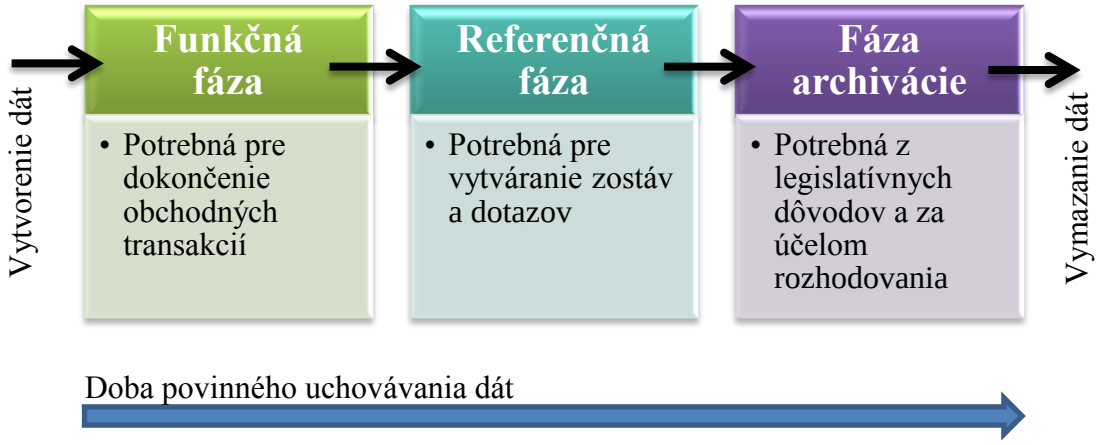
3.6.1 Životný cyklus dát

Kľúčovým prvkom archivácie dát je poznať bod, v ktorom je potrebné dáta archivovať. Pre jeho správnu identifikáciu musíme mať prehľad o celom životnom cykle dát. Obrázok 3.4 vystihuje všetky životné fázy dát počas ich užitočného života. Dáta sú vytvorené v určitom okamihu, zvyčajne nejakou transakciou typu vytvorenie produktu, spracovanie objednávky, vystavenie faktúry a iné. Po určitú dobu od vytvorenia dáta vstupujú do svojej prvej fáze života – *funkčná fáza*. V nej sú všetky dáta potrebné na každodenný beh obchodných transakcií. Transakcie prebiehajú výlučne nad dátami v spomínanej fáze.

Funkčná fáza je nasledovaná *referenčnou fázou*. Počas nej sú dáta stále potrebné k vytváraniu zostáv a dotazov. Je možné pomocou nich vytvárať interné zostavy, alebo dohľadať na požiadanie klienta.

Po uplynutí určitého časového okna, zvyčajne stanoveného v interných smerniciach firmy, dáta prechádzajú plynule do fázy, kde už viac nie sú potrebné na obchodné transakcie a je malá pravdepodobnosť ich využitia pre zostavy a dotazy. Ide o fázu archivácie. Tento stav existuje hlavne z legislatívnych dôvodov a taktiež ako podklad pre rozhodovanie a plánovanie manažmentu.

V dátovom archíve však cesta dát nekončí. Poslednou zastávkou nepotrebných dát je ich vymazanie. (6)



Obrázok 3.4 Životný cyklus dát

3.6.2 Stratégia archivácie

Archivácia dát je pre mnohé dátové úložiská životne dôležitým procesom, a to hneď z niekoľkých dôvodov. Za prvé, archivácia dát na dlhú alebo krátku dobu, umožňuje firme vracať sa „späť v čase“ a získať tak dôležité dáta pre rozhodovanie a plánovanie ako aj pre analýzu trhu a odberateľov. Za druhé, archívy dát sú uchovávané legislatívne stanovený počet rokov. Pre rôzne doklady platí doba archivácie v rozmedzí tri až tridsať rokov. Konkrétnu dobu archivácie daného typu stanovuje v účtovníctve §31 zákona o účtovníctve a to:

- Účtovná uzávierka, výročná správa – 10 rokov,

- účtovné doklady, odpisové plány, inventúrne súpisy – 5 rokov,
- účtovné záznamy, ktorými účtovné jednotky dokladujú vedenie účtovníctva – 5 rokov. (7)

Firmy, ktoré zamestnávajú zamestnancov musia podľa zákona č. 582/1991 Sb., o organizácii a vykonávaní sociálneho zabezpečenia, viesť personálnu evidenciu. Archivovať sa musia dokumenty:

- Rovnopisy evidenčných listov – 3 roky,
- mzdové listy, údaje dôchodkového poistenia – 30 rokov,
- zoznam spoločníkov, orgánov firmy – 6 rokov.

Ďalej podnikatelia, ktorý sú platcami dane z pridanej hodnoty musia daňové doklady archivovať podľa §27 zákona č. 235/2004 Sb., o dani z pridanej hodnoty po dobu 10 rokov.

Ostatné dokumenty podnikateľa zapísaného v obchodnom registre musia byť uchovávané podľa zákona č. 499/2004 Sb., o archívnictve a spisovej službe. (8)

V praxi sa využívajú tri základné stratégie archivácie, a to archivácia na pevný disk, archivácia na páskovú jednotku alebo ich kombinácia. Každá spomínaná stratégia má svoje klady a zápory, preto množstvo firiem volí práve ich kombináciu. Pevné disky slúžia prevažne na krátkodobú archiváciu, pričom páskové jednotky na dlhodobú archiváciu.

Archivácia na pevný disk má radu výhod. Prvou je, že archivácia a obnovenie dát je omnoho rýchlejšia. Druhou je indexovanie a vyhľadávanie dát. Napríklad pri hľadaní konkrétneho dokumentu je proces „obnovy z archívu“ omnoho rýchlejší, ako aj samotný proces vyhľadávania. Nevýhodou sú vyššie náklady na beh viacerých diskových polí, ktoré majú vyššiu spotrebu elektrickej energie a tiež nároky na priestor a chladenie.

Naopak výhodami archivácie na páskovú jednotku sú nižšie energetické nároky a menej potrebného priestoru. Taktiež používanie páskových jednotiek nám môže poskytnúť úroveň ochrany v podobe šifrovania dát. Druhou stránkou je zložitosť a rýchlosť ich používania. Väčšina administrátorov sa spolieha na fakt, že nebudú musieť vyhľadávať dáta na páskovom médiu. (9)

Prax ukázala, že dátové objemy pre archiváciu v rozsahu do 50TB využívajú pevné disky, rozsahy medzi 50TB až 100TB sú na hrane a zvažujú podľa ich plánov a potrieb použitie páskových jednotiek. Akákoľvek archivácia prekračujúca objem 100TB je určená výlučne pre páskové jednotky.

3.7 Manažérsky prístup

Podstatný vplyv na úspešnosť implementácie zálohovacieho systému má participácia manažmentu spoločnosti a ich zapojenie do procesu zálohovania a obnovy. Nejedná sa samozrejme o zapojenie v pravom slova zmysle, kde by manažér bol nútený konfigurovať systém. Ide skôr o funkciu kontroly funkčnosti a pripravenosti systému. Úloha manažmentu v systéme je podrobnejšie popísaná v časti 4.1.4 Ľudská vrstva.

Nástrojom kontroly z pozície manažmentu sú smernice a plány zálohovania a obnovy, kde je nutné jasne stanoviť kľúčové metriky a postupy ich spracovania a vyhodnotenia. Na ich podklade vyhodnocuje vedenie spoločnosti plnenie pracovnej náplne zamestnanca zodpovedného za správu systému zálohovania. Ďalej kontroluje na základe metrík fungovanie a správne postupy pri vykonávaní záloh a obnovy ako aj dodržovanie pravidiel zo strany užívateľov.

Forma smerníc a plánov nie je fixne stanovená žiadnym nariadením, opiera sa iba o odporúčania normy ISO 270001 – Systém riadenia bezpečnosti informácií.

Na úrovni vysokého a stredného manažmentu nie je vhodné vyžadovať absolútnu znalosť technického pozadia systému zálohovania. Naopak, manažéri očakávajú, že ak systém nebeží, budú o tom bez meškania oboznámení. Taktiež stredný manažment by mal byť schopný plniť dve dôležité funkcie v systéme zálohovania a obnovy:

- Prezentovať a obhajovať rozpočet oddelenia IT s prihliadnutím na potreby systému zálohovania a obnovy.
- Sprostredkovať komunikáciu medzi senior manažmentom a technickými zamestnancami z dôvodu reportov, analýz, auditov a testovania.

Manažment sa môže pokúsiť vykonávať spomínané body bez akejkoľvek znalosti zálohovacieho systému, avšak bude to viesť k prázdnym „recitáciám“ reportov a výstupov systému. Práve to je dôvodom potreby oboznámiť manažment so základnou funkcionalitou systému a vybudovať u nich základné povedomie o systéme zálohy a obnovy. Úplným základom sú znalosti o:

- Topológia zálohovania,
- plánovanie a úrovne,

- dostupnosť dát,
- ako možno zmierniť dopady serveru,
- možnosti dostupné k zálohovaniu databázy a špeciálnych aplikácií,
- potreba duplikácie zálohovaných dát,
- kto je administrátorom a osobou zodpovednou za systém,
- ako pristupovať k reportom a výstupom administrátora a predávať ich ďalej vyššiemu manažmentu. (10)

4 VLASTNÝ NÁVRH RIEŠENIA

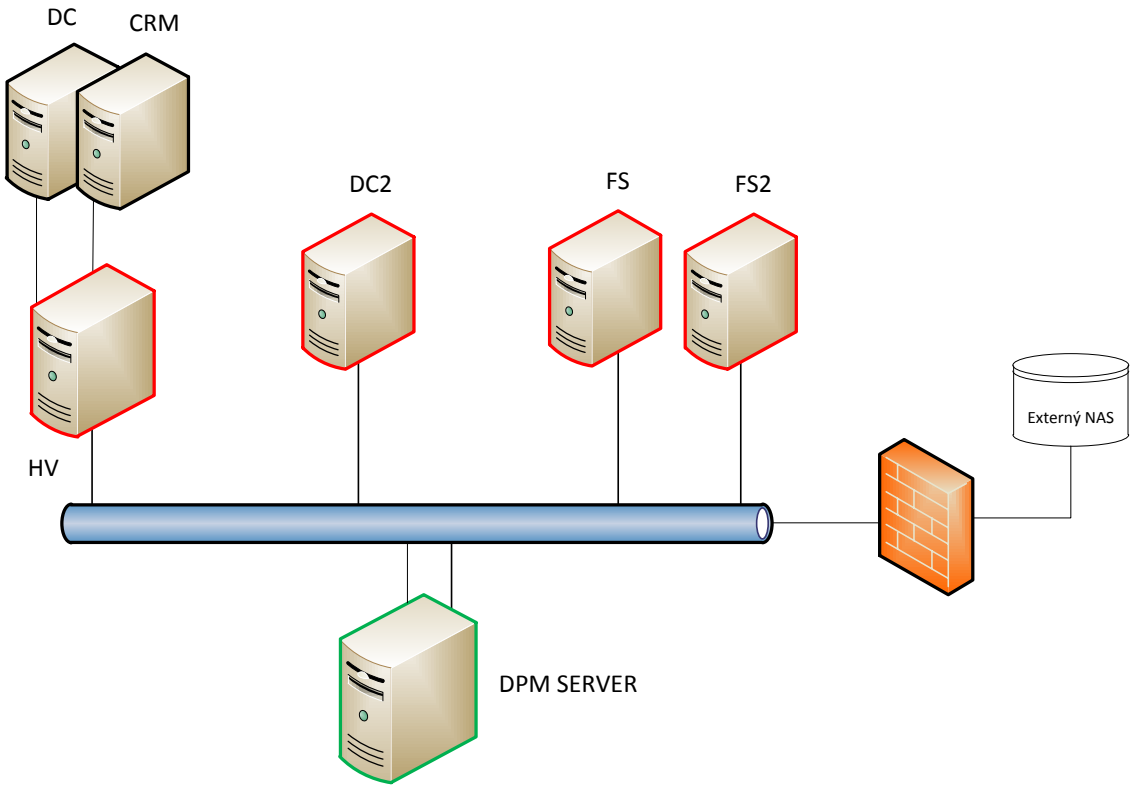
Vzhľadom k úzkej spolupráci so spoločnosťou GPO, spol. s r.o. a akútnej potrebe riešenia ich problému so zálohovaním a archiváciou je vypracovaný tento návrh. Spočíva vo vytvorení návrhu komplexného systému zálohovania produkčných serverov ako aj databázy informačného systému. Na procesy zálohovania logicky nadväzujú procesy obnovy zo záloh, kde často dochádza k zlyhaniu z dôvodu neprevedenia priebežných testov záloh. Celý systém je postavený a integrovaný do firemnej štruktúry, čím dochádza k zapojeniu všetkých vrstiev zamestnancov a delegovaniu zodpovednosti i právomoci s konkrétnym zosobnením jednotlivých povinností. Poslednou časťou praktickej aplikácie je vypracovanie stručného návrhu štruktúry archivácie dát z dlhodobého hľadiska.

V dnešnej dobe je dôležitá najmä otázka financií, preto v rámci návrhu systému zálohovania a obnovy figuruje kalkulácia nákladov.

4.1 Priblíženie návrhu riešenia

Vychádzajúc z analýzy súčasného stavu s prihliadnutím na vývoj a expanziu spoločnosti navrhujeme zaviesť systém centralizovaného zálohovania s jediným zálohovacím serverom a dostatočnou úložnou kapacitou (Obrázok 4.1).

Charakter činnosti firmy spôsobuje, že všetky servery spomenuté v časti analýzy súčasného stavu sú denne potrebné k obchodnej činnosti spoločnosti, preto odporúčame využiť technológiu online dostupnosti dát pri zálohovaní, ktorá umožní zálohovanie aj priebežne počas pracovnej doby.



Obrázok 4.1 Zobrazenie návrhu štruktúry zálohovania serverov

4.2 Norma ISO/IEC 27 001

Normy svojím charakterom prinášajú sadu odporúčaní v rámci bezpečnosti informačných systémov a zabezpečenia v IT ako takom. Spoločnosti GPO, spol. s r.o. neodporúčame zavádzať túto normatívu v plnom rozsahu vzhľadom k jej časovej a finančnej náročnosti. Navrhujeme však jej využitie pre stanovenie základných bodov bezpečnosti systému ako celku. Návrh nachádza odpovede na nižšie uvedené body, pre ktoré doposiaľ neexistovalo v rámci firmy riešenie a neboli vôbec zavedené.

4.2.1 Návrh bezpečnostnej politiky informácií

Norma sa v tomto bode zaoberá problematikou existencie dokumentu, ktorý popisuje politiku bezpečnosti informácií vo firme. Návrh obsahu dokumentu pre firmu je nasledujúci:

Spoločnosť GPO, spol. s r.o. v súlade s požiadavkami normy ČSN ISO/IEC 27001 odst. 4.2.1 b) príjme nasledujúcu Politiku bezpečnosti informácií:

- Spoločnosť považuje za zásadnú bezpečnosť dát svojich zákazníkov a venuje im maximálnu pozornosť už pri uzatváraní zmlúv tak i ďalej v jednotlivých dokumentoch,
- spoločnosť rešpektuje a dodržuje všetky relevantné regulačné, právne a normatívne požiadavky,
- zásadným pre spoločnosť je dodržovanie uzavretých zmlúv, ktorých problematike je venovaná primárna pozornosť v priebehu plnenia celej zákazky,
- spoločnosť identifikuje metodiku hodnotenia rizík a stanoví kritéria, podľa ktorých prebieha ich hodnotenie.

Spoločnosti ďalej doporučujeme ustanoviť nasledujúcu politiku riadenia prístupu k informáciám, ktorou sa riadi nastavenie všetkých oprávnení vnútri organizácie. Zásady musia obsahovať:

- každý užívateľ má prístup iba k tým informáciám, ktoré nutne potrebuje pre výkon svojej práce,
- o pridelení práv rozhoduje v rámci svojich oprávnení nadriadený zamestnanec,
- pokiaľ už oprávnenie nie je potrebné, je podľa nastavených jednotlivých firemných procesov okamžite odobrané,
- vzdialený prístup je povolený iba v rozsahu potrebnom pre výkon práce, pri jeho využití je zamestnanec povinný dodržiavať stanovené postupy a dbať na zvýšenú bezpečnosť,
- nastavenie všetkých sieťových služieb, musí ctiť zásadu „Čo nie je dovolené, je zakázané!“

Dokument musí byť schválený valným zhromaždením a predaný do užívania v rámci interného prostredia firmy ako záväzné nariadenie.

Za aktualizáciu a vypracovanie dokumentu nesie zodpovednosť konateľ A. Na základe skúseností odporúčame dokument uvádzať v rámci prílohy k pracovnej zmluve všetkých zamestnancov.

Nasleduje dátum a miesto vzniku dokumentu ako aj podpisy zodpovedných zamestnancov za jeho spracovanie, schválenie a aktualizáciu.

4.2.2 Návrh zabezpečenia ľudských zdrojov

U väčšiny systémov, ktoré prichádzajú do styku s človeko dochádza najčastejšie k zlyhaniu ľudského faktora. Práve tento krok je nutné ošetriť už v prvotnom a najdôležitejšom dokumente vytyčujúcom vzťah zamestnanca a zamestnávateľa – v pracovnej zmluve.

Pri podpise pracovnej zmluvy – zmluva musí obsahovať náležitosti súvisiace s druhom vykonávanej práce. Zmluva musí obsahovať časť zahrňujúcu

- Presnú definíciu náplne práce zamestnanca,
- vytýčenie jeho povinností,
- vytýčenie predmetov hmotného i nehmotného charakteru, za ktoré v rámci náplne práce nesie zodpovednosť.

U novo prijímaných zamestnancov je odporúčané preveriť si čiastočne v rámci medziach zákona ich bezúhonnosť a minulosť.

Zabezpečenie ľudských zdrojov nekončí podpisom pracovnej zmluvy. V rámci pracovného vzťahu sa doporučuje zamestnávateľovi pravidelne školiť zamestnancov v oblasti bezpečnosti dát, a to minimálne jedenkrát ročne. Pri ukončení pracovného vzťahu musí zamestnanec odovzdať všetky prostriedky, ktoré mu boli zverené, ako aj bezpečnostné predmety a karty.

Za vypracovanie a aktualizáciu vzoru pracovnej zmluvy je zodpovedná p. Kristína H. na pozícií personalistky. Vzor musí byť následne schválený valným zhromaždením.

4.2.3 Návrh fyzickej úrovne zabezpečenia prostredia

Exponovaným problémom je fyzické zabezpečenie prostredia firmy. Konkrétne sa zaujímame o zabezpečenie priestorov, kde sú umiestnené servery a zálohy, nakoľko priamo v klientskych staniciach sa žiadne citlivé dáta nenachádzajú.

Všetky aktívne zariadenia využívané v rámci IT sú aktuálne umiestnené v uzavretej klimatizovanej miestnosti so zabezpečením proti požiaru.

Našim odporúčaním je určenie možnosti fyzického vstupu do bezpečnostného perimetra. Prístup musí byť umožnený administrátorovi systému, a to samostatne bez nutnosti povolenia od nadriadeného. Systém vstupu bude riešený formou FAB kľúča v počte dvoch kusov, pričom jeden v rámci náplne práce preberie administrátor systému a druhý je uzamknutý vo firemnom trezore, ku ktorému má prístup iba konateľ A a konateľ B.

Výmenu zámkov zabezpečí konateľ B, ktorý zároveň odovzdá jeden kus kľúča administrátorovi. K odovzdaniu bezpečnostného kľúča navrhujeme vypracovať odovzdávací protokol, ktorý bude obsahovať:

- Meno, priezvisko, identifikačné číslo a podpis osoby, ktorá kľúč odovzdáva.
- Meno, priezvisko, identifikačné číslo a podpis osoby, ktorá kľúč preberá.
- Identifikačný kód kľúča.
- Dátum a miesto odovzdania.

Vo výsledku informuje konateľ B valné zhromaždenie o vykonanom úkone, pričom originál odovzdávacieho protokol bude založený do dokumentácie systému zálohovania.

Osobami zodpovednými za vstup neautorizovaných osôb do perimetra navrhujeme určiť všetky osoby uvedené v odovzdávacom protokole.

Výsledkom tohto opatrenia bude zamedzenie vstupu neautorizovaných osôb do bezpečnostného perimetra serverovne.

4.3 Návrh klasifikácie dát

Systém zálohovania a obnovy bez poznania dôležitosti dát vznikajúcich vo firme vedie k zbytočnému nárastu objemu zálohovaných dát. Na základe analýzy existujúcich a tvorby nových dát navrhujeme spoločnosti GPO, spol. s r.o. klasifikovať dáta z dvoch hľadísk. *Tým prvým je klasifikácia dát podľa stupňa utajenia*:

Tajné dáta,

sú dáta, ktoré v žiadnom prípadne nesmú opustiť kancelárie spoločnosti.

Ide o vysoko rizikové dáta interného charakteru, ktoré by boli konkurencii silným nástrojom. Prevažne ide o finančné toky a operácie, strategické dokumenty a autorské výtvory.

Umiestnenie:

Dáta tajného charakteru doporučujeme uchovávať na súborovom serveri v zložke DATA, pod zložke TAJNE s nasledujúcim nastavení prístupu:

- Povolení užívatelia – členovia valného zhromaždenia budú mať úplné prístupové práva k súborom v pod zložke.
- Nepovolení užívatelia – všetci ostatní zamestnanci okrem povolených.

Interné dáta,

sú dáta, ktorých únik spôsobí vážnejšie škody, pričom neohrozí priamo existenciu firmy. Ide prevažne o dáta klientov, výsledky práce zamestnancov a know-how.

Umiestnenie:

Dáta interného charakteru doporučujeme uchovávať na súborovom serveri v zložke DATA, ktorá je celá radená do tejto kategórie. Nastavenie prístupu:

- Povolení užívatelia – všetci zamestnanci spoločnosti GPO, spol. s r.o., ktorým boli pridelené prihlasovacie údaje do internej firemnej domény. Pridelené práva budú na čítanie a zápis súborov, vytváranie zložiek.
- Špeciálny užívatelia – do tejto kategórie bude patriť domain admins group v AD.

Verejne dostupné dáta,

sú všetky dáta uverejnené na webových stránkach spoločnosti, taktiež informácie, ktoré firma poskytli médiá, a ktoré sama prezentuje inou formou verejnosti, potenciálnym a existujúcim klientom.

Umiestnenie:

Dáta verejne dostupné doporučujeme uchovávať v rámci webovej stránky spoločnosti. Taktiež prezentačné materiály a referencie určené na propagáciu spoločnosti budú ukladané na súborový server v zložke IMAGE. Táto zložka bude prístupná všetkým užívateľom prihláseným v rámci firemnej internej domény.

Nastavenie vyššie uvedených prístupových práv vykoná administrátor systému, a to najneskôr sedem dní pred spustením systému zálohovania. Automaticky týmto preberá administrátor systému zodpovednosť za prístup neautorizovaných osôb do chránených zložiek. Po nastavení práv je povinný administrátor systému oznámiť túto skutočnosť konateľovi A, ktorý vykoná kontrolu správneho nastavenia pomocou testovacieho účtu domény.

Druhým odporúčaným spôsobom je klasifikácia podľa ich dôležitosti a potreby v rámci vnútropodnikových procesov. Tento prístup bude plne využívaný k určovaniu priorít dát pri vytvorení systému záloh a obnovy.

Kritické dáta,

sú svojim charakterom rozhodujúce v každodennej obchodnej činnosti. Ich strata alebo poškodenie by mohla viesť k likvidácii spoločnosti alebo ju významne oslabiť. Kritické dáta sú v prevažnej miere dokumenty požadované rôznymi štátnymi inštitúciami, na ktoré sa vzťahuje zákon o archivácii, ale aj dáta vytvárané manažmentom spoločnosti na strategickej úrovni.

Umiestnenie:

Kritické dáta doporučujeme uchovávať na súborovom serveri v zložke DATA, pod zložke TAJNE a ďalej v zložke ARCHIV, pričom do zložky ARCHIV budú mať prístup iba nastavení užívatelia domény – všetci konatelia.

Dôležité dáta,

reprezentujú dáta vytvorené zamestnancami v rámci ich náplne práce, tzn. ide o výstupy predávané klientom. Taktiež majú túto úroveň dáta, ktorých charakter je daný zákonom o archivácii na dlhšie obdobie.

Umiestnenie:

Dôležité dáta doporučujeme uchovávať na súborovom serveri v zložke DATA.

Bežné dáta,

predstavujú poslednú triedu klasifikácie dát. Ich strata nijako neohrozí chod firmy, avšak taktiež môže spôsobiť vyčísliteľnú finančnú ujmu. Ide v prevažnej miere o súkromné dáta zamestnancov, ktoré nepodliehajú zálohovaniu, ako aj dáta informačného charakteru bez pridanej hodnoty.

Umiestnenie:

Bežné dáta doporučujeme uchovávať vo vyhradenej zložke užívateľa na lokálnom PC, pričom bude nastavené pravidlo pre veľkosť priečinku maximálne 15GB. Bežné dáta celoplošného charakteru sa budú ukladať na súborovom serveri v priečinku DATA v pod priečinku OSTATNE. Nastavenie práv k tomuto priečinku bude totožné s nadradeným priečinkom.

Uvedené triedenie na kritické, dôležité a bežné dáta budú zohľadnené pri nastavení systému zálohovania a obnovy.

Databáza interného informačného systému je samostatným objektom s vysokou dôležitosťou. Odporúčame ju preto zaradiť do kritickej kategórie s príznakom tajné. Sama o sebe predstavuje veľké riziko. V prípade jej poškodenia dôjde k nevyčísliteľným stratám či už z hľadiska hodnoty informácií alebo stagnácie firmy.

Ďalším prvkom kde je nevyhnutné dáta klasifikovať je emailový server. Tento server musí byť rovnako ako databáza zaradený do kritickej úrovne tajného charakteru. Dôvodom je, že množstvo hodnotných informácií a dát je predávaným dnes už formou emailu namiesto klasickej fyzickej pošty.

Ostatné servery, na ktorých sú taktiež dáta, navrhujeme klasifikovať na dôležitú úroveň s interným charakterom. Ide o všetky ostatné severy, mimo DC2, FS a CRM.

Klientske stanice so sebou nesú najmenšiu hrozbu z hľadiska ohrozenia firemných dát, nakoľko je ich použiteľnosť obmedzená iba na uzavretú firemnú

doménu, do ktorej sa užívatelia autorizujú prideleným menom a minimálne sedem miestnym heslom obsahujúcim povinne minimálne jeden špeciálny znak, veľké a malé písmená a čísla. Ich zaradenie navrhujeme do úrovne bežné dáta, svojím charakterom však spadajú do internej réžie.

4.4 Odporučenie interných smerníc

V nasledujúcej časti riešenia navrhneme smernice, ktoré firma musí vytvoriť v rámci internej kultúry, vrátane špecifikácie ich obsahu, zodpovedností, metrík, sankcií a termínov. Jedná sa o dôležitú časť celého projektu vzhľadom k nutnosti definovania a určenia zodpovednosti konkrétnych osôb (pozícii). Často chýbajúcim prvkom v rámci interných predpisov firiem je zosobnenie zlyhania systému a prípadných chybných krokov ako administrátora tak aj manažmentu.

4.4.1 Návrh smernice zálohovania a obnovy

Smernica systému zálohovania a obnovy pre spoločnosť GPO, spol. s r.o.

Zodpovedná osoba: administrátor systému, menom Tomáš S.

Informovaná osoba: konateľ B, menom Petr D.

Osoba zodpovedná za umiestnenie a úschovu externého NAS mimo objekt spoločnosti: konateľ A, menom Róbert G.

Osoba zodpovedná za organizáciu školenia: zamestnanec úseku správy ľudských vzťahov Mgr. Linda P.

Užívateľ: každý zamestnanec firmy GPO, spol. s r.o., ktorému bolo pridelené užívateľské meno a heslo pre prihlásenie do domény.

Na schválenie: valné zhromaždenie spoločnosti

Dátum vytvorenia a prípadnej aktualizácie

Účel smernice: Účelom tejto smernice je stanovenie zásad pre korektné zálohovanie serverov a dát spoločnosti GPO, spol. s r.o.

Navrhujeme nasledujúce znenie jednotlivých článkov smernice:

Článok I.

Zálohovanie serverov sa riadi vypracovaným časovým plánom (Tabuľka 4.3 Časový plán záloh). V priebehu existencie systému záloh a obnovy musia byť *zodpovednou osobou* vykonávané nasledujúce úkony kontroly systému:

- Každých 48 hodín kontrolovať funkčnosť a správnu funkciu softvérovej časti zálohovacieho servera, výstupom kontroly bude podaná písomná správa (report) informovanej osobe.

Nástroje kontroly: Zodpovedná osoba vykoná kontrolu načítaním záznamov z monitoringu systému DPM 2012 a taktiež kontrolu načítaním záznamov operačného systému.

- Každých 7 dní preveriť konzistentnosť diskového poľa zálohovacieho servera. V prípade zistenia problému následne podať písomnú správu informovanej osobe.

  Nástroje kontroly: Konzistentnosť diskového poľa bude preverená cez administračnú konzolu radiča.
- Jedenkrát mesačne vyhľadať aktualizácie dostupné pre zálohovací server a previesť ich inštaláciu, výstupom aktualizácie bude podaná písomná správa (report) informovanej osobe.

  Nástroje kontroly: Aktualizácie operačného systému budú vyhľadané cez nástroj Windows update. Aktualizácie softvéru DPM 2012 budú vyhľadané pomocou webu Microsoft Update.
- Vždy posledný týždeň mesiaca vypracovať písomnú správu zhrňujúcu všetky udalosti systému zálohovania za mesiac. Súčasťou správy bude časť o aktuálnom stave systému a časť o prípadných požiadavkách na stranu manažmentu spoločnosti. Správu doručí elektronicky informovanej osobe.

Informovaná osoba, má v systéme zálohovania a obnovy povinnosti spracovať správy prijaté zodpovednou osobou a v prípade nezrovnalostí je povinná ju bezodkladne kontaktovať. Informovaná osoba tj. manažér spoločnosti má určené nasledujúce povinnosti:

- Vždy prvý týždeň mesiaca podáva správu o stave zálohovacieho systému a návrhy prípadných požiadaviek zodpovednej osoby celému manažmentu spoločnosti. Zároveň v prípade konania valného zhromaždenia podáva komplexnú správu o stave systému.
- Vždy k poslednému dňu aktuálneho mesiaca vykoná kontrolu umiestnenia FAB kľúča v trezore spoločnosti, ako aj jeho prítomnosť u zodpovednej osoby. O tejto kontrole vypracuje záznam, ktorý uloží taktiež do trezora.

Zodpovednosť za funkčnosť systému zálohovania a obnovy nesie zodpovedná osoba uvedená v hornej časti dokumentu. Informovaná osoba preberá plnú zodpovednosť za schvaľovanie požiadaviek zodpovednej osoby

V prípade nedodržania bodov kontrolnej činnosti, bude zodpovednej osobe uložené napomenutie s možnosťou jednorazového zníženia bonusu ku mzde až do výšky 15%.

V prípade nedodržania bodov kontrolnej činnosti alebo zlyhania procesu schvaľovania bude informovanej osobe uložené napomenutie s možnosťou jednorazového zníženia bonusu ku mzde až do výšky 15%.

Článok II.

Primárny súborový server musí byť zálohovaný. Zodpovedná osoba prevedie konfiguráciu softvéru MirrorFolder podľa nasledovných parametrov.

Tabuľka 4.1 Rozvrh nastavenia zrkadlenia súborového servera

Server	Priečinok	Cieľový server	Spôsob zrkadlenia	Časový plán
FS				
	DATA	FS2	Zrkadlenie v reálnom čase	pri zmene
	IMAGE	FS2	Zrkadlenie plánovanou synchronizáciou	každý piatok 19:00
	ARCHIV	FS2	Zrkadlenie plánovanou synchronizáciou	každú sobotu 09:00

Počas užívania systému zrkadlenia súborového serveru na záložný server ako forma zálohy je zodpovedná osoba povinná vykonávať tieto kroky:

- Každých 14 dní preveriť stav a funkčnosť systému zrkadlenia.

  Nástroje kontroly: Zodpovedná osoba preverí záznamy udalostí softvéru MirrorFolder, dostupnosť a zaťaženie servera FS a taktiež servera FS2.
- Raz mesačne, vždy však najneskôr do 10. dňa aktuálneho mesiaca preverí korektnosť zrkadlenia dát z primárneho súborového serveru.

  Nástroje kontroly: Kontrolu vykoná prehliadkou stromovej štruktúry, kde identifikuje prípadné dočasné súbory a otestuje minimálne 20

súborov na ich korektné otvorenie. V prípade zistenia problému zjedná nápravu.

- Vždy posledný týždeň mesiaca vypracuje písomnú správu zhrňujúcu všetky udalosti systému za mesiac. Súčasťou správy bude časť o aktuálnom stave systému a časť o prípadných požiadavkách na stranu manažmentu spoločnosti. Správu doručí elektronicky informovanej osobe.

Informovaná osoba v časti zrkadlenia súborového servera preberá nasledujúcu zodpovednosť za vykonanie:

- Raz mesačne vykoná overenie funkcionality systému zrkadlenia.
  Nástroje kontroly: Kontrolu vykoná uložením súboru PDF do zložky DATA, pričom veľkosť súboru nesmie presiahnuť 50MB. Následne zadá sieťovú cestu priečinka sekundárneho súborového servera v tvare \\FS2\DATA, kde zistí prítomnosť vytvoreného PDF súboru. V prípade, že sa uložený súbor nachádza okamžite na oboch serveroch pracuje systém správne. Pokiaľ sa na sekundárnom serveri neobjaví vytvorený súbor, písomne (emailom) informuje o tomto stave zodpovednú osobu a žiada o diagnostiku a nápravu stavu.
- Vždy prvý týždeň mesiaca podáva správu o stave systému zrkadlenia súborového servera a návrhy prípadných požiadaviek zodpovednej osoby celému manažmentu spoločnosti. Zároveň v prípade konania valného zhromaždenia podáva komplexnú správu o stave systému.

Zodpovednosť za funkčnosť systému zrkadlenia na sekundárny súborový server nesie zodpovedná osoba uvedená v hornej časti dokumentu. Informovaná osoba preberá plnú zodpovednosť za schvaľovanie požiadaviek zodpovednej osoby

V prípade nedodržania bodov kontrolnej činnosti, bude zodpovednej osobe uložené napomenutie s možnosťou jednorazového zníženia bonusu ku mzde až do výšky 30%.

V prípade nedodržania bodov kontrolnej činnosti alebo zlyhania procesu schvaľovania bude informovanej osobe uložené napomenutie s možnosťou jednorazového zníženia bonusu ku mzde až do výšky 30%.

Článok III.

Systém zálohovania a obnovy nie je konfigurovaný s možnosťou ochrany klientskych staníc. Ak užívateľ požaduje z určitého dôvodu zálohovanie jeho pracovnej stanice, informuje o tomto stave zodpovednú osobu. Vykoná diagnostiku požiadavku a prevedie jeho prijatie alebo zamietnutie. Zamietnutie dokumentuje písomnou správou, ktorú elektronicky doručí užívateľovi a informovanej osobe. Ak zodpovedná osoba prizná potrebu zálohovania lokálneho PC, zvolí vhodný spôsob jeho riešenia z nasledujúcich možností:

- Lokálna záloha dát na externý USB disk o potrebnej veľkosti,
- lokálna záloha dát na interný disk o potrebnej veľkosti.

Použitím vstavaných nástrojov operačného systému naplánuje zálohovanie potrebných dát, pričom záloha sa vykoná vždy po odhlásení užívateľa zo systému.

Zodpovedná osoba konzultuje s informovanou osobou požiadavky na obstaranie hardvéru. Zodpovedná osoba kontroluje minimálne raz týždenne stav lokálnych záloh PC stanice.

Za prípadnú stratu a nesprávnu funkčnosť zálohovania lokálneho PC spôsobenú nekorektnou konfiguráciou nesie plnú zodpovednosť. Ak poškodenie záloh lokálneho PC nastane z dôvodu nedodržania pokynov zo strany zamestnanca, nesie ten plnú zodpovednosť za škody spôsobené stratou dát.

Článok IV.

Mimo prvú úroveň systému záloh a obnovy musí existovať druhá úroveň, tzv. kritická záloha. K jej použitiu dôjde v prípade živelnej pohromy v sídle spoločnosti. Konfigurácia systému uchovania kritických záloh musí dodržiavať nasledovné:

- Úložisko kritickej zálohy musí byť umiestnené mimo objekt spoločnosti. Konkrétny bod umiestnenia určí osoba tým poverená.

- Objekt, kde je úložisko umiestnené, musí byť zabezpečený proti vniknutiu nepovolaných osôb. Zodpovednosť za tento fakt nesie osoba poverená výberom a umiestnením úložiska kritických záloh.
- Dáta prenášané medzi serverom umiestneným na firme a úložiskom kritickej zálohy musia byť šifrované, aby nedošlo k ich zneužitiu. Za týmto účelom musí byť použitý VPN tunel na úrovni zabezpečenia minimálne L2TP.
- Zodpovedná osoba je povinná vykonávať raz mesačne kontrolu stavu systému kritických záloh. Táto kontrola bude vykonaná na základe overenia veľkosti zdrojovej a cieľovej zložky, pričom sa vzájomne nesmú líšiť. V prípade zistenia chyby systému je zodpovedná osoba povinná vykonať bezodkladnú nápravu. Po každej kontrole vypracuje zodpovedná osoba správu o stave systému, ktorú elektronicky doručí informovanej osobe.

Na úložisko kritickej zálohy musia byť každých 14 dní, a to vždy iba počas víkendu, kopírované dáta:

- Zo servera FS2
  - zložka ARCHIV kompletne
  - zložka DATA kompletne
- Zo servera DPM
  - virtuálny disk serveru CRM
  - plná korektná záloha databázy informačného systému CRM nie staršia ako 48 hodín od bodu začiatku kopírovania.
  - plná korektná záloha databázy Exchange 2010 nie staršia ako 24 hodín od bodu začiatku kopírovania.

Kopírovanie dát musí byť plne automatizované pomocou vstavaného nástroja ROBOCOPY s príkazom MIR. Za konfiguráciu a funkčnosť kritickej zálohy nesie zodpovednosť administrátor systému.

V prípade nesprávnej konfigurácie a funkcionality systému kritickej zálohy, ktorá vedie k nepoužiteľnosti dát nesie administrátor systému plnú zodpovednosť za prípadné straty vzniknuté spoločnosti z dôvodu totálneho kolapsu. Spolu zodpovednosť

za vzniknutú situáciu preberá informovaná osoba v prípade, kedy o kolíznom stave systému bola informovaná vo vydanej správe, ale na stav nereagovala.

Článok V.

Overením správnosti zálohovania je krok testovania záloh. Proces testovania záloh musí dodržiavať nasledujúce:

- Testovanie záloh vykonáva zodpovedná osoba vždy aspoň raz mesačne za asistencie informovanej osoby.
- Cieľom testovania je obnova serveru zo záloh vykonávaných serverom DPM.
- Pri obnove dát sa uplatňuje postup kapitoly 4.7.5 dokumentácie systému zálohovania a obnovy.
- Na účely testovania obnovy bude použitý novovytvorený virtuálny server, kde celý proces prebehne.

Časový rozvrh testovania záloh sa vykonáva v polročnom cykle, pričom za toto obdobie musí dôjsť k otestovaniu korektnosti záloh všetkých zálohovaných serverov a ich aplikácií. Rozvrh je nasledovný:

Tabuľka 4.2 Rozvrhnutie činností cyklu testovania záloh

Cyklus	Server	Zálohy na testovanie
1. mesiac	DC2	Obnovenie celého servera zo zálohy BareMetal
		Obnovenie iba aplikácie MS Exchange 2010 a obnova jej databázy
		Obnovenie Active Directory
2.mesiac	CRM	Obnovenie celého servera zo zálohy Hyper-V
		Obnovenie IS MS Dynamics CRM 2011 a obnova jeho databázy s použitím diferenčných záloh
3.mesiac	FS	Obnovenie celého servera zo zálohy BareMetal
4. mesiac	HV	Obnovenie celého servera zo zálohy BareMetal
		Obnovenie virtuálnych serverov zo zálohy HYPER-V
5. mesiac	DC	Obnovenie celého servera zo zálohy BareMetal

	Obnovenie Active Directory

6. mesiac DPM	Obnovenie celého servera zo zálohy BareMetal
	Obnovenie databázy MS DPM 2012 a zapojenie radiča diskového poľa

Zodpovedná osoba spolu s asistujúcou informovanou osobou vypracujú správu z každého testovania záloh, kde uvedú podrobne kroky vykonané v priebehu obnovy. Tento dokument bude slúžiť k doplneniu dokumentácie systému záloh a obnovy. V závere správy musí byť zhrnutý výsledok obnovy t.j. úspech alebo neúspech a prípadné okolnosti, ktoré viedli k zlyhaniu.

Zodpovedná osoba je povinná odstrániť príčinu v prípade zlyhania testu obnovy a nový stav oznámiť emailom informovanej osobe.

V prípade nedodržania bodov kontrolnej činnosti bude zodpovednej osobe uložené napomenutie s možnosťou jednorazového zníženia bonusu ku mzde až do výšky 30%.

V prípade nedodržania bodov kontrolnej činnosti alebo zlyhania procesu vypracovania správy z testu bude informovanej osobe uložené napomenutie s možnosťou jednorazového zníženia bonusu ku mzde až do výšky 30%.

Pokiaľ dôjde následkom nepoužiteľnej zálohy, u ktorej neboli prevedené priebežné testy obnovy, k poškodeniu spoločnosti alebo ohrozeniu jej činnosti, nesú za tento stav plnú zodpovednosť zhodne zodpovedná osoba aj informovaná osoba.

Článok VI.

Súčasťou dokumentácie zálohovacieho systému musí byť krízový manuál, kde sú špecifikované najväčšie hrozby a presný postup ich riešenia spolu s určením zodpovednosti a rolí. Jeho vypracovanie zabezpečí administrátor systému najneskôr 30 dní po spustení systému zálohovania a obnovy a predá ho následne informovanej osobe, ktorá ho predloží na schválenie valnému zhromaždeniu.

Zodpovednosť za prípadné škody spôsobené neexistenciou krízového manuálu nesie zodpovedná osoba ako aj informovaná osoba, a to obe v plnej miere.

Článok VII.

Všetci zamestnanci spoločnosti GPO, spol. s r.o. podliehajú nariadeniu pravidelných školení. Školenia budú organizované podľa úrovní:

- Manažment spoločnosti,
- zamestnanci oddelenia IT,
- ostatní užívatelia.

Jednotlivé úrovne školenia musia prebiehať samostatne, a to najmenej jedenkrát ročne. Ich náplň je stanovená:

- Bezpečnosť práce s dátami.
- Zodpovednosť a správanie v krízových situáciách.
- Prípadné podnety a pripomienky k systému.

Určená zodpovedná osoba za organizáciu školení spolupracuje na tvorbe obsahu školení s administrátorom systému. Po ukončení školení vytvorí najneskôr do 14 dní správu pre informovanú osobu, ktorej obsahom bude priebeh a prínos školenia zamestnancom.

Článok VIII.

Každá správa vytvorená v rámci internej štruktúry systému musí dodržiavať jednotnú šablónu. Vypracovanie správy, pokiaľ nejde o automaticky generovanú zostavu, prebieha v programe WORD. Následne osoba vytvárajúca správu dokument doručí cieľovej osobe výlučne elektronickou formou – emailom. Vytvorený dokument musí dodržiavať tvar REPORT_oddelenie_názovreportu a jeho veľkosť nesmie presiahnuť 5 MB. Predloha je uvedená v prílohe dokumentu.

Tabuľka 4.3 Časový plán záloh

Server	Typ zálohy	Frekvencia zálohovania	Čas zálohovania	Predpokladaná doba trvania zálohovania	Uchovanie záloh po dobu	Dátová náročnosť
DC2						
	BareMetal - plná	denná	21:00	3 hodiny	7 dní	230 GB
	Databáza exchange - plná	denná	0:30	1 hodina	31 dní	89 GB
	Databáza exchange - inkrementálna	hodinová	00:00-23:00	6 - 12 minút	31 dní	priem. 35 MB
HV						
	BareMetal - plná	denná	21:00	3 hodiny	7 dní	380 GB
	Hyper - V - plná (všetky hosts)	denná	3:00	4 hodiny	7 dní	340 GB
CRM						
	SQL záloha - plná	denná	20:00	1 hodina	31 dní	35 GB
	SQL záloha - inkrementálna	každé dve hodiny	00:00-23:00	6 - 12 minút	31 dní	priem. 150 MB
FS						
	Bare metal - plná	denná	21:00	30 minút	7 dní	65 GB
FS2						
	Bare metal - plná	denná	21:00	30 minút	7 dní	60 GB
WIN7						
	Záloha prebieha v rámci zálohy Hyper-V					
DC						
	Záloha prebieha v rámci zálohy Hyper-V					

4.4.2 Návrh smernice archivácie

Na základe analýzy spoločnosti odporúčame vypracovať dokument smernice archivácia s nasledujúcim znením:

Zodpovedná osoba: administrátor systému, menom Tomáš S.

Informovaná osoba: konateľ A, menom Jaroslav J.

Užívateľ: každý zamestnanec firmy GPO, spol. s r.o., ktorému bolo pridelené užívateľské meno a heslo pre prihlásenie do domény.

Na schválenie: valné zhromaždenie spoločnosti

Dátum vytvorenia a prípadnej aktualizácie.

Účel smernice: Účelom tejto smernice je stanovenie zásad pre korektnú archiváciu dát spoločnosti GPO, spol. s r.o.

Článok I.

Dôležitým prvkom v systéme archivácie je ochrana dát na úložisku. Zodpovedná osoba preto určí:

- Osobu konateľa, ktorý bude niesť zodpovednosť za dodržiavanie plánu archivácie, ako aj za uschovanie externého úložiska na zabezpečenom mieste. Zabezpečené miesto predstavuje minimálne úroveň trezoru s ochranou proti požiaru a povodni.
- Vždy minimálne s predstihom 7 dní oznámi zodpovednému konateľovi nutnosť archivácie dát v konkrétnom termíne.
- Osoba zodpovedného konateľa za žiadnych okolností nesmie používať úložisko archivácie mimo priestor na firme na to vyhradený.

Pri porušení smernice archivácie z hľadiska zabezpečenia dát nesie plnú zodpovednosť zvolená osoba konateľa. Administrátor systému zodpovedá iba za časť kopírovania dát na externé úložisko.

Článok II.

Pravidlá pre presun dát do zložky ARCHIV na súborovom serveri sú:

- Zložka slúži ako výlučne úložisko neaktívnych vypracovaných projektov a zákaziek.

- Právo na čítanie, ukladanie a zmenu súborov majú iba členovia doménovej skupiny Archív. Zaradenie a priradenie určuje zodpovedná osoba podľa náplne ich pracovnej zmluvy.
- Právo na mazanie súborov zo zložky ARCHIV má výlučne zodpovedná osoba, ktorá takýto zásah smie vykonať iba po predošlej konzultácii s informovanou osobou.
- Presun dát nastáva v bode uzavretia projektu, kedy sa už nepredpokladá jeho využívanie v rámci denných obchodných procesov.
- Zodpovednou osobou za presun uzavretého projektu je osoba, ktorá bola určená ako vedúci projektu. V prípade ak vedúci projektu nemá dostatočné práva na zápis v zložke ARCHIV, požiada o vykonanie tohto kroku svojho nadriadeného, pričom presne špecifikuje dáta určené k presunu.
-

Článok III.

Užívanie zložky ARCHIV je výlučne určené k účelom získania dát, nie k ich aktualizácií. Znamená to, že súbory je možno používať ako zdroj, pričom ich pôvodný dátum poslednej zmeny nesmie byť pozmenený.

V prípade porušenia pravidla môže byť osobe zodpovednej za vykonanú zmenu znížený bonus k mzde až do výšky 10%.

Článok IV.

Plán archivácie musí byť zostavený zodpovednou osobou. Archivácia musí byť vykonávaná minimálne každých 35 dní a musí jej časové okno byť dostatočné k prevedeniu kópie zálohy zo zložky ARCHIV umiestnenej na primárnom súborovom serveri FS.

Archivácia bude prevádzaná automaticky po zapojení externého úložiska na určené miesto. Úložisko musí ostať pripojené minimálne 8 hodín, maximálne však 24 hodín.

Na úložisko vyhradené pre účely archivácie sa zakazuje ukladať akékoľvek iné súbory okrem zložky ARCHIV.

Článok V.

Kontrola systému archivácie musí prebiehať nasledovne:

- Vždy pred prerušením spojenia s externým úložiskom archívu skontroluje administrátor systému stav zrkadlenia dát. V prípade ukončenia preverí záznam systému. Stav systému reportuje informovanej osobe.
- Informovaná osoba je povinná 14 dní po doručení správy preveriť stav prípadnej navrhnutej nápravy archivácie.
- Minimálne každé dva cykly archivácie t.j. 62 dní je administrátor systému povinný preveriť integritu dát uložených na externom archíve. Tento krok vykoná kontrolou zložky na existenciu dočasných súborov a náhodne vyberie 20 súborov, ktoré otvorí. Výsledok previerky zahrnie do správy, ktorú odovzdá informovanej osobe.

V prípade nedodržania bodov kontrolnej činnosti alebo zlyhania procesu vypracovania správy z testu bude zodpovednej osobe uložené napomenutie s možnosťou jednorazového zníženia bonusu ku mzde až do výšky 30%.

Pokiaľ dôjde následkom nekonzistencie dát archívu, k poškodeniu spoločnosti alebo ohrozeniu jej činnosti, nesú za tento stav plnú zodpovednosť zhodne zodpovedná osoba aj informovaná osoba, a to v celom rozsahu.

Článok VI.

Každá správa vytvorená v rámci internej štruktúry systému musí dodržiavať jednotnú šablónu. Vypracovanie správy, pokiaľ nejde o automaticky generovanú zostavu, prebieha v programe WORD. Následne osoba vytvárajúca správu dokument doručí cieľovej osobe výlučne elektronickou formou – emailom. Vytvorený dokument musí dodržiavať tvar REPORT_oddelenie_názovreportu a jeho veľkosť nesmie presiahnuť 5 MB. Predloha je uvedená v prílohe dokumentu.

4.5 Návrh krízového manuálu

Podobne ako u smerníc navrhneme základné zaužívané postupy vo vybraných krízových situáciách, ktoré musí spoločnosť GPO, spol. s r.o. zapracovať do dokumentácie zálohovania. Hlavným účelom krízového manuálu je rýchla a presná reakcia na nečakané udalosti, kde sa minimalizuje riziko neskorej alebo nesprávnej reakcie. Doporučujeme nasledujúci obsah dokumentu krízového manuálu:

- Dátum vytvorenia krízového manuálu.
- Dátum aktualizácie krízového manuálu.
- Meno zodpovednej osoby za vypracovanie, správu a aktualizáciu dokumentu.
- Postupy známych hrozieb podľa bodu 4.5.1.

Uvedený dokument musí byť po vypracovaní schválený valným zhromaždením spoločnosti.

4.5.1 Definície hrozieb a reakcie na nich

Výpadok produkčného servera

Okamžitá reakcia: Prvou reakciou zodpovednej osoby po zistení výpadku serveru bude identifikácia serveru mimo prevádzku. Následne zodpovedná osoba vykoná na základe hlásenia diagnostiky serveru bližšie určenie chyby. Podľa charakteru chyby tzn. či je server opraviteľný v rámci jednej hodiny, bude nasledovať ďalší postup. O výpadku a zistenej chybe informuje administrátor systému konateľa B.

Ak výpadok hardvéru je opraviteľný do jednej hodiny počas pracovnej doby, zahájí zodpovedná osoba kroky potrebné k jeho náprave.

V prípade ak odhad doby opravy serveru presiahne stanovenú hranicu jednej hodiny počas pracovnej doby, ukončí zodpovedná osoba prácu na opravách serveru a zahájí okamžite proces obnovy serveru zo zálohy.

Po ukončení procesu obnovy zo zálohy vykoná zodpovedná osoba test konektivity servera a overí funkčnosť všetkých potrebných služieb. Následne informuje zodpovedná osoba konateľa B o aktuálnom stave riešenia výpadku. Server obnovený zo zálohy musí po vykonaní testov funkčnosti plne nahradzovať nefunkčný server.

Následne zodpovedná osoba vykoná kroky potrebné k oprave nefunkčného servera. Po ukončení procesu opravy servera zodpovedná osoba vykoná zálohu servera

obnoveného zo zálohy (dočasného servera), ktorú následne obnoví do opraveného servera.

Posledným krokom bude vypnutie záložného servera a spustenie obnoveného servera, čo vykoná zodpovedná osoba, prípadne osoba poverená zodpovednou osobou.

Zodpovedná osoba za riešenie: administrátor systému

Osoba informovaná o udalosti: konateľ B

Výpadok zálohovacieho servera

Okamžitá reakcia: Po zistení výpadku zálohovacieho servera vykoná zodpovedná osoba jeho diagnostiku, z ktorej určí príčinu poškodenia a jeho rozsah. O stave informuje osobu konateľa B. Následne zahájí kroky k oprave poškodenia, a to:

- Výpadok disku z diskového poľa RAID 5

Vzhľadom k možnosti servera bude výpadok riešený formou výmeny disku za behu server (HotPlug). Následne zodpovedná osoba overí spustenie procesu obnovy diskového poľa. Po jeho dokončení overí stav diskového poľa, ako aj skutočnosť zaradenia nového disku ako tzv. rezervy – HotSpare. Zodpovedná osoba oznámi konateľovi B ukončenie obnovy a stav servera.

- Výpadok hardvérovej časti servera (mimo diskov v poli)

  Väčšina serverových komponentov je vymeniteľná za behu systému, preto zodpovedná osoba po zistení chybného hardvéru vykoná jeho výmenu za nový. Ak ide o hardvér, ktorý nie je možné vymeniť za behu, zodpovedná osoba vypne server na čas potrebný k oprave. Túto skutočnosť ohlási konateľovi B. Po výmene hardvéru zodpovedná osoba otestuje funkčnosť servera a uvedie ho do prevádzky.

- Chyba softvéru OS servera

  Pri softvérovej chybe operačného systému inicializuje zodpovedná osoba diagnostiku chyby. Použije nástroje k oprave systému. Ak tieto zlyhajú a server nie je možné užívať, vykoná proces obnovy zo záloh. Po jeho úspešnom ukončení otestuje funkčnosť serveru a informuje konateľa B o ukončení opravy a stavu serveru.

Zodpovedná osoba za riešenie: administrátor systému

Osoba informovaná o udalosti: konateľ B

Výpadok primárneho súborového servera

Okamžitá reakcia: Zodpovedná osoba po zistení výpadku primárneho súborového servera vykoná základnú diagnostiku pre zistenie príčiny výpadku.

- Pokiaľ je chyba plne odstrániteľná do desiatich minút, zodpovedná osoba ju okamžite vykoná. Oznámi konateľovi B a taktiež informuje všetkých užívateľov prostredníctvom emailu.
- Ak chyba nie je odstrániteľná do desiatich minút, zodpovedná osoba okamžite preruší diagnostiku servera. Následne na doménovom kontroléri povolí skript pre zmenu mapovania sieťových jednotiek užívateľov na nový server. Informuje konateľa B o stave a zároveň informuje užívateľov prostredníctvom emailu, aby vykonali odhlásenie a následne prihlásenie do operačného systému. Týmto krokom dôjde k nastaveniu sekundárneho súborového serveru ako primárneho. Nadväzujúc na povolenie skriptu mapovania sieťových jednotiek zodpovedná osoba pokračuje v diagnostike nefunkčného súborového servera. Po identifikácii problému reportuje ďalší postup konateľovi B, ktorý dohliada na čo najrýchlejšiu nápravu.

Po odstránení chyby a spustenia primárneho servera, administrátor zmení skript mapujúci sieťové jednotky užívateľov späť na primárny súborový server a znovu o tom emailom informuje užívateľom a konateľa B o nutnosti kroku odhlásenia a prihlásenia do operačného systému.

Následne zodpovedná osoba vypracuje písomne report, v ktorom zhodnotí, či došlo k dátovým stratám a taktiež navrhne riešenie ako výpadky daného charakteru minimalizovať. Tento report odovzdá elektronicky konateľovi B, ktorý po jeho spracovaní povolí/nepovolí vykonať administrátorovi navrhnuté kroky.

Zodpovedná osoba za riešenie: administrátor systému

Osoba informovaná o udalosti: konateľ B, užívatelia

Neautorizovaný vstup do priestorov

Okamžitá reakcia: Po zistení narušenia bezpečnostného perimetra serverovne vykoná zodpovedná osoba obhliadku miesta a stav okamžite ohlási konateľovi B. Na základe rozsahu vzniknutej škody a spôsobu narušenia musí byť na miesto povolaná polícia k riešeniu. Tento krok zabezpečí konateľ B.

Zodpovedná osoba prevedie kontrolu hardvéru za účelom zistenia jeho stavu. Prípadné nezrovnalosti okamžite ohlási konateľovi B, ktorý spolupracuje s políciou.

Zodpovedná osoba v ďalšom kroku zahájі obnovu poškodeného hardvéru a zaistí jeho plnú funkčnosť. Postupuje podľa plánu pre hardvérový výpadok produkčného servera.

Zodpovedná osoba za riešenie: administrátor systému

Osoba informovaná o udalosti: konateľ B, polícia

Požiar, zatopenie

Okamžitá reakcia: Zodpovedná osoba po zistení stavu podnikne okamžite a bez zdržovania všetky kroky vedúce k zastaveniu alebo minimalizácie hrozby. Následne informuje osobu konateľa B. V prípade potreby prevedie osoba informovaná kroky k zastaveniu hrozby tzn. v prípade živlu, ktorý presahuje možnosti lokalizácie a zastavenia informuje bezpečnostné zložky objektu, ktoré povolajú potrebné jednotky na likvidáciu.

Po ukončení pôsobenia živlu zodpovedná osoba vykoná obhliadku na zistenie rozsahu poškodenia a preverí funkčnosť všetkých zariadení v lokalite pôsobenia hrozby.

V prípade serverov postupuje podľa krízového plánu hardvérového výpadku produkčných serverov, pričom dodržuje nasledujúce poradie dôležitosti:

- Najvyššia dôležitosť – servery DC2, FS, CRM (HV)
- Vysoká dôležitosť – DPM, FS2
- Nízka dôležitosť – servery určené na testovanie, ostatné servery mimo skupiny najvyššej a vysokej dôležitosti.

Ak z prieskumu stavu po hrozbe zistí zodpovedná osoba poškodenie alebo nefunkčnosť zálohovacieho servera, bezodkladne prevedie jeho nápravu podľa krízového plánu výpadku produkčného servera, prípadne podľa plánu výpadku zálohovacieho servera. Pokiaľ z krátkodobého hľadiska tj. do 48 hodín to nie je možné,

pre obnovu ostatných serverov použije zálohy na externom úložisku, ktoré je lokalizované mimo priestory firmy GPO, spol. s r.o. O stave informuje konateľa B.

Zodpovedná osoba za riešenie: administrátor systému

Osoba informovaná o udalosti: konateľ B, vrátnica objektu, hasiči

4.6 Doporučený hardvér

Náplňou časti tohto riešenia je návrh spoľahlivého systému zálohovania a archivácie, ktorý nemôže podľa aktuálneho stavu existovať bez dodatočného zakúpenia potrebnej technológie. Všetky kroky smerujúce k výberu správneho hardvéru sú silne ovplyvnené finančnou situáciou vo firme, na ktorú taktiež pôsobí dlhotrvajúca celosvetová hospodárska kríza. Výsledkom podnikania za minulé obdobie je čistý zisk 1,2 milióna korún českých, čomu bude prispôsobený nákup hardvéru.

S ohľadom na spomínanú veľkosť firmy, cca 20 zamestnancov odporúčame technológie určené pre malé a stredné spoločnosti, kde sa očakáva kompromis ceny na úkor kvality.

4.6.1 Zálohovací server DPM

Vzhľadom k zvolenej centralizovanej štruktúre zálohovania je kvalitný zálohovací server nosným pilierom celého systému. Preto odporúčame kvalitné a pomerne cenovo prijateľné riešenie, ktoré pozostáva z bežne dostupných komponentov.

Zostava

Matičná doska serverová

SuperMicro Server X8DTi/ Intel5520-ICH10R/ LGA1366/ VGA

Procesor

INTEL Quad-Core Xeon E5606 (8MB, 2.13 GHz, 2x QPI 4.8 GT/s)

Pamäte RAM

2 x KINGSTON 4GB 1333MHz DDR3 ECC Reg w/Parity CL9 DIMM

Zdroj

FORTRON zdroj AURUM 700W, 12cm fan, akt. PFC, 80PLUS GOLD

PC Skriňa

COOLERMASTER MidT HAF 912 PLUS,ATX bez zdroje, černý

Systémový disk

2 x WD 250GB HDD Raid Edition 4/ SATA300/ Interní 3,5"/ 7200RPM/ 64MB

Cena celkom 21 800,- Kč bez DPH

Diskové pole

5 x WD 2TB HDD Raid Edition 4/ SATA300/ Interní 3,5"/ 7200RPM/ 64MB

1 x Intel® RAID Controller SRCSATAWB

Cena celkom 29 800,- Kč bez DPH

4.6.2 NAS

Okrem primárneho zálohovacieho servera je v rámci štruktúry systému zálohovania navrhnutý externý sieťový disk NAS, na ktorý odporúčame kopírovať vybrané zálohy z hlavného zálohovacieho servera. Ten by mal byť fyzicky umiestnený mimo priestory firmy, napríklad v byte člena valného zhromaždenia.

Hardvér na zakúpenie:

Iomega StorCenter px4-300d Network Storage 1TB x 6

Cena celkom 23 000,- Kč bez DPH

4.6.3 Nový súborový server

Najväčším problémom zálohovania je ochrana súborových serverov. Podstatou problému je obrovské množstvo dát, ktoré je potrebné zálohovať. V našom prípade by zálohovanie celého súborového serveru (vrátane diskových polí) predstavovalo nárast objemu o 4 TB. S prihliadnutím na rozhodnutie manažmentu spoločnosti a na dobu používania aktuálneho súborového serveru, ktorá je štyri roky sme dospeli k záveru, že najlepším riešením zálohovania file serveru bude jeho replikácia na nový fileserver.

Navrhujeme zakúpiť nový file server totožnej výroby a veľkosti diskového poľa, ktorého obstarávacia cena je 109 000,- Kč bez DPH.

4.6.4 Externý sieťový disk pre archiváciu

Súčasťou riešenia je návrh jednoduchého systému archivácie dát. Za týmto účelom doporučujeme použitie externého sieťového disku o minimálnej veľkosti 1TB. Hardvér na zakúpenie:

WD 3TB WD My Book Live/ Externí 3,5"/ LAN-RJ45

Cena celkom 3 900,-Kč bez DPH

4.7 Návrh postupu zavedenia a používania softvéru

Celý proces inštalácie a konfigurácie zálohovacieho softvéru odporúčame vykonávať výlučne v kompetencii systémového administrátora, ktorý bude postupovať na základe vypracovanej smernice zálohovania a obnovy.

4.7.1 Pre rekvizity

Proponovaným krokom pred samotnou inštaláciou je zistenie a prípadná inštalácia požadovaných súčastí servera. DPM server nesmie bežať súbežne na jednom serveri spolu s Exchange serverom alebo serverom s nastavenou aplikačnou službou, prípadne na serveri, ktorý je doménový kontrolér. Osoba vykonávajúca inštaláciu musí disponovať právami na administrátorskej úrovni. Ďalej doporučujeme preveriť prítomnosť komponentov, ktoré musia byť nainštalované pred spustením inštalácie DPM 2012, a to:

- Pre verziu Windows Server 2008 R2 nutný SP1, pre nižšie verzie upgrade,
- Microsoft .NET Framework 3.5 vrátane SP1,
- Microsoft Visual C++ 2008 redistributable,
- Windows PowerShell 2.0,
- Windows Installer 4.5 alebo vyšší,
- Microsoft Application Error Reporting.

Inštalátor automaticky skontroluje prítomnosť prerekvizít a upozorní na chýbajúce prvky.

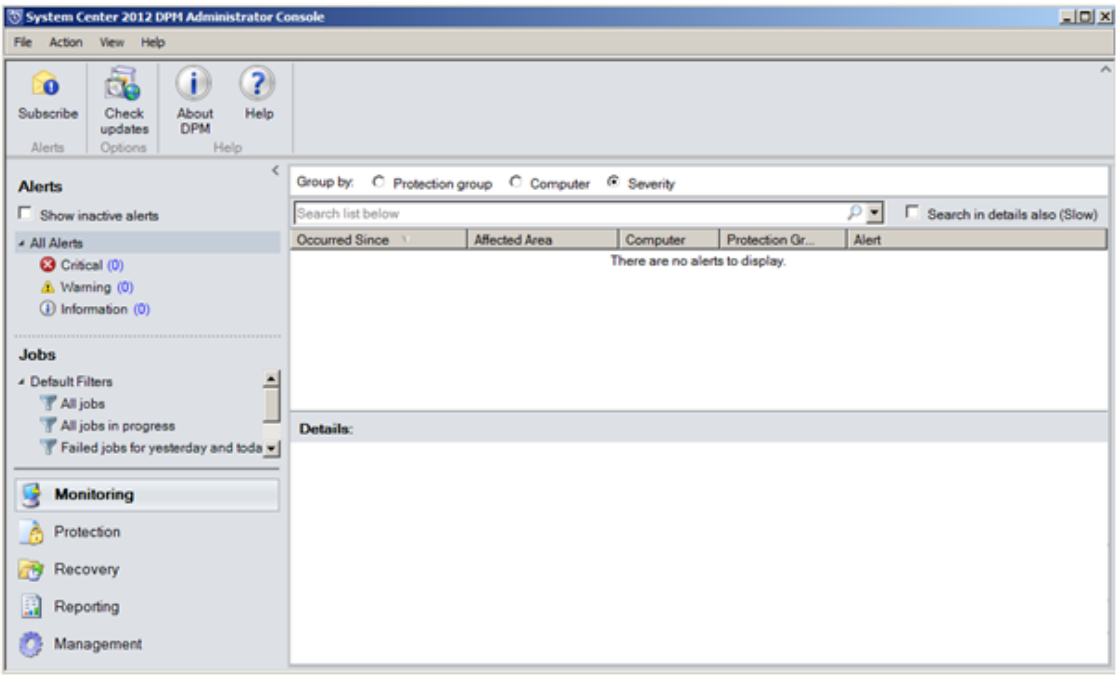
4.7.2 Inštalácia

DPM 2012 odporúčame inštalovať na OS Windows Server 2008 R2 SP1. Server disponuje systémovým diskom o veľkosti 250GB, ktorý je súčasťou poľa RAID 1 – zrkadlenie. Tým bude systém čiastočne zabezpečený pri zlyhaní jedného disku. Ochrana samotného DPM Servera proti zlyhaniu operačného systému bude riešená formou nastavenia pravidelných plných záloh serveru.

Samotný proces inštalácie je plne automatizovaný prostredníctvom sprievodcu inštaláciou, preto nepovažujeme za relevantné ho uvádzať v plnom rozsahu. Vyberieme preto iba tie najdôležitejšie kroky:

- Krok 1. V nastavení SQL databázy pre DPM server zvolíme dedikovanú inštanciu SQL servera, tzn. vytvorí sa nová databáza na DPM serveri.
- Krok 2. Pokiaľ kontrola pre rekvizít prebehne v poriadku, pokračujeme v inštalácii. V inom prípade doplníme potrebné pre rekvizity podľa bodu 4.7.1.

Inštalátor následne nainštaluje SQL server na DPM a taktiež samotný program Microsoft System Center 2012 Data Protection Manager. Po dokončení je potrebný reštart systému. Pokiaľ inštalácia prebehla korektne, po naštartovaní servera je možné spustiť administračnú konzolu (Obrázok 4.2).



Obrázok 4.2 Administračné rozhranie DPM 2012

V nasledujúcom kroku odporučíme kroky k inštalácii agentov na host-y. DPM 2012 pracuje na princípe server – agent, kde na hostiteľský server je nainštalovaný agent, ktorý vykonáva príkazy definované hlavným serverom. Jeho inštalácia je preto

ďalším krokom k správnemu fungovaniu systému záloh a obnovy. Agentov bude potrebné inštalovať na všetky servery, ktoré plánujeme zálohovať alebo ktoré budú slúžiť ako miesto obnovy zo záloh (kopírovanie dát na zdieľaný priečinok), a to sú servery DC, DC2, HV, CRM, FS, a nový FS2. Súborové servery FS a FS2 odporúčame zálohovať iba v rámci operačného systému bez diskových polí. Zároveň s inštaláciou agentov zálohovania musí prebehnúť kontrola serverov na povolenú funkciu Windows záloha serveru.

4.7.3 Konfigurácia

Časový plán záloh ako aj doby uchovania jednotlivých záloh sú uvedené v smernici zálohovania, Tabuľka 4.3 Časový plán záloh.

Prvým navrhovaným krokom konfigurácie zálohovacieho softvéru je vytvorenie diskového poľa o veľkosti 6 TB s použitím technológie RAID 5 na radiči Intel® RAID Controller SRCSATAWB, pričom ide o 4 x 2 TB disky a piaty disk o zhodnej veľkosti ako HotSpare (záložný disky). Vytvorené pole sa po inicializácii priradí do DPM 2012 ako úložisko, kam budú ukladané nastavené zálohy.

Softvér DPM 2012 pracuje so skupinami záloh rovnakého typu tzv. chránené skupiny. Druhým odporúčaním v postupe konfigurácie je vytvorenie týchto chránených skupín (protection groups) podľa typu zálohy tzn.:

- BareMetal[10] protection group
- Hyper-V protection group
- SQL protection group
- Exchange protection group

Po vytvorení protection group prejde konfigurácia do kroku pridania serverov do vytvorených skupín podľa časového plánu záloh. Administrátor ich pridá pomocou sprievodcu. Týmto krokom bude ukončená konfigurácia softvéru zálohovania DPM 2012. Systém automaticky prevedie zálohy v najbližšom stanovenom čase.

4.7.4 Doporučenie kontroly stavu systému zálohovania

Konzola softvéru umožňuje centralizovane sledovať všetky informácie a problémy systému zálohovania. Odporúčame zodpovednej osobe využívať vstavanú funkciu monitorovania systému, kde sú zobrazené všetky varovania a chyby systému

[10] Skratka BareMetal v preklade kompletná záloha servera umožňujúca obnovu na iný hardvér.

zálohovania. Najväčšiu pozornosť doporučujeme venovať kritickým chybám, ktorých následkom je nemožnosť obnovy alebo nefunkčnosť či poškodenie systému. Taktiež monitorovacia funkcia umožní administrátorovi kontrolovať prebiehajúce úlohy a vykonané úlohy s uvedením ich reálnej dátovej náročnosti.

Pri riešení prípadných problémov hlásených systémom navrhujeme využívať databázu znalostí spoločnosti Microsoft dostupnú prostredníctvom pomocníka programu Data Protection Manager 2012.

4.7.5 Postupy obnovy dát zo zálohy

Pre dodržanie nariadenia stanoveného v smernici o zálohovaní a obnove, časti testovania záloh navrhujeme, aby zodpovedná osoba postupovala v rámci zálohovacieho softvéru nasledovne.

Pre využitie funkcionalít obnovy zo záloh uložených na zálohovacom serveri zodpovedná osoba vyberie na karte „obnova“ konkrétny server, ktorého sa obnova týka. Následne rozbalením stromovej štruktúry zobrazí všetky zálohované skupiny (aplikácie) servera a napríklad pre celkovú obnovu servera vyberie skupinu BareMetal. V pravej časti administračnej konzoly zvolí čas a dátum vybraného bodu obnovy a zvolí možnosť obnoviť. Následne sa aktivuje sprievodca obnovením do vybraného bodu, kde administrátor určí kam sa bude záloha kopírovať a v prípade potreby nastaví obmedzenie dátového toku, aby tak predišiel zahlteniu internej siete a umožnil jej plynulú prevádzku počas. Dôjde ku kopírovaniu zálohy na miesto obnovy, odkiaľ je zvolená ako zdroj pri inštalácií servera. Úloha DPM servera na obnove sa týmto krokom končí.

4.8 Návrh konfigurácie záloh súborového servera

Z návrhu hardvéru vyplýva nasledujúce odporúčanie konfigurácie zrkadlenia/zálohovania dát súborového servera na nový súborový server. Zálohovanie systémových súborov bude riešené podľa smerníc zálohovania.

4.8.1 Návrh hardvérovej konfigurácie

Návrh hardvérovej konfigurácie zálohovania dát súborového servera spočíva v zakúpení a inštalácií nového súborového servera podľa časti 4.6.3. Následne doporučujeme nastaviť diskové pole RAID a ostatné parametre zhodne s pôvodným serverom FS. Princípom „zálohovania“ je pri použití zrkadlenia možnosť okamžitého prepnutia na sekundárny server v prípade výpadku primárneho servera. Tento krok vykoná komplexne administrátor systému.

4.8.2 Návrh softvérovej konfigurácie

Podľa sekcie 3.5 odporúčame pre použitie na replikáciu súborového serveru softvér MirrorFolder, ktorý zabezpečuje zrkadlenie vybraných sieťových zložiek na sekundárny súborový server.

Program MirrorFolder musí byť nainštalovaný na primárny súborový server. Nastavenie administrátorom systému je pomerne jednoduché. Administrátor vytvorí na sekundárnom serveri zložky zhodné s primárnym serverom. Ďalej musí nastaviť ako zdroj zrkadlenia zložky na primárnom serveri a ako cieľ sekundárny server. Softvér automaticky inicializuje zrkadlenie dát do cieľových adresárov. Priradenie priorít zrkadlenia zodpovedná osoba nastaví podľa smernice zálohovania a obnovy.

Konfiguráciu vykoná zodpovedná osoba – správca systému, ktorý úspešné spustenie zrkadlenia súborového serveru reportuje konateľovi B. Ten využije nástroje popísané v smernici zálohovania a obnovy k priebežnej kontrole stavu systému.

4.9 Návrh záloh totálneho zlyhania

Všetky doposiaľ spomínané časti systému zálohovania sú navrhnuté s ohľadom na minimalizáciu časového okna záloh a taktiež s prihliadnutím na zabezpečenie serverov po všetkých stránkach. Výsledkom je centralizácia celého systému zálohovania do miestnosti s ostatnými servermi a zariadeniami. Tento stav doporučujeme ošetriť z hľadiska totálneho zlyhania a vytvoriť núdzovú zálohu mimo centralizovaný objekt (Obrázok 4.1).

Navrhované riešenie núdzovej zálohy pozostáva z hardvéru (4.6.4) Iomega StorCenter px4-300d Network Storage s úložnou kapacitou 4 TB, pričom doporučujeme nastaviť pole RAID 6, ktoré je odolné voči výpadku dvoch diskov. Toto zariadenie bude umiestnené mimo priestory a budovu spoločnosti GPO, spol. s r.o., lokalita sa riadi smernicou zálohovania a obnovy dát. Po technickej stránke odporúčame na základe zistení možnosti konektivity využiť dostupnosť širokopásmového rýchleho pripojenia k internetu, ktoré bude vyčlenené na prenos dát na NAS mimo objekt firmy. Zabezpečenie prenosu bude prebiehať pomocou už používanej šifrovanej L2TP VPN[11]. Frekvencia a dáta určené na zálohovanie na externý NAS budú špecifikované v smernici zálohovania a obnovy.

Na základe skúseností doporučujeme vykonávať zálohy dát na NAS z DPM servera a sekundárneho súborového servera FS2. Eliminuje sa tým riziko zníženia času odozvy primárneho súborového serveru FS. Taktiež navrhujeme vykonať prvotné zálohovanie dát na NAS v rámci internej siete firmy a až následne zariadenie preniesť na vzdialené miesto.

V rámci centralizácie systému odporúčame použiť na kopírovanie dát zo sekundárneho FS2 vstavaný nástroj ROBOCOPY s príkazom MIR, ktorý zabezpečí zrkadlenie vybraných súborov. Rovnaký nástroj platí aj pre využitie na serveri DPM.

Konfiguráciu vykoná zodpovedná osoba – správca systému, ktorý úspešné spustenie kopírovania/zálohovania dôležitých dát (špecifikovaných v smernici zálohovania a obnovy) na externý disk mimo objekt spoločnosti reportuje konateľovi B. Ten využije nástroje popísané v smernici zálohovania a obnovy k priebežnej kontrole stavu systému.

[11] Skratka významu Virtual Private Network, v preklade virtuálna privátna sieť.

4.10 Návrh archivácie

S prihliadnutím na aktuálnu finančnú situáciu spoločnosti návrh archivácie dát spočíva v rozšírení existujúceho súborového servera, na ktorom bude vyčlenený nový logický disk určený archívu.

Korektným riešením by bolo zakúpenie páskovej jednotky o veľkosti minimálne 2TB, kde je možné bezpečne dlhodobo uchovávať dáta. S tým sú spojené náklady v objeme 40 až 50 tisíc korún českých. Takýto rozsah riešenia doporučujeme zaviesť v horizonte troch až štyroch rokov, a to na základe neustále rastúceho objemu aktívnych dát a nutnosti presunu ich časti do archívu.

Navrhujeme preto uchovávanie zložky ARCHIV na externý disk využiť hardvér podľa kapitoly 4.6.4. Princíp archivácie bez použitia páskovej jednotky bude ukladanie na spomínaný externý sieťový disk, pričom zložka ARCHIV na súborovom serveri bude totožná s obsahom externého disku. Frekvencia vytvárania archívu je špecifikovaná v smernici archivácie, nemala by však presiahnuť rámec dvoch týždňov.

Technológia doporučená pre vytváranie pravidelných kópií založená na internom nástroji operačného systému Robocopy s príkazom MIR zabezpečí zhodnosť dát na oboch miestach. Externý disk odporúčame uchovávať mimo priestory spoločnosti v chránenej schránke.

Zodpovednosť, povinnosti, postupy kontroly a prípadné sankcie sú uvedené v smernici archivácie.

4.11 Ekonomická náročnosť navrhovaného riešenia

Návrh systému zálohovania a obnovy obsahuje potrebné hardvérové a softvérové prvky, ktorých obstaranie bolo ovplyvnené finančnou situáciou firmy GPO, spol.s r.o.

Tabuľka 4.4 Ekonomická náročnosť návrhu

Typ	Predmet	Cena za kus	Počet	Náklady bez DPH celkom
Hardvér				
	DPM server	21 800,00 Kč	1	21 800,00 Kč
	Diskové pole WD 2TB	22 500,00 Kč	1	19 500,00 Kč
	Diskový radič Intel® RAID Controller SRCSATAWB	7 300,00 Kč	1	7 300,00 Kč
	Externý NAS Iomega StorCenter px4-300d	23 000,00 Kč	1	23 000,00 Kč
	FileServer SuperMicro 12 vrátane HDD	109 000,00 Kč	1	109 000,00 Kč
	Externý sieťový disk WD 3TB WD My Book Live	3 900,00 Kč	1	3 900,00 Kč
Za časť				**184 500,00 Kč**
Softvér				
	Microsoft System Center 2012 ako súčast MS Action Pack Solution Provider	7 500,00 Kč	1	7 500,00 Kč
	MirrorFolder v5.1	1 200,00 Kč	1	1 200,00 Kč
Za časť				**8 700,00 Kč**

Analýza a návrh			
Spracovanie analýzy aktuálneho stavu zamestnancom	240,00 Kč	31	7 440,00 Kč
Návrh a konfigurácia systému zálohovania a obnovy zamestnancom	220,00 Kč	42	9 240,00 Kč
Návrh a konfigurácia systému archivácie zamestnancom	220,00 Kč	12	2 640,00 Kč
Za časť			**19 320,00 Kč**
Internetové pripojenie			
UPC FIBER POWER 120Mb/S - / 10Mb/s	990,00 Kč	12	11 880,00 Kč
Za časť			**11 880,00 Kč**
Servis systémov			
Ročný servis systémov zamestnancom	200,00 Kč	280	56 000,00 Kč
Za časť			**56 000,00 Kč**

Náklady celkom za implementáciu s ročným ohľadom **280 400,00 Kč**

Spoločnosť GPO, spol. s r.o. generovala za účtovné obdobie 2010 zisk vo výške 1,2 milióna korún českých. Z toho vyplýva, že investícia do systému zálohovania a obnovy predstavuje približne 23 percent z celkového zisku. S prihliadnutím na rizikovosť chránených dát a ich dôležitosť v obchodných procesoch spoločnosti je investícia do tak komplexného systému návratná v okamihu väčšieho výpadku.

Vyčíslenie strát pri výpadku súborového servera:

Súborový server je centralizované a jediné úložisko dát vytvorených zamestnancami, čím pri jeho výpadku dochádza k vysokým stratám. Odhadovaná hodnota dát vytvorených počas 24 hodín je s prihliadnutím na objem zákaziek 26 000,-, preto je prípadné škody možné vyčísliť nasledovne:

- Výpadok po dobu 24 hodín 26 000,- Kč
- Výpadok po dobu 7 dní 182 000,- Kč
  - náklady na platy zam. 15 000,- Kč
  - penále z omeškania 5 000,- Kč

Výpadok 7 dní celkom **202 000,- Kč**

Zohľadnili sme výpadky, kde je predpoklad obnovenia dát do ich plného stavu. Pri situácii, kedy dôjde k totálnej strate dát bez možnosti obnovenia, je ich hodnota súčtom uskutočnených zákaziek za obdobie existencie spoločnosti, t.j. 10 rokov.

Z uvedených faktov vyplýva, že návratnosť investície do systému zálohovania, obnovy a archivácie pri výpadku súborového servera je vo veľmi krátkej dobe.

ZÁVER

Vlastný návrh a implementácia systému zálohovania a obnovy naplnila stanovené ciele. Navrhnutý systém prináša spoločnosti GPO, spol. s r.o. komplexnú ochranu v prípade výpadku komponentov serverov, softvérovej chyby, živelného ohrozenia alebo totálneho zlyhania. Firma je schopná v závislosti na typu zlyhania a jeho rozsahu obnoviť beh zariadenia do jednej hodiny od výpadku. Taktiež prepracovaný je aj návrh zálohovania kritických dát systému ako interná databáza informačného systému a emailová databáza, kde v prípade chyby systému alebo hardvéru je zodpovedná osoba stanovená v smernici schopná podľa presne určených postupov obnoviť databázu až do stavu poslednej celej hodiny pred výpadkom.

V rámci finančných možností spoločnosti je vyriešená i otázka archivácie, ktorá zabezpečí pravidelné ukladanie archívu na disk na bezpečnom mieste.

Napriek komplexnosti aktuálneho návrhu systému zálohovania a obnovy odporúčame spoločnosti GPO, spol. s r.o. v dobe maximálne 16 mesiacov investovať do kúpy nového zálohovacieho servera, ktorý bude plniť funkciu záložného zálohovacieho servera, nakoľko navrhnutý softvér plne podporuje štruktúru Primary/Secondary server.

ZOZNAM POUŽITEJ LITERATÚRY

(1) Consulting, Convenio. *Klasifikace dát.* [Dokument] Praha : Convenio Consulting odštěpný závod MHM computer s.r.o., 2012.

(2) Nelson, Steven. *Pro Data Backup and Recovery.* New York : Apress, 2010. s. 350. 978-1430226628.

(3) De Guise, Preston. *Enterprise Systems Backup an Recovery: A Corporate Insurance Policy.* Boca Raton : Auerbach Publications, 2008. s. 360. 9781420076394.

(4) Buchanan, Steve. *Microsoft Data Protection Manager 2010.* Birmingham : Packt Publishing, 2011. 978-1849682022.

(5) Curtis, Preston. SearchDataBackup. *Archiving storage vs. data backup storage.* [Online] 01 2010. [Dátum: 05. 05 2012.] http://searchdatabackup.techtarget.com/feature/Archiving-storage-vs-data-backup-storage-The-dos-and-donts-of-using-backups-and-data-archives#q2.

(6) Mullins, Craig. THE DATA ADMINISTRATION NEWSLETTER. *Database Archiving for Long-Term Data Retention.* [Online] 01. 10 2006. [Dátum: 01. 05 2012.] http://www.tdan.com/view-articles/4591.

(7) Borghoff, Uwe, Rodig, Peter a Scheffczyk, Jan. *Long-Term Preservation of Digital Documents: Principles and Practices.* Berlin : Springer, 2006. 978-3642070174.

(8) Lukášová, Jitka. Podnikatel.cz. *Jak ve firmě archivovat doklady?* [Online] 15. 10 2009. [Dátum: 7. 5 2012.] http://www.podnikatel.cz/clanky/jak-ve-firme-archivovat-doklady/.

(9) Kellet, Megan. SearchDataBackup. *Choosing a data archiving strategy.* [Online] 31. 03 2010. [Dátum: 09. 05 2012.]

http://searchdatabackup.techtarget.com/news/1507559/Choosing-a-data-archiving-strategy-Disk-archiving-vs-tape-archiving.

(10) H. Gregory, Peter. *IT Disaster Recovery Planning For Dummies.* Hoboken : Wiley Publishing, 2007. 978-0470039731.

ZOZNAM OBRÁZKOV

ZOZNAM TABULIEK

ZOZNAM PRÍLOH

GPO, spol. s r.o.,
Bratislavská 1234/31b, 602 00 Brno

Správa č. .....

Predmet správy:

Obsah správy:

Vypracoval: Dňa: Odoslané:

Prijal: Dňa:

IČO: 57368239 DIČ: CZ57368239 web: www.gpo.cz tel. 771 117 771