Návrh datového úložiště pro potřeby forenzní laboratoře

Bc. Ondřej Kolek

Diplomová práce
2016

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2015/2016

ZADÁNÍ DIPLOMOVÉ PRÁCE
(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Ondřej Kolek**
Osobní číslo:	**A14431**
Studijní program:	**N3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Forma studia:	**prezenční**
Téma práce:	**Návrh datového úložiště pro potřeby forenzní laboratoře**
Téma anglicky:	**Data Storage for Forensic Laboratory Needs**

Zásady pro vypracování:

1. **Zpracujte ucelený přehled právních aspektů vztahujících se na datové úložiště pro digitální forenzní laboratoř.**
2. **Proveďte analýzu, vyhodnocení rizik a nastavte míru bezpečnosti informací dle mezinárodních standardů.**
3. **Navrhněte strukturu a implementaci datového úložiště.**
4. **Porovnejte varianty uložení datového úložiště v prostorách laboratoře a v serverovně.**
5. **Vybranou variantu realizujte v testovacím provozu.**

Rozsah diplomové práce:

Rozsah příloh:

Forma zpracování diplomové práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **BECK Pall, TATE, Jon, Hektor IBARRA, Shanmuganathan KUMARAVEL a Libor MIKLAS. Introduction to Storage Area Networks [online]. 7. Armonk, New York, U.S., 2016 [cit. 2016-02-04]. ISBN 0738441430. Dostupné z: https://www.redbooks.ibm.com/redbooks/pdfs/sg245470.pdf.**
2. **GNANASUNDARAM, Somasundaram a Alok SHRIVASTAVA. Information storage and management: storing, managing, and protecting digital information in classic, virtualized, and cloud environments. 2nd ed. Hoboken, N.J.: John Wiley & Sons, 2012, xxi, 489 p.**
3. **ISO/IEC 27000:2014: Information technology – Security techniques – Information security management systems – Overview and vocabulary (2014).**
4. **Proceedings of the 14th European Conference on Cyber Warfare and Security. United Kingdom: Academic Conferences and Publishing International Limited, 2015. ISBN 978-1-910810-28-6. ISSN 2048-8602.**
5. **Storage Security: Encryption and Key Management. In: The Storage Networking Industry Association: Advancing Storage and Information Technology [online]. Colorado Springs, 2015 [cit. 2016-02-04]. Dostupné z: http://www.snia.org/sites/default/files/technical_work/SecurityTWG/SNIA-Encryption-KM-TechWhitepaper.R1.pdf.**

Vedoucí diplomové práce: **Ing. David Malaník, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **5. února 2016**

Termín odevzdání diplomové práce: **16. května 2016**

Ve Zlíně dne 5. února 2016

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

doc. Mgr. Milan Adámek, Ph.D.
děkan

doc. RNDr. Vojtěch Křesálek, CSc.
ředitel ústavu

Jméno, příjmení: Ondřej Kolek

Název diplomové práce: Návrh datového úložiště pro potřeby forenzní laboratoře

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že diplomová práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji diplomovou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – diplomovou práci nebo poskytnout licenci k jejímu využití jen připouští-li tak licenční smlouva uzavřená mezi mnou a Univerzitou Tomáše Bati ve Zlíně s tím, že vyrovnání případného přiměřeného příspěvku na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše) bude rovněž předmětem této licenční smlouvy;
- beru na vědomí, že pokud bylo k vypracování diplomové práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky diplomové práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na diplomové práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně, dne

.....
podpis diplomanta

ABSTRAKT

Obsahem této diplomové práce je návrh struktury a implementace datového úložiště pro forenzní laboratoř v prostorách univerzity. Úvodní část práce je zaměřena na právní aspekty, normy a další bezpečnostní doporučení, které jsou nezbytné pro dosažení odpovídající úrovně bezpečnosti. V praktická části práce jsou srovnány produkty firemního datového úložiště s dvěma vlastními navrženými variantami. Dále je zde zpracována analýza a vyhodnocení rizik. Nakonec je nastíněna realizace a testování jedné z navržených variant.

Klíčová slova: Návrh datového úložiště, NAS, SAN, DAS, bezpečnost datového úložiště, analýza rizik, forenzní laboratoř, ISO/IEC 27005, ISO/IEC 27040.

ABSTRACT

This diploma thesis deals with design of the structure and implementation of data storage for a forensic laboratory on the university's premises. The introductory part is focused on legal aspects, standards and other safety recommendations which are necessary to achieve an adequate level of safety. The practical part of this work is about the comparison of enterprise products with two proposed options of NAS configuration. Then there is an analysis and risk assessment. In the end there is outline of implementation and testing of one of the proposed variants.

Keywords: Proposal of data storage, NAS, SAN, DAS, security of data storage, risk analysis, forensic laboratory, ISO/IEC 27005, ISO/IEC 27040.

Tímto bych chtěl poděkovat především vedoucímu své diplomové práce, kterým byl Ing. David Malaník, Ph.D., za věcné připomínky, rady a veškerý čas, který mi věnoval. Dále bych rád poděkoval také Ing. Mariánu Svetlíkovi za poskytnuté rady při tvorbě této práce.

Motto: If you are not willing to learn, no one can help you. If you are determined to learn, no one can stop you.

Prohlašuji, že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

OBSAH

ÚVOD

Digitální forma důkazů je stále častěji součástí vyšetřování a soudních sporů. Avšak v dnešní době tyto digitální důkazy už nejsou pouze součástí počítačové nebo informační kriminality, nýbrž je nutné si uvědomit, že zasahují do každodenního života každého z nás. A jelikož nám současný trend naznačuje zvyšující se podíl páchané trestné činnosti prostřednictvím počítačů, je zřejmé taktéž rostoucí počet vyšetřovacích institucí působících v oblasti počítačové trestné činnosti.

Uchovávání informací je ústředním pilířem informačních technologií. Každým okamžikem je vytvářeno obrovské množství digitálních dat, ať už samotnými jedinci nebo korporátními subjekty. Tyto informace pak musí být uloženy, chráněny, optimalizovány a řízeny.

Není to tak dávno, co uchovávání dat bylo zprostředkováno pouze za pomocí hromady kompaktních disků nebo pásek připojených k zadní straně počítače k ukládání dat. Dokonce už i dnes výrobci chápou zásadní úlohu, že informační technologie k ukládání dat hrají důležitou roli v dostupnosti, výkonu, integraci a optimalizaci celé IT infrastruktury. Během posledních dvou desetiletí se uchovávání dat vyvinulo do vysoce sofistikovaných technologií, které poskytují širokou škálu řešení pro ukládání, správu, komunikaci, ochranu a sdílení digitálních informací.

S exponenciálním nárůstem informací a rozvojem sofistikovaných produktů, se však také objevila poptávka po profesionálních řešeních dimenzovaných na mnohonásobně vyšší nároky. Ne vždy je ale nezbytné, aby si daná instituce pořizovala drahý systém, který třeba ani zcela nevyhovuje vytyčeným požadavkům. Stačí, když disponuje dostatečnými zdroji, IT odborníky a poté existují možnosti, jak si takové datové úložiště navrhnout přesně podle vlastních představ. Tato práce se zabývá výběrem vhodných variant datového úložiště nejen z oblasti hotových firemních konfigurací, ale také vlastním návrhem nejvhodnější struktury s důrazem na splnění stanovených požadavků a stejně tak na dosažení optimálního výkonu a odpovídající bezpečnosti podle právních aspektů a norem. Dále se práce bude zabývat analýzou a vyhodnocením rizik plynoucích z umístění a samotné struktury datového úložiště.

I. TEORETICKÁ ČÁST

1 VYMEZENÍ PROBLEMATIKY A CÍLE PRÁCE

Tato diplomová práce se zabývá problematikou návrhu struktury a implementace datového úložiště pro potřeby laboratoře forenzních technologií, která v rámci své běžné činnosti může přijít do styku i s citlivými údaji. Z takového je nezbytné klást důraz na požadavky v oblasti bezpečnosti a také výkonu. Navržená řešení by měla splňovat požadované specifikace, jenž byly stanoveny následovně:

- Datové úložiště o kapacitě přibližně ~30 TB,
- Možná rozšiřitelnost úložné kapacity,
- Redundantní připojení do počítačové sítě (4 x 1GiB Ethernet),
- Redundantní napájení (2 a více zdrojů),
- Implementace ochranných systémů proti ztrátě dat,
- Dostatečný výkon pro paralelní přístup a práci vícera uživatelů.

Práce bude taktéž zahrnovat srovnání komplexních podnikových řešení (*enterprise*) a variant datového úložiště postaveného ze samostatně dostupných hardwarových komponent.

2 VÝZNAM FORENZNÍCH LABORATOŘÍ V BEZPEČNOSTI IT

V dnešní době pojem bezpečnost informací ruku v ruce se zvyšujícím se počtem digitálních zařízení stále nabývá na svém významu. Nejčastěji je pojem bezpečnost informačních technologií skloňován v podnikovém sektoru a firmy se zavedenou certifikací např. pro systém managementu jakosti dle normy ISO 9001, nebo se zavedeným modelem ISMS (Systém řízení bezpečnosti informací) se následně stávají v očích svých klientů kvalitnějšími a důvěryhodnějšími partnery.

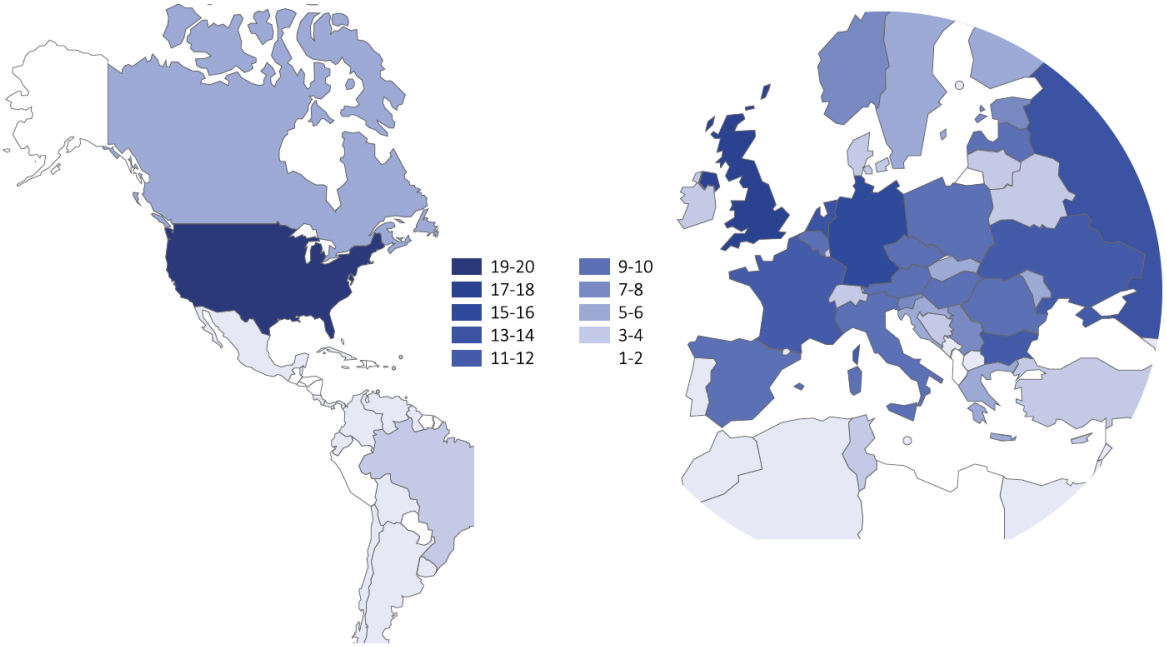
Přesto jsme svědky rostoucí míry počítačové kriminality a s tím zvyšující se poptávky po vyšetřovacích institucích působících v oblasti počítačové trestné činnosti. Obor digitální forenziky se objevil jako jeden z nejrychleji měnící se a rozvíjející se vyšetřovací specializace v širokém sortimentu trestních a občanskoprávních věcech. Také můžeme sledovat vzestup požadavků na předložení digitálních důkazů u různých justičních orgánů po celém světě, kde digitální důkaz předložený v trestním řízení a splňující jisté požadavky usnadňuje cestu k dalším důkazům a to nejen digitálním. Aby tato zkoumaná data v České republice měla forenzní charakter, musí splňovat zásady legality, integrity, přezkoumatelnosti a nepodjatosti. V USA tyto zásady řeší standardy Daubert nebo Frye. [1], [2]

Při zkoumání digitální stopy je neodmyslitelnou součástí uvědomit si co je možné od ní očekávat, na co poukazuje a jaké fakta lze díky této digitální stopě prokázat. Je proto více než žádoucí, aby forenzní zkoumání bylo úzce spjato s vyšetřovateli a nedošlo tak k mylným závěrům. Dále pak v případě spolupráce (přejímání výsledků zkoušek) mezi jednotlivými laboratořemi napříč cizími zeměmi je doporučeno získat akreditaci příslušného orgánu, jenž uzavřel dohody o vzájemném uznávání s podobnými orgány v jiných zemích. V ČR je takovým to orgánem Český institut pro akreditaci, jenž provádí nezávislé posouzení způsobilosti mimo jiné i pro normu ČSN EN ISO/IEC 17025:2005. Tato norma obsahuje podstatné požadavky, jenž musí zkušební a kalibrační laboratoř splňovat k prokázání způsobilosti a schopnosti dosahovat technicky platných výsledků. Takto akreditovaná laboratoř má následně usnadněnou spolupráci s jinými orgány v případě výměny informací a zkušeností. [2], [3]

2.1 Počítačová kriminalita v dnešní době

Statistiky z roku 2015 vydanými Europolem, konkrétně kybernetickým centrem (EC3), nám jasně ukazují, že rychlá a spolehlivá ICT infrastruktury nacházející se převážně na území

západní Evropy, je zneužívána počítačovými zločinci k hostování škodlivého obsahu a útokům na cíle uvnitř i vně EU. V Evropě je takto hostováno přibližně 13% celosvětově škodlivých URL adres (tj. online zdrojů s obsahem škodlivého kódu, nebo takové, jenž přesměrovávají na weby s nebezpečným obsahem). Nejvýznamnější podíl připadá Nizozemsku, zatímco převážně Německo, Velká Británie a Portugalsko tvoří zbylou část. Dále je to opět Německo, Velká Británie, Nizozemí, Francie a Rusko kde je hostováno znatelné množství C&C infrastruktur a phishingových domén v celosvětovém měřítku. A nakonec mezi země, které jsou na vrcholu žebříčku spamu patří Itálie, Německo, Nizozemí, Rusko a Španělsko. [4], [5]



Obrázek 1 – Mapa kyberkriminality [4]

Výše uvedená mapa kyberkriminality zobrazuje země, kde při vyšetřování počítačové trestné činnosti investigativní orgány identifikovaly dané pachatele nebo protiprávní infrastruktury. Tato mapa zahrnuje jak data související s počítačovou kriminalitou přímo, tak i případy, ve kterých byly využity IT technologie pouze jako podpůrná forma v páchání jiné protiprávní činnosti, avšak nejsou zde zahrnuta vyšetřování online sexuálního zneužití dětí. S výjimkou vyšetřování, jenž vedla do USA, Velké Británie a Německa, méně než třetina vyšetřování vedla k potřebě řešit tuto činnost skrze smlouvy o vzájemné právní pomoci (MLAT). Šlo o země, kde se vyskytovali identifikovaní pachatelé nebo C&C infrastruktury. [4], [5]

2.1.1 Dětská pornografie

Další samostatnou oblastí počítačové kriminality je dětská pornografie. Podle poslední výroční zprávy z roku 2014 vydané kybernetickým centrem EC3 ve spolupráci s organizací INHOPE, je majoritní většina kompromitujícího materiálu šířena skrze P2P sítě, přesto zde funguje značné množství komerčních hostingů s touto tématikou a nezanedbatelná část se jich nacházela také na území ČR. [6], [9]

Tabulka 1 – Počty nahlášený webových stránek s kompromitujícím materiálem [6]

INHOPE	Říjen - Prosinec 2011	Leden - Prosinec 2013	Leden - Červen 2014
URL adresy podezřelé z komerční distribuce	1138	5236	2940

Když se proto podíváme na statistiky z předešlých let, lze pozorovat, že v roce 2013 bylo registrováno až 5236 URL adres podezřelých z komerčně využívaného materiálu dětské pornografie. Tyto adresy tvoří pouze 13% celkového množství nahlášených adres. Zbylých 87% tvoří nekomerční weby. Ze statistik pak vyplývá, že počet webových stránek s kompromitujícím materiálem zřízených za účelem zisku přibývá.

V České republice bylo ještě v roce 2013 nahlášeno 125 závadných stránek, nutno dodat, že do roku 2014, však znění Trestního zákoníku (z. č. 40/2009 Sb.) neposkytovalo před sexuálními útoky na děti a obchodováním s lidmi takovou míru ochrany, jakou vyžadovala Evropská unie a novela zákona měla teprve vejít v platnost. [8]

2.1.2 Podvody s platebními kartami

V roce 2013 počet vydaných platebních karet v Evropské unii dosáhl přibližně 760 miliónů, což představuje přibližně 1,5 platební karty na obyvatele a počet transakcí se vyšplhal na 43,6 miliard eur, což činí průměrně téměř 50 eur za transakci. Rostoucí podíl bezhotovostních plateb motivuje na jedné straně počítačové zločince ve vynalézání nových metod útoků a na straně druhé vznik protiopatření a bezpečnostních prvků s cílem ochránit své klienty i podnikání. Téhož roku celková hodnota podvodných transakcí provedených pomocí karet vydaných v rámci SEPA, dosáhla 1,44 miliardy eur a to představuje nárůst o 8% oproti před-

chozímu roku. V roce 2014 pak došlo k zatčení pěti skupin organizovaného zločinu zneužívající elektronické platby. Skupiny napadly přes 50 tis. kreditních karet a odcizili více než 30 miliónů eur. [5], [7]

2.1.3 Mezery v systému potírání počítačové kriminality

Navzdory úspěchům potírající počítačovou kriminalitu, známé překážky ve vyšetřování stále přetrvávají. Jde hlavně o:

- Nedostatek možností justiční spolupráce se zeměmi mimo EU. (Východoevropské státy, včetně Ruska a zemí jihovýchodní Asie).
- Neefektivní způsob výměny informací nezbytných pro vyšetřování, zejména s osobami v soukromém sektoru.
- Nejasné a odlišné právní rámce napříč zeměmi EU, zejména v souvislosti s používáním různých donucovacích opatření, práci v utajení, online detekci, zákonného odposlechu, dešifrování atp.

3 PRÁVNÍ ASPEKTY BEZPEČNOSTI INFORMAČNÍCH SYSTÉMŮ

V legislativě České republiky lze nalézt několik zákonů, jenž řeší oblast zabezpečení informačních systémů. Nicméně je záhodno podotknout, že celá problematika je dosti složitá a samotnou definicí pojmu si lze vyložit v různém rozsahu. Nabízí se tedy dvě oblasti, jak na danou problematiku nahlížet:

1. **Právní normy** – s různou úrovní omezení své věcné a osobní působnosti. Taktéž obsahují některé kogentní pravidla, jenž jsou rozvedena více či méně do detailů podrobnějšími sekundárními (podzákonnými) předpisy.
2. **Standardy (normy)** – jedná se hlavně o technické normy, které jsou vytvářeny nadnárodními organizacemi, tudíž odráží vlastnosti institutů pro normalizaci a zpravidla odkazují na právní normy. [10]

3.1 Právní normy

Na potřebu zabezpečení informačního systému ve forenzní laboratoři lze aplikovat pouze pár právních norem, které se věnují rozličným oblastem. V podstatě neexistuje jasné právní nahlížení na problematiku v podobě právní normy, která by splňovala pojmové znaky. A po důsledném přezkoumání právních regulativů je možné konstatovat absenci obecných a vždy důsledně aplikovatelných právních norem, které by napřímo tuto problematiku řešily. Nutno také podotknout, že v legislativě ČR jsou jednotlivé zákony recipročně provázány a proto zde uvedu pouze některé z nich, jenž budou dále využity v praktické části.

- **Zákon č. 101/2000 Sb. o ochraně osobních údajů** „*Tento zákon se vztahuje na osobní údaje, které zpracovávají státní orgány, orgány územní samosprávy, jiné orgány veřejné moci, jakož i fyzické a právnické osoby.*“
    - **Osobním údajem** se ve smyslu § 4 písm. a) zákona č. 101/2000 Sb. rozumí jakákoliv informace týkající se určeného nebo určitelného subjektu údajů. Jde o informace o soukromí osob, jejich vztazích k lidem, zdravotním stavu, vlastnostech, zálibách atp.
    - **Citlivé údaje** jsou stanoveny dle § 4 písm. b) zákona č. 101/2000 Sb. taxativním výčtem osobních údajů tj. jde o úplný, konečný výčet. Patří sem zdravotní stav, jedinečné biologické rysy, politické postoje, sexuální orientace atd. U těchto údajů je kladen zvýšený důraz na jejich ochranu při zpracování dle zákona o ochraně osobních údajů.

- **Zákon č. 36/1967 Sb. o znalcích a tlumočnících § 10a** „*(1) Znalec (tlumočník) je povinen zachovávat mlčenlivost o skutečnostech, o kterých se dozvěděl v souvislosti s výkonem své znalecké (tlumočnické) činnosti, a to i po jejím skončení;* ***to neplatí, použije-li informace o těchto skutečnostech přiměřeným způsobem pro vědecké nebo vzdělávací účely.*** *Mlčenlivosti jej může zprostit orgán veřejné moci, který jej ustanovil, nebo ten, pro nějž znaleckou (tlumočnickou) činnost na základě smlouvy vykonal.*“
- **Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti** „*Tento zákon upravuje zásady pro stanovení informací jako informací utajovaných, podmínky pro přístup k nim a další požadavky na jejich ochranu, zásady pro stanovení citlivých činností a podmínky pro jejich výkon a s tím spojený výkon státní správy.*“
    - **Utajovanou informací** dle § 2 písm. a) se rozumí: „*informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu České republiky nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací*“

[zdroj: citace z uvedených zákonů]

Souhrn:

Je podstatné brát v úvahu, že na zabezpečení datového úložiště je nezbytné nahlížet jako na celek. Tedy nesoustředit se na konkrétní prvek laboratoře, ale vzít v potaz zabezpečení laboratoř jako takové. Obecně v případě digitální forenzní analýzy (DFA) platí, že lze během zpracovávání dat narazit na citlivé, osobní nebo utajované informace **pouze potenciálně** a většinou se nikdy dopředu neví, zda se při zkoumání dat takové informace budou vyskytovat. Jelikož se však jedná o univerzitní laboratoř a veškeré data budou sloužit pro vědecké a vzdělávací účely, laboratoř (znalec) není osoba povinná ze zákona, tudíž se na ni nevztahuje povinnost mlčenlivosti. Navíc by laboratoř neměla zpracovávat žádné utajované informace, a proto nebudeme vztahovat na laboratoř kritéria dle požadavků Národního bezpečnostního úřadu. Za okolnostech neočekávaného výskytu utajovaných informací, je nutné tuto věc řešit ad-hoc s kompetentními úřady, tedy prakticky pouze s NBÚ.

3.2 Standardy a normy

V dnešní době existuje celá řada standardů a doporučení, jenž reflektují specifika jednotlivých normalizačních institutů v mnohých oblastech lidské činnosti včetně bezpečnosti informací. Výběr ideálního řešení je diskutabilní a může být specifické pro každou organizaci v závislosti na řadě charakteristik, jenž definitivní řešení ovlivní. Jelikož je řízení bezpečnosti informací nutné založit na přesně definovaných postupech, mezinárodní normy tuto skutečnost velice usnadňují. Nejen v rámci legislativy ČR jsou standardy a normy doporučovány k řešení dané problematiky a usnadní tak případnou certifikaci podniků v rámci zavedení systému řízení bezpečnosti informací (ISMS). Samozřejmostí pak je, aby implementované funkce byly v souladu s platnými zákony, nařízeními a jinými právními normami.

V této kapitole bude dále nastíněn přehled nejznámějších a nejpoužívanějších nástrojů, které lze efektivně využít v oblasti bezpečnosti informací. [11], [12]

3.2.1 ITIL (Information Technology Infrastructure Library)

ITIL je mezinárodně uznávaný standard, jenž vznikl už na přelomu 90. let. Jedná se o soubor postupů k řízení IT služeb (ITSM) sladěnými s potřebami podniku. Ve své současné podobě (známý jako ITIL 2011) je publikován jako série pěti hlavních svazků z oboru řízení služeb informačních technologií, z nichž každý zahrnuje odlišnou ITSM fázi životního cyklu. Ve své současné verzi se jedná o těchto pět ústředních publikací:

- Service Strategy (Strategické procesy)
- Service Design (Návrh služeb)
- Service Transition (Uvedení služby do provozu)
- Service Operation (Provoz služeb)
- Continual Service Improvement (Neustálý proces zlepšování)

A k nim se váže ještě také kniha The Introduction to the ITIL Service Lifecycle, která je jakýmsi shrnutím předešlých 5 knih. [14]

3.2.1.1 Vlastnosti a přínosy ITIL

ITIL představuje sbírku nejlepších zkušeností („*best practice*“) z oblasti IT služeb, které tvoří tzv. rámec doporučení a návodů, avšak neřeší je do detailů. Tedy nejedná se o normu ani metodiku. Pouze se snaží navést k vytvoření vlastního systému řízení služeb. Můžeme

zde tedy nalézt popis procesů, postupů, kontrolní seznamy (tzv. check-list), které nejsou specifické pro organizaci a zaručují tak nezávislost na platformě. [14], [15]

Zavedení těchto best-practice má celou řadu kvalitativních i kvantitativních přínosů pro společnost nejen pro oddělení IT. Nejdůležitějšími přínosy tedy jsou zvýšení spokojenosti zákazníků, eliminace *sisyfovské práce*, zvýšení dostupnosti a spolehlivosti služeb, odbourání komunikačních bariér. Jako hlavní nevýhoda je často označována absence objektivního auditu, zda byly implementované prvky správně či špatně. K tomu slouží norma ISO/IEC 20000, na které je do jisté míry ITIL rámec postaven, avšak bez podstatných imperativů, tzn. zřídkakdy něco direktivně předepisuje.

3.2.1.2 Řešení informační bezpečnosti

Metodika ITIL je všestranným řešením řízení IT v organizaci, ale ke zpracování tématu této diplomové práce postačí pouze vybraná kapitola věnující se problematice informační bezpečnosti, kterou se budu dále zabývat. Kapitola řízení informační bezpečnosti (ISM - Information Security Management) je popsána v knize ITIL - Service Design a snaží se o sladění bezpečnostních best-practice v IT s obchodními procesy, tak aby došlo k zajištění bezpečnosti ve všech činnostech Řízení služeb. [11], [14]

Kapitola řízení informační bezpečnosti popisuje a nabádá k zavedení informační bezpečnosti do managementu organizace. Z největší části se zde ITIL opírá o systém řízení bezpečnosti informací (ISMS), který je blíže popsán v ISO/IEC normě 27002.

Cíle bezpečnosti:

Primárním cílem bezpečnostního managementu je chránit informační aktiva vůči hrozbám, a udržet tak jejich hodnotu pro organizaci. Podrobněji jsou cíle bezpečnost chápány následovně:

- Dostupnost informací – nejčastěji definována jako zaručení, že informace je pro oprávněného uživatele v době potřeby ihned přístupná.
- Důvěrnost informací – zajištění, že informace budou přístupné nebo sděleny pouze těm osobám, jenž mají příslušná oprávnění.
- Integrita – lze definovat jako zajištění správnosti a úplnosti informací.
- Autenticita informací – říká, že lze ověřit původ informace a potvrzuje platnost nějakého prohlášení (vyjadřuje nepopíratelnost). [13], [14]

Nežádoucí odhalení, pozměnění, nebo zničení určitých informací může vést k finanční ztrátě, vyzrazení firemního know-how, poškození dobrého jména firmy, případně i k ohrožení života zaměstnanců nebo klientů. Z takových to důvodů je nezbytné zvážit, jak vysokým stupněm ochrany daná aktiva chránit. Priority bezpečnostní politiky je pak nutné posuzovat v závislosti na obchodních procesech od začátku do konce a neopomíjet jejich vedlejší aspekty. Jelikož pouze v kontextu s ostatními potřebami organizace lze definovat bezpečnostní politiku. Navržená opatření s sebou nesou jistá omezení při práci s informacemi. Stanovit odpovídající úroveň zabezpečení reflektující skutečné potřeby organizace je možné jedině na základě detailní analýzy rizik. [15], [16]

Rámec ISM

Proces odpovědný za to, že důvěrnost, integrita a dostupnost aktiv, informací, dat, a IT služeb odpovídají dohodnutým potřebám podniku. Řízení bezpečnosti informací podporuje bezpečnost podnikání v téměř všech oblastech IT dané firmy. Proces ISM by měl zajistit, aby se politika bezpečnosti informací zavedla, udržovala a prosazovala takovým způsobem, aby v ní byly zahrnuty postupy správného i mylného využívání všech IT systémů a služeb.

Při zavádění ISM je nepostradatelné pochopit jednak IT podniku, ale také obchodní bezpečnostní prostředí včetně podnikatelských rizik, nutné legislativní požadavky, jenž se na organizaci vztahují a také podnikatelský plán a jeho rizika. [15]

Role ISM v ITIL

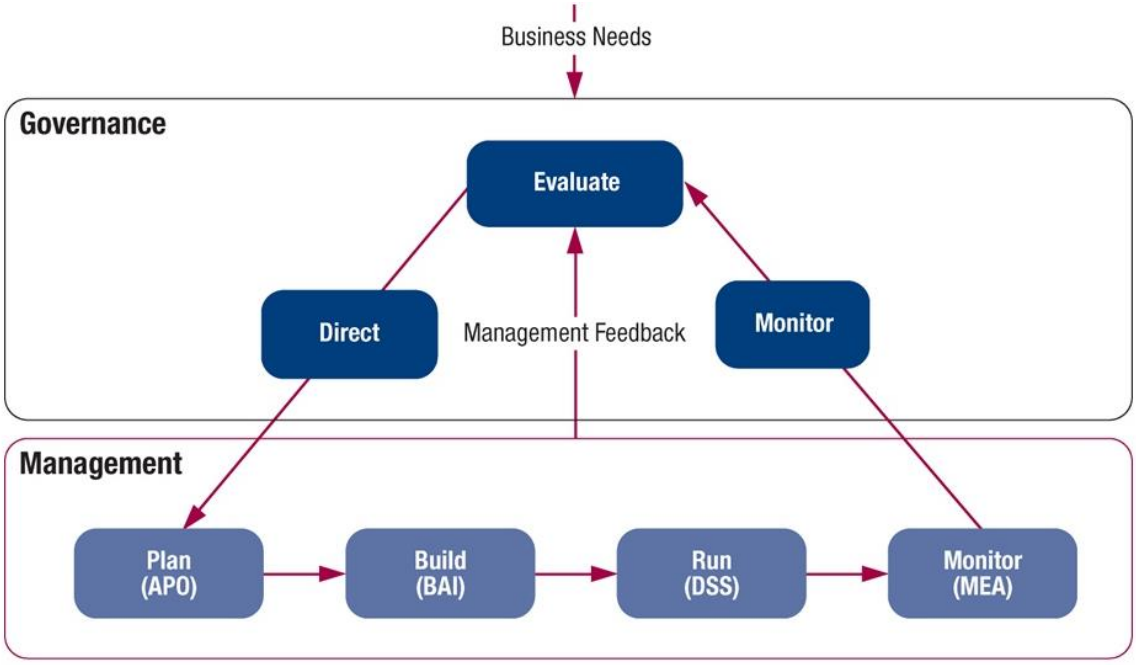
V rámci ITIL se očekává, že za veškerá aktiva, jenž organizace vlastní je zodpovědný v konečném důsledku výkonný management. V jeho kompetenci je nastavit ochranu aktiv a dále reagovat na případné problémy. ISM by tak mělo být nedílnou součástí komplexní politiky a je v zájmu všech organizací poskytující IT služby ujistit své okolí o prosazování nezbytných kontrol a praktik k prosazování těchto politik. ITIL pak vytváří rámec technik, jak zaintegrovat ISM i do ostatních oddělení organizací. [14], [15]

3.2.2 COBIT

COBIT vznikl jako akronym z anglického Control Objectives for Information and related Technology a v současné verzi COBIT 5 definuje celkem 37 procesů v IT, které jsou dále

rozděleny do pěti domén. Nejvýše postavenou doménu představuje vedení organizace (Govenrance) s 5 procesy a dále se jedná o domény určené ke každodennímu řízení pro management organizace:

- **Plan** – plánování a organizování (zahrnuje 13 procesů),
- **Build** – Osvojení a implementace (10 procesů),
- **Run** – Dodávka služeb a podpora (6 procesů),
- **Monitor** – Monitoring a vyhodnocování (3 procesy). [12], [18]



Obrázek 2 – Hierarchie domén [18]

Jedná se rámec „*best-practice*“ vytvořený společností ISACA pro IT management a IT governance. Představuje podpůrnou sadu nástrojů, které umožňují manažerům překlenout mezery mezi požadavky na kontrolu, technickými problémy a podnikatelskými riziky. [15]

COBIT definuje **bezpečnost informací** jako záruku, že v rámci podniku jsou informace chráněny proti: zpřístupnění neoprávněným uživatelům (důvěrnost), cizí modifikaci (integrita) a nedosažitelnosti informací pro oprávněné osoby (dostupnost).

Pro oblast bezpečnosti informací poskytuje konkrétní pokyny týkající se těchto odvětví:

1. Informační bezpečnostní politiky, principů a rámce.

2. Procesy zahrnující informační a bezpečnostně specifické detaily a činnosti.

3. Organizačních struktur.

4. Lidí, jejich dovedností a kompetencí. [16], [17]

3.2.2.1 Definice architektury COBIT

Prioritním cílem COBITu je identifikace informací a služeb, které jsou primární a nejdůležitější pro fungování organizace a následné určení jejich bezpečnostních požadavků. COBIT představuje řídící a auditní rámec, jenž umožní propojit IT strategii s celopodnikovou strategií, neboli nastavit strategické řízení podnikové informatiky ve shodě se strategickými požadavky služeb organizace.

V rámci COBITu je nutno sumarizovat aktiva v podobě citlivých informací, služeb, u nichž je vyžadována maximální dostupnost a věrohodné transakce (splňující podmínky autentičnosti a integrity).

- Následně je důležité rozhodnout o delegaci odpovědnosti k:
- význam dat, jejich uchování a archivace,
- systém řízení autorizace a ověřování elektronických transakcí,
- úroveň dostupnosti dat,
- přístupu a modifikaci citlivých informací. [17], [18]

3.2.2.2 Řízení informačních systému

Pro dosažení požadované úrovně informační bezpečnosti, je nezbytné docílit toho, aby veškeré ICT systémy byly využívané pouze delegovanými osobami a k věcem tomu určenými. Proto je potřeba dodržovat tyto podmínky:

- Zavést pravidla řízení přístupu k jednotlivým službám a informacím na základě potřeb jednotlivců.
- Zajistit přidělení přiměřené odpovědnosti ke správě systémů (uživatelských účtů, hesel, karet a dalších zařízení) a dodržovat kontrolu těchto aktiv, jenž představují finanční hodnotu.

- V případě narušení bezpečnosti v jakékoliv podobě, zajistit okamžité nahlášení a zaujmout patřičná opatření.
- Jasně a stručně definovat pravidla vztahující se na nakládání a sdílení informací mezi organizací a spolupracujícími stranami
- Zvážit nasazení MDM řešení a jiných bezpečnostních prostředků k ochraně mobilních zařízení.
- Nastavit přiměřená bezpečnostní pravidla vůči platným smluvním závazkům mezi obchodními stranami. [12], [19]

3.2.2.3 Fyzická bezpečnost

Stejně tak jako bezpečnost na úrovni jednotlivých procesů řízení, softwaru a managementu je důležitá i bezpečnost fyzická. COBIT tuto problematiku neopomíjí, nicméně nabádá opět pouze všeobecným rámcem *best-practice*. K ochraně IT zařízení před poškozením je vhodné dodržovat doporučení:

- Definovat a implementovat proces, který bude chránit vůči přírodním jevům, fluktuacím a výpadkům energie společně v souladu s obchodním modelem.
- Pravidelně provádět kontroly zařízení určených k dodávkám záložní energie.
- Ujistit se o ochraně a strukturovaném, organizovaném vedení datových a telekomunikačních kabelů.
- Provést analýzu klíčových IT komponent a uvážit realizaci redundantního řešení v případě interní a externí kabeláže.
- Definovat a implementovat proces k monitorování, případnému zaznamenávání incidentů a vytvořit systém reportů.
- Analyzovat možnosti umístění serveroven a jiných prvků IT pro minimalizaci hrozen narušení (např. živelné pohromy). Výsledek analýzy předat firemnímu managementu k zachování kontinuity. [20]

3.2.2.4 Soulad s právními normami a jinými požadavky

Tak jako v případě standardu ITIL i zde platí fakt, že implementované bezpečnostní funkce musí být v souladu s platnými právními normami. Doporučovaný postup obsahuje:

- Identifikovat opatření, jenž povedou v rámci plnění bezpečnostních požadavků k dodržování zákonů, a vyhlášek týkajících se dané činnosti organizace (ochrana osobních údajů, ochrana utajovaných informací, práva duševního vlastnictví a další smluvní požadavky).
- Podněcovat zaměstnance, aby na případné nedostatky upozorňovali a patřičně reagovali.

Současná verze COBIT 5 byla sladěna a harmonizována s ostatními více specifickými normami, IT standardy a osvědčenými best-practice jako COSO, ITIL, BiSL, ISO 27000 aj. COBIT tedy zastupuje funkci *integrátora* těchto různých poradenských materiálů a norem, kdy se snaží shrnout hlavní cíle pod jeden zastřešující rámec, jenž by je propojoval navzájem a zároveň k nim přidal požadavky z oblasti podnikání. [13], [18]

3.2.3 ISO/IEC 27k

Jedním z markantních opatření rodiny norem ISO/IEC 27000 je zavedení a popisu systému řízení bezpečnosti informací - ISMS (Information Security Management System). Tento pojem byl dříve definován primárně normou ISO/IEC 17799, publikovanou Mezinárodní organizací pro normalizaci (International Organization for Standardization) v roce 2000. Přestože byl obsah celé řady norem 27k sepsán obzvláště imperativně, zachoval si univerzální přístup k řešení bezpečnosti informací a dnes jsou tyto normy hlavní oporou ve spoustě bezpečnostních politikách viz. COBIT a ITIL. V současné době celou sérii ISO/IEC 27k tvoří celkem 36 norem a zaujímají široký záběr v oblasti bezpečnosti informací.

V následujících kapitolách se však budu zaobírat pouze vybranými normami týkajících se tématu této práce.

3.2.3.1 ISO/IEC 27000

Český ekvivalent této normy zavádí a definuje pojmy pro všechny následující normy řady 27000. Představuje obecný *úvod* do oblasti informační bezpečnosti a dále také ISMS.

3.2.3.2 ISO/IEC 27001

Tato mezinárodní norma si klade za cíl poskytnout doporučení jak aplikovat vybraná opatření v rámci procesu ustanovení, implementování, provozu a neustálého zlepšování systému řízení bezpečnosti informací v rámci kontextu organizace. V normě jsou taktéž zahrnuty po-

žadavky na posuzování a zabezpečení rizik informační bezpečnosti na úrovni podniku. Požadavky jsou obecně aplikovatelné bez ohledu na velikost organizace a náplň její činnosti. Poslední úpravy této normy z roku 2013 se týkají propojení a harmonizace s normami ISO/IEC 9001:2000 a ISO/IEC 14001:2004 do takové míry, aby bylo zajištěno jejich konzistentní a jednotné zavedení do provozu organizací.

PDCA & ISMS

Norma vykládá implementaci informační bezpečnosti jako kontinuální proces, nikoliv jako jednorázový projekt. Jedná se tedy o proces neustálého vylepšování systému bezpečnosti. Prostředkem tohoto vylepšování je cyklus PDCA (Plan-Do-Check-Act) viz. Obrázek 3, který se vyhýbá možnému riziku zavedení nedokonalých procesů. Případné nedostatky se řeší do té doby, než odpovídají aktuálním požadavkům potřebám organizace. [11], [21]

Systému ISMS probíhá typicky v následujících krocích:

1. **(Plánuj) Vymezení působnosti, strategie a cílů ISMS** – Tento krok je důležitý z hlediska rozsahu a strategie, jenž musí být relevantní a odpovídala tak skutečnosti. Proto by mělo před jejím stanovením dojít ke zhodnocení současného stavu.
    a. **Naplánování a schválení strategie pro bezpečnost**
    b. **Bezpečnostní politika -** musí být napsána a schválena vedením.
    c. **Analýza rizik** – důležité je zvolit vhodnou míru podrobnosti a neformálnosti zvolené metody, aby byl splněn hlavní cíl analýzy rizik (identifikace rizik a objektivní ohodnocení).
    d. **Výběr opatření a plán implementace –** tento krok zahrnuje zpracování bezpečnostních standardů jejich rozsah a obsah je definován povahou organizace. Při tvorbě je tedy důležité myslet na integraci do celkové politiky společnosti.
2. **(Dělej) Zavedení a provoz ISMS** – hlavním cílem této etapy je účelné prosazení vybraných a připravených opatření do provozu organizace.
    a. **Způsob implementace** – Osobní případně neverbální způsob předání pokynů (email, intranet apod.)
    b. **Bezpečnostní politika** – ve většině případů by se mělo jednat o změnu či verifikaci nastavení současné politiky (operačních systémů, aplikací, hardwaru atp.)

c. **Zavedení vybraných bezpečnostních opatření** – k dosažení vytyčených cílů.

d. **Řízení provozu a detekce rizik** – stanovení metrik k vyhodnocování vybraných opatření, stanovování jejich účinnosti a zavedení metod pro rychlou detekci a reakci.

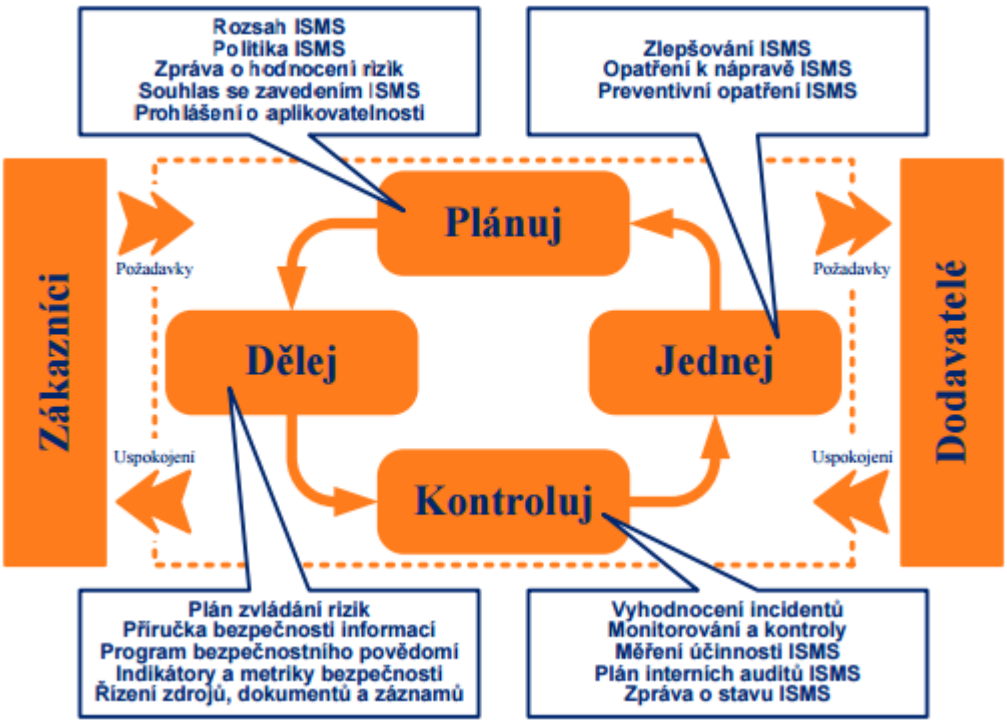
3. **(Kontroluj) Monitorování a přezkoumávání** – podstatou tohoto kroku je zajištění zpětné vazby, pravidelného sledování a vyhodnocování stavů bezpečnosti informací.

a. **Monitoring systému a kontrola** – zavedení evidence a kontroly provozu IS

b. **Audit a kontrola bezpečnostních opatření** – Na základě předchozího měření účinnosti, dohlížet na zavedení opatření a plnění stanovených cílů.

c. **Revize ISMS** – aktualizovat bezpečnostní plány s ohledem na zjištěné nedostatky.

4. **(Jednej) Údržba a zlepšování** – náplní je vyhodnocování předešlé fáze, identifikace a analýza problémů a nakonec přijetí nápravných, preventivních opatření. [21], [22]



Obrázek 3 – PDCA model pro řízení bezpečnosti informací [21]

3.2.3.3 ISO/IEC 27002

Je úzce spjata s předcházející normou ISO 27001, avšak plní jinou roli. V případě této normy lze hovořit o seznamu *best-practice* z oblasti bezpečnostních opatření, jenž mohou být příkladem při budování ISMS. Doporučení normy obsahuje 113 bezpečnostních opatření rozdělených do 14 oblastí.

3.2.3.4 ISO/IEC 27040

Tato norma byla vydána teprve v roce 2015 a v současné době neexistuje její český ekvivalent, nicméně v případě řešení této diplomové práce by mohla být klíčovým podkladem. Zabývá se bezpečnostními technikami při zabezpečení datových úložišť. Poskytuje podrobné technické pokyny pro zajištění a kontrolu důvěrnosti dat formou šifrování, ať už přenosových cest nebo datových úložišť.

3.2.4 Komparace způsobů řízení informační bezpečnosti

V předchozích kapitolách byly shrnuty 3 mezinárodně rozšířené systémy zabývající se bezpečnosti informací v organizacích. V případě standardů **ITIL 2011 Edition** a **COBIT 5** šlo o rámec poskytování osvědčených postupů pro správu služeb IT. Ve třetím případu šlo o samotné mezinárodně uznávané normy **ISO 27000**. Každá z těchto metodik přináší organizaci jistou garanci zvýšení kontroly nad IT oblastí a jejím řízením. Správné zavedení doporučovaných postupů může pomoci při vytváření vlastních strategií a postupů, optimalizovat využití omezených prostředků a snížit rizika.

Tabulka 2 – Porovnání norem a standardů [Zdroj: vlastní zpracování]

Kritérium	ITIL 2011 Edition	COBIT 5	ISO/IEC 27000
Vydání poslední verze	2011	2012	2016
Zaměřeno na	ITSM (Řízení služeb informačních technologií)	Byznys a IT Governance	ISMS
Forma	Best-practice	Best-practice	Mezinárodní normy
Rámec působnosti	ITSM v kombinaci se vztahy se zákazníky	Kompletní IT govenrance a bezpečnostní plánování	Samostatné bezpečnostní normy

Velikost organizace	Velká, střední	Velká, střední	Velká, střední, malá
Dokumentace zdarma	Ne	Ne	Ne
Implementace po částech	Problematická	Problematická	Ne
Samostatné řešení pro řízení bezpeč-nosti	Ne	Ne	Ano
Možnost certifikace	Ano	Ano	Ano

Je poměrně komplikované určit parametry, podle kterých by bylo možné objektivně srovnat standardy Řízení služeb informačních technologií, IT Governance a normy ISO/IEC 27k. Nástroje ITIL a COBIT tvoří komplexní systémy řízení IT na rozdíl od rodiny norem 27k. V některých případech je tedy nasnadě prohlásit, že určitý systém zabezpečení je vhodnější než jiný, ale v jiných případech může být situace zcela opačná. Nelze proto jednoznačně určit univerzální standard, který by byl nejlepším přístupem k jakémukoliv případu řízení IT. V mnoha případech je použití konkrétního standardu podníceno specifickými potřebami dané organizace. [23]

Standardy ITIL a COBIT jsou si do jisté míry dost podobné, jelikož jsou založeny doporučených procesních postupech pro celý management a podporu IT služeb. Jak lze v tabulce vidět, zaměřují se na způsob a definování komplexnějšího řešení pro střední a velké firmy. A oba tyto standardy v případě bezpečnosti IT vycházejí z norem ISO 27k, avšak zachovávají si obecný přístup bez konkrétnějších, důrazných doporučení. Z těchto důvodů shledávám rodinu norem ISO 27000 mnohem vhodnější pro následné řešení problematiky diplomové práce.

Zabezpečení datového úložiště podle ISO 27k

Obecně je tedy míra zabezpečení dat věcí interního posouzení rizik a nastavení bezpečnosti informací dle např. ISO/IEC 27000 s tím, že se nastaví míra akceptovatelného rizika na úroveň, která je přísnější než u „běžné“ organizace, která zpracovává citlivá data.

Při návrhu datového úložiště v praktické části této práce se tedy budu opírat primárně o pokyny uvedené v normě ISO/IEC 27040 (Security techniques – Storage security) pro bezpečnost ukládání dat.

4 DATOVÁ ÚLOŽIŠTĚ

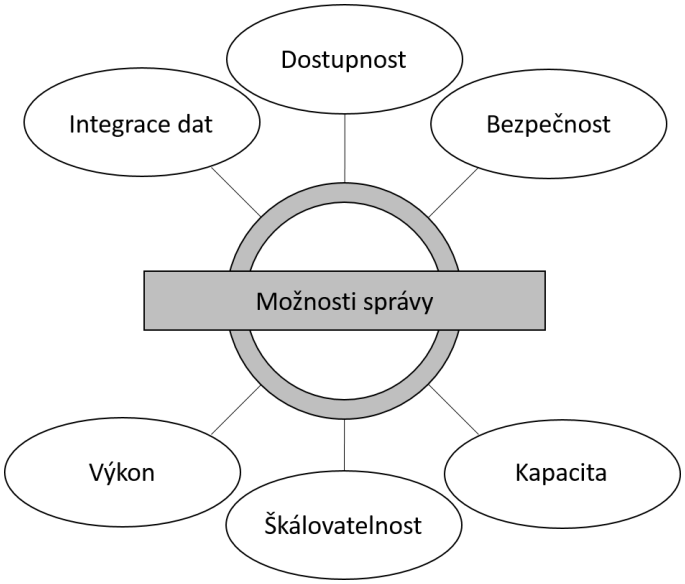
Technologií k ukládání dat je v současné době nepřeberné množství, a to od lokálních úložišť připojených přímo k serveru nebo případně ke klientské stanici, přes centrální disková úložiště až po komplexní systémy, jenž tvoří část dedikované sítě. Pokud jakákoliv organizace zvažuje pořízení datového úložiště, je nasnadě položit si několik otázek: K ukládání jakého typu dat bude zamýšlené datové úložiště využíváno? Jak velká úložná kapacita bude potřeba? Jaká bude dostupnost dat? A jistě velice častou otázkou bude také: Jak moc finančně bude realizace náročná?

V dnešní době se můžeme nejčastěji setkat s následujícími řešeními:

1) DAS (Direct Attached Storage)
2) NAS (Network Attached Storage)
3) SAN (Storage Area Network)

4.1 Klíčové vlastnosti datových úložišť

Nepřetržitý provoz datových úložišť je rozhodujícím faktorem k přežití a úspěchu mnoha institucí nejen v byznysu. Pro většinu organizací je nezbytné mít spolehlivou infrastrukturu, která zajistí přístup k datům v po celou dobu. Ačkoliv vlastnosti znázorněné na Obrázek 4 platí pro všechny prvky datového centra, následující kapitoly budou zaměřeny pouze na potřebu datových úložišť. [24]



Obrázek 4 – Klíčové vlastnosti datových úložišť [24]

Dostupnost: Zajištění dostupnosti dat a informací v případě potřeby je jednou z klíčových vlastností. Případná nedostupnost informací může způsobit nemalé finanční ztráty řadě firem (finanční instituce, oblast telekomunikací, e-komerce) během velice krátké doby. Proto je důležité mít zajištěnou spolehlivou a včasnou dispozici dat a zdrojů autorizovaným jednotlivcům. Informační systémy musí mít datovou kapacitu dimenzovanou tak, aby v definovaném čase poskytovaly dostatečný výkon, musí být schopny zotavit se z výpadků transparentním a rychlým způsobem, aby nebyla negativně narušena produktivita. Náchylná místa systému musí být ošetřena např. zavedením redundantních prvků.

Bezpečnost: Pro zabezpečení dat je nutné dokázat ohodnotit rizika a mít ochotu investovat do protiopatření. Zajistit systém proti hrozbám, a zavést zásady, postupy a integrovat prvky, jenž minimalizují rizika a komplex administrativních, technických, logických a fyzických opatření a pomohou i v případě detekce neautorizovaného přístupu k datům.

Škálovatelnost: Růst objemů dat často vyžaduje rozšiřitelnost vlastností daného systému s náhlými změnami a to vše bez přerušení činnosti nebo zamezení dostupnosti dat.

Výkon: Všechny prvky datového úložiště by měly poskytovat optimální výkon na základě požadované úrovně služeb.

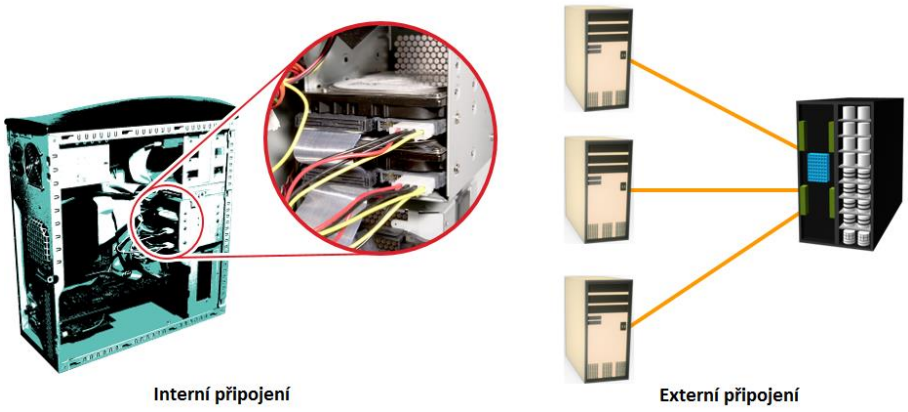
Integrita dat: Integrita je udržena, pokud je zajištěno, že data jsou totožná, se zaručeným obsahem a jsou provedena opatření proti jejich neautorizované změně. Ke změně může dojít jak vlivem chyby softwaru, hardwaru, tak i špatným úmyslem. Proto musí hardwarové, softwarové a komunikační prostředky pracovat tak, aby data uchovávaly a zpracovávaly správně a přesně, přenášely je do požadovaného cíle bez nežádoucích změn. K zachování integrity dat nám dopomohou mechanismy jako Error Correction (oprava chyb) nebo Parity Bits (paritní bity).

Kapacita: Od datových úložišť, jenž jsou použity ve větších firmách a institucích je vyžadováno dostatečných zdrojů pro ukládání a zpracování velkého množství dat. A v případě zvýšení požadavků na kapacitu, datové úložiště musí být schopno poskytnout dodatečnou kapacitu bez přerušení dostupnosti nebo s minimálním narušením. Kapacita může být spravována realokací stávajících zdrojů, nebo přidáním nových zdrojů.

Možnosti správy: K datovému úložišti by mělo být možné zajistit snadnou a integrovanou správu všech jeho elementů. Různými implementovanými funkcemi v systému správy úložiště může být dosaženo patřičné automatizace, tedy snížení lidského úsilí v běžných úlohách. [24], [27]

4.2 DAS (Direct Attached Storage)

Představuje architekturu, ve které je datové úložiště připojené přímo ke klientskému počítači, nebo serveru. Může mít podobu interního (uvnitř šasi), nebo napřímo připojeného externího úložiště. Přestože tuto implementaci ve většině oblastech nahrazují sofistikovanější architektury (NAS, SAN), své uplatnění si stále najde jako řešení u osobních počítačů a v menších pracovních skupinách.



Obrázek 5 – Interní a externí provedení DAS [25]

Interní řešení připojení DAS architektury je zobrazeno na levé části Obrázek 5, kdy je datové úložiště zasazeno uvnitř šasi počítače a nejčastěji připojeno paralelní nebo sériovou sběrnicí. Délka sběrnice je zde limitujícím faktorem pro zachování vysoké propustnosti při přenosu dat. Navíc na většinu interních sběrnic můžeme připojit pouze omezené množství zařízení, které mohou zabrat poměrně velký prostor.

Externí provedení DAS architektury je realizované na blokové úrovni, kdy je stanice (nejčastěji server) připojen skrze protokol SCSI nebo FC (Fibre channel) k datovému úložišti viz. pravá část Obrázek 5. V porovnání s interní realizací DAS, externí řešení překonává omezení ve vzdálenosti sběrnice, omezení počtu připojených zařízení a poskytuje centralizovanou správu úložných zařízení. [24], [27]

4.2.1 Výhody DAS architektury

Mezi výhody jednoznačně patří relativně nízké pořizovací náklady na rozdíl od pokročilých architektur typu NAS a SAN. Dále je to jednoduché a rychlé nasazení i konfigurace. Nastavení je řízeno pouze z hostitelského OS, na kterém se provádí veškeré správa. Celou architekturu tvoří pouze pár hardwarových prvků.

4.2.2 Omezení DAS architektury

K nevýhodám DASu patří zejména špatná škálovatelnost a omezený počet portů neboli počet připojených úložišť k jednomu počítači. Při dosažení maximální kapacity připojených zařízení může dojít až k ohrožení dostupnosti provozované služby. DAS neposkytuje optimální využití datových zdrojů v důsledku jeho omezené možnosti sdílení. Nevyužitá zdrojová kapacita nemůže být snadno realokovaná, což má za následek, že některá úložiště jsou maximálně vyčerpány a u jiných zůstává nevyužitý prostor. [24]

4.3 SAN (Storage Area Network)

SAN je vysokorychlostní, speciálně vytvořenou sítí serverů a sdílených úložných zařízení. Vznikl jako reakce na nedostatky DAS architektury a tudíž se snaží o jejich rozptýlení. SAN poskytuje konsolidaci úložišť a umožňuje centralizovanou správu dat. Naplňuje tak požadavky efektivního ukládání dat (lepší úspora místa) a poskytuje také účinnou správu a ochranu dat. Dále umožňuje fyzické oddělení dat a serverů, kdy jednotlivé prvky mohou být od sebe vzdáleny až desítky kilometrů.

Běžné nasazení SAN sítě využívá Fibre Channel protokol, nebo IP SAN (iSCSI, FCIP nebo iFCP).

- FC SAN využívá protokolu Fibre Channel k přenosu dat, příkazů a informací o stavu mezi servery a jinými zařízeními.
- IP SAN pro komunikaci používá protokoly na bázi IP. Nejběžněji se vyskytuje provedení IP SAN v kombinaci se síťovým protokolem iSCSI, jenž zapouzdřuje shromážděné data do paketů pro přenos mezi servery a úložnými zařízeními. IP SAN protokoly obvykle běží přes standardní ethernetovou síť a pro komunikaci využívají TCP/IP protokol.

IP SAN technologie je obecně vnímána jako méně nákladné a složité řešení s jednodušší správou než je tomu u FC SAN. FC SAN vyžaduje speciální hardware jako adaptéry hostitelské sběrnice a FC switche, zatímco u IP SAN lze použít běžnější a levnější ethernetové síťové prvky. Hlavní nevýhodou IP SANu je oproti řešení s FC pak menší rychlost. [27]

SAN se obecně se svou topologií a užitými technologiemi hodí daleko více do středních a velkých organizací, které požadují vysokou dostupnost svých služeb, rychlé odezvy a škálovatelnost. Všechny tyto klady jsou však vykoupeny pořizovacími náklady, jenž jsou

poměrně vysoké, protože je nutné vybudovat specifickou infrastrukturu. Po prostudování této technologie jsem došel k závěru, že není vhodná pro řešení problematiky této práce, proto se jí dále nebudu zabývat. [24], [27]

4.4 NAS (Network Attached Storage)

Výše popsaná datová úložiště uzpůsobená ke sdílení souborů po síti poskytují flexibilitu v podobě sdílení na velké vzdálenosti a navíc mezi velkým množstvím uživatelů. Na druhou stranu souborové servery využívají architektury klient-server, skrze kterou spolu komunikují a každá instance klienta může posílat žádost o data jednomu nebo více připojeným serverům. Jako řešení obrovského nárůstu dat v podnikovém prostředí, organizace velice často nasazují nové a nové souborové servery. Tyto servery jsou následně připojeny jako DAS nebo NAS řešení. Avšak celá tato strategie řeší daný problém z pohledu škálovatelnosti dost neefektivně, kdy dochází k proliferaci izolovaných *ostrovů* v podobě nevyužité datové kapacity. Další nevýhodou jsou rostoucí náklady na správu a větší složitost celé hierarchie předešlých systémů. Nejen tyto neduhy měli za následek vznik architektury NAS.

NAS představuje dedikované, vysoce výkonné sdílené úložiště pro ukládání dat, jenž umožňuje svým klientům sdílení souborů přes protokoly z rodiny TCP/IP (nejčastěji CISF, NFS, FTPS aj.) v LAN i WAN sítích. Jeho hlavní předností je konsolidace serverů a také datových úložišť, což usnadňuje správu úložišť a implementaci. Díky heterogennímu prostředí může diskovou kapacitu sdílet se servery odlišných architektur a operačních systémů. [24], [27]

4.4.1 Výhody architektury NAS

Mezi hlavní výhody patří:

Komplexní přístup k informacím: Efektivní sdílení dat a podpora konfigurací *many-to-one* i *many-to-many,* kdy je NAS schopen obsloužit vícero klientů zároveň.

Flexibilita: Architektura je nezávislá a umožňuje přístup jak unixovým tak i windows platformám skrze standardizované protokoly.

Centralizované úložiště: Centralizací úložiště můžeme minimalizovat duplicitu dat na klientských zařízeních a zajistit také vyšší bezpečnost.

Zjednodušená správa: Poskytuje rychlá a efektivní řízení disků a diskových polí.

Škálovatelnost: U jednotlivých diskových oddílů a polí je možné jednoduše a efektivně upravit velikost dle potřeby bez vzniku nevyužité kapacity.

Vysoká dostupnost: Zajištěna možnostmi vzdálené replikace, snapshoty, poli RAID.

Bezpečnost: Zprostředkovaná skrze uživatelskou autentizaci a možnosti vyhrazení pouze určité části dat danému uživateli.

Nízké náklady: Díky volbě levnějších technologií (např. Ethernetové síťové porty) jsou NASy daleko levnější než SAN architektury. [24]

4.4.2 Sdílení dat

NAS úložiště mohou přebrat odpovědnost sdílení dat většiny serverů na síti. Obvykle skrze vícero poskytovaných způsobů sdílení. Typicky se jedná o protokoly jako NFS, SMB/CIFS, FTP, případně FTPS, SFTP aj. Kombinací těchto protokolů je schopen zpracovat I/O požadavky na většině operačních systémů a poskytuje tak možnost migrace uživatelům z jednoho prostředí na jiné. [24]

4.4.2.1 Protokoly sdílení dat

1) **NFS:** (Network File System) je internetovým protokolem ke vzdálenému sdílení souborů skrze počítačovou síť. Funguje především nad transportním protokolem UDP, nicméně od verze 3 jej lze provozovat také nad TCP. Nejčastěji ho můžeme provozovat ve spolupráci s unixově založenými operačními systémy (Linux, AIX, Solaris, FreeBSD aj.).

   Implementace přenosu dat mezi klientem a serverem pomocí NFS vypadá následovně:

   - Server implementuje NFS démona *nfsd,* aby umožnil přístup k datům klientským zařízením.
   - Správce serveru může dále určit, které konkrétní data budou zpřístupněna exportem cest a parametrů typicky skrze konfigurační soubor */etc/exports* a příkaz *exportfs*.
   - Dále proběhne autentizace a navázání ověřeného spojení s klientem.
   - Klient následně zažádá o připojení exportovaných cest nejčastěji pomocí příkazu *mount,* a pokud vše proběhlo dle očekávání, vzdálené úložiště se připojí.

   pNFS: Představuje jednu z významných výhod. Stalo se součástí NFS od verze 4.1 a umožňuje klientům paralelní přístup k datům, což má za výsledek eliminaci problémů se škálovatelností a výkonu. Toho je dosaženo oddělením dat a metadat.

Bezpečnost: Samotný protokol ve starších verzích NFS v3 a v4 neměl implementovanou podporu šifrování, nicméně od poslední verze 4.1 je možné jej využít v kombinaci se síťovým autentizačním protokolem Kerberos, jenž využívá symetrické šifrování. [24]

2) **SMB/CIFS (Server Message Block / Common Internet File System)**

   Podobně jako NFS se jedná o komunikační protokol aplikační vrstvy, jenž slouží ke sdílenému přístupu k souborům, tiskárnám a jiným zařízením. Původně byl protokol vyvíjen ve společnosti IBM pod názvem SMB, později vývoj převzal Microsoft a přejmenoval jej na CIFS.

   Dnes je využíván hlavně na zařízeních s OS rodiny Windows, ale můžeme ho nalézt také na Unixu, Linuxu aj. v podobě otevřené svobodné implementace Samba.

   Stejně tak jako NFS využívá mechanismu k zabránění přepsání dat jiného uživatele. Dále je odolný i vůči chybám a dokáže automaticky obnovovat připojení v případě přerušení. [24]

   Bezpečnost: Od verze SMBv2 je možné využít volby povolení šifrování přenosu dat.

3) **FTP(S) (File Transfer Protocol)**

   Představuje další z velice často používaných protokolů pro přenos souborů mezi počítači skrze počítačovou síť. Využívá protokol TCP z rodiny TCP/IP a je zcela nezávislý na použitém operačním systému.

   Mezi hlavní nevýhody však patří přenos veškerých dat v textové (nešifrované) podobě a delší odezva než je tomu u předešlých protokolů.

   Bezpečnost: Do FTP dosud nebyl implementován mechanismus pro šifrování přenosu dat, nicméně je možné jej zkombinovat s jinými protokoly jako SSH (**SFTP**), jenž se postará o autentizaci a zabezpečení přenosových tras.

   Nebo další možností je **FTPS,** které přidává podporu TLS a SSL kryptografických protokolů. [24]

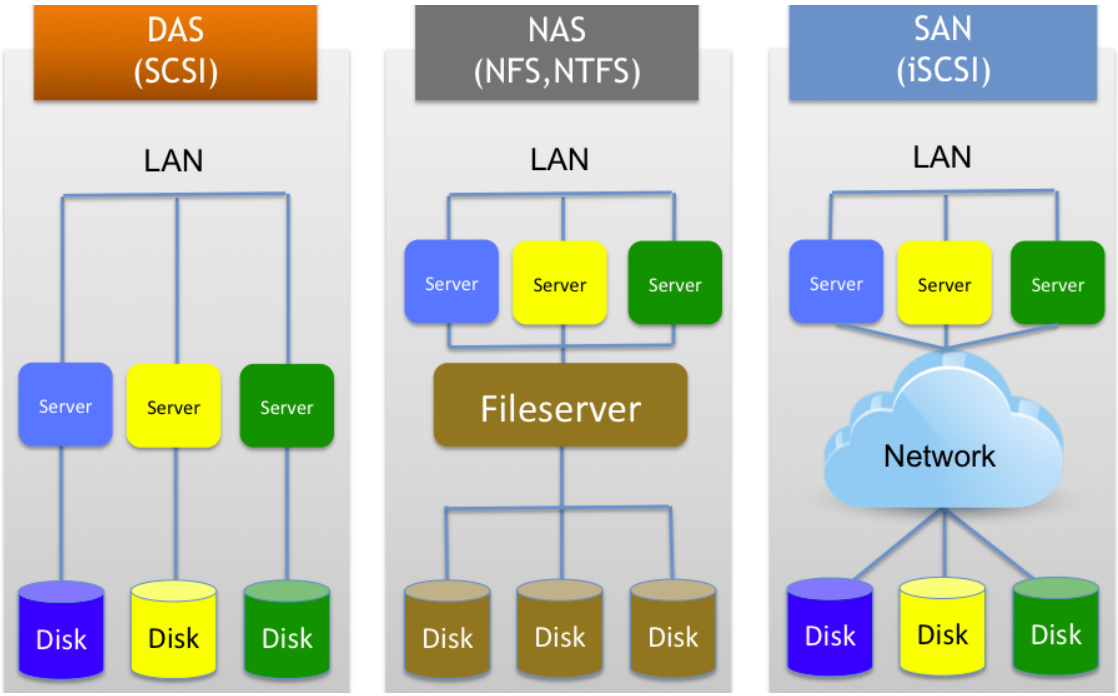
4.4.2.2 Nastavení oprávnění přístupu k datům

Drtivá většina NASů má firmware (neboli operační systém) postavený na Linuxu. Tento fakt tedy mimo jiné určuje chování a správu systému i nastavení oprávnění jednotlivých souborů a složek. Z toho vyplývá, že každý uživatel si určuje typ přístupu (např. čtení, zápis, spouštění), který bude udělen ostatním uživatelům. A při modifikaci souboru, nebo stromu složek

vícera uživatelů najednou, je spuštěn systém pro zachování integrity dat, aby tato současná editace byla možná. [24], [26]

4.5 Souhrn datových úložišť

V předešlých kapitolách byly uvedeny typy datových úložišť, jenž by byla potenciálně vhodným řešením problematiky této práce. A v této kapitole bych rád shrnul klady a zápory jednotlivých architektur.



Obrázek 6 – Srovnání architektur [28]

Jak lze vidět, typů datových úložišť máme hned několik, avšak neexistuje jediné univerzální řešení, jenž by vyhovovalo ve všech situacích. V dnešní době s neustálým růstem dat se odpouští od nasazování úložišť typu DAS a většina organizací přechází na komplexnější systémy. Architektura SAN v porovnání s NAS má velice vysoké náklady na realizaci i údržbu a také je potřeba mít v organizaci vysoce kvalifikovaný personál pro správu složité struktury. Nicméně ve fázi odhadu nákladů při rozšiřování úložné kapacity těchto zařízení se SAN jeví jako výhodnější varianta. Jelikož zatímco náklady na správu rozšířeného NAS budou stoupat, v případě SAN tomu bude naopak. Na základě uvedených informací je možné konstatovat následující:

Tabulka 3 – Srovnání parametrů [Zdroj: Vlastní zpracování]

	DAS	NAS	SAN
Přístup k datům	Klienti i servery	Klienti i servery	Servery
Přenos dat	IDE / SCSI	TCP/IP, Ethernet	Fibre Channel
Průměrná kapacita (MB)	10^3	10^3-10^6	>10^6
Komplikovanost systému	Nízká	Střední	Vysoká
Náklady na správu (ku 1 GB kapacity)	Vysoké	Střední	Nízké

NAS řešení odpovídá převážně požadavkům menším a středním organizacím s homogenní interní sítí, kde není potřeba provozovat vysoce výkonný software a jedním z klíčových faktorů je i nízká cena a jednodušší správa.

Datové úložiště SAN se nasazuje tam, kde jsou klíčovými faktory hlavně spolehlivost, odolnost proti chybám a vysoký výkon. Tyto faktory bohužel NAS stále nesplňuje, a proto se nasazení SAN architektury stává standardem hlavně na poli HA (High Availability) aplikací. Vedle stále vysoké ceny se SAN potýká ještě s jedním nedostatkem a tím je problémový přístup k datovému úložišti ze strany klientů s různými operačními systémy, kdy dochází k nekompatibilitě souborových systémů a tedy problému s dostupností dat. Nicméně tento problém můžeme vyřešit implementací NAS, nebo nasazením hybridních systémů SAN, které umožňují přístup k datům na jiné úrovni.

4.6 Souborové systémy (FS)

Jak již bylo zmíněno, většina datových úložišť je spravována Linuxovými distribucemi a jinými operačními systémy vycházejících ze základů Unixu. Z tohoto důvodu se budu věnovat pouze vybraným třem souborovým systémům, které najdeme na drtivé většině zařízení.

4.6.1 Klíčové vlastnosti souborových systémů

Neustálé se zvyšující kapacita disků a další požadavky kladou stále vyšší nároky na vlastnosti moderních souborových systémů. Mezi poslední klíčové vlastnosti souborových systémů patří mimo jiné následující vlastnosti.

4.6.1.1 Žurnál

Souborové systémy s funkcí žurnálu zapisují plánované změny v datech do speciálního záznamu tzv. žurnálu ještě předtím, než je plánovaná série změn provedena. Jedná se o cyklický buffer a v případě, že dojde k výpadku v kterémkoliv okamžiku, je možné díky žurnálu následně velmi rychle a bezpečně uvést souborový systém do konzistentního stavu.

4.6.1.2 COW (Copy on write)

Tento transakční model funguje na principu, kdy veškerá změněná data jsou zapisována do nově alokovaných bloků (tj. původní blok není přepsán) a následně dochází k vytvoření i všech ostatních bloků dat, které ukazují na nově alokované bloky. Nakonec dochází k aktualizaci metadat, neboli přesměrování ukazatelů na nově vytvořený podstrom s bloky.

Díky tomuto systému je zabráněno vytváření nekonzistentních dat. Datové struktury (stromy), které již nejsou aktuální (tzn. není na ně ukazováno z aktuálního kořene), se postupně odstraňují. [35], [37]

4.6.1.3 Deduplikace

Deduplikace představuje speciální metodu komprimace dat, založenou na principu identifikace opakujících se datových bloků na jednom úložišti. Následně probíhá nahrazování *duplicitních* kopií pouhými odkazy na první uloženou část. Účelem je tedy úspora místa na datovém úložišti. Moderní souborové systémy (jako Btrfs a ZFS) s podporou deduplikace, mohou potencionálně ušetřit nemalé procento potřebné kapacity a snížit množství I/O operace, což má za následek zvýšení výkonu. [40]

K úspoře úložného prostoru dochází mimo jiné v případech:

- Virtualizovaného prostředí – Stejné OS mohou sdílet jádro, systémové knihovny, aplikace aj.
- Souborové servery
- Mail servery aj.

4.6.1.4 Snímky (Snapshoty) a klony

Souborové systémy s podporou metody *copy-on-write* mohou poměrně snadno (bez velké zátěže a bez velkého navýšení kapacity dat) vytvářet snímky (tzv. snapshoty) a klony. Vznik snímku probíhá tak, že strom s daty je označen k zachování – proces tedy nevyžaduje žádnou

režii. Takto vzniká snímek, jenž je stavem souborového systému v určitém čase. Až v případě kdy dojde ke změně dat, jsou tyto modifikovaná data zapsána do nového stromu. Postup vytváření snímků je opět atomické.

Klony se chovají jako plnohodnotné nové souborové systémy s možnostmi připojení a následného čtení i zápisu. Při modifikaci klonovaného systému dochází k vytváření nových datových bloků, ale nezměněné oblasti jsou nadále sdíleny. [37]

4.6.2 Ext4

Ext4 představuje žurnálovací souborový systém vyvinutý pro jádro Linux. Maximální velikost svazku činí 1EiB a velikost souboru až 16TiB (pro 4KiB bloky). Je zpětně kompatibilní se svým předchůdcem Ext3 a od roku 2015 podporuje také transparentní šifrování. [32]

Jedná se o následovníka nejpoužívanějšího souborového systému na Linuxu – ext3, u kterého byly vylepšeny datové struktury, což zvedlo výkon i stabilitu. Dnes je spíše na ústupu vůči *moderním* souborovým systémům viz. Btrfs a ZFS. Převážně z důvodů absence deduplikaci dat, podpory snapshotů a transparentní komprese, jenž je v experimentálním stavu. [32], [33]

4.6.3 Btrfs

Btrfs je souborovým systémem založeným na technologii COW, původně navržen společností Oracle Corporation pro operační systém Linux. Od počátku byl zaměřen na implementaci pokročilých funkcí se zaměřením na odolnost vůči chybám, možným opravám a snadnou správu. V současnosti jej lze považovat za hlavního konkurenta ZFS, jelikož disponuje většinou moderních vlastností viz. Tabulka 4 a navíc je šířen pod otevřenou licencí GPL. [34]

4.6.4 ZFS

ZFS byl vyvinut společností Sun Microsystems pro operační systém Solaris a je kombinací souborového systému a správce disků (Volume manager). Mezi hlavní přednosti patří podpora komprimace dat, transparentního šifrování, transakční model COW, práce se snapshoty a možnosti adresace až 2^{128} bitů dat, což by představovalo ~10^{24} 3 TB pevných disků. [35]

4.6.4.1 Zpool

Na rozdíl od běžných souborových systémů (např. Ext4), které potřebují pro podporu vícero úložných zařízení správce disků (např. LVM), ZFS je postaven nad virtuálními úložišti *Zpools*. Prostor v *Zpool* je tvořený virtuálními zařízeními *Vdevs*, kterými mohou být soubory, disky, standardní softwarový RAID-1 (zrcadlení), RaidZ-1/2/3, Hot Spare disk, zařízení určení jako cache, logovací zařízení. Všechna tato zařízení dovolují jednoduché přidání nového ZFS systému. Na druhou stranu jednou z hlavních nevýhod je nepřímá a komplikovaná možnost zmenšování *Zpools*. [36]

4.6.4.2 ZFS cache: ARC (L1), L2ARC, ZIL

V ideálních případech by všechna data měla být uložena v paměti RAM, avšak ZFS je poměrně náročné na tyto prostředky, což má za následek vysoké náklady na provoz. Z těchto důvodů jsou data ukládána do mezipaměti cache. Souborový systém využívá tuto vícevrstvou architekturu paměti cache pro urychlení čtení a zápisu, které můžeme rozdělit následovně:

- **ARC (L1):** První vrstva cache se nachází ve fyzické paměti počítače a využívá algoritmu (ARC). Jedná se o velice rychlou vyrovnávací paměť, která dokáže měnit svoji velikost podle potřeby. V případě potřeby existuje také možnost fixně stanovit její velikost pro zamezení problémů s nedostatkem případně přebytkem fyzické paměti. Pokud je server vybaven příliš málo paměti RAM, dochází k obrovskému snížení kapacity pro ARC, což výrazně zpomalí souborový systém a degradaci výkonu. [37]
- **L2ARC:** Tato vrstva cache je volitelná a představuje prostředníka mezi virtuální pamětí ARC a disky. Nejčastěji je v podobě SSD disků a dokáže výrazně zrychlit čtení. Nicméně jí nelze považovat za náhradu paměti RAM, a pokud má systém málo fyzické paměti, L2ARC bude mít minimální efekt, případně k žádnému zrychlení vůbec nedojde. [37], [38]
- **ZIL:** Druhá volitelná funkce cache, jenž představuje mezipamět pro synchronní zápis, čímž zrychluje NFS nebo zápis do databází. Všechna data se zapisují do ZIL logu, který je podobný běžnému žurnálu. Takto zapsaná data se čtou až v případě výpadku proudu, či problému v kernelu a slouží jako prevence proti vzniku nekonzistentního souborového systému. [37], [39]

4.6.5 Srovnání

Tabulka 4 – Vlastnosti souborových systémů [Zdroj: Vlastní zpracování]

	Ext4	Btrfs	ZFS
Vydání stabilní verze	2006	2013	2005
Licence	GPL	GPL	CDDL
Platforma (OS)	Linux	Linux	Linux, Solaris, *BSD
Velikost bloku	1 EiB	16 EiB	256 ZiB
Maximální velikost souboru	16 TiB	16 EiB	16 EiB
Žurnál	Ano	Ano	Ano
Komprese	Ne	Ano (zlib, LZO, lz4)	Ano (LZJB, gzip)
Šifrování	Ano	Ne	Ano
Deduplikace	Ne	Ano	Ano
COW	Ne	Ano	Ano
Snapshoty	Ne	Ano	Ano
RAID	Ano	Ano	Ano

Většina operačních systémů v komerčních zařízeních NAS je postavena na jádře Linux a zvláště proto jsem se zaměřil pouze na souborové systémy s podporou této platformy. Mezi jedny z aktivně vyvíjených a moderních souborových systémů bych zařadil právě výše uvedené (viz. Tabulka 4).

Jak je vidno, Ext4 má oproti svým konkurenčním souborovým systémům značné nevýhody, ať už v podobě maximální velikosti souboru nebo komprese. Avšak mnohem kritičtější je absence podpory deduplikace, Copy-on-Write a snímků (snapshotů). Z těchto důvodů bych dal přednost raději dvou zbývajícím souborovým systémům.

V případě komparace Btrfs a ZFS je situace dosti vyrovnaná, jelikož oba dva podporují vlastnosti moderních souborových systémů. Jako výhodu ZFS vidím podporu vícero OS, avšak na druhou stranu jsou zde komplikace kolem licence CDDL, která není kompatibilní s GPL a tudíž, vznikají problémy s implementací na linuxových distribucích. [41]

4.7 RAID

RAID je akronymem pro Redundant Array of Inexpensive/Independent Disks a představuje technologii, která umožňuje paralelní práci s vícero pevnými disky jako s jedinou datovou logickou jednotkou. A poskytuje kompromis mezi odolností proti výpadku jednoho či více

disků, výkonem a kapacitou. Kromě zvýšení rychlosti (distribuováním dat na více disků zároveň), poskytuje také možnost zvýšení odolnosti proti výpadkům formou redundance (disků), což ovšem jistým způsobem snižuje kapacitu pole. [30]

4.7.1 Hlavní rozdělení technologie RAID:

- Softwarový RAID (vlastnosti):
  - Nestojí žádné finanční náklady, pouze čas CPU.
  - Podpora všech typů RAID polí.
- Hardwarový RAID (vlastnosti):
  - Cena (2 000 Kč – 45 000 Kč).
  - Potřeba dalšího kusu hardwaru (řadič).
  - Vlastní dedikovaný procesor a paměť.
  - Možnost připojit záložní baterii pro případ výpadku napájení.
  - Obnova pole je možná i bez naběhnutí operačního systému.
  - Podpora jednotlivých typů RAID je závislosti na výběru konkrétního řadiče.

Třebaže z výše uvedeného výčtu vlastností HW RAID řadiče se může zdát jako daleko výhodnější řešení oproti softwarovému, nebudu se jím dále zabývat z důvodů nekompatibility s FreeNAS operačním systémem a ZFS souborovým systémem. Hardwarové RAID řadiče v kombinaci s FreeNAS komplikují výměnu disku a nesprávná konfigurace může mít za následek ohrožení integrity dat až jejich úplnou ztrátu. [29]

4.7.2 Typy RAID polí:

4.7.2.1 RAID 0 (Stripping)

Vzniká spojením dvou a více disků, kdy se data rozmisťují střídavě po všech discích z pole, avšak je zde absence redundance. Ztráta jediného disku má za následek ztrátu všech dat z pole. Na druhou stranu disponuje nejlepším výkonem a celková kapacita pole se rovná počtu disků. [30]

4.7.2.2 RAID 1 (Mirroring - zrcadlení) a ZFS Vdev

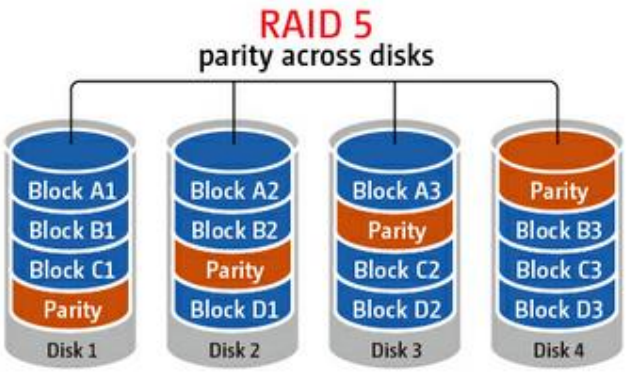
Všechna data jsou zrcadlena na všechny disky. Zaručuje tak nejjednodušší, nýbrž efektivní ochranu dat. V případě výpadku disku se pracuje s kopií, jenž je stále k dispozici. Nevýhodou je poloviční kapacita diskového pole.

Zrcadlení disků lze provést také na souborovém systému ZFS prostřednictvím Vdev. [30], [31]

Obrázek 7 – Schéma RAID 1 [31]

4.7.2.3 RAID 5 (RAIDZ1 vdev)

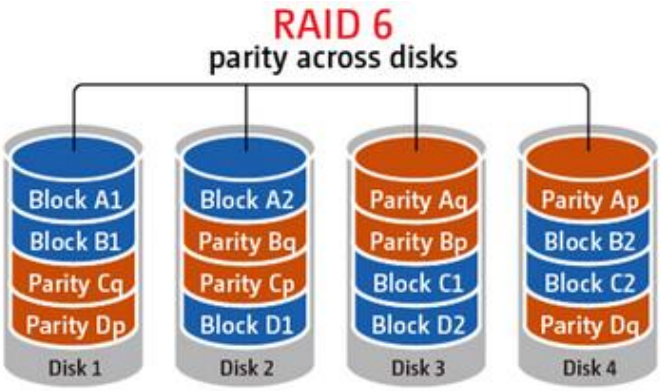
Pro vytvoření jsou nezbytné alespoň 3 disky. Data i paritní informace jsou rozmístěny střídavě po všech discích pole. Celková kapacita je ochuzena o celkovou velikost jednoho disku, jenž zabírají opravný kód. Opět lze využít paralelního přístupu k datům a diskové pole je odolné výpadku jednoho disku. [30], [31]



Obrázek 8 – Schéma RAID 5, RAIDZ1 [59]

4.7.2.4 RAID 6 (RAIDZ2 vdev)

Minimem pro vytvoření tohoto RAIDu jsou potřeba alespoň 4 disky. Jde o velice podobné provedení RAID 5 s tím rozdílem, že poskytuje vyšší bezpečnost – obsahuje 2 paritní bloky. Výkon je taktéž podobný RAIDu 5. [30], [31]



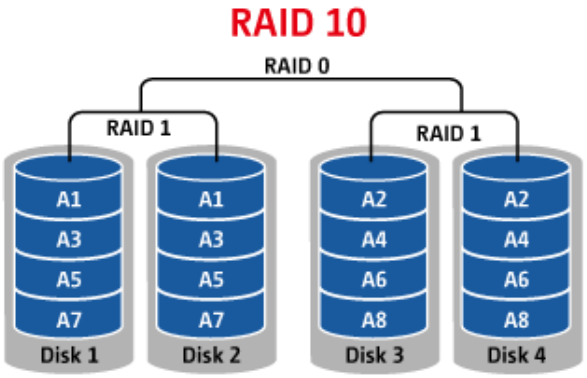
Obrázek 9 – Schéma RAID 6, RAIDZ2 [59]

4.7.2.5 RAIDZ3 vdev

RAIDZ3 vznikl jako reakce na RAID pole s disky o kapacitě 6-10TB, u kterých v případě selhání může trvat rekonstrukce chybějících dat velice dlouho (až týdny). Během této doby je zbytek disků daleko více vytíženo navíc z důvodu běžícího opravného procesu. Při použití RAIDZ3 je riziko spojené s výměnou disku ještě nižší, než v případě RAID 6. Tento typ RAIDu je opět velice podobný RAID6 (RAIDZ2), avšak disponuje až 3 paritními bloky. [30], [31]

4.7.2.6 Víceúrovňové typy RAID polí

Dále je možné setkat se i s kombinacemi předešlých typů RAID, jak těch běžných tak i RAIDZ. Častými kombinacemi RAID jsou 10, 50, 60 a 100. Výběr poté záleží na počtu dostupných disků a našich preferencích, zdali se rozhodnou pro vyšší rychlost za cenu menší odolnosti proti výpadkům, nebo opačně. A zdali jsme závislí na konkrétním souborovém systému, či nikoliv. Níže je uveden pouze schéma RAIDu 10 z důvodu využití v praktické části této práce.



Obrázek 10 – Blokové schéma RAID 10 [59]

4.7.2.7 Rezervní disk (Hot Spare)

Pojmem *Hot Spare* je často označován mechanismus k převzetí služby při selhání. Jedná se o disk, který není zapojen v poli RAID, ale jakmile dojde k havárii jednoho z využívaných disků, automaticky převezme jeho funkci a data se na něj začnou rekonstruovat bez zásahu člověka. Tento mechanismus významně snižuje dobu vystavení úložiště havárii dalšího disku a ztrátě dat, než je tomu u manuálního nahrazení.

4.8 Bezpečnost datových úložišť

Bezpečnost datových úložišť závisí na mnoha faktorech, v závislosti kterých může být úroveň rizika různě vysoká. Datová úložiště připojená do rozsáhlejších sítí jsou daleko víc vystavena hrozbám, než malé interní sítě fyzicky oddělené od internetu. Přesto k minimalizaci rizik je nutné stanovit a implementovat bezpečnostní postupy a pravidla. To nás přivádí k bližšímu zaměření se na konkrétní datové úložiště a jeho přístupové body. Veškeré potencionální přístupové body (např. osobní počítače v síti) k datovému úložišti by měly být analyzovány a měla by proběhnout identifikace možných zranitelností. [24]

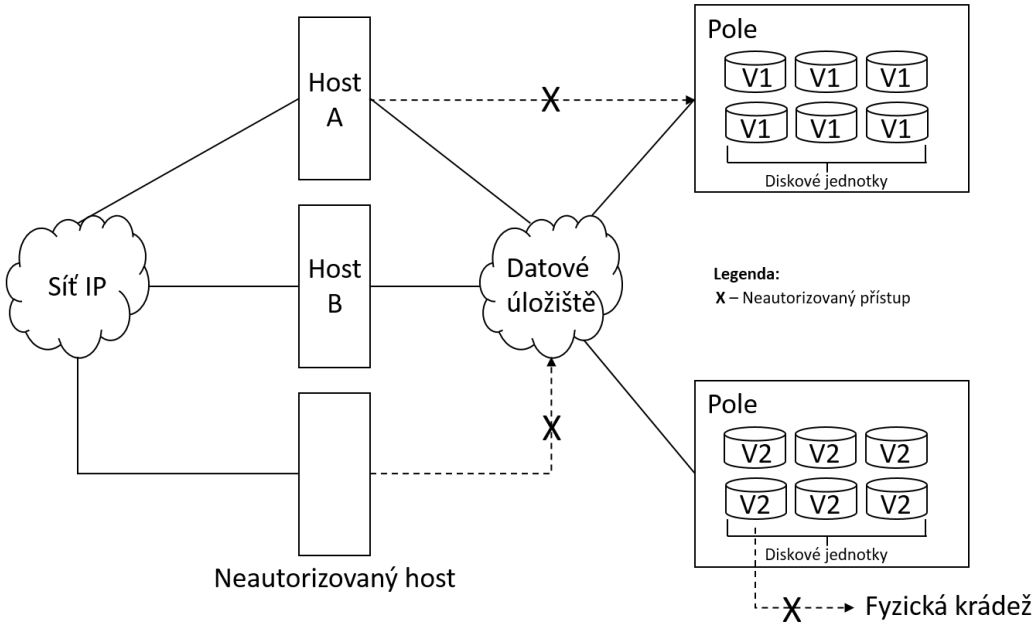
Jednotlivé hrozby v závislosti na způsobu přístupu k datovému poli je možné rozdělit do následujících oblastí:

- Přístup aplikací,
- Management přístupu,
- Zálohování, replikace, archivace.

4.8.1 Zabezpečení přístupu aplikací

Tato oblast může zahrnovat pouze ty aplikace, které mají přístup k souborovým systémům a databázovému rozhraní. Podstatným krokem při zabezpečení přístupu aplikací je opět identifikace hrozeb a přijetí nápravných opatření.

Na Obrázek 11 je znázorněn možný přístup k datům v síťovém prostředí. Potencionální hrozby jsou znázorněny písmenem X, kdy např. host A může pomocí *IP Spoofing* útoku získat identitu nebo práva hosta B za účelem přístupu do vedlejšího pole. Další hrozbu představuje neautorizovaný přístup třetí osoby k datovému úložišti skrze síť, nebo fyzicky. [24]



Obrázek 11 – Bezpečnostní hrozby [Zdroj: Vlastní zpracování]

4.8.2 Management přístupu

Řízení přístupu má možnost definovat přístupová práva k jednotlivým souborům a adresářům, ať už pro skupiny nebo jednotlivé uživatele. Pokročilé souborové systémy mají podporu implementace ACL (Access Control Lists), což jsou atributy, které umožňují specifičtější nastavení pro konkrétní uživatele a procesy. [24]

4.8.2.1 ACL (Windows platforma)

Používá dva druhy ACL, kterými jsou DACL (Discretionary Access Control Lists) a SACL (Systém Access Control Lists).

- **DACL** je běžně označován jako ACL, který určuje řízení přístupu.
- **SACL** umožňuje logovat přístupy k zabezpečeným objektům a určuje, nad jakými přístupy je nutno provést audit. [24]

4.8.2.2 ACL (Unix platforma)

V případě operačních systémů založených na Unixu je uživatel pouze *abstraktním pojmem,* který označuje logickou entitu pro přiřazení vlastnických práv a privilegií pro konkrétní soubory nebo provozování dané služby v systému. Uživatelem může být buď samotná osoba, nebo OS. Operační systém NASu identifikuje jednotlivé uživatele pomocí ID (UID), nebo

lze nastavit práva pro celou skupinu uživatelů (GID). Více k tomuto tématu je napsáno v předešlé kapitole 4.4.2.2. [24]

4.8.3 Šifrování

Jedním z nejdůležitějších aspektů zabezpečení dat je jejich ochrana na samotných diskových polích. Ohrožení na této úrovni zahrnuje manipulaci s daty a tedy narušení jejich integrity, případná krádež úložného média ohrožuje dostupnost a důvěrnost informací. Zvolením dostatečně silného šifrování je možné všechny tyto hrozby eliminovat. Stejně tak je důležité rozhodnout o způsobu zajištění, aby data odstraněná na vyřazených úložných mediích, nebude možné zpětně rekonstruovat.

Šifrování ZFS:

Budeme-li uvažovat šifrování na souborovém systému ZFS v kombinaci s operačním systémem založeným na Linuxu případně BSD, nelze využít nativního šifrování tohoto souborového systému kvůli nekompatibilitě licencí. Nicméně existují i jiné způsoby jak data šifrovat např. pomocí nástroje Dm-crypt/LUKS, eventuálně Geli (s podporou AES, Blowfish a 3DES). [42]

Při použití těchto externích nástrojů, dochází nejprve k zašifrování všech jednotek diskového pole a následně je možné vytvořit jednotlivé Zpools. Tímto způsobem je také zaručena bezpečnost dat na diskové jednotce i po vyjmutí z diskového pole. [42]

Šifrování Btrfs:

U tohoto souborového systému nebylo dosud implementováno nativní šifrování, a proto stejně tak jako ZFS musíme využít externích nástrojů jako Dm-crypt/LUKS, nebo eCryptfs. ECryptfs na rozdíl od Dm-crypt/LUKS šifruje pouze na úrovni souborového systému a tak lze šifrovat pouze vybrané složky a soubory. [34]

Tyto nástroje je možné využít v kombinaci s RAID poli a v podstatě zde neexistují limitující faktory oproti nativnímu šifrování.

4.8.4 Kerberos

Kerberos je síťovým autentizačním protokolem, který byl navržen ke komunikaci klient / server za použití symetrického šifrování. V případě nasazení tohoto protokolu, zabezpečení již nezávisí na všech klientských počítačích, ale pouze na těch, kterým byl vydán validní

tiket opravňující uživatele ke komunikaci s řídícím serverem. Kerberos tak zabraňuje odposlechům nebo zopakování již navázané komunikace a zaručuje tak integritu dat. Při nasazení v kombinaci s NAS úložištěm se Kerberos nejčastěji používá hlavně při ověřování proti Microsoft Active Directory, i když může být použit také s nástroji pro autentizaci služeb podporující Unixové systémy a protokoly CIFS, NFS aj. [43]

II. PRAKTICKÁ ČÁST

5 NÁVRH STRUKTURY DATOVÉHO ÚLOŽIŠTĚ

V teoretické části byly shrnuty současné trendy a moderní technologie, které by byly vhodné pro řešení problematiky této diplomové práce. Na základě shod požadavků z kapitoly 1 a uvážených technických řešení, bude dále navržena optimální struktura datového úložiště.

5.1 Srovnání vhodných typů úložišť

Po seznámení se se současnými architekturami z oblasti datových úložišť je výběr vhodného typu úložiště poměrně jednoznačný. Na základě souhrnu vlastností jednotlivých architektur viz. Tabulka 3 a požadavků na kapacitu (alespoň 30 TB), dostatečnou propustnost a konektivitu (4x 1 GbE) a redundantní zdroj, můžeme ihned vyloučit úložiště DAS. Při rozhodování se mezi úložišti NAS a SAN je dobré uvážit jejich cenu a přínos pro laboratoř. Oba druhy úložišť mohou být dostatečně dimenzované k potřebám laboratoře, avšak obrovskou nevýhodu představuje cena za vybudování infrastruktury SAN (viz. první sloupec zprava v

Tabulka 5) v porovnání s NAS úložišti. Přestože jsou ceny v níže uvedené tabulce spíše orientační, třikrát dražší SAN úložiště nemá rozumné opodstatnění v případě požadavků laboratoře.

Tabulka 5 – Komparace nejvhodnějších produktů na trhu [Zdroj: Vlastní zpracování]

	Synology RackStation RS3614xs+	QNAP TVS-1271U-RP-I7-32G	iXsystems FreeNAS 2U	EMC VNXe1600 SAN Storage
Typ úložiště	NAS	NAS	NAS	SAN
Konektivita	SATA II, III	SATA II, III	SATA (II) III, SAS	4 x 1 GbE/10GbE iSCSI, 4 x 8 Gb Fibre Channel
Celkový počet šachet pro disky	12x (3,5" SATA III HDD / 2,5" SATA III)	12x (3,5" SATA III HDD / 2,5" SATA III SDD)	12x 3,5" SATA III / SAS HDD	25 x 2.5" SAS/Flash (U2) / 12 x 3.5" (NL)SAS/Flash (2U)
Maximální interní hrubá kapacita	96 TB (8 TB HDD x 12)	96 TB (8 TB HDD x 12)	96 TB	400 TB
Řadič pevných disků	RAID (JBOD, 0, 1, 5, 6, 10) SW i HW	RAID (JBOD, 0, 1, 5, 6, 10) SW i HW	ZFS RAIDZ	RAID (10, 5, 6) SW i HW
SSD Cache	Ano	Ano	Ano	Ano

Operační systém	Upravený Linux - DSM	Upravený Linux - QTS	FreeNAS	IBM AIX, Oracle Linux, RedHat Enterprise Linux, Solaris …
Souborový systém interních HDD	Ext4, Btrfs	Ext4	ZFS	V závislosti na OS
Napájecí zdroj	2x 460W (Záložní / za provozu přepínatelný zdroj)	2x 500W (Záložní / za provozu přepínatelný zdroj)	2x 1280W (Záložní / za provozu přepínatelný zdroj)	4x
CPU	Intel Xeon E3-1230 v2	Intel Core i7-4790S 3,2 GHz	Intel E5-2609v2	2 x Intel Pentium 1403 v2 2-Core 2.6 GHz
RAM	8 GB DDR3 ECC (max. 4x 8 GB)	32 GB DDR3 ECC (max. 4x 8 GB)	32 GB DDR3 ECC (max. 128 GB)	16 GB
LAN	RJ-45 4x 1GbE (s podporou Link Aggregation / Failover)	RJ-45 4x 1GbE (s podporou Link Aggregation / Failover)	4x 1 GbE / Možný upgrade na 10GbE	1 GbE / 10GbE iSCSI
Cena	110 500 Kč	91 400 Kč	*106 300 Kč	302 000 Kč

* Po zkontaktování výrobce mi byla sdělena tato orientační cena (včetně DPH), nutno však připočíst také cenu za clo a dopravu z USA do ČR, jelikož firma nemá v Evropě sklady.

Při výběru vyhovujících úložišť NAS byl kladen důraz především na splnění stanovených požadavků a následně na cenu úložišť. Pro srovnání byly vybrány produkty dvou světově známých výrobců (QNAP a Synology) a dále také NAS od firmy iXsystems, jenž je certifikován pro podporu FreeNAS OS se souborovým systémem ZFS.

Všechny srovnávané NAS úložiště jsou v šasi provedení uzpůsobenému k instalaci do racku. Menší NAS úložiště v samostatných PC skříních nesplňovaly požadované kritéria, přestože byly cenově daleko příznivější.

5.2 Návrh datového úložiště na míru

Ne vždy je nezbytné spokojit se pouze s nabídkou hotových produktů na trhu a v případě specifických požadavků je možné pořídit si datové úložiště přesně na míru. Proto se budu dále v této kapitole věnovat návrhu takovéhoto řešení. Výše uvedené podnikové produkty následně porovnám s navrženou optimální architekturou NAS.

Vlastní řešení však vyžadují také specifický přístup, jelikož nelze použít uzavřený OS od výše zmíněných výrobců NASů. Z toho důvodu jsem vybral nejrozšířenější alternativy těchto OS.

Tabulka 6 – Komparace open-source OS [45]

	XPEnology	OpenMediaVault	FreeNAS
Postaveno na OS	Synology DSM	Debian	FreeBSD
Architektura CPU	x86	x86, ARM (experimentální)	x86
32 bit / 64 bit hardware	Pouze 64bit	32bit i 64bit	Pouze 64bit
Podpora souborových systémů	EXT3/EXT4/BTRFS	EXT3/EXT4/XFS/JFS/NTFS/FAT32/(ZFS, Btrfs experimentální)	ZFS/UFS
Podpora pluginů	Ano	Ano	Ano
Počet vývojářů	x	6	72
Počet změn [za posledních 12 měsíců]	x	407	1 606

Všechny tyto OS jsou zaměřeny primárně na architekturu x86_64 s podporou šifrování, většiny protokolů (NFS, CIFS, FTP aj.) a také velkého množství pluginů, díky kterým lze doinstalovat systém zálohování, Owncloud a další dodatečný software. [44]

Mnohem podstatnější je ale fakt, že jsou tyto OS vyvíjeny převážně komunitami nadšenců a neexistuje zde žádná zodpovědnost nebo garance funkčnosti a stability. Verze systémů jsou vydávány podle potřeb a ochoty lidí v komunitě. Mezi markantní rozdíly bych pak zařadil podporu odlišných souborových systémů a zaměření jednotlivých projektů na různé skupiny lidí. Zatímco XPEnology cílí na lidi se zkušenostmi se Synology DSM a také na NAS úložiště pro malé a střední firmy, OpenMediaVault přichází s vlastním řešením. Podporuje totiž i 32bit systémy, architekturu ARM a širší zástup souborových systémů. Kvůli zatím experimentální podpoře Btrfs a ZFS se hodí spíše opět pro malé a střední firmy. Posledním kandidátem je operační systém FreeNAS s obrovskou základnou členů a vývojářů. Jako jediný je možný zakoupit společně s certifikovaným hardwarem a podporou od iXsystems. Hlavní výhodu vidím v ZFS a zaměřením na velké produkční systémy. [45]

Na základě srovnání vybraných OS lze usoudit, že nejvhodnějším systémem pro připravované datové úložiště bude FreeNAS. Díky souborovému systému ZFS a počtu vývojářů, kteří jsou zárukou progresivního vývoje tohoto OS.

5.2.1 Klady a zápory

Důvody proč se rozhodnout pro stavbu vlastního řešení jsem shrnul v následující tabulce:

Tabulka 7 – Výhody a nevýhody vlastního NAS provedení [Zdroj: Vlastní zpracování]

Řešení na míru	Konfigurace obsahuje přesně to, co chceme bez přebytečných komponent	**Klady**
Podpora rozličných OS	Kdykoliv je možný přechod na novější či jiný OS	
Instalace vlastního SW	Otevřený OS nabízí možnosti implementace vlastního softwaru	
Vlastní správa OS	Veškeré problémy s kompatibilitou a chyby OS musíme řešit vlastními silami	**Zápory**
Návrh konfigurace	Návrh systému vyžaduje čas a patřičné znalosti	

5.2.2 Výběr komponent

Při výběru komponent jsem se zaměřil pouze na takové, jenž naplní požadavky kapitoly 1 a budou i jistou zárukou pro škálovatelnost NASu do budoucích let.

5.2.2.1 Základní deska

Při výběru základní desky je dobré uvážit v první řadě samotnou architekturu procesoru. V současné době můžeme na trhu narazit na zvyšující se oblibu architektury ARM, které začíná mít své postavení také na poli serverů. Protože má však tato architektura zatím velmi malou podporu ze strany operačních systémů, vybíral jsem pouze mezi produkty s paticí pro Intel x86_64.

Tabulka 8 – Komparace základních desek [Zdroj: Vlastní zpracování]

	ASROCK E3C236D4M-4L	ASUS P10S-C/4L	Supermicro MBD-X11SSi-LN4F-B	Supermicro MBD-X10SDV-6C-TLN4F-O
LAN	3x RJ45 GLAN by Intel i210 +1x RJ45 GLAN by Intel i219	4x Intel I210AT + 1x Mgmt LAN	4x Intel I210AT	1x Intel Dual port Gigabit Ethernet LAN, +1x Intel Dual port 10GBase-T Ethernet LAN
RAM	4x DDR4 2133 ECC (Max. 64GB)	4x DDR4 2133 ECC (Max. 64GB)	4x DDR4 2133 ECC (Max. 64GB)	4x DDR4 2133MHz ECC (max.128GB)
Patice pro CPU	Socket LGA 1151	Socket LGA 1151	Socket LGA 1151	Intel Xeon D SoC D-1528
SATA	8x SATA3 6Gb/s	6x SATA3 6Gb/s	6x SATA3 6Gb/s	6x SATA3 6Gb/s
PCiE	1x PCI-E 3.0 x 16 +1x PCI-E 3.0 x 4	1x PCI 32bit/33MHz, +1x PCI-E x8, +1x PCI-E x16	1x PCI-E 3.0 x8 (x16), 1x PCI-E 3.0 x8 (x8), 1x PCI-E 3.0 x4	1× PCI-E 3.0 16
M.2		2x M.2 (2280/2260/2242)	1× M.2 NGFF 2280, 2260, 22110	1× M.2 (2242/2280)
Provedení desky	ATX	ATX	ATX	Mini-ITX
Cena	7 600 Kč	6 700 Kč	9 000 Kč	18 700 Kč

Všechny čtyři uvedené základní desky jsou vybaveny velice podobnými komponenty. Z důvodu vyhovění stanoveným požadavkům jsem vybíral desky pouze se čtyřmi GbE porty, díky čemuž se vyhneme riziku nekompatibility externích síťových karet (z důvodu uzavřeného kódu ovladačů), uvolněním PCiE slotu a taktéž dosáhneme nižší ceny. Dále jsem při výběru kladl důraz na podporu ECC pamětí a dostatečného počtu SATA portů pro pevné disky. Výjimku mezi deskami tvoří Supermicro MBD-X10SDV-6C-TLN4F-O, která je díky provedení Mini-ITX rozměrům vhodná i pro instalaci do menších skříní a také je již osazena pasivně chlazeným, přesto výkonným procesorem s 6 jádry (12 vlákny) vyvinutým pro účely SAN, NAS a výkonných síťových prvků. Jako jediná z výše uvedených desek poskytuje škálovatelnost paměti RAM až do výše 128 GB, čemuž také odpovídá cena.

5.2.2.2 Procesor

Při analýze trhu a hledání nejvhodnějších procesorů byla značně limitujícím faktorem poměrně nové patice LGA 1151, kterou momentálně podporuje pouze pár procesorů, na druhou

stranu takto získáme nejmodernější technologie, u kterých se do budoucna vyhneme nekompatibilitě komponent.

Tabulka 9 – Komparace procesorů [Zdroj: Vlastní zpracování]

	E3-1220 v5	E3-1260L v5	Intel Core i5-6600
Počet jader (vlákna)	4 (4)	4 (8)	4 (4)
Základní frekvence	3 GHz	2,9 GHz	3,3 GHz
Frekvence s Turbo	3,5 GHz	3,9 GHz	3,9 GHz
L3 Cache	8 MB	8 MB	6 MB
RAM	DDR4-1866/2133, DDR3L-1333/1600 @ 1.35V		
Intel AES-NI	Ano		
Podpora ECC	Ano	Ano	Ne
TDP	80 W	45 W	65 W
Cena	6 000 Kč	8 700 Kč	6 200 Kč

Všechny tři uvedené produkty jsou na základě porovnání s procesory z Tabulka 5 výkonově dostačující, proto vidím jako klíčový faktor podporu ECC a Intel AES-NI. Pro dosažení maximálního výkonu bych doporučil E3-1260L v5 i přes vyšší cenu.

5.2.2.3 Paměti RAM

U drtivé většiny produkčních serverů a datových úložišť je kladen veliký důraz na integritu dat. Z tohoto důvodu je více než doporučeno alespoň zvážit pořízení pamětí RAM s ECC. Zvláštní důraz je poté kladen na tuto technologii v případě zamýšleného použití ZFS, které nedisponuje žádným opravným nástrojem a v případě nekonzistentního souborového systému.

Tabulka 10 – Porovnání pamětí RAM [Zdroj: Vlastní zpracování]

CRUCIAL 32GB (2x16GB) DDR4 2133, ECC, Dual Ranked	4 900 Kč
CRUCIAL 32GB (4x8GB) DDR4 2133, ECC, Dual Ranked	7 600 Kč
CRUCIAL 32GB (4x8GB) DDR4 2133	3 100 Kč
CRUCIAL 64GB (4x16GB) DDR4 2133, ECC, Dual Ranked	9 800 Kč

Jak je z tabulky zřejmé, paměti s technologií ECC jsou znatelně dražší, nicméně k minimalizaci případných problémů s datovým úložištěm bych silně doporučil raději připlatit za paměti s podporou ECC. Dalším aspektem ke zvážení je počet instalovaných modulů. Osazení 4x 8GB pochopitelně poskytuje vyšší rychlost zápisu i čtení než při nasazení 2x 16GB.

5.2.2.4 Řadiče HBA / HW RAID

Z důvodu škálovatelnosti datového úložiště bude potřeba osadit základní desku také řadičem, který poskytne další SATA porty pro pevné disky. V tomto případě se nabízí dvě možnosti a to pořídit si hardwarový RAID řadič, nebo si vystačit pouze s HBA expandérem. Budu-li uvažovat nasazení ZFS, má hardwarový RAID řadič oproti HBA značné nevýhody. První z nevýhod je fakt, že kvalitní řadič RAID stojí dost peněz (až v řádech desetitisíc korun) a dále podle zdrojů [29] a [46], způsobuje systému ZFS komplikace. Z těchto důvodů jsem vybral dva HBA řadiče s 8 interními SATA III porty.

Tabulka 11 – HBA řadiče [Zdroj: Vlastní zpracování]

LSI SAS 9207-8i 6Gb/s SATA/SAS 8 int. portů, x8 PCIe	6 700 Kč
ADAPTEC HBA 7805H Single SAS/SATA 8 int. portů, x8 PCIe	7 050 Kč

Podle seznamů referencí uživatelů a doporučení vývojářů FreeNAS [29] je mnohem vhodnější používat HBA řadiče od firmy LSI. U linuxové distribuce OpenMediaVault jsou plně podporované oba řadiče.

5.2.2.5 SSD Cache

Jak již bylo naznačeno v kapitole 4.6.4.2, moderní souborové systémy jako je ZFS disponují zabudovanými mechanismy (L2ARC, ZIL) pro zvýšení rychlosti zápisu i čtení dat z disků. Podobné mezipaměti cache (BCache, LVMCache) lze použít také i u jiných souborových systémů (Btrfs, Ext4) a to v kombinacemi nejlépe s SSD disky.

Tabulka 12 – Porovnání parametrů SSD disků [Zdroj: Vlastní zpracování]

	Intel SSD Pro 5400s	Intel SSD 750	Intel SSD DC P3500
Rozhraní	SATA 6Gb/s	PCIe NVMe 3.0 x4	PCIe NVMe 3.0 x4
Rychlost (Čtení / Zápis)	560/480 MB/s	2400/1200 MB/s	2500/1700 MB/s
Formát	Interní 2,5" SSD	2,5" SSD / HHHL (CEM2.0)	2,5" SSD / HHHL (CEM2.0)
Technologie SSD	TLC	MLC	MLC
Kapacita	480 GB	400 GB	400 GB
Enhanced Power Loss Data Protection	Ne	Ano	Ano
End-to-End Data Protection	Ano	Ne	Ano
Cena	5 250 Kč	12 300 Kč	10 500 Kč

Mít systém osazený SSD diskem v roli Cache paměti není nutností a s přihlédnutím na cenu se může zdát jako přebytečná investice. Nicméně v závislosti na velikosti datového pole a očekávaných objemů přesouvaných dat bych instalaci SSD disku rozhodně doporučil.

Při rozhodování se nad konkrétním produktem, je dobré zvážit rozhraní, přes které budeme zařízení připojovat. Jak je z tabulky patrné, zařízení se SATA 3 konektorem je dvakrát levnější než moderní technologie PCIe NVMe 3.0 x4. S cenou je také spjata použitá technologie disku, kdy SSD s TLC bude mít nižší životnost než disky s MLC *buňkami* a dále rychlost těchto zařízení, kdy i rychlost zápisu PCIe NVMe 3.0 x4 může být až dvojnásobná rychlosti SATA 3. Dalším důležitým aspektem SSD disků podpora *Enhanced Power Loss Data Protection*, která zabraňuje ztrátě dat při náhlém výpadku elektřiny. A nakonec technologie *End-to-End Data Pro-tection* (kontrola integrity dat) je spíše už přidanou hodnotou daného produktu. [47]

5.2.2.6 Pevné disky (HDD)

Na trhu najdeme obrovské množství pevných disků s rozličnými parametry. Klíčovými parametry pro naše účely je port SATA 3 a certifikace k provozu 24/7 (tedy vyhnout se diskům určeným do stolních PC). Dále bychom neměli zapomenout na velikost Cache a rychlost otáček, které ovlivňují rychlost datového pole.

Do následující tabulky jsem zahrnul pouze takové velikosti disků, které v kombinaci s RAID polem 6 a 10 vyhovují požadavku (~30 TB) z kapitoly 1. RAID pole 6 a 10 jsem vybral na základě nejlepšího poměru ceny a poskytované bezpečnosti. [47]

Tabulka 13 – Porovnání RAID polí [Zdroj: Vlastní zpracování]

Počet osazených HDD	Velikost jednoho HDD [TB]	Před / po formátování [TB]	Cache disku	Celková cena s 1 Hot Spare diskem	
10	4	32 / 29,8	64MB	50 600 Kč	RAID 6
7	**6**	**30 / 27,9**	**64MB**	**55 200 Kč**	
7	6	30 / 27,9	128MB	64 400 Kč	
6	8	32 / 29,8	64MB	66 500 Kč	
14	4	28 / 26	64MB	69 000 Kč	RAID 10
10	**6**	**30 / 27,9**	**64MB**	**75 900 Kč**	
10	6	30 / 27,9	128MB	88 550 Kč	
8	8	32 / 29,8	64MB	85 500 Kč	

Ve všech případech kombinací počtů a velikostí disků jsem přebíral ceny disků výrobce Western Digital, řady Red. Navíc je dobrým zvykem kombinovat disky z různých sérií za účelem minimalizace výskytu havarijního stavu (např. v případě chyby v jedné ze sérií disků) celého pole najednou. A proto nutno také podotknout, že ceny disků z různých sérií a od různých prodejců, které je možné zakoupit v delším časovém horizontu, budou mít proměnlivou cenu a proto je konečná cena za diskové pole pouze orientační.

Z výše uvedené Tabulka 13 vyplývá, že výsledné požadované diskové kapacity dosáhneme již s polem o 6 pozicích pro HDD o velikosti 8 TB, avšak vzhledem k dalším možnostem pozdějších rozšíření se jako výhodnější varianta jeví diskové pole s 12 a více HDD sloty, kdy není třeba hned na začátku mít disky obsazeny všechny pozice. Rozložení kapacity na větší počet disků (stejně tak modulů RAM) pak také příznivě ovlivní výslednou rychlost I/O operací pole. [50]

5.2.2.7 Šasi

Na základě provedené analýzy počtu potřebných disků pro dosažení požadované diskové kapacity, jsem vybíral také velikost šasi. Budu-li brát v úvahu možné umístění NAS úložiště v laboratoři i serverovně, uvedu dále šasi vhodná pro oba případy.

Obrázek 12 – Corsair Obsidian Series 900D [48]

První variantou vhodného šasi je skříň Corsair Obsidian Series 900D v provedení Bigtower, a proto se hodí jak do serverovny tak i do laboratoře. Skříň nepotřebuje žádné speciální chlazení nebo speciální umístění v prostoru místnosti.

Tabulka 14 – Parametry Corsair Obsidian Series 900D [Zdroj: Vlastní zpracování]

Druh skříně:	Bigtower
Podporované formáty základních desek:	ATX, Extended ATX, HPTX, Micro-ATX, Mini-ITX
Počet interních 3,5" pozic:	9
Počet externích 5,25" pozic:	4
Druh a počet napájecích zdrojů:	ATX (2x)
Cena	9 100 Kč

Hlavní výhody vidím ve variabilitě podporovaných formátů základních desek, kdy je možné osadit jakoukoliv desku z Tabulka 8 a v tomto případě bych preferoval instalaci základní desky Mini-ITX Supermicro MBD-X10SDV-6C-TLN4F-O. Dále tato skříň disponuje celkem 13 pozicemi pro HDD, což zaručuje dostatečné množství disků k vytvoření RAID 6 i 10 (při kapacitě 30TB), přidáním Hot Spare disku a ještě zbydou neosazené pozice pro budoucí škálovatelnost pole. Poslední výhodou mezi skříněmi stejného druhu je možnost instalace až 2 ATX zdrojů.

Obrázek 13 – SUPERMICRO 3U rack šasi CSE-836BA-R920B [49]

Jako druhou variantu jsem vybral šasi 3U do *rackové* skříně. I přes omezující fakt, že je toto provedení vhodné pouze pro umístění do serverovny, má nespočet výhod. Na přední straně se nachází 16 Hot-swap pozic pro 3,5“ disky a na straně zadní jsou umístěny další 2 pozice pro 2,5“ Hot-swap. Tyto Hot-swap šachty jsou velikou výhodou oproti předchozí skříni Corsair, jelikož nám umožní připojení/odpojení disků bez nutnosti vypnutí systému.

Tabulka 15 – Parametry SUPERMICRO CSE-836BA-R920B [Zdroj: Vlastní zpracování]

Druh skříně:	Rack šasi 3U
Podporované formáty základních desek:	13.68" x 13", E-ATX, ATX
Počet interních 3,5" pozic:	16x Hot-swap
Počet externích 5,25" pozic:	0
Druh a počet napájecích zdrojů:	Redundantní 920W
Cena	30 000 Kč

Díky podpoře formátu ATX základních desek, bych pro instalaci volil buďto ASUS P10S-C/4L, nebo Supermicro MBD-X11SSi-LN4F-B, která je pochopitelně doporučována stejným výrobcem, což je zárukou stoprocentní kompatibility.

5.2.3 Cenová kalkulace

Aby bylo možné objektivně srovnat nabízené hotové NAS úložiště s navrženými konfiguracemi, je záhodno uvážit taktéž ceny kompletních sestav.

Tabulka 16 – Konfigurace v bigtower skříni [Zdroj: Vlastní zpracování]

	Komponenty	**Cena**
Druh skříně:	Bigtower - Corsair Obsidian Series 900D	9 100 Kč
Základní deska	Supermicro MBD-X10SDV-6C-TLN4F-O	18 700 Kč
Procesor	Intel Xeon D SoC D-1528	V ceně desky
Paměť RAM	CRUCIAL 32GB (4x8GB) DDR4 2133, ECC	7 600 Kč
SSD disk	Intel SSD DC P3500	10 500 Kč
Řadič	LSI SAS 9207-8i	6 700 Kč
HDD disky	7x 6TB (64MB) RAID 6 + Hot-Spare	55 200 Kč
Ostatní	Kabeláž, zdroje, chadiče, aj.	10 000 Kč
Cena celkem		**117 800 Kč**

Vypočítaný průměrný příkon této sestavy (při provozu 24/7) by měl dosahovat přibližně ~225W, což při ceně 4,80 Kč/kWh vychází na spotřebu energie kolem **1 971 kWh**, tedy nákladům ve výši **9 461 Kč za rok**.

Tabulka 17 – Konfigurace v rack šasi [Zdroj: Vlastní zpracování]

	Komponenty	**Cena**
Druh skříně:	Rack šasi - 3U CSE-836BA-R920B	30 000 Kč
Základní deska	Supermicro MBD-X11SSi-LN4F-B	9 000 Kč
Procesor	E3-1260L v5	8 700 Kč
Paměť RAM	CRUCIAL 32GB (4x8GB) DDR4 2133, ECC	7 600 Kč
SSD disk	Intel SSD DC P3500	10 500 Kč
Řadič	LSI SAS 9207-8i	6 700 Kč
HDD disky	10x 6TB (64MB) RAID 10 + Hot-Spare	75 900 Kč
Ostatní	Kabeláž, chladiče, aj.	4 000 Kč
Cena celkem		**152 400 Kč**

Průměrný příkon celé sestavy (při provozu 24/7) by měl dosahovat přibližně ~310W. Při ceně 4,80 Kč/kWh pak vychází spotřeba energie na **2 715,6 kWh** a **13 000 Kč za rok**.

Souhrn:

Obě výše uvedené konfigurace jsou do jisté míry osazeny stejnými komponenty až na druhy provedení šasi a použitím počtu HDD disků. Ke hlavním přednostem sestavy z

Tabulka 16 patří použití druhu skříně – Bigtower, jenž umožňuje umístění NAS úložiště v serverovně i laboratoři. Navíc pasivně chlazený procesor sníží hlučnost celé sestavy, což shledávám jako další výhodu v případě umístění do laboratoře. Na druhou stranu kvůli menšímu počtu pozic pro HDD a zachování možnosti škálovatelnosti bude vhodnější pro tuto sestavu použít RAID 6, což má za následek (oproti RAID 10) nižší rychlost zápisu i čtení, větší náchylnost na destrukci pole a pomalejší rekonstrukci RAIDu. Položka ostatní nakonec zahrnuje také prostředky mj. pro zakoupení dvou ATX zdrojů. Celková vyšší cena konfigurace v provedení rack skříně (viz. Tabulka 17) je opodstatněná využitím spolehlivějšího RAID 10, lepší možností škálovatelnosti a provedením této skříně, která obsahuje navíc hot-swap šachty a dva zabudované zdroje.

5.3 Srovnání dostupných NAS úložišť a sestavy na míru

Shrnutí a kalkulace z předešlé kapitoly jasně ukázaly, že mnohem výkonnější, bezpečnější a více škálovatelnou konfigurací je sestava v rackovém šasi. Tuto sestavu jsem srovnal v následující tabulce s produkty z Tabulka 5.

Tabulka 18 – Komerční produkty versus vlastní sestava [Zdroj: Vlastní zpracování]

	Synology RackStation RS3614xs+	QNAP TVS-1271U-RP-I7-32G	ixSystems FreeNAS 2U	Vlastní sestava v Rack 3U šasi
Konektivita	SATA II, III	SATA II, III	SATA (II) III, SAS	SATA (II) III, SAS
Diskový úložný prostor	12x (3,5" SATA III HDD / 2,5" SATA III)	12x (3,5" SATA III HDD / 2,5" SATA III SDD)	12x 3,5" SATA III / SAS HDD	16x 3,5" SATA III / SAS HDD
Maximální interní hrubá kapacita	96 TB (8 TB HDD x 12)	96 TB (8 TB HDD x 12)	96 TB (8 TB HDD x 12)	128 TB (8 TB HDD x 16)
Řadič pevných disků	RAID (JBOD, 0, 1, 5, 6, 10) SW i HW	RAID (JBOD, 0, 1, 5, 6, 10) SW i HW	ZFS RAIDZ	SW RAID (JBOD, 0, 1, 5, 6, 10) / ZFS RAIDZ
SSD Cache	Ano			Intel SSD DC P3500
Operační systém	Upravený Linux - DSM	Upravený Linux - QTS	FreeNAS	FreeNAS / OpenMediaVault / XPEnology
Souborový systém interních HDD	Ext4, Btrfs	Ext4	ZFS	ZFS, Btrfs, Ext4 aj.
Napájecí zdroj	2x 460W (Záložní / za provozu přepínatelný zdroj)	2x 500W (Záložní / za provozu přepínatelný zdroj)	2x 1280W (Záložní / za provozu přepínatelný zdroj)	2x 920W (Záložní / za provozu přepínatelný zdroj)

CPU	Intel Xeon E3-1230 v2	Intel Core i7-4790S 3,2 GHz	Intel E5-2609v2	E3-1260L v5
RAM	8 GB DDR3 ECC (max. 4x 8 GB)	32 GB DDR3 ECC (max. 4x 8 GB)	32 GB DDR3 ECC (max. 128 GB)	CRUCIAL 32GB (4x8GB) DDR4 2133, ECC (max. 64GB)
LAN	RJ-45 4x 1GbE (s podporou Link Aggregation / Failover)	RJ-45 4x 1GbE (s podporou Link Aggregation / Failover)	4x 1 GbE / upgrade 10GbE (Link Aggregation / Failover)	4x Intel I210AT (Link Aggregation / Failover)
Cena bez disků	110 500 Kč	91 400 Kč	106 300 Kč	76 500 Kč
HDD disky	*55 200 Kč	*55 200 Kč	*55 200 Kč	75 900 Kč
Cena s disky	**165 700 Kč**	**146 600 Kč**	**161 500 Kč**	**152 400 Kč**

* Z důvodu zachování škálovatelnosti pole jsem u těchto sestav vyčíslil cenu pouze pro RAID 6 (7x 6TB (64MB) + Hot-Spare).

Ve srovnávací tabulce jsou zeleně vyznačeny ty komponenty, které jsou v dané kategorii výrazně lepší (rychlejší, robustnější, apod.) než u ostatních sestav.

Souhrn:

Podíváme-li se na první položku tabulky – druh konektivity, která byla při analýze jednou z klíčových vlastností NAS úložiště, všechny sestavy podporují konektor SATA II i III, až na produkt od ixSystems a mnou navržený NAS, které disponují navíc i SAS konektory. Výhodu vidím v možném budoucím využití tohoto konektoru, což by mělo za následek zrychlení datového pole. Druhá položka je jednoznačná, díky vyšší kapacitě lze volit různé typy RAID polí a dosáhnout tak snáze kýženého výsledku. V případě rozhodování mezi RAID a HBA řadičem, je nutné stanovit si prioritu, která je pro nás stěžejní. Zdali zvolit RAID řadič a k tomu Linuxovou distribuci (Synology DSM, QNAP QTS, či OMV), nebo si raději pořídit HBA expandér a jako OS FreeNAS se ZFS. Doporučit konkrétní operační systém není jednoduché, jelikož se jedná o kontinuálně vyvíjený software a z hlediska ovladatelnosti jde o zcela subjektivní věc. Přesto se přikláním k řešení vlastní sestavy kvůli možnosti instalace FreeNAS, OpenMediaVault i XPEnology (derivát Synology DSM). Mezi kapacitami maximálního možného osazení RAM, je pochopitelně jednoznačným vítězem ixSystems s 128 GB, na druhou stranu novější základní deska u nakonfigurované sestavy dokáže profitovat z vyšších taktů pamětí DDR4. Stejně tak nejlepším řešením na poli přenosu dat představuje taktéž ixSystems s možností *upgradu* na 10Gb Ethernet verzi. Konečným důležitým parametrem při rozhodování je i cena, kterou nejníže dosahuje sestava od firmy QNAP. Uvážím-li však, že mnou navrhnutá konfigurace je připravena pro RAID 10 a

je dražší pouze o necelých 6 tis. Kč, silně bych doporučil popřemýšlet o výhodách této varianty.

6 ANALÝZA A VYHODNOCENÍ RIZIK

V této kapitole práce bude provedena analýza aktiv a hrozeb spjatých s prostory možného uložení NAS úložiště. Budou uváženy dvě varianty uložení a to v serverovně a laboratoři. Na základě této analýzy budou navržena doporučená opatření v souladu s metodikou uvedenou v ČSN ISO/IEC 27005/2011 a ISO/IEC 27040:2015. [51], [1]

6.1 Identifikace a ohodnocení aktiv

Prvním krokem při analýze rizik (podle normy ISO/IEC 27005:2011) je identifikace a případně ohodnocení aktiv. Z předchozího popisu NAS úložiště viz. kapitola 5 je patrné, o jaké aktiva se bude jednat. Ve vztahu ke zmiňované normě je možné uvažovat o následujících skupinách aktiv: **primární** (obchodní procesy a činnosti, informace) a **podpůrná aktiva** (hardware, software, sítě, pracovníci aj). Pro ohodnocení aktiv jsem použil škálu od 1 do 5, kde nejdůležitější aktiva jsou označena číslem 5. [52], [53]

Jelikož laboratoř nebude disponovat obchodními ani příbuznými procesy jako jsou patentové nebo jinak chráněné technologie, ani procesy nutné, aby splňovala smluvní, právní nebo regulační požadavky viz. kapitola 3, kde jsem provedl analýzu právních aspektů bezpečnosti informačních systémů. Zbývá pouze kategorie primárních aktiva věnující se informacím. Zde bych zařadil veškerá data uložená na NASu, jejichž ztráta nebo omezení znemožní plnit poslání laboratoře.

Mezi podpůrná aktiva (podle normy ISO/IEC 27005, přílohy B) bych zařadil samotné hardwarové komponenty datového úložiště, operační systém NASu, síťové trasy, personál, který má přístup k úložišti a umístění (laboratoř versus serverovna).

Tabulka 19 – Inventarizace aktiv [Zdroj: Vlastní zpracování], [52]

Typ aktiv	Identifikovaná aktiva	Hodnota aktiv
Informace	Databáze NASu	5
	Data zaměstnanců univerzity	5
	Data subjektů třetích stran	5
HW	NAS úložiště i jeho jednotlivé komponenty	4
	Zařízení pro zpracování dat	2
	Nosiče dat	3
SW	Operační systémy (NASu i klientských stanic)	3
	Specifický SW ke zpracování dat	1
Služby	Připojení NASu do intranetu	4
	Připojení klientských stanic	2

	Podpůrné prvky komunikace	4
Pracovníci	Pracovníci provozu/údržby	5
	Uživatelé	3
Lokalita	Umístění NASu	4

Jednotlivá kritická aktiva z výše uvedené tabulky jsem ohodnotil na základě subjektivního posouzení.

- **Primární aktiva**
  - **Informace** (Databáze NASu, data zaměstnanců univerzity, data subjektů třetích stran) jsou dle mého názoru klíčovými položkami. Jelikož se bude jednat převážně o osobní údaje, jejich ztráta případně odcizení/zneužití může způsobit rozsáhlé škody.
- **Podpůrná aktiva**
  - **HW** – NAS úložiště i jeho dílčí komponenty by měly být chráněny před fyzickým poškozením a odcizením diskových jednotek.
  - **SW** – Operační systém NASu i klientských stanic musí být chráněn před malwarem. Specifické aplikace ke zpracování dat jsou sice nezbytnými nástroji pro práci, ale jejich případnou nefunkčnost můžeme vyřešit reinstalací apod.
  - **Služby** – Přenosové trasy mezi NASem a klientskými jsou další položkou, kterou je potřeba chránit z důvodu možného zneužití např. k odposlechům.
  - **Pracovníci** – Všechny osoby s přístupem k úložišti, by měli mít zvláštní přístupová práva, aby nedocházelo k manipulaci s cizími daty.
  - **Lokalita** – Bezpečnost NASu je přímo závislá na jeho umístění.

6.2 Identifikace hrozeb a zranitelností

Dalším krokem je příprava seznamu identifikovaných hrozeb a zranitelností, které jsou přímo svázány s aktivy z Tabulka 19. V následující tabulce jsou uvedeny pravděpodobnosti výskytu hrozeb spolu s příklady zranitelností. Ke stanovení hodnocení pravděpodobnosti hrozeb jsem použil tutéž škálu (1-5), kdy nejpravděpodobnější hrozba má číslo 5. Také jsem využil *katalogu* hrozeb z normy ISO/IEC 27005 přílohy C, případně lze využít také normu ČSN ISO/IEC TR 13335. [52], [53]

Tabulka 20 – Identifikované hrozby s příklady souvisejících zranitelností [Zdroj: Vlastní zpracování]

Identifikovaná hrozba	Pravděpodobnost hrozby	Příklad související zranitelnosti
Selhání zařízení	2	Náchylnost na vlhkost a prach zařízení
Odposlech	1	Zneužití přenosových tras
Chybné fungování	2	Technické selhání jedné z komponent zařízení
Poškození dat	3	V případě neautorizovaného přístupu
Nezákonné zpracování dat	2	Zneužití dat k jiným než akademickým účelům
Zneužití oprávnění	4	Zpronevěření cizích dat
Krádež zařízení	3	Nedostatek PZTS a MZS prostředků k zabezpečení
Krádež médií	4	
Zničení zařízení nebo médií	1	Umístění v místech kde může dojít k převrácení, spadnutí NAS, PC

6.3 Analýza rizik (matice aktiv, hrozeb a zranitelností)

V tomto kroku, jsem využil přístupu analýzy rizik pomocí matice aktiv, hrozeb a zranitelností. V následující Tabulka 21 jsem nejprve vyplnil identifikovaná aktiva spolu s jejich hodnotami a následně identifikované hrozby společně s pravděpodobnostmi. Čísla v závorkách představují hodnotu míry rizika vypočtenou na základě R = T * A * V, kde T je pravděpodobnost hrozby, A – hodnota aktiva a V je zranitelnost daného aktiva. [53]

Tabulka 21 – Matice zranitelností a rizik [Zdroj: Vlastní zpracování]

	Popis hrozby:	Selhání zařízení	Odposlech	Chybné fungování	Poškození dat	Nezákonné zpracování dat	Zneužití oprávnění	Krádež zařízení	Krádež médií	Zničení zařízení nebo médií
	Pravděpodobnost hrozby (T)	**2**	**1**	**2**	**3**	**2**	**4**	**3**	**4**	**1**
Popis aktiva:	**Hodnota aktiva (A)**									
Databáze NASu	**5**			2 (20)	2 (20)					
Data zaměstnanců univerzity	**5**		3 (15)			4 (40)				
Data subjektů třetích stran	**5**		3 (15)			4 (40)				
NAS úložiště i jeho jednotlivé komponenty	**4**	3 (24)		2 (16)	1 (12)			3 (36)		4 (16)
Zařízení pro zpracování dat	**2**	3 (12)		3 (12)	2 (12)		3 (24)	1 (6)		1 (2)
Nosiče dat	**3**	3 (18)			3 (27)	5 (30)	5 (60)		5 (60)	5 (15)
Operační systémy (NASu i klientských stanic)	**3**				2 (18)					
Specifický SW ke zpracování dat	**1**			2 (4)						
Připojení NASu do intranetu	**4**	3 (24)	4 (16)	3 (24)						
Připojení klientských stanic	**2**	2 (8)	4 (16)	2 (8)						
Podpůrné prvky komunikace	**4**	4 (32)	4 (16)	5 (40)				5 (60)		3 (12)
Pracovníci provozu/údržby	**5**				5 (75)	4 (40)	5 (120)			
Uživatelé	**3**					3 (18)	3 (36)			

6.4 Vyhodnocení rizik

V souvislosti s procesem realizace analýzy rizik jsem následně stanovil hranice pro jednotlivé úrovně rizik. Vyjádření hodnot rizik vypadají v mém případě následovně: nízká (přijatelná) rizika mají hodnotu 1-15, střední 16-40 a vysoká 41 a víc. [53], [60]

Jak je z tabulky patrné, nejpočetnějším hrozbám čelí aktiva v podobě NAS úložiště, zařízením pro zpracování dat a nosičů dat. V prvním případě se jedná hlavně o nízká rizika a pouze v jednom případě (krádež zařízení) o střední riziko. Druhým nejrizikovějším aktivem je zařízení pro zpracování dat (nejčastěji v podobě PC stanic), u kterého se navíc počítá s možným zneužitím oprávnění, což by mohlo vést k odcizení či kompromitaci cizích dat. A posledním velice rizikovým aktivem jsou přenositelné nosiče dat. Opět u nich platí to co v předchozím dvou případech, ale přibývá ještě hrozba nezákonného zpracování dat, ke kterému by mohlo dojít v případě odcizení média.

Tato analýza bohužel nepřipouští souvztažnost jednotlivých položek, přesto zde uvedu možné reciproční vztahy nejrizikovějších případů:

- NAS úložiště a jeho jednotlivé komponenty – u tohoto aktiva je nevyšším rizikem krádež zařízení, ať už jako celku, nebo pouze jednotlivých disků. Tomuto případu lze jednoduše zamezit umístěním úložiště do serverovny namísto laboratoře. A stejným opatřením bychom se vyhnuli také možnému zničení zařízení, které může vyplývat z manipulace z důvodu úklidu v laboratoři apod.
  Bohužel však nejsme schopni minimalizovat zničení (nekonzistenci) souborového systému, což by mělo za následek taktéž selhání zařízení a ztrátu dat. Přestože je v tomto případě hodnota míry rizika pouze 24, takováto ztráta by mohla mít obrovské dopady na celý chod laboratoře. Zde jako jediné východisko vidím zavedení pravidelných záloh všech kritických dat.
- Zařízení pro zpracování dat – tato aktiva mají nejvyšší vypočtené riziko u zneužití oprávnění, z čehož plyne fakt, že je velice důležité mít správně nastavenou restrikci práv (viz. kapitola 4.8.2 Management přístupu). Vyhrazením práv jednotlivým uživatelům, ale nezamezí možné odposlouchávání komunikace na přenosových trasách (viz. podpůrné prvky komunikace), což jsou další chráněná aktiva. Z toho důvodu bych taktéž doporučil používat šifrovanou komunikaci, ať už skrze SFTP nebo Kerberos. Další plynoucí hrozby už spadaly pouze do kategorie nízkého rizika, a tak se jimi nebudu dále zabývat.
- Nosiče dat – mají nejvyšší rizikovost v případech jejich odcizení a zneužití oprávnění. Tady je zřejmá provázanost s daty z klientských stanic (PC), kdy bych doporučil šifrovat, jak pevné disky počítačů, tak i přenosných médií.

7 IMPLEMENTACE DATOVÉHO ÚLOŽIŠTĚ

Skloubím-li shrnutí z předešlých dvou kapitol praktické části, vyplývají z nich následující fakta:

- Nejvhodnější sestavu datového úložiště představuje architektura NAS, u které bych na základě finančního nacenění a použitých technologií vybral právě vlastní konfiguraci *na míru* s operačním systémem FreeNAS. Všechny důvody jsem již shrnul pod Tabulka 18. S tím také souvisí samotné umístění NASu, jelikož se jedná o rackové šasi, nabízí se jediná možnost a to umístění do serverovny. Díky tomu, můžeme minimalizovat řadu rizik shrnutých pomocí matice rizik viz. Tabulka 21 a také profitovat z ideálních podmínek prostředí díky klimatických zařízení a dále také možnosti napojení záložního zdroje UPS nebo agregátu, což zabezpečení běh systému i v případě výpadku energie. Datové úložiště bude takto daleko více chráněno prostředky PZTS a MZS a stejně tak k němu bude mít fyzický přístup pouze hrstka lidí oprávněných ke vstupu do serverovny.
- Abychom se při implementaci vyhnuli dalším hrozbám, jako je odposlech a krádež dat z přenosných médií, doporučuje norma ISO/IEC 27040:2015 šifrovat spojení mezi zařízeními s minimální délkou klíče 128 bitů. Toho můžeme v našem případě pro přenos dosáhnout implementací protokolu Kerberos, který poskytuje délku klíče až AES-256. U zabezpečení disků jednotlivých zařízení, jsme limitování pouze volbou nástrojů k šifrování, kterých je však nespočet a u datového úložiště lze využít šifrování FreeNASu. [60], [2]
- V případě restrikce práv, disponuje FreeNAS vlastními nástroji pro nastavení oprávnění jednotlivých uživatelů, případně skupin k přístupu do konkrétních složek nebo médií.

Přestože vlastní konfigurace NAS úložiště pozbývá podpory a servisu ze strany výrobců, jako tomu je u QNAP, Synology aj., jedná se spíš o ideální volbu pro uživatele, kteří hledají spolehlivé a ekonomicky úspornější řešení pro ukládání dat. Stejně tak si uživatelé musejí vystačit převážně s vlastní správou, i když se v případě komplikací je možné obrátit na celosvětově rozsáhlou komunitu uživatelů.

8 REALIZACE DATOVÉHO ÚLOŽIŠTĚ A TESTOVÁNÍ

V této kapitole jsem dle navržených variant NASu, provedl testování a srovnání rychlostí čtení a zápisu RAIDZ2 versus RAID10 za využití dvou nástrojů. Výkon testovací sestavy pochopitelně neodpovídá výkonu navržené konfigurace viz. předešlá kapitola 5.3, z důvodů odlišného hardwaru. Přesto na základě výsledku srovnání se můžeme dále rozhodnout, zda investovat finanční prostředky na nákup dalších disků, nebo se raději spokojit s limity RAIDZ2, které je pochopitelně méně náročné na diskovou kapacitu.

8.1 Testovací zařízení

Testovací sestava má následující konfiguraci:

Tabulka 22 – Parametry testovacího NASu

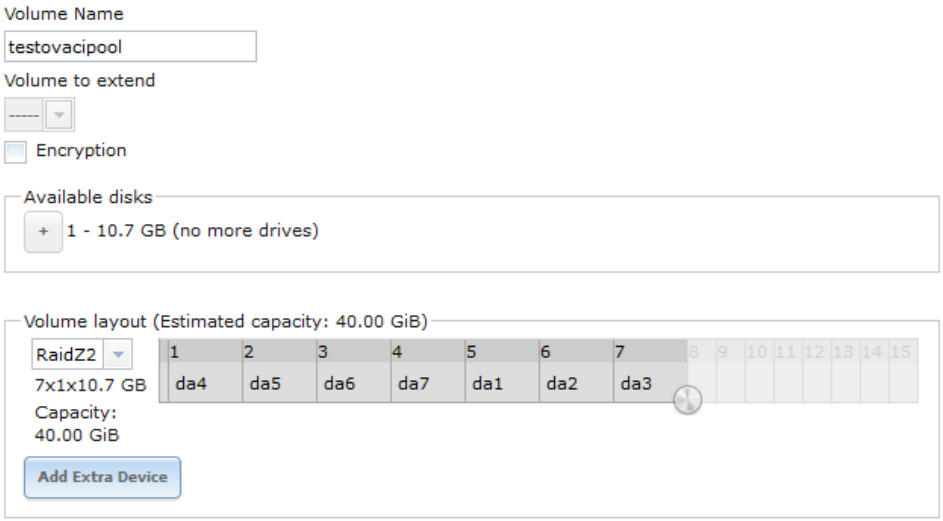
OS	FreeNAS-9.10-STABLE-201605021851 (35c85f7)
Platforma	Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz
RAM	8163MB
2x SSD	2x Crucial Balistix M200 240GB SPAN/JBOD

Na tomto hardwaru byl nejprve nainstalován hypervizor – Vmware ESXi 6.0, na kterém bylo následně vyčleněno testovacímu FreeNASu 2 jádra, 8 GB RAM a 7 virtuálních disků s kapacitami 10,7 GB.

8.1.1 RaidZ2

Postup testování:

1) V prvním případě jsem ze všech 7 disků pomocí správce disků vytvořil RaidZ2 s názvem *testovacipool*, který má po zformátování na ZFS alokovaných 36 GB.

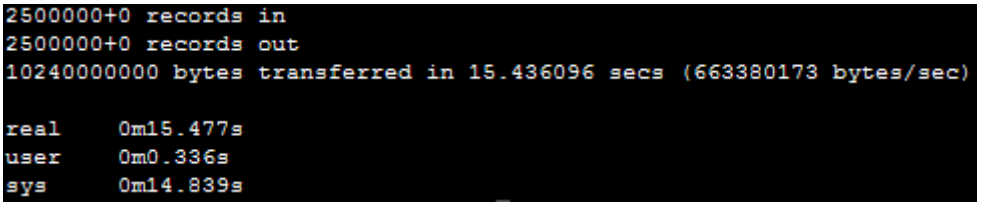


Obrázek 14 – Vytváření RAIDZ2 (7 x 1 x 10,7GB)

2) Následně jsem pomocí unixového konzolového nástroje dd provedl test zápisu 9,765 GB dat na vytvořený RaidZ2.

Použitý příkaz: *time sh -c "dd if=/dev/zero of=/mnt/testovacipool/tmp bs=4k count=2500000 && sync"*

Z parametrů příkazu lze vyčíst, že byly data zapisovány po 4 KiB, což dnes odpovídá taktéž alokovaným blokům na většině pevných disků. Další hodnota 2500000 odpovídá celkovému počtu takto zapsaných bloků dat. [56], [57]



Obrázek 15 – Výsledek testu zápisu dat na RAIDZ2

Jak je z obrázku patrné, celý průběh zápisu trval pouze 15,43 vteřin, což odpovídá průměrné rychlosti: 663380173 / (1024*1024) = **632,65 MB/s**.

3) K otestování rychlosti čtení byla nejdříve paměť RAM přepsána náhodnými daty a následně byl použit příkaz: *time sh -c "dd if=/mnt/testovacipool/tmp of=/dev/null bs=4k"* [56], [57]

```
2500000+0 records in
2500000+0 records out
10240000000 bytes transferred in 30.423773 secs (336578900 bytes/sec)

real    0m30.426s
user    0m0.252s
sys     0m30.138s
```

Obrázek 16 – Výsledek čtení dat na RAIDZ2

Z výstupu můžeme opět vyčíst, že celková doba čtení byla 30,42 vteřin a z toho vychází průměrná rychlost čtení 336578900 / (1024 *1024) = **320,99 MB/s**.

4) Druhým nástrojem k testování čtení a zápisu byl použit IOzone. Jak je z následujícího příkazu patrné, tento nástroj nabízí daleko širší možnosti nastavení, než tomu bylo u dd. A díky použitým parametrům jsem byl schopen dosáhnout detailnějších výsledků. [58]

Volaný příkaz: *iozone -M -e -+u -T -t 32 -r 128k -s 40960 -i 0 -i 1 -i 2 -i 8 -+p 70 -C*

```
Children see throughput for 32 random writers   = 2016071.75 KB/sec
Parent sees throughput for 32 random writers    =  455440.60 KB/sec
Min throughput per thread                       =    5814.66 KB/sec
Max throughput per thread                       =  525412.31 KB/sec
Avg throughput per thread                       =   63002.24 KB/sec
Min xfer                                        =    1536.00 KB
CPU utilization: Wall time    0.961    CPU time    7.988    CPU utilization 831.15 %
```

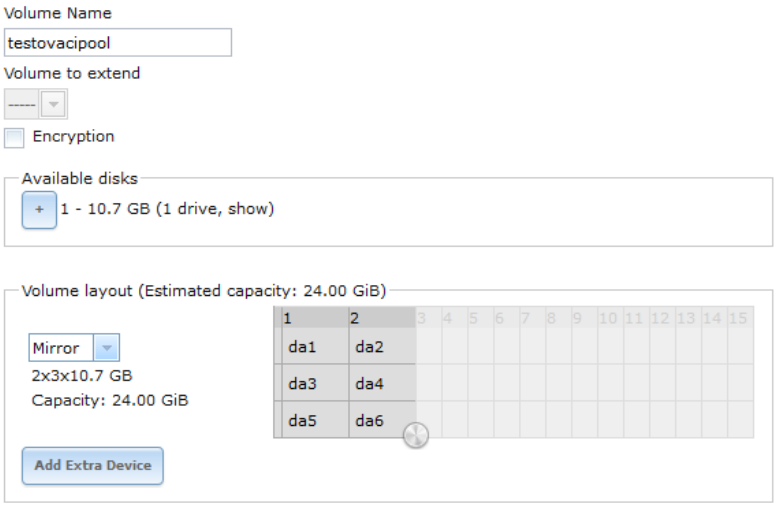
Obrázek 17 – Výsledek testu iozone na RAIDZ2

Pořízený snímek výsledku programu IOzone ukazuje jak maximální rychlost propustnosti dat na vlákno (513 MB/s), tak i minimální (5,68 MB/s) a průměrnou rychlost zápisu (61,52 MB/s).

8.1.2 Raid 10

Postup testování:

1) V prvním kroku jsem ze 6 disků pomocí správce disků vytvořil Raid 10 s názvem *testovacipool*, který má po zformátování na ZFS alokovaných 24 GB.



Obrázek 18 – Vytváření RAID 10 (2 x 3 x 10,7GB)

2) Následně jsem pomocí unixového konzolového nástroje dd provedl test zápisu 9,765 GB dat na vytvořený RaidZ2. [56], [57]

Použitý příkaz: *time sh -c "dd if=/dev/zero of=/mnt/testovacipool/tmp bs=4k count=2500000 && sync"*

Použitý příkaz je úplně totožný s předchozím, který byl použit u RaidZ2.

```
2500000+0 records in
2500000+0 records out
10240000000 bytes transferred in 15.302091 secs (669189595 bytes/sec)

real    0m15.314s
user    0m0.320s
sys     0m14.733s
```

Obrázek 19 – Výsledek testu zápisu dat na RAID 10

Celý průběh zápisu trval pouze 15,30 vteřin, což odpovídá průměrné rychlosti: 669189595 / (1024*1024) = **638,19 MB/s**.

3) K otestování rychlosti čtení byla opět přemazána paměť a následně použit stejný příkaz: *time sh -c "dd if=/mnt/testovacipool/tmp of=/dev/null bs=4k"*, [56], [57]

```
2500000+0 records in
2500000+0 records out
10240000000 bytes transferred in 30.269910 secs (338289742 bytes/sec)

real    0m30.272s
user    0m0.362s
sys     0m29.894s
```

Obrázek 20 – Výsledek čtení dat na RAID 10

Z výstupu lze opět vyčíst, že celková doba čtení byla 30,27 vteřin a z toho vychází průměrná rychlost čtení 338289742 / (1024 *1024) = **322,61 MB/s**.

4) I v případě testování s IOzone na Raidu 10 byl opět použit totožný příkaz.

Volaný příkaz: *iozone -M -e -+u -T -t 32 -r 128k -s 40960 -i 0 -i 1 -i 2 -i 8 -+p 70 -C*

```
Children see throughput for 32 random writers   = 2256343.14 KB/sec
Parent sees throughput for 32 random writers    =  188170.34 KB/sec
Min throughput per thread                       =   20760.25 KB/sec
Max throughput per thread                       = 1109905.25 KB/sec
Avg throughput per thread                       =   70510.72 KB/sec
Min xfer                                        =    1408.00 KB
CPU utilization: Wall time    0.629    CPU time    7.013    CPU utilization 1115.81 %
```

Obrázek 21 – Výsledek testu iozone na RAID 10

Výsledku z programu IOzone jsou následující: maximální rychlost propustnosti dat na vlákno (1083,89 MB/s), tak i minimální (20,27 MB/s) a průměrnou rychlost zápisu (68,86 MB/s).

8.1.3 Porovnání RAIDZ2 s RAID 10

Následující tabulka shrnuje výsledky předchozího testování zápisu a čtení dat:

Tabulka 23 – Srovnání výsledků RAIDZ2 a RAID 10

	RAIDZ2	RAID 10
dd - zápis	632,65 MB/s	638,19 MB/s
dd - čtení	320,99 MB/s	322,61 MB/s
Iozone - max.	513 MB/s	**1083,89 MB/s**
Iozone - min.	5,68 MB/s	20,27 MB/s
Iozone - průměr	61,52 MB/s	68,86 MB/s

Tabulka s výsledky jasně dokazuje, že RAID 10 je po všech stránkách výkonnější než RAIDZ2 (příp. RAID 6). Také je RAID 10 schopen dosahovat až teoretické dvojnásobné propustnosti oproti RAIDZ2 (viz. položka Iozone – max.). Co se týče výsledků nástroje dd, zde je dvojnásobná rychlost zápisu oproti čtení způsobena paralelní zápisem na 2 disky zároveň, avšak čtení se provádí pouze z jednoho SSD disku.

ZÁVĚR

Cílem této diplomové práce bylo navrhnout jednak strukturu datového úložiště, ale také zabezpečit, aby veškeré navrhnuté konfigurace byly v souladu s normami a odpovídajícími právními aspekty.

Tato práce je rozdělena na dvě základní oblasti. První, teoretická část se zabývala právními aspekty, jenž se týkají uchování a zpracování citlivých dat v rámci výkonu činnosti pracovníků forenzní laboratoře. Bylo zohledněno několik právních regulativů a následně také normy, *best-practice*, které blíže specifikují a popisují jak nejlépe zabezpečit datová úložiště. Dále se teoretické část věnovala jednotlivým druhům datových úložišť se zaměřením na jejich technologie a výhody i nevýhody jejich použití. Dalším významným bodem bylo uvážení možnosti využití rozdílných souborových systémů, na které taktéž navazuje použití konkrétního operačního systému a volba nejvhodnějšího typu pole RAID pro zabezpečení rychlosti a bezpečnosti úložiště. Poslední podkapitola teoretické části se věnovala neméně důležitému tématu zabezpečení v několika oblastech – datového pole, přenosových tras a řízení přístupu.

První kapitola praktické části je tvořena porovnáním vhodných firemních produktů pro potřeby forenzní laboratoře. Druhá, velice rozsáhlá kapitola popisuje výběr dílčích nejvhodnějších komponent s přihlédnutím na cenu a poskytnuté funkce. Takto byly navrženy dvě varianty datových úložišť podle vhodnosti umístění – do laboratoře a serverovny. Následně byla vypočtena jejich cenová kalkulace a spotřeba elektrické energie. Dalším bodem bylo srovnání těchto variant s vybranými produkty světových výrobců z první kapitoly praktické části.

Poté byla vypracována kapitola shrnující analýzu a vyhodnocení rizik uložení dvou výše popsaných variant do laboratoře a serverovny. Tato kapitola jednak shrnuje identifikaci aktiv, největších hrozeb, zranitelnosti a stanovuje hodnoty rizik podle příslušné normy. Dále následovalo zhodnocení nejrizikovějších scénářů a uvážení možných protiopatření.

Třetí největší kapitola praktické části se věnovala nejvhodnější implementaci datového úložiště na základě vyhodnocení výsledků předchozích dvou kapitol.

Poslední část diplomové práce byla věnována testování navrženého datového pole z pohledu operačního a souborového systému. Přestože testování proběhlo na jiném než navrženém

hardwaru, výsledky jasně ukazují, které typ RAID pole by byl vhodnější pro budoucí realizaci. Do budoucna by bylo záhodno srovnat výsledky testů pořízeného NAS úložiště s uváděnými výsledky jednotlivých komerčních produktů.

SEZNAM POUŽITÉ LITERATURY

[1] *Data Security Management*. 2010, **2010/1**. ISSN 1211-8737.

[2] Digitální důkazy. *ČIMIB - Český Institut Manažerů Informační Bezpečnosti* [online]. [cit. 2016-05-15]. Dostupné z: http://www.cimib.cz/novinka/22-digitalni-dukazy

[3] ČSN EN ISO/IEC 17025:2005. *Posuzování shody - Všeobecné požadavky na způsobilost zkušebních a kalibračních laboratoří*. 2. Švýcarsku, 2005.

[4] *The Internet Organised Crime Threat Assessment (IOCTA)*. Hague, 2015. ISSN 2363-1627.

[5] *High-Tech Crimes | Europol* [online]. [cit. 2016-05-15]. Dostupné z: https://www.europol.europa.eu/ec3/high-tech-crimes

[6] *Europol: Commercial Sexual Exploitation of Children Online* [online]. 2015 [cit. 2016-05-15]. Dostupné z: https://www.europol.europa.eu/content/commercial-sexual-exploitation-children-online

[7] *Europol: Situation Report - Payment Card Fraud in the European Union* [online]. 2013 [cit. 2016-05-15]. Dostupné z: https://www.europol.europa.eu/content/situation-report-payment-card-fraud-european-union

[8] *Aktuálně.cz: Sledování dětské pornografie bude trestné, rozhodla Sněmovna* [online]. 2014 [cit. 2016-05-15]. Dostupné z: http://zpravy.aktualne.cz/domaci/zapojeni-deti-do-pornografie-je-trestne-rozhodla-snemovna/r~2e05d0d6db4611e398cc0025900fea04/

[9] *Inhope.org: Stats infographics for 2014* [online]. In: . 2014 [cit. 2016-05-15]. Dostupné z: http://www.inhope.org/Libraries/Statistics_Infographics_2014/INHOPE_stats_infographics_for_2014.sflb.ashx

[10] ŠMÍD, Vladimír. *Právní aspekty bezpečnosti informačních systémů* [online]. In: . [cit. 2016-05-15]. Dostupné z: http://www.fi.muni.cz/~smid/bezpecnostIS.html

[11] *Perspektivy jakosti: Systém řízení informační bezpečnosti podle normy ISO 27001*. 2008, 2/2007.

[12] KRÁL, David. *Informační bezpečnost podniku*. Brno, 2010. Disertační práce. Vysoké učení technické v Brně. Vedoucí práce Doc. Ing. MILOŠ KOCH, CSc.

[13] RADVANSKÝ, Martin. *Zavedení managementu informační bezpečnosti v malém podniku*. Brno, 2011. Diplomová práce. Vysoké učení technické v Brně. Vedoucí práce Ing. Petr Sedlák.

[14] *Bestpractice.cz: Odborné informace o ITIL® best practice přístupu k řízení IT služeb.* [online]. [cit. 2016-05-15]. Dostupné z: https://www.bestpractice.cz/cs/Best-practice/-ITSM-ITIL-.alej

[15] *ITIL service design*. 2nd ed. London: TSO, 2011. Best Management Practice. ISBN 978-0-11-331305-1.

[16] *CleverAndSmart: CIA: Důvěrnost-Integrita-Dostupnost* [online]. [cit. 2016-05-15]. Dostupné z: http://www.cleverandsmart.cz/duvernost-integrita-dostupnost/

[17] *QAP Advice & Audit: CobiT domains and processes (COBIT 5 / 4.1)* [online]. [cit. 2016-05-15]. Dostupné z: http://www.qualified-audit-partners.be/index.php?cont=463

[18] *Systemonline.cz: COBIT 5 v malých a středních firmách* [online]. 2013 [cit. 2016-05-15]. Dostupné z: http://www.systemonline.cz/sprava-it/cobit-5-v-malych-a-strednich-firmach.htm

[19] ANDRESON, Nathan. *Cobit INFOSEC* [online]. In: . [cit. 2016-05-15]. Dostupné z: http://www.isaca.org/chapters10/Lusaka/NewsandAnnouncements/Documents/Cobit-INFOSEC.pdf

[20] *Isaca.org: DS12.5 - Physical Facilities Management* [online]. [cit. 2016-05-15]. Dostupné z: http://www.isaca.org/Groups/Professional-English/ds12-5-physical-facilities-management/Pages/Overview.aspx

[21] NOVÁK, Luděk a Josef POŽÁR. *Systém řízení informační bezpečnosti* [online]. , 10 [cit. 2016-05-15]. Dostupné z: http://www.cybersecurity.cz/data/srib.pdf

[22] MIKULECKÝ, Jan a Marek SKALICKÝ. *ISMS v malých a středních firmách* [online]. 2003, , 18 [cit. 2016-05-15]. Dostupné z: https://www.rac.cz/rac/homepage.nsf/CZ/Download/$FILE/ISMS%20pro%20SME%20051129.pdf

[23] KUFNER, V. Quo Vadis ITIL? – část VIII. DSM 1/2008, s.36-40. ISSN 1211-8737.

[24] SOMASUNDARAM, G. a Alok. SHRIVASTAVA. *Information storage and management: storing, managing, and protecting digital information in classic, virtualized, and cloud environments*. 2nd ed. Indianapolis, IN: John Wiley & Sons, c2012. ISBN 9781118223475.

[25] *Direct Attached Storage and Introduction to SCSI* [online]. In: . s. 20 [cit. 2016-05-15]. Dostupné z: http://www.cuchd.in/e-library/resource_library/University%20Institute%20of%20Computing/ITT521-Storage%20Management/Chapter%205.ppt

[26] *Svět hardware: NAS: Práce s daty a sdílení pro pokročilé - Konfigurujeme oprávnění* [online]. 2013 [cit. 2016-05-15]. Dostupné z: http://www.svethardware.cz/nas-prace-s-daty-a-sdileni-pro-pokrocile/37490-4

[27] TATE, Jon, Pall BECK, Hector HUGO IBARRA, Shanmuganathan KUMARAVEL a Libor MIKLAS. *Introduction to Storage Area Networks* [online]. 7th. 2016 [cit. 2016-05-15]. ISBN 0738441430. Dostupné z: http://www.redbooks.ibm.com/redbooks/pdfs/sg245470.pdf

[28] VERLOY, Filip. *File- and Block Storage over a WAN* [online]. In: . 2012 [cit. 2016-05-15]. Dostupné z: https://filipv.net/2012/08/02/file-and-block-storage-over-a-wan/

[29] A Complete Guide to FreeNAS Hardware Design, Part I: Purpose and Best Practices. *FreeNAS.org* [online]. 2015 [cit. 2016-05-15]. Dostupné z: http://www.freenas.org/blog/a-complete-guide-to-freenas-hardware-design-part-i-purpose-and-best-practices/

[30] DOČEKAL, Michal. Správa linuxového serveru: RAID teoreticky. In: *Linuxexpres.cz* [online]. 2009 [cit. 2016-05-15]. Dostupné z: http://www.linuxexpres.cz/praxe/sprava-linuxoveho-serveru-raid-teoreticky

[31] ZFS: You should use mirror vdevs, not RAIDZ. In: *Http://jrs-s.net* [online]. 2015 [cit. 2016-05-15]. Dostupné z: http://jrs-s.net/2015/02/06/zfs-you-should-use-mirror-vdevs-not-raidz/

[32] CORBET, Jonathan. Ext4 encryption. In: *Lwn.net* [online]. 2015 [cit. 2016-05-15]. Dostupné z: https://lwn.net/Articles/639427/

[33] Mathur, Avantika; Cao, MingMing; Bhattacharya, Suparna; Dilger, Andreas; Tomas, Alex; Vivier, Laurent (2007). *"The new ext4 filesystem: current status and future plans" (PDF).* Proceedings of the Linux Symposium. Ottawa, ON, CA: Red Hat. *Retrieved* 2008-01-15.

[34] Btrfs Wiki. *Btrfs.wiki.kernel.org* [online]. 2016 [cit. 2016-05-15]. Dostupné z: https://btrfs.wiki.kernel.org/index.php/Main_Page

[35] Moderní souborové systémy. *Systemonline.cz* [online]. 2014 [cit. 2016-05-15]. Dostupné z: http://www.systemonline.cz/sprava-it/moderni-souborove-systemy.htm

[36] *Aaron Toponce: ZFS Administration, Part I- VDEVs* [online]. 2012 [cit. 2016-05-15]. Dostupné z: https://pthree.org/2012/12/04/zfs-administration-part-i-vdevs/

[37] NEUMANN, Martin. *Měření a analýza výkonu systému souborů ZettaByte*. Praha, 2012. Bakalářská práce. České vysoké učení technické v Praze. Vedoucí práce Muzikář Zdeněk Ing., CSc.

[38] BRADEN, Gregg. *Brendan's blog: ZFS L2ARC* [online]. In: . 2008 [cit. 2016-05-15]. Dostupné z: http://dtrace.org/blogs/brendan/2008/07/22/zfs-l2arc/

[39] *ZFS Primer: FreeNAS User Guide 9.3 Table of Contents* [online]. [cit. 2016-05-15]. Dostupné z: https://doc.freenas.org/9.3/zfsprimer.html

[40] *OpenSolaris ZFS Deduplication: Everything You Need to Know* [online]. In: . 2010 [cit. 2016-05-15]. Dostupné z: http://constantin.glez.de/blog/2010/03/opensolaris-zfs-deduplication-everything-you-need-know

[41] Groklaw - Sun's Proposed CDDL License - Feedback Requested. In: *Groklaw.net* [online]. 2004 [cit. 2016-05-15]. Dostupné z: http://www.groklaw.net/articlebasic.php?story=20041205023636236

[42] FreeNAS User Guide 9.3 Table of Contents: Encryption. *Doc.freenas.org* [online]. [cit. 2016-05-15]. Dostupné z: https://doc.freenas.org/9.3/freenas_storage.html#encryption

[43] FreeNAS User Guide 9.3 Table of Contents: Directory Service. *Doc.freenas.org* [online]. [cit. 2016-05-15]. Dostupné z: https://doc.freenas.org/9.3/freenas_directoryservice.html

[44] FreeNAS vs OpenMediaVault - FreeNAS: Open Source Storage Operating System. *Freenas.org* [online]. [cit. 2016-05-15]. Dostupné z: http://www.freenas.org/freenas-vs-openmediavault/

[45] *Compare Projects - Open Hub: FreeNAS - OpenMediaVault - xpenology* [online]. [cit. 2016-05-15]. Dostupné z: https://www.openhub.net/p/_compare?project_0=FreeNAS&project_1=OpenMediaVault&project_2=xpenology

[46] A Complete Guide to FreeNAS Hardware Design, Part II: Hardware Specifics - FreeNAS - Open Source Storage Operating System. *Freenas.org* [online]. 2015

[cit. 2016-05-15]. Dostupné z: http://www.freenas.org/blog/a-complete-guide-to-freenas-hardware-design-part-ii-hardware-specifics/

[47] A Complete Guide to FreeNAS Hardware Design, Part III: Pools, Performance, and Cache. *Freenas.org* [online]. 2015 [cit. 2016-05-15]. Dostupné z: http://www.freenas.org/blog/a-complete-guide-to-freenas-hardware-design-part-iii-pools-performance-and-cache/

[48] Corsair Obsidian Series 900D, černá CC-9011022-WW. *CZC.cz* [online]. 2013 [cit. 2016-05-15]. Dostupné z: https://www.czc.cz/corsair-obsidian-series-900d-cerna/129236/produkt?gclid=CP7Z_pHdxcwCFUefGwod1TkHZA

[49] Supermicro: Products | Chassis | 3U | SC836BA-R920B. *Supermicro.com* [online]. [cit. 2016-05-15]. Dostupné z: http://www.supermicro.com/products/chassis/3U/836/SC836BA-R920.cfm

[50] RAID Tip 5 of 10 - Hot Spares. *Raidtips.com* [online]. [cit. 2016-05-15]. Dostupné z: http://www.raidtips.com/hot-spares.aspx

[51] Metodika zajištění ochrany kritické infrastruktury v oblasti výroby, přenosu a distribuce elektrické energie. *Hzscr.cz* [online]. 2012 [cit. 2016-05-15]. Dostupné z: http://www.hzscr.cz/soubor/metodika-zajis-te-ni-ochrany-kriticke-infrastruktury-v-oblasti-vy-roby-pr-enosu-a-distribuce-elektricke-energie-pdf.aspx

[52] *ČSN ISO/IEC 27005:2011: Informační technologie - Bezpečnostní techniky - Řízení rizik bezpečnosti informací*. 2013.

[53] STEINER, František. Případová studie analýzy rizik informační bezpečnosti. In: *BPM* [online]. [cit. 2016-05-15]. Dostupné z: http://bpm-tema.blogspot.cz/2007/11/ppadov-studie-analzy-rizik-informan.html

[54] ČERMÁK, Miroslav. Analýza rizik: Jemný úvod do analýzy rizik. In: *CleverAndSmart* [online]. 2013 [cit. 2016-05-15]. Dostupné z: http://bpm-tema.blogspot.cz/2007/11/ppadov-studie-analzy-rizik-informan.html

[55] *ISO/IEC 27040:2015: Information technology — Security techniques — Storage security*. 2015.

[56] Dd(1) - Linux manual page. *Man7.org* [online]. 2016 [cit. 2016-05-15]. Dostupné z: http://man7.org/linux/man-pages/man1/dd.1.html

[57] Benchmark disk IO with DD and Bonnie++. In: *JamesCoyle.net* [online]. 2013 [cit. 2016-05-15]. Dostupné z: https://www.jamescoyle.net/how-to/599-benchmark-disk-io-with-dd-and-bonnie

[58] FreeNAS User Guide 9.3 Table of Contents: Command Line Utilities - IOzone. *Doc.freenas.org* [online]. [cit. 2016-05-15]. Dostupné z: https://doc.freenas.org/9.3/freenas_cli.html#iozone

[59] WILSON, P. Backup on TS-421 - QNAP NAS Community Forum. In: *Http://forum.qnap.com* [online]. 2013 [cit. 2016-05-15]. Dostupné z: http://forum.qnap.com/viewtopic.php?t=83090#p369334

[60] Proceedings of the 14th European Conference on Cyber Warfare and Security. United Kingdon: Academic Conferences and Publishing International Limited, 2015. ISBN 978-1-910810-28-6. ISSN 2048-8602.

[61] Storage Security: Encryption and Key Management. In: The Storage Networking Industry Association: Advancing Storage and Information Technology [online]. Colorado Springs, 2015 [cit. 2016-05-15]. Dostupné z: http://www.snia.org/sites/default/files/technical_work/SecurityTWG/SNIA-Encryption-KM-TechWhitepaper.R1.pdf.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Spam	Nevyžádaná pošta
MLAT	Mutual Legal Assistance Treaty (Smlouva o vzájemné právní pomoci)
EC3	European Cybercrime Center
INHOPE	International Association of Internet Hotlines
URL	Uniform Resource Locator (Jednotná adresa zdroje)
SEPA	Single Euro Payments Area
DFA	Digitální forenzní analýza
NBÚ	Národní bezpečnostní úřad
ITIL	IT Infrastructure Library
ISM	Information Security Management
ITSM	IT service management (Řízení služeb informačních technologií)
ISMS	Information Security Management System (Systém řízení bezpečnosti inf.)
IS	Informační systém
IT Governance	Řízení informačních technologií
DAS	Direct Attached Storage
SAN	Storage Area Network
NAS	Network Attached Storage
SCSI	Small Computer System Interface
FC	Fibre Channel
iSCSI	Internet Small Computer Systems Interface
FCIP	Fibre Channel over IP
iFCP	Fibre Channel Protocol
LAN	Local Area Network
WAN	Wide Area Network

NFS	Network File System
SMB	Server Message Block
CIFS	Common Internet File System
FTP	File Transfer Protocol
TLS	Transport Layer Security
SSL	Secure Sockets Layer
HA	High Availability
VM	Volume Manager
UID	User identifier
GID	Group identifier
FS	File systems
RAID	Redundant Array of Inexpensive Disks
OMV	OpenMediaVault

SEZNAM OBRÁZKŮ

SEZNAM TABULEK