Bezpečnost informačních technologií v oblasti zabezpečení dat a internetové komunikace

Safety of information technology in data security and Internet communications

Bc. Dagmar Zábojníková

Diplomová práce
2012

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2011/2012

ZADÁNÍ DIPLOMOVÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Bc. Dagmar ZÁBOJNÍKOVÁ**
Osobní číslo:	**A10335**
Studijní program:	**N 3902 Inženýrská informatika**
Studijní obor:	**Počítačové a komunikační systémy**
Téma práce:	**Bezpečnost informačních technologií v oblasti zabezpečení dat a internetové komunikace**

Zásady pro vypracování:

1. **Vypracujte literární rešerši na dané téma.**
2. **Analyzujte současný stav bezpečnosti informačních technologií v oblasti zabezpečení dat a internetové komunikace.**
3. **Vytvořte analýzu struktury LAN a používaných operačních systémů na počítačích a serverech.**
4. **Vytvořte též analýzu uložení dat a zabezpečení vzdálených a lokálních komunikací.**
5. **Proveďte shrnutí slabých míst a návrh řešení pro jejich odstranění či částečnou eliminaci.**

Rozsah diplomové práce:

Rozsah příloh:

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

Seznam odborné literatury:

1. **THOMAS, Robert M. Lokální počítačové sítě. Praha: Computer Press, 1996. ISBN 80-85896-45-1.**
2. **STUCHLÝ, Vladimír. Počítače a komunikace. Praha 4: Computer Press, 1998. ISBN 80-85896-40-0.**
3. **DONAHUE, Raechel. Kompletní průvodce síťového experta. Computer Press, 2009. 528 s. ISBN 9788025122471.**
4. **SOSINSKI, Barrie. Mistrovství - Počítačové sítě. Computer Press, 2010. ISBN 9788025133637.**
5. **DOSTÁLEK, L., VOHNOUTOVÁ, M., KNOTEK, M. Velký průvodce infrastrukturou PKI a technologií elektronického podpisu. Computer Press, 2009. ISBN 978-80-251-2619-6.**
6. **ČANDÍK, Marek. Základy informační bezpečnosti. vyd. Zlín : Univerzita Tomáše Bati, 2004. 107 s. ISBN 8073182181.**
7. **BITTO, O. Šifrování a biometrika. BEN, 2005. 168 s. ISBN 80-86686-48-5.**
8. **KLÍMA, Vlastimil; ROSA, Tomáš. Kryptologie pro praxi - DSA, ECDSA. Dostupné z WWW: [http://crypto-world.info/klima/2004/st_2004_04_21_21.pdf].**

Vedoucí diplomové práce: **Ing. Roman Šenkeřík, Ph.D.**
Ústav informatiky a umělé inteligence

Datum zadání diplomové práce: **24. února 2012**

Termín odevzdání diplomové práce: **28. května 2012**

Ve Zlíně dne 24. února 2012

L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

prof. Ing. Karel Vlček, CSc.
ředitel ústavu

ABSTRAKT

Cílem diplomové práce je analýza současného stavu bezpečnosti informačních technologií v oblasti zabezpečení dat a internetové komunikace. V teoretické části je zpracovány základní témata jako informační bezpečnost, bezpečnostní politika, struktura LAN sítí, operační systémy, zálohování dat nebo vzdálený přístup. Praktická část se pak opírá o poznatky z teoretické části. Je zde zpracována analýza LAN sítí, použitých operačních systémů, druhů databází a zabezpečení vzdálených a lokálních komunikací. Na závěr jsou shrnuty slabé místa a jsou zde uvedeny návrhy na zlepšení.

Klíčová slova: bezpečnostní politika, LAN, operační systémy, uložení dat, virtualizace, zabezpečení

ABSTRACT

The aim of the diploma thesis is staging current state for system security of information technology in data security and internet communications. In the theoretical part there is developed literary search on the topic. There are concepts explained like safety, security policy, structure of LAN networks, operating systems, data backup or remote access. The practical part is based on knowledge of the theoretical part. There is also prepared analysis of LAN networks, used operating systems, database and security of remote and local communications in my piece of work. At the end there are summarized weak points and suggestions for improvement.

Keywords: security policy, LAN, operating systems, data storage, virtualization, security

Chci poděkovat panu Petru Mahdalovi, správci sítě firmy Česká Zbrojovka, a.s. za velkou snahu při vysvětlování daných témat, za odbornou konzultaci a za celkový čas strávený nad mou diplomovou práci. Dále chci poděkovat panu Ing. Romanu Šenkeříkovi, Ph.D za vedení mé práce v rámci UTB. Zároveň mé poděkování patří mé mamince, sestře, babičce a celé rodině Záchvějových a samozřejmě mému příteli a blízkým kamarádům. Děkuji všem za podporu, kterou jste mi dali, protože bez vás by tahle diplomová práce nebyla sepsána a dokončena.

T.G.Masaryk:

„Člověk mnoho vydrží, má-li cíl.“

Prohlašuji, že

- beru na vědomí, že odevzdáním diplomové/bakalářské 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/bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk diplomové/bakalářské 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/bakalářskou 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/bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování diplomové/bakalářské 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/bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem diplomové/bakalářské 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 pracovala samostatně a použitou literaturu jsem citovala. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze diplomové práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….

podpis diplomanta

OBSAH

ÚVOD

V současné době se pohubujeme ve společnosti, která využívá moderní informační technologie v každodenním životě. A stále víc je ohrožena zneužitím těchto technologií. Proto je požadavek na bezpečnost v dnešní době velmi důležitý. Tento požadavek se nesmí podceňovat, protože podcenění těchto požadavků vede v mnoha případech k fatálním následkům.

Cílem diplomové práce je celková analýza jak stavu bezpečnosti informačních technologií v oblasti zabezpečení dat a internetové komunikace, tak struktury LAN a používaných operačních systémech. Cílem je i vytvoření analýzy uložení dat a zabezpečení vzdálených lokálních komunikací a následné shrnutí slabých míst a návrhy na řešení pro jejich zlepšení. Celá analýza je provedena ve firmě Česká Zbrojovka, a.s. a diplomová práce může posloužit jako materiál pro případné zlepšení určitých segmentů ve firmě.

Diplomová práce je rozdělena na část teoretickou a praktickou. V teoretické části je zpracována literární rešerše na dané téma. Hlavní část je bezpečnostní politika, struktura LAN, databázové systémy, virtualizace atd. Témata této diplomové práce v teoretické části jsou sepsána z obecného úhlu pohledu a podrobně rozepsána až v praktické části. Praktická část se zabývá do hloubky bezpečností, strukturou LAN, operačními systémy, uložením dat a vzdáleným a lokálním přístupem ve firmě.

Zdůrazňuji, že vzhledem ke zveřejnění mé diplomové práce nemohou být uvedeny některé skutečnosti a fakta firmy Česká Zbrojovka, a.s.

I. TEORETICKÁ ČÁST

1 BEZPEČNOST INFORMAČNÍCH TECHNOLOGIÍ

Cílem teoretické části diplomové práce je teoretické seznámení s bezpečností informačních technologií v oblasti zabezpečení dat a internetové komunikace. Teoretická část bude sestavena tak, aby se jednoduše dal pochopit význam bezpečnost informačních technologií, a slouží taky jako základ pro pochopení praktické části diplomové práce.

1.1 Význam bezpečnosti informačních technologií v současné době

Společnost, která využívá moderní informační technologie v každodenním životě je stále víc ohrožena zneužitím těchto technologií. Oproti tomu informační technologie nabízí velkou ochranu pro společnost před různými typy hrozeb. V dnešní době je požadavek na bezpečnost stejně důležitý, jako je cena, funkčnost nebo spolehlivost. Zahrnuje široké spektrum oblastí od kryptografie až po biometriku. Ve světě, ale i v České republice je stále větší zájem o bezpečnostní výzkum a bezpečnostní inženýrství.

1.2 Základní pojmy

1.2.1 Informace

Informaci jsme schopni vnímat jako nějakou zprávu, data nebo sdělení. V minulosti byla informace chápána jako těžko uchopitelný abstraktní pojem, který byl vymezen velmi složitým popisem.

V dnešní době je informace rozdělena na 4 základní významy:

- **Sémantický –** jedná se o absolutní zisk poznání (informace) jak např. odpovídá významu jednotlivých slov.
- **Pragmatický –** příjemce rozlišuje, zda již sdělovanou informaci má či ne - sdělení toho co už vím, není podle tohoto pojetí ziskem informace.
- **Idealizovaný –** zisk informace záleží na jeho zhodnocení příjemcem a to na základě jeho předchozích zkušeností, minulých i momentálních citů a emocí, logika přitom hraje zanedbatelnou.
- **Inženýrský –** zde se pomocí pravděpodobnosti, resp. informační entropie, definuje velikost informace tak, jak ji stanovil C. Shannon v roce 1948.

1.2.2 Informační bezpečnost

Obecně bezpečnost je chápána jako ochrana něčeho před ztrátou, odcizením, poškozením nebo zničením. Informační bezpečnost si podle toho můžeme vyjádřit jako ochranu informace před těmito událostmi. V odborné literatuře ovšem často nacházíme pojmy narušení integrity, dostupnosti a důvěryhodnosti. Tyto pojmy jsou definovány následovně:

- **Integrita** – je definována jako zajištění správnosti a úplnosti informací. Musíme si uvědomit, že pokud dojde k závažným změnám dat jak úmyslně, tak i neúmyslně nemusí být tato změna detekována, popřípadě může být objevena až za delší dobu. Čím později se na chybu dojde, tím závažnější bude jeho dopad.
- **Dostupnost** – představuje požadavek zabezpečení dostupnosti informací v okamžiku jejich potřeby. Proto musí být zabezpečen vhodný řídící mechanismus pro zajištění kvality a spolehlivosti takových služeb [1].
- **Důvěrnost** – důvěrné informace a procesy musí být zpřístupněné nebo sdělitelné pouze oprávněným osobám. O nežádoucím zpřístupnění informací tedy hovoříme jako o narušení jejich důvěrnosti.

Obr. 1. Životní cyklus základních atributů bezpečnosti [14]

Z uvedených vlastností je zřejmé, že jsou tyto vlastnosti základní stavební kameny v otázce bezpečnosti informačních technologií.

V otázce informační bezpečnosti nesmíme opomenout na další pojmy, které jsou velmi důležité pro pochopení problematiky.

Základní pojmy v oblasti informační bezpečnosti jsou:

- **Riziko** – představuje možnost určité ztráty nebo škody.
- **Zranitelnost** – můžeme chápat jako slabé místo, které vede ke škodám nebo zničení daného systému.
- **Ohrožení systému** – lze chápat jako potencionální hrozbu, před poškozením nebo zničením.
- **Napadení –** představuje činnost, která vede ke způsobení ztráty nebo zničení.
- **Kontrola –** je činnost, která minimalizuje ohrožení systému.

Ohrožení systému definujeme jako:

- **Přerušení** – představuje nepoužitelnost, nedostupnost nebo ztrátu některé systémové časti.
- **Sledování** – nepovolená osoba získá přístup do systémové části.
- **Modifikace** – je případ, kdy nepovolená osoba má přístup nejen k systémové části, ale může s ní i manipulovat.
- **Falzifikace** – představuje možnost neoprávněné osoby zavést do systému falešná data nebo realizovat falešné operace.

V souvislosti s autorizovanými přístupy je významným parametrem autentizace. Autentizace je ověření identity uživatele, že je opravdu tím, za koho se vydává. Metody používané pro zabezpečení autentizace uživatele můžeme rozdělit do následujících skupin [1]:

- **Autentizace heslem** – zahrnuje pravidelnou změnu hesla, kombinace velkých a malých písmen s číslicemi, popřípadě jinými znaky, zamezení opakovaného použití hesla.
- **Autentizace pomocí občanského průkazu, identifikační karty, čipové karty atd.**
- **Biometrická autentizace** – zde jsou zahrnuty otisky prstů, charakter hlasu, dynamika podpisu atd. Velmi velké výhody biometrické autentizace jsou v rychlosti, praktičnosti, jednoznačnosti a neoklamatelnosti.
- **Autentizace pomocí certifikátů –** zde se používají šifrovací algoritmy.
- **Fyzické přístupy** – zámek, ostraha.

1.2.3 Komunikační bezpečnost

V současné době, v době veřejných sítí jsou informace velmi cenným majetkem pro každého z nás. Proto je velice důležité nespoléhat na to, že naše informace dojdou k cíli bez povšimnutí, ale myslet na to, jakým způsobem přenášené informace ochránit. Ochrana informace spočívá v šifrování.

Moderní šifrování dělíme na symetrické a asymetrické. Symetrické šifry mají pouze jeden klíč a každý, kdo ho vlastní může zprávu zašifrovat a i dešifrovat. Tenhle druh šifer se používá například pro ochranu dat na disku, přenos dat přes webové prohlížeče atd. Avšak asymetrické šifrování používá dva klíče. Soukromý klíč a veřejný klíč. Potom mohou nastat dva způsoby šifrování. První způsob spočívá v tom, že zpráva je zašifrovaná soukromým a dešifrována veřejným klíčem. Tímto způsobem se realizují digitální podpisy. A druhý způsob je, že zpráva je zašifrována veřejným a dešifrována soukromým klíčem. Tento způsob se používá pro bezpečnost zprávy. Obě techniky lze spojit.

Komunikační a tedy i počítačovou bezpečnost lze shrnout jako kvalitní ochranu informačních systémů a dat zpracovávaných na počítačích technickými a programovými prostředky jako jsou autentizace a autorizace, řízení přístupu, účtovatelnost, audit, bezpečné uložení a přenos dat a antivirová ochrana [8].

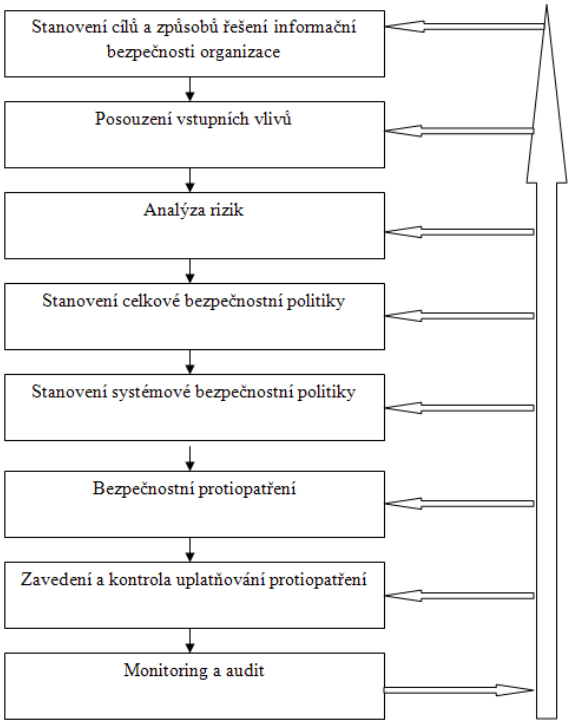
1.3 Bezpečnostní politika

Bezpečnostní politika je základní stavební pilíř, na kterém stojí celý systém informační bezpečnosti. Zahrnuje technické, fyzické, administrativní, personální, etické, právní, ekologické a sankční opatření, které se vztahuje na přístup a použití dat v informačních systémech. Bezpečnostní politiku můžeme charakterizovat tedy jako princip zajištění důvěrnosti, neporušitelnosti a dostupnosti informačních systémů. Je to tedy dokument, jehož cílem je ochrana majetku, pověsti a činnosti organizace. Po schválení, které učiní vedení organizace je tento dokument závazný pro všechny zaměstnance a je směrodatný i pro všechny externí subjekty. Zároveň je veřejně přístupný a klade se důraz na to, aby byl stručný, srozumitelný, přehledný, úplný a řešil všechny možné otázky v rámci bezpečnosti. Východiskem tedy mohou být uznávané světové standardy a metodiky.

Bezpečnostní politiku lze rozdělit do dvou časových pásem:

- **Celková bezpečnostní politika** – stanovuje celkový popis cílů a zabezpečení organizace. Je to nadčasový dokument, který je vypracován na dobu 5 až 10 let.
- **Systémová bezpečnostní politika** – zde se popisují konkrétní bezpečnostní cíle, ohrožení a opatření. Zahrnuje tedy požadavky na ochranu a nakládání s citlivými informacemi, které jsou v souladu s platnými zákony.

Z hlediska vývoje pak můžeme bezpečnostní politiku rozdělit do fází:



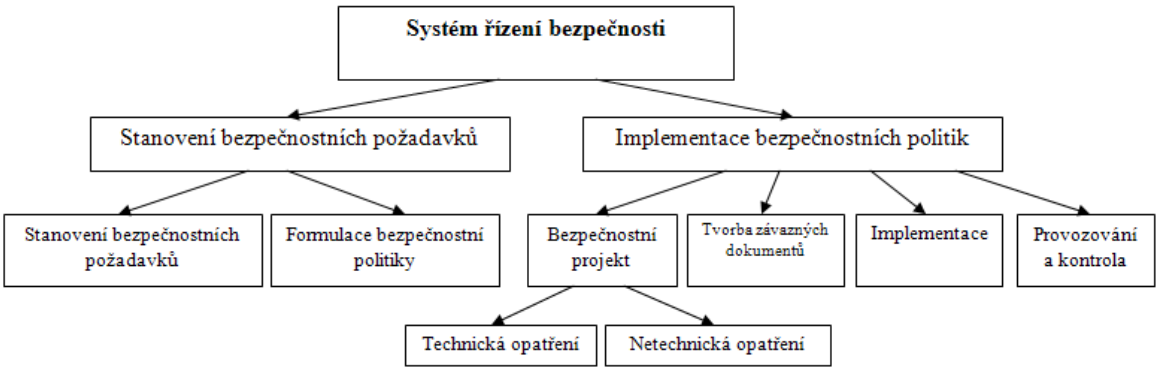
Obr. 2. Fáze vývoje informační bezpečnostní politiky [1]

Bezpečnostní politika by měla obsahovat i tzv. soubor požadavků. Tento soubor by měl zahrnovat stanovení předmětu bezpečnosti, vypracování směrnice náhrady kapacity, definování pokynů pro pravidelné hodnocení a audit bezpečnosti, vypracování a zvládnutí analýzy rizik, personální, počítačovou a komunikační bezpečnost. Taktéž pravidelnou aktualizaci havarijního plánu a její koncepci, tvorbu archivačních a záložních prostředků, prevenci, detekci a eliminaci účinků počítačových virů a kryptografické zabezpečení. A v neposlední řade klasifikaci bezpečnosti informačního systému a programových prostředků, fyzickou, provozní, právní a etickou bezpečnost, vyšetřování a hodnocení bezpečnostní politiky.

1.3.1 Úloha politiky informační bezpečnosti

Úloha politiky spočívá v definování určitých východisek v přesném pořadí. Spočívá to v ustanovení:

- **Cílů** – určují, čeho má být dosaženo
- **Strategií** – ukazují, jak se má dosáhnout cílů
- **Politiky** – značí výčet pravidel



Obr. 3. Systém řízení bezpečnosti [1]

Systém řízení bezpečnosti se potom skládá z:

- **Stanovení bezpečnostních požadavků** – je počátečním krokem tvorby systému řízení bezpečnosti. Zde se stanovují cíle, které vycházejí z obchodních cílů organizace, legislativy, smluv a interních požadavků.
- **Formulace bezpečnostní politiky** – k obchodním cílům, legislativě a smlouvám je nutné připojit bezpečnostní rizika. Pokud je všechno zpracováno, tak jak má být, lze to označit za základ bezpečnostní politiky požadované úrovně.

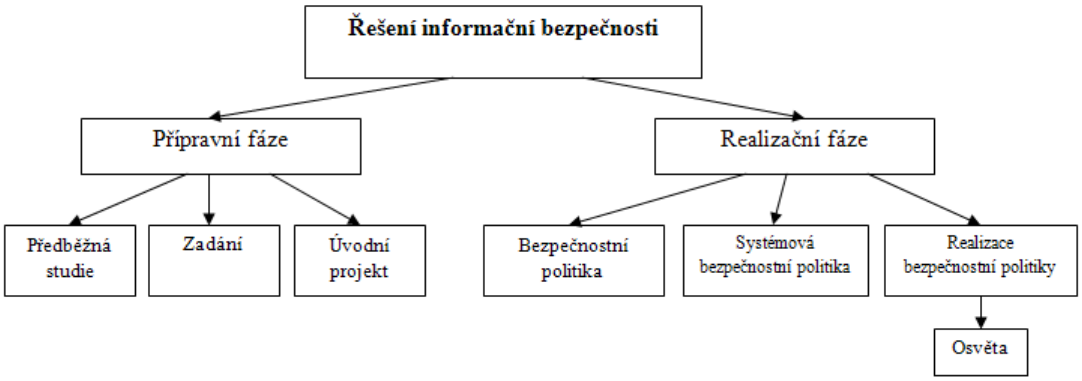
Potom implementace bezpečnostních politik obsahuje:

- **Bezpečnostní projekt** – je to návod, který přechází od požadavků k jejich řešení. Zahrnuje jak technická opatření, kde se musí najít jednotlivé komponenty a k nim navázat jednotlivá požadovaná bezpečnostní opatření, tak netechnická opatření, kde se implementuje pomocí směrnic.
- **Tvorbu závazných dokumentů** – cílem je poskytnout návod na řešení havarijních situací v organizaci. Rozděluje se na obnovu funkčnosti IT systémů organizace a na manuál zvládání bezpečnostních incidentů.

- **Implementaci** – definuje jak vypracovaný bezpečnostní projekt zavést do fungování organizace.
- **Provozování a kontroly** – bezpečnostní systém je předán do provozu, jsou procházeny jednotlivé oblasti, případné odchylky jsou dokumentovány a odstraněny.

Bezpečnostní politika a její úloha je tedy základním prvkem jistoty managementu, že aktiva organizace jsou dostatečně zabezpečena proti poškození nebo zničení.

1.3.2 Řešení informační bezpečnosti



Obr. 4. Postup řešení bezpečnosti informačních systémů [1]

Řešení informační bezpečnosti se skládá z následujících bloků:

a) Přípravní fáze:
   - **Předběžná studie** – účelem je získat základní údaje o bezpečnostní situaci v organizaci. Slouží tedy zejména k vypracování zadání pro uzavření smlouvy o realizaci bezpečnosti v informačním systému mezi zadavatelem a řešitelem.
   - **Zadání –** zadavatel formuluje svoje požadavky na bezpečnost, řešitel je koriguje s přihlédnutím k tomu, co je nutné, co je možné, co je rozumné, na co by se nemělo zapomenout, co vyžaduje zákon apod.
   - **Úvodní projekt bezpečnosti –** cílem je shrnout získané poznatky a stanovení návrhu strategie zabezpečení.

b) Realizační fáze:
   - **Bezpečnostní politika** – zde vznikne stručný a velmi důležitý dokument, z něhož budou vycházet veškeré další práce.
   - **Systémová bezpečnostní politika** – definuje, jakým způsobem se bude celková bezpečnostní politika promítat do konkrétních podmínek zadavatele. Obsahuje požadavky na bezpečnost osobních počítačů, správu dat, provoz, řízení přístupu, bezpečnostní politiku počítačové sítě, bezpečnost a správu sítí pro přenos dat, bezpečnost a správu lokálních sítí, právní a etické otázky a vzory dokumentů.
   - **Realizace bezpečnostní politiky** – zde se provádí konkrétní opatření jako je instalace softwarových a hardwarových ochran, vypracování konkrétních dokumentů atd.
   - **Osvěta** – každý pracovník organizace musí být seznámen s bezpečnostním opatřením.

1.4 Bezpečnost informačních systémů

Rozsáhlá distribuce výpočetní techniky do podniků zapříčinila i diskusi o bezpečnosti informačních systémů. Základem jsou výpočetní systémy. Jsou zde zpracována a uchována data. Zahrnuje tedy hardware, software a vlastní data, která jsou celkově označována jako **aktiva informačního systému.** Pro úplnost nesmíme opomenout v oblasti bezpečnosti informačních systémů **personál.**

Z pohledu zabezpečení systémů rozlišujeme:

- **Objekt informačního systému** – jedná se o pasivní jednotky (entity), které obsahují nebo přijímají informace.
- **Subjekt informačního systému** – představuje aktivní jednotku, tedy osobu, proces nebo zařízení.

Ochrana dat je pak rozdělena jako:

- **Počítačová bezpečnost** – ochrana dat uchovaných v počítači [1].
- **Komunikační bezpečnost** – ochrana dat při jejich přenosu [1].
- **Personální bezpečn**ost – ochrana před vnitřními útočníky [1].
- **Fyzická bezpečnost –** ochrana před přírodními hrozbami a neoprávněným přístupem.

Využití zranitelnosti tj. chyb v programu nebo jeho konfiguraci, která umožní útočníkovi získat neoprávněný přístup k datům [10], se nazývá **hrozba.** S hrozbou se můžeme setkat v podobě přírodní katastrofy, zde se velmi těžce určuje prevence, soustředí se spíš na minimální dopad na systém, např. duální uložení dat. Také mohou vznikat technické výpadky, jakou jsou výpadky elektrického napětí nebo poruchy informačního systému (hardwaru i softwaru) i zde je prevence obtížná a řešení se soustředí na minimální dopad na systém. Následně jsou hrozby neúmyslné, kde se bere v úvahu neúmyslný zásah do systému uživatelem. A nakonec jsou zde hrozby úmyslné, kde je vědomý zásah do systému uživatelem, který má za cíl narušit bezpečnost systému.

1.5 Útoky na informační systémy

Existují tři hlavní typy počítačových virů. První typ viru **napadá spustitelné soubory** a zvětšuje jim velikost, což usnadňuje napadené soubory ihned identifikovat. Druhým typem jsou viry, které **napadají zaváděcí program operačního systému.** Způsobují ochromení operačního systému napadeného počítače. Třetí typ viru **napadá uživatelské programy,** které po spuštění provedou úkony, které nebyly naplánovány.

Útočníky definujeme na **útočníky slabé síly,** jsou to amatérští nebo náhodní útočníci. Poté následují **útočníci střední síly**, jsou to převážně studenti střední a vysokých škol a posledním stupněm je **útočník veliké síly**, jedná se o profesionální útočníky z řad počítačových expertů. Není výjimkou ani interní útok od zaměstnanců firmy nebo od návštěv ve firmě.

Obranným prostředkem proti útokům je tzv. **protiopatření** [1]. Rozdělují se na preventivní, které odstraňují zranitelná místa, pak na heuristická, která snižují riziko ohrožení a následně na detekční a opravné, které minimalizují účinek útoku.

2 LOKÁLNÍ POČÍTAČOVÁ SÍŤ

Síť LAN je síť, která je omezena na určité místo, například budovu či podlaží. Používá technologie krátkého rozsahu, například Ethernet, Wi-Fi, Token Ring apod. Síť LAN je obvykle pod kontrolou podniku nebo entity, která ji potřebuje používat [3].

2.1 Základní pojmy

2.1.1 Počítačová síť

Topologie Počítačovou sítí rozumíme označení pro souhrnné technické prostředky, které realizují výměnu informaci a spojení mezi počítači. Dovolují tedy jejich uživatelům vzájemnou komunikaci podle určitých pravidel, typicky výměnu zpráv nebo společné využívání služeb [11]. První pokusy byly známy již od 60. let 20. Století, ve stejné době se začaly vyvíjet i komunikační protokoly. Nejpoužívanějším protokolem je TCP/IP, které je základním stavebním prvkem počítačové sítě v současné době.

2.1.2 Topologie

V lokálních počítačových sítích jsou důležité následující topologie:

- **Sběrnice** – byla používána v prvních dobách Ethernetu a realizovala se pomocí koaxiálního kabelu a BNC konektorů, na konci musel být vždy terminátor. Všechna zařízení jsou zapojena na společnou sběrnici. V sítích se od této technologie ustoupilo a dnes se používá převážně zapojení do hvězdy [13].
- **Hvězda** – je dnes nejpoužívanější topologie. Je zde centrální prvek, který realizuje propojení zařízení, a do něj jsou připojena jednotlivá zařízení. Jako centrální prvek slouží hub nebo switch, ale může se jednat i o router. V dnešní době se užívá i zapojení *rozšířená topologie hvězda*, vznikne zapojením několika samostatných hvězd, které propojíme dohromady přes centrální prvky.
- **Kruh** – v této topologii je každý uzel připojen ke dvěma sousedním a dohromady tvoří kruh. Standardně existuje pouze jedna cesta mezi dvěma uzly.
- **Mřížka –** zde jsou uzly propojeny s více sousedy. Buď se může jednat o plnou mřížku, kdy je každý uzel spojený se všemi ostatními nebo o částečnou mřížku, kdy některé uzly jsou přímo spojeny s více jinými uzly.

2.1.3 Síťové protokoly

Model ISO/OSI je referenční komunikační model a jedná se o doporučený model definovaný organizací ISO v roce 1983, který rozděluje vzájemnou komunikaci mezi počítači do sedmi souvisejících vrstev. V Internetu se používá protokol TCP/IP.

- **ISO/OSI**

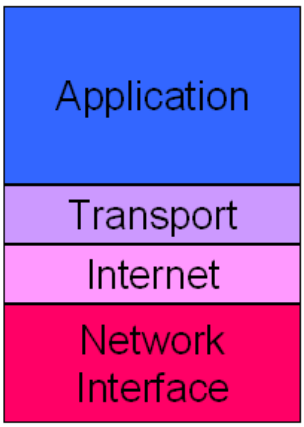
  Úkolem každé vrstvy je poskytovat služby následující vyšší vrstvě a nezatěžovat vyšší vrstvu detaily o tom jak je služba ve skutečnosti realizována. Než se data přesunou z jedné vrstvy do druhé, rozdělí se do paketů. V každé vrstvě se pak k paketu přidávají další doplňkové informace (formátování, adresa), které jsou nezbytné pro úspěšný přenos po síti [15].

Obr. 5. Model ISO/OSI [15]

- **Fyzická vrstva** – popisuje elektrické, mechanické a funkční požadavky na zpracování síťových dat.
- **Linková vrstva** – popisuje procesy, které detekují a opravují chyby během datového přenosu mezi vrstvou fyzickou a vrstvami, které jsou výše.
- **Síťová vrstva** – Definuje protokoly pro směrování dat, jejichž prostřednictvím je zajištěn přenos informací do požadovaného cílového uzlu. V lokální síti vůbec nemusí být, pokud se nepoužívá směrování.
- **Transportní vrstva –** definuje protokoly pro strukturované zprávy a zabezpečuje bezchybnost přenosu. Jsou to protokoly TCP a UDP.
- **Relační vrstva** – dohlíží na komunikaci a udržuje relaci tak dlouho, dokud je potřeba dále zajišťuje zabezpečovací, přihlašovací a správní funkce.
- **Prezenční vrstva** – řídí formátování datových přenosů. Řeší například háčky a čárky, kompresi a dekompresi, šifrování dat.
- **Aplikační vrstva –** specifikuje prostředí, ve kterém síťové aplikace komunikují se síťovými službami.

- **TCP/IP**

  obsahuje sadu protokolů pro komunikaci v počítačové síti a je hlavním protokolem celosvětové sítě Internet. Síťová komunikace je rozdělena do vrstev znázorňující hierarchii činností. Každá vrstva využívá služeb vrstvy nižší a poskytuje své služby vrstvě vyšší. Stejné vrstvy dvou různých systémů komunikují mezi sebou pomocí komunikačních protokolů za pomoci spojení, které vytvoří sousední nižší vrstva.



Obr. 6. Model TCP/IP [16]

- **Vrstva síťového rozhraní** – má na starosti vše, co je spojeno s ovládáním konkrétní přenosové cesty resp. sítě, a s přímým vysíláním a příjmem datových paketů [17].
- **Vrstva síťová** – je realizována pomocí protokolu IP a stará se o to, aby se jednotlivé pakety dostaly od odesílatele ke svému příjemci, přes směrovače.
- **Transportní vrstva** – je nejčastěji realizována protokolem TCP a zajišťuje přenos mezi dvěma koncovými účastníky, kterými jsou aplikační programy.
- **Aplikační vrstva** – zde aplikační programy komunikují přímo s transportní vrstvou.

2.1.4 Aktivní prvky LAN

Pod pojem aktivní síťové prvky se v dnešní době zařazují všechna zařízení, která slouží potřebám vzájemného propojování v počítačových sítích (zejména pak těch lokálních), a přitom nejsou jen pasivními mechanickými záležitostmi (jakými jsou například kabely, konektory apod.) [18].

Opakovače

Opakovač dokáže pracovat pouze s přenosovými protokoly fyzické vrstvy. Lze si ho představit jako jednoduchý digitální zesilovač, který si všímá jednotlivých bitů, ale neřeší, co znamenají. Přijímá tedy utlumený a zkreslený signál, který dál zesílí a správně vytvaruje, a znovu vyšle do všech ostatních kabelových segmentů. Opakovače propojují pouze takové segmenty, které mají stejnou přenosovou rychlost, proto se používají k prodloužení spojení ke vzdálenému hostiteli.

Rozbočovače

S příchodem Ethernetu se rozbočovače staly novými páteřemi ve většině instalací. Představuje způsob vzájemného propojení kabelů sítě Ethernetu, tak aby signály těchto kabelů bylo možno zopakovat na všechny ostatní připojené kabely. Lze ho v podstatě nazvat opakovačem s tím rozdílem, že opakuje signál přes více kabelů a ne jen přes jeden.

Přepínač

Přepínače pracují na linkové vrstvě. Od rozbočovačů se liší tím, že sledují, která zařízení se nachází na kterých portech a předává rámce pouze zařízením, pro která jsou určena. Je důležité, aby sítě s přepínačem nebyly příliš veliké z důvodu například všesměrového vysílání (broadcastingu) nebo přístupového omezení.

Směrovač

Směrovače mezi sebou obvykle vzájemně komunikují pomocí jednoho nebo více směrovacích protokolů. Tyto protokoly umožňují směrovačům zjistit informace o sítích jiných než těch, které jsou k nim připojeny [2]. Směrovače fungují na úrovni vrstvy síťové.

2.2 Virtuální lokální sítě

Virtuální lokální sítě, nebo jen sítě VLAN, jsou virtuální části přepínače tvořící různé logické sítě, které se chovají tak, jako by byly nakonfigurovány na samostatném fyzickém přepínači [2]. Umožňuje, aby jeden přepínač obsluhoval více lokálních sítí.

2.2.1 Popis virtuální lokální sítě

VLAN umožní správcům snadnou segmentaci sítě do logických subsítí, které jsou nezávislé na fyzické vrstvě, virtuální sítě mohou zjednodušit úlohy managementu, jako jsou např. přesun či přidání pracovní stanice a vytváření logických pracovních skupin.

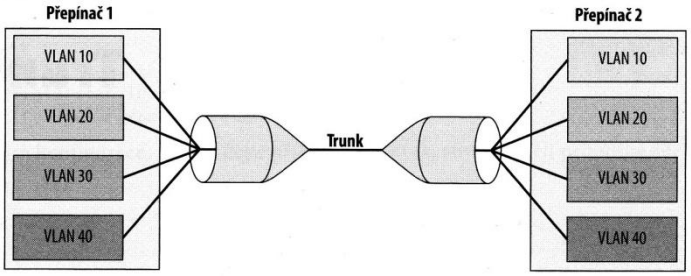
Virtuální LAN je logický segment LAN, který spojuje koncové uzly, které mohou být připojené k různým fyzickým segmentům a mohou spolu komunikovat jako by byly na společné LAN [19].

VLAN je rozdělena na čtyři typy podle:

- **Portů** – historicky první typ virtuálních sítí definuje členství v síti pro jednotlivé porty přepínače (skupiny portů). První implementace neumožňovaly rozšíření virtuální sítě přes více přepínačů. Následné generace, již byly schopné toto rozšíření poskytnout.
- **MAC adres uzlů** – lze virtuální síť s takovým rozdělením chápat jako VLAN podle uživatelů, protože jakmile se uživatel přemístí na jiný segment, jeho členství se v VLAN nezmění.
- **Síťového protokolu nebo síťových adres uzlů** – jsou založeny na informacích ze síťové vrstvy. Uzly jsou v multiprotokolových sítích přiřazeny do jednotlivých VLAN podle provozovaných síťových protokolů nebo podle adresy podsítě.
- **Skupinového IP vysílání** – paket je zde poslán na speciální adresu, která funguje jako proxy pro speciálně definovanou skupinu uzlů. Paket je tedy doručen všem členům dané skupiny. Je velmi dynamická metoda, protože se vytváří jen na určitou dobu.

2.2.2 Trunk

V terminologii Cisco je trunk rozhraním nebo spojením, které může přenášet rámce pro více sítí VLAN současně. Trunk může být použit k propojení dvou přepínačů, aby zařízení v sítích VLAN na jednom přepínači mohla komunikovat se zařízením v týchž sítích VLAN na jiném přepínači. Pokud existuje pouze jedna síť VLAN, kterou je třeba propojit, přepínače jsou propojeny na vrstvě dvě pomocí trunku [2].



Obr. 7. Schematické znázornění trunku [2]

2.2.3 VTP

Ve složitých sítích může být správa sítí VLAN časově náročná a náchylná k chybám. Protokol VTP (VLAN Trunking Protocol) je prostředkem pomocí kterého lze na centrálním zařízení spravovat názvy a čísla sítí VLAN, přičemž výsledná konfigurace se může automaticky distribuovat na ostatní zařízení [2].

Tedy provedené změny jsou poté distribuovány na každý přepínač v doméně VTP. Doména VTP je skupina propojených přepínačů se stejně nakonfigurovaným řetězcem domény VTP. Vzájemně propojené přepínače s různě nakonfigurovanými doménami VTP nebudou sdílet informace o síti VLAN. Každý přepínač se může nacházet pouze v jedné doméně VTP [2].

Myšlenka tohoto protokolu je, že změny jsou provedeny na serverech VTP, následně se rozšíří klientům VTP a všem ostatním serverům VTP v dané doméně.

3 ZÁLOHOVÁNÍ A ARCHIVACE DAT

V následující kapitole jsou popsány cíle a způsoby zálohování a archivace dat.

3.1 Zálohování dat

Ztráta dat je velmi nepříjemná, obzvlášť, co se týká firemních dat, jejich ztráta může vést až k likvidaci firmy. Mohou se totiž nenávratně ztratit nejen kontakty na partnery, ale i účetní data. V oblasti bankovnictví, zdravotnictví atd. je taková ztráta nepřípustná. K tomu, aby nedocházelo ke ztrátám dat, je prevence včasného zálohování bezesporu nejlepší.

Příčiny ztráty dat je možné rozdělit do skupin jako například porucha hardwaru, lidský faktor, softwarové selhání, počítačové viry a přírodní katastrofy.

Zálohování zahrnuje následující funkce:

- Záchrana dat po havárii
- Ochrana provozuschopnosti informačního systému
- Záchrana operačního systému a databází
- Rychlost obnovy stavu před havárií

Způsoby zálohování lze definovat jako:

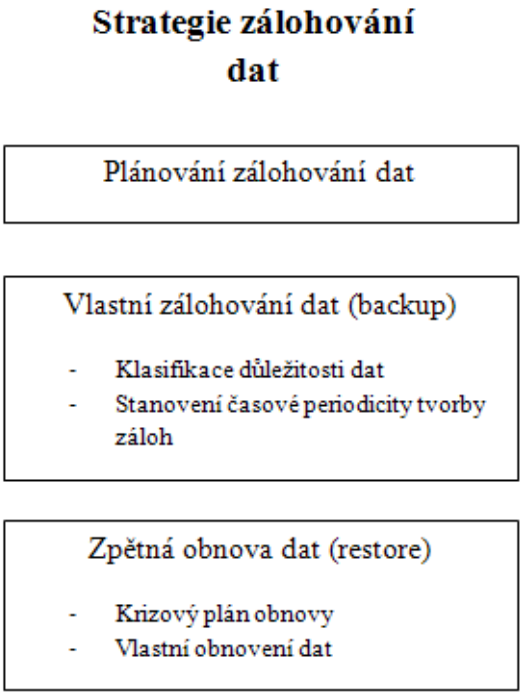
- **Výchozí** – kopie původního systému.
- **Kompletní** – jsou vždy zálohována všechna data najednou.
- **Inkrementální** – u prvního spuštění se provede kompletní záloha, ale při dalších se provádí už jen záloha dat od posledního spuštění.
- **Diferenční –** zálohují se změny od poslední kompletní zálohy.

Podle způsobu vytváření záloh rozlišujeme taky **decentralizované zálohování**, které patří mezi starší způsoby zálohování dat. Funguje na základě nahrávání dat na různá média v nepravidelných intervalech. Takové zálohování vedlo ke ztrátě dat, a taky z pohledu organizace to bylo velmi neefektivní. Problémy dále nastávaly při velkých objemech dat. Oproti tomu **centralizované zálohování** je založeno na využití velkokapacitního zálohování z centra. Je nejefektivněji realizováno páskovými systémy připojenými na obslužný počítač a jeho prostřednictvím na počítačovou síť [1]. Je to velmi spolehlivý a rychlý systém zápisu a obnovení dat. Centralizované zálohování využívá automatickou úschovu dat neboli automatické zálohování.

Strategie zálohování dat:

- **Plánování zálohování** – Plán obnovy je vlastně jakýmsi krizovým plánem, ve kterém bychom měli pamatovat na souslednost jednotlivých úkonů, které je potřeba postupně vykonat, abychom provedli rekonstrukci dat s úspěchem [1].
- **Vlastní zálohování (backup)** – zde je tzv. Backup Management, ten lze chápat jako stanovení strategie ukládání dat, stanovení objemu dat a jaká data budou zálohována.

  Prvním krokem při tvorbě backup je rozdělení zálohovaných dat podle stupně důležitosti na nekritická, nízko-kritická a kritická data. Dalším krokem je stanovení časové periodicity tvorby záloh, tedy časový navigační plán.
- **Zpětné obnova dat (restore)** – důležité je mít data nejen zálohována, ale také musíme být schopni je obnovit. Plán obnovy musí být pravidelně aktualizován a je taky dobré znát umístění médií s poslední zálohou či si zakládat dokumentaci o provedených zálohách. Používá se časová navigace, kde během zálohovacího procesu jsou veškeré informace ukládány do databáze.



Obr. 8. Strategie zálohování dat [1]

Cílem zálohování je rychle obnovit plně funkční stav informačního systému, jaký byl těsně před katastrofou. Zálohování (backup) je možné popsat jako vytvoření bezpečnostní kopie

dat nebo celého operačního systému tak, abychom mohli v případě havárie některé součásti počítače obnovit (restore) stav, který existoval těsně před vznikem poruchy [1].

3.2 Archivace dat

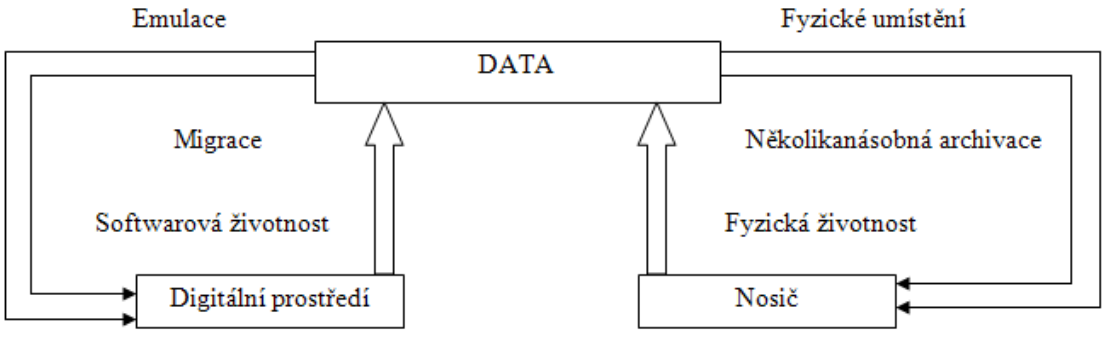
Archivace dat představuje shromažďování informací pro případné pozdější účely. Znamená to tedy trvalé uložení dat, bez možnosti dalších změn. Archivovaná data nejsou přemazávána a počítá se s technologiemi pro rychlé vyhledávání a třídění výsledků.

Archivace dat plní následující cíle a to je dlouhodobá úschova informací, uvolnění primárních prostředků pro aktuální projekty, dislokace strategických dat, rychlost vyhledávání a možnost paralelního využití [1].

Důvody pro provádění archivace jsou uchování dat pro budoucí použití, ochrana před zničením dat a nutnost uchování dokladů o provedených pracích.

Velmi důležitý pojem při archivaci dat je jejich **životnost.** Rozlišujeme tedy:

- **Softwarovou životnost** – představuje životnost digitálního prostředí, ve kterém byla data vytvořena [1]. Jsou zde dvě metody, které se používají pro eliminaci vlivu prostředí a jsou to migrace a emulace. Migrací rozumíme metodu, jak čelit morálnímu stárnutí informačních technologií. Emulací rozumíme proces pro modelování vlastností digitálního prostředí na jiném počítači, než pro které byly určeny.
- **Fyzickou životnost** – představuje tedy fyzickou trvanlivost nosičů digitálního záznamu.



Obr. 9. Vliv životnosti na archivovaná data [1]

Základním požadavkem na archivační média je dlouhodobá spolehlivost a vysoká trvanlivost. Představuje především shromažďování informací pro případné pozdější použití. Protože při práci s archivem je důležité rychlé vyhledávání a třídění výsledků, významným prvkem pro archivace dat je jejich uspořádání [1]. Média vhodná pro tuto činnost musí být charakterizována vysokou rychlostí vyhledávání a trvanlivostí.

4 OPERAČNÍ SYSTÉMY A SERVERY

V následující kapitole jsou teoreticky popsány a vysvětleny operační systémy a servery, které jsou v praktické části rozvinuty.

4.1 Operační systémy

Operační systém můžeme chápat jako programové vybavení, které slouží jako spojovací článek mezi uživatelem a technickým vybavením [20]. Hlavním úkolem operačního systému je zajištění pro uživatele možnosti ovládání počítače, vytvoření stabilního aplikačního rozhraní a přidělování systémových zdrojů.

Provádí například vstup dat z klávesnice a myši - tyto data jsou následně předána příslušným programům, komunikaci s uživatelem a následné vykonání akcí, organizaci přístupů k datům nebo do paměti, komunikaci s externími zařízeními, reakci na chybové stavy a mnoho dalšího.

Nejznámější operační systémy jsou:

- **MS-DOS** – je jedním z prvních operačních systémů pro osobní počítače od firmy Microsoft. Pracoval v textovém režimu.
- **Windows** – je dnes nejpoužívanější operační systém pro osobní počítače. Pracuje v grafickém prostředí.
- **Linux** – je velmi stabilní a oblíbený operační systém pro osobní počítače. Může pracovat, jak v grafickém rozhraní, tak textovém.
- **Mac-OS** – je určen pro počítače typu Apple Macintosh. Má grafické rozhraní.
- **Solaris 10** – je operačním systémem od společnosti Sun Microsystems. Je založen na unixových operačních systémech.

Serverové operační systémy – v dnešní době všechny kanceláře, podniky, organizace nebo učebny výpočetní techniky směřují jednoznačně ke spojování počítačů do sítí. Aby jednotlivé počítače mohly v síti mezi sebou komunikovat, musí tuto funkci podporovat operační systém. Většina moderních operačních systémů má síťovou podporu v sobě přímo zabudovanou. Potom okamžitě po nainstalování, je možné nakonfigurovat je pro práci v síti. Serverové operační systémy jsou určeny pro instalaci na servery a kromě klasických funkcí, mají v sobě zabudovanou i správu uživatelů, uživatelských práv a správu zálohování, taky přístupy a práva k datovým zdrojům apod.

Mezi serverové operační systémy patří např. Windows 2003 Server, unixové systémy, Linux, Novell Netvare apod.

4.2 Servery

Slovem server se obecně označuje počítač, který poskytuje nějaké služby nebo počítačový program, který tyto služby zrealizuje. Samozřejmě servery jsou rychlejší, stabilnější a stavěné s důrazem na chlazení a nepřetržitý provoz. Používají se na nich operační systémy Windows, Unix, Linux, Mac atd., které jsou speciálně upravené.

Servery jsou uložené v serverových místnostech. Každá serverová místnost disponuje jiným technickým vybavením, jiným připojením a podobně. Musíme tedy respektovat hardwarové požadavky, a proto není jedno, kam server umístíme.

Služby, které server poskytuje v lokální síti, mohou být například sdílení disků, tiskáren nebo schopnost ověřit uživatele podle jména a hesla – autentizace. Ve větších sítích, jako je Internet, servery uchovávají a nabízejí webové stránky a poskytují další služby, jakou jsou DNS, e-mail a jiné. Poskytování služeb zajišťuje speciální program. V unixových systémech je označován jako *démon* a u Microsoft je označován jako *service*. Komunikace s klientem probíhá pomocí definovaného protokolu.

Server jako stroj, může být určený pro více typů provozu. Všechno záleží na tom, pro co bude daný server určený. Nejčastější typy serverů jsou:

- **Síťový server** – plní úlohu routeru, firewallu a realizuje požadavky klientských počítačů.
- **Webový server** – poskytuje uživatelům přístup na server prostřednictvím protokolu http a zobrazení webových stránek.
- **Databázový server** – plní úlohu shromažďování dat, které jsou uložené v databázi.
- **Mail server** – zabezpečuje komunikaci prostřednictvím elektronické pošty. Funguje na protokolech SMTP, IMAP a POP3.
- **Aplikační server** – slouží pro řízení aplikací typu klient-server.
- **Souborový server** – poskytuje místo pro uchování dat.
- **Tiskový server** – stará se o zprostředkování a rozložení tisku na síti mezi tiskárnami, tak aby tisk probíhal plynule.

5 ZABEZPEČENÍ VZDÁLENÝCH KOMUNIKACÍ

5.1 Virtuální Privátní Síť

Virtuální privátní síť (VPN) je soukromá síť zajišťující komunikaci v prostředí veřejné sítě. Podstata VPN je taková, že v rámci již stávající infrastruktury je část kapacity vyhrazena pro komunikaci v podstatě stejným způsobem, jako by byla fyzicky oddělena [24]. Ve skutečnosti tomu tak není, a oddělení je pouze virtuální. Filosofie virtuální privátní sítě je snaha o snížení nákladů využitím veřejného prostředí pro neveřejnou komunikaci.

Soukromá komunikace v rámci veřejné sítě probíhá za pomocí šifrování datové části každého paketu anebo šifrování celého paketu a jeho následné zapouzdření do nového paketu. S VPN můžeme spojit sítě s různými protokoly.

Existují tři základní druhy VPN:

- **Bezpečné** – garantují bezpečnost, ovšem jejich nasazení a údržba není triviální.
- **Důvěrné –** jsou schopné udržovat integritu dat, zajišťovat ochranu před odposlechem a zároveň garantují kvalitu. Ovšem svoji důvěru nestaví na šifrování, ale na poskytovateli.
- **Hybridní** – jsou smíšené sítě, které těží z výhod obou výše uvedených druhů.

Virtuální privátní síť se strukturou *místo – místo* dělíme na *intranetové*, jsou v rámci dané organizace a *extranetové* jsou mezi různými organizacemi. VPN jsou i se strukturou vzdáleného přístupu a využívají se k připojování, zpravidla odkudkoliv.

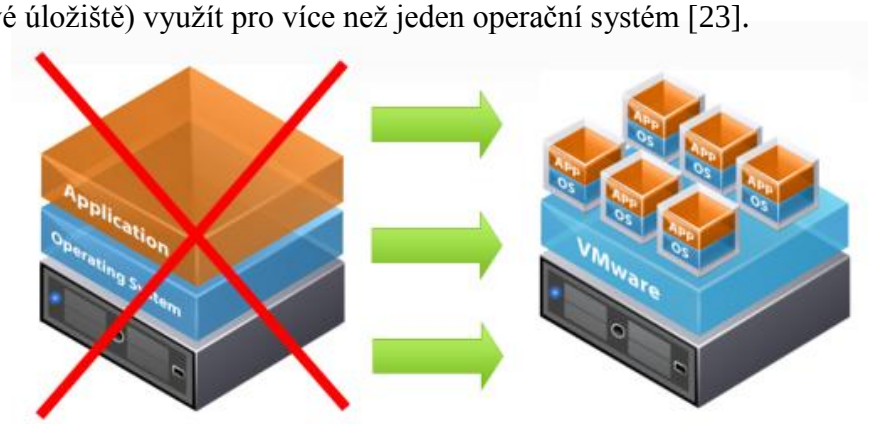
Největší výhody VPN kromě bezpečnosti je dramatické snížení nákladů na spojení. Dále nezáleží na tom, kde a jak jsou rozmístěné jednotlivé počítače nebo lokální sítě, protože dovede v rámci nezabezpečeného spojení předávat data bezpečně. V neposlední řadě i vzdálené stanice nebo servery se lépe spravují, a bezpečnostní politika na nich se lépe vynucuje.

Nicméně VPN má i své úskalí. Je zapotřebí zajištění kvalitní bezpečnosti na klientské straně. Musí se dohlížet na klienty a na jejich chování. Zde je velmi nutná bezpečnostní politika.

Každý sebemenší bezpečnostní průnik nebo incident totiž ohrožuje celou síť organizace [22].

5.2 Virtualizace

Virtualizace je abstrakce výpočetních zdrojů neboli rozdělení výpočetních zdrojů jednoho fyzického systému. Jinými slovy lze říci, že pomocí virtualizace jsme schopni jeden zdroj (pod pojmem zdroj si můžeme představit celý server, případně jeho části – procesor, síťová karta, datové úložiště) využít pro více než jeden operační systém [23].



Obr. 10. Tradiční architektura vs. virtuální architektura [23]

Existující metody:

- **Softwarová emulace hardwaru** – neboli plná virtualizace. Výhodou emulace je absolutní nezávislost na hardwaru a možnost provozovat ve virtuálních serverech nezměněné operační systémy. Nevýhodou tohoto přístupu je samozřejmě velká výkonnostní režie. Tento typ virtualizace lze tedy uplatnit jen při velmi malém počtu virtualizovaných strojů [24].
- **Virtualizace s hardwarovou asistencí –** je zaměřená na hardwarovou podporu virtualizace na úrovni procesorů, chipsetů, pamětí a dalších komponent. Umožňuje mít několik desítek virtuálních strojů na jednom fyzickém.
- **Paravirtualizace** – metoda virtualizace, která vyžaduje zásah do jádra operačního systému provozovaného ve virtuálním prostředí [24]. Výhoda je obecně nižší výkonnostní režie a nevýhoda spočívá v nutnosti používat upravené operační systémy.
- **Virtualizace na úrovni operačního systému** – Virtualizační vrstva je umístěna mezi operačním systémem serveru a virtuálními servery. Na jednom fyzickém serveru je podporován pouze jeden operační systém.

Díky možnosti provozovat mnoho virtuálních počítačů na jednom fyzickém stroji je možné vystačit s menším počtem fyzických serverů, což znamená menší spotřebu elektřiny, méně

místa, méně tepla a méně nároků na chlazení. Zároveň díky stále se zvyšujícímu výkonu současného hardwaru, je možné tento výkon lépe využít provozem hned několika serverů v různých rolích na jediném fyzickém stroji [24].

5.3 Firewall

Ve světě počítačových sítí je firewall zařízení, které řídí komunikaci na síti nastavením určitých pravidel. Nebezpečí obvykle pochází od útočníků, kteří se pokoušejí získat přístup do naší sítě z Internetu [2].

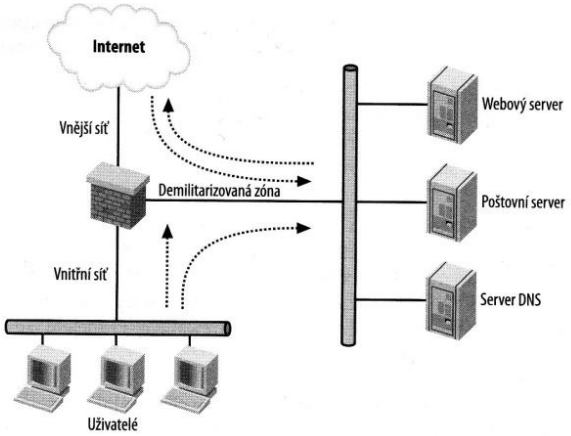
Firewallem může být samostatné zařízení, software běžící na serveru nebo směrovači nebo modul integrovaný do většího zařízení, a v dnešní době může být i firewall obsažen v domácích zařízeních, jako je modem, směrovač atd.

Firewally často podporují služby sítí VPN. Firewall běžící jako aplikace na serveru může se serverem sdílet další funkce, jako například DNS nebo elektronickou poštu [2].

Pro bezpečnost jsou doporučeny následující postupy:

- Při návrhu bezpečnostních pravidel a konfigurace firewallu je velmi důležité, aby pravidla byla dobře čitelná a srozumitelná.
- Zprávy o stavu firewallu musíme ukládat do protokolů na server a musíme tyto zprávy pravidelně kontrolovat.
- Měli bychom zakázat vše a povolit jen to, co potřebujeme [2].
- Všechno, co je spojeno s naší sítí a co pochází od třetí strany, by mělo být pod kontrolou firewallu.

Demilitarizovaná zóna – je definována jako samostatná oblast, která je připojena k firewallu. Tato síť může být přístupná jak zevnitř, tak také z vnější strany firewallu. Bezpečnostní pravidla řídí zařízení v demilitarizované zóně a jejich připojení do jiných sítí.



Obr. 11. Jednoduchá síť demilitarizované zóny [2].

Vnitřní síť navazuje spojení k jiné síti, ovšem žádná jiná síť nemůže navázat spojení k vnitřní síti. Vnější síť nemůže nevázat spojení k vnitřní síti, ale k demilitarizované ano. A demilitarizovaná zóna může navázat spojení k vnější síti, ale ne k vnitřní a jakákoliv jiná síť může navázat spojení do demilitarizované zóny. Výhoda je, že pokud dojde k útoku na poštovní server a on je narušen, útočník nezíská přístup k uživatelům ve vnitřní síti. Z návrhu ale plyne, že útočník bude mít přístup k ostatním serverům v demilitarizované zóně. Servery v této zóně by měly být uzamčeny pomocí bezpečnostních opatření.

II. PRAKTICKÁ ČÁST

6 BEZPEČNSOT INFORMAČNÍCH TECHNOLOGIÍ VE FIRMĚ

Praktická část diplomové práce je zaměřena na společnost Česká Zbrojovka, a.s. Nejprve se stručně seznámíme se současným stavem bezpečnosti informačních technologií. Následuje stručná historie firmy České Zbrojovky, a.s. V další části je stručně zobrazena strukturovaná kabeláž firmy, struktura LAN, VLAN a UPS. Následně jsou popsány používané operační systémy na počítačích a serverech. Následují kapitoly, které jsou zaměřeny na uložení dat a zabezpečení vzdálených a lokálních komunikací ve firmě. Poslední kapitola je věnována shrnutí slabých míst a řešení pro odstranění nebo částečnou eliminaci.

6.1 Současný stav bezpečnosti informačních technologií

Informační bezpečnost a její součást – bezpečnost kybernetickou – je třeba chápat jako nutnost zahrnující nejenom oblast technologickou, ale i sociální nebo psychologickou. Jednotlivé země světa jako je Korejská republika, Spojené státy americké, Japonsko, některé členské země Evropské unie a další státy, kladou na problematiku informační bezpečnosti velký důraz.

Informační technologie se stále více využívají k páchání trestné činnosti. Roste výskyt nežádoucích materiálů, které se umísťují na Internet, ale i vylákání přihlašovacích údajů do internetového bankovnictví a nebezpečné jsou také neúmyslné útoky. Informační bezpečnost je tedy oblast, která vyžaduje neustálou péči.

Česká republika patří mezi země, které jsou zásadním způsobem závislé na fungování informačních technologií, zejména v oblastech finančních služeb, dodávek pohonných hmot, elektrické energie, tepla, vody, systémů sociálního a zdravotního zabezpečení a veřejné správy. Je jen otázkou času, kdy se stane závažný incident s dopadem na tyto informační systémy, nebo kdy se země stane terčem ničivého synchronizovaného kybernetického útoku.

6.2 Historie firmy Česká zbrojovka, a.s.

O výstavbě zbrojního závodu v Uherském Brodě bylo rozhodnuto v polovině roku 1936. Uherskobrodská městská rada schvaluje dne 22. července 1936 stavbu nového závodu. Dne 28. července 1936 je proveden první výkop a tím zahájena výstavba nového závodu v Uherském Brodě.

27. 06. 1936 – založení České zbrojovky v Uherském Brodě jako pobočný závod České zbrojovky a. s. Strakonice

02. 01. 1937 – zahájení výroby v novém závodě

01. 01. 1950 – založeno Přesné strojírenství, národní podnik, Uherský Brod, jako organizační součást generálního ředitelství Přesné strojírenství v Praze

01. 04. 1958 – podnik organizačně začleněn pod Závody říjnové revoluce, národní podnik Vsetín, závod 05 Uherský Brod

01. 07. 1965 – podnik začleněn pod generální ředitelství VHJ Zbrojovka Brno pod názvem Přesné strojírenství, národní podnik, Uherský Brod

01. 01. 1983 – podnik začleněn do koncernu Agrozet Brno, pod názvem Agrozet, koncernový podnik, Uherský Brod

01. 07. 1988 – založen státní podnik Česká zbrojovka, Uherský Brod

01. 05. 1992 – založena Česká zbrojovka, akciová společnost, Uherský Brod [39].

7 STRUKTURA LOKÁLNÍ SÍTĚ

V této kapitole jsem se zaměřila na strukturovanou kabeláž v budovách firmy Česká Zbrojovka, a.s., dále na jejich páteřní síť, strukturu VLAN a napájení systému.

7.1 Strukturovaná kabeláž

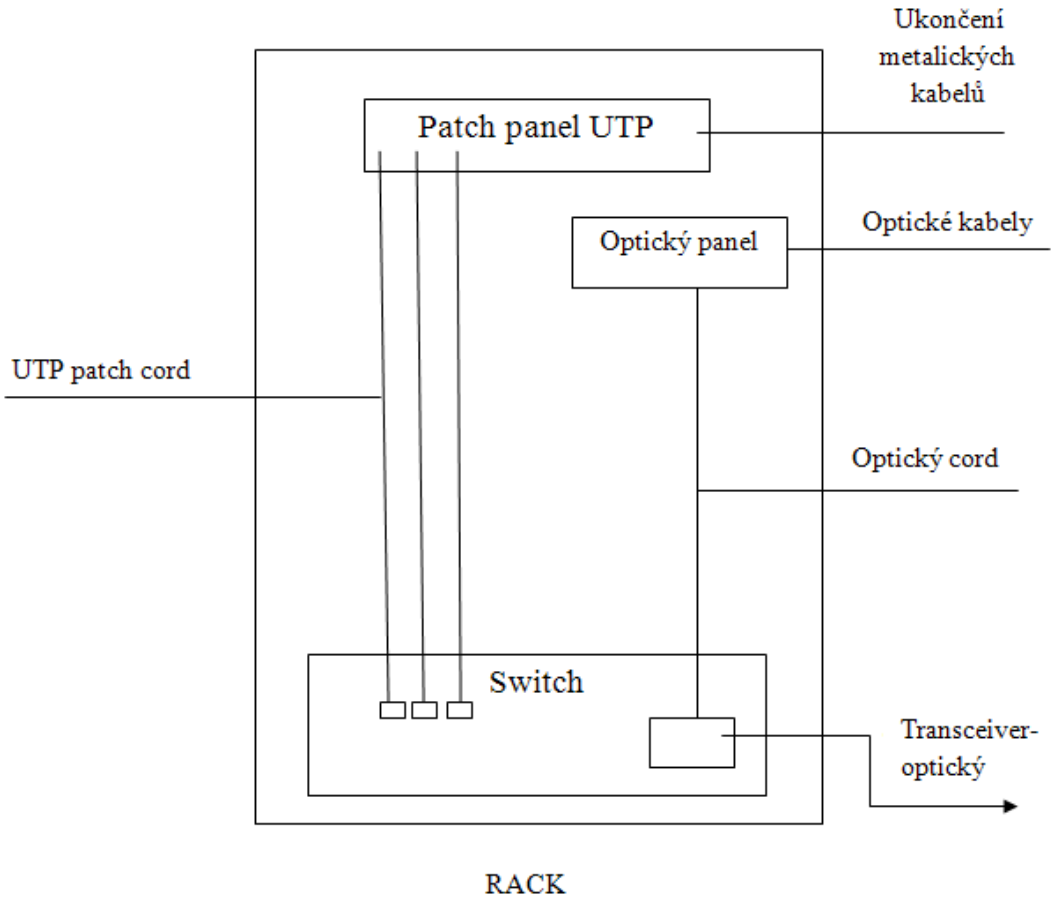
Strukturovaná kabeláž tvoří součást infrastruktury v moderních lokálních počítačových sítích. Kabelový systém umožňuje přenos nejenom dat, ale i propojení VoIP telefonů, zejména v nových budovách nebo v případě rekonstrukce starých telefonních rozvodů. Prostřednictvím přizpůsobovacích prvků, jako jsou konvertory a převodníky, je strukturovaná kabeláž používána i pro komunikační systémy. Například pro přenos videosignálu, zabezpečení objektů apod.

Strukturovaná kabeláž je provedena podle doporučení a norem. Centrální propojení v síti je zde realizováno prostřednictvím páteřních rozvodů. Jsou většinou optické, někdy i metalické, ale ty jsou nevýhodné. Páteřní optické kabely jsou zřídka v rámci budovy, ale hlavně mezi budovami. V rozvaděčích jsou umístěny propojovací systémy neboli propojovací panely (patch panel), které jsou umístěny v rozvaděčových skříních (RACK). Zadní část propojovacích panelů slouží pro ukončení kabelových rozvodů a přední část propojovacích systémů je osazena konektory RJ45 pro snadné propojení s aktivními prvky. V některých případech je spojení provedeno speciálními zářezovými konektory. Zásuvky tedy nabízejí prostřednictvím konektoru RJ45 připojení libovolných koncových prvků jako je telefon, tiskárna, CNC stroj nebo počítač. Pro připojování koncových prvků k zásuvce a propojení portů aktivních prvků s propojovacím panelem se používá propojovací kabel (patch cable nebo patch cord).

Jak propojovací panely, tak i zásuvky mají možnost popisu. Ten by měl být v rámci jednoho kabelu na obou koncích totožný. Systém popisování je spojen s číslováním místností v rámci budovy a s pořadím zásuvky. Číslování přípojných míst je nejvýhodnější spojit s číslem místnosti, protože potom dochází, ve snaze o úspory, k poddimenzování počtu přípojných míst a tím i k pozdějšímu dodělávání nových přípojných míst. Narušení posloupnosti čísel zásuvek bývá potom zbytečně matoucí.

19 - ti palcová skříň (RACK) má uvnitř aktivní prvky a propojovací panely. Součástí skříně jsou i doplňky, jako například ventilační jednotka s termostatem a dohledový systém aktivních prvků a serverů. Kabely rozvodů jsou umístěny do plastových nebo ocelových

žlabů. Žlaby jsou používány jednoduché se zásuvkami montovanými na zdi, nebo modulární, které jsou speciálně vyrobené pro montáž zásuvkových modulů.

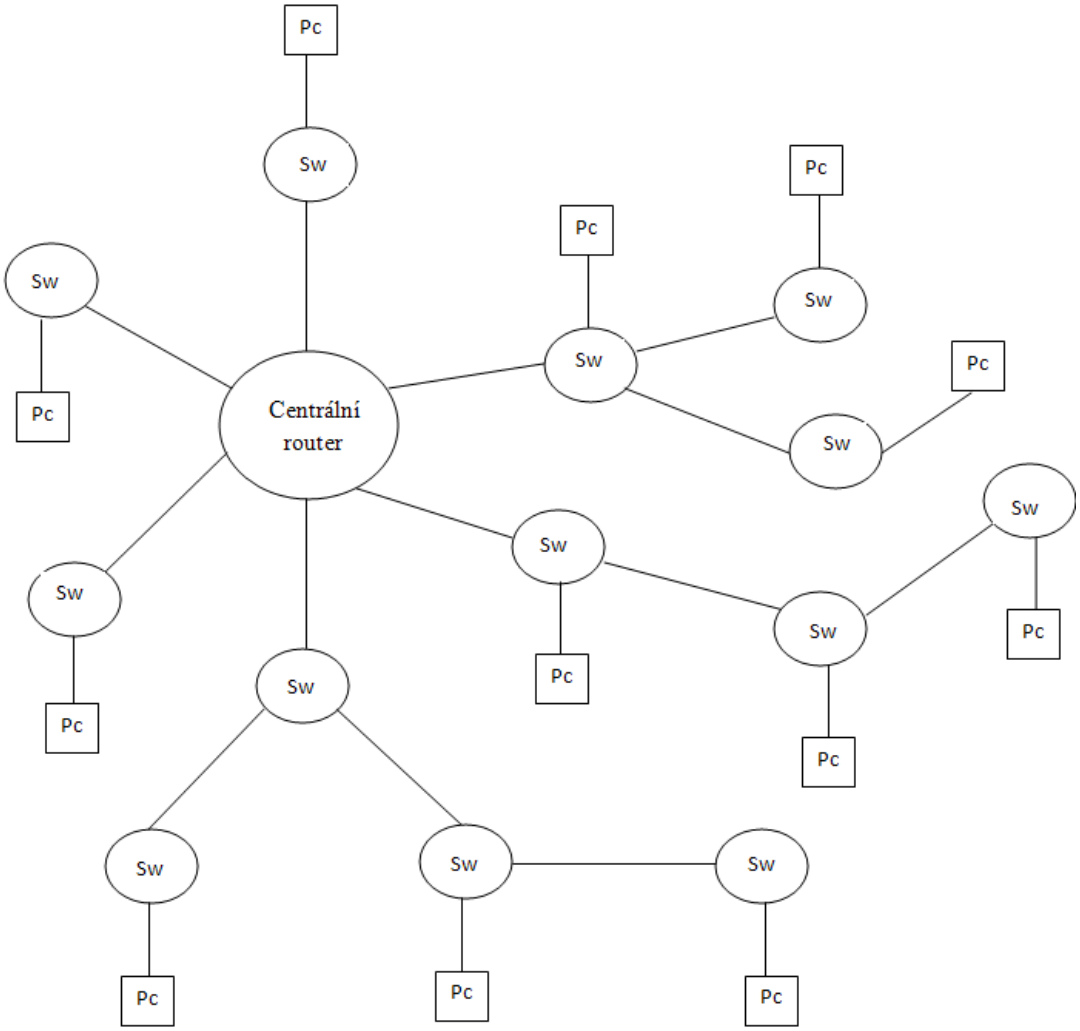


Obr. 12. Páteřní optická síť mezi jednotlivými budovami a rozvaděči[vlastní zpracování]

7.2 Struktura lokální počítačové sítě

Při vytváření sítí LAN je třeba dodržet určitá pravidla, řídit se plánem. Zde představím stručně, jak proces probíhal v historii firmy. Nejprve byly v analýze potřeb sepsány potřeby firmy. Efektivní analýza potřeb připojení PC se zabývá snižováním nákladů nebo zvyšováním zisků. Následně se provedla analýza struktury sítě. Začaly shromažďovat informace o zařízeních, a poté se řešilo kabelové vedení. Současně byly vyřešeny servery a jejich organizace. Důležitou věcí je i plán konfigurací jednotlivých zařízení, kde se upřesňují HW konfigurace, jména počítačů, adresáře serverů, uživatelů serverů, seznam tiskáren a jejich propojení.

Firma Česká Zbrojovka, a.s. má hvězdicově – sběrnicovou strukturu. Více o strukturách počítačových sítí je v teoretické části.

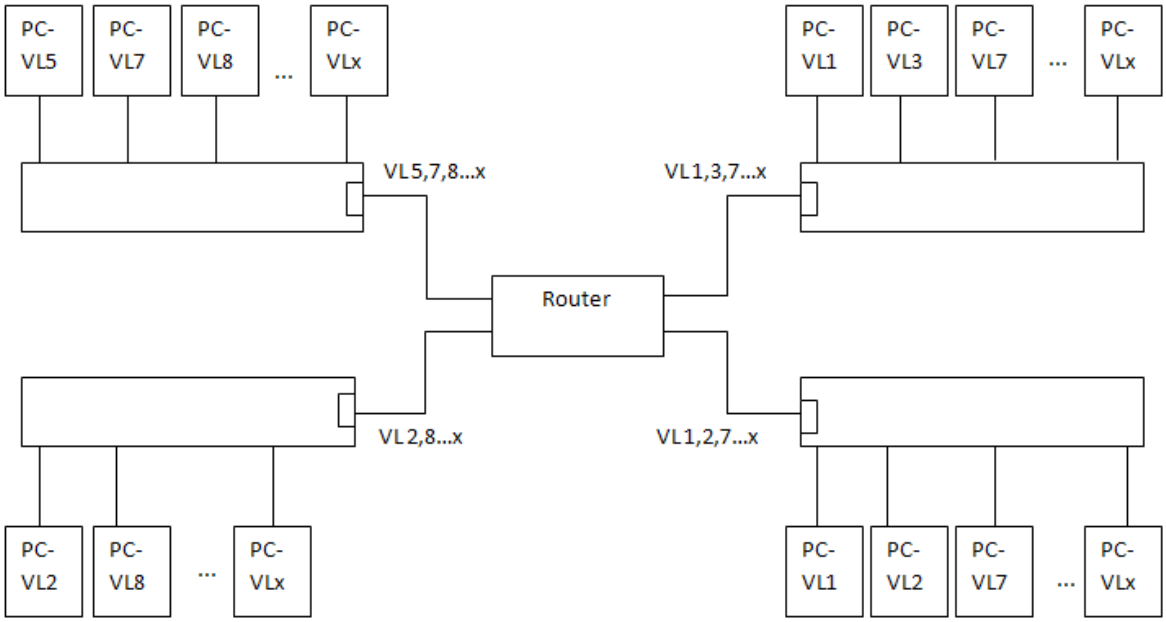


Obr. 13. Modelový příklad topologie v CZUB [vlastní zpracování]

Pozn.: Skutečná topologie v CZUB nemohla být zveřejněna z důvodu utajení informací.

7.3 Struktura VLAN

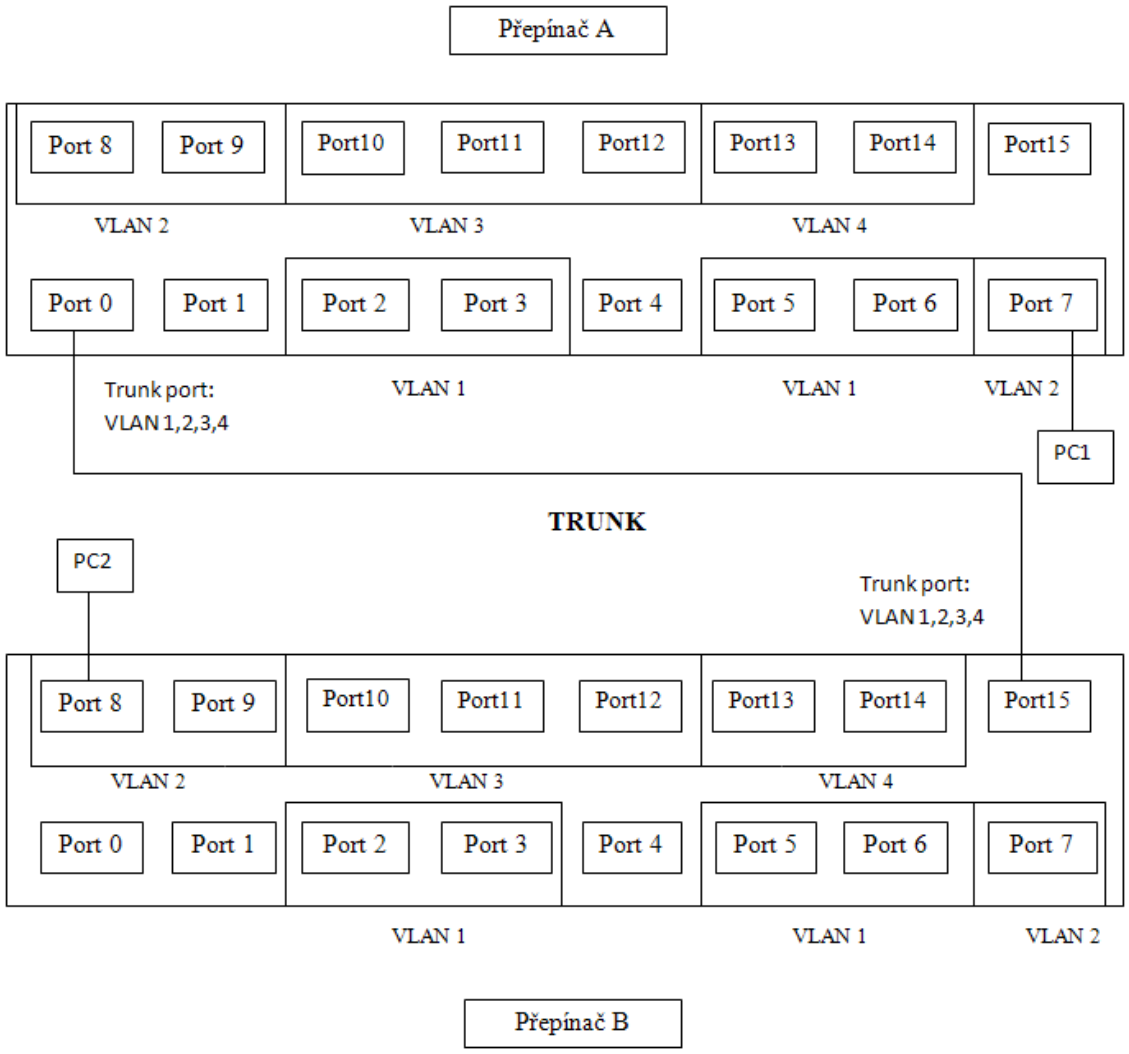
S pojmem VLAN jsme se setkali už v teoretické části. Zde popíši určitou část ve firmě, kde jsou VLAN použity a jak fungují.



Obr 14. Modelový příklad VLAN ve firmě [vlastní zpracování]

Obrázek 14. Znázorňuje propojení sítí VLAN. Počítače jsou připojeny k portům. Pro názornost je vybrána VLAN 7. Počítače komunikují s VLAN 7 v horní levé části obrázku, tak s VLAN 7 v pravé horní části a taky s VLAN 7 v pravé dolní části.VLAN je tedy propojena se stejnou VLAN v jiném místě v síti. Pokud ovšem chceme povolit komunikaci VLAN 7 s VLAN 8 je nutné toto spojení správně nakonfigurovat na routru. Je propojeno současně i vice VLAN jedním spojením, to nazýváme *trunk*.

Obrázek 15. Znázorňuje modelový příklad dvou přepínačů propojených pomocí trunku. PC1 je připojeno k sítí VLAN 2 na přepínači A a PC2 je připojeno k sítí VLAN 2 na přepínači B. Jelikož mezi těmito přepínači je v rámci trunk definována VLAN 2, potom PC1 komunikuje s PC2. Nutná podmínka pro tuto situaci je, aby trunk porty měly nadefinované VLAN požadované pro spojení. Z obrázku je patrné, že páteřní porty mají definovány všechny používané VLAN. Tyto porty jsou nazývaný *trunk porty*.



Obr. 15. Modelový příklad dvou přepínačů propojených pomocí trunku

[vlastní zpracování]

7.4 Napájení

Napájení je u serverů řešeno zálohováním veřejného rozvodu 220V, tedy zdroji nepřerušovaného napájení, takzvaných UPS. Tyto zdroje zajistí spotřebičům nepřetržitou dávku elektrické energie po dobu výpadku. Čas je omezen kapacitou UPS baterií, jedná se o časy do 10 min.

Jednotka UPS je složena z usměrňovače pro řídící obvody a nabíjecí baterie. Usměrňovač je měnič pro usměrňování střídavého napětí napájecí sítě 220V na stejnosměrné napětí pro dobíjení baterie. Usměrňovač může být neřízený (diodový), tyristorový nebo tranzistorový. Střídač je měnič pro přeměnu stejnosměrného napětí baterie na střídavé napětí 220V. Je zpravidla tranzistorový. Baterie je skupina propojených akumulátorových článků fungující

jako zásobník energie pro zálohování napájecí sítě. Je zpravidla konstrukční součástí jednotky UPS. U velkých zdrojů, popř. při velké kapacitě, může tvořit samostatný celek, často v modulovém (stavebnicovém) provedení. Kapacita baterie určuje zálohovací dobu, tj. maximální dobu bateriového provozu, která může být požadována v délce od několika minut, potřebných pro překlenutí krátkodobých poruch napájení sítě, pro řízené odstavení zálohovaných spotřebičů (např. serverů) nebo zprovoznění náhradního zdroje, k desítkám minut až po hodiny u speciálních zálohovacích systémů. Obtok (bypass) je náhradní elektrická cesta zřízená paralelně k jednotce UPS, umožňující přemostění UPS v případě jeho poruchy nebo při přetížení. Spínač UPS je spínač určený k připojení a odpojení UPS nebo obtoku k zátěži [26].

Ve firmě se používají paralelní UPS, které jsou tvořeny několika paralelně zapojenými jednotkami UPS, jejichž střídače pracují synchronně a jsou opatřeny zařízením pro rozdělování výkonu. Cílem je tedy větší výkon zálohovacího systému.

UPS jsou vybaveny i výkonným počítačovým řídicím systémem. Dokáže také řídit tvar a velikost výstupního napětí, výstupní kmitočet a přechod mezi jednotlivými provozními režimy UPS. Další funkcí řídicího systému jsou především jištění UPS pro ochranu zařízení před přetížením, přepětím, nadměrným oteplením, hlubokým vybitím baterie apod. Hlavním úkolem diagnostiky je tedy rychlá identifikace poruch, minimalizace jejich následků a včasná identifikace zhoršení parametrů, které naznačují hrozící poruchu. Výstupem poruchové diagnostiky je automatické aktivování náhradního řešení nebo automatické protokolování provozních událostí UPS.

Dalším významným úkolem řídicího systému UPS je komunikace s okolím, například se zálohovanými spotřebiči nebo s obsluhou. V prvním případě může poskytnout UPS po datové síti varování, že se přechází na bateriový provoz a v druhém případě jde o dálkovou datovou komunikaci prostřednictvím ovládacího panelu připojeného na počítačovou nebo mobilní síť s možností obsluhy ze vzdáleného centra.

8 POUŽITÉ OPERAČNÍ SYSTÉMY NA POČÍTAČÍCH A SERVERECH

V této kapitole se zaměřím na operační systémy na serverech a počítačích ve firmě, firewally, antiviry, antispyware a VMWARE.

8.1 Operační systémy

8.1.1 Operační systémy na serverech

Windows 2000 server:

Windows 2000 server je velmi zastaralý systém a sdílí stejné rozhraní jako Workstation Windows 2000 Professional, avšak má navíc další součásti pro vykonání serverových úkonů, běh infrastruktury a aplikačního softwaru. Významná komponenta je zde *Active Directory* a taky *Domain Name Server*, který umožňuje dynamickou registraci IP adres podle jména stanice.

Dále obsahuje podporu WWW, která zjednodušuje použití a zlepšuje funkčnost a zabezpečení. Dále je zde široká podpora hardwaru a zařízení, integrována služba Terminal Services, podpora sítí VPN a jiné.

Windows 2003 server:

Windows 2003 server sdílí důležité části se systémem Windows XP Workstation. Jedná se o moderní, uživatelsky příjemný operační systém pro 32, 64 bitové Windows a pro Microsoft .NET Framework. Obsahuje síťové služby, souborové a tiskové služby, ale také robustní řešení pro centralizovanou správu a zajištění síťových politik pomocí technologie *Active Directory* druhé generace, umožňující centrální autentizaci a autorizaci klientů.

Následně jsou uvedeny důležité pojmy:

Active Directory:

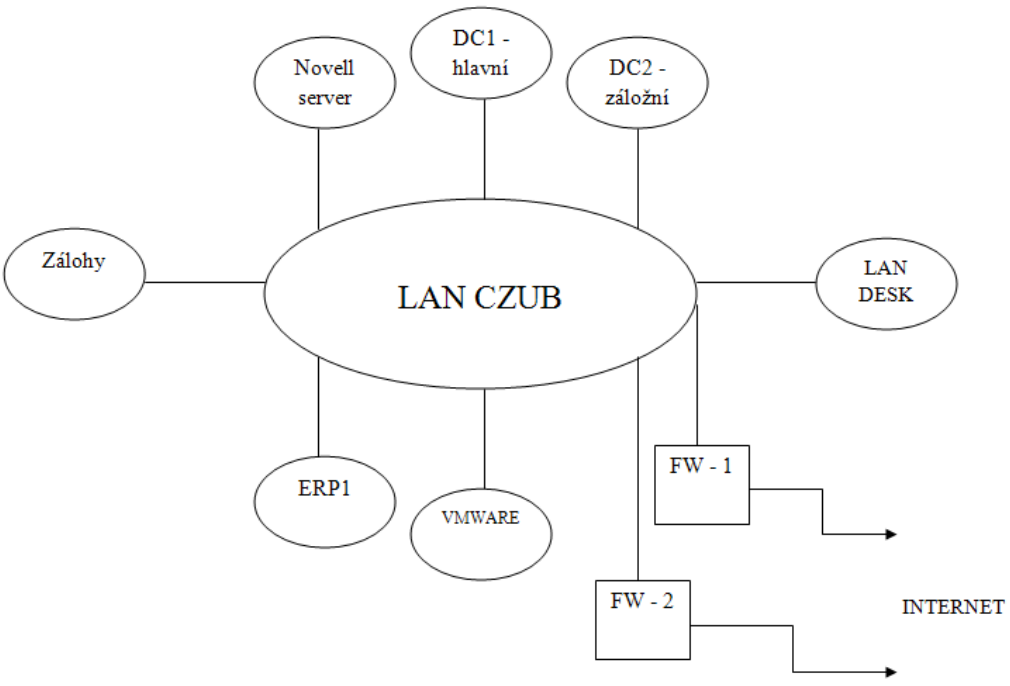
Active Directory (AD) označuje adresářovou službu ve firemním prostředí podle firmy Microsoft. Je součástí Windows serveru 2000/2003. Zahrnuje správu uživatelů, hromadné instalování aplikací a umožňuje správu politiky jednotlivých počítačů. Data uložená v AD jsou organizovány jako objekty a *Active Directory schema* definuje tyto objekty. Schéma tedy definuje druhy objektů a typy informací, které se mohou uchovávat. Jsou dva typy objektů. První se nazývá *schema classes* a druhý *schema attributes.* Logická struktura

Active Directory je tvořena pomocí lesa, stromů, domén a organizačních jednotek. Fyzická struktura je tvořena pomocí doménových řadičů a sítě.

Doménový řadič:

Doménový řadič (DC) neboli Domain Controller je počítač - server na kterém běží právě již zmiňované operační systémy Windows Server 2000/2003. DC obsahuje lokální doménovou databázi. V doméně může být více doménových řadičů a každý obsahuje úplnou repliku adresáře pro danou doménu.

Pokud máme více DC v jedné doméně a provedeme nějakou změnu v AD, tak se změna provede jen na jednom DC a následně se provede automatická replikace na ostatní DC. Označuje se to jako funkce *singlemaster*, kde je jeden DC hlavní a ostatní podřízení (slave).



Obr. 16. Modelový příklad serveru v LAN CZUB [vlastní zpracování]

8.1.2 Operační systémy na počítačích

V praxi jsou použity tyto operační systémy:

Windows 2000:

Windows 2000 je jméno pro operační systém, vyvíjený původně pod názvem Windows NT až do verze 5.0. Podporuje systém souborů *NTFS*, *Active Directory* (po přihlášení do AD), *Distributed File Systém* – je to systém souborů, která podporuje sdílení souborů, *Plug-and-play* – technologie, která umožňuje jednodušší rozpoznání a konfiguraci hardware, *DirectX* – sada knihoven, které poskytují aplikační rozhraní pro přímé ovládání moderního hardwaru. Windows 2000 je ve verzi 32 bitové. Tyto operační systémy tvoří nejmíň polovinu operačních systémů v České Zbrojovce, a.s.

Windows XP:

Windows XP byl vyroben v 32bitové verzi, ale v roce 2005 byla vydána na verzi Windows XP Professional x64 Edition, který je určen pro 64bitové procesory. Windows XP měl celkem tři aktualizované balíčky. Podporuje USB 2.0, jazyk Java, posléze bylo přidáno šifrování WPA pro bezdrátové sítě Wi-Fi, podpora Bluetooth následně byl začleněn nástroj *Windows Security Center* – poskytuje rozhraní pro antivirové programy. Ve firmě Česká Zbrojovka, a.s. operační systémy Windows XP tvoří ¼ operačních systémů.

Windows 7:

Windows 7 je ve firmě používán ve verzi 32 bitové, tak v 64 bitové. Obsahuje velkou řadu změn oproti předchozím operačním systémům Windows. V této verzi je zahrnuto rychlejší startování systému, podpora pro virtuální disky, rozpoznávání řeči anebo rukopisu dále bylo třeba *Centrum zabezpečení systému Windows* přejmenováno na *Windows Solution Center* atd. V České Zbrojovce, a.s. jsou operační systémy Windows 7 zastoupeny ¼.

8.2 Zabezpečení počítačů

8.2.1 Firewall v síti CZUB

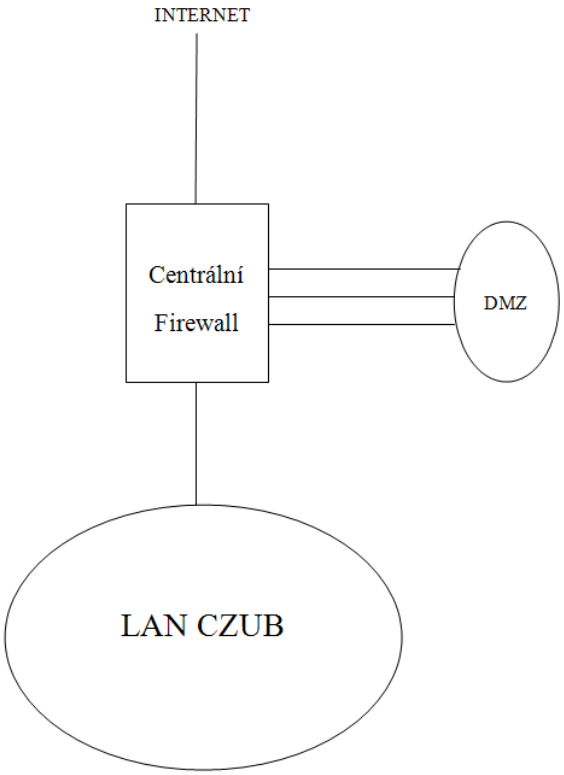
Firewally jsem popisovala v teoretické části. Zde se zaměřím na výhody a nevýhody využití firewallu ze strany firmy a způsob využití a zapojení jednotlivých částí.

Výhody:

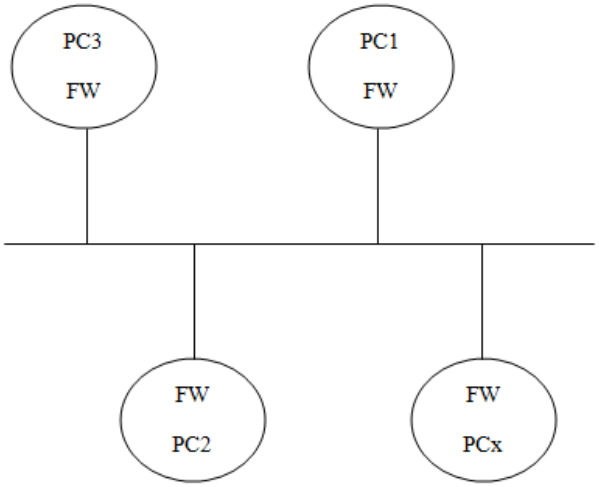
- Ochrana proti internímu napadení v LAN CZUB
- Ochrana proti externímu napadení – jedná se o napadení z venku (Internet) směrem do LAN CZUB
- Zvýšení přehledu povolených komunikací
- Zvýšení bezpečnosti
- Ochrana počítačů
- Administrace VPN připojení – bezpečná komunikace vzdálených klientů

Nevýhody:

- V komunikaci z Internetu do sítě CZUB – nutná definice pravidel
- U centrálním firewallu je nutná investice do hardwaru a softwaru



Obr. 17. Modelový příklad centrálního firewallu [vlastní zpracování]



Obr. 18. Modelový příklad firewallu v lokální síti [vlastní zpracování]

8.2.2 Antivir, antispam a antispyware

Antivir:

Antivir je počítačový software a slouží k odstranění, eliminaci a identifikaci počítačových virů a nebo malware (škodlivého softwaru). Kontroluje procesy v operační paměti a na lokálním disku a detekuje podezřelé aktivity nějakého počítačového programu. Je umístěn jak na centrálním firewallu, tak i na počítačích v síti.

Existují metody kontroly:

- **Virové slovníky** – pří kontrole souborů zjišťuje antivirový program, zda se neshoduje nějaká jeho část s některým ze známých virů, které má v databázi. Pokud je nalezena shoda, pak se pokusí opravit soubor tím, že odstraní vir ze souboru. Další možnost je, že umístí soubor do karantény (speciální složka na disku se zabezpečením přístupu uživatelů). A poslední možnost je, že smaže infikovaný soubor. Dosažením úspěchu je pravidelná aktualizace virové databáze.
- **Nebezpečné chování** – metoda, která sleduje chování všech programů. Pokud se objeví podezřelé chování, pak antivirus označí toto nebezpečné chování a upozorní uživatele, kterého pak vybídne k dalšímu postupu. Tato metoda má výhodu v tom, že ačkoli je virus zcela nový, neznámý ve virových databázích, může ho snadno odhalit. Nevýhoda je v hlášení velkého množství falešných virů.
- **Další metody –** zde je například zařazen Sandbox. Ten je využívám pro spouštění neotestovaného kódu nebo nedůvěryhodného programu v odděleném prostoru

operační paměti. Je zda zařazena i metoda, která předchází spouštění všech kódů kromě těch, které byly již dříve označeny uživatelem za důvěryhodné.

Antispam:

Antispam je software, který zachytává a označuje nevyžádanou poštu, která je hromadně rozesílaná uživateli nebo roboty z většinou neexistujících adres. Zde jde o přesné identifikování, kdy e-mail ještě není a kdy je už spamem. Využívá se systém hledání příznaků v e-mailu a každý z nich ohodnotí určitým počtem bodů. Pokud součet bodů překročí definovanou mez, označí jej jako spam. Je tedy velmi důležité správné nastavení Antispamu. Antispam je umístěn na firewallu, zřídka na stanicích a ve vyšších verzích MS Outlook.

Antispyware:

Antispyware je software, který má za úkol odstraňovat *spyware* - jsou to programy, které využívají internetu k odesílání dat z počítače bez vědomí uživatele. Může způsobit vysokou škodu vynesením citlivých informací z počítače. Zaznamenávají každý krok, který na Internetu provedeme. Mohou to být seznamy webových stránek, ale i přihlašovací údaje a hesla. Antispyware si musí poradit se spyware, který způsobuje stahování a instalaci dalšího škodlivého softwaru bez vědomí uživatele nebo změnu chování prohlížeče.

Komplexní ochrana v CZUB je eTrust:

Ve firmě je použit antivirus a antispyware **eTrust**, který využívá centrálního řízení, tedy vnutí počítači aktualitu a nastavení. Antivirus eTrust pro stanici nebo server má lokální skener, který pracuje v režimu „resident“ pod jménem Realtime Monitor a k tomu má další škály skenerů. Grafické rozhraní je přehledné a navíc má Log Viewer, což je velmi dobrý způsob přehledu o všem, co antivirus zaznamenal. Dále je zde centralizovaná správa. Administrátorská konzole slouží především k definování centrálních politik a jejich aplikaci na cílové počítače. Je zde možnost určení politiky pro ochranu poštovní komunikace na klientských strojích. Spravování a navazování politik na stanicích je vyřešeno pomocí hierarchické struktury skupin, kterou si navrhne administrátor. Používá se rozhraní pro vzdálenou instalaci antiviru na klientské stanice. Můžeme monitorovat síť, vyhledávat počítače v síti za účelem činnosti eTrust systému.

8.3 Proxy server

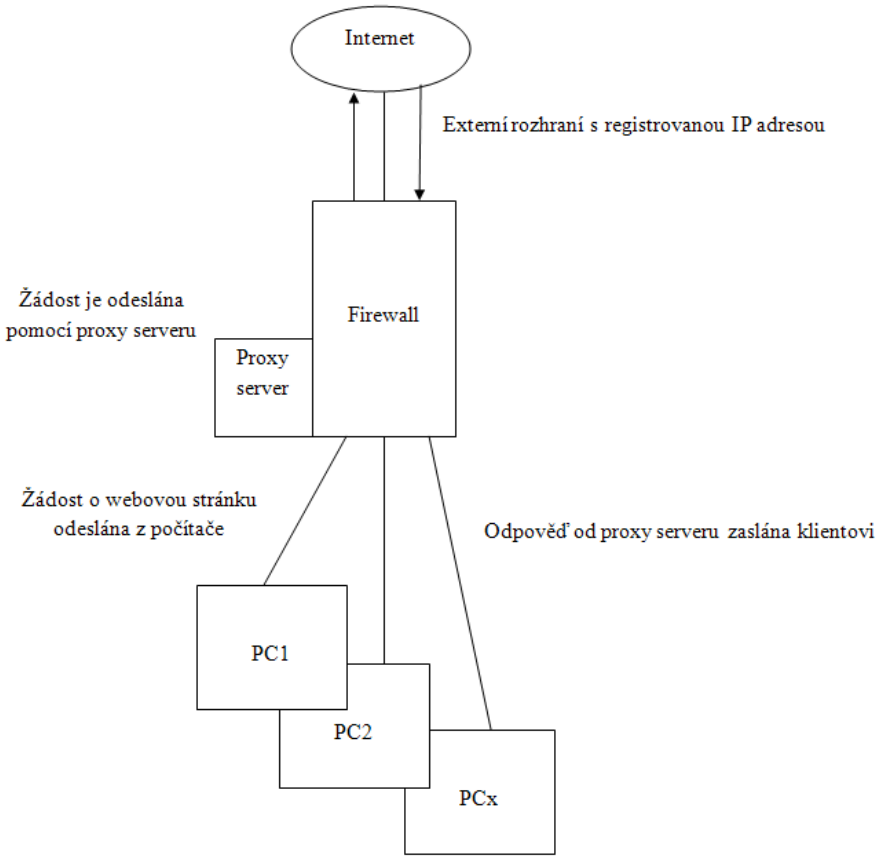
Proxy server:

Proxy server je umístěn mezi klientem a serverem a dělá mezi nimi prostředníka v komunikaci. Proxy se tedy vůči klientovi tváří jako server a přebírá jeho požadavky. Ty pak odešle serveru a přebírá i odpověď, kterou odešle klientovi. Proxy serverem se ve firmě zabezpečuje komunikace v síti (kontroluje přístup do internetu, povoluje pouze služby, které jsou povoleny politikou firmy). Jsou zde dva druhy proxy serverů:

- **Aplikační Proxy server –** je jen pro určité služby typu: http, ftp atd. A na straně klienta stačí nastavit jen jméno proxy serveru a port (Mozilla Firefox, MS Internet Explorer).
- **Socket proxy servery –** funguje pro různé TCP, UDP služby a musí být podpora na straně klient (instalován program, který tento přenos vyžaduje).

Využívá se i *HTTP Proxy cache*, což je typ proxy serverů disponující pamětí pro uchování odpovědí serverů, které jsou k dispozici při dalším požadavku. Důležitý je i *Squid* – je to proxy cache server, který umí obsluhovat protokoly http, ftp a další využívající url.

Proxy server je v CZUB server, který funguje jako prostředník mezi webovým prohlížečem a Internetem. Ve společnost CZUB se používá speciální Proxy Server s logováním probíhajících přenosů.



Obr. 19. Modelová ukázka proxy serveru v síti [vlastní zpracování]

8.4 VMWARE – virtualizace serverů a PC

Virtualizace přináší mnoho výhod a firma je založena na nejmodernější virtualizační platformě na trhu a to na softwaru VMware vSphere. Virtualizace pomáhá firmě snížit kapitálové výdaje prostřednictvím konsolidace serverů a optimalizovat provozní výdaje pomocí automatizace.

Virtualizace fyzických serverů umožňuje vytvoření flexibilnější infrastruktury IT, takže firma reaguje rychle na změny na trhu a potřeby provozu IT. Samozřejmě s virtualizací aplikací se prodlužuje životnost starších aplikací a eliminují se konflikty spojené s instalací. U detašovaných pracovišť se může pracovní plocha přesunout do oblasti VMware, kde bude poskytována jako spravovaná služba a zároveň se tím zachová potřebná kontrola a zabezpečení. Virtualizace pro systém Windows usnadňuje migraci operačních systémů.

Virtualizace firemních serverů umožňuje pomocí VMware virtualizovat i nejnáročnější aplikace jako je třeba Oracle, MSSQL, MS Exchange a podobně. Dále dynamicky přiděluje zdroje podle potřeby aplikací a to umožňuje dodržet požadované úrovně služeb.

VMware podporuje virtualizaci pro mnoho typů hardwaru a softwaru nevyjímaje oblasti pro uložení dat, sítě a zabezpečení. Aby byla virtualizace úspěšná, klade se důraz na zabezpečení a soulad s předpisy. Pro řešení virtuální sítě se využívají funkce, standardy a předpisy fyzické sítě. A virtualizace úložiště poskytuje vysoce výkonný přístup ke zdrojům sdíleného úložiště.

Příklady softwaru v CZUB:

- Výpočetní prostřední pracovních ploch a koncových uživatelů – VMware View, VMware Workstation atd.
- Správa infrastruktury a provozu – Management Suite, VMware center Server atd.
- Správa IT podniku – VMware Service Manager atd.
- Oblast zabezpečení – VMware vShield App atd.
- Správa aplikací – VMware Studio atd.
- VMware vSphere – v provozu, kde je větší počet serverů a jsou zde požadavky na větší spolehlivost.

9 ULOŽENÍ DAT

V této kapitole jsem se zaměřila na databázové systémy, zálohování dat, databázový stroj, SQL, DB2 a intranet portál.

9.1 Databázové systémy

Databáze jsou významné pro svou efektivnost, jednoduché uložení dat a rychlý přístup k nim. Je to softwarové vybavení, které zajišťuje práci s daty. Databázové systémy mají v CZUB následující vlastnosti:

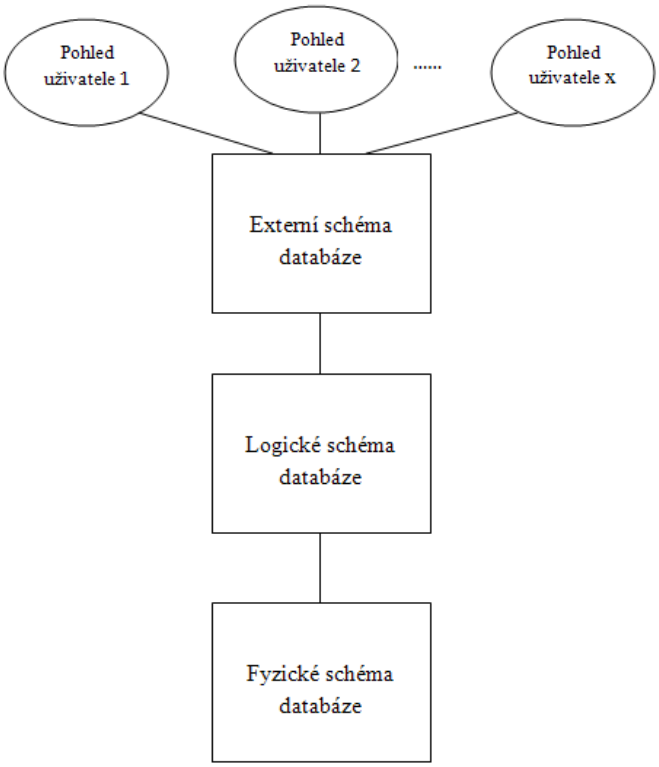
- Struktury datových souborů jsou odděleny od aplikačních programů
- Přístup k datům je jen prostřednictvím databáze
- Umožňuje přístup více uživatelů současně na úrovních čtení/zápis
- Snadné zálohování
- Transakční logy
- Rekonstrukce při zálohování

Data jsou uložena v centrálně zpracovávané struktuře dat – *databázi*. Centrální správa databáze je realizována pomocí programového vybavení, které se nazývá *systém řízení báze dat*. Tento systém zahrnuje:

- Prostředky pro popis dat, označovány jako jazyk typu DDL.
- Prostředky pro popis algoritmu, označovány jako jazyk typu DML. Používá se například pro aktualizaci dat nebo výběru dat z databáze.

Obrázek znázorňuje architekturu databázového systému složeného z následujících částí:

- **Externí úroveň** – představuje pohled uživatele na data. Představují je tiskové sestavy, formuláře pro vstup a výstup dat a jiná důležitá data, která obsahují informaci prospěšnou pro uživatele.
- **Konceptuální úroveň** – je integrovaný pohled celé databáze a často je označována za logické schéma databáze. Na jednom databázovém stroji může být instalováno více databází.
- **Interní úroveň** – představuje fyzické uložení dat a metody přístupů k nim a je označován jako fyzické schéma.



Obr. 20. Architektura databázového systému [vlastní zpracování]

Sdílení dat:

Data jsou sdílena všemi aplikačními programy, což má za následek snížení redundance a pozitivní vliv na celkovou itegrovanost informačního systému. Odpovědnost se přenesla z jednotlivých agend na databázový systém. Zde je předpoklad, že provoz má na starost pověřená osoba neboli *administrátor databáze*. Ten odpovídá za všechny úrovně v databázi.

Integrita:

Integrita neboli celistvost je stav databáze, kdy jsou data přístupná a využitelná v aplikačních programech a mezi hodnotami položek platí vztahy, které jsou stanoveny v databázi. Narušení integrity může způsobit technické vybavení nebo chyby v aplikačních programech. V případě ztráty integrity se použije kopie databáze k její obnově. Databáze je tedy vybavena nástrojem pro kopírování celé databáze nebo její části do záložního paměťového média (jsou zde velké nároky na rychlost komunikačních linek). Vzhledem k tomu, že bývá databáze rozsáhlá, je zde patrná náročnost kopírování. Proto kopírování nelze provádět často a využívá se tzv. žurnálová záložní paměť – zde se při každé změně dat v databázi zaznamenává stav menších oblastí před změnou a po změně (transakční logy).

9.2 Architektury databáze, zálohování dat a databázový stroj

Aplikační architektury databáze:

- **Jednovrstvá centralizovaná architektura –** je to architektura s použitím centrálního počítače. Na centrálním počítači je společně báze dat a systém řízení báze dat, zde dochází i k zpracování požadavků a vstupních dat. Terminál pouze zajišťuje komunikaci uživatele s centrálním počítačem a taky zobrazení požadavků. Výhodou je podpora víceuživatelského přístupu k datům a nevýhoda je velká časová prodleva zpracování. V CZUB se používá tato architektura pro speciální aplikace na počítačích. Jsou použity v menším měřítku.
- **Jednovrstvá architektura s lokální databází –** systém zde běží bez použití sdílení informací mezi více uživateli. Výhodou je zde rychlost, není potřeba DB server, není potřeba počítačová síť a nevýhoda spočívá v omezení množství dat. Tento typ architektury se v CZUB používá v malém měřítku.
- **Dvouvrstvá architektura –** je rozdělena do dvou skupin. První skupina se nazývá *File - Server*. Databáze je zde umístěna na serveru. Sdílení a poskytování dat je realizováno prostřednictvím sítě a systému řízení báze dat na počítačích uživatelů. Jsou zde velké nároky na kapacitu datových přenosů. A druhá skupina je *Klient – Server*. Zde systém řízení báze dat běží na serveru, kde je umístěna i databáze. Na počítačích uživatelů běží aplikace pro přijetí požadavků a zobrazení výsledků. Výhoda je snížení množství dat v síti a minimální zatížení sítě. V CZUB je to řídicí systém SAP apod.
- **Vícevrstvá architektura –** výkon je zde spojený s aplikačními službami na serveru a uživatel pracuje jen s uživatelským rozhraním. Datové a aplikační služby jsou rozděleny do samostatných celků. Tato architektura je třívrstvá. V CZUB je to systém SAP, WEB apod.

Zálohování dat databází:

Zálohování dat je velmi důležité pro minimalizaci ztráty dat. Zálohuje se v různých periodách a provádí se na přepisovatelná media, jako jsou pásky, magneto-optický disk, CD apod. Musí platit, že zálohování musí probíhat často, v době nejmenšího provozu – v noci a záloha se vytváří na externích médiích. Musí se uchovávat i historie provedených databázových operací, na to slouží *transakční log*. Zálohy jsou vždy uchovávány po určitou dobu v rámci dne až měsíců.

Databázový stroj:

Databázový server je počítač a v něm jsou uloženy databáze, které běží v databázovém stroji. To je aplikace, která pro klienty zpracovává veškerá data. Mezi nejznámější databázové stroje patří SQL, Oracle, Paradox apod. Může mít vyhrazený prostor na jedné z pracovních stanic nebo v databázovém serveru. Používá se spíš druhý případ a to z hlediska lepšího zpracování dat a zabezpečení. Zpracovává tedy dotazy na databázi od klientů, kteří mají k tomuto serveru přístup.

9.3 SQL a DB2

Ve firmě Česká Zbrojovka, a.s. jsou použity v databázi jazyk SQL a databázový systém DB2. V této kapitole jsou oba dva pojmy stručně popsány.

SQL:

Historie jazyka SQL se začala psát v letech 1970 a 1980. První standard byl přijat v roce 1986, který byl opraven v roce 1992 pod názvem SQL92. Tento standard je v oblasti relačních databází standardem dodnes. Jazyk obsahuje nástroje pro tvorbu databází – tabulek a nástroj pro manipulaci s daty – vkládání dat, aktualizace atd. Jazyk SQL patří do kategorie deklarativních programovacích jazyků. Rozumí se tomu, že se kód jazyka SQL nepíše v žádném samostatném programu, ale vkládá se do programovacího jazyka. Se samotným jazykem můžeme pracovat tak, že se terminálem připojíme na SQL server a do příkazového řádku zadáváme příkazy jazyka SQL.

SQL jazyk se skládá z částí určené pro administrátory a návrháře a pak pro koncové uživatele a programátory. Jazyk SQL se skládá ze čtyř částí. První část je jazyk *DDL*. Tento jazyk vytváří databázová schémata a katalogy. Druhá část je jazyk *SDL*, který definuje způsob ukládání tabulek. Třetí část je jazyk *VDL*, který používají návrháři a správci. Čtvrtou částí je jazyk *DML*, který obsahuje základní příkazy jako například select, insert, delete atd. Tyto příkazy využívají nejčastěji programátoři a koncoví uživatelé.

DB2:

DB2 je relační databázový systém od firmy IBM určený pro databázové aplikace s vysokými požadavky na spolehlivost a robustnost. DB2 je možné použít ve všech typech řešení včetně transakčních aplikací. Má nízké nároky na administraci a zajistí bezpečné uložení všech dat. Podporuje standardy a i platformy jako J2EE a Microsoft NET.

DB2 je rozdělen na 3 typy:

- **DB2 Personal Edition** – databázový systém pro jednoho uživatele nebo pro vývoj.
- **DB2 WorkGroup Edition** – víceuživatelský databázový systém navržený pro pracovní skupiny a oddělení podniku.
- **DB2 Enterprise Server Edition** – víceuživatelský databázový systém pro celopodnikové aplikace.

10 ZABEZPEČENÍ VZDÁLENÝCH A LOKÁLNÍCH KOMUNIKACÍ

10.1 VPN komunikace

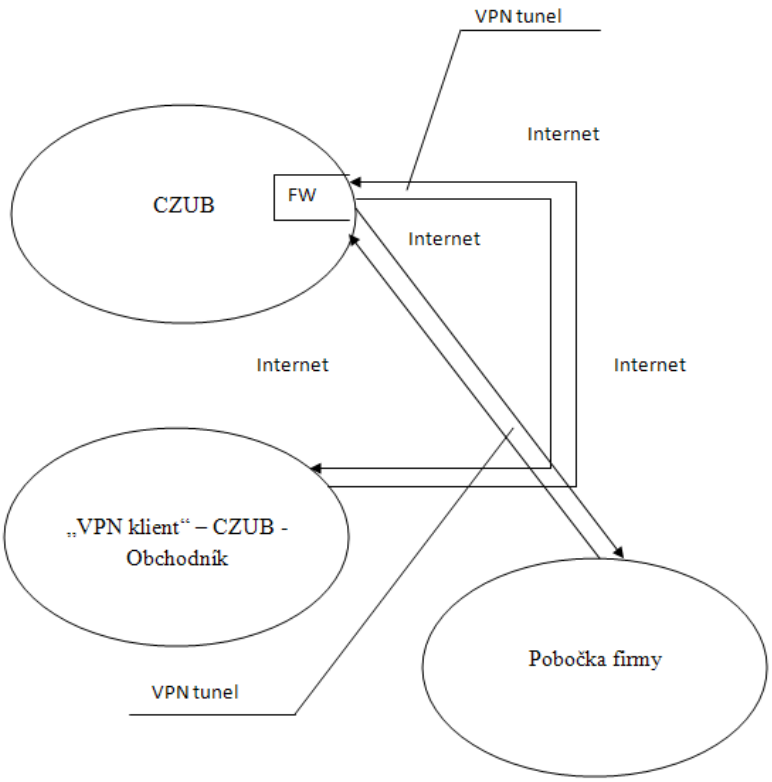
V CZUB je řešeno propojení informační struktury odlehlých pracovišť pomocí sítě VPN. Je to soukromá síť, která využívá veřejného propojení, nejčastěji Internetu, ke spojení vzdálených bodů a uživatelů. Vzdálení pracovníci firmy mají tímto způsobem zajištěný přístup k firemním serverům a intranetu. VPN taky spojuje pobočky firmy a tvoří extranety mezi důvěrnými partnery. Při navazování spojení je totožnost obou stran ověřována pomocí digitálních certifikátů a následně dojde k autentizaci. Veškerá komunikace je šifrována, proto se toto spojené považuje za bezpečné. K propojení ve firemní síti je zprovozněn VPN server, dále je zajištěno připojení k Internetu. VPN klienti se pak připojují pomocí Internetu z jakéhokoliv místa. V CZUB se používá k propojení vzdálených objektů Open VPN a Cisco VPN.

Remote – Access:

Tento typ sítě je navržen pro uživatele, kteří pracují z domu nebo jsou na cestách. Síť VPN se tedy využívá k uskutečnění vzdáleného přístupu na server ve firmě s použitím infrastruktury veřejné sítě, jako je Internet.

Site – to – Site:

- **VPN – uživatelé** – jsou ve firmě instalováni na notebooky a mají jednoduché pravidla.
- **VPN – pobočky** – mají definovány složitější pravidla a mají i vyšší nároky.



Obr. 21 Modelový příklad sítě VPN v CZUB [vlastní zpracování]

10.2 ERP

ERP je komplexní informační systém firmy CZUB, který zastřešuje informace související s výrobou, účetnictvím, dodavatelskými činnostmi, řízení lidských faktorů apod. Dokáže tak pokrýt veškeré potřeby firmy. ERP systémy integrují veškerá data a procesy firmy do jednoho celku. K tomu je zapotřebí množství softwarových a hardwarových modulů.

Implementace ERP systémů byla velmi nákladná, ovšem velmi důležitá. Všechny procesy se do ERP systému nadefinovaly tak, aby provádění těchto procesů bylo jednoduché, efektivní a provázané. Implementace měla následující postup:

- Definování ekonomické úrovni
- Programování
- Testování
- Přenos do reálného prostředí

Většinou jsou nainstalované tyto druhy systémů:

- Vývojový systém – zde jsou programátoři.
- Testovací/konsolidační systém – testují se zde kódy vytvořené ve vývojovém prostředí. Jednou za cca měsíc se provede obnovení do testovacího systému a zjišťuje se, zda systém funguje správně. Tuto činnost provádí konzultanti.
- Produkční systém – jsou zde ostrá data a naprogramované změny se aplikují jen v případě důkladného otestování. Zde pracují běžní zaměstnanci firmy.

Přínosy ERP systému:

- Zrychlení podnikových procesů
- Centralizace dat a snížení chybovosti
- Úspory v investicích do hardwaru a softwaru
- Zvýšení bezpečnosti
- Rychlejší výstupy pro vedení firmy

Vymezené pojmy:

Tenký klient:

Je počítačový program, který je závislý na serveru, na kterém běží všechny aplikace. Vyskytují se jako součást širší počítačové infrastruktury, kde více klientů sdílí své data se stejným serverem. Samotné klientské zařízení slouží pouze k zobrazování informací a k přenosu uživatelských vstupů zpět na server. To znamená, že veškerý software se většinou nachází na jednom systému a samotní uživatelé k němu přistupují z různých míst. Je tedy jedno, ze které stanice se přihlásí, vždy dostanou své nastavení, data, aplikace atd. Zvyšuje se zde bezpečnost z důvodu, že klienti nemohou instalovat vlastní programy. Z toho plyne, že je zde menší zátěž na počítače.

Tlustý klient:

V tomto případě je na straně serveru pouze služba, která zpracovává požadavky klienta do datového úložiště a obdržená data přeposílá zpátky na klienta. Tlustý klient bývá obvykle aplikace, kde je vyžadována instalace, nebo alespoň podpora spouštění aplikací ze vzdáleného počítače. Z toho plyne, že je zde větší zátěž na lokální počítače.

10.3 Tiskový systém – komunikace, zabezpečení

Pro tiskové řešení ve firmě je velmi důležité spojení těchto aspektů:

- Hardwaru – jde o multifunkční tiskárny nebo kopírky připojené do počítačové sítě.
- Softwaru – pro zabezpečení a sledování tisku, evidenci uživatelů atd.
- Služeb – zajišťují provoz systému jako je údržba, oprava atd.

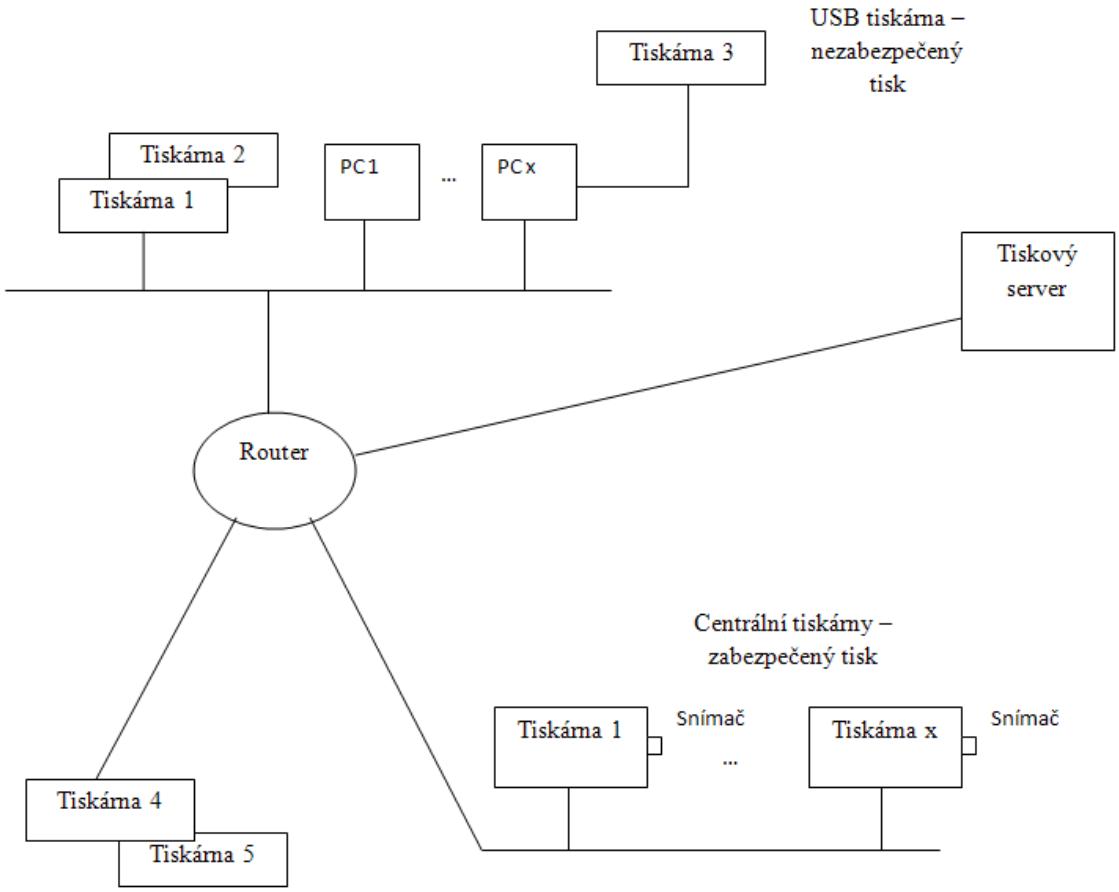
Tiskový server:

Tiskový server je zařízení, které propojuje tiskárnu s klientem prostřednictvím počítačové sítě. Může mít jednu nebo více sdílených tiskáren. Úkolem tiskového serveru je přijímat a zpracovávat požadavky k tisku, které uživatel zadává a následně je předává příslušné tiskárně. Tiskový server je i zařízení, které spojuje jednu nebo několik tiskáren v rámci LAN sítě. Propojení je realizováno RJ-45 konektorem, sériovým, paralelním portem nebo USB.

Bezpečný tisk:

Zajištění bezpečnosti tiskových dat ve firmě je velmi náročný proces. Základem ochrany přístupu k datům je najít, definovat nebo omezit zdroje tiskového provozu a komunikačních protokolů. Neopomíjí se zde ani na funkce bezpečného tisku v síťovém prostředí. To zaručí, že se k citlivým materiálům nedostane nepověřená osoba. Zabezpečení spočívá v tom, že k tisku dojde až poté, co uživatel identifikuje buď svým heslem na klávesnici multifunkčního zařízení, nebo identifikační kartou. Velmi důležitým článkem je i vzdálená správa bezpečnostních funkcí tiskových systémů a jejich integrace do firmy.

Rozlišujeme tedy zabezpečený tisk a veřejný (nechráněný) tisk. Z obrázku je patrné, že zabezpečený tisk je v rámci centrálních tiskáren, kde je použit snímač čipové karty. Oproti tomu nechráněný tisk je v případě, kdy nejsou použity výše zmiňované metody, a k tiskárně může přistoupit kdokoliv.



Obr. 22 Modelový příklad tiskového systému v CZUB [vlastní zpracování]

11 NÁVRHY ZLEPŠENÍ

V této kapitole provedu shrnutí slabých míst a navrhnu řešení pro jejich odstranění či částečnou eliminaci v CZUB.

Wi-Fi:

Bezdrátové připojení může zpříjemnit pracovní dobu nebo zjednodušit práci firmě, ale riskuje se tím ohrožení citlivých dat. Ve většině případů jsou bezdrátové firemní sítě nedostatečně zabezpečeny. A je to i znát na větším počtu krádeží dat z firem. Svědčí o tom i fakt, že se k bezdrátové síti může připojit člověk sedící v autě na parkovišti. Další riziková skupina je pracovní notebook, který zaměstnanci firmy mohou využívat pro práci z domova.

Pro zlepšení bezdrátového připojení bych navrhovala následující:

- Pro možnost omezení průniku signálu z míst, kde je Wi-Fi používáno dát speciální tapety, metalické barvy, pokovená skla nebo omezení dosahu signálu.
- Vice kontrol zaměstnanců, zda si nepořídili nový přístupový bod, který používají ze své kanceláře bez vědomí IT oddělení.
- Proškolení nezkušených zaměstnanců, aby nenarušili bezpečnost nevědomky.
- Přístupové body by měly být zabezpečeny všemi nejmodernějšími metodami.

Výměna switchů:

Switch, jakožto aktivní síťový prvek, který propojuje jednotlivé segmenty sítě, by měl být co nejlepším stavu. V CZUB se používají switchů jak staré, tak i nové. Staré switche jsou z řad 3COM 42xx a 3COM 45xx. Tyto typy switchů jsou zastaralé, tím pádem nespolehlivé, mají vysokou spotřebu, špatné chlazení a životnost je nižší než u nových. Z těchto důvodů bych volila postupnou výměnu switchů. Staré switche bych vyměnila za novější z řady HP.

Hlídání teploty:

Nedostatkem v serverových místnostech CZUB je hlídání teploty. Měl by být dohled teploty a vlhkosti v okolí serverů, diskových polí a podobně. Dohled teploty by měl být i uvnitř rozvaděče (RACK). Teplota by se měla hlídat nejen v serverových místnostech, ale i v dalších důležitých objektech. Pro větší bezpečnost bych navrhovala napojení těchto místností na PCO. Je to pul centrální ochrany. PCO nepřetržitě monitoruje sledované objekty, data jsou přenášena na dohledové centrum PCO, zde jsou vyhodnocena a pokud je

zjištěna odchylka od standardu, postupuje se podle smluvně dohodnuté reakce. Jako je výjezd hlídky nebo zásah odborného pracovníka.

UPS:

Jak jsem už zmínila v praktické části, jsou ve firmě použity paralelní UPS. Tyto UPS jsou výkonné a dostačující, ale existují i výkonnější UPS. Jsou to redundantní UPS. Tyhle UPS jsou tvořeny několika jednotkami UPS, tak aby se zvýšila spolehlivost zálohovacího systému. Dále bych navrhla zavedení motorgenerátoru pro hlavní serverovou místnost, kde jsou UPS. Motorgenerátor funguje jako záložní zdroj zpravidla pro dlouhodobější dodávky energie v rámci hodin až dnů. Může být vybaven i externí nádrží s automatickým přečerpáváním paliva a tím se umožní delší chod.

Upgrade Windows Serverů:

Jak již bylo zmíněno v praktické části, tak se ve firmě CZUB používají jak zastaralé operační systémy na serverech, tak novější. Vyřadila bych zastaralý operační systém Windows 2000/2003 Server a nahradila bych ho novým Windows 2008 Serverem. Tento operační systém vychází ze stejného kódu jako Windows Vista. Výhody jsou v přebudovaném síťovém modulu, který obsahuje IPv6, zvýšení rychlosti a bezpečnosti, lepší zálohování atd.

Stejně tak u operačních systémů na počítači bych vyřadila Windows 2000. Tento operační systém bych nahradila systémem Windows 7.

Cloud computing:

V CZUB zatím není reálně cloud computing. Proto bych do vylepšení zařadila právě tuto oblast. Pojem cloud computing lze charakterizovat jako poskytování služeb nebo programů uložených na severech na Internetu s tím, že uživatelé k nim mohou přistupovat například pomocí webového prohlížeče odkudkoliv.

Cloud computing poskytuje flexibilnější a efektivnější způsob jak vyhovět rostoucím požadavkům firmy. Představuje tedy nový model, který zjednodušuje IT tím, že efektivně pracuje s myšlenkou sdílené virtuální infrastruktury. Infrastruktura je dodávána na požádání, automaticky spravována a využívána jako služba. Výhody jsou optimalizované prostředí, které zvyšuje výrazně výkon IT – jsou využívány stávající prostředky, aby firma nemusela zbytečně investovat do infrastruktury, zajištění oprávnění pro koncové uživatele a současné zachování dohledu nad IT a pravomocemi, firma může nadále podporovat

stávající technologie a rozhoduje, zda je nasadí interně nebo externě, aniž by se omezovali na jednu technologii nebo dodavatele.

Jsou nabízeny tři úrovně přechodu na cloud:

- Infrastruktura a správa – základ pro cloud, založený na virtualizaci a možnost sjednoceni zdrojů veřejné a soukromé oblasti.
- Platforma aplikací pro cloud – umožňuje vývojářům vytvářet a spouštět aplikace pro cloud.
- Výpočetní prostředí koncových uživatelů – je zde poskytován zabezpečený přístup k aplikacím a datům z libovolného zařízení, kdekoliv a kdykoliv.

ZÁVĚR

Cílem diplomové práce byla analýza současného stavu bezpečnosti informačních technologií v oblasti zabezpečení dat a internetové komunikace, vytvoření struktury LAN a používaných operačních systémů na počítačích a serverech. Dále analýza uložení dat a zabezpečení vzdálených komunikací a v neposlední řadě shrnutí slabých míst a návrh pro jejich odstranění nebo částečnou eliminaci.

Práci jsem realizovala ve firmě Česká Zbrojovka, a.s., která je v současnosti jedním z největších světových producentů ručních palných zbraní. Původně byl podnik zaměřen na výrobu vojenských zbraní, ale později začal vyrábět i zbraně pro sportovní, lovecké i civilní využití.

Diplomová práce má dvě části s názvem teoretická a praktická část. V teoretické části jsem se věnovala významu informační bezpečnosti v současné době. Poté jsem důkladně popsala bezpečnostní politiku. Dále jsem se v teoretické části zabývala obecně strukturou LAN. Věnovala jsem pozornost základním pojmům, které jsou důležité pro pochopení následující problematiky, dále prvkům LAN a topologii sítí. Obecně jsou i popsány virtuální privátní sítě. V další části je popsána záloha a obnova dat, operační systémy na počítačích a serverech a velmi důležitá součást je i zabezpečení vzdálených komunikací. Praktická část je, jak už jsem zmínila zaměřena na konkrétní firmu. Zde jsem se hlavně soustředila na praktické pochopení problematiky z teoretické části. Dozvěděla jsem se, jak je uspořádána LAN struktura, jaké prvky se používají, jak jsou reálně udělané rozvody v budovách. Jaké se používají operační systémy. Praktické využití virtualizace, VLAN a firewallů a jeho výhody a nevýhody. Názorná ukázka databázových systémů a jejich využití. A v neposlední řadě jak funguje zabezpečení vzdálených a lokálních komunikací ve firmě.

Zdůraznila bych zde ještě, že vzhledem ke zveřejnění práce byly utajeny některé interní informace firmy.

Tato práce by mohla pomoc k řešení některých slabých míst ve firmě, nebo aspoň k jejich částečnému odstranění. Myslím si, že bylo dosaženo cíle, který byl stanoven na začátku.

ZÁVĚR V ANGLIČTINĚ

The aim of my dissertation is the analysis of present security situation in the information techlology in the field of data security and the internet comunication, the formation of the LAN structure and the operation systems used in computers and servers. There is also the analysis of saving data and protection of distant communication and last not least the summary of weak places and suggestion for their removal or partial elimination.
I realized my piece of work at Česká Zbrojovka, a.s., one of the biggest world producers of hand firearms. The company was originally focused on production of military arms but they have started to produce arms for sporting, hunting and also civil use later.
There are two part in my dissertation, the theoretical part and the practical part. In the theoretical part I dealt with the meaning of information security nowadays. Then I carefully described safety policy. I also generally concerned on structure of LAN. I payed attention to basic terms, that are important for understanding of the following issues and I was also concentrated on LAN elements and the net topology.
There are also generally described virtual private networks. In the next part, there is broadly depicted the backup and the data recovery, the operating systems on computers and servers and a very important part is the security of the distant communications. The practical part, as I mentioned, is directed at the particular company. In this place, I mainly concentrated on the practical understanding of issues from the theoretical part. I got to know about the organization of the LAN structure, what components are used, how the distribution system is in fact carried-out in the buildings, which operating systems are used, their advantages and disadvantages, practical application of virtualization, VLAN and firewalls. I also learnt about the database system, about its use and also how does work the security of distant and local communications in the company.
I would like to emphasize that due to the publishing my piece of work, some internal information was undisclosed.

This dissertation could be helpful in solving some weak places in the company or to remove some of their parts. I think target set at the beggining was reached.

SEZNAM POUŽITÉ LITERATURY

Monografická literatura:

[1] ČANDÍK, Marek. *Základy informační bezpečnosti*. Zlín: Univerzita Tomáše Bati, 2004, 107 s. ISBN 80-7318-218-1.

[2] DONAHUE, Gary A. *Kompletní průvodce síťového experta*. Brno: Computer Press, 2009, 528 s. ISBN 978-80-251-2247-1.

[3] THOMAS, Robert M. *Lokální počítačové sítě*. Praha: Computer Press, 1996, 277 s. ISBN 80-85896-45-1.

[4] STUCHLÝ, Vladimír. *Počítače a komunikace*. Praha 4: Computer Press, 1998. ISBN 80-85896-40-0

Elektronické zdroje:

[5] *Výzkum informačních technologií z hlediska bezpečnosti*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.fit.vutbr.cz/research/vzamer/np/>

[6] *Informace* [online]. 2008 [cit. 2012-05-01]. Dostupný z WWW: <http://www.inflow.cz/informace-veda-pravda>.

[7] *Bezpečnost v počítačové komunikaci*. [online]. 2007 [cit. 2012-05-01]. Dostupný z WWW:<http://www.linuxexpres.cz/praxe/bezpecnost-v-pocitacove-komunikaci>.

[8] *Komunikační a počítačová bezpečnost*. [online]. [cit. 2012-05-01]. Dostupný z WWW:<http://www.tsoft.cz/komunikacni-a-pocitacova-bezpecnost>.

[9] *Bezpečnostní politika organizace*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.aec.cz/download.php?f=cb947e6d14f1006e0aa1fa8571570ab3>.

[10] *Vybrané hrozby informační bezpečnosti organizace*. [online]. [cit. 2012-05-01]. Dostupný z WWW: < http://www.cybersecurity.cz/data/Pozar2.pdf>.

[11] *Jak fungují počítačové sítě*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://extrahardware.cnews.cz/jak-funguji-pocitacove-site-pro-zacatecniky>.

[12] *Základy PC: počítačové sítě snadno a rychle*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://pctuning.tyden.cz/navody/zaklady-stavba-pc/7543-zaklady_pc-pocitacove_site_snadno_a_rychle>.

[13] *Počítačové sítě - základní topologie*. [online]. [cit. 2012-05-01]. Dostupný z WWW:<http://www.samuraj-cz.com/clanek/pocitacove-site-zakladni-topologie/>.

[14] *Integrita*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.cleverandsmart.cz/integrita/>.

[15] *Model ISO/OSI*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://site.the.cz/index.php?id=4>.

[16] *Model TCP/IP*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.hardwaresecrets.com/article/433>.

[17] *Síťový model TCP/IP.* [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.earchiv.cz/a92/a231c110.php3>.

[18] *Aktivní síťové prvky - co jsou a k čemu slouží*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.earchiv.cz/a94/a438c500.php3?print=1>.

[19] *VLAN - historie a význam*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.svetsiti.cz/clanek.asp?cid=VLAN-1-historie-a-vyznam-242003>.

[20] *Operační systémy*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://drogo.fme.vutbr.cz/opory/pdf/uai/operacni_systemy/OS03.pdf>.

[21] *Co je server*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://svetserverov.sk/co-je-to-server/>.

[22] *VPN - pomocník (nejen) v bezpečnosti*. [online]. [cit. 2012-05-01]. Dostupný z WWW:<http://www.systemonline.cz/it-security/vpn-pomocnik-nejen-v-bezpecnosti.htm>.

[23] *Virtualizace.* [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.oldanygroup.cz/virtualizace-vmware-zakladni-informace-9/>.

[24] *Virtualizace v kostce*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.systemonline.cz/virtualizace/virtualizace-v-kostce.htm>.

[25] *Strukturované kabeláže*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.svetsiti.cz/clanek.asp?cid=Strukturovane-kabelaze-uvod-942001>.

[26] *Napájení.* [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.4-construction.com/cz/clanek/zdroje-neprerusovaneho-napajeni-ups/>.

[27] *Active Directory*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/>.

[28] *Proxy server*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.fi.muni.cz/~kas/p090/referaty/2003-jaro/skupina10/proxy.html>.

[29] *Antivirus.* [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://securityworld.cz/securityworld/antivirus-pro-celou-sit-1233>.

[30] *Virtualizace.* [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.vmware.com/cz/virtualization.html>.

[31] *Databáze.* [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.uai.fme.vutbr.cz/~mseda/DBS02_BS.pdf>.

[32] *Databáze a SQL*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://interval.cz/clanky/databaze-a-jazyk-sql/>.

[33] *DB2*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.notes.cz/NotesWebsite.nsf/20EAA2594B778EB9C1256F2B00437107/$File/DB2_Database%20Server(final).pdf>.

[34] *Databázový stroj*. [online]. [cit. 2012-05-01]. Dostupný z WWW: <http://www.levny-serverhosting.cz/databazovy-server.html>.

[35] *VPN řešení.* [online]. [cit. 2012-05-09]. Dostupný z WWW: <http://www.zyxel.cz/usg/studie/WP_VPN_reseni.pdf>.

[36] *Tenký a tlustý klient*. [online]. [cit. 2012-05-09]. Dostupný z WWW: <http://www.zive.cz/clanky/tenci-klienti--nahrada-za-kancelarska-pc/sc-3-a-130227/default.aspx>.

[37] *Zabezpečený tisk.* [online]. [cit. 2012-05-09]. Dostupný z WWW: <http://securityworld.cz/securityworld/zabezpeceny-tisk-ochrana-informaci-i-penezenek-973>.

[38] *Firemní zabezpečení Wi-Fi sítí*. In: [online]. [cit. 2012-05-09]. Dostupný z WWW: <http://www.internetprovsechny.cz/9-z-10-firemnich-wi-fi-siti-neni-dostatecne-zabezpeceno/>.

Ostatní zdroje:

[39] MAHDAL, P. *Analýza poskytovaných benefitů firmou Česká Zbrojovka, a.s.* UTB ve Zlíně, fakulta technologická, Bakalářská práce, Zlín 2009. 57s.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

IT	Informační Technologie.
IP	Internet Protocol – číslo, které jednoznačně identifikuje síťové rozhraní v počítačové síti.
LAN	Local Area Network – lokální síť.
TCP/IP	Transmission Control Protocol / Internet Protocol – síťový protokol.
BNC	Bayonet Neill–Concelman – druh konektorů, použitý pro koaxiální kabel.
ISO/OSI	International Organization for Standardization - Open Systems Interconnection – referenční komunikační model.
VLAN	Virtual Local Area Network – virtuální lokální síť.
MAC	Media Access Control – je jedinečný identifikátor síťového zařízení.
VTP	VLAN Trunking Protocol – Protokol pro VLAN.
DNS	Domain Name Systém – je hierarchický systém doménových jmen.
SMTP	Simple Mail Transfer Protocol – internetový protokol určený pro přenos elektronické pošty.
IMAP	Internet Message Access Protocol – je internetový protokol pro vzdálený přístup k emailové schránce.
POP3	Post Office Protocol 3 – je internetový protokol, který se používá pro stahování emailových zpráv.
VPN	Virtual Private Network – virtuální privátní síť.
RACK	Standardizovaný systém umožňující přehlednou montáž.
RJ45	Nejčastěji používaný typ zapojení síťových kabelů.
UPS	Uninterruptible Power Supply – zařízení nebo systém, který zajišťuje souvislou dodávku elektřiny pro zařízení, která nesmějí být neočekávaně vypnuta.
DC	Domain Controler – doménový řadič
AD	Active Directory – adresářová služba u Microsoft.

NTFS New Technology File Systém – označení pro souborový systém.

USB Universal Serial Bus – způsob připojení periférií k počítači.

CZUB Česká Zbrojovka Uherský Brod

UDP User Datagram Protocol – protokol ze sady protokolů internetu.

HTTP Hypertext Transfer Protocol – protokol určený pro výměnu hypertextových dokumentů ve formátu HTML.

FTP File Transfer Protocol – protokol pro přenos souborů.

DDL Data Definition Language – jazyk pro popis dat.

DML Data Manipulation Language – jazyk pro popis algoritmu.

SQL Structured Query Language – je standardizovaný dotazovací jazyk používaný pro práci s daty.

DB2 Databázový software.

UTP Unshielded twisted pair – nestíněná kroucená dvojlinka.

NTFS New Technology File Systém – souborový systém (organizace dat ve formě souborů, jsou například uloženy na pevném disku v počítači).

PC Personal Computer – osobní počítač.

ERP Enterprise Resource Planning – systém, který automatizuje množství procesů ve firmě.

IPv6 Internet Protocol version 6 – je internetový protokol.

PCO Pult Centrální Ochrany – ostraha objektů na dálku.

SEZNAM OBRÁZKŮ