Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Bakalářská práce

Návrh ICT infrastruktury zvolené organizace

Petr Kolařík

! ! !

Místo této strany vložíte zadání bakalářské práce.
(Do jedné vazby originál a do druhé kopii)

! ! !

Čestné prohlášení

Prohlašuji, že svou bakalářskou práci "Návrh ICT infrastruktury zvolené organizace" jsem vypracoval samostatně pod vedením vedoucího bakalářské práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené bakalářské práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne _____

Petr Kolařík

Poděkování

Rád bych touto cestou poděkoval Ing. Davidu Buchtelovi za konzultace problematiky zvolené práce a vstřícný přístup. Dále bych rád poděkoval JUDr. Pavlu Novákovi za konzultaci a možnost náhledu do interních procesů firmy.

Návrh ICT infrastruktury zvolené organizace

Design of ICT infrastructure in Chosen Company

Souhrn

Tato práce se zabývá problematikou ICT, konkrétně ICT infrastrukturou advokátní kanceláře. K objasnění problematiky bylo využito odborné literatury a internetových článků. Práce dále popisuje současný stav infrastruktury advokátní kanceláře a na základě SWOT analýzy vyhodnocuje nedostatky. Vlastní návrh pak vychází z příležitostí analýzy a snaží se o modernizaci a funkční zlepšení této infrastruktury. Závěrem je pak shrnuta celá práce, vypočítány orientační ceny navrhovaného řešení a popis oblastí návrhu, které se dočkaly realizace.

Summary

This work deals with ICT infrastructure of law office. To clarify the problems being used special literature and Internet articles. The work also describes the current state of infrastructure of law office based on SWOT analysis evaluates the shortcomings. Custom project is based on the analysis od opportunities and seek to modernize and improve the functional infrastructure. Finally, it summarizes the whole work, calculated the indicative price of the proposed solution and description of the projets which were implemented.

Klíčová slova: ICT, infrastruktura, hardware, software, ISO normy, síťové technologie, mobilní zařízení, bezpečnost

Keywords: ICT, infrastructure, hardware, software, ISO standards, network technologies, mobile device, security

Obsah

Seznam tabulek

1 Úvod

Informační a komunikační technologie jsou fenoménem současnosti. Neustálým vývojem a zdokonalováním, je získáván stále rychlejší tok informací, větší místo pro ukládání dat a mnohem kvalitnější komunikaci. Technika je dnes využita téměř v každé organizaci, bez rozdílu velikosti či zaměření. S těmito trendy však také přichází různá úskalí, například potřeba vybrat vhodné ICT řešení pro konkrétní organizaci.

V souvislosti s rychlým nárůstem moderních principů technologií v ICT také stoupá počet specializovaných firem zabývajících se touto problematikou. Jedná se zejména o poradenské společnosti, které zkoumají současný stav podniku a poté vyhotovují návrhy na vylepšení. Dále pak přibývá společností zabývající se tvorbou a implementací Informačních Systémů, webhostingem, serverhostingem, službami pro denní správu ICT a v neposlední řadě existuje nespočet organizací zabývajících se tvorbou webových prezentací a aplikací.

Bohužel společnost mnohdy podceňuje význam ICT a snaží se v tomto směru ušetřit. Někteří lidé si stále neuvědomují význam informací a sílu komunikace v běžném životě či podnikání. Mnohdy tyto technologie považují dokonce za samozřejmost a nepřemýšlí nad inovací současného řešení infrastruktury.

ICT je potřeba řešit neustále, podporovat core business procesy, obnovovat staré zařízení a systémy, protože správně navržená architektura šetří čas, peníze a usnadňuje každodenní práci.

2 Cíl práce a metodika

2.1 Cíl

Hlavní cíl práce je vymezen na základě pozorování současného stavu ICT architektury ve zvolené organizaci a to vytvoření návrhu ICT infrastruktury zkoumané organizace tak, aby odpovídala moderním současným principům a technologiím.

Dílčími cíly práce jsou příprava organizace na certifikace ISO, zejména splnit vybraná doporučení ISO. Dále pak obnova současné výpočetní techniky, zajištení efektivnější prezentace a poukázat na nedostatky stávající architektury.

2.2 Metodika

Pro zpracování práce bude provedena analýza sekundárních dat. Informace budou čerpány z odborných publikací a internetových zdrojů pro splnění cílů. Na základě získaných informací bude provedeno třídění dat a jejich zpracování.

V praktické části pro návrh infrastruktury bude vytvořen popis stávající architektury dané organizace a její vyhodnocení pomocí SWOT analýzy.

Na závěr pak bude vypočítána předpokládaná cena nové infrastruktury, bude popsáno, které části návrhu byly úspěšně realizovány, které byly zamítnuty a zhodnocena celá práce.

3 Přehled současných principů a technologií

ICT je velmi používaná odborná zkratka pro informační a komunikační technologie. ICT jak ho známe dnes vzniklo ze zkratky IT přidáním komunikací, když počítače začaly mezi sebou komunikovat.

3.1 Technické standardy a normy

ISO je zkratkou mezinárodní organizace pro normy „International Organization for Standartization“ sídlící v Ženevě, ve Švýcarsku.

3.1.1 ISO 9000 – jakost

ISO 9000 je souborem norem, anglicky se mnohdy uvádí, jako „ISO 9000 familly“.

„*Normy ISO řady 9000 byly přijaty v roce 1987 a v přibližně sedmiletých cyklech byly aktualizovány. Dále uvedený výklad vychází z tzv. velké revize schválené koncem roku 2000. Doporučení pro systém řízení jakosti jsou uvedena v několika normách ISO, přičemž každá z norem má jinou funkci*“ (Veber, 2007).

Označení 9000 pak doplňuje, že se jedná se o standardy jakosti systémů řízení. Normy ISO řady 9000 byly formulovány pro zkvalitnění systémů řízení u organizací různých velikostí a druhů, jak uvádí organizace ISO na své webové prezentaci. Dále uvádí, že velký význam je přikládán komunikaci mezi jednotlivými organizacemi, ať již tuzemskými či mezinárodními. Organizace musí splňovat příslušná kriteria, aby mohla být oceněna certifikátem ocenění řady ISO.

Tabulka 1: Specifikace a vývoj ISO norem

Norma	Specifikace
ISO 9000	Definuje elementární principy jakosti manažerských systémů.
ISO 9001	Používá se při samotném zavádění jakosti systému řízení. Jedná se o označení schopnosti poskytovat produkty, které splňují potřeby a očekávání zákazníků.
ISO 9004	Navazuje na normu 9001. Norma ISO 9004 je doporučena spíše, jako směrnice k neustálému zlepšování výkonu organizace. Lze použít společně s normou 9001, avšak není určena pro certifikační či smluvní účely.
ISO 19011	Poslední z norem řady 9000 hovoří o auditu systémů managementu kvality a environmentálního managementu.

Zdroj : (iso.org , 2011) [online]

3.1.2 ISO 20000 – provozování

Standardem ISO/IEC 20000 dle Voříška. ISO/IEC 20000 je prvním mezinárodním standardem pro management služeb v ICT, který vychází z normy BS 15000, která byla vyvinuta britskou skupinou BSI a zaměřuje se na zkvalitnění, snížení nákladů a zefektivnění u ICT procesů. Norma je rozdělena do dvou částí ISO 20000-1 a ISO 20000-2. První část normy uvádí požadavky na organizaci, která chce využívat certifikovaných norem. Ve druhé části norma pojednává o samotné implementaci do řídícího procesu obsahující doporučené postupy.

Pro tuto normu je dle Voříška (2008) typická následující struktura:

- Předmět normy;
- Všeobecné definice;
- Plánování a implementace managementu služeb;
- Požadavky na systém řízení;
- Plánování a provedení nových nebo změněných služeb;
- Procesy dodávky služeb;
- Procesy vztahů;
- Procesy řešení;
- Řídící procesy;
- Proces uvolnění.

Voříšek (2008) dále tvrdí, že je ISO 20000 alternativou pro standard ITIL „IT infrastrukture Library“, ze které také mnohdy vychází a je kompatibilní s normami řady ISO 9000 a ISO 27001.

3.1.3 ISO 27000 – informační bezpečnost

Poslední z řad norem ISO, kterými se tato práce zabývá, je řada 27000. Řada 27000 objasňuje postupy a směrnice pro systémy řízení v organizacích ICT a úzce se zaměřuje na bezpečnostní postupy v systémech řízení.

> Hodnocení systému řízení bezpečnosti informací je charakterizováno jako soustava organizačních a technických opatření, která zajišťují shromáždění a vyhodnocení informací o stavu bezpečnosti informací dle předem stanoveného rozsahu, jak popisují autoři Pour, Gála a Šedivá (2009).

Dle chrantesidata.cz (2010) v současnosti existuje mnoho technologií, které vyžadují uvědomění zaměstnanců o bezpečnostní politice podniku. Ať se již jedná o digitální podpisy, certifikáty pro přístup do zabezpečených částí interního systému, zabezpečené přihlášení na firemní účet nebo o zabezpečení dat samotných. Zaměstnanci organizace si často neuvědomují bezpečnostní rizika své práce. Proto je žádoucí implementace normy ISO 27000.

Po implementaci této normy má klient záruku, že jeho data budou zabezpečena dle metod nejlepší praxe (best practise). Navíc doporučuje pravidelné bezpečnostní kontroly, aby se zabránilo tzv. „bezpečnostním dírám“.

Dle iso.org (2011) obsahuje řada 27000 soubor dílčích částí (norem), které organizace ISO oficiálně nazývá „ISO 27000 family“. Tento soubor je v současné době nekompletní, jelikož je stále mnoho norem ve vývoji. Následuje tedy tabulkový přehled publikovaných norem a dále stručný výčet norem připravovaných.

Tabulka 2: Specifikace ISO/IEC a jejich vývoj

Norma	Specifikace
ISO/IEC 27000	Definuje přehled norem a terminologii.
ISO/IEC 27001	Tato norma určuje požadavky na řídící systém ICT, kterých je nutné dosáhnout pro certifikaci a které je nutné udržovat pro zachování dané certifikace. Vychází z britské normy BS7799 část 2.
ISO/IEC 27002	Norma 27002 poskytuje tzv. „best practise recommendation“. Jedná se o soubor nejlepších doporučení v oblasti zabezpečení, která byla ověřena v praxi. Bezpečnost daná normou 27002 je definována standardem CIA*.
ISO/IEC 27003	Norma určující směrnice pro implementaci zabezpečení do systému řízení ICT v organizaci. Norma se skládá z následujících částí: • Úvod • Rozsah • Všeobecné definice • Strukturu tohoto standardu • Schválení řídícími pracovníky pro zahájení projektu implementace systému řízení bezpečnosti informací (ISMS) • Definice rozsahu a politiky • Analýza vedení organizace • Posuzování rizik a plán jejich eliminace • Projektování systému řízení bezpečnosti informací

Norma	Specifikace
ISO/IEC 27004	Další z norem řady 27000 je norma 27004, která poskytuje organizacím doporučená opatření pro zefektivnění norem zabezpečení a tím i eliminaci rizik. Mezi tyto opatření patří například odpovědnost za řízení, analýza dat s pravidelným hlášením…
ISO/IEC 27005	Smyslem této normy je poskytnutí směrnic pro eliminaci bezpečnostních rizik v systému řízení a správy informací.
ISO/IEC 27006	Standard 27006 je normou, která klade požadavky na akreditované organizace, jež udělují certifikace v souladu s normou 27001. Norma se skládá z 10 částí: • Rámec působnosti • Normovaná doporučení • Terminologie a definice • Principy • Základní požadavky • Strukturální požadavky • Požadavky na zdroje • Požadavky na informace • Požadavky na proces • Požadavky na systém řízení pro udělení certifikace
ISO/IEC 27011	Tato norma je určena pro organizace s telekomunikačním zaměřením certifikovaných normou ISO 27002 a poskytuje pro ně specifický soubor doporučení.
ISO/IEC 27033-1	Norma zabývající se koncepcí zabezpečení sítě.
ISO/IEC 27799	Poslední s publikovaných norem řady 27000 je specifická norma 27799, která se zabývá zdravotnickými organizacemi a poskytuje jim směrnice k ochraně osobních a zdravotních údajů pacientů/klientů.

Zdroj : (iso.org, 2011) [online]

Stručný výčet připravovaných norem řady ISO 27000 dle organizace ISO (iso.org, 2011) [online]:

- ISO / IEC 27007 - Směrnice pro řízení bezpečnosti informačních systémů auditu (se zaměřením na systém řízení)
- ISO / IEC 27008 - Pokyny pro auditory o kontrolách ISMS
- ISO / IEC 27013 - Směrnice o integraci norem ISO / IEC 20000-1 a ISO / IEC 27001
- ČSN ISO / IEC 27014 - Informační bezpečnostní rámec řízení
- ČSN ISO / IEC 27015 - Pokyny pro zabezpečení systému řízení informací ve finančnictví a pojišťovnictví
- ISO / IEC 27031 - Směrnice udávající nutnou připravenost informačních a komunikačních technologií pro zajištění kontinuity provozu (v podstatě ICT kontinuity složka v řízení kontinuity podnikání)
- ISO / IEC 27032 - Směrnice pro kybernetické bezpečnosti
- ISO / IEC 27033 - IT bezpečnosti sítí, založena na ISO / IEC 18028:2006 (1. část je již vydávána)
- ISO / IEC 27034 - Směrnice pro zabezpečení aplikací
- ISO / IEC 27035 – Řízení bezpečnostních událostí
- ISO / IEC 27036 - Směrnice pro zabezpečení outsourcingu
- ISO / IEC 27037 - Pokyny pro identifikaci, sběr a / nebo získávání a uchovávání digitálních důkazů

3.1.4 CIA

CIA (Confidentiality, Integrity, Availability) neboli Důvěrnost, Integrita a Dostupnost.

Důvěrností rozumí Pour, Gála a Šedivá (2008) zabránění úniku dat a informací ve prospěch nepovolaných osob nebo systémů. Důvěrnost je důležitou součástí zabezpečení systémů ICT a to z důvodu ochrany osobních dat tak, aby se data nedostala do rukou třetí strany. Prosazování politiky důvěrnosti je docíleno pomocí šifrování přístupů a přenosů informací.

Pour, Gála a Šedivá (2008) dále definují integritu jako aktuálnost a úplnost dat. Data splňují integritu systému, pokud je zaručeno, že nemohou být změněna třetí osobou či nežádaným programem (virem). Integrita však může být narušena samotnými uživateli systému, kde mohou záměrně či omylem smazat nebo zásadně pozměnit důležitá data.

Posledním z trojice standardu CIA je Dostupnost. Dostupnost bývá většinou procentuálně vyjádřená hodnota, která vypovídá, s jakou pravděpodobností jsou data přístupná. Je třeba eliminovat veškeré nežádoucí vlivy, jako nestabilita serveru, bezpečnostní opatření proti útokům na systém a záložní zdroj energie, aby byla dostupnost dat pokud možno co nejvyšší pro autorizované subjekty, jak definují Pour, Gála a Šedivá (2008).

Dle Webera jsou jedním z největších rizik při udržení hladiny dostupnosti tzv. DoS útoky, které jsou doménou hackerů. DoS útoky jsou útoky, které zaplavují informační toky a tím brání přístupům do systému. Mohou mít různé podoby na základě odesílaných informací, tzv. paketů. Nejčastější z nich jsou útok jednoho paketu, kdy daný paket obsahuje všeobecně bezpečnostní chyby software systému a zneužije jich pro blokování dostupnosti. Druhým, vysoce používaným útokem, je více paketový útok. Tento způsob je doménou spíše skupin útočníků, kteří v jednu chvíli rozesílají velké množství požadavků na server, což vede k zahlcení serveru, mnohdy dokonce až k pádu, čímž je opět potlačena dostupnost.

3.2. Software

Software je nedílnou součástí všech složitějších elektronických zařízení a slouží k jejich bezprostřednímu ovládání. Jedná se o tzv. „programové vybavení“, které obsahuje soubor instrukcí, které koncový uživatel ovládá pomocí uživatelského rozhraní. Pro účely ICT infrastruktury podniku lze rozlišit 4 typy software a to operační systémy, databázový software, programové vybavení jednotlivých stanic a samotné aplikace.

3.2.1 Operační systémy

Operační systémy, zkratkou OS, jsou základním uživatelským nástrojem pro komunikaci se zařízením. Operační systémy lze rozdělit do několika skupin, dle typu zařízení a dle využití.

„Operační systém (OS, Operating System) je množina programů, která řídí všechny ostatní programy zpracované počítačem. Po spuštění počítače je jádro operačního systému – kernel zavedeno do vnitřní paměti počítače v průběhu procesu ‚bootování'" (Gála, Pour, Toman, 2006)

Dle Gály, Poura a Tomana (2006) pak lze definovat, že operační systém má 5 základních funkcí:

- Správní;
- Meziprocesovou ;
- Sprostředkovatelskou;
- Řídící;
- Komunikační.

Operační systémy existují pro různá složitější elektronická zařízení a mohou být rozděleny do 4 kategorií, dle Gály, Poura a Tomana (2006):

Tabulka 3: Přehled operačních systémů

Pracovní stanice	Server	Mobilní zařízení	Speciální
• Microsoft Windows (Verze: 2000, XP a 7) • Linux • MAC OS X.	• Microsoft Windows 2008 Server • MAC OS Server • Solaris • Red Hat Linux • Novell Netware • AIX • HP-UX	• Palm OS • Microsoft Windows Mobile • Symbian • Blackberry • Android • MAC OS X	• IOS Pro komunikační zařízení (routery/switche) • TRON – OS používaný ve spotřební elektronice • Nucleous RTOS – OS pro GPS zařízení

Zdroj : (Gála, Pour, Toman, 2006)

3.2.2 Databázový software

Pour, Gála a Šedivá (2009) tvrdí, že existují dva přístupy k uložení dat. Jsou to přístup tradiční (souborový) a přístup databázový. Autoři dále popisují tradiční přístup k ukládání dat jako hierarchii, kde nejvyšší úrovní je báze dat (anglicky database). Nížšími úrovněmi jsou pak soubor dat, záznam položka a znak. Při tradičním přístupu je tedy nutnost využívat souborového systému

"*Databázový přístup se vyvíjel a postupně vznikl model hierarchický, síťový, relační, objektově relační a objektový. V současné době je nejrozšířenějším modelem relační model databáze.*" Gála, Pour, Toman (2006)

Důvodem existence databází je dle Gilfillana (2003) potřeba neustále měnit data v informace a naopak. Dále tvrdí, že databáze je uložištěm faktů, které je navrženo dle potřeby.

Pro účely malých databází postačí software Microsoft Access. Pro větší databáze je pak mnoho dalších výrobků a produktů, až po ty největší producenty, jako jsou Oracle a SAP, kteří nabízejí řešení na míru velkým společnostem, jak tvrdí Schels (2007).

3.2.3 Programové vybavení pracovních stanic

Nebo také základní programové vybavení je software umožňující funkčnost programů z ostatních skupin.

Mezi základní programové vybavení pracovních stanic lze zařadit například balíček Microsoft Office, který v základní verzi obsahuje velmi využívané programy Word, který je dle Procházky (2011) využíván především pro psaní textu a hromadnou korespondenci.

Dalším užitečným programem v kancelářském balíku Office je dle Procházky (2011) Excel, který slouží, jako primitivní databázový software obsahující však výpočetní moduly pro lepší práci s čísly, dále pak Powerpoint, který je využíván pro

tvorbu a prezentování prezentací a v neposlední řadě Outlook, což je e-mailový klient se serverovými možnostmi.

Samozřejmě existuje nesčetně opensource alternativ k výše vypsanému vybavení, avšak je zde velké riziko nekompatibility v podobě rozhození formátu, špatné komunikace s produkty jiných značek např. OpenOffice, které popisuje Štědroň (2009).

3.2.4 Aplikace

Aplikace nebo také aplikační programové vybavení je software podporující chod podniku tím, že usnadňuje komunikaci, předávání a archiv informací a podporuje tak jednotlivé podnikové procesy.

Aplikace lze dle Poura, Gály a Šedivé (2009) rozdělit na 4 skupiny dle využití:

- Transakční aplikační software;
- Manažerský software podporující rozhodování při řízení;
- Aplikační software pro inovaci a rozvoj;
- Infrastrukturní aplikační software.

3.3 Hardware

Hardware se zabývá přehledem současného technického vybavení. Popisuje oblasti serverů, osobních počítačů, mobilních zařízení a kancelářských periférií.

3.3.1 Servery

Servery, nebo také služební počítače jsou centrálním mozkem síťové koncepce podniku. Obecně platí, že server je vysoce výkonný počítač či superpočítač, který je určen pro náročné výpočty. Mnohdy mívá organizace serveru i více, záleží na rozloze a rozsahu dané sítě, kde reagují na požadavky jednotlivých počítačů osobních, zpracovávají je a odesílají odpovědi.

Dle Poura, Gály a Tomana (2006) řadíme služební počítače do 3 hlavních typů:

- Midrange – je kategorie serverů, které mají uplatnění především v menších organizacích, které se skládají z menšího množství osobních počítačů;
- Mainframe – je serverovým řešením pro větší firmy a organizace;
- Supercompter – Superpočítač nachází využití zejména ve vědě a technice, kde slouží pro nejsložitější výpočty.

3.3.2 Osobní počítače

Osobní počítač je velmi rozšířeným pracovním nástrojem. V dnešní době se prakticky žádná firma bez počítače neobejde. Počítač je značným pomocníkem např. při správě dat, komunikaci, výpočtech.

Osobní počítače můžeme dle Gály, Poura a Tomana (2006) rozdělit do dvou skupin a to na přenosné (např. notebook, netbook) a nepřenosné.

a) Přenosný osobní počítač se vyznačuje tím, že obsahuje vše potřebné k chodu v rámci jednoho kusu, což v praxi znamená, že notebook má displej, klávesnici i myš řešenou formou touchpadu, jak tvrdí Gála, Pour a Toman (2006).

b) Oproti tomu počítač nepřenosný se skládá ze skříně tzv. case, ve které jsou uloženy všechny počítačové komponenty, kterými zpravidla bývá základní deska, procesor, grafická karta, zvuková karta, pevný disk, zdroj napětí a mechanika přehrávající multimédia, většinou DVD mechanika či čtečka karet. Nepřenosný osobní počítač však potřebuje ke svému plnohodnotnému používání ještě zařízení přídavná, tzv. periferie. Jedná se zejména o monitor, klávesnici a myš, jak tvrdí Gála, Pour a Toman (2006).

Výběr počítačové sestavy je dle Procházky (2011) stěžejní záležitost každé organizace. Na trhu existuje široká škála typů, proto je nutné si uvědomit, jaké využití bude požadovaná sestava mít. Dalším aspektem při výběru sestavy je její optimalizace. Optimální sestava je taková sestava, která má mezi sebou oficiálně kompatibilní komponenty a je do budoucna rozšiřitelná. Varianty sestav jsou optimalizovány pro 3 nejčetnější skupiny, jedná se o počítače kancelářské (tzv. office), výkonné (někdy uváděno multimediální) a herní. Počítače kancelářské jsou naprosto postačující pro většinu organizací, skvěle poslouží na kancelářskou práci. Druhým typem jsou sestavy výkonné, které nachází uplatnění především v oblastech s nutností větších výpočtů,

například společnosti pracující v programech CAD. Posledním, nicméně neopomenutelným typem jsou počítače herní. Herní se nazývají pro to, že jsou určeny především pro hráče počítačových her, které jsou samy o sobě velice náročné a vyžadují moderní a výkonný hardware. Nicméně využití tohoto druhu počítačů nejdeme i ve firmách, jedná se nejčastěji o firmy zabývající se tvorbou 3D efektů/modelů.

3.3.3 Mobilní zařízení

Mobilní zařízení se poslední dobou těší vysokému růstu popularity. Jedná se o přenosná zařízení, která se mnohdy svou technologií blíží osobním počítačům.
Procházka (2010) rozlišuje několik druhů mobilních zařízení:

- Mobilní telefony;
- Notebooky;
- Netbooky;
- Kapesní počítače.

3.3.4 Tiskárny, skenery, a jiné

Tiskárnou se rozumí výstupní zařízení, které slouží k přenesení digitálního obsahu na listinný. Existuje mnoho různých výrobců, jako nejvýznamnější výrobce lze uvést například Hewlett-Packard, Canon, či Epson. Tiskárny se dělí pak na lokální a síťové či laserové a inkoustové.

Rozdělení tiskáren podle Slowíka (2006):

a) Inkoustové tiskárny jsou v současné době velmi dostupné. Jejich ceny začínají okolo 800 Kč, čili jsou vhodné do domácností a menších firem. Inkoustový tisk však není velmi kvalitní, jelikož se jedná pouze o inkoust na papíře bez jakékoliv ochrany, čili se často stává, že se vytištěný dokument poškodí.

b) Laserové tiskárny jsou již mnohem kvalitnější, na rozdíl od inkoustové tiskárny, která obsahuje cartridge s inkoustem, laserová tiskárna využívá toner, který obsahuje prášek. Technologie tisku pak spočívá v „zažehlování“ prášku z toneru na papír, čili k jeho vyšší kvalitě a životnosti. Dříve byly laserové tiskárny výsadou pouze větších podniků, jelikož jejich cena astronomicky převyšovala ceny inkoustových tiskáren.

V současnosti se však tyto trendy, s narůstajícím počtem konkurence, továren a levnějších technologií, mění avšak stále zůstávají 2x až 3x dražší, než-li tiskárny inkoustové.

Dalším zařízením je skener, který dle Slowíka (2006) umožňuje naopak přenést listinnou podobu do podoby digitální pomocí snímače, který snímá vložený papír a převede jej do digitálního formátu, z pravidla PDF. Nejvýznamnějším kritériem při porovnávání kvality scanneru je jeho rozlišení, které se udává v jednotkách DPI (čím vyšší, tím lepší).

Slowík (2006) dále uvádí multifunkční zařízení, které je posledním z typů zařízení, které převádějí listinnou podobu na digitální a opačně. Toto zařízení se stává hitem, jelikož spojuje výše uvedené zařízení v jedno a doplňuje ještě o kopírku. Existují opět verze inkoustové a laserové, lišící se v kvalitě tisku a ceně.

3.4 Síťové technologie

Síťové technologie jsou z hlediska komunikace nepostradatelným prvkem. V souvislosti s tématem práce lze rozdělit technologie na WAN, LAN, Internet a Intranet.

3.4.1 Dle rozsahu

a) WAN

Technologie WAN (Wide Area Network) je dle Cafourka (2010) označení pro rozsáhlé nebo rozlehlé počítačové sítě, spojující více menších lokálních sítí LAN či jednotlivých uživatelů. Mnohdy jsou sítě WAN rozsáhlé v rámci celé země či dokonce kontinentu. Správu takovéto sítě již nezajišťují jednotlivci, nýbrž organizace či více organizací.

b) LAN

Místní síť (Local Area Network, LAN) „*je základním prostředkem propojení prvků sítě na podnikové úrovni a dnes je často využívána i v domácnostech. Někdy je taková síť pojmenována zkratkou SOHO (Small Office/Home office LAN)*“ Gála, Pour a Šedivá (2009).

Gála, Pour a Šedivá (2009) dále uvádějí, že dle topologie sítí je pro LAN typická stromová topologie, dle které jsou počítače v síti propojeny do tvaru stromu. Stromová topologie vychází z topologie hvězdicové a to spojením jednotlivých aktivních prvků, které jsou v centrech hvězd. Stromová topologie je využívána především ve větších počítačových sítích různých firem a organizací.

3.4.2 Dle využití

a) Internet

Procházka (2011) definuje Internet, jako nejrozsáhlejší počítačovou síť na světě, která dříve byla určena pouze pro vědecké a akademické pracovníky. V současné době internet používá většina populace a to nejen v podobě připojení z domova, ale také internet mobilní, který je díky moderním technologiím dostupný široké škále uživatelů.

Procházka (2010) dále tvrdí, že Internetová síť je v podstatě shluk menších počítačových sítí, kde jsou jednotlivé počítače identifikovány v souladu s protokolem TCP/IP.

Procházka (2010) popisuje, že Internet je významnou komunikační technologií spojující celý svět a díky tomu poskytuje perfektní možnosti k přenášení informací, marketing a služby, mezi které řadíme např. také e-mail, instant messengery a jiné.

Historie internetu sahá až do roku 1969, kde byl vývoj internetu započat a v průběhu let jej vědci a akademikové výrazně zlepšovali až do roku 1994, kdy se dostává internet na veřejnost, postupně se z něj stává komerční záležitost a v současnosti internet využívá několik miliard lidí po celém světě dle Procházky (2010).

b) Intranet

Intranet je výraz odvozený z angličtiny, jehož význam se překládá jako vnitřní síť. Procházka (2010) definuje intranet, jako privátní síť nacházející využití především ve společnostech a organizacích. Využívá stejných protokolů, jako internet.

„*Sítě intranet se běžně používají k ukládání interního obsahu, který se týká společnosti, například informace o zásadách společnosti nebo zaměstnaneckých výhodách. Jelikož je zabezpečení důsledně řízeno správcem, mohou být nastavení zabezpečení poněkud méně omezující než nastavení použitá pro obsah pocházející z internetu.*“ Procházka (2010)

Procházka (2010) dále tvrdí, že rozdíl mezi internetem a intranetem je dán především adresací, kde k internetu uživatel přistupuje pomocí domény, přičemž na síťi intranetu z pravidla domény nejsou. Na interní síti lze pak na rozdíl od internetu nastavit různá práva, což lze pro zónu internetu značně obtížně.

c) Extranet

Extranet je dle Gály, Poura a Tomana (2006) určen pro ekonomické subjekty. Tato síť je sítí kontrolovanou, řízenou a poskytuje cílený a vybraný zdroj informací.

3.5 Bezpečnost

Bezpečnost dat je důležitou součástí každé infrastruktury. Aby nedošlo ke ztrátě nebo zneužití dat, je třeba vytvořit bezpečnostní opatření.

3.5.1 Normy a předpisy

V podniku je třeba nejdříve stanovit normy a předpisy, které pokryjí celkovou bezpečnost ICT systému. Tyto normy většinou vychází z předem zpracovaného projektu. Daný projekt je poté zaveden do pracovního procesu formou různých směrnic, školení a nařízení.

Dalším krokem by mělo být nastavení určité kontroly těchto norem. Thomas (2005) uvádí, že adekvátním nástrojem pro podobnou kontrolu je sestavení týmu pro kontrolu zásad zabezpečení. Takový tým dělí Thomas (2005) na 5 pracovních skupin, ze kterých by mělo vzejít 5 zástupců, tj. jeden zástupce z každé skupiny. Skupiny lze tedy vyčlenit na: Vedení firmy, Oddělení bezpečnosti, Uživatelská sféra, Právní oddělení a Publikační skupina.

- Vedení firmy, které vydává nařízení o používání daných norem a předpisů
- Oddělení informační bezpečnosti pak zaujímá odbornou stránku týmu
- Uživatelská sféra je také jeden s důležitých zástupců v takovémto týmu, jelikož se jedná o zásady, se kterými se uživatelé potýkají denně.
- Právní oddělení zajišťuje kontrolu, zda-li zásady splňují právní normy
- Publikační skupina pak zastupuje informovanost jednotlivých zaměstnanců a způsob, jakým informovat.

3.5.3 Fyzická bezpečnost

Pro formulaci fyzické bezpečnosti lze vycházet z normy ČSN ISO/IEC 27001, dle které se fyzická bezpečnost člení na jednotlivé problémové oblasti. Tyto oblasti výborně popisuje článek na webovém portálu www.securityworld.cz, kde autoři Vít, Marek (2010) definují tyto oblasti:

„ Jsou to zaprvé zabezpečené oblasti, tedy v podstatě fyzická bezpečnost sídla, budovy a místnosti včetně oken a vstupních dveří, dále elektronické zabezpečovací a požární systémy. Je to ale i fyzické oddělení zařízení na zpracování informací od zařízení vlastněných někým jiným, dále kontrola vstupu do těchto zabezpečených oblastí nebo ochrana před vlivy požárů, povodní a výbuchů (tedy před katastrofami přírodními i těmi způsobenými lidskou činností). V neposlední řadě je to také řízení v prostorách, kam se mohou dostat neoprávněné osoby, nebo materiál (zásilky) od nich.
Zadruhé se jedná o záležitosti týkající se zařízení na zpracování informací, jejich správné umístění, dodávky potřebných služeb (jako jsou elektřina a plyn), dále o silové i telekomunikační rozvody, údržbu a bezpečnost mimo organizaci, když je zařízení na opravě, nebo když mají zaměstnanci notebooky a počítače doma. Důležitá je rovněž bezpečná likvidace informací ve všech formách, tedy dokumentů nebo paměťových médií, ale i postupy popisující odprodej nebo likvidaci zastaralých osobních počítačů nebo jejich přemisťování, tedy tvorba předávacích protokolů, inventur a povolení pro odvoz přes recepci či vrátnici.“ (Vik, Marek; 2010)

3.5.4 Řízení vstupů k datům a aplikacím

Data a aplikace jsou bezpečnostním rizikem každé organizace, proto je důležité řídit k nim přístup.

Toto řízení spočívá zejména v přímém omezení přístupu, které bývá většinou realizováno za pomocí uživatelských účtů, které jsou zabezpečeny hesly, různými firewally, místními zásadami zabezpečení a dalšími systémovými nástroji, které zabraňují přístupu k datům zvenčí. Tato opatření jsou zaváděna zejména proti útokům tzv. Hackerů.

Dle Harpera, Harrise, Eagla, Nesse a Lestera (2008) Hacker v IT terminologii označení pro útočníka, který se snaží o proniknutí k citlivým informacím či aplikacím. Nejdříve provede průzkum terénu, z kterého zjistí potřebné informace pro tzv.

„nabourání“ systému. Nejcitlivější oblasti v tomto procesu jsou přítomnost na internetu a vzdálený přístup. Platí zde přímá úměra, že čím méně je řízený přístup k datům, tím jednodušší je únik informací do rukou třetích osob.

4 Vlastní návrh ICT infrastruktury v podniku

Vlastní návrh má přispět k zefektivnění běhu společnosti. K realizaci bylo využito dostupné literatury a zaměstnání ve zvolené organizaci.

4.1 Současný stav

Důležitou částí návrhu infrastruktury bývá popis a zhodnocení současného stav. Zvolená organizace má již nějakou dobu vybudovánu infrastrukturu.

4.1.1 Problematika ICT v organizaci

Zvolenou organizací práce je advokátní kancelář, kde je kladen důraz především na shromažďování velmi velkého množství dat v podobě pohledávek, evidence případů a jejich procesních stavů. Organizace se zabývá mimo jiné vymáháním pohledávek. Součástí je specializované oddělení s názvem „Call Centrum“. Zde je potřeba vysoká procentuální dostupnost této služby v pracovní době. Další poskytovanou službou organizace je nonstop právní poradenství. Klienti mohou využívat několik druhů služeb počínaje telefonickým kontaktem formou nonstop linky, až po osobní kontakt s právním konzultantem.

Velmi závažnou problematikou, spjatou s „core businessem“ podnikání, je ochrana osobních údajů. Citlivé informace je nutno patřičně chránit odděleným přístupem pro jednotlivé zaměstnance.

4.1.2 Funkční architektura

Zvolená advokátní kancelář má funkční informační i telekomunikační architekturu.

Informační architektura je tvořena zejména ze 2 hlavních serverů, kde první z nich je určen pro informační systém Prométheus spadajícím do kategorie backend systémem. Druhý zastává funkci centrálního serveru a hromadného uložiště souborů.

Architektura je také tvořena 6 menšími servery, z nichž první server vykonává službu „pošťák“, zprostředkovanou pomocí e-mailového klienta. Druhý server slouží, jako informační středisko pro advokátní pracovníky. Ve středisku se nalézá soubor informací využitelných při soudních případech a kláních. Třetí server hostuje

encyklopedii celé advokátní kanceláře, která obsahuje zpětnou historii, evidenci případů a záznamy z jednání. Zbylé 3 servery jsou využívány pro archivaci starých a nepoužívaných spisů. Řešení menších serverů využívá službu správce vzdálené plochy.

V kanceláři se nachází 40 síťově propojených pracovních stanic, umístěných v doméně, přístupné pouze z vnitřní sítě. Architektura dále obsahuje přístupové bezpečnostní prvky např. uživatelské účty, kamerový systém napojený na bezpečnostní agenturu a přístupový systém na bázi čipových karet.

Součástí architektury je pak připojení VPN na bázi PPTP protokolu, využívané pro externí pracoviště a ve výjimečných případech pro práci z domova.

Telekomunikační část tvoří telefonní ústředna, ke které jsou připojeny všechny pevné telefony v budově. Pro externí hovory ústředna disponuje několika linkami.

Správu informačního systému provádí externí společnost. Druhá externí společnost zajišťuje správu interní sítě a telefonních linek.

4.1.3 Software

Nejvyužívanější softwarem kanceláře je operační systém pracovních stanic Microsoft Windows XP, který je využíván na všech osobních počítačích. S pracovními stanicemi pak souvisí další programové vybavení, které tvoří placený software např. Symantec anti-virus, kancelářský balík Microsoft Office 2003 a Microsoft Office 2007. Z neplacených tak zvaných „freeware“ aplikací např. PDF Creator, Mozilla firefox a RealVNC.

Organizace disponuje licencemi Microsoft Windows Server 2008, které doplňuje Microsoft Exchange Server. Software informačního systému poskytuje externí firma A posteriori, v rámci specializovaného systému pro advokátní kanceláře Prométheus.

4.1.4 Hardware

Hardwarové vybavení kanceláře je poměrně různorodé, servery jsou výkonnostně rozdílné dle využití. Nejvýkonnější server je nasazen pro informační systém Prométheus. Konfigurace serveru informačního systému je Intel Xeon E5620, který disponuje dvěma paměťovými moduly o velikosti 4GB RAM, pevným diskem SAS/SATA II v RAID poli a příkonem 675W / 2U. Druhý výkonný server je o

konfiguraci Intel Xeon Nocona 3,6 GHz, 8GB RAM, 1 TB pevný disk SATA II v RAID poli a příkonem 710 W.

Pracovní stanice lze rozdělit na tři generace:

- Intel Celeron 733 MHz, 80GB pevný disk, 256 MB DDR RAM (nejstarší),
- Intel Pentium IV 2,4 GHz, 150 GB pevný disk, 1 GB DDR RAM
- Intel Pentium Dual Core E2160, 100 GB pevný disk , 2 GB DDR2 RAM

4.1.5 Síťová infrastruktura

Firemní počítačová síť se skládá z vnitřní sítě definovanou doménou. Vnitřní síť obsahuje veškeré pracovní stanice nacházející se v sídle firmy, síťové disky (hromadné uložiště, operativní disk informačního systému). Síť je chráněna firewallem a výstupní webové stránky, tak zvané frontend systémy, jsou umístěny v demilitarizované zóně.

4.1.6 Související interní předpisy

Interní předpisy jsou v souladu s prioritou zabezpečení dat. Každý pracovník má své přihlašovací údaje do počítače a informačního systému. Fyzický přístup do budovy je pak řízen čipovou kartou, unikátní pro každého zaměstnance. Zaměstnanci jsou smluvně vázáni k mlčenlivosti a neposkytování dat třetím osobám.

4.1.7 Hodnocení současného stavu infrastruktury

Ke zhodnocení současného stavu ICT bylo použito SWOT analýzy, jak uvádí tabulka č.3.

Tabulka 4: SWOT analýza

Silné stránky	Slabé stránky
• Systém pro správu pohledávek • Rychlost zpracování dat • Call Centrum	• Ztráta dat • Nedostatečná záloha • Zatěžování sítě a pracovních stanic v důsledku monitoringu pracovních ploch • Nejednotnost evidence advokátních případů • Strohá webová prezentace • Přetížení ústředny • Nízká garance dostupnosti služeb • Absence evidence VPN přístupů
Příležitosti	**Hrozby**
• Externí záloha • Zajištění propustnosti sítě • Zrychlit reakční dobu při ICT poruše • Evidence VPN přístupů • Vytvoření manažerského informačního systému • Pověření pracovníků k využívání osobně přiděleného digitálního podpisu	• Ztráta dat • Ztráta klientů • Zneužití digitálního podpisu • Odcizení dat

Zdroj: (vlastní, 2011)

4.2 Vlastní návrh

Návrh eliminuje hrozby a rizika ve výše uvedené SWOT analýze. Jak organizačními (procesními) opatřeními a technickými prostředky. Návrh je v souladu se standardy mezinárodních norem ISO 9000, ISO 20000 a ISO 27000. Pro zvolenou organizaci je přechod na tyto normy velmi důležitý pro udržení současné klientely a získání klientely nové.

4.2.1 Organizační opatření

Dle výše uvedených ISO norem návrh počítá s přípravou pro budoucí cetifikaci. S certifikací je spojeno dodržení doporučení těchto norem. Proces certifikace dle ISO norem je časově velmi náročná operace. Pro účely práce bylo vyčleněno několik níže uvedených opatření opírajících se o normy ISO 20000 a ISO 27000:

a) Pokrytí smlouvy s dodavateli, subdodavateli: Zde je třeba striktně definovat procesy související s dodavateli a subdodavateli.
b) Rozšíření interních předpisů: Jelikož jsou procesy zpracovávání a uchovávání dat advokátní kanceláře závislé na ICT technologiích, je nutnost rozšířit Interní předpisy a směrnice pro core business procesy i na ICT oblast. Vedení musí tyto směrnice striktně popsat a vyžadovat jejich dodržování.
c) Smlouvy s poskytovateli a dodavateli ICT služeb a komponent: Problematika správy a zpracování choulostivých dat vyžaduje smluvní garanci ze strany externích poskytovatelů a dodavatelů. Součástí tohoto návrhu je tedy smluvní závazek obsahující mlčenlivost a ochranu proti zneužití dat.
d) SLA parametry vyhodnocování (monitoring): Externí společnosti Dator 3 a Aposteriori jsou smluvními partnery advokátní kanceláře v oblasti ICT služeb a dodávání komponent. Je však nezbytné rozšířit tyto smlouvy o normované reakční doby. Reakční doba je doba, za kterou je společnost povinna odstranit vzniklý, řádně reportovaný, problém. Dále je nutnost vést přehlednou evidenci služeb help desk, service desk a dodávání komponent. Nedodržení výše zmíněných návrhů bude sankciováno dle upravených smluvních podmínek, což zajistí plnění normy ISO 20000.
e) Sledování průběhu odstranění závady: Další z úskalí outourcingu je řešení závady externí firmou. Vhodným nástrojem pro monitoring této činnosti je incident management, který sleduje průběh za pomocí písemné dokumentace, případně doplňkově pomocí kamerového systému či výpisu logů.
f) Zásada čtyř očí pro jednotlivé vrstvy ICT infrastruktury: Zásadou čtyř očí je řešena problematika vzájemného kontrolování. Potřebná je kontrola veškerých vrstev dané infrastruktury kontrolorem či řídícím pracovníkem. Pro tuto zásadu je důležité, že kontrolní pracovník musí kontrolovat práci jiného pracovníka, nikoliv svoji.
g) Zajištění kontinuity: Procesem kontinuity je myšlena záruka doby obnovy. Subjekt

této práce nemá proces zajištění kontinuity definovaný. Záruku doby obnovy je nutno, z hlediska organizačního opatření, definovat směrnicí. Vzhledem k finančním ztrátám z neočekávané situace je důrazně doporučeno určit dobu obnovy, co nejkratší v řádu několika hodin či dnů, v závislosti na rozsahu této údálosti.

4.2.2 Technické opatření

a) Vyhodnocování logů: Každý ICT proces v organizaci je nutné logovat. S logováním procesů úzce souvisí jejich vyhodnocování. Vyhodnocením se rozumí pravidelná kontrola a následné vyvození důsledků.
b) Fyzická bezpečnost: Při práci s citlivými daty na osobní údaje a daty na kterých závisí chod firmy je nutné dodržovat bezpečnostní předpisy. Co se týče fyzické bezpečnosti, jedná se zejména o řízení vstupů do budovy. Advokátní kancelář však postrádá řízení přístupu do serverovny. Jelikož má organizace řízený fyzický přístup do budovy na bázi čipových karet, návrhem je rozšíření využití čipových karet také do serverovny. Tímto řešením získá zaměstnavatel evidenci přístupů a spolu s kamerovým systémem úplný přehled o veškerých úkonech.
c) Uživatelské účty: Uživatelské účty jsou nezbytnou součástí bezpečnosti vnitřní sítě podniku. V souvislosti s touto problematikou bylo navrženo využití cestovních profilů. Toto opatření by mělo zabránit sdílení uživatelských účtů mezi pracovníky, kteří již profil na daném PC mají nastaven.
d) Interval obměny hesel: Důležitou součástí technického opatření je obměna hesel uživatelských účtů. Politika advokátní kanceláře je nastavena na obměnu hesla jednou za 2 měsíce. Vzhledem k citlivosti dat je navrhováno zkrátit tuto lhůtu na 1 měsíc. Dalším aspektem je obměna hesel u informačního systému, který tento proces nemá nastaven. Návrhem tedy je nastavit proces obměny hesel také u informačního systému.
e) Zálohování: Proces zálohování je nejdůležitějším zabezpečením proti ztrátě dat. Současný způsob zálohování je dle ISO norem nedostačujícím. V současné době zálohování probíhá pouze v rámci budovy, kde jsou uchovávány jak servery, kde je aktuální záloha, tak externí disky, které se fyzicky nacházejí o patro výše. Návrh počítá s riziky vyhoření budovy či krádeže, proto bylo kanceláři důrazně doporučeno využití zálohy uchovávané mimo budovu. V návrhu byla zvolena

společnost Casablanca INT, která uvádí následující opatření:

- non-stop fyzická ostraha
- evidence vstupu čipovými kartami
- kamerový systém
- uzamykatelné stojany a boxy
- systém EPS
- protipožární ochrana
- stabilní hasící zařízení: systém Fogtec, tj. vysokotlaká mlha –demineralizovaná, nevodivá

Zdroj: casablanca.cz [online]

Hlavní výhodou této služby je smluvně garantovaná záloha dat mimo budovu advokátní kanceláře.

f) Archivace: Současný proces archivace je nedostatečný. Data jsou archivována pouze jeden týden na externích discích, které jsou týdnem následujícím přepsány. Návrh počítá s kompletní archivací dat dle následujícího schématu.
   - Denní archivace: Každý den je zabalen do archivu dle data
   - Týdenní archivace: Jednotlivé dny jsou zabaleny do archivu s číslem týdne
   - Měsíční archivace: Všechny týdny daného měsíce jsou archivovány pod příslušný měsíc v roce.
   - Roční archivace: Všech 12 měsíců je archivováno do uplynulého roku
g) Skartace: Skartací dat je myšlena kompletní likvidace dat. Je důležité si uvědomit, že tento proces je nevratný. Proto je nutné si pod tímto pojmem představit výmaz dat nejen ze současné databáze, ale také ze záloh a archivů. Organizaci bylo doporučeno tento proces řídit a pravidelně kontrolovat. Správným nastavením řídícího procesu a důkladným proškolením všech delegovaných osob lze eliminovat ztráty způsobené neodborným zásahem.
h) Zajištění kontinuity: Záruka obnovy se týká také technického opatření. V této oblasti

4.2.3 Software

V souvislosti s návrhem nového hardware bylo navrženo dokoupení šesti OEM licencí Microsoft Windows XP. OEM licence se vztahuje pouze na jeden počítač a vzhledem k množství počítačů v organizace je ekonomicky výhodnější.

Druhou částí návrhu softwarového řešení je pořízení Manažerského Informačního Systému (zkráceně MIS). MIS řeší otázku bezpečnosti z hlediska omezeného přístupu k informacím na bázi uživatelských účtů zabezpečených hesly. Hlavním přínosem tohoto řešení bude dostupnost informací pro vedení společnosti na jednom místě, logování změn dat a možnost předem definovaných exportů. Volba MIS je doporučena realizovat výběrovým řízením. V součinnosti s vítězem výběrového řízení by měl být zřízen speciální tým konzultantů ze strany advokátní kanceláře, který bude mít realizaci projektu MIS jako hlavní pracovní náplň. Kanceláři bylo doporučeno obsadit tento tým lidmi z různých oblastí činnosti společnosti a jednoho vedoucího delegovaného k řídícím úkonům spojených s návrhem a následnou implementací.

Návrh počítá s využitím uvnitř i vně společnosti, proto je třeba definovat jaká data budou zpřístupněny zvenčí a jaká pouze z vnitřní sítě. MIS je primárně backend systémem. Nutností je využít zabezpečeného kanálu pro výstup mimo vnitřní síť. Řešení výstupu lze provést pomocí šifrování SSL protokolu HTTPS.

Technologickou část by tvořila kombinace programových jazyků HTML, PHP, JavaScript a AJAX. Navrhovaným databázovým řešením je pak produkt společnosti Oracle využívající technologii SQL, která je v současnosti nejpoužívanějším řešením v kombinaci s výše zmíněnými jazyky.

Po úspěšném vytvoření MIS je třeba zajistit pozvolnou implementaci do chodu společnosti. Proces implementace musí doprovázet procesy testování systému a odstraňování dílčích nedostatků. V případě úspěšné implementace musí zaměstnavatel zajistit příslušné školení pro práci se systémem. Dalším aspektem zavedení do ostrého provozu je definice směrnic pro zaměstnance tvořící obsah systému.

4.2.4 Hardware

Hardware zvolené organizace je velmi různorodý. Nachází se zde několik generací počítačů. Hlavním cílem je obměnit nejstarší generaci, která je již 6 let stará a vykazuje značně nevyrovnané a nedostatečné výkony. Podniku bylo navrženo zakoupení 5ti počítačových sestav od firmy Hawlett Packard, konkrétně se jedná o typ

HP Compaq 500B MT, Intel E5700, jehož hodnota činí 5199 Kč bez DPH a které nahradí onu nejstarší generaci.

Konfigurace navrhovaného PC (heureka.cz ,2011) [online]:

- Počet jader: dvoujádrový procesor
- Výrobce procesoru: INTEL
- Typ procesoru: Core 2 Duo
- Označení procesoru: E5700
- Frekvence procesoru (MHz): 3000
- Provedení počítače: micro provedení
- Typ paměti: DDR3
- Velikost paměti RAM: 4GB
- Typ pevného disku: HDD
- Kapacita pevného disku (GB): 750
- Otáčky pevného disku (ot/min): 7200
- Typ optické mechaniky : DVD±R/RW
- Typ grafické karty: nesdílená paměť
- Model grafické karty: ATI Radeon 5450
- Zvuková karta: ANO
- Čtečka paměťových karet : NE
- DVI výstup: ANO
- Operační systém : BEZ OS

Tento počítač byl zvolen hned z několika důvodů. Prvním důvodem je poměr cena/výkon, kde dvoujádrový procesor spolu se 4GB operační paměti zajišťují velmi dobrý výkon pro kancelářské aplikace.

Druhým důvodem je grafická karta ATI Radeon 5450. Grafická karta byla nutná pro připojení dvou monitorů.

Třetím důvodem byla absence operačního systému. Toto bylo nutné, protože obchodní řetězce distribuují počítačové sestavy pouze s operačním systémem Microsoft Windows 7. Vnitřní politika advokátní kanceláře je však nastavena na prostředí operačního systému Microsoft Windows XP.

Dále bylo doporučeno nakoupit 5ks externích pevných disků WESTERN DIGITAL My Book Essential 1000GB v hodnotě 2000 Kč pro potřeby zálohování dat. Na základě zpracovaného návrhu na zálohování byla navržena záloha každý pracovní den na jiný pevný disk.

4.2.5 Informační kanály

Informační kanály jsou důležitou součástí každé společnosti. Při řešení problematiky informačních kanálů bylo ve SWOT analýze uvedeno, že advokátní kancelář ani oddělená služba nonstop právní poradny nemají vhodně řešené podávání informací klientům. V souvislosti s tímto zjištěním byl návrh prezentace rozdělen do následujících čtyř bodů:

a) Webová prezentace advokátní kanceláře

   Důležitým informačním kanálem společnosti je webová prezentace. Pro advokátní kancelář toto platí dvojnásob, jelikož cílem je získávání klientely. Navrženo bylo vypracování jednoduché prezentace za použití technologií HTML a CSS. Advokátní kancelář již delší dobu používá vlastní grafické logo a barvy. Proto webová prezentace tyto grafické prvky převezme. Při jednání o nové podobě prezentace s majitelem advokátní kanceláře bylo vysloveno přání vytvořit jednoduché intro v podobě animace. Na toto přání bylo doporučeno využít technologie Adobe Flash.

b) Webová prezentace právní nonstop služby

   Jak bylo výše uvedeno, advokátní kancelář se také zabývá právním poradenstvím, které se oficiálně prezentuje, jako jiná společnost. Pro tuto společnost byl touto prací vytvořen návrh složitější webové stránky s vlastním redakčním a platebním systémem. V tomto případě se návrh opíral taktéž o technologie HTML a CSS, ke kterým byl přidán značkovací jazyk PHP a databáze MySQL. Pro platební systém byl vznesen návrh na použití 3D secure payment, který vyniká svou bezpečností při platbách kartou na internetu.

c) Facebook

   Facebook je fenoménem současnosti, ale také velmi mocným marketingovým nástrojem a informačním kanálem. V souladu s požadavky advokátní kanceláře byl vypracován návrh založit fanouškovskou facebook stránku, která bude pouze pro nonstop právní služby. Dále bylo doporučeno propojení facebook stránky

s webovými stránkami, což zajistí rozhraní vytvořené vývojáři Facebooku.

d) Infolinka

Posledním doporučením z hlediska informačních kanálů je zřízení telefonní infolinky zdarma, která by byla z větší části obsluhována automatem. Odbornější dotazy by pak byly přepojovány na operátora. Toto řešení je žádoucí z důvodu obrovského množství telefonních čísel, které kancelář již má zřízeno. Bohužel není srozumitelné, které číslo slouží pro jakou službu. Tento rozcestník by velmi ulehčil přetížení telefonních linek.

4.3 Realizace

4.3.1 Orientační cena

Níže uvedená tabulka číslo 4 reprezentuje orientační ceny jednotlivých položek návrhu, v kolonce produkt je uveden obecný název, v kolonce cena je uvedena orientační cena za všechny kusy jednotlivé položky a v kolonce počet je doporučený počet k zakoupení.

Tabulka 5: Orientační ceník

Produkt	Cena	Počet
Počítačové sestavy	25995 Kč	5
Operační systém	7495 Kč	5
Externí HDD	10000 Kč	5
Webové stránky	40000 Kč	2
MIS včetně realizačního týmu	500000Kč	1
Virtuální server	36000 Kč / rok	1
Příprava na ISO	50000 Kč	1

4.3.2 Skutečné nasazení

Advokátní kanceláři byl předložen tento návrh a na základě tohoto návrhu byly vybrané doporučení realizovány. Byly nakoupeny počítačové sestavy pro modernizaci výpočetní techniky spolu s operačními systémy.

Dalším úspěchem návrhu bylo zakoupení externích pevných disků pro potřeby lokální zálohy, čímž se organizace mírně přiblížila implementaci norem ISO.

Realizace webových stránek byla bohužel pouze částečná a to pouze pro službu nonstop právních rad. Webová prezentace pro advokátní kancelář je stále v jednání.

Manažerský Informační Systém a virtuální server byl prozatím z důvodu vysoké investice zamítnut, nicméně věřím, že v budoucnu bude ještě probírán.

5 Závěr

Cílem práce bylo seznámit se s problematikou ICT, konkrétně navrhováním infrastruktury zvolené organizace.

Postup byl založen na základě odborné literatury, ze které bylo vyčleněny nejdůležitější poznatky týkající se mého téma. Pro získání přehledu o aktuálních principech a technologiích bylo využito aktuálních internetových článků souvisejících s tématem. Z důvodu existence funkční architektury byl započat přínos zkoumáním současného stavu infrastruktury z pozice praktikanta ve zvolené organizaci. Praxí bylo získáno dostatečné informace pro popis stávajícího stavu a na základě SWOT analýzy jsem tento stav byl zhodnocen.

Zhodnocení stavu ukázalo, že stávající architektura je již nevyhovující a neodpovídá současným trendům a technologiím. ICT infrastruktura projevovala nedostatky především ve stáří některé výpočetní techniky, která se ukázala být více jak 5 let stará. Dalšími vážnými nedostatky byly určeny nízká podpora doporučení norem ISO a téměř úplná absence informačních kanálů.

Řešení stěžejních problémů bylo vypracováno do vlastního návrhu, kterým pokračoval můj odborný výzkum. Prvním krokem byla obnova staré výpočetní techniky, která již nezvládala novější infrastrukturu. Druhým krokem pak byla objednávka doporučených webových prezentací a zřízení facebook stránky.

Advokátní kancelář poměrně vstřícně přijala tyto návrhy a tím zkvalitnila svoji infrastrukturu. Hlavním úspěchem práce vidím přiblížení se několika částem norem ISO. Věřím, že v budoucnu se podaří prosadit více doporučení odpovídajících zejména normám ISO 20000 a 27000 a zajistit tak certifikaci. Certifikace by pro kancelář mohla znamenat znatelný nárůst klientely a minimalizaci hrozících ztrát.

6 Seznam použitých zdrojů

Tištěné dokumenty:

CAFOUREK, Bohdan. *Windows 7 : kompletní příručka*. Praha : Grada Publishing, 2010. 336 s. ISBN 978-80-247-3209-1.

GÁLA, Libor; POUR, Jan; TOMAN, Prokop. *Podniková informatika : počítačové aplikace v podnikové a medzipodnikové praxi, technologie informačních systémů, řízení a rozvoj podnikové informatiky*. Praha : Grada Publishing, 2006. 482 s. ISBN 80-247-1278-4.

GILFILLAN, Ian. *Myslíme v MySQL 4 : knihovna programátora*. Praha : Grada Publishing, 2003. 752 s. ISBN 80-247-0661-X.

HARPER, Allen, et al. *Hacking : manuál hackera*. Praha : Grada Publishing, 2008. 400 s. ISBN 978-80-247-1346-5.

POUR, Jan; GÁLA, Libor; ŠEDIVÁ, Zuzana. *Podniková informatika*. 2., přepracované a aktualizované vydání. Praha : Grada Publishing, 2009. 496 s. ISBN 978-80247-2615-1.

PROCHÁZKA, David. *První kroky s internetem*. 3., aktualizované vydání. Praha : Grada Publishing, 2010. 108 s. ISBN 978-80-247-3255-8.

PROCHÁZKA, David. *Nebojte se počítače : pro Windows 7 a Office 2010*. Praha : Grada Publishing, 2011. 128 s. ISBN 978-80-247-3717-1.

SLOWÍK, Josef. *Nebojte se počítače*. 2. aktualizované vydání. Praha : Grada Publishing, 2006. 139 s.

ŠTĚDROŇ, Bohumír. *Open Source software : ve veřejné správě a soukromém sektoru*. Praha : Grada Publishing, 2009. 124 s. ISBN 978-80-247-3047-9.

THOMAS, Thomas. *Zabezpečování počítačových sítí : bez předchozích znalostí*. Brno : Computer Press, 2005. 340 s. ISBN 80-251-0417-6.

VEBER, Jaromír. *Řízení jakosti a ochrana spotřebitele*. 2. aktualizované vydání. Praha : Grada Publishing, 2007. 201 s. ISBN 978-80-247-1782-1.

VOŘÍŠEK, Jiří. *Principy a modely řízení podnikové informatiky*. Praha: Oeconomica. 2008. ISBN 978-80-245-1440-6.

VOŘÍŠEK, Jiří. *Strategické řízení informačního systému a systémová integrace*. Praha: Management Press. 2002. ISBN 80-85943-40-9.

VRANA, Ivan; RICHTA, Karel. *Zásady a postupy zavádění podnikových informačních systémů*. Praha: Grada Publishing. 2005. ISBN 80-247-1103-6 .

Elektronické zdroje:

Bezpečnost v kostce [online]. 2010 [cit. 2011-03-30]. Chrantesidata.cz. Dostupné z WWW: <http://www.chrantesidata.cz/cs/art/472/>.

SCHELS, Ignatz. *Excel 2007 : vzorce a funkce* [online]. Praha : Grada Publishing, 2008 [cit. 2011-03-24]. Dostupné z WWW: <http://books.google.com/books?id=BYsow4MxYtAC&printsec=frontcover&hl=cs&source=gbs_ge_summary_r&cad=0#v=onepage&q&f=false>. ISBN 978-80-247-2074-6.

VIK, Jaroslav; MAREK, Rudolf. *Securityworld.cz* [online]. 2010-12-20 [cit. 2011-03-23]. Fyzická bezpečnost a ochrana IT. Dostupné z WWW: <http://securityworld.cz/securityworld/fyzicka-bezpecnost-a-ochrana-it-3307>.

WEBER, Filip. *DoS a DDoS útoky a ochrana proti nim* [online]. 2008 [cit. 2011-03-28]. Svetsiti.cz. Dostupné z WWW: <http://www.svetsiti.cz/view.asp?rubrika=Technologie&clanekID=324>.

7 Přílohy

Příloha číslo 1: Současné logo advokátní kanceláře

Příloha číslo 2: Současné logo nonstop služby právního poradenství