Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačního inženýrství

Diplomová práce

Bezpečnost podnikové ICT infrastruktury z hlediska vnitřního napadení

Vedoucí práce: Ing. David Buchtela Ph.D.
Autor práce: Bc. Jaroslav Duda

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Katedra informačního inženýrství

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Duda Jaroslav

Informatika

Název práce

Bezpečnost podnikové ICT infrastruktury

Anglický název

Security of Company ICT Infrastructure

Cíle práce

Cílem diplomové práce je vytvořit návrh a popsat možnou realizaci celé ICT infrastruktury pro konkrétní organizaci s důrazem na bezpečnost nejen proti okolnímu světu, ale i proti možnému napadení z vnitřní sítě. Jedná se tedy o návrh řešení pro zajištění bezpečnosti sítě, proti možnému napadení z prostor firmy, které za normálních okolností považujeme za zcela bezpečné.
V diplomové práci budou uvedeny principy použité pro konkrétní zapojení datové sítě zvolené organizace, které však platí všeobecně. Dále budou popsány použité datové kabelové rozvody. Budou zde rozepsány jednotlivé typy hardwarových zařízení, včetně jejich konfigurace a v neposlední řadě zde budou zmíněny i použité softwarové systémy a jejich nastavení.
Tato práce si klade za cíl ukázat jakým způsobem lze vytvořit bezpečný funkční ICT systém a na základě zde vytvořeného popisu pomoci dalším organizacím nebo jednotlivcům při vytváření bezpečného ICT systému pro jejich konkrétní požadavky.

Metodika

Uvedené postupy, principy, informace a data v této diplomové práci, jsou sepsané dlouholeté znalosti a zkušenosti autora z praxe (autor pracuje v oboru informačních technologií od roku 1994) nebo samostudia a případné chybějící detailní informace jsou citovány z veřejně dostupných zdrojů jako jsou knihy nebo dnes největší celosvětová knihovna, za kterou je považován internet. Všechny citace jsou v této diplomové práci řádně označeny.
Velká část této diplomové práce pojednává o popisech principů a technických parametrů jednotlivých součástí celého ICT řešení, popřípadě norem a zavedených standardů.
Veškeré zde uvedené principy následně budou demonstrovány na, v praxi používaném, ICT systemu společnosti Česká rafinérská a.s. Litvínov. Nutno si uvědomit, že ICT system je jako živý organismus, který se neustále vyvíjí a mění. Z části vlivem potřeb a požadavků organizace a z části nově dostupnými technologiemi. Proto zde demonstrovaný stav je, v době vzniku této práce, ve fázi přípravy, tedy před uzavřením samotnou realizací.

Harmonogram zpracování

06/2012-08/2012 Upřesnění zadání práce a shromažďování literárních zdrojů
09/2012 Kontrola průběhu práce - 1.zápočet
09/2012-12/2012 Analýza informačních zdrojů a tvorba rešeršní části práce

Rozsah textové části

60 - 80 stran

Klíčová slova

ICT infrastruktura, bezpečnost, server, síť, switche, routery, počítače, sdílení dat, aplikace, firewall.

Doporučené zdroje informací

WERNER, Feibel. Encyklopedie počítačových sítí. Přeložil Martin Blažík – Libor Spěvák. Vydání první. Praha: Computer press, 1996. 1230 s. ISBN 80-85896-67-2

SCHATT, Stan. Počítačové sítě LAN od A do Z. Přeložil Tomáš Rutrle. Vydání první. Praha: GRADA, 1994. 378 s. ISBN 80-85623-76-5

HUNT, Craig. Konfigurace a správa sítí TCP/IP. Přeložil Ing. Jiří Veselský. Vydání první. Praha: Computer press, 1997. 456 s. ISBN 80-7226-024-3

ŠETKA, Petr. Mistrovství v Microsoft Windows Server 2003. Brno: Computer press, 2003. 671 s. ISBN 80-251-0036-7

Vedoucí práce

Buchtela David, Ing., Ph.D.

Ing. Martin Pelikán, Ph.D.
Vedoucí katedry

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

prof. Ing. Jan Hron, DrSc., dr.h.c.
Děkan fakulty

V Praze dne 12.10.2012

Čestné prohlášení

Prohlašuji, že svou diplomovou práci "Bezpečnost podnikové ICT (Information and Communication Technologies) infrastruktury z hlediska vnitřního napadení" jsem vypracoval zcela samostatně pod vedením vedoucího diplomové práce a za použití odborné literatury, a případně dalších informačních zdrojů, které jsou citovány v práci a následně uvedeny v seznamu literatury na konci diplomové práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Kralupech nad Vltavou dne 29.března 2013 _____

Poděkování

Dovolte mi, zde vyjádřit poděkování vedoucímu mé diplomové práce Ing. Davidu Buchtelovi Ph.D. za odborné vedení při tvorbě a zpracovávání diplomové práce. Dále bych rád poděkoval rodině, především manželce a dětem, za trpělivost a pevné nervy. Dozajista v době tvorby této práce to se mnou mnohdy nebylo jednoduché.

Bezpečnost podnikové ICT infrastruktury z hlediska vnitřního napadení

The Safety of Corporate ITC Infrastructure in terms of Internal Attack

Souhrn

Obsahem této diplomové práce, je zpracování problematiky bezpečnosti ICT infrastruktury ve zvolené společnosti z hlediska bezpečnosti proti možnému vnitřnímu napadení. Jsou zde zmiňovány jednotlivé vrstvy datových sítí, rozdělené dle známých standardů. Je zde popsáno konkrétní zapojení využívající dvou datových center, s možností připojení koncových zařízení, pomocí různých komunikačních protokolů. Při zajištěné bezpečnosti umožňující sdílení dat, případně aplikací, mezi jednotlivými uživateli. S možností práce kontraktorů či kmenových uživatelů z externích prostor, prakticky odkud koliv na světě. Za splněné podmínky, že má dotyčný možnost vzdáleného připojení ke sledované síti pomocí připojení k internetu.

Závěrem této diplomové práce je konkrétní popis jednoho možného řešení daného problému ve zvolené společnosti se dvěmi datovými centry ve dvou různých výrobních areálech. Které jsou umístěny v od sebe vzdálených lokalitách. Při zajištění stejného uživatelského prostředí nezávisle na lokalitě i s možností bezpečného připojení uživatele při práci externě, tedy i na služebních cestách či případně z domova nebo dovolené. S popisem bezpečnostních opatření proti možnému napadení.

Summary

The content of this thesis is to treat the problem of ICT security infrastructure in the selected companies in terms of internal security against possible attack. The various layers of data networks, distributed according to known standards, are mentioned as well . It describes specific involvement using two data centers, with connection terminals, using different communication protocols. Ensuring safety for sharing data or applications between users. With the ability to work contractors or ordinary users of external space, virtually anywhere in the world. Under the condition that there is any possibility of a remote connection to the monitored network using an Internet connection.

The conclusion of this thesis is a specific description of one possible solution to the problem in the selected company with two data centers in two different production sites which are located in widely separated locations. While ensuring the same user experience

regardless of location with the possibility of a secure connection the user when working externally, even on business trips or possibly from home or on vacation, with the description of the security measures against possible attack.

Klíčová slova: ICT infrastruktura, bezpečnost, server, síť, switche, routery, počítače, sdílení dat, aplikace, firewall.

Keywords: ICT infrastructure, safety, server, net, switch, router, computers, sharing data, aplications, firewall.

Obsah:

1. Úvod 13
2. Cíl práce a metodika 15
   - 2.1. Cíl práce 15
   - 2.2. Metodika 15
3. Přehled principů a dostupných technologií 16
   - 3.1. Model ISO/OSI – TCP/IP 16
   - 3.2. Datové rozvody 17
     - 3.2.1. Typy rozvodů 17
     - 3.2.2. Aktivní prvky 18
     - 3.2.3. Zabezpečení rozvodů 21
       - 3.2.3.1. Mechanické 21
       - 3.2.3.2. Elektronické 22
       - 3.2.3.3. Sofistikované 22
         - 3.2.3.3.1. VLAN 22
         - 3.2.3.3.2. Standard IEEE 802.1x 23
         - 3.2.3.3.3. MAC filtry 24
   - 3.3. Síťové služby a protokoly 24
     - 3.3.1. Komunikační protokoly 25
       - 3.3.1.1. IP verze 4 25
       - 3.3.1.2. IP verze 6 27
       - 3.3.1.3. NETBUI 28
       - 3.3.1.4. IPX/SPX 28
       - 3.3.1.5. Komunikační vrstvy 28
     - 3.3.2. Služby podporující chod sítě 29
       - 3.3.2.1. DNS 30
       - 3.3.2.2. WINS 30
       - 3.3.2.3. DHCP 30
   - 3.4. Systémy a aplikace 31
     - 3.4.1. Systémy serverové 31
       - 3.4.1.1. Katalog sítě 32
       - 3.4.1.2. Tisk 32

3.4.1.3. Vzdálené přístupy 32
3.4.1.4. Data na mobilních zařízeních 33
3.4.2. Systémy aplikační 34
3.4.2.1. Komunikace 34
3.4.2.1.1. Elektronická pošta 34
3.4.2.1.1.1. Protokol SMTP/SMTPS 35
3.4.2.1.1.2. Služba router 35
3.4.2.1.1.3. POP3/POP3S/IMAP/IMAPS 35
3.4.2.1.1.4. Aplikace elektronické pošty 36
3.4.2.1.1.5. Online komunikace 36
3.4.2.1.1.6. VOIP 37
3.4.2.1.2. Informační systém 37
3.4.2.1.2.1. Koordinace zaměstnanců 38
3.4.2.1.2.2. Účetní systém 38
3.4.2.1.2.3. Skladové hospodářství 39
3.4.2.1.3. Společná data 39
3.4.2.1.3.1. Diskový prostor 39
3.4.2.1.3.2. Intranet/extranet 40
3.4.2.1.3.3. Databáze 41
3.4.2.1.4. Společné aplikace 42
3.5. Zařízení - Aplikace s bezpečnostním aspektem 42
3.5.1. Firewall 42
3.5.2. Antivir 44
3.5.3. Antispam 45
3.5.4. Zálohování 46
3.5.5. Dohledový a varovný systém 47
3.5.6. Nástroje pro správu sítě 48
3.6. Bezpečnost dat – šifrování 48
3.6.1. Šifrování synchronní 49
3.6.2. Šifrování asynchronní 50
3.6.3. RSA 50
3.6.4. Vodoznaky 51

3.6.5. Další možnosti šifrování 51
3.6.6. Elektronický podpis 52
3.7. Bezpečnost komunikace 53
3.7.1. IDS 54
3.7.2. IPS 54
3.8. Právní ochrana firmy 54
3.8.1. Interní směrnice/normy 55
3.8.2. Zákony ČR 56
3.8.3. OSA 56
4. Vlastní návrh bezpečnosti ICT infrastruktury z hlediska vnitř. napadení 57
4.1. Výchozí stav Kralupy 58
4.2. Výchozí stav Litvínov 65
4.3. Propojení areálů 71
4.4. Uživatelské prostředí 72
4.5. Prostředí společnosti a dohled ICT systémů 72
4.6. Projekt „Redundance optických tras“ 73
4.7. Projekt „Definice SLA“ 76
4.8. Projekt „Interní směrnice a normy“ 76
4.9. Projekt „Bezpečnost datových rozvodů“ 77
4.10. Projekt „Propojení areálů a internet“ 77
4.11. Projekt „Nezávislé datové centrum“ 78
4.12. Projekt „NAS“ 78
4.13. Projekt „Virtualizace serverů“ 79
4.14. Projekt „Zálohování dat“ 80
4.15. Projekt „VLAN“ 81
4.16. Projekt „Šifrovaná komunikace“ 83
4.17. Projekt „IPS/IDS“ 84
4.18. Projekt „E-learning“ 84
4.19. Projekt „Čipové karty“ 86
4.20. Projekt „802.1x“ 87
4.21. Projekt „Rizika“ 88
4.22. Ostatní využívané bezpečnostní systémy 89

5. Zhodnocení výsledků a doporučení 90
6. Závěr 91
7. Seznam použitých zdrojů 93
8. Seznam obrázků 95

1. Úvod

Bezpečnost informačních technologií je v současné době velmi dynamicky se rozvíjející obor, který v sobě zahrnuje mnohá odvětví. Tento obor se vyvíjí tak rychle, jak rychle se vyvíjí elektronická kriminalita. Mnohé, dříve zavedené standardy se mění dle aktuálně získaných znalostí a dovedností. Přehodnocuje se pohled na dříve zcela běžně používané a z hlediska bezpečnosti dostatečné technické specifikace. V této diplomové práci se budeme zabývat problematikou vnitřní sítě firmy a její bezpečnosti. Tedy bezpečností síťě jako takové, ale zároveň i bezpečností komunikace po této síti a následně bezpečností dat na síti uložených.

Bezpečnost vnitřní sítě je významná oblast, která se mnohdy velmi podceňuje nebo spíše se ve většině případů vůbec neřeší. Každý zaměstnavatel vychází z přesvědčení, že vnitřní síť je bezpečná neb se na ní pohybují pouze zaměstnanci společnosti a jejich zájmem je pomáhat firmě, tedy nikoliv jí škodit. Bohužel si neuvědomují, že tomu v mnoha případech takto není.

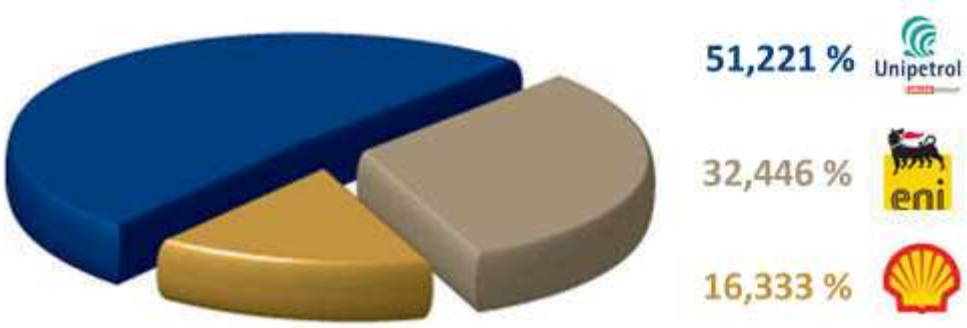
V dnešní době, kdy jsou zcela běžně využívány špionážní techniky pro získání informací o všem možném, co by mohlo přetáhnout zákazníky v konkurenčním boji nebo by nějakým způsobem mohlo firmu poškodit (například propuštěný zaměstnanec), je poté otázka bezpečnosti a ochrany dat pro společnost prioritní. Velice často to začnou společnosti řešit až na základě vlastních negativních zkušeností.

V této práci se budeme konkrétně zabývat bezpečností datové sítě z hlediska vnitřního napadení a v praktické části popíšeme bezpečnostní prvky použité v konkrétní organizaci. Jedná se o společnost Česká rafinérská a.s. Litvínov („Rafinerie v srdci evropy“) [online, www.crc.cz]. Tato společnost je největším zpracovatelem ropy a výrobcem ropných produktů v České republice. Provozuje dvě rafinérie ropy situované v Litvínově a Kralupech nad Vltavou. Byla založena 28. dubna 1995. Česká rafinérská je společným podnikem Unipetrolu a renomovaných zahraničních společností Eni a Shell.

Česká rafinérská je provozována jako přepracovací rafinérie, resp. nákladové středisko svých zpracovatelů, kteří nakupují ropu a ostatní suroviny ke zpracování v rafinériích v Litvínově nebo Kralupech nad Vltavou a veškerou produkci prodávají zákazníkům v tuzemsku a zahraničí.

Česká rafinérská se stále řadí mezi nejvýznamnější tuzemské společnosti. Je držitelem certifikátu ISO 9001, ISO 14001 a OHSAS 18001. Dlouhodobě se věnuje dárcovství, pomoci neziskovým organizacím a podpoře regionům kde působí.

Akcionáři společnosti Česká rafinérská a.s. Litvínov a jejich podíly ve společnosti jsou znázorněny na obrázku 1.



OBR. 1 Podíly akcionářů společnosti, ZDROJ: WWW.CRC.CZ

Společnost Unipetrol a.s. zastupovala zájmy státu České republiky až do okamžiku, kdy společnost Unipetrol a.s. celých 100% podílu bylo odprodáno vládou České republiky polskému vlastníkovi PKN Orlen v roce 2005.

2. Cíl práce a metodika

2.1. Cíl Práce

Cílem mé diplomové práce je vytvořit návrh a popsat možnou realizaci celé ICT infrastruktury pro konkrétní organizaci s důrazem na bezpečnost nejen proti okolnímu světu, ale i proti možnému napadení z vnitřní sítě. Jedná se tedy o návrh řešení pro zajištění bezpečnosti sítě, proti možnému napadení z prostor firmy, které za normálních okolností považujeme za zcela bezpečné.

V diplomové práci budou uvedeny principy použité pro konkrétní zapojení datové sítě zvolené organizace, které však platí všeobecně. Dále budou popsány použité datové kabelové rozvody. Budou zde rozepsány jednotlivé typy hardwarových zařízení, včetně jejich konfigurace a v neposlední řadě zde budou zmíněny i použité softwarové systémy a jejich nastavení.

Tato práce si klade za cíl, ukázat jakým způsobem lze vytvořit bezpečný funkční ICT systém a na základě zde vytvořeného popisu pomoci dalším organizacím nebo jednotlivcům při vytváření bezpečného ICT systému pro jejich konkrétní požadavky.

2.2. Metodika

Uvedené postupy, principy, informace a data v této diplomové práci, jsou sepsané dlouholeté znalosti a zkušenosti autora z praxe (autor pracuje v oboru informačních technologií od roku 1994) nebo samostudia a případné chybějící detailní informace jsou citovány z veřejně dostupných zdrojů, jako jsou knihy nebo dnes největší celosvětová knihovna, za kterou je považován internet. Všechny citace jsou, v této diplomové práci, řádně označeny.

Velká část této diplomové práce pojednává o popisech principů a technických parametrů jednotlivých součástí celého ICT řešení, popřípadě norem a zavedených standardů.

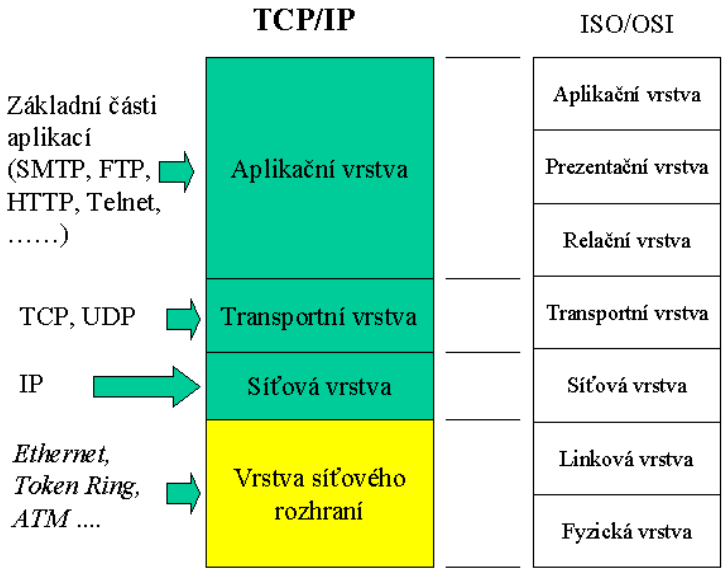
Veškeré zde uvedené principy následně budou demonstrovány na, v praxi používaném, ICT systému společnosti Česká rafinérská a.s. Litvínov. Nutno si uvědomit, že ICT systém je jako živý organismus, který se neustále vyvíjí a mění. Z části vlivem potřeb a požadavků organizace a z části nově dostupnými technologiemi. Proto zde demonstrovaný stav je, v době vzniku této práce, ve fázi přípravy, tedy před uzavřením samotnou realizací.

3. Přehled principů a dostupných technologií

Kapitola 3. a všechny její jednotlivé podkapitoly, jsou věnovány teoretickým základům, principům a postupům, bez kterých by svět ICT nebyl schopný správně pracovat, komunikovat, přenášet či sdílet data a případně plnit ještě další očekávané či požadované funkce. Okruh požadovaných funkcí se neustále rozšiřuje na základě požadavků uživatelů. Stále se vyvíjejí se nové technologie, případně starší již nevyhovující technologie se postupně opouští.

3.1. Model ISO/OSI – TCP/IP

Základním standardem v datové komunikaci je referenční komunikační model ISO/OSI (International Standards Organization / Open Systems Interconnection) nebo novější, dnes rozšířenější verze komunikačního modelu TCP/IP (Transmission Control Protocol / Internet Protocol).



OBR. 2 POROVNÁNÍ MODELŮ ISO/OSI A TCP/IP, ZDROJ: WWW.EARCHIV.CZ

Zmíněné dva standardy definují jednotlivé komunikační vrstvy modelu architektury datové komunikace. [Hunt, 1997, s. 4] Zároveň, tyto standardy definují i funkci zmíněných vrstev v komunikačním procesu, který se využívá při přenosu dat, nebo nějaké informace mezi alespoň dvěma koncovými zařízeními. Zmíněný model ISO/OSI má vrstev sedm, oproti tomu model TCP/IP má čtyři vrstvy. Jednotlivé vrstvy těchto modelů budou v této diplomové práci rozepsány do větších podrobností v následujících kapitolách.

3.2. Datové rozvody

Datovými rozvody nazýváme nejnižší vrstvu modelu ISO/OSI. Jedná se o fyzickou vrstvu představující propojení minimálně dvou nebo více různých zařízení za pomoci nějakého kabelu, linky, optiky a podobně. Tedy pomocí něčeho, na co se „dá rukama sáhnout“. V dnešní době technologického boomu však jsou i tyto fyzické propojení realizovány pomocí bezdrátových technologií.

3.2.1. Typy rozvodů

Datové rozvody rozlišujeme podle jejich určení, umístění, využití a podobně. Podle zvolených parametrů pak tyto datové rozvody zařazujeme do různých typů.

Máme základní rozdělení typů sítí na LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network), WLAN (Wireless LAN) a další.

LAN – [Shatt, 1994, s. 32] Jedná se o komunikační síť užívanou jedinou organizací na omezenou vzdálenost, která umožňuje sdílení informací a technických prostředků. Je realizována, pomocí různých kabelových rozvodů. V dnešní době nejčastěji strukturovanou kabeláží kategorie 5E nebo vyšší. Dříve byly používány různé typy kabelů například koaxiální RG58 a další. Nejčastěji se síť LAN využívá v rámci jedné budovy, případně kanceláře nebo v soukromí domova.

MAN – [Werner, 1996, s. 584] Je typ komunikační sítě, která obvykle pracuje na vyšších rychlostech než sítě typu LAN. MAN sítě propojují několik sítí typu LAN. Většinou se k tomuto účelu využívají optické kabely různých typů a provedení (například multimode nebo singlemode). Mnohdy využívané především organizacemi s působností v několika lokalitách s nutností vzájemné spolupráce nebo výměny nějakých dat.

WAN – [Werner, 1996, s. 1064] Je typ komunikační sítě, která se využívá pro připojení sítí mezi sebou. Nejčastěji je dnes takto označováno připojení sítě LAN nebo MAN do sítě sítí neboli do celosvětové informační sítě internet, případně na nějaké odloučené pracoviště společnosti, které nevyžaduje silnou konektivitu k ostatním zařízením organizace.

WLAN – Jedná se o typ sítě LAN za využití bezdrátového přenosu dat. Což významě zvýší mobilitu a komfort uživatele nebo možnost měnit umístění připojených zařízení. Mnohdy je tento komfort vyvážen snížením rychlosti přenesených dat.

Druhů kabelů pro samotnou realizaci jednotlivých typů sítí je mnoho. Jen pro ukázku si zmíníme několik druhů kabelů a jejich nejčastější využití:

a) Koaxiální kabel - [Shatt, 1994, s. 50] využívaný hlavně pro rozvody televizního signálu například ve společných rozvodech v bytových domech.
b) Kroucená dvojlinka – [Shatt, 1994, s. 49] různé varianty kabelu TP (twisted pair). Lišící se použitým stíněním nebo podle určení do jakého prostředí se mám konkrétní kabel používat. Dnes se jedná o nejvyužívanější kabel pro sítě typu LAN.
c) Optický kabel - [Shatt, 1994, s. 54] Nejačastěj využívané v sítích typu MAN. Problematické převody signálu mezi elektrickým signálem a světlem. Zároveň má nespornou výhodu v galvanickém odpojení objektů a velmi širokou propustností dat. Lze využít multimódové nebo single módové vlákna (liší se počtem signálů převáděných v jedné vlnové délce v rámci jednoho vlákna).
d) Další kabely širokopásmové nebo kabely se základním pásmem dnes spíš pro speciální využití. Samozřejmě i další typy kabelů v této práci neuvedené.

3.2.2. Aktivní prvky

Základním stavebním kamenem každé infrastruktury datové sítě, jsou tak zvané aktivní prvky. Jedná se o zařízení, která jsou součástí sítě a jejich hlavní činností je připojovat koncová zařízení (jako jsou počítače, servery a podobně) a následně zajistit předávání posílaných dat při propojení a komunikaci mezi jednotlivými koncovými zařízeními. Tato zařízení mají různé provedení. Liší se počtem přípojných míst (portů), rychlostí přenášených dat v dnešní době nejběžnější rychlosti ethernetové sítě jsou 10/100/1000 MB/s. Také se liší provedením, zda jsou určeny do kanceláře nebo montovatelné do rozvodných skříní (racků). Rack je uzamykatelná skříň různého provedení (stojací nebo montovatelné na zeď) do které se soustřeďují datové rozvody od jednotlivých koncových zařízení a jejich konečného umístění v budovách. Do těchto racků se poté montují zmiňované aktivní prvky, které následně zajišťují komunikaci mezi těmito koncovými zařízeními na vyšších vrstvách komunikačního modelu ISO/OSI a podobně. Některé základní typy si v této práci uvedeme.

OBR. 3 Různé aktivní prvky, ZDROJ: WWW.CISCO.COM

BRIDGE – [Werner, 1996, s. 104] Jedná se o HW (hardware) zařízení, které umožňuje packetům procházet z jedné sítě do druhé. Tyto bridge (mosty) pracují na druhé nejnižší vrstvě komunikačního modelu ISO/OSI, na linkové vrstvě. Spojují dvě různé sítě, které se pak pro vyšší vrstvy komunikačního modelu ISO/OSI tváří jako jedna síť.

HUB – [Werner, 1996, s. 452] HUB je HW zařízení, které může být jednou ze součástí infrastruktury sítě. Toto zařízení slouží k propojování jednotlivých koncových zařízení nebo dalších aktivních prvků sítě. Zajišťuje předávání dat z jednoho portu na všechny porty, které má k dispozici. Což má za následek, že se data přenáší i k zařízením, které je nepotřebují, a snižuje se tím celková datová propustnost sítě. Další možností využití hubů je jako zesilovače signálu. Tedy jejich využití pro zesílení signálu předávaných dat při přenosu na větší vzdálenosti.

SWITCH – [Werner, 1996, s. 966] jedná se o sofistikovanější elektronické zařízení, které má obdobné vlastnosti jako zařízení typu HUB. Tedy propojuje koncová zařízení a zároveň také zesiluje přenášený signál. Má však mnoho dalších vlastností navíc. Disponuje větší datovou propustností. Která se zásadně zvyšuje tím, že se data nerozesílají na všechny dostupné porty. Což umožňuje komunikaci více portů současně. Například zařízení připojené k portům 8 a 10 spolu mohou komunikovat (předávat si data) ve stejný okamžik, jako jiná obdobná zařízení připojená třeba k portům 2 a 5.

Zařízení typu switch je dnes nejpoužívanější a nejrozšířenější aktivní prvek používaný pro jakýkoliv typ sítě. Existují v mnoha provedeních od nejlevnějších, do kanceláří nebo spíše domácností, mnohdy sloučené s dalšímy aktivními prvky jiného typu (routry, brány, přístupovými body a podobně), až po ty nejdražší, které mají i jiné možnosti využití například pro sledování chybovosti portů nebo možnosti změn konfigurace switche. Jako rozšířené vlastnosti si můžeme uvést například možnost zcela oddělit komunikaci dvou portů mezi sebou od ostatní komunikace zbylých portů nebo nebo možnost sledování

provozu na jednotlivých portech, či jen obyčejné vypínání a zapínání portů pro komunikaci a podobně. Jednou z velmi používaných vlastností je i zabudování SNMP (Simple Network Management Protocol) protokolu, který se využívá pro sledování stavu a funkčnosti jednotlivých zařízení, zejména ve větších a rozsáhlejších sítích. Těchto rozšířených vlastností bychom zde mohly uvést opravdu velmi mnoho.

Některá zařízení typu switch (většinou dvě a více zařízení stejného typu, ale až vyšších řad, ty nejnižší řady toto nenabízí) se dají vzájemně spojovat pomocí speciálního kabelu. (tak zvaně stackovat - stohovat). Takto propojená zařízení se pak tváří, jako jedno zařízení o více portech.

ROUTER – [Werner, 1996, s. 876] neboli směrovač je aktivní prvek, který má za úkol poskytnout cestu z jednoho síťového uzlu na další uzel umístěný v jiné síti. Jednotlivé sítě mohou být propojeny přes několik dalších sítí. Tyto zařízení pracují v síťové vrsvě komunikačního modelu ISO/OSI (internetové vtstvě komunikačního modelu TCP/IP). Nejprve router určí cestu a následně poskytne spojení pro tuto cestu. Směrovač se zároveň používá jako filtr packetů v závislosti na síťových protokolech. Routry umožňují rozdělit jednu větší síť (s více než 254 koncovými zařízeními v jedné síti) na několik menších sítí, třeba dle určení nebo funkce. Routery také umožňují propojení různých architektur sítí například ethernet (síťová architektura dle standardu IEEE 802.3), FDDI (Fiber Distributed Data Interface) – síťová architektura dle standardu X3T9.5 určená pro přenosy dat prostřednictvím optických kabelů při velmi vysokých rychlostech, Token ring - je síťová architektura dle standardu IEEE802.5 založená na kruhové síťové architektuře a metodě předávání peška (tokenu) při řízení přístupu k síti, a další.

MEDIA KONVERTOR – Jsou hardwarová zařízení (převodníky) převádějící signál nesoucí data z jednoho média na druhé. Dnes se nejčastěji používají převodníky mezi optickými kabely a metalickými kabely. Tedy ze světelného přenosu dat (pomocí optického kabelu single mode nebo multimode) na elektrický přenos dat (nejčastěji na strukturovanou kabeláž). Připadně VDSL (Very high bit-rate Digital Line Subscriber), kdy se signál z telefonní linky převádí na strukturovanou kabeláž. Těchto převodníků je celá řada, prakticky by se dalo konstatovat, že pokud je technicky možné převádět signál z jednoho přenosového média na druhý, pak pro tento převod existuje alespoň jeden typ převodníku. Mnohdy je typů převodníků velké množství a rozlišují se například vzdáleností pro jak dlouhý kabel je možné je použít a podobně.

PŘÍSTUPOVÝ BOD – Access pointy (AP) jsou hardwarová zařízení, pomocí nichž dokážeme nahradit kabelové rozvody sítí typu LAN, MAN, WAN. Využívají bezdrátový přenos dat pomocí signálu přenášeného vzduchem. Poskytují luxus v podobě mobility koncových zařízení a uživatelů, ale za cenu možných ztrát (například důsledkem nějakého rušení) a mnohdy i za cenu nižší propustnosti přenášených dat. WLAN (Wireless Local Area Network) je označení pro bezdrátový přenos dat na síti. Pro tyto účely jsou dnes vyhrazená kmitočtová pásma s nosnou vlnou 2,4 GHz a 5 GHz, která jsou vyhrazena ČTÚ (Český telekomunikační úřad) pro veřejné použití v České republice.

3.2.3. Zabezpečení rozvodů

Prvotním prvkem bezpečnosti datové sítě je zabezpečení datových rozvodů tak, aby společnost (domácnost, firma, korporace a podobně) byla schopna ochránit svá data před jejich odcizením, ztrátou, zneužitím a případně dalším možným nežádoucím nakládáním s daty, které firma mnohdy dlouze a náročně sbírá, skladuje a využívá pro svou činnost. Takto získaná data jsou její největší konkurenční výhodou, hodnotou nebo akvizicí, která jí přináší nějakou přidanou hodnotu či dokonce zisk.

3.2.3.1. Mechanické

Mezi nejzákladnější kameny bezpečnosti patří fyzické zabezpečení rozvodů a koncových zásuvek. Tedy podle pravidla: „Kde nic není, ani smrt nebere.“ Což v datových sítích znamená: Kde nevede žádná síť, tam je každá síť bezpečná. Každý správce/administrátor sítě, by tedy měl zajistit, aby byla síť jen tam, kde bude využívána nebo pokud je připravena síť s výhledem do budoucna. Tedy více připravených přípojných míst. Měla by, tato dočaně nevyužívaná místa, být natolik zabezpečená, aby nemohlo dojít k připojení nějakých nežádoucích zařízení, které by mohly sledovat provoz na síti a odchytávat nebo dokonce měnit data na síti uložená.

Mezi mechanické zabezpečení se počítá demontáž nepoužívaných datových zásuvek, nebo umístění datových zásuvek do zamykatelných skříněk, či minimálně nepropojení těchto koncových přípojných míst do nějakého aktivního prvku (tedy položený kabel s přípojným místem, který ale nikam nevede) a další mechanické překážky, zamezující volný přístup k přípojnému místu.

3.2.3.2. Elektronické

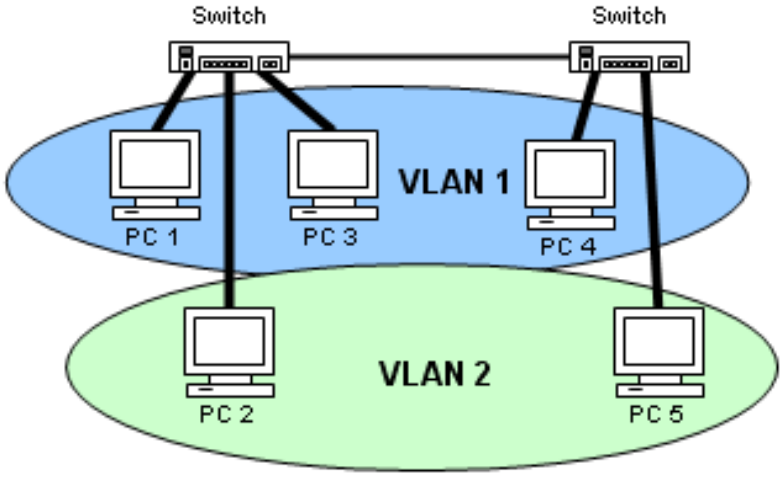
Elektronické zabezpečení umožňují aktivní prvky již od střední třídy a samozřejmostí je to u vyšších tříd. Jednáse o základní technickou funkci umožňující na základě nastavení přepnout port, ke kterému je připojené nějaké přípojné místo, do stavu up (zapnuto) nebo do stavu down (vypnuto). Porty ve stavu up umožňují komunikaci do sítě, zatímco na portech ve stavu down, žádný přenos dat neprobíhá.

3.2.3.3. Sofistikované

Jedná se o řešení bezpečnosti s nějakou vyšší logikou zabezpečení nebo alespoň rozdělení provozu a přenosu dat po síti. Zde si uvedeme několik možností, jak zvýšit bezpečnost dat a komunikace na síti.

3.2.3.3.1. VLAN

VLAN (Virtual Local Area Network) – [Shatt, 1994, s. 98] Virtuální sítě jsou řešení pro sítě u kterých je požadováno nějakým způsobem efektivně řídit provoz po síti. Pomocí této logiky jsme schopni na jedné fyzické síti vytvořit hned několik logických sítí, které se jeví jako jedna síť, avšak komunikace mezi jednotlivými logickými sítěmi může být pomocí různých pravidel řízena, povolována nebo zakazována, směrována a podobně. Nespornou výhodou je, že provoz jedné virtuální (logické) sítě nijak neovlivňuje provoz jiné virtuální sítě.



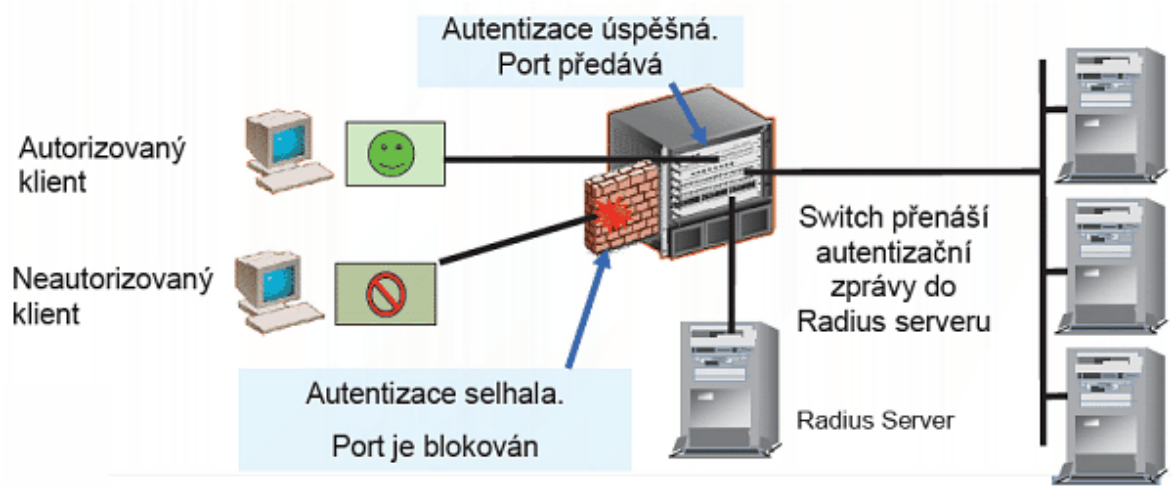
OBR. 4 ZNÁZORNĚNÍ VIRTUÁLNÍCH SÍTÍ, ZDROJ: WWW.LUPA.CZ

Nejčastěji se virtuální sítě vytvářejí například podle lokalit nebo podle účelu koncových zařízení, které jsou do konkrétní virtuální sítě zařazené. Rozdělení se dá udělat například VLAN1 – laboratorní přístroje, VLAN2 – servery, VLAN3 – Administrativní budova, VLAN4 – Výrobní budova a podobně.

V dnešní době se tyto virtuální sítě dokonce dají měnit dynamicky (bez nutnosti připojovat koncové zařízení kabelem pokaždé k jinému portu aktivního prvku), aktivní prvky s vyšší logikou dokáží na základě centrální správy a agentů v koncových zařízeních poznat, že toto koncové zařízení nemá například poslední aktualizaci antivirového programu a podle toho přiřadí koncové zařízení do virtuální sítě s možností přístupu pouze do internetu, ale se zakázaným přístupem na servery s daty společnosti. Po aktualizaci antivirového programu automaticky dojde ke změně zařazení koncového zařízení do jiné virtuální sítě s jinak definovanými přístupy. Takto lze koncová zařízení zařazovat do různých virtuálních sítí podle předem definovaných pravidel administrátorem.

3.2.3.3.2. Standard IEEE 802.1x

Standard IEEE 802.1x [online, www.compunet.cz] definuje ověřování připojených koncových zařízení a uživatelů pro připojení k datové síti. Toto ověřování se provádí na základě autentizace a autorizace k radius serveru a to dle nastavených pravidel. Aktivní prvky v datové síti musí tento standard podporovat, aby bylo zajištěno jeho bezproblémové využívání.



OBR. 5 ZNÁZORNĚNÍ OVĚŘOVÁNÍ STANDARDEM 802.1X, ZDROJ: WWW.COMPUNET.CZ

Ověřování na základě standardu 802.1x může být provedeno například zadáním jména a hesla, případně na základě vydaného certifikátu nějakou certifikační autoritou.

Pokud proces autorizace proběhne v pořádku, pak je port aktivního prvku, ke kterému je koncové zařízení připojeno, otevřen pro následnou komunikaci a přenos dat. Pakliže proces autorizace z nějakého důvodu neproběhne úspěšně, poté je tento port na aktivním prvku blokován pro další komunikaci.

3.2.3.3.3. MAC filtry

Každé zařízení, které má nějaké komunikační rozhraní, tedy nějaký port pro připojení do jakékoliv datové sítě, má pro toto rozhraní přidělenou již od výrobce tak zvanou MAC (Media Access Control) adresu [Werner, 1996, s. 580].

Tato adresa je složena ze šesti dvoumístných hexadecimálních znaků (například 78:8e:45:90:ce:f2). Tato adresa je celosvětově jedinečná. Každý výrobce dostává přiřazenou první polovinu tohoto čísla z centrálního registru a pro každý výrobek (například síťovou kartu, router a podobně) pak přiřadí tuto přidělenou část a druhou polovinu tohoto čísla pak volí sám pro každý jednotlivý výrobek. Na základě těchto adres lze vytvořit tabulku (seznam MAC adres), podle kterého je následně umožněn přístup do datové sítě, či naopak je tento přístup zakázán.

Bohužel dnešní systémy umožňují snadno změnit MAC adresu jednotlivých komunikačních rozhraní. Pro běžného uživatele je tato funkcionalita dnešních systémů zbytečná a pro bezpečnostní administrátory je tato funkcionalita naprosto nežádoucí. Pro někoho, kdo chce získat přístup do datové sítě pro nějaké nezákonné účely, je tato možnost jistě vítaným ulehčením jeho činnosti.

3.3. Síťové služby a protokoly

Síťové služby a protokoly pracují v komunikačním modelu ISO/OSI od třetí vrstvy (network) a výš. Síťové služby jsou různé aplikace, programy, služby a podobně, které nějakým způsobem pomáhají nebo jsou důležité pro chod sítě.

Komunikační protokoly zajišťují přenos dat mezi jednotlivými zařízeními k síti připojené, tak aby došlo podle pravidel komunikačního protokolu k úspěšnému předání dat od zdroje (místo kde jsou data k dispozici) ke koncovému zařízení (místo, které si data vyžádalo).

3.3.1. Komunikační protokoly

Komunikační protokoly [Šetka, 2003, s. 39] na spodní vrstvě komunikačního modelu ISO/OSI jsou využívány pro základní komunikaci dvou zařízení mezi sebou, tedy umožňují vzájemnou komunikaci těchto zařízení na jedné společné síti. Vyšší komunikační vrstvy v sobě obsahují specializované komunikační protokoly například pro přenos elektronické pošty a podobně. Těmito komunikačními protokoly se budeme zabývat později. Jelikož jsou na vyšších vrstvách komunikačního modelu.

Pro vzájemnou komunikaci dvou zařízení není nutné, aby obě zařízení komunikovali na stejné síti za využití stejného komunikačního protokolu. Samozřejmě tato cesta, pokud jsou tato zařízení na stejné síti i na setjném komunikačním protokolu, je nejsnazší a nejrychlejší. Toto však není podmínkou, lze za pomoci mnohých „překladatelů - routerů“ (zařízení umožňující komunikaci mezi různými sítěmi) spojit dvě zařízení, každé připojené do jiné sítě a třeba i využívající jiný komunikační protokol. Zjednodušeně řečeno „Pakliže existuje, alespoň jedna cesta umožňující komunikaci dvou zařízení, pak je tato komunikace možná.“

3.3.1.1. IP verze 4

V dnešní době je nejpoužívanější protokol TCP/IP verze 4. [Šmrha - Rudolf, 1995, s. 9] Který vzešel z první sítě tohoto typu, ze sítě pojmenované ARPANET. Tato síť byla vyvinuta jako testovací pro americké ministerstvo obrany v roce 1970.

IP protokol je celá skupinu různých komunikačních protokolů. V této skupině je pak každý protokol s předem definovanou funkcionalitou. Některým těmto protokolům se budeme následně v této diplomové práci ještě věnovat.

IP adresa verze 4 je číslo složené z 32 bitů, které se rozděluje do čtyř částí po osmi bitech (zvané oktety) a oddělené tečkou (například 001.004.002.003, 112.036.064.253 a podobně). Tato adresa musí být přiřazená ke každému zařízení, které má po této síti komunikovat. Každému zařízení je přiřazena alespoň jedna IP adresa (identifikuje zařízení), zároveň je přiřazena maska sítě (identifikuje počet možných zařízení na dané síti), dále se přiřazuje i výchozí brána za předpokladu, že je možná komunikace i do jiné sítě než jaká je definovaná na základě IP adresy a masky.

Každá IP adresa musí splňovat určitá pravidla, aby bylo možné ji přiřadit nějakému zařízení:

i. První adresa ze zvolené sítě je neurčitá a označuje celou síť, proto není možné tuto adresu přiřadit nějakému konkrétnímu zařízení.
ii. Další adresu, kterou nelze přiřadit žádnému konkrétnímu zařízení je poslední adresa ze zvoleného rozsahu. Tato adresa je určená pro všesměrově zasílané packety (části dat) určené pro informace všech zařízení na dané síti. Jedná se o broadcasting.
iii. Adresa je složena z jednotlivých oktetů. Hodnoty každého oktetu jsou tedy v rozsahu 2^8 (8 bitů) tedy 0-255.
iv. Každá přiřazená IP adresa musí být na dané síti jedinečná. Pakliže dojde k situaci, kdy se k jedné síti připojí dvě zařízení se stejnou IP adresou, dojde ke konfliktu, zařízení jsou od sítě odpojena, dokud nedojde k nápravě. Tedy dokud se alespoň na jednom zařízení IP adresa nezmění na nějakou dosud volnou IP adresu v dané síti.

IANA (Internet Assigned Numbers Authority) je organizace odpovědná za poskytování IP adres pro celý svět na síti sítí, tedy na internetu. Tato organizace vyčlenila několik rozsahů IP adres pro neveřejné použití. Jedná se o rozsahy s maskou sítě typu A (255.000.000.000) rozsah je od 010.0.0.0 do 010.255.255.255, dále o rozsahy s maskou sítě tybu B (255.255.0.0) tedy adresy od 172.016.000.000 až do 172.031.255.255, a v neposlední řadě i rozsahy s maskou sítě typu C (255.255.255.0) tedy rozsahy od 192.168.000.000 až do 192.168.255.255.

Je možné použít neveřejnou adresu z rozsahu 010.0.0.0 a k němu použít masku sítě tybu C, což má za následek rozdělení jedné velké sítě do několika menších. Toto se využívá ve větších sítích, kde je zapotřebí nějakým způsobem řídit provoz na síti, či nějakým způsobem regulovat provoz na síti.

Neveřejné rozsahy jsou určeny pro sítě oddělené od internetu pomocí NAT (Network adrress Translation). Tedy pomocí nějakého překladače adres, který nahrazuje neveřejné adresy z vnitřní sítě za adresu veřejnou na vnějším rozhraní, což má za následek, že se síť o několika i tisících zařízení na internetu zobrazuje jako zařízení jediné, které má přiřazenu jednu veřejnou IP adresu.

IP adresa společně s maskou sítě určuje kolik zařízení je schopno spolu komunikovat přímo. Například zařízení s adresou 192.168.035.126 a maskou

255.255.255.0 dokáže přímo komunikovat se zařízenímy v rozsahu adres 192.168.035.001 – 254 (0 je celá síť a 255 je adresa pro broadcast, jak bylo uvedeno dříve). Někdy se velikost sítě (maska sítě) zpisuje ve formátu 192.168.35.126/24. Tento zápis je dle standardu CIDR (Classless InterDomain Routing).
Maska sítě musí být ve tvaru, kdy ve dvojkovém zápisu nesmí být přerušen sled jedniček z levého kraje. Maska 255.255.255.0 ve dvojkovém zápisu se zapisuje takto: 11111111.11111111.11111111.00000000 z tohoto vyplývá, že nelze použít jakoukoliv masku sítě (například nelze použít masku 255.255.251.0, protože tato vypadá ve dvojkovém zápisu následovně 11111111.11111111.11111011.00000000 a tudíž není splněna podmínka nepřerušeného sledu jedniček).

IP protokol verze 4 je dnes nejpoužívanější a nejrozšířenější komunikační protokol protokolů.

3.3.1.2. IP verze 6

Vlivem obrovské celosvětové expanze internetu je však celý rozsah IP adres IP protokolu verze 4 dnes již na hranici plného obsazení. Z tohoto důvodu je vyvíjen nový protokol na obdobném principu nazvaný IP protokol verze 6.

Základním rozšířením je rozsah adres, které jsou složeny již ze 128 bitového čísla (u TCP/IP verze 4 byly adresy „jen“ 32 bitové). V této novější verzi je již v základním nastavení zprovozněno několik nových funkcí. Je zde podpora vyšší bezpečnosti dat (automatická podpora IPsec – IP security protokolu). Je zde zvýšena podpora pro mobilní zařízení. Dále se zvyšuje podpora QoS (Quality of Service), jde o podporu a lepší zajištění chodu služeb, kdy na základě pravidel dostanou přiřazené větší pásmo služby pro video a hlas na úkor například přenosu mailů a podobně. Záleží na nastavených pravidlech. Je zde výrazně zlepšeno rozdělování packetů (fragmentace).

IP verze 6 není zpětně kompatibilní pro plnohodnotný provoz s IP verze 4, pokud tedy chceme nebo potřebujeme využívat obě verze IP protokolu je zapotřebí používat nějaký router nebo převodník, tak aby bylo možné pracovat se zdroji na dvou různých verzích protokolu.

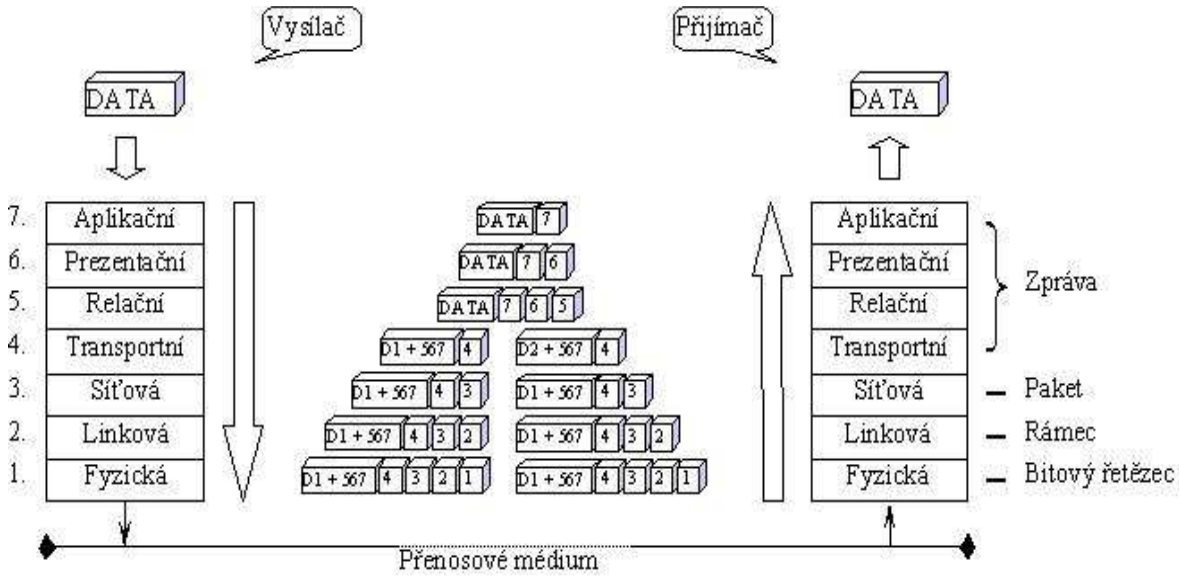
3.3.1.3. NETBEUI

NETBEUI (NETBios Extended User Interface) protokol [Šetka, 2003, s. 40] byl vytvořen firmou Microsoft a určen pro sítě malého rozsahu. Vyznačoval se velmi snadnou instalací, ale bez možnosti směrování a konfigurace. Každý počítač měl v sobě zabudovanou službu browser, která hledala další dostupná zařízení na síti s tímto protokolem. Pokud žádné nenašla, přiřadila si funkci Master browser. Master browser však mohl být na síti jen jeden. Tuto funkci z pravidla zastával počítač nebo server s nejrychlejší odezvou, který pak poskytoval data ostatním zařízením o sousedech na síti. Pokud se připojilo nějaké nové zařízení do sítě, snažilo se převzít onu roli master brokeru, což mnohdy vedlo k poněkud pomalejšímu zobrazení sousedících zařízení. V některých zařízeních se používá i dnes, ale už jen jako nadstavba TCP/IP protokolu.

3.3.1.4. IPX/SPX

Systém od firmy Novell, který byl svého času nejrozšířenější síťový systém na světě, využíval svůj vlastní komunikační protokol IPX/SPX (Internetwork Packet Exchange / Sequenced Packet Exchange). Tento systém byl bezpečnější a spolehlivější než systémy jiných výrobců. Dnes se však využívá méně, zejména z důvodu horší podpory ze strany koncových zařízení.

3.3.1.5. Komunikační vrstvy



OBR. 6 Toky dat v komunikačním modelu ISO/OSI, ZDROJ: SITE.BOREC.CZ

Jednotlivé vrstvy komunikačního modelu ISO/OSI a podobně tak i jiných komunikačních modelů (TCP/IP a podobně) si mezi sebou předávají data. Každá vrstva může předávat data jen vrstvám ve svém přímém sousedství. K předání dat mezi zařízeními dojde za podmínky, že všechny vrstvy od té nejspodnější po vrstvu předávající požadovaná data jsou funkční a svolné k přenosu dat.

V následujícím obrázku (Obr. 7) jsou popsané jednotlivé vrstvy komunikačního modelu ISO/OSI, pro jakou funkci jsou jednotlivé vrstvy definovány a jsou zde uvedeny i příklady jejich možného využití.

vrstva		jednotka	Funkce vrstvy	Příklad
7	Aplikační	Data	Síťové procesy pro aplikaci, ověření uživatelů, vše závislé na aplikaci	Telnet, FTP
6	Prezentační	Data	Reprezentace dat a šifrování, kóduje data pro přenos	MIDI, MPEG
5	Relační	Data	Spojení mezi aplikacemi, Správa session. Udržuje spojení mezi dvěma počítači.	NetBIOS
4	Transportní	Segmenty (segments)	Spojení systémů, zajišťuje kompletní přenos dat, kvalita služby. Řeší odesílání dat od zdroje k cíly pomocí segmentace a potvrzování.	TCP, UDP
3	Síťová	Pakety (packets)	Logická adresace - routování, určení cesty packetu.	IP, ICMP, ARP, RIP
2	Linková	Rámce (Frames)	Fyzická adresace MAC, datový tok, synchronizace rámců, detekce chyb.	Ethernet, FDDI, Token, RING, PPP, SLIP
1	Fyzická	Bity (Bits)	Fyzické parametry linky, optika, kabel, rádio. Signály a binární přenos.	802.11g, 10Base-T, RS232

OBR. 7 Vrstvy komunikačního modelu ISO/OSI

3.3.2. Služby podporující chod sítě

Různé aplikace nebo koncová zařízení, která poskytují ostatním zařízením na síti nějakou službu a tím podporují chod sítě. Případně usnadňují připojení nových koncových zařízení ke stávající síti nebo dokáží zařadit koncové zařízení do správné sítě nebo omezit koncovému zařízení jeho provoz na síti až po úplné odpojení od sítě.

3.3.2.1. DNS

Nejvyužívanější službou na síti je služba DNS (Domain Naming Systém) [Hunt, 1997, s. 54] ta služba má za úkol přiřazovat jménům (například www.crc.cz nebo K110.crc.local a podobně) IP adresu zdroje, kterou má (služba, počítač a jiné) přiřazenou a na kterou se má komunikace mezi koncovými zařízeními nasměrovat, aby došlo k přenosu požadovaných dat.

DNS má hierarchickou strukturu jmenné konvence. Neveřejné sítě si mohou určit jména, jak chtějí. Ve veřejné části (tedy na internetu) je určeno několik základních domén I. řádu (CZ – národní doména České republiky, COM – doména pro komerční sféru, ORG – doména pro neziskové organizace a další). Každý, kdo chce využívat nějaký název pro své zdroje (například pro prezentaci firmy) si může zaplatit registraci libovolného názvu (tedy pokud tento název již není využíván) pro použití názvu v doméně II. řádu (například crc.cz, seznam.cz, microsoft.com a podobně).

3.3.2.2. WINS

Obdobnou službou, jako je DNS, je i služba WINS (Windows Internet Naming Service). [Osif, 2001, s. 328] Má stejnou funkci, také přiřazuje jméno konkrétní IP adrese, ale nemám hierarchickou strukturu. Každé zařízení, které ví o WINS službě (má ve své konfiguraci přiřazenu adresu pro službu WINS) samo řekne svůj název a svou IP adresu a požádá i zápis do tabulky WINS, aby dalo ostatním zařízením využívající WINS o sobě vědět. Zápisy v tabulce systému WINS se aktualizují například při restartu zařízení. Tento systém se využívá zejména v lokálních sítích založených na platformě firmy Microsoft.

3.3.2.3. DHCP

Pro připojení koncového zařízení do sítě bez nutnosti manuální konfigurace síťového rozhraní nám pomůže služba DHCP (Dynamic Host Configuration Protocol). [Šetka, 2003, s. 123] Tato služba přiřadí každému koncovému zařízení, které má nastaveno získat konfiguraci sítě automaticky z DHCP, alespoň základní konfiguraci síťového rozhraní (IP adresu, masku sítě, výchozí bránu). Takto je možné nastavit daleko více

možností využívající nastavení sítě, jako WINS, DNS server, přiřazení zařízení k doménovému jménu a podobně. Každý DHCP server má přidělen určitý rozsah adres, ze kterého dynamicky adresu přiděkuje koncovým zařízením. Běžně se tak stává, že jedno zařízení má adresu stále stejnou a jinému zařízení se adresa může různě měnit.

3.4. Systémy a aplikace

Systémy jsou neprázdné, účelově definované skupiny prvků a vazeb mezi jednotlivými prvky, které na základě svých vstupů a výstupů, vykazují kvantifikovatelné chování. V IT tento název (Systém) používáme pro označení takových softwarových (SW) a hardwarových (HW) řešení, která jsou schopna pracovat samostatně nebo již jsou natolik robustní a komplexní, že dokáží vyvolat dojem samostatnosti. Naproti tomu aplikace, jsou SW produkty, ktreré pro svou práci využívají zdrojů systému nebo pomoocí systému něco ovládají.

3.4.1. Systémy serverové

Serverové systémy pracují na koncových zařízeních označených jako server. Jejich hlavním úkolem je, nabídnout k dispozici dostupné a definované zdroje tohoto zařízení ostatním zařízením na síti.

Mezi serverové systémy patří mnoho systémů od různých výrobců. Některé jen pro ilustraci zde zmíníme.

Systém UNIX – [Klander, 1998, s. 487] Původně vyvinutý firmou At&T se stal jedním z nejvíce využívaných systémů na straně serverů a velkých sálových počítačů (Mainfraimů), který umožňuje plně využít hardwarových prostředků zařízení na kterých je provozován. S nadsázkou se dá říci, že je tolik verzí tohoto systému, na kolika zařízeních je provozován. Jeho výhody jsou ve výkonu a přesnosti.

Systém WINDOWS server – [Šetka, 2003, s. 2] od firmy Microsoft byl vyvinut v několika různých verzích. Velice úspěšná firma v oblasti systémů pro osobní počítače vyvinula několik verzí systému i pro serverové zařízení, aby zajistila svým zákazníkům kompletní služby od jednoho dodavatele. Výhodou systémů od firmy Microsoft je jejich rozšířenost a uživatelská přívětivost. Snadno se dají instalovat a konfigurovat, za cenu horšího využití používaného hardware a mnohdy instalovaných i nepotřebných nebo nechtěných součástí.

Systém Novell Network - [Currid, 1993, s. 80] tento systém vyvinula a prodávala firma Novell. Býval to jeden z nejrozšířenějších serverových systémů na světě. Bohužel se firma novel soustředila jen na serverové systémy a přístup uživatelů zajišťovala pomocí klientských aplikací. Což vedlo ke zpomalování pracovních stanic uživatelů a následně k odlivu zákazníků a k opouštění tohoto systému.

Zde jsem uvedl nejznámější serverové systémy, které měli nebo mají nějaký zásadní vliv na vývoj a provoz serverových systémů.

3.4.1.1. Katalog sítě

Katalogem sítě rozumíme službu běžící na síti s hierarchickou strukturou (stromovou strukturou), která se stará o zařazení všech zdrojů na síti dostupných a zároveň se stará i o přístupy k těmto zdrojům. Jsou zde zařazeny účty jednotlivých uživatelů, jejich členství ve skupinách, jejich přístupová omezení k jednotlivým zdrojům na síti (diskovému prostoru, aplikacím, tiskárnám, terminálům a podobně).

Nejrozšířenější katalog je dnes Active Directory (AD) firmy Microsoft či obdobný produkt od firmy Novell nazvaný eDirectory. Ale existují i další.

3.4.1.2. Tisk

Jednou z nejzákladnějších činností je tisk nějakých výstupů. Nespornou výhodou, je síťový tisk, kdy koncové zařízení (tiskárna) je umístěné v jiných prostorách (například ve skladu) než kde se nachází žadatel (uživatel a počítač nebo terminál na kterém požadavek zadává) o tento výstup a také v jiném místě než jsou uložená data. Variant síťového tisku je několik. Od obyčejného sdílení lokální tiskárny (tiskárny připojené přímo kabelem k počítači), přes tiskárny připojené pomocí svého síťového rozhraní do datové sítě, až po velké tiskové servery umožňující konkrétní logiku ve využívání tiskových front a jejich dynamickému přiřazování koncovým zařízením (tiskárnám, které se starají o výsledný tisk).

3.4.1.3. Vzdálené přístupy

Samostatnou kapitolou jsou vzdálené přístupy, tyto přístupy se zřizují pomocí různých technických řešení z důvodů například dnes velmi oblíbené home office (práce z domova) nebo standardní práce ze služebních cest. K těmto účelům

se používá několik variant technických řešení, jak zpřístupnit data firmy pro své zaměstnance, kontraktory nebo pro širokou veřejnost.

VPN – (Virtual Private Network) Vytváří šifrované spojení (tak zvaný tunel) mezi koncovým zařízením v podobě nějaké softwarové aplikace (na straně uživatele v externím prostředí firmy) a nějakým serverem (většinou firewallem s veřejným rozhraním na straně firmy). Prostřednictvím VPN je pak následně koncovému uživateli umožněno pracovat z různých míst vně areálu firmy, jako kdyby byl v areálu, jsou mu takto zpřístupněny některé nebo dokonce všechny zdroje sítě úplně stejně jako by se nacházel v prostorách firmy.

Terminál server (TS) – [Osif, 2001, s. 354] Tento server se specifickou funkcionalitou má za úkol zpřístupnit uživatelské prostředí vzdáleně se připojujícím uživatelům. Což vede ke vzdálenému připojení uživatelů do firmy s možností pracovat dle uživatelských práv se zdroji datové sítě, jako kdyby byl uživatel připojen v areálu firmy, a vzdáleně se přenáší pouze obrazová informace a vstupy od uživatele (klávesnice, myš a podobně). Což značně snižuje objem přenášených dat a následně vytížení veřejných linek. Dále tento způsob přístupu zásadně zlepšuje stabilitu systému, protože ani případné přerušení spojení mezi TS a uživatelem neznamená ztrátu dat. Pouze dojde k odpojení od session na TS, ke které se uživatel může znovu připojit a pokračovat tak v nedokončené práci.

Terminálové služby má, v nějaké omezené podobě, téměř každý operační systém určený pro počítače nebo servery. Nebo lze zvolit nějaké jiné dodavatelské řešení jako je například systém CYTRIX, případně Microsoft Terminal server či jiné.

3.4.1.4. Data na mobilních zařízeních

Současná doba si žádá mít dostatek aktuálních informací prakticky v jakoukoli dobu a na jakémkoli místě se nacházíme. Proto přístupnost dat (minimálně alespoň nějaké omezené části dat) společnosti je pro její zaměstnance a zákazníky klíčové, což vede ktak dynamickému rozvojitohoto oboru. Pokud tedy chce společnost být úspěšná na trhu, nemůže si dovolit opomenout tuto možnost přístupu pro své zákazníky či zaměstnance zprovoznit. Jedná se tedy o možnost přístupu k datům společnosti na mobilních, tedy přenosných, ale méně výkonných zařízeních jako jsou tablety nebo mobilní telefony označované jako chytré telefony.

3.4.2. Systémy aplikační

Aplikační systémy neboli systémy skládající se z více na sobě nezávislých softwarových modulů, které jsou mezi sebou propojené a sdílejí svá data do různých částí jednotlivých modulů, tak aby se data pouze rozšiřovala, ale neduplikovala, tudíž aby nebyla stejná data v systému na několika místech najednou a nezabírala tak zbytečně místo na disku nebo v paměti.

3.4.2.1. Komunikace

Pro každou společnost je zásadní jakým způsobem dokáže pracovat s informacemi, jak tyto informace dokáže předávat v interní komunikaci [Přikrylová - Jahodová, 2010, s. 18] (komunikace v rámci firmy mezi zaměstnanci, odděleními, divizemi, vedením společnosti, v rámci jednotlivých pracovních týmů i mezi různými týmy a podobně) a také jak se dokáže prezentovat společnost v očích veřejnosti, nebo jak společnost prezentuje své produkty veřejnosti a především pak cílové skupině svých zákazníků.

Dnes nejrozšířenějším komunikačním kanálem je komunikace pomocí elektronických zařízení, jako je telefonní hovor, elektronická pošta, online komunikátory nebo různé, dnes celosvětově velmi oblíbené, sociální sítě a další způsoby.

3.4.2.1.1. Elektronická pošta

Jedním z dnes nejrozšířenějších komunikačních kanálů je elektronická pošta. [Šetka, 2003, s. 619] Jedná se o obdobu klasické dopisní pošty, ale prostřednictvím elektronických zařízení. Jako má každý svou adresu pro doručování klasické papírové dopisní pošty, tak v elektronickém světě má také nějakou adresu ve formátu elektronickém (například jaroslav.duda@crc.cz – část adresy před znaménkem @ je prakticky libovolná – každý si zde může zadat cokoliv, dle své fantazie (musí se pouze vyvarovat některých speciálních znaků *, !, a podobně) při zakládání poštovní schránky, druhá část pak obsahuje doménové jméno). Stejně jako v klasické poště je i v elektronické obdobě zajištěno pouze jediné a to je příjemce elektronické pošty dle zvolené adresy. Odesilatel je vždy anonymní! Příjemce může mít i několik různých elektronických adres. Záleží pouze na každém uživateli, zda a kolik adres si vytvoří, na různých free (bezplatných) e-mailových službách dostupných volně na internetu, kde zpravidla stačí pouhá registrace.

3.4.2.1.1.1. Protokol SMTP/SMTPS

Rodina TCP/IP protokolů má jeden protokol určený pro předávání elektronické pošty mezi jednotlivými uzly (servery) na internetu. SMTP (Simple Mail Transfer Protocol) [Šmrha - Rudolf, 1995, s. 81] případně jeho šifrovaná varianta SMTPS. Šifrování se budeme věnovat v některé další kapitole.

SMTP protokol je určen pro odesílání elektronické pošty od uživatele na server nebo pro předávání elektronické pošty mezi jednotlivými servery.

Každý mail se předává na cílovou adresu dle doménových jmen, na základě překladů v DNS přiřazeným MX záznamům. MX záznam v DNS je záznam, na který server má být doručována adresa pro doménu (například crc.cz). Na internetu nelze mít konkrétní adresu víc než jednou, každá adresa musí být unikátní.

3.4.2.1.1.2. Služba router

Na každém serveru pro elektronickou poštu běží nepřetržitě služba router, která se stará (dle nastavení od administrátora) o kontrolu předem definovaných front, určených pro řazení elektronické pošty a o následné doručení této pošty na nadřazený SMTP server nebo dle MX záznamů v DNS o doručení elektronické pošty přímo určenému SMTP serveru pro danou doménu.

3.4.2.1.1.3. POP3/POP3S/IMAP/IMAPS

Další protokoly z rodiny TCP/IP protokolů pro elektronickou poštu jsou protokoly POP3 (The Post Office Protocol verze 3) a IMAP (Internet Message Access Protocol) a jejich šifrované varianty POP3S a IMAPS. Jedná se o protokoly určené pro komunikaci mezi serverem, na kterém je vytvořena schránka pro konkrétné adresu elektronické pošty, a programem (aplikací), kterou uživatel využívá pro usnadnění práce s elektronickou poštou. Tedy její čtení, řazení mazání, vyhledávání a podobně.

Rozdíl mezi těmito protokoly je v komunikaci se serverem. POP3 protokol primárně vytvoří kopii zprávy v lokálním úložišti uživatelské aplikace a následně elektronickou poštu na serveru podle předem nastavených pravidel smaže či po nějakou omezenou dobu zachová. Pomocí POP3 protokolu se tedy nejprve vytvoří kopie zprávy a s touto kopií se následně pracucuje.

IMAP protokol se chová naprosto odlišně, jeho primární funkcí je zpřístupňovat elektronickou poštu přímo ze schránky na serveru, tedy nevytváří se žádná kopii zpráv, ale pracuje se přímo s dokumenty ve schránce vytvořené na serveru. I tento protokol umožňuje vytváření kopií zpráv, například pro práci tak zvaně offline, tedy bez možnosti přímého připojení do schránky v reálném čase.

3.4.2.1.1.4. Aplikace elektronické pošty

Aplikace a systémy pro práci s elektronickou poštou musíme rozdělit do dvou kategorií. První kategorii tvoří systémy serverové, pracující prakticky nepřetržitě nebo pokud možno s minimálními výpadky v řádu hodin. Jedná se o systémy, starající se o komunikaci a předávání dokumentů mezi jednotlivými servery spravujícími adresy a zároveň schránky uživatelů. Mnohdy poskytují další služby navíc, jako je například řazení schránek do skupin, vytváření mailing listů, vytváření aliasů (přiřazení více adres jedné schránce a podobně). Představitely této části jsou především Microsoft Exchange server, Lotus Domino server nebo menší řešení od české firmy jako je Kerio Connect a spoustu dalších.

Druhou kategorii pak tvoří aplikace uživatelské, tedy software umožňující uživateli pracovat se svou elektronickou poštou. Tedy minimálně alespoň základní úkony pro práci s elektronickou poštou, jako je čtení, vytváření, mazání případně editaci a další možné úkony potřebné pro práci s elektronickou poštou, které uživatel využívá (řazení do složek, automatické odpovědi a podobně). K těmto účelům se využívají tak zvaní poštovní klienti. Jedná se o aplikace instalované lokálně či na přenosném USB flash disku. Případně se využívá WEBKLIENT neboli přístup do schránky pomocí nějakého internetového prohlížeče.

3.4.2.1.1.5. Online komunikace

Online komunikace je jakási obdoba výměny elektronické pošty, ale v reálném čase, tedy kdy ve stejném okamžiku spolu komunikují minimálně dva (lze i více najednou) uživatelé. Pro tento způsob komunikace se využívají různé aplikace, tak zvané mesangery. V České republice je nejrozšířenější ICQ, následován například SKYPEm, MSM (Misrosoft Messenger) a dalšími. Tyto Messengery jsou zdarma (provoz je hrazen zobrazovanou reklamou), ale jejich určení je pouze pro soukromou komunikaci,

tedy pro komunikaci v rámci nějaké komerční či korporátní sítě je zakázáno. Toto omezení je v mnoha případech slušně řečeno nedodržováno. Pro korporátní sféru jsou určeny jiné produkty (například Lotus Sametime), které jsou zpoplatněné, ale je možné zprovoznit jejich napojení i na ostatní sítě určené pro soukromou komunikaci. Mnohdy nám tyto online komunikátory ukazují stav, zda je uživatel připojen nebo není, tedy zda sedí u „svého“ počítače. Někdy i tato informace stačí ke sdělení informace, že lze dotyčnému zavolat. Dnešní messengery nabízejí mnohem víc než jen předávání textových zpráv v reálném čase, ale nabízejí i přenos hlasu nebo videa a částečně jsou schopné nahradit klasické telefonní přístroje (pevné i mobilní) nebo dokonce vylepšit komunikaci mezi uživateli při videohovorech.

Zvláštním způsobem online komunikace pak jsou sociální sítě (například Facebook, Twiter, Linkedin a další), kde uživatelé sdílí údje ze svého soukromí, komunikují online se svými kamarády, spolupracovníky i ostatními uživateli. Tyto sítě jsou dnes velmi rozšířené a oblíbené. Mnohdy mají veliký vliv na ovlivňování názorů ostatních spoluuživatelů těchto sociálních sítí.

3.4.2.1.1.6. VOIP

VOIP (Voice Over Internet Protokol) [online, www.fyan.cz] Jedná se moderní jednoduchou službu, která využívá pro přenos hlasu datové přenosy. Každý telefonní přístroj má přiřazené telefonní číslo, jako tomu je u klasických telefonních přístrojů. Pro přenos hlasu se nepoužívá telefonní sítě, ale sítě datové. Což v dnešní době vede ke snížení nákladů za provoz telefonních přístrojů, tedy hlavně za poplatky spojené s provozem těchto přístrojů.

3.4.2.1.2. Informační systém

Informační systém (IS) je soubor lidí (zaměstnanci společnosti) plus data (která má společnost k dispozici a může s nimi nějakým způsobem nakládat) plus ICT (informační a komunikační technologie, které společnost využívá). Způsob využívání a možnosti informačního systému má zásadní vliv na celou společnost, na její způsob práce, komunikace se zákazníkem, konkurence schopnost či samotné fungování společnosti interně či externě tedy ve vztahu komunikace mezi zaměstnanci i komunikace a prezentace s okolím společnosti.

3.4.2.1.2.1. Koordinace zaměstnanců

Každá společnost (pakliže má několik zaměstnanců) si musí, alespoň formálně, vymezit nějakou organizační strukturu zaměstnanců. Každé vytvořené pracovní pozici by měla definovat její pravomoci a zároveň pracovní náplň a způsob hodnocení. Organizační struktura společnosti je hierarchická (stromová) struktura jednotlivých oddělení (divizí, sekcí, provozů a podobně) společnosti, ke kterým jsou připojeny jednotlivé pracovní pozice a k těmto pozicím jsou následně přiřazeni konkrétní zaměstnanci a jejich pracovní náplň, mzdové ohodnocení a pravomoci vyplývající ze zastávání dané pracovní pozice. Definicí organizační struktury společnost definuje informační kanály, pomocí kterých vedení společnosti informuje zaměstnance o plánech a cílech společnosti a pomocí kterých se snaží vytyčených cílů dosáhnout.

Každý zaměstnanec musí být zařazen do formální organizační struktury, dle které vykonává odpovídající práci a následně je hodnocen. Nicméně tento zaměstnanec může být začleněn i do dalších organizačních skupin, které se vytvářejí za nějakým účelem. Například na základě nějakých úkolů, projektů a podobně. Jedná se mnohdy o týmy a subtýmy zajišťující například bezpečnost na pracovišti, nebo týmy pro hledání a zdokonalování stávajících procesů, nebo pro vytváření nových procesů ve společnosti. Případně zajišťující nějaký projekt či speciální zakázku.

3.4.2.1.2.2. Účetní systém

Každá společnost podnikající na území České republiky musí mít živnostenský list nebo musí být zapsaná v obchodním rejstříku. Pro každou takto vytvořenou společnost platí zákony České republiky, které mimo jiné stanovují podmínku pro vedení daňové evidence (z minulosti známé jako jednoduché účetnictví, vhodné pro menší firmy, kterým ze zákona nevyplývá povinnost vést jinou formu účetnictví) nebo podvojného účetnictví. Pro zpracování této agendy slouží nějaký účetní systém, který se mnohdy skládá z různých modulů. Jednotlivé moduly spolu zpracovávají obdobná data. Základním modulem je vedení účetnictví, vykazování daní pro finanční úřady, stanovovaní obratů firmy či evidence aktuálních stavů finančních prostředků, evidence hmotného a nehmotného majetku a ze zákona vyplývající odpis hodnot. Speciálním modulem bývá zpracování mezd a odměn a odvodů pro zaměstnance a majitele společnosti.

3.4.2.1.2.3. Skladové hospodářství

Velmi důležitým systémem pro společnost je aplikace pro evidenci a nakládání se zbožím, které má firma skladem (zboží určené pro prodej zákazníků, náhradní díly pro potřeby firmy, produkty a meziprodukty pro výrobu a podobně). Takovéto systémy jsou založené většinou na nějakém databázovém systému a umožňují evidenci a nakládání s jednotlivými položkami ve skladu. Samozřejmostí jsou inventurní sestavy položek, evidence pohybů skladových položek, jejich obrátkovost za určité období a podobně.

3.4.2.1.3. Společná data

Každý zaměstnanec společnosti při své práci generuje nemalé množství dat, ať už pro svou vlastní potřebu, nebo pro potřebu někoho dalšího (ať pro zaměstnance společnosti, nebo pro dodavatele případně odběratele, nebo pro externě spolupracující jiný subjekt a podobně). Pro lepší zastupitelnost zaměstnanců (například z důvodu nemoci, dovolených a podobně) nebo pro spolupráci jednotlivých oddělení případně týmů, je zapotřebí zajistit kontinuální fungování společnosti. K těmto zmíněným účelům (případně i jiným, dalším, zde nespecifikovaným účelům) je nutné umožnit vytvořená data sdílet společně s dalšími zaměstnanci nebo subjekty.

3.4.2.1.3.1. Diskový prostor

Ke sdílení dat mezi uživateli se využívá ve velké míře nějaký společný diskový prostor, ke kterému má přiřazená různá práva (čtení, zápis, editace, mazání či případně nějaká další) omezený počet uživatelů, kteří s těmito daty z nějakého důvodu potřebují pracovat. Pakliže se jedná o nějaká konkrétní data určená všem zaměstnancům lze tento diskový prostor snadno zpřístupnit, jedná se pouze o nastavení správných přístupových práv.

Představitelem této skupiny systémů pro sdílení dat je například Souborový server, [Shatt, 1994, s. 44] který svou diskovou kapacitu zpřístupní pomocí vytvořeného sdíleného adresáře s omezením přístupů dle přiřazených přístupových práv. Každý souborový server může svůj diskový prostor rozdělit a vytvořit tak více sdílených diskových prostorů. S těmito prostory může administrátor serveru různě pracovat (zvětšovat, zmenšovat, přesouvat, zálohovat, archivovat a podobně).

Dalším představitelem pro sdílení souborů (obsahující potřebná data) je FTP server [Šmrha - Rudolf, 1995, s. 75], který využívá obdobně diskový prostor jako souborový server, ale liší se zejména použitým protokolem (ftp na portu 20 nebo 21) pro přístup k tomuto diskovému prostoru. Je primárně určen jen k uchování a předávání dat, ale už nejde s těmito daty pracovat přímo z FTP serveru. Pokud s těmito daty potřebuje uživatel pracovat, musí si tato data nejprve uložit lokálně, následně je zpracovat (provést nějakou změnu) a po tomto zpracování upravená data znovu nahrát na FTP server pro další sdílení s ostatními uživateli. Obdobně i zde je omezení přístupu řešeno přístupovými právy pro jednotlivé uživatele.

Dalším možným prostředkem pro sdílení dat jsou externí disky nebo flash paměti, jedná se o sdílený prostor, přímo připojitelný nejčastěji pomocí USB portu k počítačům uživatelů. Data se sdílejí pomocí postupného připojování k jednotlivým počítačům, tedy nejsou k dispozici všem uživatelům najednou ve stejnou dobu. Práva na soubory se zde nijak neomezují. Uživatel, který má možnost si konkrétní externí disk nebo flash paměť připojit ke svému počítači, získá právo pracovat se všemi daty na těchto zařízeních uloženými. Za pomoci nějaké softwarové aplikace lze tyto přístupy omezit, například zašifrovat některá uložená data nebo dokonce celý externí disk, takto ošetřená data jsou přístupná po zadání předem určeného hesla. Některé externí disky mají možnost připojení do datové sítě, kde dokáží pracovat na stejných principech, jako dříve zmíněný souborový server nebo FTP server.

3.4.2.1.3.2. Intranet/extranet

Přednosti internetu, jeho zpřístupňování informací široké veřejnosti našlo uplatnění i v informačních systémech společností. Pro čtení informací stačí nějaký jednoduchý prohlížeč s minimálními nároky na hardware. Jednoduchost HTTP (Hypertext Transfer Protocol) vedla k vytvoření jakých si elektronických nástěnek využívaných pro informovanost zaměstnanců. Intranet představuje prezentaci výsledků firmy, plánů vedení, hodnocení zaměstnanců, prezentace jednotlivých oddělení a podobné informace nebo sdělení určené pro vnitřní potřebu firmy a využívajících stejných systémů a prostředků, jako se využívá v prostředí internetu. Za podmínky, že z internetu tyto informace nejsou veřejně přístupné.

Extranet je naproti intranetu prezentace firmy do veřejného světa internetu. Tedy většinou zcela veřejné informace, které společnost chce prezentovat internetové veřejnosti. Například personální obsazení vedení společnosti, tiskové zprávy, informace o výrocích a produktech firmy a další informace. Jedná se o marketingovou prezentaci firmy. Extranet, ale také slouží pro přístup zaměstnanců, dodavatelů a odběratelů k informacím, které jsou pro ně určené, ale nejsou zcela veřejné (například směrnice a normy firmy, podklady pro výběrová řízení a podobně). Tyto informace jsou většinou přístupné po zadání nějakého uživatelského jména a hesla.

3.4.2.1.3.3. Databáze

Pro efektivnější práci s daty se využívají databáze a databázové systémy [Werner, 1996, s. 241], které snižují redundanci uložených dat (ukládání stejných dat vícekrát) a zvyšují jejich aktuálnost (stačí aktualizovat na jednom místě). Tyto systémy umožňují, vytváření a zpracování metadat (metadata – jsou data o datech). Databáze dělíme podle jejich práce s daty na relační (data uspořádává do tabulek – relací) a objektové (jednotlivá data jsou řazena do objektů).

Databázové systémy pracují na principu transakčních požadavků. Uživatel se databáze zeptá na to, co chce. Za pomoci nějakého dotazovacího jazyka (například SQL – structured query language, OQL – object query language, DQL – data query langure a další). Přitom mu je lhostejné, jak se k těmto datům dostane. O zpracování jednotlivých požadavků se stará SŘBD (systém řízení báze dat), který je dodáván jako součást databázového systému.

Komerčně nejprodávanější, nejúspěšnější a nejrozšířenější databázové systémy jsou Oracle Database od společnosti Oracle, nebo od společnosti Microsoft SQL server toto jsou velké robustní systémy pro zpracovávání a uchovávání velkého množství dat. Pro menší firmy jsou pak dostatečné menší řešení, jako jsou Microsoft Access (určený pro malé „kancelářské“ databáze) nebo nějaké open source řešení (řešení s možností provedení úprav pro vlastní potřeby a dle vlastních požadavků, lze zasahovat přímo do zdrojového kódu), které je mnohdy k dispozici zdarma.

Objektově orientované databáze jsou relativně nová technologie, která ještě není tolik rozšířená v komerčním světě. Její výhodou je dědění vlastností od nadřazených objektů a tím dochází k ještě větší redukci objemu uchovávaných dat.

3.4.2.1.4. Společné aplikace

Společné – sdílené aplikace je takový software, který využívá více uživatelů. Jedním typem společné aplikace je lokální instalace na každý počítač ve společnosti a data v této aplikaci vytvořená lze následně sdílet s ostatními uživately přičemž je zajištěno jejich snadné otevření či editace někým jiným než jen autorem.

Druhým typem sdílených aplikací jsou aplikace spouštěné z nějakého společného diskového prostoru a jejich používání je omezeno například počtem současně využívajících uživatelů pro danou aplikaci. Tento typ aplikace je v korporátní sféře velmi rozšířen, jelikož nezabírá zbytečně prostor na každém počítači, ale zároveň je dostupný nějaké skupině oprávněných uživatelů.

3.5. Zařízení – Aplikace s bezpečnostním aspektem

Hardwarová zařízení, případně aplikační software určený k zajištění nebo alespoň ke zvýšení bezpečnosti a ochrany dat a zařízení v majetku společnosti, jsou velmi důležité pro ochranu know-how a prostředků společnosti. Tyto bezpečnostní prvky jsou používány jako základní kameny bezpečnostní ochrany společnosti, ale často se také využívají jako preventivní kroky nebo rozšiřující články celého ICT systému společnosti. Tyto zařízení a aplikace se snaží omezit možné ztráty vzniklé náhlou ztrátou dat případně výpadkem systému z důvodu nějakého napadení firmy, výpadku nějakého zařízení, nebo sabotáže. Obor bezpečnosti je velmi široká oblast zavislá na možnostech podniku, na tom jak vysokou hodnotu mají nashromážděná data pro společnost. V nemalé míře se každá společnost musí chránit i před velmi rychle roustouci kriminalitou v kybernetickém světě.

3.5.1. Firewall

Základním stavebním kamenem každého ICT systému (pokud se nejedná o jakési dedikované pracoviště bez možnosti jakéhokoliv připojení k dalším zařízením nebo k nějaké datové síti) je zařízení pojmenované firewall [Werner, 1996, s. 403]. Jedná se o zařízení, které staví jakousi pomyslnou zeď mezi dvě zařízení, případně mezi dvě nebo více datových sítí.

Firewall je zařízení, které nesmí chybět v žádné společnosti ani domácnosti, pakliže využívají připojení do internetu. Internet neboli síť sítí je veřejný prostor přístupný prakticky komukoliv a ne každý ho využívá pouze s čistými úmysly. Proto je firewall nepostradatelný pro řízení přístupů z internetu do interní sítě společnosti (domácnosti) a zároveň dovoluje řídit i komunikaci do internetu. Firewally se využívají primárně pro oddělení interní sítě od sítě veřejné (internet) nebo od sítě z pohledu majitelů společnosti méně důvěryhodné než je vlastní interní síť. Například se firewall používá pro oddělení různých sítí, pokud v jednom areálu je více firem, které si spolu sdílí nějaká data a potřebují tedy přímou konektivitu mezi zdroji v obou sítích. Mnohdy se vytváří tak zvaná DMZ (Demilitarizovaná zóna), což je určitý bezpečnostní mezičlánek využívaný pro data přístupná z veřejné nebo externí sítě oddělená jedním firewallem na straně vnější a druhým firewallem na straně mezi DMZ a interní sítí. Mnohdy je toto řešení zajišťované jedním firewallem o více portech, které řídí komunikaci mezi jednotlivými porty. Lze nastavit pravidla pro prakticky jakoukoliv komunikaci mezi konkrétními porty, které firewall má k dispozici.

Firewally existují v různém provedení, jako jakási krabička s několika porty a nějakým administrátorským rozhraním pro jeho konfiguraci a správu, nebo jako software pracující na serveru nebo počítači s více porty a v neposlední řadě i každý počítač s možností připojení do nějaké sítě by měl využívat firewall v systému, případně nějaký softwarový produkt nainstalovaný z důvodu ochránění svých lokálních dat před nežádoucím přístupem.

Pakliže je firewall využíván směrem do veřejné sítě, je vhodné využít možnosti NAT (Network Address Translation), kdy firewall nahrazuje výchozí případně cílovou adresu adresou použitou u veřejného připojení, čímž chrání celou síť, protože celá interní síť (například o 800 počítačích) se ve veřejné síti poté vyznačuje jako zařízení o jedné adrese (tedy jako jeden počítač).

Firewally umožňují využívat překlady adres, řízení komunikace, mnohdy i určování šířky využívaného pásma pro jednotlivé porty. Mapování těchto portů a jejich překlad. Například lze vytvořit internetovou prezentaci na více serverech v DMZ, které v DMZ běží na standardních portech určených pro http (port 80), které z internetu jsou viditelné pod stejným doménovým jménem lišící se mapovaným portem (například www.crc.cz:8080 a www.crc.cz:8081). Jak je vidět, obě tyto prezentace

běží v DMZ, každá na jiném serveru, ale z internetu jsou přístupné, prakticky téměř pod stejným názvem, který se liší pouze v použitém mapovaném portu. Možnosti nastavení pravidel firewallu jsou v rámci elektronické komunikace téměř neomezené, tedy lze komunikaci úplně zakázat (i přes fyzické propojení není možná žádná komunikace) až po úplné otevření firewallu (lze tedy nastavit otevřenou komunikaci, kdy se firewall chová, jako kdyby vůbec nebyl).

3.5.2. Antivir

Bezpečnostním prvkem pro ochranu dat před jednoznačně škodlivým softwarem jako jsou různé viry, červy, rootkity, trojské koně a mnohá další, jejichž jediným cílem je získat neoprávněně nějaká data z napadeného počítače (většinou hesla a přístupové údaje), nebo nějakým způsobem poškodit uložená data, nebo dokonce poničit celý systém. Z těchto důvodů je zapotřebí využívat nějaké antivirové řešení.

Antivirové řešení [Werner, 1996, s. 32] a především její rezidentní část (permanentně běžící) má za úkol ochránit systém, na kterém je spuštěna, před aktuálně známými škodlivými softwary (viry a podobně). Aktuálnost antivirového programu je tedy v dnešní době velmi kritická záležitost, kterou je zapotřebí mít na paměti a nějakým způsobem je nutné tuto aktuálnost zajistit například pravidelným stahováním nových definicí od výrobce antivirového řešení (běžně k aktualizacím dochází minimálně jednou denně, mnohdy i častěji).

Pro kontrolu systémů, zda jsou tak zvaně čisté (tedy bez nějakého škodlivého software), se používají různé testy, heuristické analýzy a podobně. Tyto testy by měli být spouštěny pravidelně na každém chráněném systému a to z jednoho celkem důležitého důvodu. Jedná se o to, že antivirové systémy většinou reagují na zjištěný škodlivý software, tedy nedokáží tento software zachytit, pokud o něm nevědí. To nahrává právě šiřitelům těchto škodlivých programů, že alespoň po nějakou dobu (většinou než vyjde nová aktualizace) jsou se svým škodlivým programem úspěšní. Proto dnes nelze říct se stoprocentní jistotou, že systém není ničím napaden. Možná je, ale využívané antivirové řešení o škodlivém programu zatím neví.

Pokud mám systém, na kterém již je nějaký škodlivý software uložen nebo dokonce napadl některé soubory, antivirový systém za pomoci testů je schopen jemu známý škodlivý software buď ze systému odstranit, nebo minimálně detekovat. Pakliže antivirový

systém detekuje škodlivý program, nejprve se pokusí vyléčit napadené soubory, pokud se mu to nepodaří (třeba i za pomoci speciálních léčebných utilit), snaží se napadený soubor ze systému odstranit (nejprve uložit do karantény – karanténa je speciální místo, pro uložení napadených souborů, případně úplně smazat), což v případě napadení zaváděcích částí systému může vést až ke kolapsu tohoto systému a k nutnosti jeho následné reinstalace.

Mnohé společnosti pro zvýšení ochrany proti škodlivému softwaru používají více stupňovou antivirovou ochranu. První stupeň antivirové ochrany je nazývána ochrana na komunikačních uzlech společnosti (propojení s dalšími subjekty), tedy hlavně testování komunikace na firewallech a podobně. Druhý stupeň antivirové ochrany je použití antivirového systému na všech sdílených zdrojích společnosti, tedy na serverech nabízejících nějaký prostor pro sdílení informací nebo souborů (tedy většinou na serverech). Třetí stupeň antivirové ochrany se zabývá ochranou zařízení určených pro práci uživatelů, tedy většinou jde o ochranu jednotlivých počítačů a podobně.

3.5.3. Antispam

Antispam je specifický bezpečnostní prvek, který má za úkol uchránit uživatele od elektronické pošty o kterou nežádali a která si klade za cíl je oslovit s nějakou nabídkou (většinou se tedy jedná o reklamní poštu) případně se současným zasláním nějakého škodlivého softwaru. Objem této nevyžádané pošty je zhruba 80 - 95% z celkového objemu zaslané elektronické pošty, což jistě není zanedbatelné množství. Tato nevyžádaná pošta nejen, že zbytečně zahlcuje poštovní schránky uživatelů a zabírá podstatnou část jejich prostoru, ale především s ní uživatel stráví velikou spoustu času, který by jinak mohl věnovat smysluplné práci.

Antispamové filtry nabízejí spoustu možností využití. Stejně jako antivirová řešení se používají ve více stupních. Také se jejich databáze rozšiřují na základě veřejných black listů a definic (databáze elektronické pošty, odesílatelů, SMTP serverů a podobně, které byli na základě nějakého hodnocení označeny jako rozesílatele spamu a následně zařazeny do veřejných databází), princip je obdobný jako u antivirových systémů. Také v tomto případě je nutné zajistit aktuálnost dat. Prvním stupněm bývá předřazení antispamového filtru před mail server, tedy nejprve projde elektronická pošta antispamovým řešením a pokud splní stanovené podmínky

je následně doručena na mail server (není nasazeno vždy, ale je to jeden ze způsobů řešení). Druhým stupněm je antispamový filtr integrovaný do mail serveru (toto řešení je velmi rozšířené). Posledním stupněm je pak antispamové řešení na koncovém zařízení kde se spouští nějaký klient elektronické pošty. Tato řešení mnohdy bývají součástí antivirového systému, kdy dodavatel antivirového systému zároveně umožňuje i využití antispamových filtrů.

3.5.4. Zálohování

Ochrana dat není jen zajištění bezpečnosti proti nějakým možným útokům, nebo proti ohromnému množství existujícího a stále nově se objevujícího škodlivého softwaru. Pod ochranou dat [Shatt, 1994, s. 349] také rozumíme možnosti, kdy svá data chráníme před ztrátou, nebo poškozením z důvodů jako je například nechtěné smazání, případně nekorektně provedené změny v datech a podobně. K těmto účelům nám slouží systémy, které umožňují vytvořit nějakou zálohu dat.

Mnohdy se jedná o pouhou kopii dat uložené na dalším místě, případně na několika místech (čím větší počet kopií, tím samozřejmě větší jistota, že o data nepřijdeme). Vhodné je k tomuto účelu využít k tomuto účelu vyhrazených diskových polí nebo externích disků. Je to velmi snadná varianta, která však vyžaduje spoustu diskového prostoru. Jedná se o jakousi redundanci dat a mnohdy i několika násobnou.

Pro sofistikovanější zpracování problematiky zálohování se využívá nějakého zálohovacího systému (například Legato, ARCserv a další). Tyto systémy pracují na základě pravidelných zálohovacích procesů (někdy nazvané jako joby), které dle zadaných pravidel provedou automaticky zálohu. Některé umožňují dokonce zálohu online, tedy kompletní zálohu systému za provozu, toto se využívá například u databází nebo u dalších systémů, které neustále pracují se svými daty, a není tedy nutné provádět nějakou časově náročnou odstávku systému z důvodu provedení zálohy.

Pro zefektivnění doby potřebné pro provedení zálohovacích jobů se využívají tři základní způsoby zálohování. Každá společnost si má možnost zvolit, jakým způsobem si bude, a zda vůbec, své data zálohovat a samozřejmostí je i následná obnova dat z provedených záloh, která je neméně důležitá. První způsob je nejnáročnější na dobu potřebnou pro provedení zálohy, jedná se o full zálohu, tedy o kompletní zálohování stavu

dat a systémů ve stavenou dobu. Tento typ zálohy je potřeba provádět pravidelně v nějakém časovém období. Jelikož je velmi náročný na čas, provádí se nejčastěji o víkendu, tedy jednou týdně, nebo méně často. Druhým typem zálohy je diferenciální záloha, která ušetří čas tím, že provádí zálohu pouze změněných dat od poslední full zálohy. Nicméně čím vzdálenější je datum od provedení poslední full zálohy a čím více změn v systémech a potažmo datech se provede, tím je provedení diferenciální zálohy delší a po nějaké době se blíží full záloze. Třetím možným způsobem provádění zálohování jsou zálohy inkrementální. Které provádí zálohy pouze změněných dat a systémů od poslední provedené jakékoliv zálohy (full zálohy nebo předešlé inkrementální zálohy). Tento způsob vede k relativně rychlému provedení zálohování, ale zase neúměrně zvyšuje dobu pro obnovu systémů. Obnova dat podle jednotlivých způsobů zálohování se mění. Pokud společnost využívá pouze full zálohování, pak stačí obnovit data dle požadovaného datumu z příslušné full zálohy. Pokud společnost využívá diferenciální zálohování, bude pro obnovu dat a případně celého systému potřebovat minimálně dvě příslušné zálohy, tedy jak diferenciální zálohu, tak full zálohu od které se diferenciální záloha prováděla. Nejnáročnější obnovou je pak obnova z inkrementálních záloh, protože například pro kompletní obnovu nějakého systému bude zapotřebí použít příslušnou full zálohu a všechny inkrementální zálohy, které byly od této full zálohy vytvořené. Obnovit systémy, lze přepsáním poškozených dat nebo obnovení na jiné místo, jiný hardware, nebo pod jiným názvem a následně lze porovnávat, zda jde skutečně o požadovaná data, nebo zda se bude obnova provádět ještě z jiných většinou starších záloh.

3.5.5. Dohledový a varovný systém

Snahou každé společnosti by měl být pro aktivní přístup tedy předcházet (v tom lepším případě), nebo alespoň bezprodleně reagovat na vzniklé problémy v ICT systémech ve společnosti využívaných. Jakýkoliv i drobný výpadek, třeba jen malé části ICT ve společnosti, je velmi nákladná záležitost a z těchto důvodů je pro každou společnost klíčové, tyto nepříjemné náklady minimalizovat.

Na trhu je spousta systémů a aplikací určených k tomuto účelu, které bych rozdělil do dvou skupin. První skupina čeká na informace, které jí formou ticketů zašlou samotná sledovaná zařízení v případě nějaké (většinou chybové nebo informativní)

události (eventu). Daný software pak podle předem definovaných nastavení s příchozím ticketem provede následné kroky. Tyto kroky mohou být od pouhého záznamu do nějakého losovacího souboru, přes vytvoření incidenčního ticketu v nějakém helpdeskovém řešení společnosti, až po okamžité upozornění odpovědné osoby (případně několika osob) různými kanály jako je SMS, informace na pager, elektronická pošta a podobně.

Druhou skupinou jsou pak aktivní systémy, které si sami kontrolují, zda systémy a služby na nich běžící jsou v korektním stavu. Nejsou odkázány jen na zaslání ticketů od zařízení, ale samy aktivně zjišťují, zda jsou služby, nebo systém aktivní, případně v jakém je stavu. Na základě případných indicií (například zvýšené chybovosti) dokáží dopředu upozorňovat na budoucí možné problémy a podobně.

3.5.6. Nástroje pro správu sítě

Pro efektivní správu ICT systému společnosti je téměř nutností využívat nějaký nástroj pro hromadné ovládání jednotlivých částí systémů. Každé zařízení připojené do datové sítě i každý využívaný systém umožňuje provádět změny svého nastavení, říkáme tomu provádět změny konfigurace. Což je pro správu systému naprosto dostatečné řešení dodávané přímo výrobcem zařízení, nicméně toto řešení je téměř nepoužitelné u rozsáhlejších sítí o několika desítkách a mnohdy i podstatně větších počtech koncových zařízení, kde je zapotřebí využití nějaké centrální správy pro více zařízení nebo systémů najednou. K těmto úkonům slouží sofistikované systémy (například HP openview, Tivoli a podobně) případně různé administrátorské konzole jako je například MMC (Microsoft management Console) [Šetka, 2003, s. 245], které jsou na základě ruzných plug-inů (softwarové rozšíření funkcionality) rozšiřující své dovednosti a možnosti administrace různých zařízení pomocí jedné administrátorské konzole. Případně i jiné konzole pro jiné systémy nebo zařízení.

3.6. Bezpečnost dat – šifrování

Bezpečnost dat, tedy především informace předávané mezi dvěma subjekty (dříve mezi lidmi, dnes častěji mezi zařízenímy, které lidé využívají pro předávání informací) je problém, který se začal řešit již v dobách krále Herodota tedy někdy do doby pátého století před naším letopočtem. [Singh, 2003, s. 6] Kdy se začali využívat

první známky šifrované zprávy zvané steganografie. Steganografie je ukrývání zprávy jako takové. Známé jsou případy, kdy se zpráva napsala na oholenou hlavu posla, který vyrazil na cestu až po tom co mu opět hlavu pokrývaly vlasy. Steganografii lze rozdělit na dvě větve (transpozici a substituci).

Při použití transpozice se písmena uspořádají v jiném pořadí, než v jakém se nachází původně. Jedná se o jakousi přesmyčku. Dříve se namotal okolo tyče pruh kůže, na který se napsala zpráva, která šla dekódovat (přečíst) příjemci po namotání tohoto pruhu kůže na jinou tyč o stejném průměru.

Při použití substituce se nahrazují jednotlivé znaky písmen, jinými písmeny, takže je zpráva na první pohled nesmyslná posloupnost znaků. Například: A <-> V, H <-> B, O <-> Q, J <-> K za použití této substituce nám ze slova AHOJ vznikne nic neříkající slovo VBQK.

Šifrování je tedy již velmi starý obor, který od doby svého vzniku, ušel hodně dlouho cestu, která je lemována různými milníky vedoucí ke stále složitějším způsobům ochrany předávané cenné informace. Některé způsoby a možnosti šifrování v této diplomové práci uvedeme v následujících kapitolách.

"*Šifrování je často jedinou možností, jak chránit cenná data*".

3.6.1. Šifrování synchronní

Šifrování synchronní je způsob šifrování, kdy dochází k šifrování i dešifrování dat za použití stejného klíče (čím delší nebo složitější je použitý šifrovací klíč, tím je složitější jeho rozluštění a tím většího množství času potřebuje případný narušitel k získání zašifrovaných dat) nebo lze použít identickou kopii klíče. Jedná se o velmi rozšířený, snadno použitelný a jednoduchý způsob šifrování dat. Jeho předností je jeho veliká rychlost a snadnost využití. Nevýhodou tohoto řešení je problém s prvotním předáním klíče. Pokud je to možné, klíč se předává osobně ještě před předáním první šifrované zprávy, případně se využívají odlišné cesty a způsoby pro předání zprávy a klíče. Pokud se jedná o elektronický klíč, předává se například pomocí flash paměti, FTP serveru, jinou adresou elektronické pošty a podobně. Rozhodně není vhodné předat nejprve klíč a následně zašifrovaná data stejnou cestou.

3.6.2. Šifrování asynchronní

Asynchronní šifrování je další novější způsob zabezpečení dat, který využívá dvou různých šifrovacích klíčů. Jeden šifrovací klíč se používá pro šifování (jedná se v mnoha případech o klíč veřejný tedy volně dostupný) a druhý pro dešifrování dat (jedná se tajný klíč, který není volně k dispozici, tedy je využíván pouze příjemcem šifrovaných dat). Pokud chce někdo předat nějaká cenná data, použije veřejný klíč příjemce pro zašifrování dat a následně takto ochráněná data doručí příjemci, který za pomoci svého soukromého (tajného, neveřejného) klíče dokáže data dekódovat a následně přečíst. Při použití této varianty nedochází k žádnému předávání klíčů (odpadá tím problém známý ze synchronního šifrování), pokud tedy někdo cítí potřebu chránit předávaná data, pouze využije veřejného klíče příjemce.

3.6.3. RSA

Šifrovací RSA algoritmus považovaný za jeden z nejbezpečnějších vytvořili tři matematici Rivest, Shamir a Adleman. [Klander, 1998, s. 128] Tento šifrovací algoritmus zahrnuje konstantu, která reprezentuje maximální délku šifrovaného bloku. Šifrovací proces se provádí pomocí tří kroků. Za využití veřejného šifrovacího klíče (E) a soukromého šifrovacího klíče (D) s délkou minimálně 512 bitů (dnes běžně používaná délka klíče je již 2048 bitů). V prvním kroku se převede text na celé číslo v rozsahu 0 až n-1, rozdělené dle maximální délky šifrovaného bloku. Ve druhém kroku se zpráva zašifruje pomocí celého čísla bloku umocněného veřejným klíčem (tedy $block^E$) a následně se s výsledkem provede operace modulo (aritmetická operace, jejímž výsledkem je celočíselný zbytek po celočíselném dělení) výstupem druhého kroku je zašifrovaný dokument (C), který následně nějakým způsobem doručíme příjemci. Třetím krokem je následné dešifrování. Vezme dokument C a umocníme ho soukromým šifrovacím klíčem (D) tedy C^D, provedeme operaci modulo n, následně získáme množinu hodnot reprezentující jednotlivé bloky a tyto číselné bloky převedeme zpět na text za pomoci stejné metody, jakou jsme použili pro převod původního textu. RSA algoritmus tedy pro svou funkci využívá kombinaci synchronního šifrování a následně asynchronního šifrování.

3.6.4. Vodoznaky

Do elektronických dokumentů lze vkládat dodatečnou informaci pomocí techniky vložení vodoznaku. Vodoznak lze vložit viditelný, částečnně viditelný nebo skrytý, tedy na první pohled neviditelný. Nejznámější využití vodoznaku, je u tištěných dokumentů v podobě nějakého obrázku či nápisu tištěného přes text dokumentu. Využívá se například pro označení přísně tajných dokumentů a podobně. Částečně viditelný vodoznak se hojně využívá k ochraně cenin, tedy například bankovek, certifikačních listin a dalších, kdy je vodoznak viditelný proti nějakému světelnému zdroji a jedná se o jeden z prvků ochrany ověřující pravost bankovky nebo dokumentu, který vodoznaku pro svou ochranu využívá.

Vodoznak je dále využíván jako ochrana před neoprávněným využitím autorských děl (například obrázků, video ukázek, zvukových záznamů a podobně) na internetu. Každý autor fotografie má možnost, před zveřejněním svého díla na internetu, vložit nějakou formu vodoznaku. Digitální vodoznak je prakticky neodstranitelná informace, zejména protože není znám princip, který byl použit pro jeho vložení.

Viditelný vodoznak, tedy takový, který na první pohled viditelně pozmění autorovo dílo (většinou překrývá nějakou část díla) a jasně dává najevo, že dílo označené vodoznakem je autorsky chráněno. Pokud tedy toto dílo někdo chce použít pro své potřeby, musí si dohodnout, za jakých podmínek autor k použití svého díla svolí a zda poskytne zdroj díla bez vodoznaku.

Neviditelný vodoznak je stejně jako viditelný vodoznak určen pro ochranu před zneužitím nějakého díla. Jeho využití je v určení vlastnictví v případných právních sporech, které vyvolá autor díla chráněného neviditelným vodoznakem po zjištění, že jeho dílo bylo někde prezentováno nebo využito bez vědomí autora.

3.6.5. Další možnosti šifrování

V předešlých kapitolách jsme si představili některé základní možnosti ochrany ceněných dat. Způsobů jak chránit svá data je nepřeberné a stále se rozšiřující množství. V této kapitole si jen zmíníme další možnosti, které je dnes možné využít.

Diffie a Hellman - [Klander, 1998, s. 131] v roce 1976 odstartovali boom otevřeného výzkumu v kryptografii, když poprvé zveřejnili šifrování s veřejným klíčem,

která zároveň umožňuje elektronickou distribuci klíčů. Až o 2 roky později byl vytvořen kompletní kryptografický systém RSA zmiňovaný v jedné z předešlých kapitol.

Hash – [Klander, 1998, s. 136] Message digest (výtah zprávy) je minimálně 128 bitová jednocestná hašovací funkce. Jednocestná, protože nelze odhalit tvar vstupních dat při znalosti výsledných dat. Jedná se o podobnou funkci, jakou zastává kontrolní součet. Tento kontrolní součet se využívá k identifikaci, zda zpráva byla změněna. Teoreticky je nemožné (výpočetně neproveditelné) nahradit původní zprávu nějakou novou zprávou, která by vytvořila stejný message digest (hash). K těmto účelům se využívá algoritmů RSA-MD2 a RSA-MD5, které jsou dnes velmi populární.

PEM - [Klander, 1998, s. 137] (Privacy Enhanced Mail) Standardy umožňující využití různých kryptografických technik k zajištění utajení, autentizace a integrity zpráv. Integrita zprávy v PEM zajišťuje a potvrzuje uživateli, že zpráva během přenosu od odesilatele nebyla nijak pozměněna.Autentikace v PEM umožňuje uživatelům ověřit, že odesilatelem je opravdu ten, za kterého se vydává. Utajení zprávy v PEM umožňuje skrýt obsah zprávy před lidmi, kterým tato zpráva není určena.

PGP - [Klander, 1998, s. 139] (Pretty Good Privacy) Je často označován jako hybridní kryptografický systém skládající se ze čtyř kryptografických částí. Využívá symetrické šifrování (jediný sdílený klíč), asymetrické šifrování (soukromý a veřejný klíč – RSA nebo Diffie-Hellman, záleží na použité verzi PGP), jednocestnou hashovaní funkci a nakonec ještě standardní generátor náhodných čísel.

Možností jak chránit data, která jsou pro nás cenná, je spousta. V této kapitole je pouze úzký výpis možných řešení, který neobsahuje všechny dostupné systémy a možnosti využitelné pro dekleraci vlastníka, ochranu dat před zneužitím (změnou dat), nebo před přečtením nějakou neoprávněnou osobou.

3.6.6. Elektronický podpis

Elektronický podpis (digitální podpis) [Klander, 1998, s. 151] je využíván pro ověření identity odesílatele. Ověřuje tedy pravost uváděných údajú o odesílateli a pokud nebyla zpráva nějak pozměněna, také ověřuje věrohodnost samotné předávné zprávy.

Digitální podpis je unikátní (jedinečná) hodnota, která je tvořena speciálním softwarem pomocí aplikace matematických funkcí a šifrovacího klíče na zprávu

nebo soubor. Tato unikátní hodnota potvrzuje totožnost autora zprávy a dále i to, zda se zprávou během přenosu od odesilatele k příjemci nebyla zpráva nějak pozměněna.

Digitální podpis využívá DSS (Digital Signature Standard) který definuje standard vlády Spojených států Amerických pro digitální podpisy a matematické funkce použité v digitálním podpisu.

Digitální certifikáty jsou vizuální prezentací unikátní hodnoty, která ověřuje obsah podepsaného souboru a totožnost autora pomocí ověření třetí strany. Třetí stranou rozumíme nějakou certifikační autoritu, která vydává jakési razítko potvrzující uvedené údaje. Obdoba klasického razítka na tištěné dokumenty při ověření podpisu dotčené osoby u notáře nebo na úřadě. V České republice je takovouto certifikační autoritou například Certifikační autorita Postsignum od české pošty. Celosvětově jsou známé certifikační autority například Verisign nebo Thawte a jiní.

3.7. Bezpečnost komunikace

Bezpečnost komunikace tedy ochrana přenosu zpráv nebo dat mezi různými systémy a následně osobami je možné řešit pomocí šifrování, jak jsme si částečně popsali v předešlé kapitole. Mnohdy ale nejde pouze o ochranu dat při přenosu informací, ale je zapotřebí ochránit komunikační kanál jako takový. Případně ochránit zdroje společnosti před nějakým útokem. Pokud pomineme nemožnost komunikace z důvodu fyzického odpojení (například přerušení vedení nebo závada hardware), existují možnosti, jak cíleně vyřadit zdroj (většinou server) případně komunikační linku (nějaké propojení) z provozu a tím zamezit předání informace od odesilatele k příjemci a tím poškodit zájmy společnosti.

Bezpečnost elektronické komunikace se snažíme zajistit využitím různých systémů. Jejichž pomocí dokážeme detekovat mnohé ze známých možností útoků. Na základě získaných výsledků z těchto systémů jsme následně schopni aplikovat různé obranné mechanizmy pro snížení, případně úplnému zabránění, úspěšnosti těchto útoků.

Sledování celého přenosu informací od jejího vytvoření, úspěšného vyslání odesilatelem, přenesení od odesilatele k příjemci (bez jakýchkoliv změn a pokud možno neprodleně, při zajištění ochrany před odposlechem informace), až po doručení příjemci a zajištění úspěšného přečetení zaslané informace. Toto jsou nezbytné části komunikace, jejichž bezpečnost je nutné zajistit.

3.7.1. IDS

IDS – (Intrusion Detection Systems) [online, www.4safety.cz] je zařízení (případně software) využívající složitý centrální systém pro detekci narušení bezpečnosti datové sítě (potencionální útok). Tyto systémy se skládají z různých sond a centrální databáze. Jednotlivé sondy slouží k detekci těchto útoků a pracují na úrovni síťové komunikace nebo na úrovni lokální detekce útoků. Veškerý průchozí provoz systémem IDS je analyzován pomocí technologie PAD (Protocol Anomaly Detection), která nám dokáže odhalit nekorektní provoz na síti nebo nekorektní požadavky na lokální zdroje. Po PAD analýze, je následně provoz (jednotlivé packety) ještě kontrolován oproti záznamům (signaturám) v databázi. Podobný systém aktualizací, jako využívají například antivirové systémy je využíván také systémy IDS pro lepší a rychlejší detekci možných napadení. Problémem těchto detekčních systémů (například z důvodu vývoje stále nových standardů a jejich implementací a podobně) se stává, že korektní provoz na síti mohou vyhodnotit, jako potenciální útok.

3.7.2. IPS

IPS – (Intrusion Prevention Systems) je obdobou systému IDS s rozšířenou funkcionalitou. Neslouží tedy pouze k detekci případných anomálií nebo útoků, ale dokáže sám účinně proti těmto jevům zasáhnout, například vyvoláním poplachu, filtrováním packetů, násilným resetováním spojení, blokováním adresy ze které k útokům dochází, případně vypnutí portu a podobně. Systémy IPS jsou jakousi nadstavbou bezpečnosti datové sítě společnosti, která tyto systémy využívá. Stávají se jakousi druhou vrstvou bezpečnost (první vrstvou je firewall). Nasazení těchto systémů však skýtá nejedno zákoutí, kde se mohou vyskytnout nějaké nežádoucí účinky při jeho nasazení a provozování, proto nejní vhodná jejich implementace do každého prostředí.

3.8. Právní ochrana firmy

Každá společnost i osoba vyskytující se na území České republiky musí dodržovat ústavu a zákony platné v České republice. Zejména pak pokud chce podnikat na území České republiky je její chování právně závazné sbírkou zákonů a obecně přijatými

normamy a vyhláškami. Případné porušení je pak posuzováno podle obchodního zákoníku (pokud jde o porušení v rámci pracovních a obchodních vztahů) nebo trestního zákoníku pokud jde o trestnou činnost. Orgány činné v trestním řízení mají možnost v rámci zákona nařídit urovnání zjištěného stavu, udělit pokutu, zakázat činnost, případně vyvodit trestní odpovědnost konkrétních osob (v krajním případě až omezením svobody).

3.8.1. Interní směrnice/normy

Společnosti často využívají možnosti vytvářet (mnohdy nad rámec zákona) své vlastní normy a směrnice pro interní potřebu. Tyto interní normy a směrnice často zpřísňují a upravují chování zaměstnanců společnosti (nebo jejích kontraktorů, návštěvníků a dalších osob) ve vztahu k majetku společnosti, k prezentaci společnosti na veřejnosti, k využívání a správě zdrojů, které jsou ve vlastnictví společnosti. Často využívaný je tak zvaný dress code. Směrnice upravující vzhled zaměstnance firmy. Jaké má používat ochrané pomůcky při vstupu do určité výrobní části společnosti (obzvláště přísné podmínky bývají například v chemických provozech), zda má být oblečen v nějaké uniformě a tato mu musí být společností poskytnuta a podobně.

Interní směrnicí se upravují specifikace, co je považováno za výrobek, meziprodukt společnosti a co už ne. Interní směrnice velice často pokrývají oblasti bezpečnosti práce v prostorách společnosti. Určují se odpovědné osoby za různé pracovní oblasti a podobně. Interní směrnice dále upravují nakládání s informacemi, které zaměstnanec dostane k dispozici při vykonávání své pracovní náplně. Interní směrnicí se upravuje činnost odborové organizace, zejména její aktivity pro zaměstnance společnosti v mimo pracovní dobu sponzorované společností. Interní směrnice si společnost vytváří sama. Mnohé společnosti často přejímají celé nebo alespoň nějaké části interních norem od jiných společností se stejným zaměřením. Například norma ISO/IEC 27000 je velmi využívána, protože upravuje oblasti Informační technologie – Bezpečnostní techniky – Systémy řízení bezpečnosti informací. Porušení těchto interních směrnic ze strany zaměstnance vede k upozornění ze strany nadřízených osob. V případě závažných porušení těchto vnitřních norem to může vést k nějakému postihu zaměstnance (pokutě, odebrání osobního ohodnocení a podobně) a v krajním případě až k rozvázání pracovního poměru podle §53 sb. Případně dalších § vztahujících se k ukončení pracovního poměru.

3.8.2. Zákony ČR

Jak již bylo uvedeno každý občan i každá společnost nacházející se na území české republiky musí dodržovat ústavu a zákony ČR. V této kapitole si pouze uvedeme některé zákony vztahující se k elektronickému zpracování dat, nebo zákony upravující chování osob a společností ve vztahu k těmto elektronickým datům.

Zákon č. 101/2000 sb. o ochraně osobních údajů, který upravuje práva a povinnosti každého, kdo nějakým způsobem pracuje s osobními údaji jiných osob (jméno, adresa, rodné číslo a podobně).

Zákon č. 29/2000sb. Zákon o poštovních službách, který se svou částí o poštovním tajemství vztahuje i na elektronickou poštu.

Zákon č. 40/2009 sb. Trestní zákoník, který svým obsahem vymezuje trestné činy (kromě jiného i proti majetku, hospodářské činnosti atd.) a ukládá sazebník trestů

Zákon č. 513/1991 sb. Obchodní zákoník, který svým obsahem upravuje vztahy mezi obchodními partnery.

Spoustu dalších jednotlivých zákonů, které jsou platné a všichni je musí dodržovat, jinak jim hrozí nějaký trest.

3.8.3. OSA

Ochranný svaz autorský (OSA) [online, www.osa.cz] je dle informací § 18 odst. 2 zákona č. 101/2000 Sb. v pl. zn. – organizace pro práva k dílům hudebním. Zpracovává osobní údaje za účelem výkonu kolektivní správy majetkových autorských práv. Zpracovává adresní, identifikační a jiné osobní údaje svých členů i osob s jiným vztahem k OSA získané od subjektů údajů a z vlastní činnosti, a to v místě svého sídla a v místě regionálních pracovišť. Příjemci jsou fyzické a právnické osoby v České republice a v zahraničí. OSA byl založen samotnými autory 9. Října 1919. V současné době OSA zastupuje více než 7000 domácích a více než milion zahraničníchnositelů autorských práv (skladatelů, textařů, nakladatelů).

Je důležitým mostem mezi autory a uživateli jejich děl. Autorům poskytuje služby spojené s výběrem a následným rozúčtováním autorských odměn, včetně zpracování dat od uživatelů a právních služeb. Uživatelům usnadňuje přístup k legálnímu užití hudby všech žánrů z celého světa.

4. Vlastní návrh bezpečnosti ICT infrastruktury z hlediska vnitřního napadení

ICT infrastruktura každé společnosti musí zajistit správné fungování všech využívaných systémů při dosažení maximální možné dostupnosti všech zdrojů na datové síti a zajištění jejich bezpečnosti. Pokud je ve společnosti dokonce zaveden nepřetržitý provoz (tedy jsou kladeny velmi vysoké nároky na dostupnost, s velkým omezením pro servisní odstávky), pak jakýkoliv výpadek představuje veliký problém, který nejen ohrožuje výrobu a následně vede k obrovským finančním a materiálovým ztrátám, ale zároveň je podstatně důležitější zajistit dostupnost a bezpečnost všech ICT systémů. Ve zvolené společnosti Česká rafinérská a.s. je nepřetržitý provoz zaveden. Výrobní část společnosti se orientuje na chemický průmysl a nakládá s nebezpečnými látkami. Výrobní činností zvolené společnosti je rafinace ropy a jejích derivátů, tedy výroba benzínů, nafty, lehkých i těžkých topných olejů, leteckých paliv a vedlejších produktů jako jsou plyny (především LPG), síra a další produkty nebo meziprodukty.

Jedná se o společnost, která vznikla při privatizaci 1. 1. 1996 kdy ze stávajících chemických podniků v Kralupech nad Vltavou (Kaučuk) a v Litvínově (Chemopetrol) byly vyčleněny pouze provozy rafinerie a v rámci privatizace do tohoto podniku vstoupil zahraniční investor, který investoval do rozvoje podniku včetně celého informačního systému firmy. Společnost má výrobu a kancelářské prostory ve dvou různých rozlehlých a odlehlých areálech, které však sdílí s dalšími společnostmi a areály nejsou v jejím vlastnictví (tedy za některé služby platí, protože je využívá většinou na základě nájemních smluv případně smluv o spolupráci, či jiných obchodních smluv.

V současné době společnost provozuje ve dvou nezávislých datových centrech přibližně 70 serverů, datovou síť propojující v každé lokalitě několik samostatných budov a k této síti se připojuje (v českém měřítku větší počet, celosvětově se však jedná o malou společnost) přibližně pět set koncových zařízení, na kterých pracuje zhruba šet set zaměstnanců, případně v rámci konkrétních projektů do sítě přistupuje i několik desítek kontraktorů (nasmlouvaných dodavatelů).

Nejprve si v této diplomové práci popíšeme výchozí stav ICT systému ve společnosti Česká rafinérská a.s. a následně si uvedeme jednotlivé navržené

projekty (kroky postupně na sebe navazující, realizované dle investičních plánů – tedy některé již realizované, jiné ve fázi příprav nebo již projektově připravené, ale před samotnou realizací) vedoucí k zajištění větší bezpečnosti celé ICT infrastruktury z hlediska vnitřního napadení.

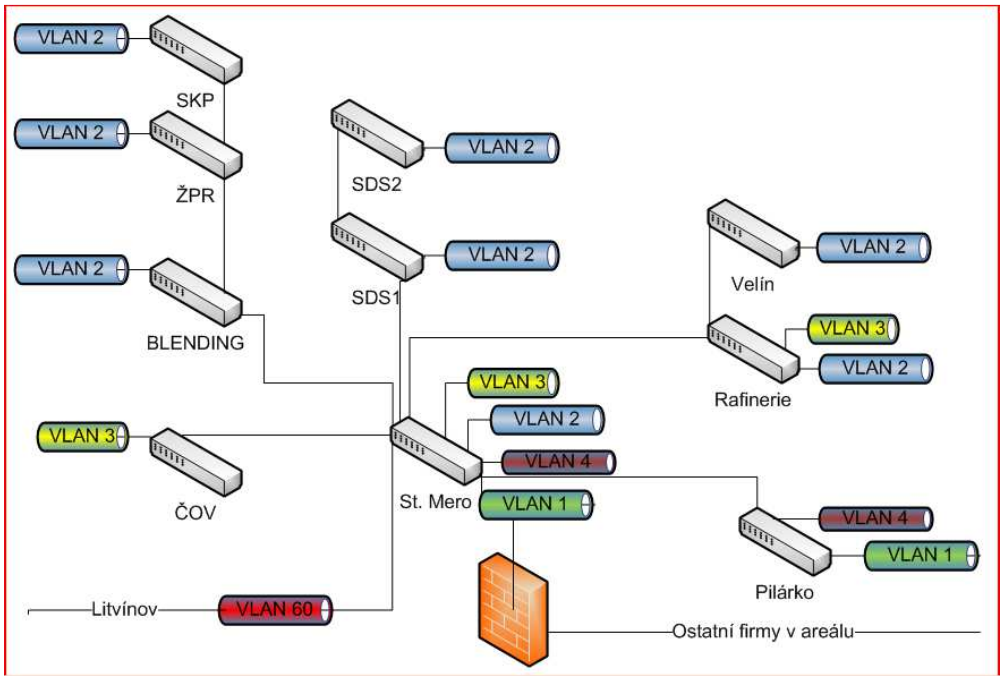
V této diplomové práci budeme vycházet ze stavu ICT infrastruktury společnosti, který reflektuje skutečný stav v blíže nespecifikovaném okamžiku. Přesné datumy nejsou předmětem této práce a nebudou zde uváděné již z prostého faktu, že zmiňovaná společnost je velmi rizikovou společností, která mimo jiné zajišťuje (alespoň z části) státní hmotné rezervy pro celou Českou republiku, dále nakládá s hořlavinami a látkami označovanými jako nebezpečné. Ze stejných důvodů zde nejsou uvedené ani názvy přesné označení budov, IP adres, serverů a podobně.

Tato práce si klade za cíl zvýšení bezpečnosti stávající ICT infrastruktury datové sítě společnosti z hlediska vnitřního napadení. Jedná se zajištění a především budoucímu zamezení nežádoucím mimořádným událostem, jak jsou ve společnosti označovány všechny případy, kdy došlo z nějaké příčiny ke změnám oproti normálnímu běžnému stavu výroby nebo provozu společnosti. Mimořádné události jsou například, požár v areálu, poškození majetku společnosti ze strany zaměstnance nebo kontraktora (ať už k úmyslnému nebo neúmyslnému), odcizení majetku společnosti, případně poškozování práv třetích stran ze strany zaměstnanců společnosti a následné vyšetřování orgánů činných v trestním řízení, jak se několikrát v minulosti potvrdilo, vedoucí k obvinění a následnému odsouzení konkrétních osob a podobně, což pro společnost představuje nemalý problém.

4.1. Výchozí stav Kralupy

Začneme popisem výchozího stavu ICT ve společnosti v menším ze dvou areálů, tedy v Kralupech nad Vltavou. Jedná se o areál, který sdílí několik společností. O ostrahu a docházkový systém se stará společnost Synthos (případně pomocí nějakých dalších subdodavatelských společností), zároveň je společnost Synthos (nástupce původní společnosti Kaučuk), dodavatelem některých surovin a energií pro zvolenou společnost, jako je například pára, teplárna, elektrická energie a další. V tomto areálu se nachází několik budov ve vlastnictví České rafinérské, jedná se o budovy administrativního charakteru nebo výrobní budovy, které jsou vybavené datovými rozvody typu LAN

tvořené strukturovanou kabeláží splňující německou normu kategorie 6 (jedná se o normu vyhovující chemickému provozu a zajištění vysokorychlostního připojení koncových zařízení lépe, než v té době schválená kategorie 5E pro českou republiku, tato norma je poněkud striktnější ve svých parametrech pro vysokorychlostní datové rozvody). Tyto datové rozvody využívají modulární systém společnosti AMP, který dokáže snadno měnit možnosti využití jednotlivých koncových zásuvek (přípojných míst). Při použití jednoho typu kabelu a výměny koncových modulů v zásuvkách (zvaných inserty), lze měnit způsoby využití i přenosové parametry, existují inserty pro propojení telefonní sítě (RJ11), datové sítě (RJ45), koaxiálního kabelu (BNC), dokonce lze pomocí optických převodníků v insertu přepojit optické vlákno na metaliku a naopak. Těchto variant je veliká spousta a společnost AMP tento systém i nadále rozšiřuje. Výrobce garantuje 25 let pro používání tohoto systému bez ztráty parametrů. To je jistě vítaný bonus, který snadno vyváží jeho přiměřenou cenu. V Kralupech nad Vltavou je jedno datové centrum zahrnující speciální místnost nazvanou serverovna a centrum datových rozvodů. Ostatní budovy v areálu jsou propojené pomocí optických kabelů s budovou s datovým centrem. Jedná se tedy o spojení pomocí sítí typu MAN a využívá se zapojení do hvězdy, kde datové centrum je středem těchto optických spojení. Tato fyzická infrastruktura sítě, je rozdělana do několika menších virtuálních sítí pomocí VLAN. Tyto sítě jsou distribuované (rozložené) přes několik budov.



OBR. 8 Propojení jednotlivých budov a VLAN, areál Kralupy

Rozložení jednotlivých VLAN v jednom areálu je pouze dle počtu připojených koncových zařízení. Dále je směrování pomocí VLAN využíváno ke směrování dat mezi lokalitami.

Serverovna je tedy speciálně upravená místnost, která má instalovanou antistatickou dvojitou podlahu pro snažší připojení jednotlivých racků (skříně ve kterých jsou montované jednotlivé zařízení, jako jsou servery, aktivní prvky, záložní zdroje, diskové pole a podobně). Tato místnost využívá vyšší zabezpečení před vstupem neoprávněných osob. Je vybavená speciální vzduchotechnikou, využívanou pro chlazení převážně v zimních měsících, hlavně při venkovních teplotách pod -5^{o}C, kdy nelze zcela využít instalované chladicí systémy (klimatizaci). Klimatizace je zde instalovaná ve dvojím provedení (duálně), tedy dvě zcela samostatné chladící jednotky schopné zajistit v této místnosti prakticky stálou teplotu okolo 23^{o}C a to každá jednotka samostatně. Tyto jednotky jsou však navzájem propojené a dokáží spolu komunikovat. Tato komunikace zajišťuje pouze předání určitých stavů. Například pokud běžící jednotka přestane z nějakého důvodu správně fungovat (většinou z důvodu poruchy), automaticky se zapne druhá jednotka. Případně pokud je v provozu první jednotka na maximální výkon, a přesto začne teplota v místnosti stoupat, přičemž dosáhne úrovně až 27^{o}C, pak se přidá i druhá jednotka, aby došlo opět k následnému snížení teploty na požadovaných 23^{o}C.

Serverovna je napájena dvěmi přívody 220V z různých směrů a různých trafostanic, je zde stykačová logika, která při výpadku napájení z hlavní trafostanice automaticky přepne na záložní připojení. Je zde také možnost připojit agregátor pro napájení serverovny v případě odstávky celé elektrické sítě. Mezi tímto přepínaným přívodem a jednotlivými záložními zdroji (UPS) v racích je ještě vložen velký centrální záložní zdroj schopný udržet celou serverovnu při výpadku obou přívodů zhruba dalších 20 minut navíc, teprve po vyčerpání nastupují svou činnost záložní zdroje přímo v racích.

Serverovna je dále vybavena protipožárnímy systémy, jako jsou napojení na centrální pult u hasičů s informacemi z kouřových čidel v serverovně, protipožárními dveřmi, protipožární klapky ve vzduchotechnice a další úpravy. Profesionální hasičský sbor, který je v areálu přítomný a je umístěn nedaleko od budovy s datovým centrem, je vyškolen a seznámen s postupy, jak postupovat v případě požáru této budovy (jaké použít hasební látky i kde a jak co odpojit a podobné důležité informace).

Naše společnost se podílí větší částí na přispěvcích potřebných pro provoz a vybavení hasičského záchraného sboru.

V serverovně jsou umístěny různé systémy, nejprve si popíšeme jejich hardwarovou specifikaci. Serverovna je sice jedna větší místnost (původně na jejím místě byly zřízené tři kanceláře pro celkem deset lidí), ale je virtuálně rozdělana na několik částí. V jedné části jsou umístěné již zmíněné klimatizace a pod stropem je rozvedena jejich vzduchotechnika. V druhé čísti je umístění centrálního záložního zdroje se stykačovým přpínačem přívodů napájení, které jsme si také již popisovali. Ve třetí části se nachází řada vedle sebe stojících a navzájem propojených rackových skříní, které se dělí na další dvě části. Na část rozvodů a aktivních prvků a na část serverovou.

V rozvodové a aktivní části jsou umístěny racky se zakončením místní sítě LAN (tedy rozvodů od jednotlivých koncových zásuvek umístěných v kancelářích nebo na chodbách stejné budovy), zakončení je provedeno pomocí patchpanelů označených příslušným kódem (většinou číslem a písmenem) každé zásuvky, dále jsou zde zakončeny sítě MAN. Tedy všechny optické kabely vedoucích do ostatních budov v Kralupském areálu. Dále jsou zde umístěny jednotlivé aktivní prvky. Je zde umístěn hlavní router lokality, zajišťující směrování dat mezi jednotlivými virtuálními sítěmi (VLAN), jsou zde koncové prvky typu switch s managementem a s rychlostí portů 10/100/1000. Jsou zde dále media konvertory pro převod metalického signálu na optický (pro připojení optických kabelů). Je zde umístěn firewall, který odděluje a řídí datovou komunikaci mezi sítí společnosti a ostatními společnostmi v areálu, se kterými společnost elektronicky komunikuje (nejedná se o úplně všechny společnosti působícími v areálu, ale řekněme s podstatnou částí z nich).

V serverovně v Kralupech je přibližně 30 provozovaných hardwarových serverů, každý server má své diskové pole. Jedná se o servery přibližně tří výkonnostních řad, využívané podle náročnosti systémů na nich běžících. Všechny servery jsou od stejného výrobce Hewlet-Packard (dříve Compaq) a navzájem se liší velikostí paměti (RAM 1,2,4GB) typem serveru (DL360, DL320, DL180), tedy obměnou hardware (jiná základní deska a použitý chipset - sada čipů na desce) a počtem použitých procesorů. Vzhledem k několikaletému provozu, jsou zde postupně starší servery (obměna hardware serverů se provádí pravidelně, přibližně po 4 letech) nahrazovány novějšími a zároveň výkonnějšímy modely nebo novějšími generacemi stávajících typů.

Softwarové systémy často zahrnují i několik hardwarových serverů, případně jeden hardwarový server dokáže obsloužit více (méně náročných) systémů současně.

Nejčastěji používané serverové operační systémy ve společnosti, jsou operační systémy od společnosti Microsoft (převážně Windows standard server ve verzi 2003 nebo 2008). Je zde využívána activ directory (AD) pro ověřování uživatelů v rámci jedné domény s několika subdoménami. Hlavní doména (crc.local), pomocí které se spravují objekty na síti (například tiskárny, počítače, uživatelé … a tak dále). Správou rozumíme nastavení jejich konfigurace a především přidělení práv co kdo (uživatel) nebo kam (zdroje na síti) může mít přístupné nebo naopak je mu přístup zakázán.

Služby podporující chod sítě jsou instalované na více serverech (v Kralupech konkrétně na dvou serverech), kdyby došlo k nějakému výpadku, aby nedošlo k odstávce celé sítě. Jedná se o služby jako je DNS, WINS (překlad IP adres na názvy zařízení), DHCP služba neboli přiřazování IP adres koncovým zařízením, u kterých z nějakého důvodu není zapotřebí mít stále stejnou adresu. Což jsou prakticky všechna zařízení s výjimkou tiskáren, serverů a případně nějakých dalších zařízení, ke kterým je zapotřebí přistupovat a proto je vhodné, aby byly stále na stejné adrese.

Pro sdílení souborů je zde využíván FILESERVER, na kterém jsou umístěny domovské adresáře všech uživatelů primárně sídlících v Kralupech, Dále je tento serer využíván pro sdílené datové prostory v rámci krátkodobých nebo dlouhodobých projektů. K těmto projektům přistupují zaměstnanci zařazení do konkrétních projektových týmů. Členy těchto projektů jsou zaměstnanci z různých oddělení společnosti.

LIMS (Laboratory Information Management Systém) – jedná se o celý soubor různých systémů potřebných pro práci certifikované laboratoře. Tento systém pracuje nad databázovým systémem společnosti Oracle, pomocí kterého zpracovává a uchovává, případně i archivuje analyzovaná data. Získává data z laboratorních zařízení, jako jsou například analyzátory a další obdobná specifická zařízení, kterými je laboratoř vybavena. Tento systém využívá vestavěné aplikace pro okamžité zobrazování naměřených výsledků a získaných hodnot. Takto získaná data se zobrazují všem zaměstnancům centrálního velínu výroby, kteří jsou zodpovědní za kvalitu výroby a na základě těchto hodnot jsou schopni upravit výrobu a tím i výsledný produkt. Tento systém nadále vydává certifikáty kvality každého produktu vyvezeného z areálu. K distribuci se využívají autocisterny (jedno nebo více komorové) a také cisternové vagony. Certifikát se vydává v okamžiku

expedice produktu z areálu společnosti ke každému expedovanému množství produktu. Tento systém obstarává činnost pro obě lokality.

SAP (Systems - Applications - Products in data processing) – Velmi robustní systém zastřešující ekonomickou část společnosti Více informací si k tomuto systému uvedeme v Litvínovské části. V kralupech je pouze testovací prostředí pro testování úprav, které jsou po jejich otestování následně implementovány do produktivního systému.
LD (Lotus Domino) – Jedná se o groupware systém. Tento systém zajišťuje převážně elektronickou poštu a online elektronickou komunikaci mezi zaměstnanci (lotus Sametime – obdoba ICQ a podobných systémů, ale určený pro korporátní sféru a umožňující, nejen krátké zprávy, ale i jiné způsoby a možnosti například web konference a podobně). Jsou zde umístěny dva servery lotus domino. Jeden obhospodařuje elektronické poštovní schránky zaměstnanců sídlících primárně v Kralupech a dále je zde server zajišující archivaci starých mailů a zároveň tento online server (Lotus sametime) pro online komunikaci pomocí krátkých textových zpráv.

O tiskové služby se stará print server, který obhospodařuje všechny tiskové fronty pro jednotlivé systémy (SAP tiskne v Postscriptovém formátu, ostatní systémy využívají PCL – Printer Command Language verze 5 nebo 6). Proto pro téměř všechny tiskárny nebo multifunkční zařízení existují dvě různé fronty. Print server řídí tisk všech těchto zařízení umístěných v Kralupech, ale zároveň je připraven obsloužit (v případě výpadku Litvínovského printserveru) všechna tisková zařízení i v Litvínově. Společnost není zastáncem malých tiskáren u každého počítače a v rámci behaviorální politiky zavedla velká multifunkční zařízení ve společných prostorách (chodby, společné místnosti a podobně). Jde hlavně o dva aspekty tohoto řešení. Uživatel, který pro každý vytisknutý papír musí zvednout své tělo ze židle, si nejprve rozmyslí, zda je opravdu nutné tento papír tisknou, čímž se podařilo snížit počet vytištěných listů (což vede k ochraně životního prostředí, a odrazí se to ve formě snížení nákladů). Druhým aspektem je zvýšený pohyb zaměstnanců se sedavým zaměstnáním v podobě určité přestávky v práci. Což mělo jistě pozitivní vliv na zdraví zaměstnanců a jejich pracovní výsledky.

Systém COTAS je specifický systém, zajišťující kontrolu a průběh plnění autocisteren. Kontroluje ADR (Evropská dohoda o přepravě nebezpečných věcí) jednotlivých cisteren, řídí provoz na plnících lávkách i samotný proces plnění. Jelikož se jedná o velmi nebezpečné prostředí, je zde kladen důraz na bezpečnost.

Řidič vozu má přidělenou identifikační kartu. Po přihlášení pomocí této karty se zkontroluje, zda byl řádně proškolen a je mu umožněno zadat parametry pro plnění autocisterny se kterou přijel. Každá autocisterna má svou další kartu, která po přihlášení nastaví parametry vozu, jako jsou velikosti jednotlivých komor, kolika komorová cisterna to je, zda má platnou ADR a podobně. Následně se zkontroluje, zda je kontrakt (na který přijede vozidlo naplnit) platný a je možné na něj dále čerpat. Pokud ano, je vozidlu přiřazena plnící lávka. Řidič následně projede vrátnicí na příslušnou lávku, musí se obléci do předepsaného obleku včetně všech ochranných pomůcek (brýle, rukavice, pevná obuv a podobně), musí vozidlo připojit k zemnícímu vedení a teprve následně připojit přívodní hadice. Po těchto úkonech je pak vozidlo systémem cotas automaticky naplněno, tak aby nedošlo k přeplnění (přetečení) komory. Při odjezdu jsou řidiči vydány certifikáty kvality k načerpaným produktům a dodací listy. V případech, kdy nějaká podmínka není splněná, dojde k zákazu naplnění autocisterny až do té doby, dokud nedojde ke zjednání nápravy.

Pro menší aplikace je využíván aplikační server. Společnost využívá aplikace třetích stran pro některé své činnosti. Typicky sem patří komunikace s bankami, nebo aplikace pro plánování a rozvoj výroby. Případně aplikace, které využívají některá oddělení, ale zároveň nejsou podporou výroby, ale podnikání společnosti. Různé BI (bussines inteligent) systémy například pro různé investice případně zhodnocování finančních prostředků společnosti a mnohé další aplikace.

Pro ochranu dat před jejich ztrátou se využívá zálohovací server s připojenou páskovou knihovnou a nainstalovaným zálohovacím softwarem společnosti Legato. Toto je jediný server, který je umístěn mimo datové centrum z důvodu bezpečnosti. Jedná se zejména o ochranu v případě, kdy by došlo ke zničení datového centra (požárem, poškozením nebo zničením budovy ve které datové centrum je umístěno a podobně). Využívá se víkendové full zalohování všech systémů (tedy kompletní záloha), nebo alespoň důležitých dat a konfigurací systémů. V týdnu (v pracovních dnech) se pak provádí pouze inkrementální zálohy. V pracovní době se následně provádí klony pásek, na kterých je uložena full záloha a tyto klony se z páskové knihovny vyjímají a uchovávají v budově velínu. Jedná se o budovu postavenou se zesílenými obvodovými zdmy tak, aby odolala všem nárokům, stejným jako pro atomový kryt a byla schopná odolat i pádu dopravního letadla.

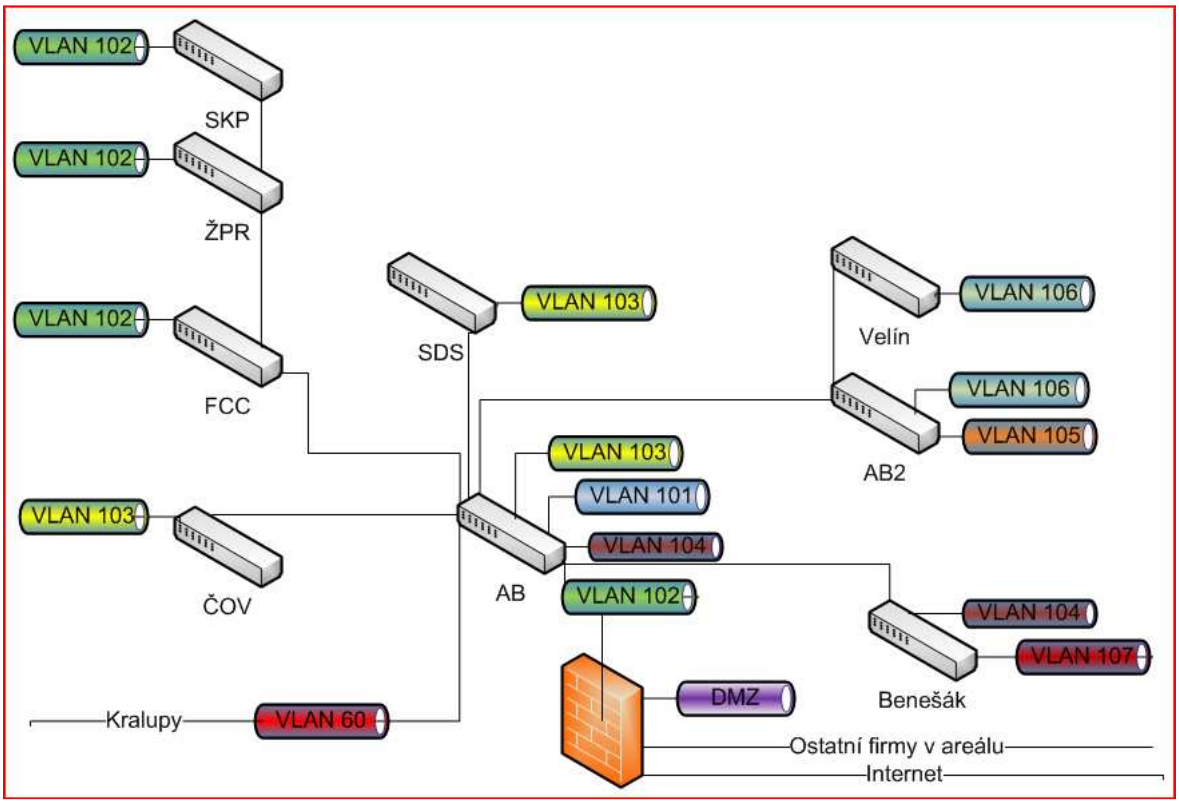
Pro elektronickou komunikaci po datové síti se využívá komunikační model TCP/IP. Je využíván neveřejný IP prostor třídy B, ale s maskou třídy C. Využívá se to pro snadnější řízení provozu na síti (adresa tedy vypadá například takto 172.16.1.120, maska 255.255.255.0 a výchozí brána 172.16.1.1) Můžeme tak mít k dispozici dostatečný počet virtuálních sítí (VLAN). Z obrázku (viz obr. 8), který jsme si uvedli již dříve, je znázorněno používání pěti VLAN v areálu Kralupy, které se liší změnou IP adresy ve třetím oktetu. VLAN 1 jedna má přidělený rozsah adres 172.16.1.x (x=0-255), VLAN 2 pak využívá rozsah adres 172.16.2.x, VLAN 3 využívá rozsah 172.16.3.x a tak dále na stejném principu jsou následně přidávány další VLAN podle potřeby.

4.2. Výchozí stav Litvínov

Druhým areálem společnosti, kde se nacházejí výrobní jednotky je v Litvínově, také zde si popíšeme výchozí stav pro diplomovou práci. I tento areál sdílí několik společností. O ostrahu a docházkový systém se stará společnost Chemopetrol, zároveň je společnost Chemopetrol, dodavatelem některých suroviny a energií pro námi zvolenou společnost, jako je například pára, teplárna, elektrická energie a další. Stejné nebo lépe řečeno obdobné podmínky, jako v prvním areálu jsou i v Litvínovském areálu. Jsou zde v majetklu společnosti některé budovy administrativní i výrobní. Za použití stejných norem, stejného modulárního systému a konec konců i stejného dodavatele (jedna firma a dva areály, tudíž se v drtivé většině projektů podílí stejný dodavatel na projektech v obou lokalitách) jsou zde vytvořeny sítě typu LAN a MAN. Tedy používá se i zde systém od výrobce AMP a pro kabeláž norma pro kategorii 6.

V Litvínově je stejně jako v Kralupech jedno datové centrum tvořené zvláštní místností opět označovanou jako serverovna, obsahující stejné centrum datových rozvodů. Ostatní budovy v areálu jsou propojené pomocí optických kabelů s budovou s datovým centrem. Jedná se tedy o spojení pomocí sítí typu MAN a využívá se znovu zapojení do hvězdy, kde datové centrum je středem těchto optických spojení. Tato fyzická infrastruktura sítě, je rozdělana do několika menších virtuálních sítí pomocí VLAN. Tyto sítě jsou distribuované (rozložené) přes několik budov. V tomto směru si jsou oba areály velice podobné, liší se snad jen rozlohou a umístěním jednotlivých systémů. O areálu v Kralupech se v narážkách říká, že se jedná o jakýsi zmenšený model Litvínova.

VLAN v litvínovském areálu jsou vytvářeny stejně jako v Kralupech, tedy dle potřeby a počtu přípojných míst.



OBR. 9 Propojení jednotlivých budov a VLAN, areál Litvínov

Serverovna v Litvínově je vybavena prakticky totožně jako v Kralupech. Jsou zde složitější úpravy vzduchotechniky, což pramení ze stavebního rozložení serverovny. Litvínovská serverovna je totiž vybudovaná ze dvou větších, vzájemně propojených místností, muselo dojít k zesílení nosných konstrukcí, z důvodu velkého zatížení a z důvodu umístění serverovny do prvního poschodí budovy. Takže je zde viditelné rozdělení, kde v první místnosti je místo pro racky zaplněné jednotlivými servery pro využívané systémy a ve druhé části, jsou umístěné aktivní prvky a datové rozvody. I zde je vstup do serverovny hlídán vstupním docházkovým systémem, který se snaží zabránit vstupu neoprávněných osob. Stejný princip chlazení serverovny jako v Kralupech, je používán i v tomto centru. Je zde využívána jak vzduchotechnika (pro zimní měsíce), tak opět dvě propojené chladící jednotky zajišťující téměř stálou teplotu v obou částech serverovny na úrovni 23^{o}C. Napájení serverovny je také ze dvou různých trafostanic, tyto přívody musely být při budování serverovny dokonce posíleny, aby vydržely předpokládáný příkon, princip přepínání, těchto přívodu je použitý stejný

jako v Kralupech. Stejný je také způsob zapojení centrálního záložního zdroje a menších záložních zdrojů umístěných ve všech racích pro servery a aktivní prvky.

Protipožární bezpečnostní předpisy v Litvínově jsou téměř totožné, jako v Kralupech. Oba areály jsou chemickým prostředím, tedy prostory s velmi nebezpečným provozem. Proto i zde jsou v datovém centru instalované protipožární systémy napojené na centrální pult chemického areálu, který má pod správou profesionální hasičský sbor. Vzhledem k velikosti areálu V Litvínově je i vzdálenost od datového centra větší než v kralupech, nicméně s dojezdem do tří minut od nahlášení požáru a to buď telefonicky nějakou osobou, nebo automaticky při oznámení nějakým čidlem.

V části pro datové rozvody jsou umístěny racky se zakončením místní sítě LAN (metalické rozvody obdobně jako v Kralupech), jsou zde zakončeny i optické kabely sítí MAN, které vedou (viz obrázek 8) do ostatních budov společnosti v Litvínovském areálu.

Aktivní prvky v této části tvoří hlavní router pro lokalitu, několik switchů s managementem a s rychlostí portů 10/100/1000. Rozdělen do několika virtuálních sítí VLAN. Několik mediakonvertorů a dalších aktivních prvků. Je zde hlavní firewall pro oddělení interní datové sítě společnosti od internetu, který zároveň vytváří demilitarizovanou zónu (DMZ) pro servery které jsou spravované z vnitřní sítě, ale zároveň na ně přistupují i uživatelé z veřejné sítě (internetu). Dále tento firewall odděluje a řídí provoz s ostatními společnostmi v litvínovském areálu, se kterými si naše společnost vyměňuje elektronická data, na základě nějaké dodavatelsko/odběratelské spolupráce. Litvínovská serverovna je větší a je zde provozováno přibližně 50 hardwarových serverů, i zde má každý server svůj diskový prostor a platí zde stejná pravidla pro obměnu hardware serverů jako v Kralupech. Jsou zde i stejné výkonové řady serverů od stejného výrobce (Hewlet Packard).

Softwarové systémy v druhé lokalitě fungují prakticky stejně jako v Kralupské lokalitě, zde si popíšeme jen rozdíly. Služby jako AD, DNS, DHCP, WINS a další, které podporují chod celé datové sítě, jsou nakonfigurovány prioritně pro Litvínovskou část datové sítě, v případě potřeby jsou schopné plnohodnotně nahradit tyto služby i pro Kralupskou část datové sítě (toto platí oboustranně).

Sdílení souborů na FILESERVERu v Litvínově zajišťuje domovské adresáře uživatelů primárně sídlících v dané lokalitě, dále zajišťuje sdílené datové prostory pro jednotlivá oddělení vytvářená na základě organizační struktury společnosti

(skupiny uživatelů s právy mazat, vedené v organizační struktuře v jedné organizační jednotce = v organizační struktuře jednomu oddělení). Toto je řešeno hierarchicky (stromovou strukturou), tedy nadřízení mají přístup do všech oddělení, které jsou pod jejich patronací, ale podřízení nemají k dispozici data, která jsou uložena na vyšší úrovni, než je jejich zařazení.

SAP (Systems - Applications - Products in data processing) – Tento robustní systém zastřešující hlavně ekonomickou část společnosti. Naše společnost provozuje moduly pro účetní a daňovou správu, modul pro skladovou evidenci, modul pro práci s lidskými zdroji (HR modul), dále se využívá SAP portál pro interní intranet (jakási nástěnka s informacemi pro všechny zaměstnance společnosti). Na části portálu funguje webový e-obchod s kancelářskými potřebami, s pitím a s drobnostmi do kuchyně, kde si může každý zaměstnanec společnosti pro potřeby celého oddělení objednat, co uzná za vhodné. Pokud je to v dalším kroku schváleno nějakým nadřízeným, který určí, z jakých peněz tento nákup bude hrazen. Následně je vygenerována objednávka na konkrétního předem smluvně vázaného dodavatele, který zajistít dodání objednávky na místo určení.

LD (Lotus Domino) – Groupware systém v Litvínově zajištuje elektronickou komunikaci společnosti s okolním „světem“. Jsou zde umístěny tři servery lotus domino. Jeden obhospodařuje elektronické poštovní schránky zaměstnanců sídlících primárně v Litvínově, další činností tohoto serveru je provoz groupware aplikací (telefonní seznam zaměstnanců, rezervace zasedacích místností, rezervace firemních automobilů a podobně). Další server zajišuje komunikaci mezi jednotlivými LD servery v rámci celé společnosti a zároveň vytváří SMTP servery pro všechny systémy v interní síti, které zasílají nějaké informativní maily uživatelům. Dále je zde umístěn Blackberry enterprise server, který zajišťuje předávání elektronické pošty, úkolů a adresáře společnosti na blackberry mobilní zařízení od společnosti RIM. Třetí server LD je umístěn do DMZ a zajišťuje odesílání mailů od zaměstnanců společnosti na adresy příjemců v internetu a zároveň je příjemcem elektronické pošty z interntu pro domény crc.cz a ceskarafinerska.cz. Provozuje se na něm služba Lotus Traveler, která je obdobou systému Blackberry, ale funguje téměř na všech „chytrých“ mobilních zařízeních. Oba systémy jsou velmi podobné a mají své výhody i nevýhody. Traveler je v rámci licence Lotud Notes zdarma. Patří sem ještě jeden server umístěný v DMZ, i když není z dílny IBM

(výrobce Lotus Domino), ale jelikož veškerá příchozí elektronická pošta z internetu tímto serverem projde a je následně zkontrolována zda se nejedná o spam, je na místě zde jeho uvedení. Jedná se o Symantec message gateway, která na základě pravidelných aktualizací dokáže účinně filtrovat nevyžádanou poštu. Vytváří reporty pro prezentaci managementu, jak účinné řešení IT využívá. Lze zde ručně definovat pravidla, co a jak se má udělat s příchozí elektronickou poštou v případě, kdy se jedná o spam, potenciální spam nebo o zavirovaný dokument.

Tiskové služby jsou v Litvínově řešeny zrcadlově oproti řešení v Kralupech. Tedy primárně zajišťují funkcionalitu pro tisková zařízení umístěná v Litvínově, ale v případě nějakého výpadku Kralupského printserveru je možné zajistit tímto serverem i obsluhu tiskových zařízení umístěných v Kralupech.

Systém COTAS je také v Litvínově u plnících lávek pro autocisterny. V Litvínově je menší počet lávek než v Kralupech. Protože Kralupy mají lepší geografickou polohu pro distribuci paliv po České republice a proto většina plnění autocisteren je prováděna právě v Kralupech. Hotové produkty případně meziprodukty, z Litvínova do Kralup, jsou dopravovány pomocí produktovou.

Systém EMC Documentum je špičkový systém pro správu, editaci, archivaci dokumentů a případně jejich verzování (zaznamenávání uložených změn). Pracuje nad databází systému Oracle, ve které si uchovává metadata (data o datech). Pracuje s dokumenty jako s přílohami a umožňuje jejich snadné verzování. Lze vytvářet dokumenty na základě šablon (tedy předem definovaných polí). Umožňuje vytvářet dokumenty z formulářů a podobně. Zde se to využívá pro ukládání smluv a jejich různých verzí včetně schvalovacího workflow (schvalovací předem definovaný postup po sobě následujících kroků – každý schvalovatel může schválit dokument, napsat připomínku nebo zamítnout dokument a podobně). Tento systém se nadále využívá pro technickou dokumentaci výrobních zařízení, jsou zde zaznamenávany všechny změny (opravy, rekonstrukce, změny technologií a podobně).

Další službou provozovanou v Litvínovském data centru je server proxy pro přístup koncových zařízení v datové síti společnosti do internetu. Je zde zavedena filtrace internetových stránek s nevhodným obsahem. Filtruje se pomocí vyhledávání nežádoucích slov, jako je sex a podobné výrazy. Je zde možnost vytváření statistik, jaké stránky konkrétní zaměstnanec navštěvuje a podobně. Tyto statistiky

se nevyhodnocují průběžně (pokud není se zaměstnancem žádný problém, může si na internetu brouzdat, jak chce bez omezení, kromě již zmíněných filtrů). Pokud je se zaměstnancem veden, ze strany společnosti, nějaký spor (neplní si své úkoly řádně, nebo zapříčinil nějakou mimořádnou událost), pak se tyto statistiky na vyžádání příslušného manažera vyhodnocují a pokud se zde objevují stránky například nadměrného přístupu k sociálním sítím nebo sázení na internetu a pododbně, jsou tyto statistiky považovány jako přitěžující okolnost.

V litvínovském data centru jsou další dva servery pro menší aplikace třetích stran obdobně, jako tomu je v Kralupech. Stejně je řešeno i zálohování pomocí jednoho serveru a páskové knihovny, za využití stejného principu zálohování pomocí systému Legato.

VLAN sítě v litvínovském areálu (viz obr. 9) jsou vytvářené také dle počtu zařízení. Adresace koncových zařízení pro jednotlivé VLAN je následující: VLAN 101 má přidělený rozsah adres 172.16.101.x (x=0-255), VLAN 102 pak využívá rozsah adres 172.16.102.x, VLAN 3 využívá rozsah 172.16.103.x a tak dále, na stejném principu jsou následně přidávány další VLAN podle potřeby.

Další součástí datového centra jsou dva servery, jeden se využívá pro centrální správu všech parcovních stanic a vzdálených instalací antivirového řešení od společnosti Symantec, tento server má u sebe vytvořený obraz všech aktualizací vydaných výrobcem, které každých deset minut kontroluje, zda není vytvořená nějaká nová aktualizace. Koncové stanice pak aktualizují své lokální virové definice z tohoto serveru, takže nedochází k nadměrnému zatěžování internetového připojení. Druhý server je používán jako distribuční. Jsou na něm vytvářené instalační balíčky jednotlivých aplikací, které jsou pomocí SMS (System Management Server) serveru distribuovány na koncové stanice, součástí tohoto serveru je stahování a distribuce aktualizací oprav a záplat vydávaných společností Microsoft v pravidelných intervalech (cca 1x za měsíc), případně mimořádně vydaných kritických oprav i mimo toto pravidelné zveřejňování.

V datovém centru v Litvínově je vytvořená demilitarizovaná zóna (DMZ). Jedná se o zvláštní segment sítě s veřejnými adresami, který je oddělen na obou stranách firewallem, tedy jak na straně do interentu, tak na straně do interní sítě společnosti. Zde se nachází všechny servery přístupné z internetu. Je zde webový portál pro prezentaci firmy. Dále je zde server zpřístupňující pro kontraktory znění norem, které musí dodržet u projektů, na kterých spolupracují. Dále je zde server pro antivirovou a antispamovou

kontrolu příchozí elektronické pošty (Symantec Message Gateway) a server pro odchozí poštu ze společnosti na ostatní internetové domény. Tento server zajišťuje také replikaci několika databází, případně aplikací s jinými společnostmi v holdingu Unipetrol, kteří také využívají Lotus Domino. Je zde také softwarový router pro Blackberry zařízení.

Všechny systémy ve vnitřní síti komunikují v obou lokalitách v nezabezpečeném režimu s výjimkou systému Lotus Domino, který byl vyvíjem pro armádu Spojených států Amerických s důrazem na bezpečnost. Proto tento systém komunikuje na speciálním TCP portu 1352 a využívá asynchronního šifrování.

4.3. Propojení areálů

Propojení areálů je zajišťováno pomocí microvlného spojení, za pomoci několika retransakčních stanic (trasa prochází vzdušnou cestou s přímou viditelností z Litvínova přes Milešovku a Škarechov do Kralup) v 5GHz licencovaném pásmu. Záložní spojení, které se využívá, jen v případě nefunkčního primárního propojení, a je zajišťováno 30-ti kanálovým ISDN propojením, kdy jednotlivé kanály se připojují dle provozu na lince.

Na firewallu společnosti jsou další dvě vnější rozhraní, jedno je připojené do společené sítě celého holdingu Unipetrol. Tato síť je neveřejná a je využívána pro propojení systémů, jako je například systém ISDL pro železniční dopravu (řazení vlaků), propojení účetních systémů v podobě předávání dodacích a fakturačních údajů a další systémy, které si vyměňují automaticky nějaká data. Není předmětem této diplomové práce zde jednotlivé systémy vyjmenovávat.

Je zde využíván extranet switch, který zajišťuje VPN (Virtual Private Network) šifrované spojení mezi instalovaným klientem (většinou na notebooku zaměstnance společnosti, ale existují i vyjímky, kdy má zaměstnanec doma pevný počítač společnosti, například při dlouhodobé rehabilitaci a jeho přítomnost na pracovišti není striktně vyžadována) a extranet switchem. Toto spojení vytvoří přes internet jakýsi tunel a počítač nebo notebook, se pomocí tohoto spojení připojí do vnitřní sítě společnost. Nadále pak zaměstnanec pracuje úplně stejně, jako by se nacházel v některém ze dvou areálů společnosti. Případně je mu umožněno pracovat pomocí terminál serveru od společnosti Microsoft a to v případě, že spojení do internetu je zajišťované nějakou pomalejší linkou.

Kontraktoři (zaměstnanci externích společností, kteří mají podepsaný kontrakt na práci v nějakém projektu) se dělí do několika skupin. První skupina má pouze přístup na veřejně dostupné věci (ošetřené jménem a heslem) z internetu (normy, nějaké smlouvy, případně různé dokumenty). Druhá skupina pracuje přes VPN připojení, pomocí terminál serveru na systémech, ke kterým má přidělená práva. Třetí skupinou jsou kontraktoři, kteří pracují přímo v areálech společnosti, a je jim dán k dispozici počítač v datové síti společnosti s příslušně omezenými právy.

Připojení společnosti do internetu je oddělené pomocí firewallu s NAT (Network Address Translation), celá síť společnosti se na internetu objevuje pouze pod jednou veřejnou IP adresou. Připojení je realizováno pomocí WIFI s rychlostí až 8 MGbp.

4.4. Uživatelské prostředí

Uživatelské prostředí pro všechny zaměstnance vychází z jednoduchého požadavku, aby uživatel nebyl vázán konkrétním počítačem. Každý uživatel může využít služeb jakéhokoli volného počítače, kdekoli v areálu společnosti. Přihlásí se pod svým jménem a heslem a bude mít k dispozici minimálně základní věci. Přístup do své elektronické pošty a aplikací v groupware, přístup do systémů Documentum, SAP, LIMS, bude moci tisknout na nejbližší tiskárně, dále bude mít přístup na intranet i internet. Bude mít k dispozici své projekty, svůj domovský adresář i společný adresář pro oddělení. Bude moci využívat lokálně instalované aplikace a programy, jako jsou MS Office, prohlížeč pdf souborů, prohlížeč dwg souborů a další programy, které jsou součástí předem připravené image disku koncových zařízení. Jedinné co nebude mít k dipozici jsou licencované programy, které vyžadují nějakou (alespoň minimální) lokální instalaci a jsou omezené počtem instalací, takovéto programy bude mít k dispozici jen v počítači, který je umístěn v uživateli přiřazené kanceláři. Tyto programy se doinstalovávají IT technikem ze SMS serveru, na požadavek nadřízeného nebo dle vyplývajících potřeb dané konkrétní pracovní pozice zaměstnance.

4.5. Prostředí společnosti a dohled ICT systémů

Výrobní části společnosti pracují ve velmi nebezpečném prostředí za souvislého, nepřetržitého provozu. Proto je kladen velký důraz na dostupnost všech služeb a výrobních kapacit. ICT struktura je základním kamenem pro fungování společnosti v takto náročném

provozu. Dostupnost služeb a datové sítě je tedy klíčová a je stanovena dle SLA (Service Level Agreement) na 99% dostupnosti všech ICT systémů (včetně infrastruktury) v období jednoho roku. Nedodržení této hranice znamená snížení osobního ohodnocení všech zúčastněných zaměstnanců. Proto ICT oddělení hledá všechny možnosti a prostředky k dosažení této 99% hranice. Využívá dohledové nástroje od výrobce hardwaru, využívá dohledu systémem WhatsUp, který dokáže hlídata pomocí SNMP protokolu všechna zařízení na síti a nejen dostupnost zařízení, ale i jednotlivých služeb nebo programů spuštěných na jednotlivých zařízeních. Správa systémů musí být co nejjednodušší, proto se využívá standardních management konzolí jako je MMC (Microsoft Management Console) pro správu domény, případně HP overview což je konzole pro správu hardware serverů a další podpůrné systémy, které slouží jak pro konfiguraci a nastavování práv uživatelů a zařízení, ale zároveň dokáží identifikovat vzniklý problém a okamžitě uvědomit zodpovědné pracovníky na vzniklou situaci, tak aby došlo k okamžité reakci (v pracovní době k nápravě, a v mimo pracovní dobu, dle nastavených SLA a pohotovostí zodpovědných zaměstnanců) ze strany zaměstnanců společnosti případně v kooperaci se smluvním partnerem. Tyto systémy mnohdy dokáží identifikovat možný problém, ještě před tím než k závadě dojde (například vyhodnotí zvýšenou chybovost disku a podobně).

V další části diplomové práce si popíšeme jednotlivé projekty, které ve svém důsledku vedou ke zvýšení bezpečnost ICT infrastruktury z hlediska vnitřního zabezpečení. Po ukončení jednotlivých projektů dojde vždy v určité části ICT infrastruktury ke zvýšení bezpečnosti. V podobě například bezpečnějších dat společnosti, nebo ke zvýšení dostupnosti, spolehlivosti a bezpečnosti celé ICT infrastruktury. Jednotlivé projekty nejsou nijak seřazené, některé stále probíhají, jiné jsou již realizované nebo alespoň z části realizované, některé byly připravené, ale nakonec k jejich realizaci z nějakých důvodů nedošlo a podobně. Pořadí je zapsané, tak jak autorovi přišly na mysl, a ne jak šly chronologicky za sebou, nebo se souběžně pracovalo na více projektech zároveň.

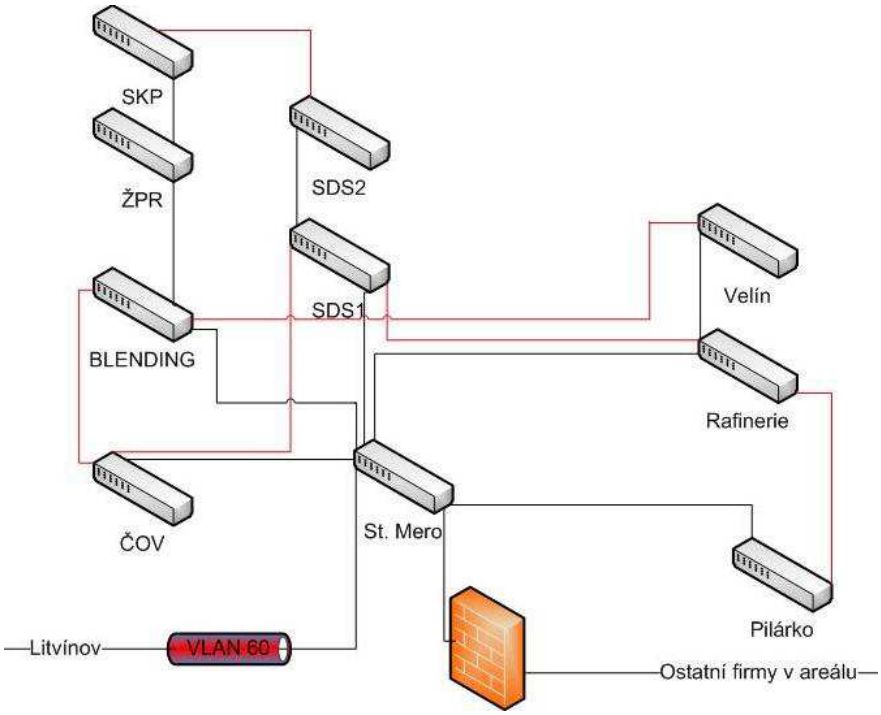
4.6. Projekt „Redundance optických tras“

První projekt, který si zde uvedeme, je projekt nazvaný „Redundance optických tras“. Tento projekt si klade za cíl v každé lokalitě zajistit dostupnost a funkční připojení

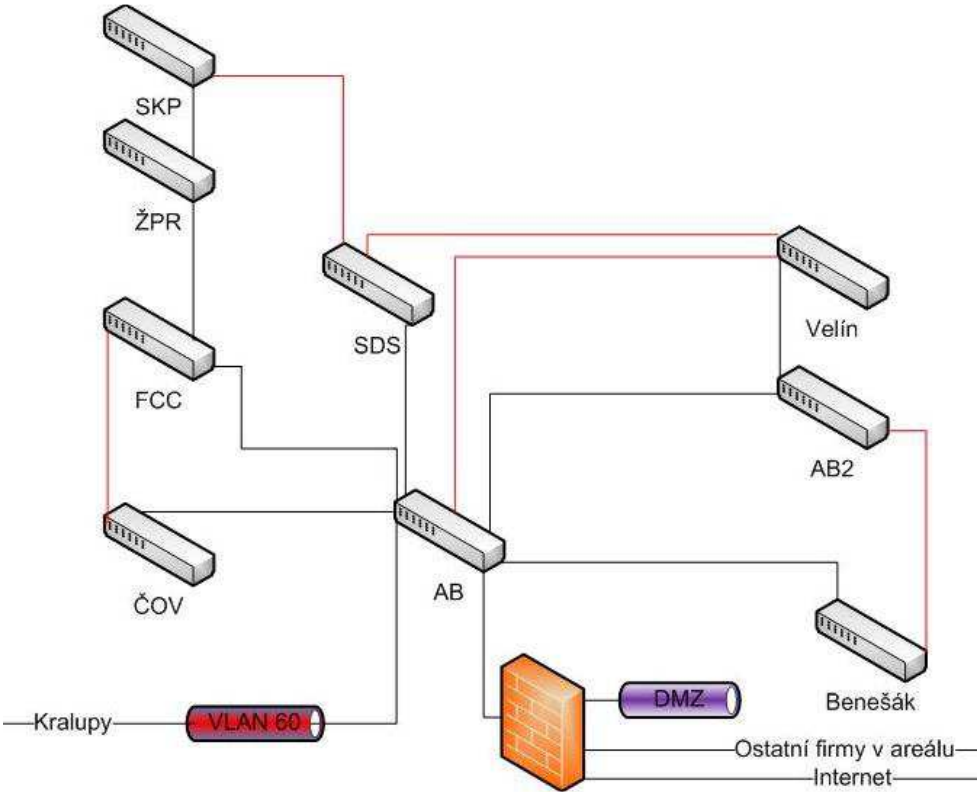
všech budov i v případě přerušení některé optické trasy. Jak se prokazatelně stalo při jedné mimořádné události, kdy došlo k lokálnímu požáru pod potrubním mostem, na kterém zaroveň byla vedena trasa optického kabelu datové sítě, jenž byl tímto požárem zasažen až došlo k celkovému spálení optického kabelu v délce přibližně patnácti metrů. Problém vznikl i přesto, že nikdo neporušil žádné, doté doby známé bezpečnostní předpisy. V oblasti, kde k požáru následně došlo, byly v jeden okamžik nahlášené dvě opravy, jedna měla za úkol opravit tepelné těsnění poškozené na plynovém potrubním vedení. Vyškolený zaměstnanec opravu prováděl dle předpisů i s platným pracovním povolením. Jenže při odstraňování poškozené tepelné ochrany došlo k drobnému úniku plynu, který je těžší než vzduch a ten se dostal k zemi. Přibližně třicet metrů od této opravy se chystal zaměstnanec kontraktora opravovat část konstrukce potrubního mostu. Také měl všechna potřebná povolení, dokonce i na práci s otevřeným ohněm, jelikož pracoval s elektrickou bruskou, od které létají jiskry. Měl připravený hasicí přístroj a všechny ochrané pomůcky dle předpisů. Problém byl v tom, že tyto práce byly hlášené správně, ale každá na jiné části provozu podle příslušnosti těchto konstrukcí, takže je povoloval pokaždé jiný směnový manažer zodpovědný za svou část provozu a tudíž o té druhé prováděné opravě neměl žádné informace. Následně došlo k tomu, že onen pracovník brousil frézou, mezi nohama mu létaly jiskry a za ním vzplanul na zemi se povalující plyn. Naštěstí se nikomu nic nestalo, ale škody šli do milionů korun a došlo k odpojení několika velmi důležitých budov. Na základě této události došlo ke změně bezpečnostních předpisů při práci s otevřeným ohněm (vždy musí být přítomna jednotka hasičů), dále došlo ke změně při schvalování povolení na práci (povolení musí schválit jak směnový manažer, tak také ředitel rafinerie). ICT oddělení dokázalo obnovit připojení zasažených budov pomocí náhradního spojení během přibližně šesti hodin. Nicméně následně došlo k vytvoření projektu redundance optických tras v obou areálech.

Na obrázcích je zakreslen výsledný stav pro obě lokality, kterého chce společnost dosáhnout. Jak mají být jednotlivé budovy propojeny (viz obr.10 a obr.11 – červené propojení jsou nově budované trasy na základě tohoto projektu). Bylo zdůrazněno pravidlo minimálně dvou přívodů optických tras, pokaždé z jiného směru, do budovy. Což následně bylo dodrženo s výjimkou budovy ŽPR v Kralupech, jelikož se jedná o přetlakovou místnost, je zde zbudován pouze jeden vstup pro optické kabely. Zde je z pohledu bezpečnosti kritické místo, kdy nám posledních přibližně 15 metrů vedou optické kabely

stejnou trasou. Jedná se tedy o potenciální bezpečnostní problém, o kterém je vedení společnosti informováno. Tento potencionální problém bude řešen někdy v budoucnu při případné rekonstrukci celé plnící rampy.



OBR. 10 Projekt redundance optických tras, areál Kralupy



OBR. 11 Projekt redundance optických tras, areál Litvínov

Tento projekt je téměř dokončen. Zbývá dovybudovat poslední trasu v Kralupech mezi budovou SKP a budovou SDS2, kde tomu brání geografická poloha těchto budov, kdy nelze vybudovat přímou trasu, jelikož mezi objekty je soukromé pole a vybudování trasy pouze areálem by znamenalo trasu o zhruba tři kilometry delší a tím pádem i vyšší náklady. Tento projekt tedy dosud není uzavřen. Stále je v jednání několik variant pro tuto poslední trasu a zatím není jasné, která varianta bude zvolena.

4.7. Projekt „Definice SLA“

Projekt číslo dva „Definice SLA“, kdy vedení definuje (ve spolupráci s ICT oddělením) systémy a služby, které jsou pro společnost klíčové a jaké požaduje reakce a definuje nejdelší časy ke zjednání nápravy (v případě nějaké mimořádné události, závady na hardware a podobně). V návaznosti na definované SLA jsou následně drženy některé díly skladem, případně se podepisuje smlouva s dodavatelem o dodání vadného zařízení do nějakého časového úseku. Jedná se především o oblasti aktivních prvků a serverů, případně některých dílů. Tento projekt je při každé změně v některém systému (upgrade serverů, výměna aktivních prvků a podobně) znovu podroben kontrole a následně upravován, aby platil dle aktuálního stavu systémů.

4.8. Projekt „Interní směrnice a normy“

Projekt číslo tři mělo za úkol vedení ICT oddělení a jednalo se o definici interních norem a předpisů pro chování uživatelů na datové síti společnosti. Při tvorbě vlastních předpisů vycházelo vedení ICT ze dvou zdrojů jedním je převzetí norem DEPTS od svého akcionáře společnosti Shell a dále dle certifikátů kvality ISO 9000, kterým prochází výroba a laboratoře společnosti. Výsledkem jsou interní předpisy zveřejněné na intranetu společnosti a každý zaměstnanec má povinost se s nimi seznámit a dodržovat je. Jedná se zejména o dodržování pravidel o vytváření elektronického obsahu a nepovoleném stahování obsahu a aplikací z internetu, aby nedošlo k poškozování práv třetích subjektů. Při zjištění nepovoleného obsahu ze strany ICT oddělení je zjištěn konkrétní zaměstnanec, který si nedovoleně pořídil a na discích společnosti uchovává nepovolený obsah (videa, mp3, instaloval aplikace z internetu a podobně). Tento zaměstnanec je upozorněn

elektronicky od ICT odd., a zároveň je informován zaměstnancův nadřízený. V případě, že se toto opakuje, může to vést až k ukončení pracovního poměru se zaměstnancem.

4.9. Projekt „Bezpečnost datových rozvodů“

Projekt číslo čtyři je pravidelný projekt, který se opakuje přibližně každé dva roky. Jde o bezpečnost datových rozvodů. ICT technik má za úkol zkontrolovat všechny koncové datové zásuvky. Datové rozvody jsou mnohdy vybudovány i do míst, kde se pouze předpokládá jejich využití někdy v budoucnu, ale dosud nejsou využívány. Proto ICT technik zkontroluje všechny zásuvky a v racku odpojí od aktivního prvku koncové zásuvky, které jsou nevyužívané a hlavně jsou snadno přístupné (na chodbách, ve volných kancelářích a podobně). Tím se snažíme zvýšit bezpečnost datové sítě znemožněním nechtěného a nepozorovaného odposlechu dat na síti. Samozřejmě existuje několik koncových zásuvek, které nejsou využívané trvale, ale je žádoucí, aby zůstaly zapojené do aktivního prvku (například pro sdílené kanceláře pro zaměstnance, kteří přijedou z druhé lokality se svým notebookem a podobně). Takovéto zásuvky se „vypínají“ na konkrétním aktivním prvku (nastavují se do stavu „down“) ke kterému jsou připojené.

4.10. Projekt „Propojení areálů a internet“

Projekt číslo pět „Navýšení rychlosti přípojení do internetu a změna propojení areálů společnosti“. Vzhledem k vysokým provozním nákladům u microvlného spojení (licencované pásmo není zdarma) a v případě výpadku u záložní ISDN (den provozu podle přenesených dat vyšel i na 250.000,- korun), se v rámci tohoto projektu hledalo řešení, které bude levnější, stabilnější a v rámci možností i rychlejší. Zvažovali se varianty položení optického kabelu podle produktovodů, ale to bylo shledáno jako rizikové. Nakonec se vybralo řešení nabídnuté firmou Sloanpark, která je zároveň poskytovatelem připojení do internetu pro naši společnost. Jedná se o řešení pomocí optických kabelů, kdy byly nabídnuty dvě rozdílné trasy. Jedna se využívá pro primární propojení s rychlostí fast ethernetu (100Mbps full duplex) a druhá trasa, která vede jinou geografickou trasou a je vedena jako záložní s omezenou propustností (20Mbps). Dále bylo změněno i připojení společnosti do internetu. Propojení je nyní realizováno optickým připojením o rychlosti 80Mbps se záložním bezdrátovým připojením o rychlosti 16Mbps. Oproti původnímu propojení došlo k vyraznému navýšení přenosové rychlosti a stability

spojení a to jak mezi areály, tak do internetu. Navíc to vedlo ke snížení pravidelných měsíčních finančních nákladů zhruba o jednu čtvrtinu.

4.11. Projekt „Nezávislé datové centrum“

Projekt číslo šest „Nezávislé datové centrum“, zvažoval z důvodu bezpečnosti systémů umístění jednoho datového centra mimo areály společnosti a jeho napojení na obě lokality, tak aby při nějakém, zejména teroristickém, útoku na rafinerie byla data zcela ochráněna. Uvažovalo se o trojúhelníkovém zapojení, pokaždé dvěmi různými optickými trasami. Zvažovaná lokalita byla v oblasti Loun, které jsou geograficky vhodné pro tento projekt. Projekt se připravoval zejména po teroristických útocích ve Spojených státech Amerických z 11.září 2001. K realizaci nakonec nedošlo, z důvodu vysokých pořizovacích nákladů. Nicméně upravily se zálohovací zvyklosti ve společnosti. Servery pro zálohování, včetně páskových knihoven, byly umístěny do jiných budov, než ve kterých jsou umístěné datová centra (serverovny). Pokud by došlo ke zniční budovy s datovým centrem, aby bylo možné systémy relativně rychle znovu obnovit ze záloh a na základě toho došlo k minimálnímu výpadku ICT systémů společnosti a tím se zároveň minimalizovala účetní ztráta společnosti.

4.12. Projekt „NAS“

Projekt číslo sedm „NAS“. Pro větší ochranu dat před jejich ztrátou (například z důvodu vadného disku) ve velkém počtu malých diskových polí, který měl každý server k dispozici. Byl vytvořen projekt pro instalaci robustního řešení NAS (Network Area Storage) a připojení všech stávajících serverů k tomuto poli a odpojení zastaralých lokálních polí. Bylo vybráno řešení od společnost Hewlet Packard EVA 4100. Tento plně redundantní systém zaručoval vysokou dostupnost dat a byl instalován v litvínovském datacentru. Následovalo postupné připojování stávajících serverů v litvínovské lokalitě k tomuto poli, s tím spojené migraci dat ze stávajících diskových polí a jejich následné odpojení. Byla vykázána úspora na elektrické energii po odpojení všech lokálních diskových polí a také poklesl počet výměn jednotlivých disků (vykazující zvýšenou chybovost). Tento projekt jistě přinesl spoustu dobrého. Přes vysoké pořizovací náklady dokázal ušetřit spoustu prostředků do budoucna. Bohužel také zapříčinil nejdelší výpadek ICT systémů v historii společnosti. Při updatu firmwaru

jednotlivých disků v poli, který byl řádně certifikován výrobcem. Společnosti bylo doporučeno jeho provedení na využívaném poli zástupcem výrobce. Bohužel po provedení firmwaru u zhruba poloviny disků, kde vše proběhlo korektně, u dalšího disku došlo k zamrznutí procesu a následně k nedostupnosti všech dat na tomto NAS umístěných. Odstávka systémů a oprava ze strany výrobce trvala celých 28 hodin, než došlo k obnově činnosti celého NAS zařízení. V průběhu oprav se uvažovalo o přivezení jiného pole s podobnými parametry a následně obnovu všech systémů ze záloh. Dle propočtů by obnova všech systémů trvala přibližně 36 hodin, z tohoto důvodu se obnova dat nerealizovala a čekalo se na vyřešení vzniklé situace ze strany výrobce. Což se také po 28 hodinách podařilo, nicméně nebyla to levná záležitost. Jelikož chyba nevznikla na hardwaru NAS zařízení, ale na jeho softwarové části, která však nebyla součástí servisní smlouvy. Výrobce neúčtoval prvních 24 hodin, kdy hledal příčinu problému. Následující 4 hodiny si plně vyúčtoval, z důvodu speciálně programovaného fixu (opravný balíček) pro společností využívaný NAS. Až sedmá varianta tohoto fixu byla úspěšná a NAS zařízení znovu začalo fungovat stejně jako před vzniklým problémem.

4.13. Projekt „Virtualizace serverů“

Projekt číslo osm „Virtualizace serverů“. V rámci zvýšení bezpečnosti serverů z hlediska jejich dostupnosti a také na základě snižování nákladů při pravidelné obměně hardwaru serverů, byl spuštěn projekt vizualizace a snižování počtu serverů. Tento projekt následoval po projektech číslo šest a sedm. Na platformě VMware ESXi je vytvořené virtuální prostředí s hardwarovou konfigurací o šesti serverech (nodech) s celkovou kapacitou 48 CPU (4 jádrové procesory) a 164GB RAM s připojením již dříve zmiňovaným NAS. Stávající servery byly rozdělené do tří kategorií podle náročnosti jejich migrace do tohoto prostředí. V první kategorii byly přesouvány menší systémy, případně byly slučovány servery, které plnily stejnou funkci v obou lokalitách. Jedná se o servery pro elektronickou poštu, které jsou nově jen v litvínovském datacentru. Zároveň se spojily dva mailové servery do jednoho. Dále se migrovaly servery pro doménu, AD, distribuci aplikací, printservery a podobné servery. Stejně tak se sloučily aplikační servery a vyžívá se již jen jeden opět v litvínovském virtuálním prostředí. Ve druhé kategorii byly přesouvány systémy se složitější strukturou (například LIMS, Databázové servery a další). V poslední kategorii pak byly přesouvány nejnáročnější

systémy, jako je SAP a všechny jeho podsystémy (nákup, portál a podobně). V kralupském datacentru bylo vytvořeno obdobné virtuální prostředí s podstatně skromnější hardwarovou konfigurací. Bylo využito jednoho lokálního diskového pole a do VMware ESXi prostředí byly zařazeny dva nejvýkonnější hardwarové servery, které ve společnosti zůstaly volné po migraci systémů do litvínského virtuálního prostředí. V tomto kralupském datovém centru tedy zbyly jen nejnutnější služby sítě, které jsou nutné pro zajištění chodu sítě v případě přerušení spojení mezi lokalitami. Zůstaly zde servery zajišťující dostupnost služeb AD, DHCP, DNS, WINS, print server, file server a několik testovacích serverů, vše ostatní bylo přesunuto do Litvínova.

4.14. Projekt „Zálohování dat“

Projekt číslo devět „Zálohování dat“. Po projektu číslo osm a s tím spojené velké přesuny dat do litvínovského datového centra, musle dojít ke změnám v dosavadním způsobu zálohování. Objem dat byl najednou tak veliký, že víkendová záloha prodloužila dobu zálohování až do pondělních odpoledních hodin. Následné klonování pásek (tyto pásky se z páskové knihovny vyndavají a uchovávají v trezoru) trvalo až do odpoledních hodin ve středu. Což ve svém důsledku znamenalo nemožnost provádět obnovu dat z pásek v období od pátečního večera až do středečního odpoledne. Stejně tak první inkrementální záloha se prováděla až v nočních hodinách ve středu. Tento stav byl vyhodnocen jako neúnosný a byl vytvořen nový projekt pro zálohování dat. Ve výběrovém řízení bylo vybráno deduplikační zařízení s diskovou cache, pracující se stávajícím zálohovacím systémem společnosti Legato i se stejnou páskovou knihovnou. Zálohovací proces byl následně upraven. Některé servery se přestaly zálohovat jako dosud souborově, ale využilo se možnosti VMware ESXi systému vytvořit v daný okamžik obraz (image) běžícího serveru. Tato image byla následně přenesena na zálohu, odkud ji lze kdykoliv obnovit. Tohoto principu se využilo u serverů, kde se neprovádějí časté změny. Zejména u serverů umístěných v demilitarizované zóně. Zapojení deduplikačního zařízení a diskové cache do zálohovacího procesu mělo téměř neuvěřitelný progres pro stávající zálohovací praktiky ve společnosti. Radikálně se snížil objem zálohovaných dat (přibližně o dvě třetiny), zároveň se změnila doba zálohování z řádu několika dní na zálohování v řádu hodin. Navíc obnovovat jde prakticky okamžitě po ukončení zálohovacího save setu. (Save set – část zálohování například jeden server, nebo jeden

diskový prostor. Záleží, jak jsou jednotlivé save sety definovány v zálohovacím procesu a jak postupně na sebe navazují.) Záloha nyní probíhá nejprve na diskovou cache při použití deduplikačnícho zařízení, následně je záloha prováděna z diskové cache na páskovou knihovnu a stejně jako dosud probíhá následné klonování pásek. Toto řešení má jednu nespornou výhodu, že to již neblokuje systém pro obnovu dat a je tedy možné obnovovat i při současném klonování pásek nebo zálohování na páskovou knihovnu z diskové cache.

4.15. Projekt „VLAN“

Projekt deset „Využití VLAN dle společných rysů segmentu sítě“. Neudržitelný stav využívání VLAN dle počtu koncových zásuvek je z hlediska bezpečnosti ne zrovna dostatečné využití nabízených možností VLAN. Proto vznikl projekt na správnou definici a následnou distribuci jednotlivých VLAN na konkrétní porty aktivních prvků a následně na konkrétní koncové zásuvky. Stávající rozdělení IP rozsahu jedné VLAN bylo následující (toto rozdělení je pro všechny VLAN v obou areálech stejné). VLAN 1 má IP rozsah rozdělen následovně: 172.16.1.x tato část adresy je stejná v celé virtuální síti. Poslední oktet sítě se pak rozděluje následovně 0 – celá síť, 1 router (pro stanice default gateway – výchozí brána), 2 – 20 rozsah pro aktivní prvky, 21 – 40 rozsah pro servery, 41 – 130 rozsah pro přiřazování DHCP serverem v Kralupech, 131 – 210 rozsah pro přiřazování DHCP serverem v Litvínově, 211 - 230 rozsah pro zařízení, která vyžadují pevné přiřazení IP adresy (například tiskárny, analyzátory, multifunkční zařízení a podobně), 231 – 254 speciální adresy pro zařízení ICT oddělení (HP overview – Compaq imide manager, whatsup a podobné administrátorské nástroje), 255 broadcast.

Nové rozdělení vždy vyčlení téměř celý rozsah pro daný účel při zachování následujících pravidel. VLAN 1 má nově rozdělení takto 172.16.1.x (tak jako dosud), 0 celá síť, 1 router (pro stanice/servery default gateway – výchozí brána), 2 – 254 pro servery, 255 broadcast. Obdobně je to pro všechny další VLAN, kde se liší jen využití IP adres v rozsahu 2 – 254, kde jsou adresy v tomto rozsahu přiřazovány příslušným DHCP serverem, pokud nějaké zařízení vyžaduje stále stejnou IP adresu (například tiskárny), je tato adresa na základě MAC adresy (Media Access Control -

jednoznačný identifikátor síťového rozhraní) zařízení přiřazována permanentně – zařízení pokaždé dostane stejnou adresu.

VLAN 1 je tedy 172.16.1.2 - 254 určena pro připojení serverů v Kralupech ve správě ICT oddělení, tyto adresy se přidělují ručně. VLAN 2 má rozsah 172.16.2.2 – 254 určen pro Laboratoře a laboratorní přístroje, tyto adresy se přidělují DHCP serverem. VLAN 3 má rozsah 172.16.3.2 – 254 určen pro koncové zařízení v budově St. MERO, také přiřazované pomocí DHCP. VLAN 4 a 5 mají rozsah 172.16.4(5).2 – 254 rozsahy pro koncová zařízení v administrativních budovách, přiřazované pomocí DHCP. VLAN 6 a 7 mají rozsah 172.16.6(7).2 – 254 rozsahy pro koncová zařízení ve výrobních budovách, přiřazované pomocí DHCP. VLAN 8 má rozsah 172.16.8.2 – 254 rozsahy pro druhé síťové rozhraní serverů využívané jen pro zálohování dat, adresy jsou přiřazované ručně a mají stejnou koncovou část adresy, jako rozhraní přes které je provozován běžný provoz. VLAN 9 má rozsah 172.16.9.2 – 254 rozsahy pro koncová zařízení, která nejsou v majetku společnosti a je zde umožněn pouze přístup do internetu a nikam jinam, přiřazované pomocí DHCP. VLAN 10 má rozsah 172.16.10.2 – 254 rozsahy pro iLo zařízení v serverech, přiřazované IP adresy ručně. iLo zařízení je speciální karta pro ovládání hardware serverů, tato karta umožňuje vzdáleně provádět úkony, které je jinak nutné dělat přímo na zařízení (například vypnout a zapnout tlačítko power na serveru a podobné činnosti). VLAN 11 má rozsah 172.16.11.2 – 254 rozsahy pro koncová zařízení v učebnách společnosti (využívané při školení zaměstnanců), přiřazované pomocí DHCP.
VLAN 31 má rozsah 172.16.31.2 – 254 rozsahy pro správu aktivních prvků, přiřazované ručně. VLAN 50 má rozsah 172.16.50.2 – 254 rozsahy pro koncová zařízení v oddělené síti řidícího systému rafinerie v Kralupech, přiřazované ručně oddělením MaR (měření a regulace), které má tento systém ve své správě.

Pro propojení areálů jsou využívané virtuální sítě VLAN 60 pro primární spojení pomocí fast ethernetu ve full duplex módu (2*100Mbps), a také VLAN 61 pro záložní spojení o rychlosti 20 Mbps.

V litvínovské části datové sítě jsou virtuální sítě nastavené následovně. VLAN 100 je tedy 172.16.100.2 - 254 určena pro připojení serverů v Litvínově ve správě ICT oddělení, tyto adresy se přidělují ručně. VLAN 101 má rozsah 172.16.101.2 – 254 určen pro ICT oddělení na testovací účely, tyto adresy se přidělují

DHCP serverem. VLAN 102 má rozsah 172.16.102.2 – 254 určen pro Laboratoře a laboratorní přístroje, tyto adresy se přidělují DHCP serverem. VLAN 103,104 a 105 mají rozsah 172.16.103(4,5).2 – 254 určen pro koncové zařízení v administrativních budovách, také přiřazované pomocí DHCP. VLAN 106 a 107 mají rozsah 172.16.106(7).2 – 254 rozsahy pro koncová zařízení ve výrobních budovách, přiřazované pomocí DHCP. VLAN 108 má rozsah 172.16.108.2 – 254 rozsahy pro druhé síťové rozhraní serverů využívané jen pro zálohování dat, adresy jsou přiřazované ručně a mají stejnou koncovou část adresy, jako rozhraní přes které je provozován běžný provoz. VLAN 109 má rozsah 172.16.109.2 – 254 rozsahy pro koncová zařízení která nejsou v majetku společnosti a je zde umožněn pouze přístup do internetu a nikam jinam, přiřazované pomocí DHCP. Tento rozsah je využíván hlavně ve WIFI sítích v zasedacích místnostech společnosti, ve kterých jsou pořádány veřejné besedy na různá témata. VLAN 110 má rozsah 172.16.110.2 – 254 rozsahy pro iLo zařízení v serverech, přiřazované IP adresy ručně. VLAN 111 má rozsah 172.16.111.2 – 254 rozsahy pro koncová zařízení v učebnách společnosti (využívané při školení zaměstnanců), přiřazované pomocí DHCP.
VLAN 131 má rozsah 172.16.31.2 – 254 rozsahy pro správu aktivních prvků v dané lokalitě, přiřazované ručně. VLAN 150 má rozsah 172.16.150.2 – 254 rozsahy pro koncová zařízení v oddělené síti řidícího systému rafinerie Litvínov, přiřazované ručně oddělením MaR (měření a regulace), které má tento systém ve své správě.

4.16. Projekt „Šifrovaná komunikace“

Projekt jedenáct „šifrovaná komunikace systémů v lokální síti“. Aktivní prvky jsou ve společnosti pravidelně obměňovány po dosažení životnosti zařízení, která je výrobci běžně udávaná zhruba na pět let. V okamžiku kdy bylo dosaženo hranice 90% všech aktivních portů ve společnosti s rychlostí 10/100/1000Mb a k tomu příslušně i uživatelských koncových zařízení (počítačů a notebooků), schopných pracovat na nejvyšší rychlosti. Byl zahájen další krok ke zvýšení bezpečnosti komunikace na interní síti. Všechny systémy, které to umožňovaly, byly přepnuté na šifrovanou komunikaci a nešifrovaná komunikace byla zakázána. Systémy jako Lotus Domino, SAP, Documentum, LIMS, Intranet a další, od tohoto projektu komunikují většinou pomocí asynchronního šifrování. Problémem zůstávají některé menší aplikace vytvářené speciálně na zakázku, které šifrovanou komunikaci neumožňují. Na základě požadavku ICT oddělení

jsou některé aplikace postupně upravovány, tak aby splňovaly požadavek na šifrovanou komunikaci. U některých aplikací se toto shledalo, jako neadekvátní požadavek (zbytečně nákladné). Zejména u aplikací, které budou nahrazené jiným již připravovaným řešením na základě dalšího připravovaného projektu. V tuto chvíli lze říci, že přibližně 80% všech systémů již komunikuje po datové síti v šifrovaném režimu. Šifrovaná komunikace přinesla podstatně větší bezpečnost dat při přenosu po datové síti, zároveň se tato změna znatelně neprojevila na subjektivním zpomalení chodu systémů. Což byla velká obava ze strany vedení společnosti a některých členů ICT oddělení.

4.17. Projekt „IPS/IDS“

Projekt dvanáct „IPS/IDS“ V rámci zvyšování bezpečnosti interní sítě byl vytvořen projekt pro zavedení IPS/IDS systému. V obou lokalitách byla instalována dvojice FireWall modulů HP Thread Management Services (TMS) do centrálních prvků od společnosti Hewlet Packard (HP). Tyto moduly jsou v routovaném firewall módu bez podpory IPS v režimu HA Active/standby. Pomocí těchto modulů je také zajišťována bezpečnost dat pomocí šifrovaného spojení IPSec Site-to-Site VPN, toto řešení ja nasazeno na VLAN 60 a VLAN 61, tedy na sítě zajišťující propojení obou areálů a to jak na primárním spojení, tak také na záložním spojení. Dále je bezpečnost v každé lokalitě posílena zařízením Cisco IPS 4240 připojené k centrálnímu prvku v dané lokalitě. Toto zařízení je v monitorovacím módu a spolupracuje s NIM (Network Immunity Manager) systému HP PCM (ProCurve Manager), který je již součástí infrastruktury sítě. Tento systém centrálně spravuje jednotlivé aktivní prvky, které jsou ve společnosti využívány. Modul NIM aktivně vyhledává hrozby v lokální síti a současně přijímá hlášení od HP aktivních prvků prostřednictvím sFlow vzorků a pro hloubkovou analýzu podezřelého provozu využívá sondu IDS, na kterou pomocí metody zrcadlení portů přesměrovává podezřelou komunikaci. NIM ze sondy IDS přijímá hlášení o inspekci a na základě předem definovaných pravidel aplikuje již předem vytvořené bezpečnostní politiky.

4.18. Projekt „E-learning“

Projekt číslo třináct „Zavedení e-learningu“. Bezpečnost ICT infrastruktury z hlediska vnitřního napadení, je ze strany ICT oddělení řešena za pomoci různých

prostředků, které jsou součástí jiných kapitol této diplomové práce. Nezanedbatelnou částí bezpečnosti je i preventivní činnost před možnými hrozbami a to zejména z důvodu neznalosti vlastních zaměstnanců. Jedna část je vytvoření různých norem a směrnic, které jsou volně k dispozici každému zaměstnanci na intranetu společnosti, se kterými se každý zaměstnanec má seznámit. Interním šetřením bylo zjištěno, že takto vytvořených norem a směrnic je velká řada a seznámení se se všemi by zahrnovalo pro každého zaměstnance přibližně jeden týden po nástupu do zaměstnání vytížení na celou pracovní dobu. Samozřejmě, že toto se liší podle pozice, na které je zaměstnanec zařazen. Z tohoto důvodu bylo rozhodnuto o výběru nějakého e-lerningového systému, pro účinější a rychlejší formu seznamování, alespoň s těmi nejzákladnějšímy pravidly. Nakonec byl vybrán systém Edovo od společnosti Trask Solutions a.s. Praha. Tento systém umožňuje vytvářet elektronické kurzy a následně po splnění otázek v testu, vydá osvědčení o absolvování online kurzu (certifikát). V tomto systému jsou kurzy dobrovolné, které může absolvovat každý zaměstnanec společnosti. Mezi tyto dobrovolné kury patří například práce s různými programy, jako jsou součásti MS Office, co a kde najdete na intranetu, práce s elektronickou poštou a podobně. Dále jsou zde kurzy povinné při nástupu do zaměstnání, jako například jak se přihlásit do systému, co je a není dovoleno uchovávat na datové síti společnosti, jak se pracuje se systémy Documentum, SAP, LIMS a další podobné kurzy. V neposlední řadě jsou zde kurzy povinné, které se navíc ještě pravidelně opakují. Do této skupiny patří zejména školení řidičů, první pomoc na pracovišti, rozmístění hasicích přístrojů a jejich použití, informace o novinkách zejména v legislativě a ve využívání ochranných pomůcek a podobně. Kurzy se inovují nebo vytváří nové, dle požadavků jednotlivých oddělení, případně při změnách směrnic nebo legislativy. Kurzy vytváří školicí středisko společnosti, které má za úkol, především u zaměstnanců výroby, kontrolovat a certifikovat jednotlivé zaměstnance, tak aby mohli být uznáni způsobylí pro vykonávání práce na výrobních zařízeních. Tito zaměstnanci, každé dva roky musí své znalosti znovu obhajovat formou školení a testů, v případě neobhájení jsou jim odebrány některé pravomoce a příslušně snížen plat. Znovu mohou žádat o přezkoušení až po půl roce od neúspěšného obhájení svých pravomocí.

4.19. Projekt „čipové karty“

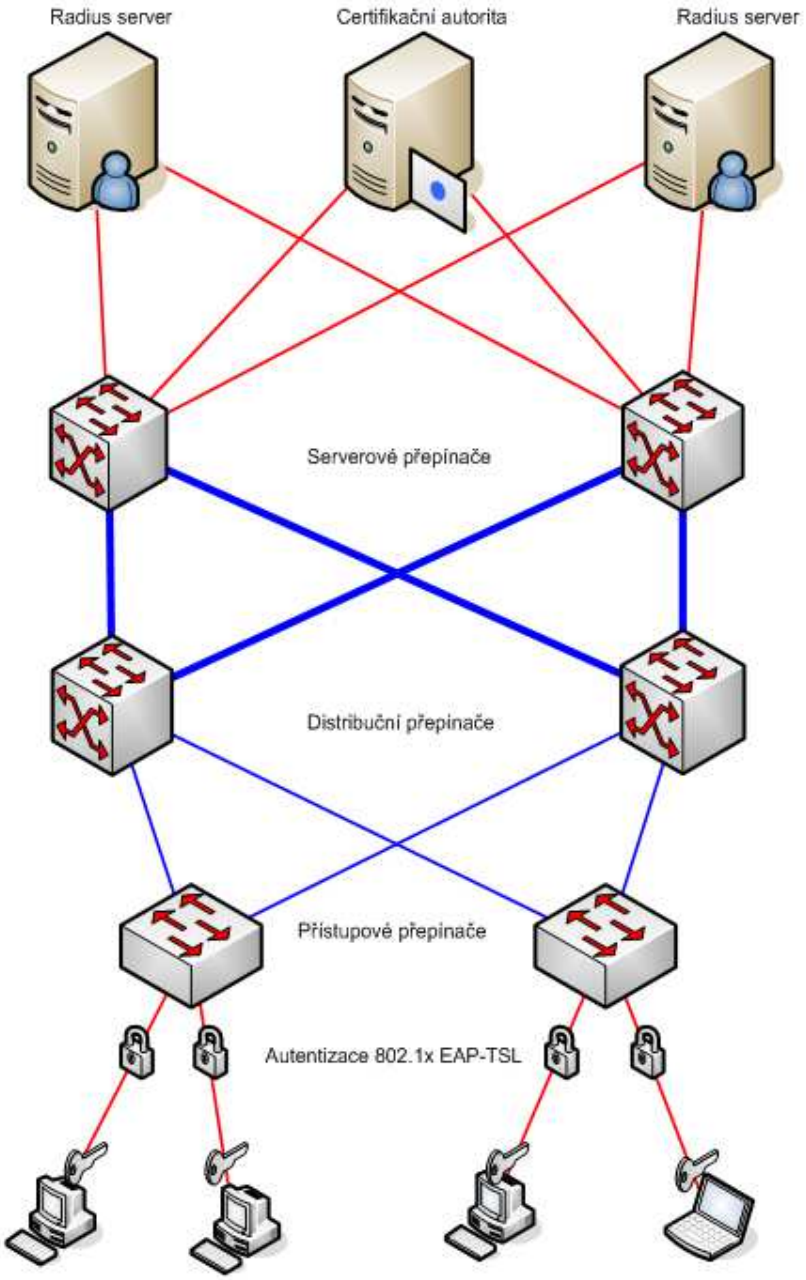
Projekt čtrnáct „Ověřování zaměstnanců pomocí čipových karet“. Ve společnosti jsou nastavená pravidla pro přihlášení uživatelů do systému. Autentizace uživatelů je prováděna na základě přiděleného uživatelského jména a hesla. Kdy tvrdost hesla je nastvena na 8, což představuje heslo o minimálně osmi znacích. Heslo musí obsahovat malé a velké písmeno abecedy, dále musí obsahovat číslo a speciální znak. Toto heslo se následně každých 31dní musí změnit. Systém si pamatuje posledních 15 použitých hesel a nedovolí je znovu použít. I přes tato poměrně striktní opatření, byl tento systém autentizace vyhodnocen jako dostatečný s výhradou a doporučením přejít na nějaký vyšší stupeň zabezpečení přístupu do systému. Bylo doporučeno přejít na ověřování pomocí čipové, případně bezdotykové karty nebo pomocí biometrických zařízení. Biometrická zařízení pro množství a vysoké náklady na dovybavení dalším hardwarem v podobě čteček biometrických údajů. Proto se ICT oddělení rozhodlo jít cestou čipových nebo bezdotykových karet. Tomuto systému i nahrál fakt, že každý zaměstnanec již má nějakou bezdotykovou kartu, kterou využívá pro vstup do některého z areálů společnosti. Docházkové systémy v jednotlivých areálech systém karet využívají a tak by se tyto karty daly využít i pro přihlašování do systémů společnosti. Jak se posléze ukázalo, oba využívané systémy jsou natolik rozdílné a spolu naprosto nekompatibilní navíc ani jeden není ve správě společnosti, která tyto systémy jen využívá, ale ve správě je mají jiné společnosti. Což vedlo ke složitým jednáním všech tří zainteresovaných společností. Naší společnosti šlo o to, aby zaměstnanec měl jednu kartu využívanou jak pro docházkový systém, tak zároveň pro přihlášení do systému. Navíc pokud by to bylo možné, aby měl jeden zaměstnanec jen jednu kartu a mohl se pohybovat v obou areálech. Karty využívané v areálu Litvínov, jsou standardní karty a šlo je bezproblémově využít v běžných čtečkách dodávaných například jako součást klávesnice u stolních počítačů nebo bylo možné využít bežných čteček karet přímo instalovaných v noteboocích zaměstnanců. V areálu Kralupy jsou využívány karty a celý systém docházky od společnosti Honeywell, které mají vyšší stupeň zabezpečení, ale umí komunikovat jen se čtečkami od této společnosti, což by opět znamenalo vysoké náklady na pořízení nutného hardwaru. Začalo se zvažovat řešení s možností použít karty z litvínovské části. Uživatelé v Litvínově by měli jednu kartu jak pro docházku, tak pro přihlášení do systému. Zatímco uživatelé v Kralupech

by měli karty dvě jednu pro vstup do areálu a druhou pro přihlášení do systému. Což bohužel nesplňuje podmínku, aby byl zaměstnanec nucen kartu pro přihlášení do systému nosit u sebe a nedocházelo k situacím, kdy svou kartu zapomene na stole a někdo tuto kartu bude moci zneužít. Proto od tohoto systému (v jedné lokalitě dvě karty pro zaměstnance) bylo upuštěno. Následně jsme vstoupili do jednání s výrobcem karet, zda by bylo možné vytvořit kombinovanou kartu, která by splňovala oba standardy pro bezdotykové systémy docházkových systémů v obou lokalitách a zároveň integrovala čip pro připojení na čipové čtečky v běžných zařízeních, které by se využili pro připojení do systému společnosti. Vlastně by se jednalo o tři různé karty integrované do jedné. Od výrobce jsme dostali potvrzení, že je schopen tyto kombinované karty vyrobit. Proto jsme opět vstoupili do jednání s vlastníky obou docházkových systémů, zda by přistoupili na možnost využívat námi dodaných integrovaných karet pro naše zaměstnance. Případně nahradili své dosud využívané karty všem uživatelům za nové integrované karty. Bohužel společnost Synthos nepřistoupila na žádný z našich návrhů s odůvodněním, že by to narušilo bezpečnost jejich systému. Díky tomuto rozhodnutí došlo ke krachu tothoto projektu a nadále se využívá systém autentizace v podobě jména a hesla.

4.20. Projekt „802.1x“

Projekt patnáct „Využití možností protokolu 802.1x“. Po neúspěšném zavedení projektu číslo čtrnáct (Ověřování zaměstnanců pomocí čipových karet) byl vytvořen projekt na realizaci ověřování připojených koncových zařízení pomocí protokolu 802.1x. Byl posílen Radius server (o další server) dosud využívaný pouze pro ověřování uživatelů připojujících se vzdáleně přes internet pomocí VPN připojení. Byl zprovozněn server certifikační autority (CA) na platformě Microsoft, pomocí kterého jsou generovány všechny neveřejné certifikáty využívané ve společnosti. Lze je zde generovat, případně zneplatňovat a podobně. V tuto chvíli probíhá distribuce certifikátů na všechna koncová zařízení v majetku společnosti. Po této distribuci bude zprovozněna bezpečností architektura AAA (Authentication, Authorization, Accounting). Tato architektura poskytuje rozšířené zabezpečení ICT infrastruktury. Základem jsou služby pro autentizaci uživatele, zároveň poskytuje mechanismy přidělování přístupových práv ke zdrojům a zároveň prostředky k vyhodnocování využívání těchto zdrojů. Certifikáty jsou uloženy

na discích koncových zařízení. Zařízení, která neumožňují uložit certifikát lokálně, jsou ověřovány na základě MAC adresy. Ověřování probíhá pomocí UDP RADIUS (Remote Authentication Dial In User Service) protokolu.



OBR. 12 PROJEKT 802.1X, ZDROJ: WWW.YS.CZ

4.21. Projek „Rizika“

Projekt šestnáct „Vyhodnocování rizik“. Společnost vybízí své zaměstnance k vyhledávání možných rizik. Za každou nahlášenou rizikovou situaci (označovanou jako

skoro nehodu – upozornění na možnou nehodu, ke které dosud nedošlo) je každý zaměstnanec odměněn v podobě nějakých marketingových předmětů, jako jsou trička s logem firmy nebo hrníček na čaj a podobně. Takto zjištěná rizika jsou následně řešena a dochází k takovým úpravám, aby k žádné nehodě po úpravách již nemohlo dojít. Toto se týká i ICT systémů, kde jsou na odhalování rizik zaměstnanci ICT oddělení sami zodpovědní. V pravidelných intervalech dochází k testování funkčních systémů některou externí firmou certifikovanou pro provádění bezpečnostních testů a na základě výsledků, dochází k dalším úpravám všech systémů, případně ke zdůvodnění z jakého důvodu je potenciální riziko ponecháváno v systému (například otevřené porty, případně otevřený SMTP server a podobně). Ze strany certifikované firmy dochází jak k testování systémů přístupných z internetu, tak i k testování ve vnitřní síti, kde mají povoleno spouštět nedestruktivní testy. Toto testování probíhá tajně, bez vědomí zaměstnanců ICT oddělení, aby bylo otestováno jejich chování v kritických situacích a zda nezneužívají svých práv k obcházení bezpečnostních politik a podobně.

4.22. Ostatní využívané bezpečnostní systémy

Ostatní systémy zvyšující bezpečnost dat, datové sítě, komunikace na síti využívané společností již od počátku, ale dosud v práci nezmíněné. Do této kapitoly patří zejména antivirové řešení od společnosti Symantec vytvořené ve třech úrovních umístěné na koncových zařízeních, na serverech a na komunikačních uzlech (hlavně na proxy serveru, firewallu). Symantec řešení je využíváno i pro detekci nežádoucích programů jako jsou různé malware, freeware a trial verze různých z internetu zkoušených prográmků. Dalším velmi významným bezpečnostním prvkem je firewall, který odděluje jednotlivé VLAN sítě a řídí komunikaci mezi těmito virtuálními sítěmi a v neposlední řadě odděluje celou interní síť společnosti do sítě internetu a od sítí třetích stran přímo napojených na tento komunikační uzel. Jedná se zejména o společnou síť holdingu Unipetrol a také o další sítě některých kontraktorů, většinou sídlících ve stejných areálech jako naše společnost.

5. Zhodnocení výsledků a doporučení

Obsahem této kapitoly je zhodnocení poznatků z teoretické části této diplomové práce. Tyto poznatky jsou následně aplikované v podobě popisu dílčích projektů realizovaných nebo připravovaných v konkrétní společnosti, které v konečném důsledku vedou k zajištění bezpečnosti podnikové ICT infrastruktury z hlediska vnitřního napadení.
V dnešním kybernetickém světě je bezpečnost velmi rychle se vyvíjející obor, který je velmi důležitým článkem ochrany společnosti (jejích systémů, dat a know-how). Proto bezpečnostní prvky zaváděné dnes jako novinky v oblasti bezpečnosti, se za pár let mohou ukázat jako zcela nedostatečné. Je tedy velmi důležité stále sledovat novinky a postupný vývoj, které se v tomto oboru neustále objevují a rozšiřují tak možnosti zaváděné bezpečnosti. Samotné řešení tohoto problému, v této diplomové práci, je soubor prezentovaných projektů, které jsou postupnými kroky řešící určité oblasti bezpečnosti ICT infrastruktury zvoleného podniku. Tyto projekty realizované postupně jistě vedly ke zvýšení bezpečnosti oproti uvedenému výchozímu stavu, který je v této práci popsán v dostatečném rozsahu i přesto, že nejsou uváděny všechny detaily samotné konfigurace, což s ohledem na společnost není žádoucí. Společnost prochází nepravidelným auditem a nedestruktivním testům ochrany využívaných systémů a to jak z internetu, tak tajně v prostorách společnosti. Testování je tajné, aby nikdo ze zúčastněných osob (především z ICT oddělení) nemohl nějakým způsobem testování ovlivnit. Výsledky těchto testů a auditů jsou dány k dispozici vedení společnosti a ICT oddělení, které výsledky může okomentovat a na případná zjištění aplikovat procesy pro odstranění možných rizik. Auditorských společností, které jsou schopni na zakázku provést bezpečnostní audity ICT infrastruktury, včetně praktických nedestruktivních testů, je celá řada. Při posledním prováděném auditu ICT bylo využito společnosti Deloitte. Výsledkem posledního auditu byl dokument, jehož výsledkem bylo konstatování, že se jedná o bezpečné řešení ICT infrastruktury s drobnými výhradami.

6. Závěr

Diplomová práce na téma bezpečnost podnikové ICT infrastruktury z hlediska vnitřního napadení, jejíž součástí je uvedení teoretických principů, možností postupů, případně uvedení alternativních řešení některých směrů bezpečnosti ICT infrastruktury. V této práci není možné uvést všechny teoreticky možné varianty řešení bezpečnosti, není reálné uvést ani všechny možné části, které pojem bezpečnost skrývá a je nutné tyto obory bezpečnosti, vzhledem k prostředí společnosti a vzhledem k tématu diplomové práce, vzít v úvahu, alespoň jako podklady při rozhodování o dostupných způsobech řešení. Na základě požadavků poté zvolit nejvhodnější variantu řešení. Řešení se v naší společnosti vybírá ve dvou fázích, nejprve se řeší technická způsobilost navrhovaných řešení, kdy tým odborníků vybere taková řešení, které splňují technické požadavky daného projektu. Takto vybrané návrhy řešení poté ve veřejné aukci soutěží s cenou své nabídky, kde nejlevnější nabídka vyhrává a je následně testována a nasazena do ostrého provozu. Technická část je tedy zcela oddělena od ceny a je jasně deklarována jako podstatně důležitější, přičemž řešení, která nesplňují byť jen z malé části technické požadavky, nemohou postoupit do druhého kola a vyhrát soutěž jen nízkou cenou (která je mnohdy jejich jedinou výhodou).

V praktické části diplomové práce je uvedeno, jaké projekty zajišťující různé směry v oblasti bezpečnosti ICT infrastruktury, které byly zvoleny při řešení této oblasti v konkrétní společnosti Česká rafinérká a.s. Jednotlivé projekty byly realizované, nebo právě probíhá jejich realizace, v několika předešlých letech. Autor této diplomové práce byl zaměstnán ve společnosti od 1.4.1996 a uvádí zde jen zlomek projektů, kterých se zúčastnil buď jako člen týmu definující technickou specifikaci jednotlivých projektů, případně jako realizátor implementace jednotlivých řešení, případně jako vedoucí některých projektů, zajišťující celý průběh od plánování, přes výběr dodavatele až po úspěšné nasazení vybraného řešení.

Autor se snažil deklarovat praktické využití, jednotlivých kroků uvedených v této diplomové práci. Využívaných v reálném provozu konkrétní společnosti. Jistě existuje mnoho alternativních řešení zvoleného problému, které v této práci nejsou uvedené. Autor si zároveň nedovoluje označit vybrané řešení jako optimální řešení. Při řešení problému spojeného s bezpečností velice záleží na finančních možnostech společnosti

(řešení bezpečnosti jsou velmi nákladná záležitost) zavádějící bezpečnostní prvky do své ICT infrastruktury. Také velmi záleží na společnosti, co sama vyhodnotí jako potenciální riziko pro její fungování a co za riziko vůbec nepovažuje, případně dočasně za riziko nepovažuje.

Nevyužité možnosti bezpečnosti ICT systémů v této práci jsou například využití možnosti ověřování pomocí biometrických údajů, jako jsou různé čtečky otisků prstů, případně scan oční duhovky a podobné systémy. Dále zde není například zmíněna možnost využívání nějakých technických zařízení s měnícím se kódem (různé token řešení a podobně).

Obor bezpečnosti v ICT světě je velmi dynamický a velice důležitý. Proto je nutné neustále sledovat vývoj nových technologií v této oblasti a pokud možno pokusit se o jejich co největší a nejaktuálnější využívání ve společnosti. Kriminalita v oboru ICT systémů je stále častější a sofistikovanější, dozajisté není snadné se jí bránit a proto je velmi nebezpečné jakoukoliv část bezpečnosti pocenit nebo dokonce zanedbat.

7. Seznam použitých zdrojů

[1] Česká rafinérská a.s. [online]. 2012. <http://www.crc.cz>

[2] Highteck [online]. 2012. <http://www.highteck.net>

[3] HUNT, Craig. *Konfigurace a správa sítí TCP/IP*. Přeložil Ing. Jiří Veselský. Vydání první. Praha: Computer press, 1997. 456s. ISBN 80-7226-024-3

[4] WERNER, Feibel. *Encyklopedie počítačových sítí*. Přeložil Martin Blažík – Libor Spěvák. Vydání první. Praha: Computer press, 1996. 1230s. ISBN 80-85896-67-2

[5] ŠETKA, Petr. *Mistrovství v Microsoft Windows Server 2003*. Brno: Computer press, 2003. 671 s. ISBN 80-251-0036-7

[6] ŠMRHA, Pavel – RUDOLF, Vladimír. *Internetworking pomocí TCP/IP*. Vydání první. České Budějovice: KOOP, 1995. 134s. ISBN 80-85828-09-X

[7] SCHATT, Stan. *Počítačové sítě LAN od A do Z.* Přeložil Tomáš Rutrle. Vydání první. Praha: GRADA, 1994. 384 s. ISBN 80-85623-76-5

[8] Netconfig [online]. 2012. <http://www.netconfig.org>

[9] Computernet [online]. 2012. <http://www.compunet.cz>

[10] Microsoft Technet: Data Flow in the ISO Model. MICROSOFT [online]. 2012. <http://technet.microsoft.com>

[11] SAMURAJ-cz.com: Forum. [online]. 2012. <http://www.samuraj-cz.com>

[12] OSIF, Michal. *Windows 2000 Server a Advanced Server – Poradce experta*. Vydání první. Praha: GRADA, 2001. 604 s. ISBN 80-247-0078-6

[13] KLANDER, Lars. *Hacker Proof.* Přeložil Ing. Jan Kučera. Vydání první. Brno: UNIS Publishing s.r.o., 1998. 648 s. ISBN 80-86097-15-3

[14] CURRID, Cheryl – SAXON, Stephen. *Novell Netware 4.0 úplný průvodce*. Přeložil Ing. Oldřich Přichystal. Vydání první. Praha: GRADA, 1993. 752 s. ISBN 80-7169-059-7

[15] RUSSEL, Charlie – CRAWFORD, Sharon – GEREND, Jason. *Microsoft Windows Server 2003 – Velký průvodce administrátora*. Přeložil Bohdan Cafourek – Miroslav Hrubý. Vydání první. Praha: CP Books, 2005. 1374 s. ISBN 80-251-0579-2

[16] VRANA, Ivan Ing. CSc. – RICHTA, Karel doc. Ing. CSc. *Zásady a postupy zavádění podnikových informačních systémů.* Vydání první. Praha: GRADA, 2005. 188 s. ISBN 80-247-1103-6

[17] GÁLA, Libor – POUR, Jan – TOMAN, Prokop. *Podniková informatika*. Vydání první. Praha: GRADA, 2006. 484 s. ISBN 80-247-1278-4

[18] TOMAN, Prokop. *Informatika pro koncového uživatele*. Vydání první. Praha: Profession Publishing, 2011. 172 s. ISBN 978-80-7431-057-7

[19] Ochranný svaz autorský pro práva k dílům hudebním, o. s. [online]. 2013. <http://www.osa.cz>

[20] PŘIKRYLOVÁ, Jana – JAHODOVÁ, Hana. *Moderní marketingová komunikace*. Vydání první. Praha: GRADA, 2010. 320 s. ISBN 978-80-247-3622-8

[21] KOTLER, Philip – ARMSTRONG, Gary. *Marketing*. Přeložil Ing. Jiří Michek. Dotisk 2011. Praha: GRADA, 2004. 864 s. ISBN 978-80-247-0513-2

[22] Fayn. [online]. 2013. <http://www.fayn.cz>

[23] SINGH, Simon. *Kniha kódů a šifer*. Přeložil Petr Koubský – Dita Eckhardtová. Vydání první. Praha: Dokořán, 2003. 384 s. ISBN 80-86569-18-7

[24] 4Safety. [online]. 2013. <http://www.4safety.cz>

8. Seznam obrázků

OBR. 1 Podíly akcionářů společnosti ČeR a.s., ZDROJ: WWW.CRC.CZ

Obr. 2 Porovnání modelů ISO/OSI a TCP/IP, ZDROJ: WWW.EARCHIV.CZ

Obr. 3 Různé aktivní prvky, ZDROJ: www.cisco.com

Obr. 4 Znázornění virtuálních sítí, ZDROJ: WWW.LUPA.CZ

Obr. 5 Znázornění ověřování standardem 802.1x, ZDROJ: WWW.COMPUNET.CZ

Obr. 6 Toky dat v komunikačním modelu ISO/OSI, ZDROJ: SITE.BOREC.CZ

Obr. 7 Vrstvy komunikačního modelu ISO/OSI

Obr. 8 Propojení jednotlivých budov a VLAN, areál Kralupy

Obr. 9 Propojení jednotlivých budov a VLAN, areál Litvínov

Obr. 10 Projekt redundance optických tras, areál Kralupy

Obr. 11 Projekt redundance optických tras, areál Litvínov

Obr. 12 Projekt 802.1x, ZDROJ: WWW.YS.CZ