Vysoká škola ekonomická v Praze

Fakulta managementu v Jindřichově Hradci

Diplomová práce

Pavel Dohnal

2007

Vysoká škola ekonomická v Praze

Fakulta managementu

Jindřichův Hradec

Diplomová práce

2007

Vysoká škola ekonomická v Praze

Fakulta managementu v Jindřichově Hradci

Katedra informatiky

Bezpečnost a ochrana dat v počítačových sítích malých organizací

Vypracoval:

Pavel Dohnal

Vedoucí diplomové práce:

Ing. Pavel Pokorný

Kněžice, duben 2007

Prohlášení

Prohlašuji, že diplomovou práci na téma

»**Bezpečnost a ochrana dat v počítačových sítích malých organizací**«

jsem vypracoval samostatně.

Použitou literaturu a podkladové materiály

uvádím v přiloženém seznamu literatury.

Kněžice, duben 2007

podpis studenta

Anotace

Bezpečnost a ochrana dat v počítačových sítích malých organizací

- Obecné technické, programové, organizační a personální otázky bezpečnosti počítačových sítí LAN (informační a bezpečnostní politika firmy, technické možnosti, programová řešení, klady a zápory jednotlivých řešení a přístupů).
- Bezpečnost dat - opět technické, programové, organizační a personální aspekty problému.
- Internet, internetová konektivita a bezpečnost dat (ochrana sítí, firewall -porovnání).
- Návrh konkrétního řešení a uspořádání sítě pro malou organizaci vycházející z výše uvedených teoretických poznatků včetně konfigurace a ekonomického hodnocení zavedení a chodu sítě s implementovanými bezpečnostními prvky.

duben 2007

Poděkování

Za cenné rady, náměty a inspiraci

bych chtěl poděkovat

Ing. Pavlovi Pokornému

z Vysoké školy ekonomické v Praze,

Fakulty managementu v Jindřichově Hradci.

Obsah

Úvod

Motto:

Do pěti let se bezpečnost stane v IT oblasti hlavním a nejdůležitějším bodem. Všechny ostatní, malicherné problémy budou zapomenuty a cílem většiny běžných uživatelů bude „přežít v džungli internetu“.

Petr Kratochvíl, CHIP září 2006 str. 30

V dnešní době si lze jen stěží představit úspěšnou organizaci a to nejen z oblasti veřejného sektoru, ale i ze soukromé sféry, která by se zcela obešla bez použití informačních systémů. Informační technologie umožňují nejen efektivní správu a řízení činností v těchto organizacích, ale i komunikaci vůči jejich okolí. A právě s propojením informačních systémů přichází největší bezpečnostní rizika. Lze si samozřejmě říci, že nejbezpečnější je ponechat informační systém zcela izolován. Toto by bylo ještě možné v rámci organizace, která se nachází v určitém geografického prostoru (např. budovy). Co však v případě, že jednotlivé pobočky jsou vzdáleny desítky, nebo i tisíce kilometrů? Zde by již toto nebylo možné. Nehledě k tomu, že většina systémů by znemožněním získávat a naopak poskytovat informace ostatním uživatelům nejen z vlastní organizace ztrácela významnou část své funkčnosti. Tak jak jsou označována určitá období v lidských dějinách podle nejvýznamnějších technologických změn, v minulosti např. období průmyslové revoluce, dnes hovoříme o věku informačních technologií. Informační technologie vytváří nezbytné předpoklady budoucího rozvoje, bez nich by byla práce s informacemi nejen neefektivní, ale již i nepředstavitelná.

S prudkým rozvojem moderních technologií informačních systémů se však zvyšuje i možnost jejich zneužití. Téměř každý den se setkáváme s případy počítačové kriminality, zneužívání údajů, elektronických krádeží i podvodů. Toto vše nás upozorňuje právě na nutnost jejich dostatečného zabezpečení, neboť případná nedbalost by mohla přinést nedozírné následky.

Zabezpečení počítačových sítí je velice rozsáhlá problematika, která v sobě zahrnuje celou řadu relativně samostatných okruhů. Patří sem např. problematika šifrování dat, topologií sítí,

firewallů a celková bezpečnostní politika organizací. Chtěl bych v této práci uvést základní principy a postupy, které je vhodné použít při zabezpečování lokálních sítí organizací. Rovněž bych rád upozornil na hlavní triky a postupy, jichž používají hackeři pro napadení sítí a počítačů, jelikož tyto postupy je nutné znát pro účinnou obranu před těmito útoky. Hlavním cílem této diplomové práce je nejen navrhnout konkrétní počítačovou síť, ale i vyzdvihnout myšlenku nutného zabezpečení a ochrany dat na příkladu malé organizace, především zabezpečení proti útokům z vnějšího prostředí – Internetu.

V první části této práce se budeme zabývat základními pojmy, které je třeba znát pro pozdější porozumění námi vytvářených konfigurací. Jelikož v dnešní době je většina místních sítí postavena na použití protokolu TCP/IP, zrovna tak jako i naše počítačová síť, proto mu věnuji pozornost v úvodu. Je zde stručně popsán protokol IP a TCP a vysvětleny základní pojmy jako je síťová maska, rozdělení IP adres do tříd, speciální síťové adresy, funkce portů. Z rodiny protokolů TCP/IP jsem vybral k bližšímu seznámení několik nejznámějších, které budeme potřebovat i při našem návrhu počítačové sítě pro obecní úřad v Kněžicích. Jde o protokoly používané pro poštovní provoz SMTP, POP3, IMAP4, přístup na webové servery HTTP a dále protokoly používané v rámci LAN UDP, LDAP, SMB/CIFS a jejich zabezpečené varianty prostřednictvím SSL, nebo IPSec. Za důležité považuji rovněž se alespoň stručně zmínit o typických útocích na počítačové sítě i jednotlivé počítače. Mezi významné možnosti ochrany patří kryptografie, zrovna tak jako bezpečné prokázání identity jednotlivých uživatelů - jejich autentizace. Postup autentizace je popsán na příkladu systému Kerberos. Veškerá technická opatření se však míjejí účinkem, pokud selže nejslabší článek bezpečnosti a tím bývá právě člověk, proto se rozhodně nevyplácí podceňovat organizační a personální otázky, jakož i fyzické zabezpečení systémů. Jelikož zabezpečení počítačových sítí i jednotlivých aplikací je třeba realizovat v rámci celkové bezpečnostní politiky, součástí práce je i příloha č.1 - článek autorů Rudolfa Marka a Jiřího Dastycha zabývající se principy bezpečnostní politiky.

Důležitou okolností ovlivňující bezpečnost, je použitý operační systém. V našem případě je použit pro server zajišťující služby pro chod počítačové sítě systém Microsoft Windows

Server 20003 Standard Edition. Budeme se stručně zabývat uživatelskými účty, přístupovými právy k souborům a adresářům, systémovou bezpečnostní politikou, programovými možnostmi zabezpečení. Konkrétně zde budou popsány možnosti a využití systému EFS, který je součástí Windows Serveru 2000 a 2003. V programovém vybavení žádného počítače v dnešní době snad již nemůže scházet antivirový program

Třetí kapitola se zabývá firewally. Nejprve obecnými principy, druhy, jejich možnostmi a později již konkrétním firewallem, kterým je Kerio WinRoute. Jeho instalací, postupem definice jednotlivých komunikačních pravidel a možnostmi nastavení. Velice stručně je zde rovněž provedeno srovnání několika firewallů, na rozdíl od Keria WinRoute určených k zabezpečení pouze jednoho osobního počítače.

V poslední části přikročíme k vlastnímu návrhu počítačové sítě pro Obecní úřad v Kněžicích. Začneme se stručným seznámením s tímto obecním úřadem a jeho požadavky kladenými na počítačovou síť. Na základě těchto potřeb je navrženo vytvoření počítačové sítě včetně serverů a provozovaných služeb. Významná část této kapitoly je věnována právě nastavení firewallu nainstalovaného na serveru Gate (firewall Kerio WinRoute) a chránícího celou počítačovou síť před útoky z Internetu a to jak nastavením komunikačních pravidel, tak i filtrováním protokolu HTTP. Jelikož druhý server Apl je postaven na linuxové distribuci Fedora Core, jejíž součástí je i firewall iptables, využijeme jej ke zvýšení zabezpečení serveru. Dosud jsme se věnovali otázkám bezpečnosti spíše z pohledu správců informačních systémů, stručně se podíváme na bezpečnost i z pohledu uživatelů. Zmíníme se o nejčastějších příčinách ztráty dat, kterými jsou jednak hardwarové a softwarové poruchy, ale samozřejmě také chybná manipulace uživatele. Další část je věnována velice stručnému seznámení s bezpečnostními nastaveními Internet Exploreru, neboť o některých jeho nastaveních nemají často uživatelé dostatečný přehled. Na závěr práce jsem se snažil o stručné finanční zhodnocení námi navrhované malé počítačové sítě.

1 Obecné otázky bezpečnosti LAN

Pro správné pochopení nejrůznějších v dalším textu probíraných technik je nutné se seznámit se základními principy fungování počítačových sítí a základními pojmy jako jsou např. síťové protokoly, typické útoky na počítačové sítě, možnosti šifrování, bezpečnostní politika atd.

1.1 Obecně o sítích

1.1.1 Lokální počítačové sítě

LAN (Local Area Network) - lokální (místní) počítačová síť je tvořena nejméně dvěma, většinou však více počítači, které jsou spolu propojeny (např. kroucenou dvoulinka, optickým, koaxiálním kabelem, mikrovlnným spojením atd.). Součástí sítě nejsou pouze počítače, ale i další zařízení, které můžeme rozdělit do dvou skupin, a to na aktivní a pasivní zařízení (prvky). Počítače propojené pomocí LAN mohou navzájem sdílet nejen data, ale i různá periferní zařízení jako jsou třeba tiskárny, modemy pro přístup do dalších sítí atd. Připojené počítače bývají nejčastěji ve vlastnictví jedné organizace a nachází se na geograficky omezené ploše, např. v rámci jednoho patra nebo jedné budovy, přičemž jejich počet může dosahovat stovek, či tisíců.

Dle způsobu komunikace mezi počítači, mohou být LAN založeny na modelu:

Client-server - kdy jeden z počítačů (obvykle ten nejvýkonnější) slouží jako server a ostatní v síti zapojené počítače pracují pouze jako stanice.

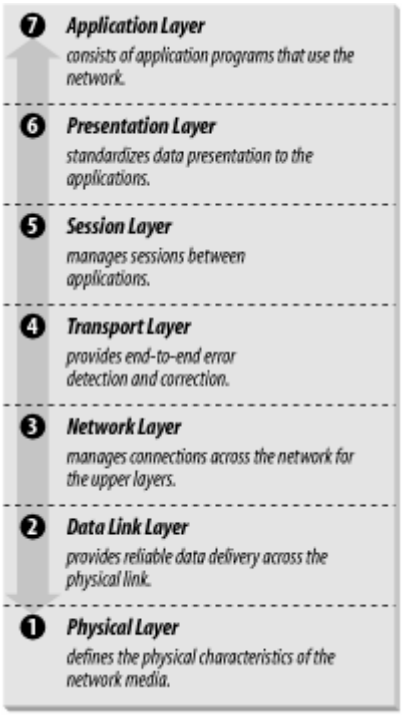
Peer-to-peer - (rovný s rovným), kdy všechny do sítě zapojené počítače jsou si rovny v tom, že každý z nich může pracovat současně jako pracovní stanice i jako server. V tomto případě mohou tedy všechny počítače nabízet své služby (diskety, tiskárny, přístup na Internet) ostatním počítačům zapojeným do sítě. Dnes se s tímto modelem často setkáváme i v rámci Internetu, kde však tyto sítě bývají „trnem v oku“ organizacím zabývajícími se ochranou

autorských práv, neboť právě v těchto sítích jsou často sdíleny soubory chráněné autorskými právy.

1.1.2 Referenční model ISO/OSI

Referenční model ISO/OSI byl vytvořen organizací ISO (International Standards Organization) jako standard pro provoz komunikačních systémů pod názvem Reference Model of Open Systems Interconnection (Referenční model propojování otevřených systémů), proto bývá někdy označován i jako RMOSI. V roce 1984 byl přijat pod označením ISO 7498. Model se skládá ze sedmi vrstev, pro něž stanoví úkoly za jejichž plnění jednotlivé vrstvy zodpovídají. Definování jednotného modelu tedy umožnilo spolupráci produktů různých výrobců [1].

Obr 1.1: Vrstvy referenčního modelu ISO/OSI



Pramen: Craig Hunt, TCP/IP Network Administration , 3rd Edition

Dle [2]:

Aplikační vrstva – realizuje aplikačně orientované služby, podporuje různá aplikační rozhraní pro implementaci elektronické pošty, přenosů souborů apod. Její součástí bývají i přímo

procesy, které tyto aplikační funkce plní - definuje způsob, jakým komunikuje se sítí aplikace (programy např. databázové systémy, textové editory, el. pošta). Programy, které poskytují služby na úrovni této vrstvy, jsou např. FTP (File Transfer Protocol), SMTP (Simple Mail Transport protocol), DNS (Domain Name Server) a celá řada dalších.

Prezentační vrstva – provádí aplikační funkce, které se požadují dostatečně často na to, aby se pro ně vyplatilo najít obecné řešení místo toho, aby každý uživatel hledal jejich řešení sám. Specifikuje způsob, jakým jsou data formátována, prezentována, transformována a kódována. Zabezpečuje např. funkci konverze, použití speciálních grafických či znakových sad a pod.

Relační vrstva – je zodpovědná za synchronizaci a správné řazení paketů v síťovém spojení, za udržení spojení, za zajištění odpovídající bezpečnosti přenášených dat. Umožňuje, aby si uživatelé (procesy) aktivní v různých uzlech mezi sebou zavedli relace (sessions) a koordinovali svoji činnost v zavedených relacích.

Transportní vrstva – zaručuje adresování koncových komunikujících zařízení působících v uzlech sítě a kvalitu přenosu mezi nimi. Z aplikačních dat připravuje transportní segmenty obsahující mimo jiné adresu koncového zařízení v uzlu, které jsou dále službami síťové vrstvy upravovány na pakety (mj. doplňovány o adresy komunikujících uzlů) respektive jsou z těchto paketů zpět sestavovány.

Síťová vrstva - je označována jako paketová. Úkolem je určit jednoznačnou adresu či přeložit hardwarovou adresu na síťovou, nalézt směr (optimální cestu) od zdroje k cíli, zajistit a udržet logické spojení mezi dvěma uzly. Pro směrování toku dat sítí se zavádí nezávislá identifikace komunikujících partnerů v síti, tzv. síťové adresy, které jsou na fyzickém adresování prakticky vždy nezávislé. Data jsou pro účely směrování toku dat dělena na pakety.

Linková (spojová) vrstva - má za úkol zajistit přenos celých bloků dat (velikosti řádově stovek bajtů), označovaných jako rámce (Frames). Datový spoj se volitelně může chovat jako bezchybový – kontroluje rámce, zda byly přeneseny správně (podle různých kontrolních součtů) a potvrzuje přijetí bezchybně přenesených. Jsou-li poškozeny , vyžádá si jejich

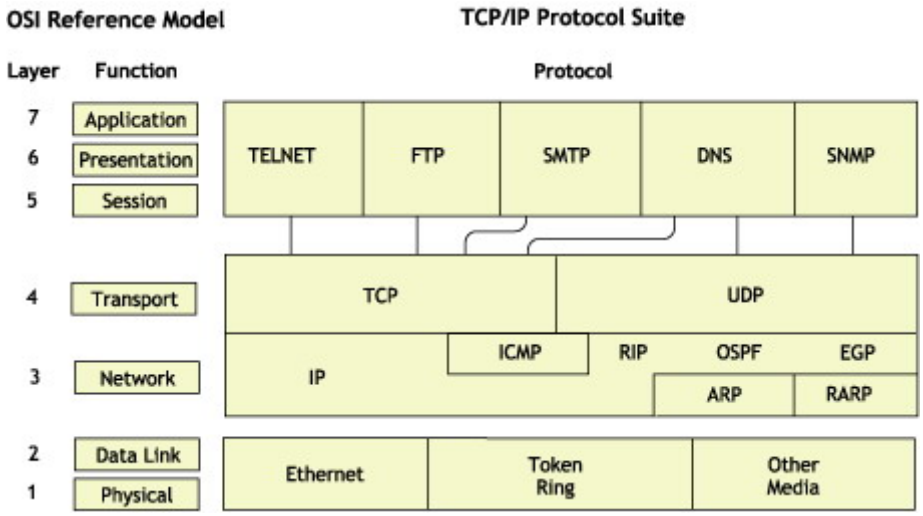
opětovné vyslání. Řeší se zde i problém soupeření při přístupu k sdílenému přenosovému médiu při žádostí vysílat.

Fyzická vrstva - zajišťuje přenos na úrovni jednotlivých bitů bez ohledu na jejich význam. Úkolem je předávat tyto bity mezi jednotlivými stanicemi prostřednictvím fyzické přenosové cesty. Na této úrovni se definuje typ použitého kabelu a konektorů, význam jednotlivých jehel konektorů, formát elektrického signálu (kolik mikrosekund trvá přenos jednoho bitu, zda přenos může běžet oběma směry současně) atd.

1.1.3 Síťové protokoly

Protokoly umožňují vzájemnou identifikaci komunikujících uživatelů, upravují formáty přenášených dat, reakce na detekované chyby přenosu atd., umožňují tedy síťovým zařízením aby se mezi sebou „domluvili“. Existují dvě základní skupiny protokolů a to protokoly založené na modelu ISO/OSI a na modelu TCP/IP. V dnešní době je v sítích LAN nejrozšířenějším protokol TCP/IP, proto mu také věnuji hlavní pozornost. Síťové protokoly ISO/OSI jsou často založeny na proprietálním řešení firem např. protokoly XNS (Xerox Network Systém), Apple Talk, SNA (Sytem Network Architecture) a další.

Obr. 1.2: Přehled umístění protokolů v modelu ISO/OSI

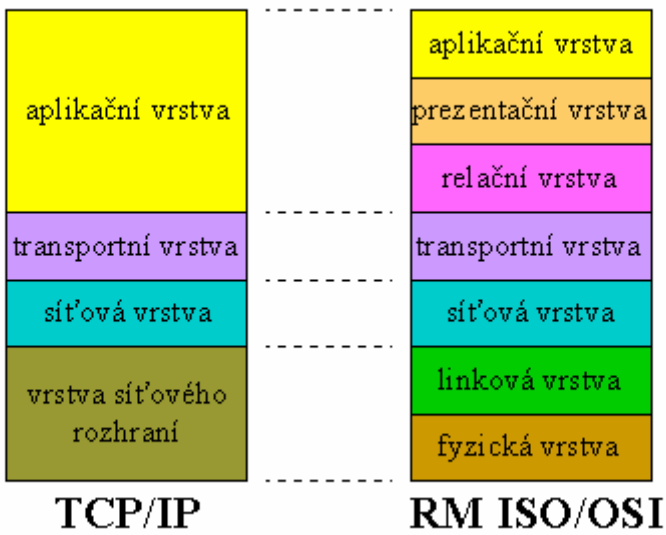


Pramen: Novell TCP/IP Administration Guide for NetWare 6.5, August 2003

1.1.4 Protokoly TCP/IP

V současnosti jsou nejpoužívanějšími protokoly ve většině počítačových sítí právě skupina protokolů TCP/IP. Velmi často je však TCP/IP považován za jeden protokol. Ve skutečnosti je TCP/IP celá sada protokolů, která se skládá z několika vrstev. Jako příklad protokolů jež jsou součástí sady TCP/IP pracujících na různých vrstvách nad protokolem IP lze uvést protokoly TCP, UDP, HTTP, FTP, SMTP, POP3, IMAP4, SMB/CIFS. Protokol TCP/IP byl vyvinut koncem 70-tých let pro testovací síť amerického ministerstva obrany známou jako ARPANET, která se později rozrostla do dnešního Internetu. Oficiálním protokolem používáným v ARPANETu se stal v roce 1983. Na rozdíl od modelu ISO/OSI obsahujícího sedm vrstev, tak jak bylo uvedeno v předchozí části, model TCP/IP zjednodušuje počet vrstev na čtyři. Neznamená to však, že by v tomto modelu některá vrstva chyběla, pouze některé vrstvy v modelu TCP/IP plní funkci více vrstev podle ISO/OSI.

Obr. 1.3: Srovnání vrstev TCP/IP a ISO/OSI



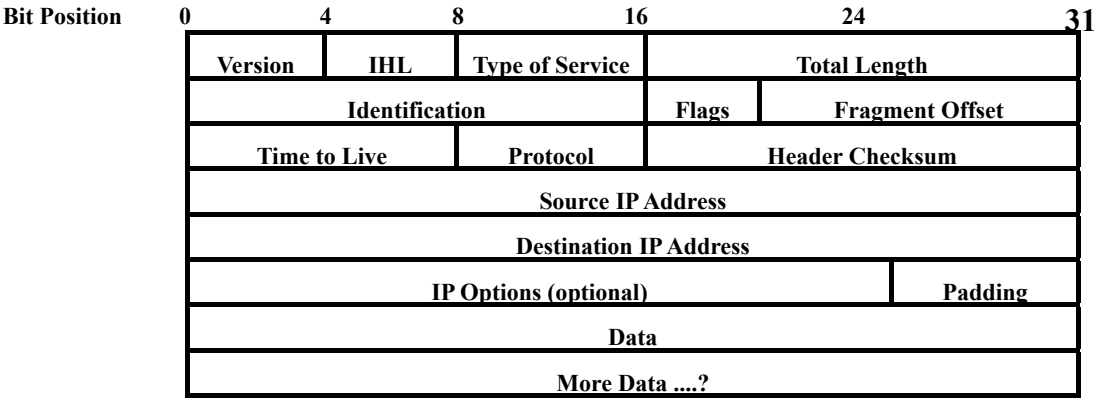
Otázka bezpečnosti nebyla při návrhu protokolu TCP/IP brána v potaz. Protokol byl navrhován tak, aby byl co možná nejvíce efektivní a flexibilní, proto přenosové cesty založené na tomto protokolu nejsou nikterak zabezpečeny. Data nejsou zabezpečena z hlediska přenosu na úrovni síťové vrstvy (mohou se ztrácet), nejsou zabezpečena proti

odposlechu (nejsou šifrována). Tyto problémy je nutné ošetřit na aplikační úrovni, jakož i otázku autentizace uživatele, která je často podceňována např. přenos hesla v nezašifrované podobě. Těmito problémy trpí i běžné protokoly postavené na TCP/IP, proto je velice jednoduché např. poslat e-mail s jiným jménem ze smyšlené adresy. Tyto nedostatky je snaha odstranit použitím vrstvy/protokolu SSL, který zabezpečuje data na úrovni mezi aplikační a transportní vrstvou. Umožňuje tedy zašifrovat přenášená data a ověřit důvěryhodnost serveru, k němuž se připojujeme, pomocí digitálních certifikátů. Další možnost zabezpečení nabízí IPSec. Jde o rozšíření protokolu IP o poskytování šifrovacích služeb. IPSec poskytuje podobné služby jako SSL, ale na síťové vrstvě, takže aplikace vůbec o existenci IPSec nemusí vědět. IPSec můžeme tedy použít na jakýkoliv IP protokol.

1.1.4.1 Internet Protocol: IP

IP protokol představuje nespojovaný a nespolehlivý protokol s částečnou detekcí (ne však korekcí) chyb. IP pakety jsou základem provozu TCP/IP. Strukturu IP paketu ukazuje obrázek 1.2. Pro nás jsou důležité tyto položky:

Obr. 1.4: Struktura paketu IP



Pramen: Casad Joe, Sams Teach Yourself TCP/IP in 24 Hours, Third Edition

- IHL délka hlavičky IP paketu v 32-bitových slovech

- TOTAL LENGTH délka celého paketu v bytech
- IDENTIFICATION, FLAGS, FRAGMENT OFFSET kontrolují fragmentaci a znovu složení IP paketu
- PROTOCOL označuje, který vyšší protokol byl k vytvoření IP paketu použit
- SOURCE a DESTINATION IP ADDESS určují zdrojovou a cílovou adresu IP paketu

Každý počítač nebo jiné síťové zařízení má v IP síti přidělenou jednoznačnou adresu. Adresa patří síťovému připojení a nikoliv počítači, jedno síťové připojení však může mít přiděleno i několik adres (tyto další jsou vytvořeny jako virtuální adresy). Adresa je určena 32-bitovým číslem[1] a nejčastěji je zapsána v tečkové notaci – každý bajt je oddělen tečkou, např. 192.168.0.1. Tato adresa je rozdělena do dvou částí: na identifikátor sítě a identifikátor počítače. Identifikátor sítě určuje adresu sítě, zbytek (identifikátor počítače) adresu počítače v této síti [3].

Tab 1.1: Základní typy adres podle protokolu IP

třída	horní bity	síťová část	ident. počítače	počet adres	obsahuje sítě
A	0	7	24	16777214	1.0.0.0 – 126.0.0.0
B	10	14	16	65534	128.0.0.0 – 191.255.0.0
C	110	21	8	254	192.0.0.0 – 223.255.255.0
D	1110		multicasting		224.0.0.0 – 239.255.255.255
E	1111		pro budoucí využití		240.0.0.0 – 254.255.255.255

Pramen: Volně dle Microsoftu

Již několik let je slyšet názor, že IP adres umožňujících připojení k Internetu (veřejných IP adres) je nedostatek a že budou velice brzy vyčerpány, což se však dosud nestalo. Vždy se našlo řešení, jak tento problém obejít (připojení přes NAT, proxy servery). Proto byl také navržen protokol IPv6 který má tento a některé další nedostatky původního IP protokolu

[1] Zde se zabývám IPv4, existuje i novější IPv6, která je podstatně odlišná

odstranit. Protokol IPv4 je definován v RFC 791, strukturu adres IPv6 je možné nalézt v RFC 4291.

Kromě výše uvedeného rozdělení mají některé síťové adresy speciální význam:

- Adresa 0.0.0.0 se nazývá implicitní směr (default route). Používá se např. u bezdiskových stanic při zavádění operačního systému (bootu), kdy ještě není známa jejich IP adresa, ale už musí pomocí TCP/IP komunikovat.
- Síťová adresa 127.0.0.0 a všechny adresy z této sítě (např. 127.0.0.1) jsou přiděleny speciálnímu rozhraní na počítači nazývajícímu se zpětnovazební rozhraní (loopback interface) a chovajícímu se jako uzavřený obvod.
- Adresa 255.255.255.255 je tzv. hromadná adresa. Pakety s touto adresou jsou určeny všem stanicím na stejném segmentu jako odesílatel.
- Adresa s nulovými bity v části identifikujícími počítač 172.30.169.0/24 vyjadřuje celou síť (segment 172.30.169.1-254), adresa se samými jedničkami v části identifikující počítač vyjadřuje všechny síťové zařízení na této síti 172.30.169.255/24.
- Některé z adres jsou určeny pro sítě, které nejsou dostupné z Internetu. Jsou to tyto adresy: 10.0.0.0–10.255.255.255 (ze sítě A), 172.16.0.0–172.31.255.255 (ze sítě B) a 192.168.0.0–192.168.255.255 (ze sítě C).

1.1.4.2 Transmission Control Protocol: TCP

TCP je spojový a spolehlivý protokol s detekcí i korekcí chyb. Je protokolem transportní vrstvy definovaným v RFC 793. Kromě něj na této vrstvě bývá používán protokol UDP, který je rychlejší, ale nespolehlivý – nemá korekci chyb, toto přenechává aplikaci. Protokol TCP zajišťuje následující funkce:

- Navázání spojení před zahájením přenosu dat a ukončení spojení po skončení přenosu
- Propojení transportní a aplikační vrstvy. Pro identifikaci programů v aplikační vrstvě, kterým náleží data v TCP spojení, používá dvojici tzv. zdrojového a cílového portu.

Číselné kódy portů jsou uvedeny v hlavičce TCP paketu. Porty se rozdělují na vyhrazené, jejichž čísla jsou menší než 1024 a jsou pro jednotlivé služby pevně stanoveny a volné, které slouží pro uživatelské programy.

- Vytváření tzv. proudu dat, kdy data nejsou chápána jako jednotlivé pakety (z pohledu IP protokolu), ale jako spojitý proud dat.
- Kontrolu doručení a správnosti dat za pomoci potvrzení, čísla paketu a kontrolního součtu.
- Řízení toku dat. Příjemce udává, kolik bajtů je schopen ještě přijmout, pak se přenos pozdrží, dokud příjemce neoznámí volnou kapacitu pro příjem.

Protokol TCP vytváří spolehlivý proud dat, který uživatelské aplikace již nemusí dále kontrolovat. Nevýhodou protokolu TCP je vyšší režie na zabezpečení správnosti dat, a tím větší zatížení linek a pomalejší přenos dat [4].

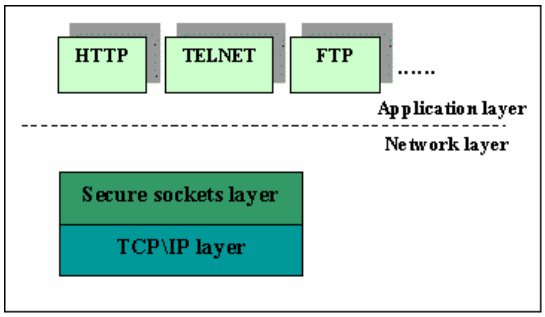
1.1.5 User Datagram Protocol: UDP

Když jsme se zabývali protokolem TCP, nesmíme vynechat druhý nejznámější protokol pracující v transportní vrstvě nad IP a tím je právě UDP. UDP je poměrně jednoduchým rozšířením IP, hodícím se pro aplikace přenášející data po malých nezávislých kvantech. Podobně jako TCP i UDP využívá zdrojový a cílový port. Oproti protokolu IP umožňuje vybavit navíc datagramy kontrolním součtem, takže lze již zjistit případné chyby při přenosu, neumí však stále zajistit potvrzení příjmu paketu. O toto se musí jednotlivé aplikace postarat sami. UDP využívají aplikace, které nevyžadují trvalé spojení komunikujících procesů a pracují s malým objemem přenášených dat (přenos požadavků a odpovědí na ně, apod., je použit např. při komunikaci s DNS serverem). Jeho výhodou je tedy rychlost a jednoduchost, je definován v RFC 768.

1.1.6 Secure Socket Layer: SSL

Stále častěji se dnes setkáváme s použitím SSL. Mnoho běžných uživatelů Internetu si ani neuvědomí, že při navázání zabezpečeného spojení z internetového vyhledávače k webovému serveru využívají právě tento mechanizmus. Zrovna tak i například většina freemailových serverů umožňuje zabezpečit připojení přes SSL. Mezi transportní vrstvu (např. typicky TCP/IP) a aplikační vrstvu (např. HTTP, SMTP, POP3) je vložena ještě další mezivrstva mající za úkol zajistit zašifrování komunikace a autentizaci zúčastněných stran viz. následující obrázek.

Obr. 1.5: Umístění protokolu SSL v modelu TCP/IP



Pramen: Odvárka, Petr: SSL protokol a jeho akcelerace

SSL je protokol dělený na vrstvy, z nichž nejvýznamnější jsou: SSL Record Protocol zodpovědný za zabalení dat protokolů vyšší vrstvy a SSL Handshake Protocol mající na starost vytvoření bezpečné komunikace mezi klientem a serverem.

SSL funguje na principu asymetrického šifrování. Zúčastněné strany mají dva klíče – soukromý a veřejný. Zatímco jak již z názvu vyplývá veřejný klíč je určený ke zveřejnění a tedy i tomu, aby byl ostatním uživatelům dostupný, soukromý je nutno naopak uchovat v tajnosti. Právě tímto klíčem můžeme rozšifrovat data která byla zabezpečena pomocí odpovídajícího veřejného líče.

Navázání SSL spojení citované dle encyklopedie Wikipedia:

„Ustavení SSL spojení (SSL handshake, tedy potřásání rukou) pak probíhá následovně:

- Klient pošle serveru požadavek na SSL spojení, spolu s různými doplňujícími informacemi (verze SSL, nastavení šifrování atd.).
- Server pošle klientovi odpověď na jeho požadavek, která obsahuje stejný typ informací a hlavně certifikát serveru.
- Podle přijatého certifikátu si klient ověří autentičnost serveru. Certifikát také obsahuje veřejný klíč serveru.
- Na základě dosud obdržených informací vygeneruje klient základ šifrovacího klíče, kterým se bude kódovat následná komunikace. Ten zakóduje veřejným klíčem serveru a pošle mu ho.
- Server použije svůj soukromý klíč k rozšifrování základu šifrovacího klíče. Z tohoto základu vygenerují jak server, tak klient hlavní šifrovací klíč.
- Klient a server si navzájem potvrdí, že od teď bude jejich komunikace šifrovaná tímto klíčem. Fáze handshake tímto končí.
- Je ustaveno zabezpečené spojení šifrované vygenerovaným šifrovacím klíčem.
- Aplikace od teď dál komunikují přes šifrované spojení. Například POST požadavek na server se do této doby neodešle.“[5].

Citováno dle Petra Odvárky [6]:

Protokol SSL byl vyvinut společností Netscape Communications. Verze, která byla uvedena pro používání, byla označena jako 2.0. Měla poměrně dost slabých míst a byla snadno napadnutelná. První významná úprava bezpečnostních vlastností byla ve verzi 3.0. Později, jako další oprava SSL protokolu provedená v rámci IETF, vznikl protokol TLS (Transaction Layer Security), který je také někdy označován jako SSL 3.1. SSL 3.0 a TSL jsou velmi podobné a mají několik drobných rozdílů.

1.1.7 Internet Protocol Security: IPSec

IPSec vytváří bezpečnostní systém pracující na síťové vrstvě rozšířením IP hlavičky. Umožňuje šifrovat protokoly pracující na vyšších síťových vrstvách včetně libovolného TCP nebo UDP spojení. Jde tedy o soubor mechanizmů vytvořených k zabezpečení provozu na úrovni IP protokolu a to ať již verze 4, nebo 6. IPSec byl vytvořen pracovní skupinou se stejným názvem v rámci organizace IETF (Internet Engineering Task Force) a první verze byla publikována v RFC v roce 1995.

IPSec je možné použít jak v IPv4, kde máme možnost si zvolit zda jej použijeme či nikoliv, tak v IPv6, v němž je jeho použití povinné. Pro vzájemnou komunikaci dvou účastníků je třeba vytvořit dva jednosměrné spoje, které jsou označovány jako Security Association. (SA). Každý z těchto spojů může být zabezpečený pomocí jednoho ze dvou protokolů - AH (Authentication Header) nebo ESP (Encapsulating Security Payload).

Labouret Ghislaine v článku A technical paper giving an overview of the IPsec standard píše:

„These objectives are met through the use of two security mechanisms, the AH and ESP "protocols", which are added to traditional IP processing:

- Authentication Header (AH) is conceived to ensure integrity and authentication of IP datagrams, without data encryption (i.e. without confidentiality). The principle of AH is to add an additional field to the traditional IP datagram; this field makes it possible for the receiver to check the authenticity of the data included in the datagram.
- Encapsulating Security Payload (ESP) is primarily designed for ensuring confidentiality, but can also provide data authenticity. The principle of ESP is to generate, from a traditional IP datagram, a new datagram in which the data and eventually the original header are encrypted.“ [7].

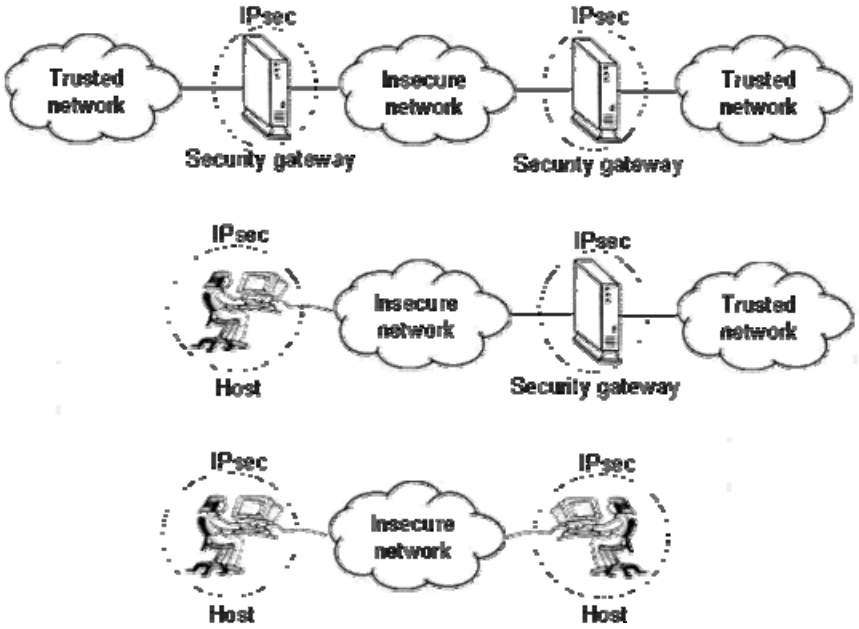
Jak tedy z výše uvedeného vyplývá, hlavním cílem je umožnění vzájemné autentizace a zjištění případné modifikace dat při přenosu (kontrola integrity dat), nebo šifrování dat. Tyto oba mechanizmy však mohou být vzájemně kombinovány.

Každý SA spoj je unikátně identifikován následujícími parametry:

- Cílovou IP adresou paketů
- Identifikátorem použitého protokolu (AH nebo ESP)
- Security Parameter Index (SPI)

IPSec ukládá aktivní SA spojení do databáze nazvané Security Association Database (SAD). Při použití IPSec můžeme rozlišit tři základní způsoby nasazení v závislosti na tom, na jakém zařízení je použit – zda jde o koncové zařízení (host), nebo o bezpečnostní bránu (security gateway). Na následujícím obrázku vidíme v prvním případě situaci, kdy jsou dvě vzdálené privátní sítě propojeny přes nedůvěryhodnou síť – např. Internet. V tomto případě je Virtual Private Network (VPN) vytvořena mezi dvěmi bezpečnostními bránami. Druhý obrázek zachycuje situaci, v níž se mobilní uživatel připojuje přes Internet do privátní důvěryhodné sítě. A v posledním případě vidíme dva uživatele, kteří potřebují spolu zabezpečeně komunikovat přes nedůvěryhodnou síť.

Obr. 1.6: Možnosti nasazení IPSec



Pramen: Labouret Ghislaine: IPSec: a technical overview, December 1998

IPSec umožňuje pracovat ve dvou módech:

- V transportním módu, kdy jsou zašifrována přenášená data, ale vlastní IP hlavička zůstává nezašifrovaná .
- V tunnelovém módu, kdy i původní IP hlavička je zašifrována a nahrazena novou hlavičkou.

Pro správnou funkci IPSec je nutné zajistit vzájemnou výměnu klíčů mezi komunikujícími stranami. Toto lze provést buď ručně, nebo pomocí protokolu IKE (Internet Key Exchange) pro dynamickou správu klíčů. Původní verze IPSec však tento mechanizmus neobsahovala, byl přidán až později spolu s dalšími vylepšeními [7].

1.1.8 Protokoly založené na TCP/IP

Jelikož rodina protokolů založená na TCP/IP je velice rozsáhlá a stále vznikají další, v této části stručně popíšu pouze některé, které jsou důležité pro fungování v naší síti. Jde hlavně o nastínění jejich funkce a používaných portů, což budeme potřebovat v dalších částech této práce (při konfiguraci firewallu). Jelikož jsem se dosud nezmínil o tom, k čemu porty slouží, musím to zde napravit. Aplikace komunikují s okolními zařízeními tj. nejenom se servery, pracovními stanicemi, ale i síťovými tiskárnami a pod. pomocí tzv. portů. Port si můžeme představit jako adresu, na níž naslouchá některá ze služeb. Pokud potřebujeme použít určitou službu, obrátíme se na ni na adrese kde se nachází tj. na příslušný port. Jelikož není možné, aby každá aplikace používala libovolný port podle toho, jak zrovna programátora při jejím psaní napadlo, organizace s názvem IANA (Internet Assigned Numbers Authority) se stará o jejich přidělování. Protože by však bylo nemožné (a i zbytečné), aby byly veškeré porty registrovány, jsou rozděleny do tří skupin. Je logické, že určité porty musí být standardizovány tak, aby pokud se aplikace obrátí na určitý port bylo vždy jisté, jakou službu zde nalezne. Na druhou stranu však potřebujeme i určitý rozsah portů, které mohou být dynamicky přidělovány a umožnit tak použití právě volného portu (používá se pro odchozí spojení). Proto tedy více skupin.

Cituji z [8]:

> Porty se dělí na tzv. standardní (Well Known Ports), ty IANA je přiděluje i registruje a jsou vyčleněné pro procesy operačního systému. Druhou skupinou jsou tzv. registrované (Registered Ports). Tuto skupinu IANA nepřiděluje ale registruje ji. Tyto porty jsou využívány běžnými programy. Třetí, poslední, skupinou jsou tzv. dynamické (Dynamic/Private Ports). Ty jsou určeny pro volné použití, IANA nepřiděluje ani neregistruje jejich použití

Na každém portu může běžet pouze jedna služba. Pokud použijeme jako transportní protokol TCP a protokol UDP se stejným portem, není možná jejich záměna. Např. pokud použijeme TCP s portem 53, není možné aby se dostal na UDP port 53 (tyto porty využívá DNS server). Port se může nacházet v otevřeném stavu, tj. běží na něm služba a naslouchá požadavkům, nebo v zavřeném stavu, pokud není daná služba provozována (samozřejmě může být port otevřen a pomocí nastaveného filtru se může tvářit jako zavřený, nebo naopak může být použit jako návnada – tj. tvářit se jako by na něm daná služba běželo, což však není pravda. Toto však už závisí na nastavení firewallu)

Tab. 1.2: Rozdělení portů

Skupina	Rozsah
Standardní (Well Known Ports)	0 – 1023
Registrované (Registered Ports)	1024 – 49151
Dynamické (Dynamic/Private Ports)	49152 – 65535

Pramen: PeterS, server pcsvet.cz (http://www.pcsvet.cz/art/article.php?id=5242)

Aplikační protokoly, kterými se budeme dále zabývat mají přiděleny standardní porty, na nichž naslouchají příslušné služby. Porty pro jejich zabezpečené verze prostřednictvím SSL však, s výjimkou HTTPs (port 443), nejsou standardizovány, nicméně je zvyklostí použít určité konkrétní porty.

Tab. 1.3: Používané porty

Protocol	Port	Standard dle IANA
http	80	Ano
Http	443	Ano
SMTP	25	Ano
SMTPs	995	Ne
LDAP	389	Ano
LDAPs	636	Ne
POP3	110	Ano
POP3s	465	Ne
IMAP4	143	Ano
IMAP4s	993	Ne

1.1.8.1 HyperText Transfer Protocol: HTTP

HTTP je jedním z protokolů aplikační vrstvy definovaným v RFC 2616 a používaným pro komunikaci mezi WWW servery a jejich klienty (browsery). Uživatel prostřednictvím prohlížeče (browseru) požádá webový server o zaslání konkrétní WWW stránky a ten mu ji odešle. Tento požadavek a následná odpověď je předána protokolem HHTP. Verze 1.0 byla vytvořena jako bezestavová, tzn. že každý požadavek od klienta byl brán jako jediný (neexistuje zde vztah k předchozím požadavkům). Od rozšíření verze HTTP 1.1 zavádí možnost trvalého spojení, které je ukončeno teprve na základě odpojení klienta, nebo ukončení severem, další vyznamné rozšíření se týká virtuálních serverů. WWW služba pro protokol HTTP naslouchá na portu 80.

Protokol HTTP neobsahuje žádné možnosti zabezpečení jako autentizaci uživatele a šifrované spojení. Tyto nedostatky odstraňuje protokol HTTPs. Jde vlastně o protokol HTTP, který pracuje nad vrstvou SSL/TLS. Abychom mohli navázat zabezpečené spojení se serverem, je nutné, aby tento vlastnil certifikát podepsaný certifikační autoritou a tím bylo zaručeno, že se vlastník certifikátu nevydává za někoho jiného. Hlavička 'Host' protokolu http je pak poslána navázaným SSL spojením. O SSL/TLS budou i zmínky dále, neboť tento protokol je možné

(nejen možné ale i velice vhodné) použít nejen pro WEB ale i pro zabezpečení dalších služeb např. pošty, ftp atd. Při použití protokolu HTTPs www služba naslouchá na portu 443.

1.1.8.2 Simple Mail Transfer Protocol: SMTP

Jde o protokol určený ke vzájemné komunikaci mezi poštovními servery definovaný v RFC 821 tj. slouží k předávání poštovních zpráv mezi těmito servery. Komunikace probíhá tak, že klient MUA (Mail User Agent) předá zprávu prvnímu MTA (Mail Transfer Agent) zabezpečujícímu poštovní provoz v doméně odesilatele a ten ji pošle dále na příslušný MTA, spravující poštu v doméně adresáta zprávy (zpráva však může být předávána přes celou řadu MTA – jde o hledání cesty). Ačkoliv označení MUA se může zdát na první pohled složité, jde o program, v němž klient píše zprávu – nejčastěji asi Microsoft Outlook, pine, nebo celá řada dalších programů, výběr je opravdu obrovský. MTA je označení poštovního serveru, i zde lze nalézt velké množství programů např. Sendmail, Microsoft Exchange atd. Odesílající SMTP server vytvoří dvoucestný kanál k přijímajícímu SMTP serveru - je třeba nejen předat zprávu, ale i informovat odesílatele o neúspěšnosti (úspěšnosti) doručení. U protokolu SMTP však narážíme na celou řadu omezení mezi něž patří i nutnost dostupnosti jak příjemce, tak i odesilatele - pokud je poštovní server adresáta zprávy nedostupný, odesílající server to vyhodnotí jako chybu a pokouší se o opakované doručení zprávy. S touto vlastností se setkal téměř jistě každý uživatel - jde o situaci kdy obdržel správu, že poštovní server není dostupný a pokus o doručení bude opakován v následujících dvou dnech a teprve poté bude poštovní zpráva odstraněna. (Této vlastnosti využívá i poštovní server na Fakultě Managementu jako nejjednoduší ochrany proti spamu – server první zprávu odmítne a teprve na druhý pokus ji přijme, neboť servery k rozesílání spamu pokus o doručení neopakují. Lze však narazit i na problémy, pokud některé servery jako je např. Tiskali pokus neopakují). Protokol SMTP se tedy nepoužívá pro přenos poštovních zpráv až k MUA (koncovým klientům), kteří nejsou trvale dostupní. Doručení koncovému adresátovi zajišťují jiné protokoly a to nejčastěji POP3 (Post Office Protocol, verze 3), nebo IMAP (Internet Message Access Protocol). Kromě vlastního doručení zprávy SMTP zajišťuje i další služby jako ověření, zda adresát existuje,

vyplnění zpáteční adresy apod. Zároveň však také umožňuje zjistit informace o správci systému nebo o existenci účtů jednotlivých lidí na daném počítači, což může vést k ohrožení bezpečnosti systému (záleží na nastavení systému a povolených službách). Odesílající klient kontaktuje server na standardním portu 25. Také protokolem SMTP není možné navázat bezpečné spojení, může být lehce odposlechnut. Rovněž neumožňuje ověření odesílatele, neboť údaje o odesílateli zprávy, předmětu, příloze má možnost odesílající vyplnit libovolnými údaji. Příjemce zprávy poté vidí jako odesílatele někoho důvěryhodného, kdo však zprávu neposlal. Toto je samozřejmě možné si ověřit prohlédnutím cesty mailu, přes které poštovní servery zpráva putovala, což však běžného uživatele nemusí napadnout. Obranou je opět zvýšení zabezpečení komunikace použitím SSL. Při použití SSL naslouchá poštovní server na portu 995. Zde pokládám za samozřejmé, že server není tzv. Open-Relay SMTP server akceptující odesílání zpráv z jakékoliv domény do jakékoliv domény, protože takovýto nezabezpečený poštovní server může být využit spamery k rozesílání spamu. V minulosti však s tímto měly problémy i velké freemailové servery, které se tak dostaly na černou listinu (antispammerský seznam). Řešením je pečlivá konfigurace poštovního serveru akceptující odesílání pošty pouze z vlastní domény (rozsahu adres).

1.1.8.3 Lightweight Directory Access Protocol: LDAP

Citováno z [9]:

> Protokol určený pro udržování adresářů a práci s informacemi o uživatelích (např. pro vyhledávání adres konkrétních uživatelů v příslušných adresářích, resp. databázích). Protokol LDAP je založen na doporučení X.500, které bylo vyvinuto ve světě ISO/OSI, ale do praxe se ne zcela prosadilo, zejména pro svou "velikost" a následnou "těžkopádnost". Protokol LDAP již ve svém názvu zdůrazňuje fakt, že je "odlehčenou" (lightweight) verzí, odvozenou od X.500.

Protokol LDAP je protokol založený na modelu klient/server. Klient se připojí k serveru a pošle mu svůj požadavek. Server přijme požadavek, zpracuje jej a výsledek vrátí klientovi. LDAP jako služba je vlastně aplikace pro ukládání dat, jejich organizaci a přístup k nim. Jedná se o databázi určenou především pro aplikace, které zacházejí s daty, k nimž je velmi často přistupováno, ale nejsou příliš často měněna. Data jsou uložena uspořádaně do stromové struktury.

Z hlediska bezpečnosti je v rámci protokolu použit mechanizmus autentizace (lze použít základní, nebo poměrně komplexní SASL spočívající v použití autentizačního mechanismu např. Kerberos jímž se budeme zabývat v pozdější části, popř. u veřejných složek žádnou), autorizace - řízení přístupových práv k jednotlivým objektům, vlastní komunikace je zabezpečena pomocí SSL. Protokol LDAP přistupuje standardně k portu 389, pokud je zabezpečen pomocí SSL používá port 636 [10].

1.1.8.4 Post Office Protocol version 3: POP3

Jde o protokol pracující na aplikační vrstvě TCP/IP spojení, který se používá pro stahování emailových zpráv ze vzdáleného serveru na klienta. POP3 protokol byl standardizován v roce 1996 jako následník protokolů POP1 a POP2 v RFC 1939. Je vhodný zejména pro uživatele mající omezené připojení k Internetu (jako je např. vytáčené připojení), neboť umožňuje stažení poštovních zpráv ze vzdáleného poštovního serveru na místní disk. V offline režimu (odpojen od Internetu) může uživatel si již číst zprávy libovolně dlouho. Jeho hlavní nevýhodou však je skutečnost, že uživatel nemá možnost si vybrat zprávy, které chce stáhnout do svého počítače, tedy i ty které nehodlá číst jako např. spam. Toto omezení však vyplývá z implementace protokolu do poštovních klientů, většina jich však umožňuje ponechat kopie zpráv na serveru. Pokud použijeme příkazy pro komunikaci s POP3 serverem z příkazové

řádky, můžeme si např. vypsat informace o jednotlivých zprávách (LIST [n][2]), nebo stáhnout pouze určitou zprávu (RETR n[3]).

POP3 ve svých počátcích podporoval pouze nešifrované přihlašovací mechanismy. Dnes již máme na výběr od asi bohužel stále nejrozšířenějšího nezabezpečeného přenosu hesel (heslo je po zachycení na síti čitelné) po metodu APOP, kdy heslo je již zašifrováno, takže i při odposlechnutí komunikace není možné jej jednoduše na první pohled odhalit. Standardní port používaný protokolem POP3 je 110, je možné ho opět použít v kombinaci s SSL, potom používá port 465. POP3s při použití ve Windows Server 2003 se službou certifikačního úřadu vyžaduje vystavení certifikátu virtuálního POP3 serveru. Po této standardní instalaci mají uživatelé na výběr, zda použijí šifrované spojení, nebo nikoliv. Pokud použijí pro konfiguraci poštovního klienta průvodce, pak tento jim defaultně nabídne nešifrovanou komunikaci, proto je velice pravděpodobné že nevyužijí možnosti POP3s. Server je však možné nakonfigurovat tak, aby vyžadoval zabezpečené připojení a dokonce i nastavit, že se serverem mohou komunikovat pouze klienti podporující 128-bitové šifrování. Server POP3 má po vystavení a instalaci certifikátu k dispozici dvojici klíčů (veřejný a soukromý klíč). Ty bude používat pro bezpečnou výměnu šifrovacího klíče s každým připojeným klientem. Certifikátem se bude zároveň klientům prokazovat při navazování spojení a pro klienty by měl být důvěryhodný (obdobně jako u všech ostatních protokolů zabezpečených pomocí SSL). Certifikát POP3 serveru je možné použít i pro server SMTP za předpokladu stejných názvů POP3 a SMTP serveru, jinak musí mít vystaven jiný vlastní certifikát.

1.1.8.5 Internet Mail Access Protocol version 4: IMAP4

Také IMAP4 stejně jako POP3 slouží k manipulaci s poštovními zprávami uloženými na poštovním serveru, ale pracuje s nimi odlišným způsobem. Zatímco POP3 stahuje (a podle nastavení i maže) zprávy z poštovního serveru a ukládá je na místní počítač, IMAP4 se

---

[2] LIST [n], kde n je volitelný argument

[3] RETR n, kde n je povinný argument

zprávami pracuje na serveru. Na serveru zprávy také zůstávají dokud nejsou klientem označeny ke smazání. Jednoduše řečeno, IMAP4 pracuje se vzdálenými poštovními složkami stejným způsobem, jako by byly umístěny přímo na místním disku. Na poštovním serveru používajícím IMAP můžeme mít tedy nejen nově došlou poštu, ale i složky se staršími dopisy a kopie odeslaných dopisů (POP3 samozřejmě také umožňuje ponechat kopie přečtený zpráv na serveru). Jelikož se složky běžně ponechávají na serveru, jsou přístupné po síti z jakéhokoliv počítače, což je hlavní výhodou protokolu IMAP4. Pro zobrazení obsahu složky stačí načíst ze serveru pouze údaje z hlaviček. Ze serveru můžeme přenášet na místní počítač buď celé zprávy (a přečíst si je až po odpojení od serveru), nebo naopak pouze hlavičky zpráv (a nepotřebné zprávy smazat bez stahování). Pokud používáme více počítačů, může každý z nich obsahovat kopii nejen našich poštovních zpráv, ale i celých složek. Složky si můžeme buď jednorázově zkopírovat, nebo výhodnější je nastavit si automatickou synchronizaci složky na serveru s místní. Bezpečnostní mechanizmus použitý u protokolu IMAP4 je stejný jako u protokolu POP3 tj. vždy je vyžadováno ověření uživatele. To je možné od prostého přenosu hesla v textové formě (nešifrovaného), přes APOP až po použití SSL. Nejvhodnější je samozřejmě použít IMAP4 v kombinaci s SSL a komunikovat tak se serverem šifrovaně. IMAP server naslouchá na portu 143, při použití SSL je to port 993. IMAP verze 4 je definován v dokumentu RFC 3501.

1.1.9 Protocol SMB/CIFS

Protokol SMB (Server Message Block) je používán v sítích fy. Microsoft pro sdílení souborů, disků, tiskáren a dalších zařízení po síti. Setkat se s ním však můžeme nejen v těchto sítích s operačními systémy Windows, ale i unixových systémech díky jeho otevřené implementaci vyvíjené v rámci Open source software známé jako Samba. Vznik protokolu je spojen s firmou IBM, která dala protokolu základ v tzv. IBM PC Network SMB Core Protocol [11], další vývoj zajistily firmy Microsoft a INTEL. Tento protokol byl použit již v operačním systému MS-DOS (využíval jej i známý příkaz *net use*) a od té doby jej můžeme nalézt ve všech systémech Windows. Označení SMB je používáno u starších verzí protokolu, novější

(od Windows NT4.0) jsou označeny jako CIFS. „SMB is a client server, request-response protocol.“ [11].

„The Common Internet File System (CIFS), also known as Server Message Block (SMB), is a network protocol whose most common use is sharing files on a Local Area Network (LAN). The protocol allows a client to manipulate files just as if they were on the local computer. Operations such as read, write, create, delete, and rename are all supported – the only difference being that the files are not on the local computer and are actually on a remote server.“ [12].

Použití rozhraní NetBIOS nad protokolem TCP/IP je upraveno v RFC 1001 a RFC 1002. V ISO/OSI modelu je protokol umístěn na aplikační a presenční vrstvě.

Obr. 1.7: Umístění protokolu SMB v modelu ISO/OSI

<table>
<tr><th>OSI</th><th colspan="4"></th><th>TCP/IP</th></tr>
<tr><td>Application</td><td colspan="4" rowspan="2">SMB</td><td rowspan="3">Application</td></tr>
<tr><td>Presentation</td></tr>
<tr><td>Session</td><td>NetBIOS</td><td rowspan="3">NetBEUI</td><td>NetBIOS</td><td>NetBIOS</td></tr>
<tr><td>Transport</td><td rowspan="2">IPX[1]</td><td rowspan="2">DECnet</td><td>TCP&UDP</td><td>TCP/UDP</td></tr>
<tr><td>Network</td><td>IP</td><td>IP</td></tr>
<tr><td rowspan="2">Link</td><td rowspan="2">802.2,
802.3,802.5</td><td>802.2</td><td rowspan="2">Ethernet V2</td><td rowspan="2">Ethernet V2</td><td rowspan="2">Ethernet or
others</td></tr>
<tr><td>802.3,802.5</td></tr>
<tr><td>Physical</td><td colspan="5"></td></tr>
</table>

Pramen: Sharpe Richard, Just what is SMB?, October 2002, Samba Webpages

Z obrázku je patrné umístění protokolu SMB, nicméně odpovídá starším verzím protokolu používajícím rozhraní NetBIOS[4], které dnes pro CIFS již není nutné viz.

[4] NetBIOS bývá často označován jako protokol, ve skutečnosti však jde o softwarový interface (API) pro přístup k síťové komunikaci na úrovni relační vrstvy.

„In Windows NT it ran on top of NBT (NetBIOS over TCP/IP), which used the famous ports 137, 138 (UDP) and 139 (TCP). In Windows 2000, Microsoft added the possibility to run SMB directly over TCP/IP, without the extra layer of NBT. For this they use TCP port 445.“ [13].

Při použití NetBIOS je port 137 používán pro jmennou službu (NetBIOS názvy počítačů) zajišťovanou WINS serverem (od Windows 2000 již není třeba, jeho úlohu přebírá DNS server, pokud jej tedy někde nalezneme je to z důvodu zpětné kompaktibility se staršími verzemi Windows - v síti jsou použity i starší operační systémy jako WfW3.11, Win95, Win98, WinMe). Port 138 je použit pro komunikaci se síťovým okolím, pokud jej zakážeme, služba procházení síťového okolí nebude funkční, neboť používá tento port k vytvoření seznamu připojených počítačů. Port 139 je použit pro vlastní přenos dat, tedy přenos souborů z disků, ale i přenos úloh do sdílených tiskáren. Pokud zakážeme tento port, nebude také fungovat příkaz *net send* pro posílání zpráv (pokud je také zablokován port 135, jinak se použije). Od verze Windows 2000 je možné použít port 445.

SMB model definuje dvě úrovně bezpečnosti [11]:

- Na úrovni sdílení - zabezpečení je aplikováno na úrovni sdílení. Pro každé sdílení je nastaveno heslo a pouze uživatel, který zná heslo se dostane na tyto soubory. Tento model byl použit ve Windows for Workgroups, Windows 95, 98 a Me.
- Na úrovni uživatele - každý soubor má nastaveny uživatelská přístupová práva. Uživatel se tedy nejprve musí přihlásit k serveru, který ověří jeho totožnost a přístup ke sdíleným souborům je poté povolen podle jeho přístupových práv.

1.2 Typické útoky na počítače a počítačovou síť

Každý počítač, který je připojen do sítě, může být z této sítě napaden. V této části popíši možné druhy útoků a způsoby získávání důležitých informací, které jsou k útokům potřebné.

V poměrně nedávné době patřil mezi hlavní důvody napadení počítačů jejich výpočetní výkon, paměť a disková kapacita, které tak útočník získal pro vlastní využití. I když by se dnes mohlo zdát že tyto důvody již odpadly, není tomu tak zcela. Vzpomeňme si na velké množství počítačů, na které hackeři pronikli nikoliv proto, aby získali data na nich uložená, ale z důvodu jejich ovládnutí. Takto vytvářené sítě poté zneužívají k rozesílání spamové pošty, nebo DoS útokům - výkon ovládaných počítačů využijí k následným útokům. Dalším častým důvodem je snaha „ukradnout“ cizí identifikaci a získat tak přístup k systémům či informacím, k nimž by normálně neměl přístup. K asi nejčastějším typickým útokům v počítačových sítích patří: Odposlech sítě, odposlech hesel, chybná autentizace, využitích chyb v programech, útoky způsobující nedostupnost služeb, ovlivnění trasy IP paketů a využití sociálního inženýrství a malware.

1.2.1 Odposlech sítě

Pokud získá útočník fyzický přístup k datové kabeláži, aby mohl připojit vlastní počítač (nebo notebook), popřípadě přímo přístup k nezabezpečenému počítači, může pomocí softwaru sledovat všechny pakety, které kabely procházejí. Existuje celá řada programů, které toto umožňují, mezi nejznámnější patří Packet Sniffer, IP Sniffer, Ethereal. Tyto programy však nemusí být určeny pouze k útokům, administrátoři je mohou využít pro analýzu síťového provozu při odhalování závad. Jelikož většina provozu TCP/IP není často šifrována, je velice jednoduché odposlouchávat hesla (POP3, SMTP, HTTP), nebo přenos souborů.

1.2.2 Odposlech hesel

Hesla jsou základním způsobem autentizace. Ochrana a utajování hesel by proto mělo být samozřejmostí. Pokud se útočníkovi podaří zjistit heslo, otevře si tak cestu k získání dat. Zjišťovat hesla je možné následujícími způsoby:

- „Odkoukání“ hesla, např. pokud si ho oprávněná osoba píše na klávesnici, nebo pokud si ho poznamenala někam na papír. Při tomto útoku se však útočník nemusí fyzicky

nacházet přímo na místě útoku, může použít např. kameru. Dnes je již běžnou věcí, že si uživatelé pořídí k počítači tzv. „internetovou kameru“, aby při komunikaci se navzájem viděli. Pokud je tato kamera vhodně nasměrovaná (je vidět na klávesnici) a nedostatečně zabezpečená před přístupem z Internetu, může být zneužita útočníkem. Často můžeme narazit na hesla zapsaná v kalendáři, na lístečku přilepením na monitor, nebo na klávesnici. Ochrana před tímto útokem je jednoduchá: hesla si musí každý uživatel pouze pamatovat a při zadávání hesla do počítače jej zadávat tak, aby jej nikdo další nemohl sledovat.

- Útok hrubou silou – útočník se snaží většinou automaticky vygenerovat všechna možná hesla a uhodnout tak správné. I před tímto druhem útoku je ochrana jednoduchá – po několikátém neúspěšném zadání hesla se systém na delší dobu uzamkne. Odemknutí je poté provedeno automaticky po uplynutí určitého času, nebo ještě bezpečnější je nutnost odemknutí správcem systému. Díky tomu je většina těchto útoků časově neproveditelná, neboť jsou odhaleny dříve než mohlo dojít k průniku (např. ze záznamů v logovacích souborech).
- Jelikož však hesla musí být někde fyzicky uloženy, může se útočníkovi podařit jej získat právě z tohoto umístění. Pokud by toto heslo bylo uloženo v nezakódované podobě, útočník by tak mohl s vynaložením minimálního úsilí získat požadovaný přístup (ať již k souborům, různým programům, nebo do systému). Většinou jsou však tyto hesla uložena v zašifrovaném tvaru. Pro jejich rozšifrování může útočník opět použít metodu útoku hrubou silou, kdy se bude pokoušet generovat náhodná hesla, nebo na základě informací o dané osobě bude zkoušet „jednoduchá“ slova. Uživatelé často používají jednoduchá slova, která se snadno pamatují, doplněná o číslovku. Při odhalování takovéhoto hesla může útočník využít některého z programů „slovníkového“ typu, které zkoušejí heslo odhalit použitím slov ze slovníků. Existuje celá řada programů pro získávání hesel např. z *.pdf, *.rar souborů. Obrana je opět jednoduchá – používat dostatečně dlouhá slova, kombinace velkých a malých písmen, čísla a obecně nealfabetické znaky.

- Často bývají k získání hesla použity programy monitorující stisknuté klávesy na klávesnici. Takovýto program se může dostat do počítače různými způsoby, často si jej nainstaluje nevědomky sám uživatel např. prostřednictvím trojského koně. Na Internetu je k dispozici celá řada takovýchto programů, asi mezi nejznámější patří Homekey Logger, který je freeware. Mezi další patří např. Stealth Keylogger, Spytech SpyAgent, SpyMyPC PRO, Ardamax Keylogger atd. Tyto programy však již nejsou freeware, ale umožňují celou řadu dalších funkcí jako je monitoring navštívených www stránek, on-line komunikace (chatu), odesílaných a přijatých e-mailů, spuštěných programů, ukládání snímků obrazovky atd. Tyto programy jsou již vyvíjeny komerčně za účelem zabezpečení počítače (sledování veškeré činnosti), takovéto sledování i když pod heslem bezpečnosti však může být lehce zneužito.
- Ačkoliv si uživatel nastaví heslo splňující nároky na složitost, může být velice snadno odhaleno. Uživatelé mívají často ve zvyku si usnadňovat práci s vypisování hesel tím, že si toto heslo uloží (typickým příkladem je ukládání hesel pro přístup na webové stránky) a věří, že toto heslo jim z „těch hvězdiček“ nikdo nemůže ukrást. Potom ovšem stačí si odskočit do vedlejší kanceláře a umožnit tak útočníkovi na pár minut fyzický přístup k PC. Ten pouze spustí program PassView a heslo si bez problémů přečte. Těchto programů opět existuje na Internetu celá řada jako např. Asterisk Key, GrabWinText atd.

1.2.3 Chybná autentizace

Chybná autentizace je předpokladem pro mnohé útoky. Chybná autentizace znamená, že ověřovací mechanizmus mylně identifikoval uživatele. S pojmem autentizace souvisí i pojem autorizace (často bývají spolu zaměňovány). Autorizace znamená, že na základě identifikace (autentizace) jsou uživateli přiděleny příslušná práva a to může být jak k určitým souborům, prováděným akcím atd. Ověřovat uživatele je možné podle celé řady kritérií. Asi nejjednoduší je identifikace podle počítače z něhož se uživatel přihlásil (ověření podle zdrojové adresy), jde ovšem o tak primitivní identifikaci, že zde těžko můžeme mluvit o nějakém zabezpečení.

V případě nulového požadavku na zabezpečení, pouze pro základní odlišení uživatelů můžeme toto použít v místní síti (nemůžeme potom používat DHCP server). Častější je ověření heslem přenášeným po síti, zde lze hovořit již o vyšší spolehlivosti. Pokud však je heslo přenášeno v nezašifrované textové podobě, hrozí nebezpečí jeho zachycení, jak jsme si řekli již v předchozí části. Proto vhodnějším způsobem je zajistit přenos hesla šifrovaně, nejlépe pokud provádíme autentizaci pomocí asymetrického šifrování, kdy uživatel má svůj soukromý klíč uložen na externím médiu např. chipové kartě.

1.2.4 Chyby v programech

Asi nejčastějším způsobem pronikání do počítačových sítí, nebo počítačů je využití známých i neznámých chyb v programech. Na Internetu existují seznamy obsahující známé chyby u jednotlivých verzí programů. Pokud útočník zjistí jaké jsou na počítači, který hodlá napadnout nainstalovány programy, potom může z těchto seznamů zjistit jejich slabiny a pokud nejsou odstraněny, tak je využít. Z tohoto důvodu je nutné aplikovat záplaty na operační systémy i jednotlivé programy ihned po jejich zveřejnění, nejlépe automaticky a nespoléhat se na určitého člověka, který může selhat.

1.2.5 Nedostupnost služby

Doposud popsané útoky znamenaly v případě své úspěšnosti prolomení do systému. Útoky způsobující nedostupnost služby (denial of service attacks) sice prolomení do systému neznamenají, ale znamenají nefunkčnost jedné nebo více nabízených služeb nebo dokonce celého systému. Příkladem takového útoku může být zaslání požadavku, na který neumí služba reagovat a který způsobí pád běžící služby. Poměrně časté jsou i útoky typu zahlcení. Server s běžící službou je zahlcen požadavky tak, že již není schopen v rozumném časovém intervalu reagovat. I když v tomto případě nedojde k proniknutí do systému, škody způsobené takovýmto útokem mohou být veliké. Pokud útočník způsobí nedostupnost serveru společnosti zabývající se prodejem zboží po Internetu, ekonomická ztráta již není

zanedbatelná. A nemusí jít pouze o organizace zabývající se obchodem, často jde i o softwarové firmy, jejichž prestiž tím značně utrpí (př. Microsoft). V nedávné době se objevily pokusy o vydírání některých společností právě hrozbou DoS útoku.

1.2.6 Ovlivnění trasy IP paketů

Ovlivnit trasu, kterou prochází IP pakety můžeme zásahy do směrování (směrovacích tabulek). Těchto změn může být zneužito k usnadnění průniku pomocí chybné autentizace. Útočník se přitom vydává za počítač připojený do jiného síťového segmentu (který je ovšem útočníkovi fyzicky nedostupný), čemuž napadený počítač uvěří a považuje počítač za důvěryhodný. Útočník tak může změnou směrování získat přístup povolený pro jiný počítač, nebo může vstoupit mezi dva komunikující počítače a tato komunikace poté prochází přes něj. Tento postup se používá zejména k překonání šifrované komunikace, kdy útočník sdílí šifrovací klíč s každým z napadených strojů a vydává se za jejich protějšek. Často bývá využíván u WiFi sítí, kdy určitý počítač se vydává za bránu a teprve poté předává data skutečné bráně. Díky tomu má přístup ke všem datům, které komunikující počítače zasílají. Pokud útočník dokáže změnit směrovací tabulku v routeru, může způsobit nedostupnost určité podsítě z jiné podsítě – špatné směrování vede ke ztrátě paketů. Ztížit provedení tohoto typu útoku lze tím, že router používá pouze statické směrování – tedy pouze napevno ručně zadané hodnoty směrování v routovací tabulce.

Ochrana před nevítanými prostředníky je možná pomocí komunikace kryptované prostřednictvím soukromého a veřejného klíče. Aby nebylo možné, nebo alespoň obtížné odposlechnout veřejný klíč komunikující stanice, měl by být tento klíč distribuován jinak než po Internetu [14].

1.2.7 Sociální inženýrství, malware

Veškeré firewally, organizační politiky, šifrování, prostě bezpečnostní opatření jsou zbytečné v okamžiku, kdy útočník zaútočí na nejslabší článek celého bezpečnostního systému a tím je

právě člověk. Tato nejjednodušší a současně i nejúčinnější metoda útoku se označuje jako sociální inženýrství a právě ona je zodpovědná za velké množství úspěšných průniků do systému. Sociální inženýrství (social engineering) je metoda založená na oklamání uživatele, přesvědčuje jej, aby jednal tak, jak po něm požaduje útočník. Za normálních okolností by uživatel nesdělil heslo žádné cizí osobě, útočník však navodí situaci, ve které uživatel toto heslo útočníkovi prozradí s pocitem, že se zachoval správně. Nemusí se však jednat přímo o prozrazení hesla, stačí i přesvědčit jej o tom, aby např. otevřel soubor v příloze elektronické pošty, vyplnil na webu formulář s citlivými údaji atd. Těchto metod sociálního inženýrství využívají i některé druhy malwaru.

Výraz *malware* se skládá ze dvou anglických slov - „malicious“ (zákeřný) a „software“. Skupina programů která je takto označována však nevznikla na základě technické specifikace, ale jde o skupinu vyjadřující určitý záměr autora. Patří sem různé programy, přičemž jejich chování a projevy jsou velice rozdílné. Avšak i záměry autorů se mohou odlišovat. Původním cílem tohoto software nemuselo být pouze někomu uškodit, často šlo spíše o dokázání si programátorských schopností a snad i ostatní pobavit. Oproti tomu však vznikaly i viry, jejichž cílem bylo poškodit nejen data, ale i hardware počítače. Dnes je nejdůležitějším motivem těchto autorů patrně zisk - snaží se o získání důvěrných informací, čísel bankovních účtů, hesel a celkové ovládnutí počítače a jeho pozdější využití pro odesílání spamu. Malware tak jednoznačně poškozuje uživatele, od pouhého obtěžování až po krádeže finančních prostředků z účtů. Pod souhrnné označení malware se dle encyklopedie Wikipedia zahrnují počítačové viry, trojské koně, backdoor, spyware, adware a někdy i hoaxy.

Počítačový vir je program, který se šíří bez vědomí uživatele tím, že svůj kód připojí k jiným programům. Právě jeho šíření je základní vlastností virů. Zatímco dříve se viry nejčastěji šířily pomocí disket, dnes se s takovýmto virem můžeme setkat pouze výjimečně. Dnes jich většina využívá připojení k Internetu, šíří se prostřednictvím elektronické pošty a dalších komunikačních programů jako je např. ICQ.

Trojský kůň je jednoduchý program většinou předstírající nějakou užitečnou činnost. Po svém spuštění může skutečně vykonávat činnost která je od něj očekávána, na pozadí však provádí

akce pro něž byl vytvořen, což může být destrukční činnost, např. smazat soubory na pevném disku apod., nebo nainstalovat jiný program např. spyware. Trojský kůň sám o sobě nemá schopnost se automaticky šířit a proto jej nelze řadit k počítačovým virům.

Backdoor je program, který jak již z jeho názvu vyplývá, vytvoří v systému "zadní vrátka" umožňující útočníkovy proniknout do počítače. Mimo útočníků, kteří backdoor vytvořili však těchto zadních vrátek často dokáží zneužít i jiné programy, které scanováním portů zjistí bezpečnostní mezeru a pomocí ní proniknou do počítače.

Spyware je špionážní program, který shromažďuje informace o uživatelích. Můžou to být např. údaje o navštěvovaných webových serverech, nainstalovaných aplikacích na počítači apod. Často jsou používány také tzv. keyloggery monitorující veškeré stisknuté klávesy. Spyware se snaží o získání hesel k účtům, k různým aplikacím. Takto získaná data odesílá na definované adresy.

Adware a spyware jsou pojmy spolu často spojované. Za Adware považujeme reklamní okna (popup-okna, reklamní bannery) upozorňující na komerční stránky. Adware bývá i součástí instalací programů, zejména freewareových a bez souhlasu s jeho instalací není možné nainstalovat daný program. Zde je však součástí licenční smlouvy a můžeme to považovat za formu distribuce. Pokud je uživatel řádně upozorněn na jeho instalaci a souhlasí s ní, nelze proti němu nic namítat. V případě že se instaluje tajně, bez upozornění jednoznačně tím uživatele obtěžuje - minimálně tím že zvyšuje objem přenesených dat a zabírá část výpočetního výkonu počítače.

Hoaxem označujeme poplašné zprávy. Ve skutečnosti se nejedná o žádný škodlivý program, je to pouze e-mail varující před určitým nebezpečím (nejčastěji viry, ale nemusí se týkat pouze výpočetní techniky – viz. v nedávné době varování před nastraženými injekčními jehlami na sedadlech v hromadných dopravních prostředcích). Toto varování může vypadat na první pohled velice věrohodně a tak sami uživatelé se starají o šíření této zprávy a zbytečně zvyšují počet mailových zpráv.

Phishing, česky také označovaný jako „rhybaření“ - metody používané na Internetu ke krádeži identity, hesel, údajů o platební kartě. Vše většinou začíná nevyžádaným e-mailem,

který Vás varuje před některým nebezpečím, popřípadě Vám oznamuje výhru. Odesílatelem jsou důvěryhodné instituce – banky, poskytovatelé připojení apod., žádající Vás o určité potvrzení, vyžadující odeslání citlivých informací (údajů o platební kartě). Někdy bývá v této zprávě uveden odkaz na podvržené webové stránky, na nichž máte provést svoji autorizaci (na první pohled vypadají jako originální). Člověk, který uposlechne a provede požadované se tak stane další obětí phishingu. Nemusí však jít pouze o e-mail, již se objevily i případy telefonního volání VoIP žádající provedení určitých úkonů.

Jedinou možnou a účinnou obranou proti metodám sociálního inženýrství je opatrnost uživatelů a jejich nedůvěřivost. Hesla zásadně nikomu nesdělovat – administrátor systému je nepotřebuje, je schopen heslo změnit. Nedůvěřovat informacím týkajících se citlivých údajů doručených např. e-mailem, vždy si takové informace ověřovat.

Obrana proti malwaru spočívá nejen na uživatelích, ale i především na správcích počítačových sítí. Samozřejmostí je instalace antivirových programů a jejich pravidelná aktualizace, programů odhalujících spyware. Dodržování pravidel bezpečnostní politiky jako je nastavení firewallů blokujících přístup k některým stránkám, zákaz uživatelů instalovat si na počítače vlastní programy, automatické mazání příloh v elektronické poště podle přípony atd.

1.3 Programové možnosti zabezpečení

Mezi důležité prostředky zvyšující bezpečnost celých počítačových sítí, jakož i dat v nich se nacházejících patří kryptografie. Kryptografie je založena na změně dat šifrovacím algoritmem tak, aby data mohly být rozšifrovány do původní podoby pouze osobami (nebo zařízeními), která k tomu mají náležité oprávnění. Pokud tedy již dojde k odcizení zašifrovaných dat, neznamená to automaticky i jejich prozrazení. Důvodem šifrování bývá často nutnost zabezpečit data umístěná na počítači, k němuž mohou získat přístup i jiné osoby (ať už díky útoku z LAN, i z Internetu, popřípadě přímo přístup k fyzickému zařízení počítače), jakož i nutnost ochrany dat při přenosu přes nezabezpečené prostředí. Takovým

prostředím může být např. Internet či jiná veřejná datová síť. V zásadě existují dva základní druhy kryptografických technik. Šifrování s jedním klíčem (symetrické šifrování) a šifrování se dvěma klíči (asymetrické šifrování).

1.3.1 Symetrické šifrování

Při symetrickém šifrování se používá pouze jeden klíč a to jak pro zašifrování zprávy, tak i pro její rozšifrování. Hlavní výhodou symetrických algoritmů je jejich rychlost – proto je můžeme najít v aplikacích pro šifrování v reálném čase (např. vytvářejících zašifrované diskové oddíly apod.). Na jedné straně máme tedy výhodu jejich rychlosti, na druhou stranu však symetrické šifrování přináší i určité omezení. Jedním z těchto omezení je nutnost odesílatele i příjemce se domluvit na jednom klíči, který musí uchránit před prozrazením třetí osobě. Při komunikaci zabezpečené pomocí symetrického šifrování se v praxi používá metoda, při níž se i během komunikace mění šifrovací klíč. Tím se samozřejmě sníží riziko prozrazení všech dat, ale nastává další problém – jakým způsobem předat klíč příjemci. Asi nejznámějším příkladem symetrické šifry je DES (Data Encryption Standard), vyvinutý v 70. letech v USA pro americkou vládu firmou IBM, který se stal národním standardem.

Velkým problémem je také nutnost velkého počtu klíčů. Pokud by každá dvojice na Internetu chtěla uskutečňovat bezpečnou komunikaci, bylo by zapotřebí celkem n(n-1)/2 klíčů, což sebou nese problémy jejich bezpečného uložení a správy (např. pro pouhý 1 000 000 uživatelů by bylo třeba celkem 499.999.500.000 klíčů což je již obrovské číslo).

Mezi symetrické algoritmy, které se v současnosti nejvíce používají patří DES, Blowfish, CAST, IDEA, MARS, RC4, RC5, RC6, Skipjack, Twofish.

1.3.2 Asymetrické šifrování

O asymetrických algoritmech bývá také často hovořeno jako o algoritmech s veřejným klíčem. Jsou založeny na existenci dvou klíčů pro každého uživatele - veřejného a soukromého.

Veřejný klíč není nutné tajit, naopak tento klíč je určen k zveřejnění širokému okolí tak, aby byl komukoliv dostupný. Oproti tomu soukromý klíč klade na své zabezpečení a utajení daleko vyšší nároky. Každý uživatel jej musí pečlivě uschovat a chránit před případným prozrazením. Asi základní metodou zabezpečení je ochrana pomocí hesla, přičemž vlastní klíč může být umístěn na disku počítače, na disketě, popř. v flash paměti, toto však vyhoví pouze nejméně náročným požadavkům. Daleko vyspělejší (a samozřejmě i finančně náročnější) je umístění klíče do chipové karty, při němž soukromý klíč tuto kartu nikdy neopustí – k rozšifrování je vždy nutná příslušná chipová karta.

Asymetrické šifrování je založeno na principu jednocestných funkcí. Pojem jednocestné funkce (One-Way-Function) zavedl R. Needham v sedmdesátých letech. Jde o funkci $f:x \rightarrow y=f(x)$, umožňující snadné vypočítání $y=f(x)$, ale pro všechna y je obtížné vypočítat x. Asymetrická kryptografie využívá tuto asymetrii k vytvoření funkcí, u kterých platí tyto dvě základní pravidla - je snadné provést dopřednou operaci – tedy zašifrování, ale je však velice obtížné tuto operaci invertovat (dešifrovat) bez znalosti potřebných informací.

Kryptografie využívá princip jednocestné funkce s použitím dvou odlišných klíčů, které jsou však ve vzájemné vazbě. Jeden klíč je použit pouze k šifrování, druhý pouze k dešifrování.

Při použití veřejných a soukromých klíčů mohou tedy nastat dvě situace:

- Mnoho odesilatelů k jednomu příjemci (many-to-one) - veřejný klíč je dán k dispozici širokému okolí a soukromý klíč se udržuje v tajnosti. To znamená, že kdokoliv může použít veřejný klíč, aby provedl zašifrování dat, avšak pouze osoba vlastnící soukromý klíč, je může dešifrovat (mnoho lidí může šifrovat a zasílat zprávy jednomu příjemci a pouze tento příjemce je dokáže dešifrovat).

- Jeden odesílatel k mnoha příjemcům (one-to-many) – osoba mající soukromý klíč může zabezpečit data proti změně doplněním kontrolního součtu, samotná data však nejsou šifrována. Všichni ostatní, kteří mají k dispozici veřejný klíč si mohou ověřit, zda bylo opravdu použito daného soukromého klíče a zda nedošlo od té doby ke změně dat. Toto je princip digitálního podepisování (jedna osoba zprávu podepíše, přičemž její podpis si může ověřit velký počet lidí).

Asymetrická kryptografie snižuje počet klíčů potřebných pro zabezpečení komunikace. Každý uživatel disponuje dvěma klíči (soukromým a veřejným), proto je za předpokladu n uživatelů zapotřebí pouze 2n klíčů. Další výhodou je i jednoduší distribuce veřejného klíče, neboť tento není nutné předávat způsobem, který by zabránil jeho zachycení.

Teoreticky je však možné z veřejného klíče vypočítat klíč tajný. Nemusíme nutně najít hodnotu původního originálního klíče, stačí nalézt klíč dávající stejný výsledek šifrování. K výpočtu této hodnoty je však nutné mít k dispozici velký výpočetní výkon, což je v současnosti nerealizovatelné. Vzhledem k tomu, jak se zefektivňuje kryptoanalýza a jak roste výkon počítačů, je třeba na toto nebezpečí pamatovat.

1.3.3 Kombinace symetrické a asymetrické šifry

V předchozí části jsme si řekli o výhodách i nevýhodách obou metod šifrování. Z nich vyplývá, že šifrování zpráv pomocí symetrické šifry je sice rychlé, avšak problém představuje bezpečné předání šifrovacího klíče druhému účastníkovi. Při použití asymetrické šifry sice odpadá problém předání klíčů, je však výpočetně náročné. Proto se asymetrické šifrování nepoužívá při častém šifrování velkého objemu dat.

Řešení tohoto problému spočívá v použití kombinace symetrické a asymetrické šifry. Symetrická šifra, neboť je velmi rychlá, slouží k samotnému šifrování a dešifrování dat a asymetrická šifra se zase použije na bezpečný přenos klíče symetrické šifry. Jelikož tento klíč není velký a jeho přenos se neprovádí příliš často, výpočetní náročnost zde nevadí. Asymetrická šifra tedy vytváří zabezpečený kanál pro přenos symetrického klíče [15].

1.3.4 Zabezpečení přihlášení - autentizační systém Kerberos

Autentizační systém Kerberos je definován v RFC 1510 a byl přijat jako norma konsorcii OSF (Open System Foundation) a UNIX International. Setkat s ním se můžeme v mnoha systémech, nejen od firmy Microsoft, ale i zejména v open-source produktech. Společnost Microsoft jej začala využívat od verze Windows 2000, v dřívějších systémech nebyl k dispozici. Ačkoliv na první pohled vypadá autentizace jako typický příklad použití asymetrického šifrování, Kerberos je založen na symetrické kryptografii. V rámci autentizačního systému jsou běžně používány kryptografické systémy DES, IDEA a RSA.

Autentizační systém Kerberos zabraňuje zbytečnému přenosu hesel přes počítačovou síť, přičemž tato síť je považována za nedůvěryhodnou (nezabezpečenou). V takovéto síti je však nutné, aby existoval jeden server kterému všichni uživatelé důvěřují. A tím je právě server Kerberos, což je vlastně nezávislá třetí strana, vůči které se účastníci komunikace autentizují.

1.3.4.1 Postup autentizace v systému Kerberos

Postup autentizace je zde citován dle Doc. Ing. Jana Staudka, Csc. jak jej uvádí v článku Autentizace a kryptografie v časopise LANcom číslo 12/98. Server Kerberos sdílí s každou síťovou entitou, jejíž identitu potvrzuje, tajný klíč a znalost tohoto klíče je považována za důkaz identity. Kerberos sdílí tajné klíče také s aplikačními servery, jež jím vydávaná potvrzení identity uznávají. Klienti a aplikační servery počátečně nesdílejí žádný klíč.

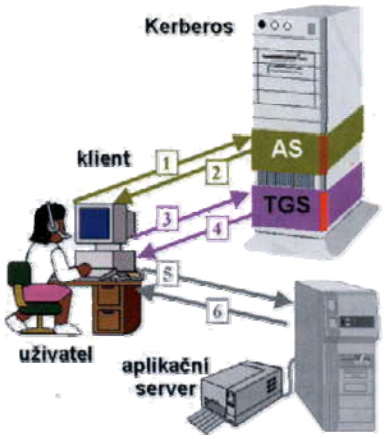
Vnitřně je Kerberos logicky dělen na dvojici serverů:

- AS (Authentization Server) – zajišťuje autentizaci uživatelů spouštějících klientské procesy.
- TGS (Ticket Granting Server) – stará se o udělování důvěryhodných identifikačních průkazů (tiketů) klientům žádajícím o služby aplikační servery.

Primárním cílem systému je, aby v doméně, kterou obsluhuje, byl každý aplikační server schopen ověřit identitu klienta a aby se při tom uživatelovo heslo sítí nepřenášelo. Pokud by

pokaždé, když uživatel požaduje po aplikačním serveru poskytnutí některých služeb, muselo docházet k přenosu hesla, zvyšovalo by se výrazně bezpečnostní riziko a možnost zachycení hesla. Server Kerberos si proto udržuje vlastní databázi, která obsahuje údaje o každém jím spravovaném uživateli.

Obr. 1.8: Průběh autentizace v systému Kerberos



Pramen: Staudek, Jan: Autentizace a kryptografie. LANcom, číslo 12/1998

Uživatel si otevírá relaci na své pracovní stanici udáním svého přihlašovacího jména procesu pro otevření relace. Tento proces vystupuje jako přihlašovací klient, který v kroku (1) předá přihlašovací jméno uživatele autentizačnímu serveru AS, který v databázi Kerbera vyhledá uživatelovo heslo, z tohoto hesla generuje tajný klíč a tímto klíčem zašifruje počáteční pověřovací listiny TGT (Ticket Granting Ticket), které vrátí klientovi.

Jakmile přihlašovací klient počáteční pověřovací listiny TGT přijme (2), vyžádá si od uživatele zadání hesla. Z tohoto hesla generuje stejným postupem jako AS tajný klíč. Pokud tímto klíčem přijaté počáteční pověřovací listiny úspěšně dešifruje, je uživatel oprávněn se přihlásit, neboť udal správné heslo. Může tedy po TGS požadovat vlastní pověřovací listiny pro jednotlivé obsluhované aplikační servery – tikety.

Klient zasílá TGS serveru Kerbera zprávu (3) se žádostí o získání tiketu, který pro aplikační server potvrzuje identitu klienta. Tento tiket bude následně klient používat jako autentizační

průkaz při žádostech o provedení služby aplikačním serverem. Důvěryhodnost tiketu je dána šifrováním pomocí tajného klíče sdíleného Kerberem a aplikačním serverem, který je generován na základě hesla uživatele známého jak lokálně v klientovi, tak i v databázi autentizačního serveru Kerberos (heslo se tudíž po síti nepřenáší).

Kerberos generuje tajný klíč pro symetrickou kryptografii použitou pro komunikaci klienta s aplikačním serverem a definuje jeho dobu platnosti. Klientu tyto informace důvěryhodně vrátí ve zprávě (4) společně s identifikátorem aplikačního serveru, identifikačním tiketem klienta pro aplikační server, který umí dešifrovat jenom tento server a který mu sděluje hodnotu klíče pro symetrickou šifrovanou komunikaci mezi serverem a klientem a dobu jeho platnosti. Poté se již může klient po dobu platnosti tiketu opakovaně obracet na aplikační server s žádostmi o provedení služby, aniž by musel opakovaně žádat o vydání nového tiketu.

V okamžiku, kdy klient zprávou (5) žádá aplikační server o provedení služby, aktualizuje si svůj autentizátor uvedením časového razítka, definujícího okamžik generování žádosti. Aplikační server požadovanou službu provede jen tehdy, pokud se identifikace žadatele v autentizátoru a v tiketu shoduje a když autentizátor je v rámci časové platnosti čerstvý tj. dosud nepoužitý. Aplikační server se klientu autentizuje zprávou (6), kterou prokazuje, že umí zpracovat časové razítko.

Cílem systému Kerberos není rozhodnout o tom, zda je uživatel pro určitou službu autorizován, jeho úkolem je pouze provedení autentizace - identity uživatele. O prověření autorizace se již musí postarat aplikační server sám [16].

1.4 Organizační a personální otázky zabezpečení

Organizační a personální otázky jsou nedílnou součástí bezpečnostní politiky uplatňované v rámci organizace. Musí být přesně a detailně stanovena pravidla pro zaměstnance, kteří jsou oprávněni k výkonu svých pracovních povinností používat informační a komunikační technologie a data informačního systému.

Informačním systémem je obecně myšlen souhrn prostředků výpočetní techniky, informačních a komunikačních technologií, HW, SW, OS, programového vybavení a dat, tvořících jeden celek používaný zaměstnanci firmy, k němuž mají jednotliví uživatelé rozdílný přístup podle definovaných bezpečnostních opatření. Každý uživatel přebírá spolu s účtem a oprávněními do informačního systému i odpovědnost za svoji činnost. V rámci bezpečnostní politiky musí být stanoveny i postihy a sankce za případné porušení těchto povinností. Požadavky na personální zabezpečení závisí na přístupu k bezpečnostní politice. Můžeme rozlišit základní typy:

- Promiskuitní, tedy nejméně omezující. Je postavena na odpovědnosti a uvědomění jednotlivých uživatelů. Spoléhá se na to, že uživatelé budou vykonávat pouze takové činnosti, které jsou jim povoleny. Jejich oprávnění však nejsou technickými prostředky omezeny.
- Liberální dávající uživatelům volnost ve vybraných oblastech mimo výslovně zakázaných činností. Při dodržování těchto zákazů se však již nespoléhá pouze na uvědomění uživatelů, ale vynucuje si je technickými omezeními. Je bezpečnější než promiskuitní politika, ale náročnější na provozní náklady.
- Opatrná zakazuje dělat vše, co není výslovně povoleno. Tato politika již volí opačný přístup k uživatelům. Vychází z toho, že vše je zakázáno a jednotlivým uživatelům na základě jejich pracovních činností a postavení přiděluje oprávnění.
- Paranoidní zakazující dělat vše, tedy i to, co by mohlo být povoleno. Je nejbezpečnější, v konečném důsledku však může vést k izolaci systému, snížení výkonnosti uživatelů, kteří jsou příliš omezováni [17].

V rámci každé organizace je uplatňována určitá bezpečnostní politika jako výsledek rozhodovacích procesů vrcholových manažerů, jejíž součástí je například i stanovení předpisů bezpečnosti práce, požární ochrany atd. Z tohoto vyplývá, že bezpečnostní politika informačního systému není pouze výsledkem rozhodnutí osoby zodpovědné za správu

informačního systému. Vždy se jedná o opatření uskutečňovaná v rámci komplexní bezpečnostní politiky – jednotlivá opatření přijatá v nejrůznějších oblastech podobně jako dílky skládačky dávají dohromady v konečném důsledku právě celkovou bezpečnostní politiku. Pokud tedy posuzujeme jednotlivé části, vždy je musíme vidět v rámci celku. Tímto mám na mysli pouze to, že není možné mít sice dokonale zabezpečený informační systém, v němž jsou elektronická data chráněna před zneužitím a současně v papírové formě tyto data jsou komukoliv volně dostupná. Z tohoto příkladu je vidět, že takováto bezpečnostní politika není dobře nastavená a že vykazuje určitou mezeru.

1.4.1 Havarijní plán

Bezpečnostními opatřeními se snaží organizace zabránit selháním a nežádoucím stavům. Navzdory všem opatřením však může k takovémuto selhání dojít a proto musí bezpečnostní politika obsahovat i plán, jakým způsobem v těchto případech postupovat. Tento plán bývá označován jako havarijní plán. Havarijní plán, jelikož je součástí celkové bezpečnostní politiky musí být opět schválen vedením organizace, upravuje různé postupy, jakož i pravomoci konkrétních osob. Součástí můžou být taková opatření jako je možnost nařídit práci přesčas, ve svátky, jakož i odvolat zaměstnance z dovolené. Tento plán by měl v podstatě upravit cíle a jednotlivé postupy vedoucí k nápravě, jakož i odpovědnost osob za jejich dosažení. Za významnou část bezpečnosti je třeba považovat i ochranu hesel a bezpečnostních kódů. Tyto hesla sice zná pouze oprávněná osoba, která k nim má přístup při výkonu své funkce, takže nehrozí jejich zneužití. Co však v případě, že se s touto osobou něco stane? Pokud by došlo ke ztrátě administrátorských hesel do systémů, které nelze jinak změnit (např. vlastník systému, účet root může změnit jiná systémová hesla) byl by to velice vážný problém. V praxi se toto řeší uložením nejdůležitějších hesel do zapečetěné obálky a jejím uložením do trezoru, do něhož má přístup pouze vedoucí organizace.

Mezi základní požadavky, které musí každá bezpečnostní politika informačního systému v návaznosti na personální a organizační uspořádání obsahovat, patří úprava následujících vlastností: roztřídění informací - jejich klasifikace, zřizování a rušení uživatelů, nebo přístupů

pro práci s těmito informacemi, školení a vzdělávání a rovněž i otázky zastupitelnosti jednotlivých osob.

1.4.2 Klasifikace informací

Důležitým předpokladem pro práci s daty je jejich klasifikace a zařazení do příslušných tříd -bezpečnostních tříd. Nejčastěji bývají data rozděleny do tří základních tříd:

- Bez označení
- Důvěrné
- Přísně důvěrné

Bez označení – jde o běžná data, která nepodléhají žádnému zvláštnímu režimu utajení, oproti tomu přísně důvěrné vyjadřuje nejvyšší míru utajení. U firem patří do této kategorie nejcennější informační aktiva, jako jsou např. projekty, konstrukční plány, výrobní technologie a postupy, data z účetnictví.

Takřka ve všech organizacích dochází ke zpracování osobních údajů, minimálně pro účely evidence zaměstnanců a mezd. Osobní údaje zpracovávané v IS se řídí ustanoveními zákona č. 101/2000 Sb., o ochraně osobních údajů, který rozeznává dva stupně klasifikace údajů a to osobní a citlivé osobní.

Pokud v organizaci dochází ke zpracování utajovaných skutečností podle NBÚ – zákon č. 412/2005 Sb., jsou tyto data rozděleny do čtyř stupňů utajení:

- Přísně tajné
- Tajné
- Důvěrné
- Vyhrazené

V rámci organizace musí být určeno, jakým způsobem je s jednotlivými kategoriemi pracováno, stanovení okruhů lidí majících k nim přístup, jakož i sledování jejich pohybu.

1.4.3 Zřizování a rušení uživatelů, nebo přístupů

Ve většině organizací pracovník, který rozhodl o přidělení přístupových práv jak do počítačové sítě tak i jednotlivých aplikací je sám osobně nepřiděluje. Toto má na starosti nejčastěji správce počítačové sítě. I zde by měly být jasně stanovená pravidla a postupy pro přidělování a odebírání přístupových práv do systémů.

Pro zřízení, nebo změny uživatelského přístupu by měl být vytvořen základní profil uživatele pro danou funkci/skupinu uživatelů a jim odpovídající přístupová práva. Vedoucí pracovník poté při zadávání požadavku zvolí pro daného uživatele vhodný profil. Ve většině případů totiž vedoucí pracovník nemá dostatečný přehled o tom, která jednotlivá práva jsou nezbytně nutná pro výkon činnosti a která jsou již nadbytečná a zbytečně mohou vést k ohrožení systému. Tomuto zabráníme právě standardizací práv do jednotlivých oblastí, kdy správce na základě požadavku vedoucího přiděluje již předem odkonzultované a odzkoušené oblasti práv. Jednotlivé odlišnosti je poté možné doladit již pro konkrétní uživatele.

Poměrně důležitou otázkou je také rozdělení kompetencí a s tím souvisejících přístupových práv mezi jednotlivé správce systému v rozsáhlých organizacích. Každý správce IS by měl mít přiděleny administrátorské přístupy pouze k aplikacím, za jejichž provoz zodpovídá. Jako příklad je možné uvést např. oddělení funkce správce operačního systému serveru, který bude mít k němu administrátorský přístup a správce databázového serveru, který bude administrovat DTB server, popř. někdo další může být zodpovědný za server DNS atd.

1.4.4 Školení a vzdělávání

Základním předpokladem pro úspěšné uplatňování bezpečnostní politiky je seznámení všech zúčastněných osob s jejími zásadami. Toto seznámení je nutné provést již při nástupu nového pracovníka do zaměstnání v rámci vstupního školení. Upozornit jej na jeho práva a povinnosti ve vztahu k používání informačního systému a ochraně dat, jakož i na případné sankce za jejich porušení. Průběžná školení jsou pořádána v případech, kdy dochází k implementaci

nových informačních a komunikačních technologií, nových systémů či aplikací a je zaměřeno nejen na jejich správné používání, ale i zabezpečení.

Ve větších organizacích, které mají vlastní oddělení zabývající se správou a údržbou informačních systémů, takováto školení často provádí právě pracovníci tohoto oddělení. Nicméně v případě nasazení nových systémů či aplikací, mohou tyto školení být zajišťována externími firmami.

1.4.5 Požadavek zastupitelnosti

V souladu s náplní práce zaměstnanců a pro zajištění procesů kvalifikovaných jako kritické s vysokou prioritou platí požadavek zastupitelnosti a převzetí odpovědnosti v době nepřítomnosti. Není vhodné řešit zastupování formou sdělení hesla zastupující osobě, jak se často stává v praxi. Systémovým řešením v tomto případě je umožnit zástup pomocí přidělení práv k zastupování v rámci aplikace. V budoucnu se tak zamezí dohadům, kdo co v rámci aplikace provedl a kdo za to zodpovídá (nemusí uplynout ani příliš dlouhá doba a lidé si již obtížně vzpomínají na své zásahy do aplikace). Platí zásada, že každý zodpovídá za vykonané úkony a to i v rámci zastupování za jinou osobu a toto vše by mělo být zpětně dohledatelné.

1.5 Fyzické zabezpečení IS

Zde musíme samozřejmě rozlišovat mezi přístupem k jednotlivým počítačům nacházejícími se většinou v jednotlivých kancelářích a serverům, popřípadě počítačovým rozvodům a zařízením sítě nacházejících se obvykle v serverovnách. Přístup do serverovny je přísně omezen pouze na oprávněné zaměstnance. Serverovny bývají vždy pečlivě zabezpečeny před neoprávněným vniknutím, počínaje zámkem na dveřích, který bývá mimo klíčový systém (nelze se dovnitř dostat univerzálním klíčem), dveře na otevírání čipovou kartou. Často bývají vybaveny kamerovým systémem monitorujícím vstup do serverovny. Dále bývají standardně

vybaveny klimatizací a čidly elektronických požárních hlásičů. K bezpečnosti serveroven přispívá i to, že nejsou označeny a případný útočník nemůže tak lehce zjistit jejich umístění.

Oproti tomu jednotlivé počítače takovéhoto stupně ochrany nedosahují. A zde je právě třeba klást důraz na zodpovědný přístup jednotlivých pracovníků. Pokud zaměstnanec krátkodobě opouští pracoviště, je jeho povinností zabezpečit přístup do IS minimálně:

- spořičem obrazovky s nutností zadat heslo,
- uzamčením stanice/odhlášením ze systému, kdy je při opětovném přihlášení heslo povinně vyžadováno,
- uzamčením kanceláře, použitím autentizačních prostředků (např. vyjmutím čipové karty, USB tokenu s certifikátem)

Po skončení pracovní doby, nebo při dlouhodobém opuštění pracoviště je uživatel povinen vždy před odchodem:

- řádně ukončit běžící aplikace, odhlásit se ze systému,
- vypnout počítač

1.5.1 Biometrie

V dnešní době se stále častěji v praxi setkáváme s metodami biometrie, jako jedním z významných prostředků fyzického zabezpečení. Zatímco dříve tyto techniky patřily pouze do oblasti science-fiction, dnes musí biometrické prvky obsahovat i taková běžná věc, jakou je pas (v rámci EU bylo k tomuto přistoupeno na nátlak USA). Slovo biometrie pochází z řeckého bios (=život) a metron (=měřit). Studuje metody určené pro unikátní rozpoznávání lidí založené na jednom, nebo více podstatných fyzických nebo behaviorálních (tj. týkajících se chování) rysech. V oblasti informačních technologií biometrií rozumíme technologie, které měří a analyzují lidské fyzické a behaviouristické charakteristiky pro účely ověření (autentizace). Výhodou těchto metod ověření je to, že odpadá nutnost pamatování si hesel, používání chipových karet a dalších prostředků, které je obvykle nutné nosit při sobě. Další

podstatnou výhodou je jednoznačnost identifikace, neboť tyto vlastnosti nelze člověku „odcizit“. I u těchto metod však lze proces autentizace ošálit – záleží na vyspělosti technologií a samozřejmě „stupni výzkumu“. Každá nová technologie vyžaduje určitý čas na dostatečné prozkoumání a samozřejmě ověření v praxi.

Nejčastěji používanou metodou je identifikace podle prstů. Tento způsob ověření je relativně levný (oproti jiným metodám) a již dobře prozkoumaný. Dnes je již běžné, že např. notebooky jsou vybaveny snímačem otisku prstů (zatím pouze ty dražší modely). Je však třeba připomenout že tuto metodu nelze považovat za naprosto 100%. Novou technologií poměrně rozšířenou je také identifikace na základě oční duhovky. Avšak i oční duhovka se může v průběhu života měnit např. následkem úrazů hlavy, očních nemocí. Jde o jeden z nejrychlejších způsobů biometrické identifikace. Poměrně jednoduchým a finančně nenáročným způsobem rozpoznávání je identifikace na základě hlasu. Obvykle bývá používána jako doplněk k některé jiné metodě. Kromě těchto nejčastěji zmiňovaných způsobů existují i další jako je identifikace podle obličeje na základě jeho tvaru a dalších rysů, umožňující rychlou identifikaci jedince nacházejícího se ve skupině osob. Tento systém byl testován např. na amsterodamském letišti Schiphol, nebo na fotbalovém stadionu PSV Eindhoven. Také je možné identifikovat jedince na základě dynamiky podpisu – každý člověk má totiž charakteristický způsob podepisování. Vyhodnocuje se pohyb a tlak v jednotlivých částech podpisu. Obvyklé metody již v současnosti nedostačují (krádeže karet, prozrazení hesel atd.), v budoucnu se tedy stále častěji budeme setkávat s použitím těchto nových metod významně přispívajících ke zvýšení bezpečnosti.

2 Bezpečnost dat

Jelikož součástí této práce je vytvoření návrhu počítačové sítě založené na produktech společnosti Microsoft (konkrétně MS Windows Server 2003 a klientské PC Windows XP Professional) v této části se budu zabývat možnostmi zabezpečení dat právě v takovéto síti.

2.1 Zabezpečení na úrovni operačního systému

Počítačová síť založená na technologiích Microsoftu, složená z klientských počítačů, na nichž jsou nainstalovány různé verze operačního systému Windows může být vytvořena jako síť složená z rovnocenných počítačů, nebo jako síť s řídícím počítačem (popř. počítači). První možnost je postavena na členství PC v pracovní skupině. Této možnosti lze použít jako jednoduchého a levného řešení u velice malého počtu počítačů, kdy všechny počítače jsou na stejné úrovni. Počítače neumožňují účinnou vzájemnou spolupráci a není možné jednoduše zajistit jejich společnou správu. Zrovna tak i nastavení zabezpečení dat je otázkou nastavení každého jednotlivého počítače.

Druhá varianta je založena na vytvoření vlastní domény a její správu prostřednictvím serveru a právě možností zabezpečení dat v takovéto síti se budu dále zabývat. Základním předpokladem je instalace serveru ve funkci doménového řadiče. Ve verzi Windows NT to byl PDC (Primary Domain Controller), který mohl být v síti pouze jeden a jednoho, nebo více BDC (Backup Domain Controller). Od verze Windows Server 2000 je správa domény založena na Active Directory. Tady bych se rád ještě vrátil k pojmu doména a stručně vysvětil, co to vlastně znamená.

Doména je vlastně databáze obsahující informace o objektech v síti. Tj. obsahuje všechny účty uživatelů, skupiny uživatelů, účty počítačů, informace o tiskárnách a informace o dalších objektech. Doména tedy představuje logické seskupení objektů v síti a právě počítač, na kterém je uložena databáze Active Directory je nazýván řadičem domény. Veškeré dotazy na adresářovou službu vyřizuje právě tento počítač. Na rozdíl od verze Windows NT již není

rozlišováno mezi primárním a záložním řadičem, ale každý Active Directory obsahuje stejné informace – při nedostupnosti jednoho se počítače automaticky obrátí na další.

2.1.1 Uživatelské účty

Aby se uživatel mohl přihlásit do počítačové sítě, je nutné, aby v ní měl zřízen uživatelský účet. Každý uživatel má svůj vlastní, použití jednoho společného účtu pro více uživatelů je naprosto nevhodné řešení. Uživatelský účet nám umožňuje nejen se přihlásit do sítě a nastavit přístupová práva, ale i sledovat a vyhodnocovat aktivity uživatelů v síti, což je velice důležité v případě výskytu problémů. V neposlední řadě nám usnadní konfiguraci a správu uživatelů, pokud se vyskytnou konkrétní požadavky na individuální nastavení uživatelských profilů. V počítačích s doménou se vyskytují dva druhy účtů: místní a doménový. Pro nás však místní účty nemají žádný význam, dále budeme brát v potaz pouze doménové účty (místní by se uplatnily v případě pracovní skupiny), umožňující nastavení oprávnění v rámci domény. Aby nebylo nutné nastavovat práva pro každého uživatele zvlášť, jsou účty organizovány do skupin uživatelů. Další podstatnou věcí ovlivňující možnost nastavení přístupových práv k souborům je souborový systém, jakým byly naformátovány disky používané serverem. Je samozřejmostí, že na serveru nebude použit filesystém FAT, popř. FAT32, ale pouze NTFS umožňující nastavení přístupových práv k adresářům i souborům.

2.1.2 Nastavení přístupových práv k souborům a adresářům

Při použití filesystému NTFS je možné udělovat oprávnění pro jednotlivé soubory i jednotlivé adresáře. Pokud některému uživateli přidělíme oprávnění na úrovni adresáře, bude toto oprávnění platné i pro všechny podadresáře a soubory v nich umístěné, neboť v systémech Windows je standardně povolena dědičnost z nadřízených objektů na podřízené. Pokud bychom však potřebovali toto dědění práv zrušit, je toto samozřejmě také možné – stačí zrušit zatržení položky Zdědit po nadřazeném objektu položky oprávnění.

Tab. 2.1: Standardní oprávnění NTFS

Oprávnění	Význam
Read	Umožňuje číst obsah souboru a jeho atributy
Read & Execute	Stejné jako Read, u spustitelného souboru umožňuje jeho spuštění
List Folder Contents	Použité pouze u složky – umožňuje zobrazit obsah složky
Write	Umožňuje vytvářet nové soubory a provádět změny ve stávajících
Modify	Umožňuje měnit název souboru a odstraňovat existující soubory
Full Controll	Umožňuje měnit seznam řízení přístupu
Special Permissions	Umožňuje nastavit speciální oprávnění

Pramen: Šetka Petr, Mistrovství v Microsoft Windows Server 2003, Computer Press, 2003

Pokud budeme potřebovat udělit přístup ostatním uživatelům k datům umístěným na jiném počítači v síti, musíme tyto složky nastavit jako sdílené a nastavit oprávnění ke sdílení. Je možné přidělit následující oprávnění: Full Controll, Change, Read. Ve Windows Serveru 2003 je výchozí nastavení pro skupinu Everyone oprávnění Read, narozdíl od systémů Windows 2000 a Windows XP Professional, kde bylo výchozí oprávnění Full Controll. Nastavení přístupových práv na úrovni NTFS se použije vždy, tedy i pro místně přihlášeného uživatele, na rozdíl od oprávnění ke sdílení platících pouze pro uživatele vzdáleně se přihlašujícího. Výsledkem je tedy stav, kdy pro vzdálené uživatele přistupující k počítači prostřednictvím sítě platí průnik obou nastavených pravidel. Pokud například uživatel Everyone bude mít nastaveno právo ke sdílení Full Controll a na úrovni NTFS pouze Read, výsledkem bude oprávnění pouze ke čtení. Další důležitou vlastností filesystému NTFS je vlastnictví souboru. Každý soubor má totiž svého vlastníka a platí pravidlo, že vlastník může se svým souborem dělat cokoliv chce – může měnit seznam řízení přístupu k danému objektu a to nejen pro vlastní účet. Vlastník tedy ačkoliv nemusí mít přiděleno oprávnění Full Controll, může si sám jakékoliv oprávnění přidělit, popřípadě komukoliv odebrat.

2.1.3 Konfigurace zabezpečení počítačů a sítě

Nastavení zabezpečení při přihlašování uživatelů, přístupová práva na úrovni souborů a adresářů, šifrování dat atd. jsou jistě velice důležité nástroje zvyšující bezpečnost počítačové

sítě i jednotlivých počítačů. Kromě nich má však správce k dispozici další neméně důležitý nástroj a tím je definování zabezpečení na úrovni domény jak pro všechny, tak i jednotlivé počítače i uživatele. Již v systému Windows NT Server existovala možnost nastavit toto chování prostřednictvím souborů bezpečnostní politiky. Ve verzích Windows 2000 a 2003 Server máme možnost nastavit zabezpečení pomocí objektu zásad skupiny v rámci služby Active Directory. Pokud chceme nadefinovat zásady pro určité konkrétní uživatele, nebo počítače, vytvoříme si novou organizační jednotku, do níž přiřadíme požadované a definujeme konkrétní bezpečnostní politiku. My se stručně podíváme na přehled možností nastavení jednotného zabezpečení pro celou doménu. Toto můžeme nastavit v rámci Default Domain Policy – Security Settings, kde máme k dispozici následující položky:

Tab. 2.2: Přehled položek Domain Policy - Security Settings

Název položky	Význam
Account Policies	Určuje, jak budou vypadat hesla doménových uživatelů, zda se v určitém časovém rozmezí účet zamkne a parametry a časová platnost lístků protokolu Kerberos.
Local Policie	Konfiguruje audit činností v síti, přiřazení práv uživatelům a skupinám a základní možnosti zabezpečení.
Event Log	Zásady pro konfiguraci protokolů událostí.
Restricted Groups	Definuje a hlídá členství v konkrétních skupinách.
System Services	Které služby se budou při spuštění počítačů spouštět automaticky, které budou nastavené na ruční spouštění a které budou zakázány.
Registry	Umožňuje zakázat přístup ke konkrétním větvím registru, nebo naopak povolit přístup běžným uživatelům.
File Systém	Pomocí této části lze definovat oprávnění NTFS na konkrétní soubory či složky v počítačích, kterých se tyto zásady týkají.
Public Key Policies	Definuje agenty obnovení dat, automatické zapisování certifikátů pro účty počítačů, důvěryhodné certifikační úřady (obecné i v rámci vlastní sítě).
Software Restriction Policies	Omezení softwaru – umožňuje omezit spouštění nepovolených programů.
IP Security Policies on Active Directory	Definuje podepisování a šifrování paketů protokolu IP v síti.
Wireless Network (IEEE 802.11) Policie	Zásady bezdrátové sítě umožňují konfigurovat zabezpečení provozu v místní bezdrátové síti.

Pramen: Šetka Petr, Mistrovství v Microsoft Windows Server 2003, Computer Press, 2003

2.2 *Programové možnosti zabezpečení*

Programové možnosti zabezpečení jsou velice široké. Existuje celá řada specializovaných aplikací zabývajících se touto oblastí. Proto zde uvádím pouze jako příklad použití systému EFS vzhledem k tomu, že je součástí operačního systému Windows Server 2003 a nevyžaduje tedy již další náklady na jeho pořízení. V dnešní době je nemyslitelné provozovat počítač bez dostatečné ochrany proti virům a dalším formám malwaru, proto se zde zmiňuji i o tomto.

2.2.1 Systém EFS

Od systému Windows 2000 a pozdějších se objevila možnost využít šifrovací systém souborů (Encrypting File System, EFS). Šifrovat lze jak jednotlivé soubory, tak i celé složky. Pokud uživatel používá systém EFS, na první pohled nepozná rozdíl oproti běžné práci s nezašifrovanými soubory, neboť činnost šifrování a dešifrování je před uživatelem skryta (proces běží na pozadí – lze si ovšem představit, že na velmi pomalém počítači při šifrování velkého počtu souborů dojde ke zpomalení PC).

EFS využívá kombinace dvou typů šifrování – symetrického i asymetrického. Celý systém pracuje na stejném principu kombinace symetrického a asymetrického šifrování jako jsme si již řekli v předchozí části, kapitola 1.3. Uživatelská data jsou zašifrována s použitím symetrického šifrování a poté je tento klíč asymetricky zašifrován pomocí veřejného klíče uživatele. Aby byla zajištěna důvěryhodnost veřejného klíče uživatele, je nutné aby jej ověřila nezávislá třetí strana, které všichni zúčastnění důvěřují – Certifikační autorita. Teprve podepsáním veřejného klíče certifikačním úřadem vznikne certifikát, se kterým pak jednotliví uživatelé pracují v rámci systému EFS. V tomto systému je uživatel, který soubor zašifroval současně i tím, komu je soubor určený a kdo jej může rozšifrovat.

V systémech Windows dochází k vygenerování páru klíčů automaticky při prvním pokusu o zašifrování souboru, samozřejmě za předpokladu, že uživatel ještě nemá klíče vygenerované. Do takto zašifrovaného souboru má poté přístup pouze vlastník souboru, tedy uživatel, který

soubor zašifroval. Od verze Windows XP Professional však přibyla možnost určit i další uživatele, kteří budou moci soubor rozšifrovat.

To, jak mohou uživatelé využívat tohoto systému šifrování v praxi závisí nejen na použité verzi operačního systému u klientského PC, verzi serveru, ale i na něm poskytovaných službách. Základním předpokladem, jak už bylo výše zmíněno, je, aby uživatel používal operační systém Windows XP Professional (jinak nebude moci přidat další uživatele). V počítačové síti, ve které je provozován Windows Server 2003 je nutné nainstalovat na server službu Certifikační úřad, která bude automaticky publikovat všechny vystavené certifikáty uživatelů v doméně Active Directory – o tom se můžeme přesvědčit u jednotlivých uživatelů na záložce Published Certificates (nutným předpokladem však je, aby existoval pro daného uživatele certifikát – tedy tento uživatel již musel v minulosti provést šifrování). Při instalaci lze zvolit mezi dvěma typy certifikačního úřadu:

- Certifikační úřad pro rozlehlé sítě – tento certifikační úřad vystavuje certifikáty pouze pro uživatele, kteří mají v dané doméně doménový účet.
- Samostatný certifikační úřad – tento typ certifikačního úřadu je schopen vystavovat certifikáty nejen uživatelům s doménovým účtem, ale i ostatním uživatelům.

V běžné počítačové síti, kde nepotřebujeme vystavovat certifikáty cizím uživatelům je vhodné použít certifikační úřad pro rozlehlé sítě, neboť tento má jednu velice důležitou vlastnost. Narozdíl od samostatného certifikačního úřadu umožňuje vystavovat certifikáty automaticky. Předpokladem pro vystavení certifikátu je vždy ověření uživatele (je to samozřejmost i když žádáte o vystavení certifikátu kterýkoliv certifikační úřad – např. asi u nás nejznámější První certifikační autorita), neboť certifikační autorita vystavením certifikátu potvrzuje Váš „elektronický podpis“ s tím, že je opravdu Váš, podobně jako notář ověřující podpis na dokumentu (Ten však potvrdí pouze jeden podpis, certifikační autorita potvrzením umožní podepisovat jakékoliv množství dat. Sice zde píši o podpisu, ale týká se to i šifrování dat viz. předchozí části - veřejný a soukromý klíč). Pro certifikační úřad pro rozlehlé sítě je dostatečným důkazem Vaší identity existence doménového účtu.

Kromě dvou výše uvedených možností instalace, nabízí instalace na výběr ještě mezi kořenovým a podřízeným certifikačním úřadem. Rozdíl mezi nimi je patrný již z jejich názvu – podřízený musí být ověřen kořenovým cert. úřadem, zatímco kořenový si podepíše veřejný klíč sám (podepíše klíč sám sobě). Aby fungovala služba automatického vystavování certifikátů je nutné kromě instalace certifikačního úřadu pro rozlehlé sítě použít Windows Server 2003 a to konkrétně verzi Server 2003 Enterprise Edition. Poslední podmínka je velice důležitá, neboť verze Server 2003 Standard toto neumožňuje. Poté stačí již jen v šabloně certifikátu EFS povolit automatický zápis a nakonfigurovat objekt zásad skupiny pro automatický zápis certifikátu. Uživatel, který teď hodlá umožnit přístup k zašifrovaným datům i uživateli, který sám dosud nešifroval tak nyní může učinit, neboť požadovaný certifikát je automaticky vystaven. V této části jsme se zabývali výhodami použití systému EFS a vystavováním certifikátů pro uživatele, ale použití certifikačního úřadu je mnohem širší – můžeme vystavovat certifikáty např. počítačům. A na závěr ještě poznámku: Soukromý klíč je uložen v uživatelském profilu. Pokud tedy dojde k odstranění, nebo poškození profilu například chybou systému, přijde uživatel i o soukromý klíč a možnost přístupu k datům, proto bych rád upozornil na možnost exportu soukromého klíče a jeho bezpečnou archivaci [18].

2.2.2 Antivirové zabezpečení

Zrovna tak jako pravidelné zálohování dat je v dnešní době velice důležitá i ochrana počítačů před různými viry, trojskými koni atd. Na každém počítači by měl být nainstalován antivirový program - v síti skládající se z většího počtu počítačů již není možné, aby každý takovýto antivirový program byl konfigurován a spravován individuálně. Zde je třeba použít centralizované řešení umožňující správu všech klientských stanic ze serveru na němž běží řídící program. Vhodné je také zabránit uživatelům měnit nastavení antivirového programu, neboť uživatelé potom mají tendenci vnímat např. pravidelně spouštěnou antivirovou kontrolu disků jako obtěžování a zpomalování jejich počítače. Takováto kompletní kontrola všech disků v počítači by měla být spouštěna minimálně jedenkrát týdně. Toto samotné by však

samozřejmě nestačilo, proto musí být trvale zapnuta rezidentní antivirová ochrana běžící na pozadí a kontrolující veškeré operace s daty, které uživatel provádí v reálném čase. Důležité je také zajistit pravidelnou aktualizaci antivirové databáze, což je činnost za niž je odpovědný správce systému. Aktualizace by měly být stahovány ihned po jejich vydání a automaticky instalovány na všechny počítače v síti. Vzhledem k tomu, že i nejznámější a nejčastěji používané antivirové programy mívají problémy s odhalováním adware, je vhodné je použít v kombinaci ještě s jiným specializovaným programem.

2.3 Organizační a personální otázky zabezpečení dat

Ani to nejlepší zabezpečení počítačové sítě nezabrání úspěšnému útoku na počítačovou síť, pokud uživatelé nedodržují základní bezpečnostní pravidla. Mezi takovéto minima patří především požadavek na neodhalitelnost hesla uživatele, pravidelné zálohování dat, antivirová kontrola, záložní zdroj a apod.

2.3.1 Požadavky kladené na hesla

Pokud si uživatel zadá jako heslo snadno odhadnutelné slovo, nebo dokonce si heslo napíše někam, odkud jej lze lehce získat, potom jsou veškerá další bezpečnostní opatření zbytečná. Pravidla na složitost a zabezpečení hesla lze stanovit prostřednictvím Default Domain Policy v části Account Policies pro celou doménu. Nelze je stanovit pro určitého uživatele (skupinu uživatelů) jinak tj. pokud bychom požadovali pro některého uživatele jiné podmínky, nemohl by být členem této domény, ale musela by se vytvořit další doména s jinak definovanými pravidly.

Windows 2003 Server obsahuje již předdefinované zásady, které vedou k nutnosti používat poměrně bezpečná hesla. Heslo musí splňovat požadavek na složitost – musí obsahovat alespoň tři ze čtyř možností a to: malá písmena, velká písmena, číslice a speciální znaky. Maximální stáří hesla je nastaveno na 42 dnů, poté je musí uživatel změnit, jinak je mu

přihlášení zakázáno. Výjimku tvoří účty, které mají ve vlastnostech zaškrtnuté políčko Heslo je platné stále. Minimální délka hesla je stanovena na 7 znaků. Minimální stáří hesla 1 den, tj. pokud si uživatel změní heslo, musí jej používat nejméně jeden den – tímto zabráníme tomu, aby uživatelé rychle „protočili“ hesla a vrátili se k používání původního. Historie hesel si pamatuje 24 hesel, není tedy možné používat pouze dvě hesla a ty mezi sebou měnit. Dalším důležitým nastavením jsou zásady uzamčení účtu – počet neúspěšných přihlášení, po kterých se účet uzamkne, po jaké době po zamčení se počítadlo neúspěšných přihlášení nuluje a po jaké době po zamčení se účet automaticky odemkne, nebo zda jej je nutné odemknout ručně.

2.3.2 Zálohování dat

Při rozhodování o způsobu zálohování dat je třeba vzít v úvahu důležitost a nenahraditelnost jednotlivých druhů dat. Je poměrně zbytečné zálohovat data, která jsou snadno dostupná a opakují se u velkého množství uživatelů, pro každého uživatele zvlášť (v praxi se často vytvoří jeden image disku společný pro všechny uživatele, který se použije jako základ pro obnovu systému a poté se jednotlivá data obnoví z individuálních záloh). Nadbytečně velké objemy dat zbytečně zpomalují vlastní zálohování a zabírají místo ať již na disku, nebo jiném záznamovém médiu. Je tedy zbytečné provádět zálohu u všech uživatelů zálohu celého operačního systému, spíše je třeba se zaměřit na vlastní uživatelská data a konfigurace, které jsou pro každého uživatele jedinečné. Na zálohování můžeme pohlížet také z hlediska toho, kde zálohy probíhají. Samozřejmě jiné jsou požadavky na zálohování serverů a jiné jednotlivých pracovních stanic. Je takřka nemyslitelné, aby na serverech neprobíhalo automatické zálohování – a to ať již serverů poskytujících různé např. síťové služby, kde budeme minimálně zálohovat konfigurace, nebo zejména aplikačních se zpracovávanými daty. Zatímco na serverech je toto automatické, uživatelé na svých počítačích většinou nemají automatické zálohování ve zvyku. O to větší je to pro ně překvapení, pokud následkem např. chyby programu, hardwarové poruchy, napadení počítače virem nebo i omylem uživatele o svoje data přijdou. Proto by nebylo příliš vhodné ponechat toto pouze na starost uživatelům, ale vhodným způsobem se postarat o zabezpečení i jejich dat. Zálohováním uživatelských dat

se však budeme zabývat později. Jak jsem se již výše zmínil, servery jsou z tohoto hlediska podstatně lépe zabezpečeny, zejména aplikační. Zálohy zde můžeme vytvářet buď jako celkové, nebo přírůstkové (zrovna tak i na pracovních stanicích uživatelů).

3 Internet a bezpečnost dat

Při připojování lokálních chráněných sítí k veřejným je prvořadým požadavkem zachovat bezpečnost lokálního informačního systému a přitom neomezovat funkčnost propojení s okolím. Útok zvenčí je typickou hrozbou pro informační systém, který je připojen k veřejné síti či Internetu. Hlavním prostředkem pro zabezpečení vnitřní sítě je firewall. V předchozích částech probírané možnosti zabezpečení chránily počítačovou síť i před útoky zevnitř. Tyto útoky bývají často opomíjeny, nebo podceňovány a právě nedostatky v této oblasti bývají příčinnou mnoha úspěšných napadení systémů.

3.1 Připojení k Internetu

Zde si řekneme, co to vlastně znamená připojení k Internetu a jakým způsobem je možné jej realizovat. Rozlišit můžeme dva základní způsoby připojení: připojení k Internetu s veřejnou IP adresou a připojení bez veřejné IP adresy. Uživatel, který je připojený k Internetu přes veřejnou IP adresu je vlastně součástí Internetu, je ostatním uživatelům z Internetu dostupný a může jim tak poskytovat svoje služby např. provozovat webový server. Uživatel bez veřejné IP adresy se k Internetu připojuje přes počítač, který má veřejnou adresu, takže z Internetu je viditelný pouze tento počítač a nikoliv již uživatel přes něj se připojující. Tento druhý způsob je častější a je typický pro připojení firem. Firma v tomto případě má k dispozici jednu, nebo více veřejných adres, přes které se připojují jednotliví uživatelé lokální sítě. Jde tedy o situaci, kdy pro velký počet místních uživatelů máme k dispozici pouze malý počet veřejných adres. Toto je v praxi řešeno připojením uživatelů přes proxy server, nebo použitím Network Address Translation (dále jen NAT). V místní síti potom mají uživatelé přiděleny lokální IP adresy a to ať již pevné, nebo dynamicky přidělované (prostřednictvím DHCP serveru) z adresového prostoru pro neveřejné sítě (viz kapitola 1.6.2.1 Internet Protocol: IP). Základní rozdíl mezi proxy serverem a NAT spočívá v tom, že proxy server si ukládá data požadovaná uživateli do místní cache, NAT však nikoliv. Proxy server tak v případě, že uživatelé přistupují často ke stejným webovým stránkám vede ke zrychlení, neboť data nejsou pokaždé

stahována z Internetu z webového serveru, ale z vyrovnávací paměti serveru (cache). I u proxy serveru je možné vypnout cacheování, tím by však ztrácel svůj smysl (cacheování funguje u http proxy, socks proxy již z principu nemůže, neboť pracuje pouze s IP pakety - pouze upraví adresu paketu tak, jako by byl odesílatelem on sám a protokoly z vyšší úrovně se ho vůbec netýkají). Při konfiguraci prohlížeče u uživatele je třeba nastavit adresu proxy serveru zprostředkujícího spojení a port (např. Squid používá port 3128). Toto odpadá při použití transparentního proxy serveru, kdy nemusíme nic nastavovat, router náš požadavek zachytí a místo cílovému počítači jej pošle proxy serveru, který se zeptá za nás a odpověď si uloží do cache i pro další zájemce.

Použití neveřejné IP adresy přispívá také ke zvýšení bezpečnosti počítačové sítě, neboť celá struktura lokální sítě je skryta za veřejnou IP adresou. Připojení k Internetu můžeme rozdělit na komutované, tedy dočasné připojení (Dial-Up, ISDN, mobilní) a pevné, kdy uživatel je připojen stále (pronajatý datový okruh, bezdrátové připojení, DSL technologie, kabelová televize, satelit, silové okruhy).

3.2 WiFi

V předchozí části jsme si řekli několik informací o připojení k Internetu, základní druhy připojení převzaté ze serveru http://tutorialy.lupa.cz/internetove-pripojeni jsou stručně uvedeny v příloze číslo 2. Jelikož naše místní síť bude připojena pomocí bezdrátového připojení, podíváme se právě na vytváření bezdrátových sítí trochu podrobněji. Často bývá tento způsob komunikace označován jako WiFi (Wireless Fidelity). Ve skutečnosti je WiFi komerční označení a logo výrobků pracujících podle standardu IEEE802.11a/b/g – zařízení takto označená musí být mezi sebou kompaktibilní.

802.11b – označuje standard bezdrátových sítí v nelicencovaném pásmu 2,4 až 2,4835 GHz (rozsah 83,5 MHz). I když jde o bezlicenční pásmo, jeho uživatelé musí dodržet určité podmínky jako je např. maximální vyzařovaný výkon, který může být maximálně 100 mW. Toto pásmo je v České republice rozděleno na 13 kanálů. Aby nedocházelo k vzájemnému

rušení kanálů, je nutné použít kanály tak, aby mezi nimi byla vzdálenost 5 kanálů. Maximální teoreticky dosažitelná rychlost tohoto standardu je 11 Mb/s.

802.11g - jde o rozšíření 802.11b a zvyšuje přenosovou rychlost na 54Mb/s při zachování kompaktibility

802.11a - tento standard pracuje v licencovaném pásmu 5 GHz (od 5,47 do 5,725 GHz). Teoretická přenosová rychlost je 54 Mb/s. Jelikož není u nás tak často používán, není zde tak velké nebezpečí vzájemného rušení jako u 802.11b.

Na konci můžeme najít i další písmena, která označují různé verze standardu IEEE802. Síť založená na bezdrátové technologii je označována jako WLAN [19].

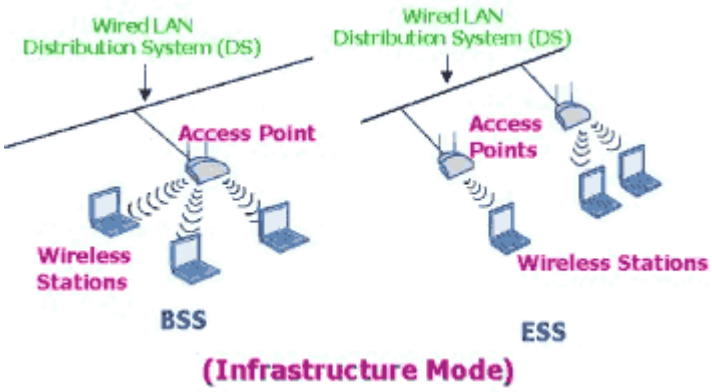
Existují dvě základní topologie, jak mohou být sítě WLAN propojeny. A to jako takzvaná Ad-Hoc síť, která nepoužívá přístupové body. V této síti jsou veškerá zařízení na stejné úrovni a komunikují mezi sebou navzájem. Jednotlivé počítače jsou vybaveny Wi-Fi adaptérem a komunikují mezi sebou přímo – nepotřebují základnové stanice. Tato struktura bývá používána v jednoduchých sítích, nebo jako dočasný způsob propojení zařízení. Její výhodou je jednoduchost, rychlost vytvoření a samozřejmě finanční nenáročnost, přináší ovšem i určité nevýhody, zejména omezení v dosahu neboť všechny komunikující zařízení musí být v dosahu jeden druhého.

Obr. 3.1: Topologie Ad-Hoc

Pramen: Knapovský, Miroslav: WiFi: Průniky do sítí a připojení k Internetu

Druhá topologie nazývaná Infrastrukturní připomíná klasickou síť LAN postavenou na strukturované kabeláži. Stejně jako v „kabelové“ síti jsou všechny počítače připojeny do HUBU, v infrastrukturním režimu se počítače prostřednictvím WiFi propojují přes přístupové body (access point). Ačkoliv se dnes v LAN místo Hubu používají spíše Switche, funkce přístupového bodu se podobá Hubu, v případě připojení WLAN na LAN přibírá i funkci routeru. Existuje široký výběr přístupových bodů plnících funkci brány (gateway) pro připojení k Internetu prostřednictvím technologií xDSL, ISDN a poskytujících služby jako DHCP, NAT, firewall, možnost připojení USB zařízení a jejich mapování do sítě. Infrastrukturní síť podstatně rozšiřuje rozsah pokrytí. Všechny zařízení již nemusí být v dosahu jedno druhého, postačí, pokud jsou zařízení v dosahu přístupového bodu, který komunikaci předá dále, jak je vidět na následujícím obrázku.

Obr. 3.2: Topologie Infrastrukturní režim



Pramen: Knapovský, Miroslav: WiFi: Průniky do sítí a připojení k Internetu

Bezdrátová technologie WiFi neslouží jen k vytváření sítí v domácnostech, kancelářích a obecně v uzavřených prostorách, ale často je použita i jako venkovní řešení propojení. A to buď jako veřejné přístupové body tzv. „hotspoty“, nebo k přímému propojení např. dvou budov. Při venkovním použití mají přístupové body větší pokrytí (s použitím externích či směrových antén k přímému propojení), nicméně jejich vyzařování je omezeno předpisy Českého telekomunikačního úřadu. Data se v bezdrátových sítích vysílají všesměrově a tak

není těžké je odposlechnout. Základním prostředkem zabezpečení navržený organizací IEEE byl šifrovaný protokol WEP [20].

3.3 Firewall

Na rozdíl od opatření uvedených v předchozích částech, firewall chrání vnitřní síť pouze před útokem z vnějších sítí. Jedná se o prostředek, který odděluje bezpečnou síť od nezabezpečené. Pojem firewall však neznamená jen programové a technické vybavení, chránící síť před nezabezpečeným přístupem z vnější sítě. Především představuje použití bezpečnostní politiky, která definuje povolené služby a možnosti přístupu pomocí technických prostředků. Princip firewallu spočívá v tom, že nutí veškerý síťový provoz (mezi vnitřní a vnější sítí) procházet přes kontrolní systém, analyzuje komunikaci a na základě této analýzy povolí nebo zakáže propojení. Firewallem může být jak router, nebo počítač s alespoň dvěma síťovými kartami (popř. jiným rozhraním), na němž je nainstalován vhodný operační systém s programovým vybavením.

Firewall se skládá z jednotlivých prvků a závisí na našich požadavcích, které služby budeme od něho očekávat. Základem pro rozdělení firewallů je rozdělení podle informací, které firewall vyhodnocuje, do následujících skupin:

- paketový filtr
- firewall pracující na úrovni spojení
- firewall s proxy službami, pracující na aplikační vrstvě
- dynamický paketový filtr

3.3.1 Paketový filtr

Paketový filtr je jednoduchý firewall, který společně s překladem adres NAT bývá často používán ve směrovačích a přepínačích, neboť díky jeho jednoduchosti je velice rychlý. Tento firewall povolí, nebo naopak zakáže komunikaci na základě vyhodnocení údajů z IP hlavičky. Mezi tyto údaje patří fyzické rozhraní, zdrojová a cílová IP adresa, použitý přenosový protokol vyšší vrstvy (např. TCP, UDP) a zdrojový a cílový port. Umožňuje tedy jen velice jednoduché rozlišení mezi povolenou a nepovolenou komunikací, neboť provoz kontroluje pouze podle IP hlavičky a není schopen kontrolovat protokoly vyšších vrstev (některé umí rozlišit službu jako např. DNS, POP3 na základě použitého portu). Nelze tedy od něho očekávat např. filtrování protokolu http podle URL adres jako u firewallu s proxy službami [21].

3.3.2 Firewall pracující na úrovni spojení

Tento firewall vyhodnocuje spojení z hlediska toho, jaký paket se snaží projít přes firewall. Z tohoto pohledu můžeme pakety rozdělit na ty, které slouží k navázání nového spojení a takové, které patří k již navázanému spojení a jsou součástí komunikace. Můžeme tedy povolit navázání spojení pouze na základě námi předdefinovaných pravidel tj. mezi povolenými účastníky na odchozí i příchozí straně. Tento firewall udržuje tabulku navázaných spojení a kontroluje, zda procházející pakety patří některému z platných spojení. U požadavků na navázání nové komunikace ověřuje povolení této komunikace.

Cit. dle [21]:

Firewall obvykle udržuje následující informace o existujících spojení:

- jednoznačný identifikátor spojení, používaný pro sledování spojení
- stav spojení (handshake, ustanoveno, uzavřeno)
- sekvenční informaci
- zdrojovou IP adresu, tedy adresu, odkud paket pochází
- cílovou IP adresu, tedy adresu, kam má být paket doručen
- fyzická síťová rozhraní, na které paket přichází
- fyzická síťová rozhraní, ze kterého paket odchází

3.3.3 Dynamické paketové filtry

Dynamické paketové filtry fungují podobně jako výše zmíněné filtry na úrovni spojení. Opět kontrolují pakety, zda slouží k navázání nového, či k již existujícímu spojení. Navázání spojení je povoleno pouze z místní sítě, přičemž z vnějšího rozhraní je zablokováno. Poté další pakety, realizující vlastní komunikaci mohou procházet oběma směry. Také tento firewall tedy udržuje tabulku platných spojení a do LAN propustí pouze pakety, které jsou odpovědí na pakety z místní sítě [21].

3.3.4 Aplikační firewally

Při použití aplikačního firewallu dochází ke skutečnému logickému oddělení vnitřní sítě od vnější. Narozdíl od paketových filtrů zadrží aplikační firewall všechny pakety a pro povolená spojení toto sám naváže.

„Aplikační firewall vyhodnocuje informace na aplikační vrstvě ve všech paketech předtím, než povolí spojení. Udržuje kompletní informace o stavu všech spojení. Kromě toho

vyhodnocuje informace, které se objevují pouze v aplikační vrstvě, jako jsou například hesla uživatelů, nebo požadavky na služby.“[21].

Princip činnosti takovéhoto firewallu spočívá v tom, že uživatelské programy místo aby komunikovaly přímo se skutečným cílovým počítačem (na němž běží daná služba), komunikují s aplikačním firewallem. A až teprve firewall předává tyto požadavky cílovým počítačům, řídí a kontroluje spojení a dále zabraňuje přenosu nepovolených dat. Aplikační firewally jsou podstatně bezpečnější než paketové filtry, ale na druhé straně jsou pomalejší a je možné je použít pouze u služeb, které podporují. Častou součástí firewallu bývá také antivirový program, který kontrolou obsahu přenášené informace zabrání proniknutí virů do místní sítě, nebo např. HTTP proxy, který cacheováním dokumentů zvýší průchodnost spojení do vnější sítě.

3.3.5 Obecné výhody a nevýhody firewallu

Firewall umožňuje:

- Skrytí lokální sítě. Firewall může pracovat tak, aby byl z vnější sítě viditelný pouze on a lokální počítačová síť umístěná za ním, již vidět není.
- Oprávněným uživatelům vnější i lokální sítě umožňuje obousměrnou komunikaci podle nastavených přístupových omezení.
- Překlad privátních adres (Network Address Translation – NAT).
- Umožňuje identifikaci a autentizaci uživatelů.
- Kontroluje přístup k síťovým službám kontrolou dat přes něj procházejících.
- Zabraňuje neautorizovanému přístupu uživatelů z vnější sítě ke zdrojům lokální sítě.

Nedostatky firewallů:

- Firewall chrání pouze proti útokům z vnější sítě, nikoliv proti vnitřním útokům.

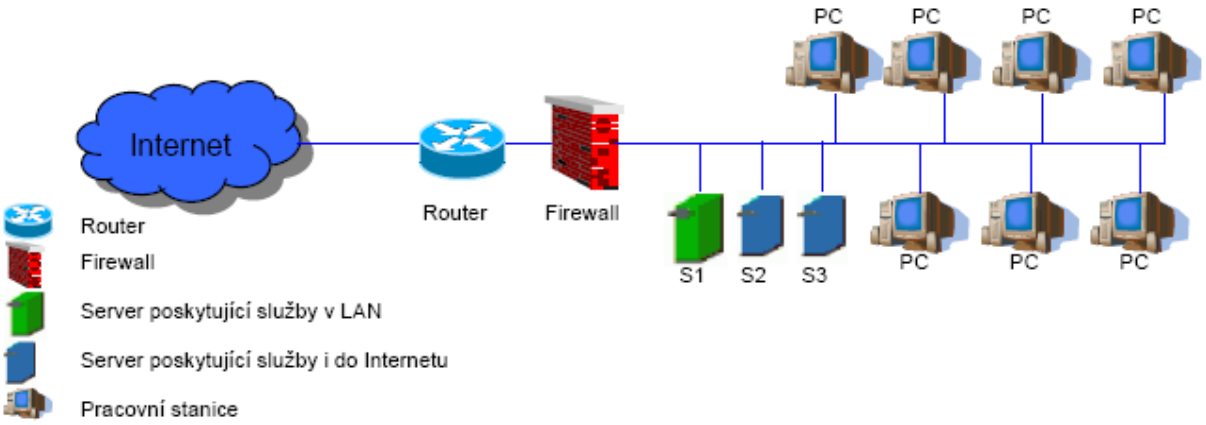
- Nechrání před útoky vedenými přes data např. prostřednictvím pošty, www atd., (např. viry v zašifrovaném souboru), pokud není samozřejmě doplněn antivirovým programem.
- Nezabrání odposlechu, modifikacím, nebo zničením dat při přenosu po síti.
- Pokud uživatel vytvoří alternativní cestu pro připojení do vnější sítě, vyřadí tak firewall z provozu. Nemusí to být přímo fyzické připojení pomocí telefonní linky (např. modemem), či bezdrátové připojení, stačí vytvořit šifrovaný spoj – „tunel“.

3.3.6 Topologie sítě a umístění firewallu

Aby mohl firewall plnit svoji úlohu, je nutné jej začlenit do existující počítačové sítě. Jeho umístění závisí na požadovaných službách, velikosti síťového provozu a v neposlední řadě i finančních možnostech vlastníka sítě.

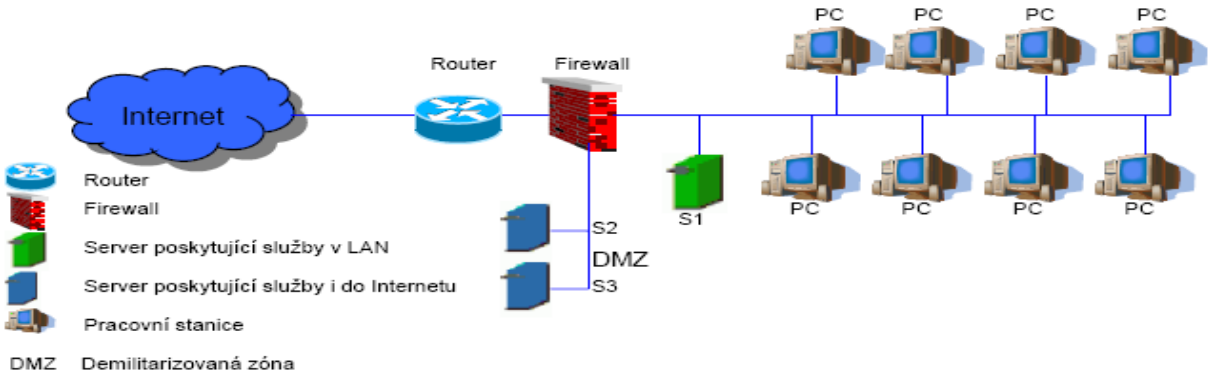
Nejjednodušším zapojením firewallu je umístit jej hned za router (firewall může plnit i funkci routeru), tedy na vstup do místní sítě. Toto zapojení je sice nejjednodušší a tím i nejméně finančně náročné, ale poskytuje nejnižší úroveň zabezpečení – lze je použít v případě, pokud na vnitřní síti není umístěn žádný server poskytující služby směrem ven, do Internetu.

Obr. 3.3: Umístění firewallu č.1



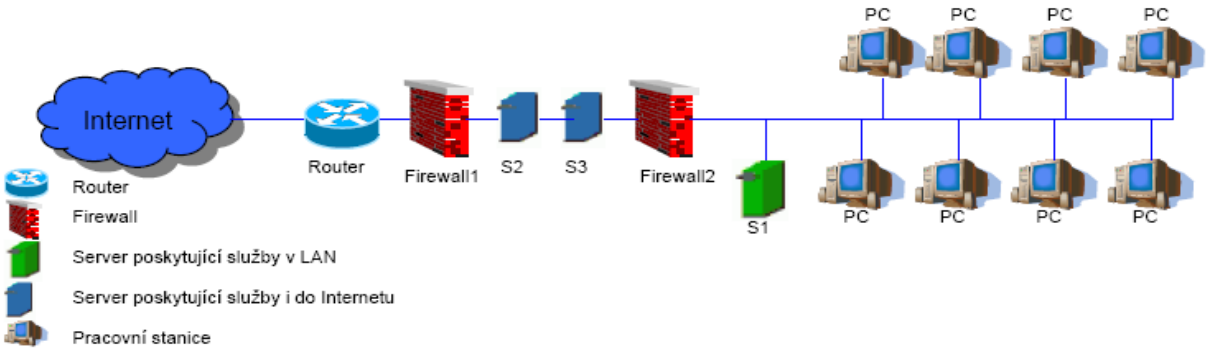
Pokud však hodláme provozovat servery dostupné i z Internetu, vhodnější variantou je vytvoření tzv. demilitarizované zóny, ve které se nachází pouze tyto servery. Nejsou již tedy součástí vnitřní sítě, jsou od ní odděleny. Toto řešení však vyžaduje aby firewall obsahoval tři síťová rozhraní. V případě, že se útočníkovi podaří napadnout firewall, získá tím přístup i do vnitřní sítě.

Obr. 3.4: Umístění firewallu č.2



Nejbezpečnějším řešením pro jednoduchou síť je vytvoření demilitarizované zóny s použitím dvou firewallů. První chrání přístup do demilitarizované zóny, druhý přístup do vnitřní sítě. Pokud se útočníkovi podaří proniknout prvním firewallem, nezíská tím automaticky i přístup do vnitřní sítě jako v předchozím případě. Nevýhodou tohoto řešení je jeho finanční náročnost (koupě a údržba dvou firewallů), zpomalení rychlosti přenosu dat a to jak mezi Internetem a vnitřní sítí, tak i vnitřní sítí a demilitarizovanou zónou.

Obr. 3.5: Umístění firewallu č.3



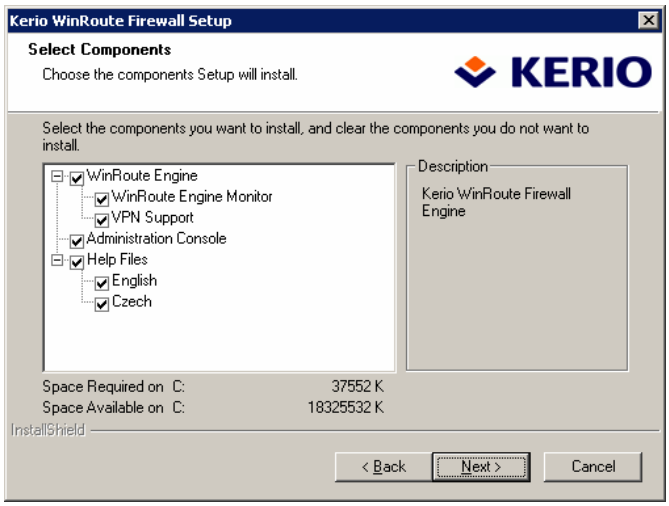
3.4 *Kerio WinRoute Firewall*

Jedním z představitelů softwarových firewallů určených pro připojení počítačových sítí malých a středních podniků, nebo organizací pracující na platformě Windows je Kerio WinRoute. V současné době je k dispozici verze 6.3, my se však zabýváme předchozí verzí 6.2. Tato verze obsahuje mimo vlastního firewallu ještě i celou řadu dalších nastavení, které zvyšují bezpečnost připojení k Internetu jako je např. Kerio VPN Server, Kerio VPN Klient, Antivirová kontrola, ISS Web Orange Filter.

3.4.1 Instalace

Požadavky na výkon počítače pro provoz WinRoute nejsou příliš vysoké, jako minimum je uváděn procesor Intel Pentium II, nebo kompaktibilní 300 MHz, 128 MB operační paměti RAM, volné místo pro instalaci 50 MB, dvě síťové rozhraní a operační systém Windows 2000, XP, nebo Server 2003. Doporučený filesystém je NTFS, neboť aplikace nastaví plná přístupová práva pouze pro Administrátora a systém. Vlastní instalace je jednoduchá, probíhá standardně jako většina programů určených pro OS Windows s možností výběru instalace: plná, minimální a vlastní, umožňující výběr instalovaných komponent.

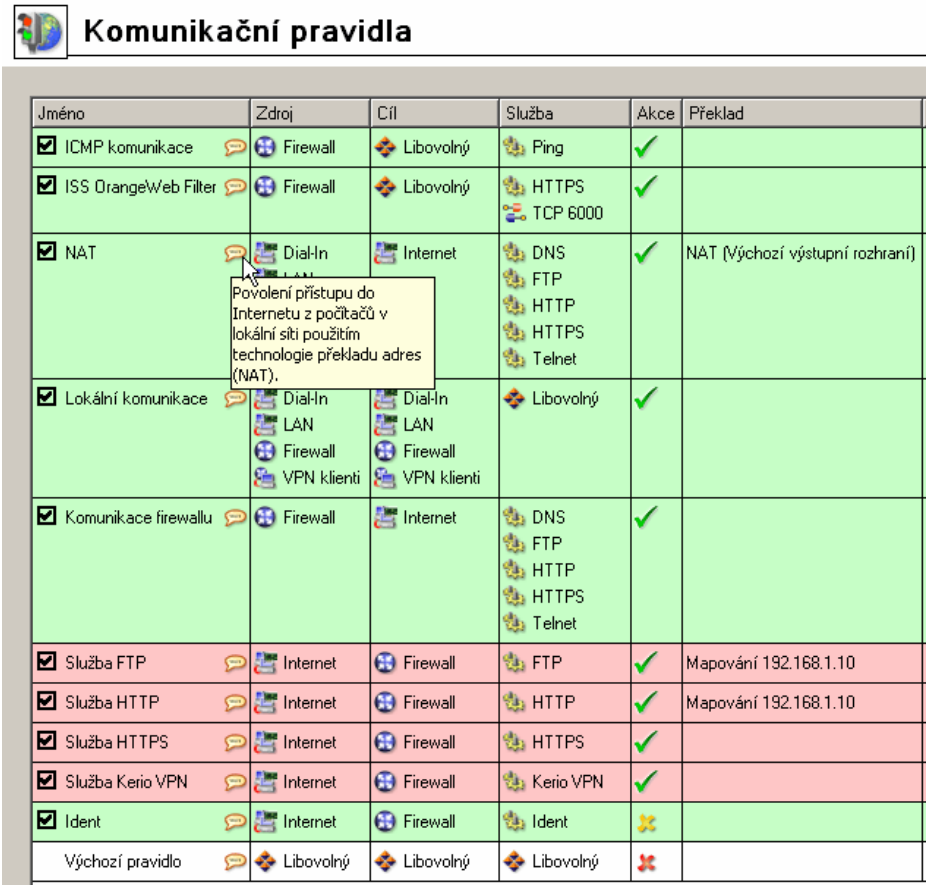
Obr. 3.6: Instalace Kerio WinRoute



Pramen: Kerio WinRoute

Po instalaci je možné si spustit průvodce nastavením komunikačních pravidel, který v osmi krocích vytvoří základní pravidla pro síťový provoz. Předně je zde třeba definovat rozhraní připojené do místní sítě a rozhraní připojené k Internetu s určením zda jde o vytáčené, nebo pevné připojení. Průvodce dále nastaví, které služby v Internetu mohou uživatelé místní sítě používat a naopak, které služby poskytované v rámci místní sítě budou přístupné i z Internetu. Důležité je i nastavení překladu adres NAT, pokud jej budeme používat, jakož i VPN od firmy Kerio. Jde samozřejmě o nastavení základních pravidel, přesnější nastavení musí být již provedeno ruční konfigurací. Tabulka s nastavenými pravidly pak může vypadat např. následovně:

Obr. 3.7: Nastavení komunikačních pravidel



Komunikační pravidla

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
ICMP komunikace	Firewall	Libovolný	Ping	✓	
ISS OrangeWeb Filter	Firewall	Libovolný	HTTPS TCP 6000	✓	
NAT	Dial-In	Internet	DNS FTP HTTP HTTPS Telnet	✓	NAT (Výchozí výstupní rozhraní)
Lokální komunikace	Dial-In LAN Firewall VPN klienti	Dial-In LAN Firewall VPN klienti	Libovolný	✓	
Komunikace firewallu	Firewall	Internet	DNS FTP HTTP HTTPS Telnet	✓	
Služba FTP	Internet	Firewall	FTP	✓	Mapování 192.168.1.10
Služba HTTP	Internet	Firewall	HTTP	✓	Mapování 192.168.1.10
Služba HTTPS	Internet	Firewall	HTTPS	✓	
Služba Kerio VPN	Internet	Firewall	Kerio VPN	✓	
Ident	Internet	Firewall	Ident	✗	
Výchozí pravidlo	Libovolný	Libovolný	Libovolný	✗	

Povolení přístupu do Internetu z počítačů v lokální síti použitím technologie překladu adres (NAT).

Pramen: Kerio WinRoute

Z předchozího obrázku je patrné, jakým způsobem se pravidla vytvářejí. Kromě jména, které je pouze označením pravidla a může být libovolné, další položky již ovlivňují proces komunikace. Zdroj označuje rozhraní, z kterého pakety přichází a cíl kam mají být odeslány, služby, na které se dané pravidlo vztahuje, jakým způsobem má být s nimi zacházeno (povolit, zakázat, zahodit) a další nastavení mapování (zde je vidět zapnutý NAT pro odchozí komunikaci celé řady služeb z místní sítě do Internetu a opačným směrem mapování http a ftp na adresu jiného serveru v místní síti). Je nutné si všimnout, že komunikace počítače s firewallem je nastavena zvlášť (má veřejné rozhraní, nepotřebuje tedy NAT), jakož i pravidel pro komunikaci v rámci místní sítě.

3.4.2 Konfigurace komunikačních pravidel

Překlad adres (NAT) provádí nahrazování zdrojových IP adres (tedy adres přidělených v rámci místní sítě) veřejnou adresou (popřípadě více veřejnými adresami), jak jsme si řekli již v předchozí části. Po obdržení odpovědi na takovýto paket WinRoute provede přeposlání na adresu z místní sítě, z níž byl požadavek odeslán. Nastavit lze překlad na adresu výstupního rozhraní, kdy WinRoute automaticky detekuje tuto IP adresu, na adresu rozhraní – výběr konkrétního rozhraní, na jehož adresu bude IP adresa paketu překládána (vhodné tam, kde se může výstupní rozhraní měnit, např. více vytáčených linek) a na konkrétní IP adresu.

Při překladu cílové adresy (označované též jako mapování portů), umožňující zpřístupnit služby běžící v místní síti uživatelům z Internetu, je možné nastavit překlad na IP adresu konkrétního počítače i překlad na jiný port (může být změněna nejen cílová adresa, ale i cílový port).

Obr. 3.8: Typické komunikační pravidlo NAT pro sdílené připojení k Internetu

Jméno	Zdroj	Cíl	Služba	Akce	Překlad
NAT	LAN	Internet	Libovolný	✓	NAT (Výchozí výstupní rozhraní)

Pramen: Kerio WinRoute

Zdroj označuje rozhraní, které je připojeno do místní sítě, cílem je veřejné rozhraní. Tyto mohou být zadány několika způsoby:

Konkrétní počítač	(název, nebo IP adresa)
Rozsah IP adres	(např. 192.168.1.20 - 192.168.1.30)
Skupina IP adres	(uživatelem nastavené)
Podsíť s maskou	(192.168.10.0/255.255.255.0)
Názvem síťového rozhraní	(zde např. LAN),
VPN	(příchozí, nebo odchozí spojení)
Jménem uživatele	(skupin uživatelů)
Firewall	vlastní PC, na němž běží firewall

Z položky Služba je patrné, že zde jsou povoleny všechny bez omezení. Ve WinRoute je definována celá řada standardních služeb (např. HTTP, FTP, DNS atd.), uživatelé si však mohou nastavit své vlastní, které poté použijí v pravidlech[5]. Služby slouží ke zpřehlednění vytvářených pravidel a usnadňují tak administrátorovi orientaci. Jde vlastně o pojmenování určitého protokolu spolu s použitými zdrojovými a cílovými porty (tedy určení aplikace, které na nich běží). Typy protokolu jsou nejčastěji TCP, nebo UDP, je však možné vybrat i jiný určený číslem protokolu v hlavičce IP paketu.

Cílový a zdrojový port je možné určit jako:

Libovolný	(všechny bez omezení)
Rovná se	(jeden konkrétní port)
Větší než/Menší než	(vyšší, nebo nižší čísla portů)
Různý od	(s výjimkou uvedeného)

[5] Seznam předdefinovaných služeb je uveden v příloze č. 3

V rozsahu	(rozsah od - do)
Seznam	(seznam portů)

Dále vidíme, že jde o pravidlo povolující komunikaci a že je použit překlad adres. Za zmínku stojí ještě možnosti prováděných akcí:

- povolit – firewall povolí komunikaci a pakety poté projdou bez omezení
- zakázat –spojení bude odmítnuto, nicméně klient obdrží o zákazu zprávu
- zahodit – používá se pro ukrytí firewallu, neboť ten neodesílá žádnou zprávu, pouze zablokuje pokus o připojení. Klient se tedy pokouší spojit tak dlouho, dokud nedojde k vyhodnocení síťové chyby.

Dosud jsem se nezmínil o jedné důležité schopnosti WinRoute a tím je použití inspekčních modulů. Inspekční modul kontroluje komunikaci příslušného aplikačního protokolu a může ji určitým způsobem upravovat (filtrovat). Příkladem může být použití inspekčního modulu HTTP monitorujícího přístup na WWW servery, kdy můžeme zakázat přístup na některé servery. Defaultně po vytvoření pravidla toto pravidlo používá vhodný inspekční modul, pokud jej však nechceme používat, musíme jej ručně vypnout.

3.4.3 Filtrování protokolů HTTP a FTP

Součástí Kerio WinRoute jsou i moduly umožňující filtrovat protokoly HTTP a FTP. Aby bylo možné tyto filtry použít, nesmí být komunikace šifrována prostřednictvím SSL (HTTPs a FTPs) a u FTP není možné použít zabezpečené přihlašování (SASO), vše samozřejmě za předpokladu povolených příslušných inspekčních modulů. Z tohoto omezení vyplývá riziko spočívající v obcházení filtrování právě pomocí zašifrovaného spojení, kdy uživatel se může připojit k proxy serveru v Internetu prostřednictvím HTTPs. Tomuto však můžeme zabránit

promyšleným nastavením pravidel zakazujících přístup k určitým serverům v Internetu právě pomocí zašifrovaného spojení.

Filtrovat WWW stránky můžeme omezováním přístupu na adresy konkrétních webových serverů, zablokováním vybraných objektů HTML jako jsou ActiveX, flash animace apod., dále můžeme na stránkách kontrolovat výskyt určitých slov a v případě jejich nalezení zakázat přístup na stránky. Pokud používáme modul ISS OrangeWeb Filter, který je sice součástí instalace firewallu avšak k jeho provozování musíme mít zakoupenou licenci, můžeme blokovat stránky i na základě jeho hodnocení.webových stránek (tento modul využívá celosvětovou databázi obsahující klasifikace WWW stránek)

Při sestavování filtru je vhodné použít následující postup. Určení uživatelů, na něž bude filtr aplikován, specifikace URL (může jít jak o jednu cílovou adresu, tak i celou skupinu adres), požadovaná akce (zde můžeme povolit, nebo zakázat přístup), můžeme stanovit i dobu, ve které se filtr použije, dále můžeme nastavit skupinu zdrojových IP adres na něž se pravidlo vztahuje (tímto ho můžeme omezit na určité počítače, bez ohledu na přihlášené uživatele) a omezení na pouze určité MIME objekty.

Vytváření pravidel pro FTP je obdobné jako pro WWW stránky, pouze kontrolovaná kritéria jsou odlišná – týkají se FTP provozu. Kromě již tedy výše zmíněných pravidel pro www stránky, můžeme filtrovat FTP provoz a zakázat přístup FTP servery omezením podle jména souboru, omezením přenosu souborů na jeden směr (např. pouze download) a blokováni určitých příkazů protokolu FTP.

3.4.4 Antivirová kontrola

WinRoute umožňuje spolupráci s antivirovými programy, které kontrolují přenos dat protokoly HTTP, FTP, SMTP a POP3 na výskyt virů. Součástí WinRoute je vestavěný antivirový program McAfee, pro jehož použití je však nutné získat platnou licenci, nebo lze použít některý z podporovaných externích programů jako jsou:

- Grisoft AVG Email Server Edition

- Symantec Antivirus Scan Engine 4.0
- Alwil avast! 4.0 for Kerio
- eTrust Antivirus, NOD32
- Sophos Antivirus
- VisNetic Antivirus Plug-in 4.

Aby bylo možné kontrolovat komunikaci antivirovým programem, musí být spuštěn příslušný inspekční modul.

3.4.5 Uživatelské účty

WinRoute umožňuje kontrolu a řízení přístupu nejen podle IP počítače, ale také na základě uživatelů a skupin. Přihlášení k firewallu a autentizace uživatelů je možná následujícími způsoby:

- ručně – zadáním do internetového prohlížeče adresy přihlašovací stránky
- přesměrováním – po zadání WWW stránky je uživatel přesměrován na přihlašovací stránku a teprve až po přihlášení se dostane na požadovanou WWW stránku
- automaticky – každému uživateli je přiřazena IP adresa počítače ze kterého se přihlašuje (nelze použít, pokud více uživatelů pracuje na jednom počítači)
- automaticky použitím NTLM – v případě, že uživatel používá doménový účet, lze nastavit jeho automatické ověření v NT, nebo Active Directory doméně (podporované prohlížeče: Microsoft IE, Mozilla, Firefox, Netscape)

Použitím účtů ve WinRoute nejenže můžeme nastavovat komunikační pravidla pro jednotlivé uživatele, ale i sledovat a vyhodnocovat jejich provoz, nastavovat kvóty objemu přenesených dat. Je možné sestavovat různé statistické přehledy, při použití ISS OrangeWeb Filter i podle

obsahu navštívených stránek (rozdělení na jednotlivé kategorie jako např. finance, zdraví, zaměstnání atd.).

3.5 Firewally pro pracovní stanice

Zatímco v předchozí části jsme se zabývali Kerio WinRoute firewallem určeným k připojení celé počítačové sítě, nyní se podíváme na některé další firewally pro zabezpečení osobního počítače opět určené pro platformu Windows.

Firewally chránící osobní počítač před útoky ze sítě (typicky z Internetu), viry a únikem dat se obvykle skládají ze čtyř modulů: Síťová bezpečnost, bezpečnost systému, detekce útoků a filtrování obsahu WWW stránek. Tyto moduly se mohou v jednotlivých programech nazývat odlišně, popřípadě i některý chybět či naopak jich může být i více (např. kontrola pošty, doplněk pro Microsoft Office). Modul síťové bezpečnosti kontroluje veškerý síťový provoz (TCP/IP) a to buď podle nastavených pravidel - IP adres, použitého protokolu, portů, nebo podle aplikací, kterým je možné povolit nebo zakázat síťovou komunikaci. Bezpečnost systému kontroluje spouštění aplikací v operačním systému. Kontroluje, zda nedošlo od posledního spuštění ke změně ve spustitelném souboru (jeho záměna), zda běžící aplikace má oprávnění spustit jinou aplikaci. Detektor útoků je schopen rozpoznat nejčastější způsoby útoků a zablokovat je. Některé firewally mají integrován systém kontroly WWW stránek podle jejich obsahu jako je blokování pop-up oken, blokování reklam, aktivního obsahu i bránění odeslání důvěrných informací.

3.5.1 Porovnání několika nejznámějších firewallů

Pro porovnání jsem si vybral pět poměrně nejrozšířenějších osobních firewallů. Snažím se o srovnání jejich možností, snadnosti nastavení ale i jejich ceny. Jsou to:

- ZoneAlarm Pro 4
- Norton Personal Firewall 2004

- McAfee Personal Firewall Plus 5.0
- Firewall integrovaný ve Windows XP.

Integrovaný firewall Windows XP

Jeho jednoznačnou výhodou je to, že je součástí operačního systému. Uživatel ho tak má k dispozici okamžitě po instalaci Windows a není tedy nutné vynakládat další prostředky na zakoupení samostatného firewallu. Dalším přínosem zejména pro méně znalé uživatele je jeho okamžité zapnutí po instalaci, zkušenější samozřejmě vědí kde jej vypnout (tito si pořídí možná některý z dále uvedených firewallů). Tento firewall je tedy určen naprostým začátečníkům jako základní minimum pro bezpečnost. To byly tedy výhody a teď se již musím zmínit o nedostatcích. Jeho největším nedostatkem je fungování pouze ve směru z Internetu do počítače tj. příchozí provoz, neumožňuje žádnou kontrolu odchozího provozu. Pokud se tedy do počítače dostane nějaký malware (např. spyware), může Vaše data odesílat naprosto volně do Internetu. Dosud jsme mluvili o firewallu integrovaném ve Windows XP, s příchodem service packu 2 došlo i ke změnám ve firewallu. Firewall kontroluje již i odchozí směr, v defaultním nastavení po instalaci je však nastavení zabezpečení v odchozím směru naprosto nedostatečné. Firewally, které jsou dále uvedeny již samozřejmě kontrolují jak příchozí, tak i odchozí směr a liší se tedy především snadností nastavení bezpečnostních pravidel a některými svými možnostmi. Vzhledem k tomu, že mezi firewally je velká konkurence, snaží se jednotlivé softwarové firmy nezaostávat a doplňují své firewally obdobnými možnostmi jako jejich soupeři. Proto u každého programu uvádím i jeho verzi, neboť lze předpokládat, že jejich možnosti se budou postupně sobě navzájem přibližovat a pro další verze již toto srovnání nemusí platit.

Zone Alarm Pro 4

Patří k nejznámějším firewallům, především jeho volně použitelná varianta (freeware pro nekomerční účely). Průvodce instalací umožňuje srozumitelné a přehledné základní nastavení,

jako je blokování pop-up oken, omezení reklamních bannerů. Ochranná opatření je možné nastavit hrubě pomocí posuvníku, nebo detailně definovat pomocí pravidel. Umožňuje nastavit pravidla pro jednotlivé programy, neobsahuje však filtr webového obsahu, pouze filtr Java/Javascript a filtr ActiveX/Cookies. Obsahuje program pro učení. Za příplatek 10 eur je možné získat verzi s „blacklistem“, což je databáze známých rozesilatelů spamu. Jeho cena je cca 50 eur.

Norton Personal Firewall 2004

Jde o firewall s jednoduchou obsluhou nabízející celou řadu funkcí podobně jako Zone Alarm Pro 4. Na rozdíl od něho však neumožňuje skenování e-mailů a neobsahuje filtr javascriptu. Také nemá žádný sebeučící program. Jeho cena je cca 50 eur.

McAfee Personal Firewall Plus 5.0

V tomto případě jde o čistý firewall, neobsahující mnoho doplňků. Nabízí blokování portů, určení pravidel pro jednotlivé programy i vyloučení konkrétních IP adres a sítí. Chybí úplně filtrování obsahu webu (Javascriptů, ActiveX, Cookies), skenování e-mailů. Cena je cca 40 eur.

Agnitum Outpost Firewall 4.0

Jde o firewall, který je ve verzi Free pro domácí použití k dispozici zdarma, má však pouze omezené vlastnosti. Placená verze 4.0 poskytuje mnohem širší nabídku služeb. Sleduje veškerý datový provoz, má filtr reklamních oken, blokuje cookies a ovládací prvky ActiveX, dokonce umí omezit přístup na některé internetové stránky pomocí seznamu filtrů. Nainstaluje se s přednastavenými pravidly, které poté může uživatel jednoduše upravit. Program se také umí učit - jakmile se některá aplikace pro kterou není dosud nastaveno žádné pravidlo pokusí komunikovat s Internetem, zeptá se, zda má být spojení povoleno či

zablokováno. Vlastní pravidla lze vytvářet s pomocí pomocníka, který na základě aktivního spojení vytvoří pravidlo.

Tab. 3.1: Shrnutí možností vybraných firewallů

Firewall	Cena Euro	Blokování POP-UP oken	Filtr Java	Filtr ActiveX	Program pro učení	Skenování emailů
Windows XP	0	Ne	Ne	Ne	Ano	Ne
Zone Alarm Pro 4	50	Ano	Ano	Ano	Ano	Ano
Norton Personal Firewall 2004	50	Ano	Ano	Ano	Ano	Ne
McAfee Personal Firewall Plus 5.0	40	Ano	Ne	Ne	Ano	Ne
Agnitum Outpost Firewall	40	Ano	Ano	Ano	Ano	Ano

V dnešní době je v oblasti bezpečnosti patrná snaha firem o vytváření komplexních programů sloužících k ochraně počítače. Jde o programy obsahující nejen firewall, ale i antivirový program, ochranu proti spyware, antispamové filtry. Většina výše uvedených společností má ve své nabídce programy, které se liší právě svými možnostmi (a samozřejmě cenou), z nichž nejvybavenější verze mají v názvu „Internet Security“.

4 Návrh malé počítačové sítě

V této části využijeme předchozích poznatků k návrhu uspořádání počítačové sítě pro malou organizaci, určení bezpečnostní politiky pro její provoz, konfiguraci jejich částí, jakož i hodnocení ekonomických nákladů.

4.1 Informace o lokalitě

Pro návrh počítačové sítě jsem si vybral organizaci působící v oblasti samosprávy a to obecní úřad. Konkrétně jde o Obecní úřad v Kněžicích (Kněžice okres Jihlava, kód obce 590843). Pro úplnost se zmiňuji o tom, že kromě Kněžic v okrese Jihlava existují i Kněžice okres Nymburk (537292) a Kněžice okres Chrudim (574007). Obec Kněžice má v současné době 1455 obyvatel, jde tedy o malou obec s malým obecním úřadem. Agenda, kterou obec vede je odpovídající obcím této velikosti. Mezi nejznámější příklady agend patří vedení matriky a další činnosti související s hospodařením obce, jako je odpadové hospodaření, poplatky ze psů atd., úplný výčet činností je uveden v příloze číslo 4. Obec zřídila dvě organizace: Obecní kino Kněžice a ZŠ Kněžice. Hlavním programem, ve kterém je vedeno hospodaření obce je informační systém od fy. Gordic. Počet počítačů potřebných k provozu obce je 12, z toho pracovních stanic je 10. Pět počítačů je určeno k provozu administrativy obecního úřadu (starosta obce + úředníci vykonávající samosprávu i státní správu v rámci přenesené působnosti) + dalších pět slouží k provozu knihovny včetně centra poskytujícího veřejné připojení k Internetu a poslední dva poskytují služby související s provozem počítačové sítě a připojení k Internetu (směrovač s firewallem, doménový controller, aplikační server + poštovní a webový server). Předpokladem pro správnou funkci služeb poskytovaných do Internetu je registrace domény 3 řádu: knezice.ji.cz (DNS záznam včetně směrování pošty). V současné době má obec registrovanou doménu knezice.com, což není vzhledem k typu koncovky com nejvhodnější. Asi nejvhodnější adresa www.knezice.cz je již bohužel obsazena (není využita žádnou ze zmiňovaných obcí, ale rekreačním zařízením Kněžická chalupa v Krkonoších, Kněžice okres Nymburk používají adresu www.obec-knezice.cz a Kněžice

okres Chrudim www.kneziceuronova.cz), nicméně lze zvolit i jiné adresy jako např. www.knezice.eu, či www.knezice.info. Poštovní server nemá v současné době žádný vlastní a využívá přihrádky knezice@iol.cz.

4.2 Síťová infrastruktura

Ještě v nedávné minulosti byla drtivá většina lokálních sítí vybudována na dvou principech: Ethernet a Token Ring - jejich základní odlišnost spočívá v politice řízení přístupu k přenosovému médiu. Zatímco TokenRing využívá řízeného přístupu, kdy v jednu chvíli může vysílat pouze jedna stanice, Ethernet o tento přístup soupeří s ostatním stanicemi (v jeden okamžik může tedy vysílat více stanic, následkem čehož dochází ke kolizím). V dnešní době je většina sítí postavena právě na Ethernetu a strukturované kabeláži. Také my při návrhu naší sítě použijeme právě Ethernet se strukturovanou kabeláží, neboť přestože pořizovací náklady jsou vyšší než u tenkého Ethernetu, jde o perspektivnější řešení. Tenký ani tlustý Ethernet se dnes již nepoužívají, setkat s nimi se můžeme maximálně v některé hodně zastaralé LAN. Pro propojení použijeme kabely UTP (Unshielded Twisted Pair) kategorie 5e. Jsou vhodné pro přenosové rychlosti 100 MBit/s, což je vzhledem k našim potřebám i ceně nejvhodnějším řešením. Kabely budou ukončeny v jednotlivých místnostech datovými zásuvkami s jedním nebo dvěma vývody RJ45 pro připojení pracovních stanic, na druhé straně v místnosti plnící funkci serverovny v datovém rozvaděči na propojovacích panelech. Jako aktivní prvky budou použity switche s přenosovou rychlostí 100Mbit/s.

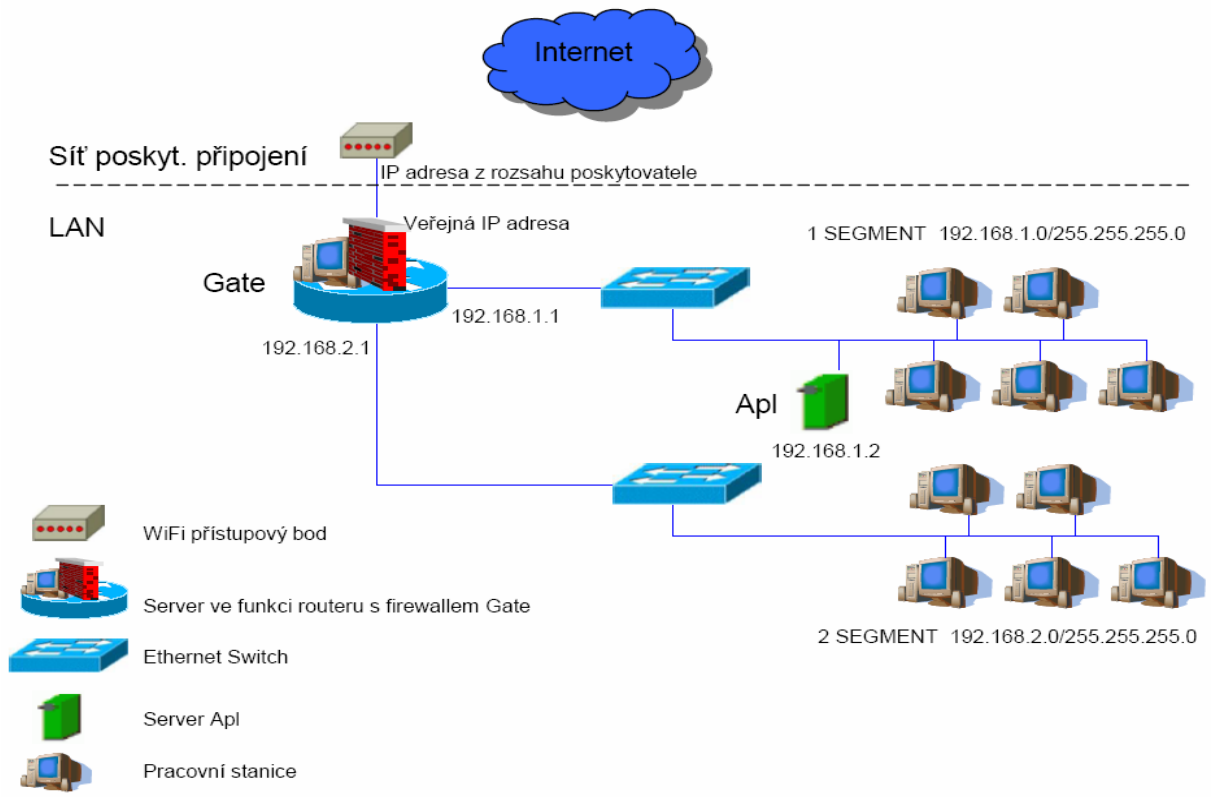
4.2.1 Logické schéma sítě

Logická struktura sítě se vztahuje k síťové vrstvě modelu ISO/OSI a zachycuje ve schématu LAN všechny klíčové prvky pro tuto vrstvu. Patří sem především aktivní prvky jako switche, huby, routery a servery. Jak je patrné z následujícího schématu, připojení místní sítě k Internetu je zajištěno bezdrátovým spojem WiFi a je chráněno proti útokům z Internetu

firewallem instalovaným na osobním počítači nazvaném gate.knezice.ji.cz, plnícím současně i roli serveru. Tento počítač má celkem tři síťová rozhraní, první slouží k připojení bezdrátového přístupového bodu a druhé dvě k připojení místní sítě skládající se ze dvou segmentů. Segment jedna 192.168.1.0/255.255.255.0 je segment důvěryhodný určený k připojení počítačů pracovníků obecního úřadu a serveru apl, segment dva 192.168.2.0/255.255.255.0 je méně důvěryhodný a slouží k připojení počítačů ve veřejné knihovně poskytujících připojení k Internetu pro veřejnost.

Bezdrátovým přístupovým bodem je OvisLink WL-5460AP 802.11g umožňující zabezpečení nejen dnes již nedostatečným WEP, ale i WPA2. Nicméně my si vytvoříme spojení šifrované pomocí IPSec (tunnel mode) z našeho serveru gate na router poskytovatele připojení.

Obr. 4.1: Logické schéma sítě



Pro lepší orientaci v návrhu zde uvedu přehled základních údajů o serverech, ačkoliv se o nich dozvíme více v další části.

Tab. 4.1: Stručný přehled serverů

Název	Operační systém	Síťové rozhraní	Poskytované služby
Server Gate	Windows Server 2003	192.168.1.1 – segment 1 192.168.2.1 – segment 2 Veřejná IP – Internet	Firewall - WinRoute, DNS, Active Directory, souborový a tiskový server
Server Apl	Fedora Core 4	192.168.1.2	Webové služby – Apache, poštovní služby - Sendmail

4.2.2 Topologie zabezpečení v této síti

V návrhu sítě je důsledně oddělen provoz pracovníků obecního úřadu od provozu sloužícího veřejnému přístupu na Internet. Tímto zajistíme jednak větší datovou propustnost na zaměstnanecké síti, ale zejména její větší bezpečnost v případě narušení bezpečnosti nebo odposlechu na síti pro veřejnost. Mezi těmito sítěmi i vstupem z Internetu je zapojen firewall. Na firewallu nastavíme pravidla pro omezení přístupu mezi těmito sítěmi, jakož i odlišné možnosti přístupu na Internet.

4.3 Síťové služby

4.3.1 DNS

V místní síti je implementován systém jmenných služeb (DNS – Domain Name Service), který umožňuje provádět rezoluci doménových jmen aktivních síťových prvků, tj. přiřazení IP adresy doménovému jménu a zpětnou rezoluci (přiřazení jména dané IP adrese).

Cit. dle [22]:

> Doménové jméno se skládá z řetězců vzájemně oddělených tečkou. Jméno se zkoumá zprava doleva. Nejvyšší instancí je tzv. root doména, která se vyjadřuje tečkou zcela vpravo (tato tečka bývá často vypouštěna). V root doméně jsou definované generické domény (*Top Level Domains – TLD*): edu, com, net, org, mil, int a arpa, které se používají převážně v USA, a

dále podle normy ISO-3166 dvojznakové domény jednotlivých států. Pro Českou republiku je vyhrazena doména cz.

Pokud počítač potřebuje zjistit potřebnou informaci z DNS serveru, nejčastěji IP adresu cílového počítače, popřípadě naopak přidělit IP adrese jméno, obrátí se na DNS server, který má v konfiguraci TCP/IP nastaven jako primární (nejčastěji místní jmenný server). Každý DNS server zná IP adresy kořenových serverů, proto se obrátí na některý z kořenových serverů majících informace o nejvyšších doménách a v ní se nacházejících serverech. Kořenové servery (v současné době je jich 13 a jsou označeny písmeny abecedy) mají přehled o všech existujících doménách nejvyšší úrovně. Požadavek na informaci je předán příslušnému DNS serveru nejvyšší domény, který jej předá níže podle domény v níž se počítač, na nějž je dotazováno, nachází. Takto se postupuje dolů jednotlivými úrovněmi stromu doménových jmen až dotaz dorazí k serveru, jenž má informaci o cílovém počítači. Tento pošle konečnou odpověď a vyhledávání je tím ukončeno.

DNS servery se při vyřizování dotazů mohou chovat dvěma způsoby:

- rekurzivní řešení dotazu - server převezme vyřizování dotazu, sám místo tazatele prochází strom doménových jmen a až najde odpověď, pošle ji tazateli. Rekurzivní přístup sice server více zatěžuje, ale jelikož jím projde odpověď, může si ji uložit do vyrovnávací paměti a poskytnout ji při příštím stejném dotazu ihned z paměti. Takto se obvykle chovají lokální servery.
- nerekurzivní řešení dotazu - server se dotazem dále nezabývá, tazateli pouze poskytne adresy dalších serverů, na něž se má obrátit pro další informace. Takto se obvykle chovají servery nejvyšší úrovně a obecně vyšších úrovní doménové hierarchie, neboť rekurzivní řešení dotazu by kapacitně nezvládli.

Pro DNS dotazy jsou používány protokoly TCP i UDP na portu 53. Dotazy, které nevyžadují přenos většího objemu dat, což jsou běžné dotazy na překlad jména na IP adresu a naopak, jsou uskutečňovány pomocí protokolu UDP (délka je omezena na 512b). Větší objemy dat jsou přenášeny pomocí protokolu TCP, což mohou být dotazy na informace o dané zóně spravované jmenným serverem – přenosy mezi primárním a sekundárním serverem. Dále se DNS používá pro zjištění poštovního serveru starajícího se o doručování v dané doméně, nadřazeného jmenného serveru, nebo k výpisu IP adres nebo jmen všech počítačů v doméně.

Systém jmenných služeb je zajišťován DNS serverem, který je nainstalován na serveru gate.knezice.ji.cz a integrován do LDAP. Jelikož místní síť není součástí Internetu (její struktura je skrytá firewallem a pouze tento je tedy viditelný z vnějšku), můžeme stanovit libovolný název domény, my ale použijeme stejný název jako má naše registrovaná doména.

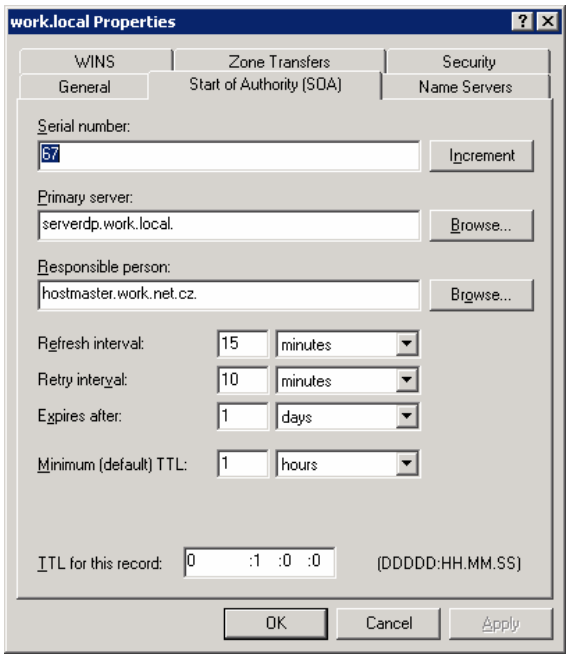
Doménové jméno: knezice.ji.cz

Dotazy v rámci místní sítě zodpovídá lokální jmenný server, s dotazy, které není schopen zodpovědět se obrací na server poskytovatele připojení. Toto zcela neodpovídá předchozímu popisu práce DNS obracejícího se na kořenové servery. Náš server totiž pracuje jako forwarding server, který bývá použit ke snížení zátěže připojení do Internetu. S rekurzivním dotazem se obrací na server poskytovatele (forwarder), který je připojen vyšší rychlostí. Ten převezme řešení dotazu (rekurzivní řešení) a odpověď pošle našemu forwarding serveru. Pokud se forwarding serveru nepodaří získat od forwardera odpověď, sám se pokusí kontaktovat root name servery . Jelikož náš DNS server bude mít povolen přístup pouze na DNS servery poskytovatele, nebude nikdy kontaktovat kořenové servery – pracuje jako slave server.

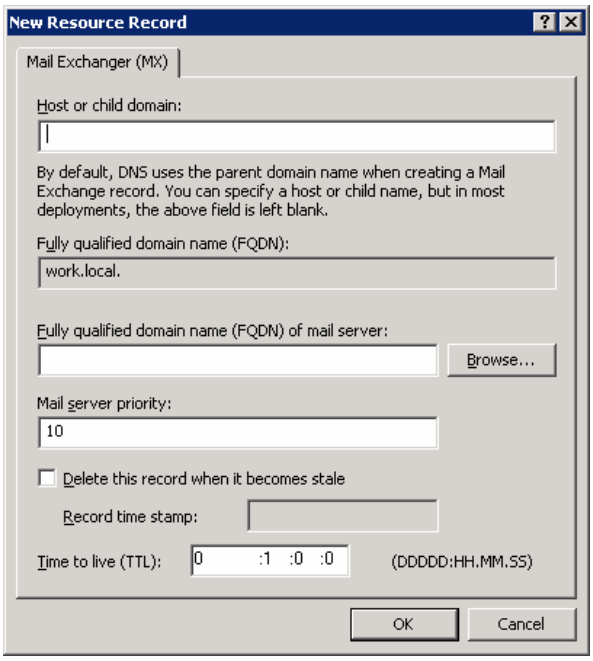
Primární jmenný server: gate.knezice.ji.cz

Po instalaci DNS serveru s nastavením „forward and reverse lookup zones“ musíme vytvořit zónu pro naši doménu. Konfigurace je obdobná jako u unixového serveru BIND, pouze s tím rozdílem, že konfigurační data nezapisujeme přímo do souboru, ale nastavujeme je přes rozhraní Windows (i v unixových systémech však existují pomocné utility pro usnadnění konfigurací).

Obr. 4.2: Vlastnosti SOA



Obr. 4.3: Přidání MX záznamu



V našem případě bude konfigurace forward zóny vypadat následovně:

```
@      IN  SOA  dns.knezice.ji.cz.  admin.gate.knezice.ji.cz. (
               200611170 - sériové číslo
               1h       - refresh
               5m       - retry
               1w       - expire
               1d       - TTL
               )
       IN  NS        dns.knezice.ji.cz.
       IN  MX  0     mail.knezice.ji.cz.

gate     IN A     192.168.1.1
apl      IN A     192.168.1.2
pc1      IN A     192.168.1.3
pc2      IN A     192.168.1.4
 .
 .
dns      IN  CNAME  gate
mail     IN  CNAME  apl
www      IN  CNAME  apl
```

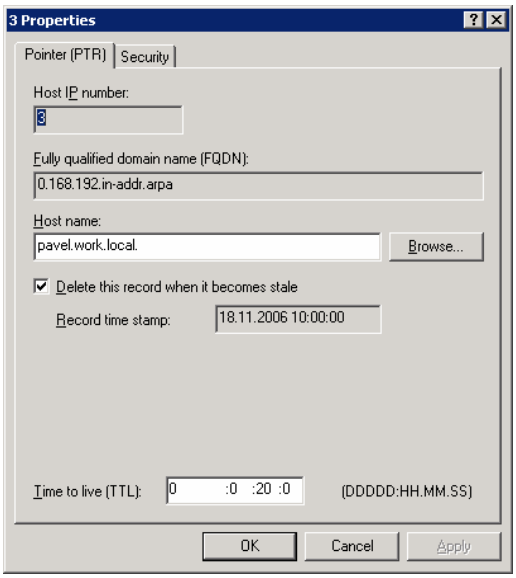
V naší konfiguraci jsou nastaveny aliasy (definice IN CNAME) i pro jednotlivé služby, což v budoucnu nám může usnadnit přesun těchto služeb na jiné servery (při rozrůstání sítě).

A konfigurace reverse zóny:

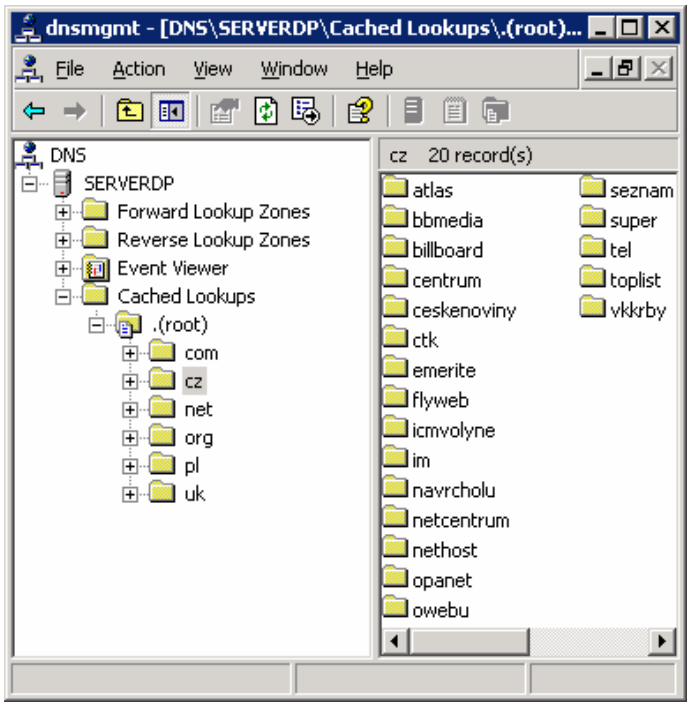
```
@      IN  SOA  dns.knezice.ji.cz.  admin.gate.knezice.ji.cz. (
            200611170 - sériové číslo
            1h      - refresh
            5m      - retry
            1w      - expire
            1d      - TTL
            )

1          IN PTR  gate.knezice.ji.cz.
2          IN PTR  apl.knezice.ji.cz.
3          IN PTR  pc1.knezice.ji.cz.
4          IN PTR  pc2.knezice.ji.cz.
```

Obr. 4.4: Přidání PTR záznamu



Obr. 4.5: Cached lookups



4.3.2 E-mail

Všichni zaměstnanci obecního úřadu mají k dispozici elektronickou poštu. Poštovní služby zajišťuje server Sendmail, který je nainstalován na serveru apl.knezice.ji.cz. Adresy uživatelů se skládají ze dvou částí oddělených znakem @, kde první část je jméno uživatele, které je jedinečné v rámci místní sítě a druhá část je identifikace obce + doménové jméno poskytovatele připojení. E-mailová adresa je ve tvaru uživatel@domena. Pro jednotlivé uživatele budou vytvořeny aliasy ve tvaru jmeno.prijmeni@domena.

E-mailová adresa: jan.novak@knezice.ji.cz

Po instalaci Sendmailu a nastavení DNS serveru bude poštovní server schopen přijímat poštu adresovanou na uživatel@apl.knezice.ji.cz. My však potřebujeme, aby přijímal poštu i pro adresy uživatel@knezice.ji.cz. Toto provedeme v souboru *sendmail.cw,* ve kterém je uveden seznam domén, pro které je poštovním serverem, přidáním nového řádku:

knezice.ji.cz

Elektronická pošta je doručována mezi poštovním serverem apl v místní doméně a poštovním serverem poskytovatele připojení prostřednictvím zabezpečeného protokolu SMTP (port995). Poštovní server zajišťuje doručování pošty v rámci místní domény, ostatní poštu posílá nadřízenému poštovnímu serveru.

Nadřízený poštovní server: poštovní server poskytovatele připojení

Poštovní server: apl.knezice.ji.cz

Předpokladem pro správné fungování pošty je v DNS záznamech poskytovatele připojení definování MX záznamu pro naši síť (poštovní server), jinak nebude zajištěno směrování pošty na náš počítač s veřejnou IP adresou. V případě, že nebude náš poštovní server dostupný, bude pošta doručena na záložní server patřící poskytovateli připojení viz. druhý MX záznam v DNS. U poskytovatele připojení budeme mít v DNS serveru vytvořenou zónu knezice.ji.cz, ve které bude pouze jeden počítač a tím bude naše brána gate.

```
IN  MX   10      gate.knezice.ji.cz.
IN  MX   50      poštovní server poskytovatele
```

```
gate    IN      A       veřejná IP adresa
www     IN CNAME        gate.knezice.ji.cz.
```

V našem případě máme registrovanou doménu knezice.ji.cz jako doménu nižšího řádu u našeho poskytovatele připojení a využíváme jeho jmenné a poštovní servery. Toto však není pravidlem, můžeme si registrovat doménu 2. řádu např. „knezice.cz“ (tato doména je již však obsazená) a využívat libovolné DNS a poštovní servery. Obec Kněžice, jak jsem se již zmínil v úvodu, používá doménu knezice.com, což není zrovna nejvhodnější vzhledem k určení (a obecnému povědomí) této koncovky.

4.3.3 WWW služby

Na aplikačním serveru apl.knezice.local bude nainstalován webový server Apache, který bude poskytovat své služby nejen v rámci místní sítě, ale i do Internetu. Komunikace mezi klientem a serverem se děje fyzicky na bázi TCP/IP protokolu, aplikačně pak pomocí HTTP protokolu. Klient kontaktuje http server a zašle mu dotaz nebo informační odkaz a dostane odpověď. A právě jak dotazy, tak i odkazy a odpovědi mohou být možným zdrojem nebezpečí. Útočníci často využívají nedostatků v zabezpečení, nebo chyb v programech. Navrácený dokument (odpověď) může obsahovat formátovací přepínače, které explicitně říkají, jaký program má být pro prohlížení dokumentu vyvolán. Toho například využívá i standard MIME. Důvěra k navrácenému dokumentu tak může vést k napadení klienta.

Webový server může být napaden dotazy a odkazy. Pokud server spouští na zpracování dotazu nějaký lokální program, je nutné tyto parametry ošetřit před neočekávanými hodnotami (ať již zadanými úmyslně či nedopatřením). Tímto způsobem může útočník spustit na serveru jiný lokální program, který mu umožní získat data, popřípadě zajistit přístup na server.

Adresa WWW serveru: www.knezice.ji.cz

4.3.4 Sdílení souborů a tiskáren

Uživatelské složky s jejich dokumenty jsou umístěny na serveru gate.knezice.ji.cz a veškerá data v nich jsou šifrována pomocí systému EFS. Každému uživateli se již při spuštění počítače připojí automaticky jeho složka a on s ní pracuje stejně, jako by data byla umístěna na místním disku. Uživatel se dostane pouze na své dokumenty. Kromě těchto osobních složek jsou zde umístěna i data, které musí být přístupné všem pracovníkům obecního úřadu. Tyto se nachází ve společném adresáři, do kterého mají všichni pracovníci přístup a jsou rovněž šifrovány pomocí EFS, jako příjemce však není uveden pouze jeden člověk, ale celá skupina oprávněných uživatelů. Na serveru je rovněž umístěna tisková fronta pro společnou síťovou tiskárnu.

4.3.5 Směrování

Směrování mezi místní sítí a Internetem, jakož i mezi segmenty místní sítě zajišťuje server gate.knezice.local s nainstalovaným firewallem, v jehož rozhraních končí všechny síťové segmenty. Žádný jiný počítač v místní síti se směrování neúčastní, všechny počítače mají pouze nastavenou implicitní cestu, která ukazuje na adresu rozhraní směrovače do daného segmentu.

4.4 Server gate.knezice.ji.cz

Operačním systémem použitým na tomto serveru je Microsoft Windows Server 2003 Standard Edition, který je nainstalován a nakonfigurován pro plnění role doménového kontrolleru (Active Directory), DNS serveru, souborového a tiskového serveru. Veškerá komunikace mezi serverem a ostatními pracovními stanicemi je zabezpečena pomocí IPSec. Server plní také úlohu brány pro přístup do Internetu a směruje pakety mezi oběma lokálními segmenty a Internetem. Na serveru je nainstalován firewall WinRoute verze 6.2, o jehož možnostech jsem se zmiňoval v předchozích částech a jenž chrání místní síť proti útokům zvenku z Internetu.

Právě z tohoto důvodu je třeba věnovat jeho zabezpečení velkou pozornost, neboť nejenže jsou na něm umístěna důležitá data, ale pokud se útočníkovi podaří do něj úspěšně proniknout, otevírá se mu cesta do místní sítě. Dále se tedy budeme zabývat nastavením firewallu chránícího celou naši síť.

4.4.1 Konfigurace komunikačních pravidel

Při definování jednotlivých pravidel budeme vycházet ze zásady, co není povoleno je zakázáno – jde o použití restriktivní politiky jak jsme si řekli již na začátku. Důležité je i stanovit správné pořadí pravidel, neboť tyto jsou vyhodnocovány odshora dolů, tedy tak, že se provede první příkaz odpovídající konkrétnímu komunikačnímu požadavku. Těmito pravidly oddělíme nejen provoz mezi místní sítí a Internetem, ale i mezi oběma segmenty místní sítě. V programu Kerio WinRoute si ještě vytvoříme dvě skupiny, které použijeme při nastavení firewallu. Skupinu Pracovníci, do které zařadíme všechny zaměstnance obecního úřadu a skupinu Knihovna pro možnost nastavení oprávnění i pro počítače v knihovně.

Tab. 4.2: Nastavení komunikačních pravidel Kerio WinRoute

	Jméno	Zdroj	Cíl	Služba	Akce	Překlad
1.	Lokální komunikace v důvěryhodné síti	Segment 1 Firewall	Firewall Segment 1	libovolná	Povolit	
2.	Lokální komunikace v přístupné síti	Segment 2 Firewall	Firewall Segment 2	LDAP, LDAPs, DNS, PING, IPSec, IKE, Kerberos, Microsoft-DS	Povolit	

3.	Komunikace mezi oběma segmenty	Segment 1 Segment 2	Segment 2 Segment 1	HTTP, HTTPs, PING	Povolit	
4.	DNS	Firewall	DNS poskyt	DNS	Povolit	
5.	Komunikace Firewallu	Firewall	Internet	FTP, HTTP, HTTPs, PING	Povolit	
6.	Odesílání pošty	Apl	mt*	SMTPs	Povolit	NAT
7.	WWW bez ověření	Segment1 Segment2	Internet	HTTP	Povolit	NAT
8.	NAT	Pracovníci Knihovna	Internet	HTTP, HTTPs, FTP	Povolit	NAT
9.	Mapování portů	Internet	Firewall	HTTP, SMTP HTTPs	Povolit	mapov. na 192.168.1.2
10.	Ireny	Internet	Firewall	Ident	Block	
11.	Výchozí pravidlo	libovolný	libovolný	libovolný	Drop	

mt* - nadřízený poštovní server poskytovatele připojení

1. V prvním pravidle povolujeme provoz bez omezení mezi segmentem jedna a firewallem, tj. žádný síťový provoz zde není blokován.
2. Provoz mezi segmentem dva a firewallem je omezen pouze na služby LDAP, LDAPs, DNS, PING, IPSec, IKE, Kerberos a Microsoft-DS. Omezení přístupu z segmentu dva je vytvořeno z důvodu vyšší bezpečnosti, neboť tyto počítače používají různí anonymní uživatelé k přístupu na Internet ve veřejné knihovně, přičemž jde o relativně samostatnou skupinu PC a plný přístup do sítě zaměstnanců by byl zbytečný a pouze

by zvyšoval bezpečnostní rizika. Zrovna tak není povolen ani protokol NetBios,takže počítače z tohoto segmentu nebudou moci prohlížet okolní síť. Všemi těmito službami (resp. protokoly) jsme se zabývali již v úvodní časti, snad jen pro připomenutí: IPSec -protokol umožňující vytvořit zabezpečené spojení na síťové vrstvě a s ním související IKE zajišťující dynamickou výměnu kryptografických klíčů, systém Kerberos sloužící k autentizaci uživatele a Microsoft-DS, což je vlastně pouze jiné označení pro SMB/CIFS (sdílení souborů a tiskáren).

3. Zde nastavujeme pravidla pro komunikaci mezi oběma segmenty navzájem. Vzhledem k tomu, že uživatelé ze segmentu dva přistupují na webový server umístěný v segmentu jedna, je třeba povolit protokol HTTP a HTTPs. Pro testovací účely je povolen i PING..
4. S dotazy na jmenný server se pracovní stanice nesmí obracet přímo na jmenné servery v Internetu, ale na DNS server v místní síti, který se teprve sám dotáže serveru (serverů) poskytovatele, ostatní adresy jsou blokovány.
5. Dále definujeme pravidla pro přístup do Internetu přímo z Firewallu (zde není nutné provádět NAT) protokoly FTP, HTTP, HTTPs a PING..
6. Tímto pravidlem povolujeme odesílání pošty ze serveru Apl pouze nadřízenému poštovnímu serveru poskytovatele.
7. Další dvě pravidla souvisí s přístupem uživatelů na Internet a prováděním překladu zdrojových adres. Na první pohled by se mohlo zdát, že pravidla jsou duplicitní. První povoluje provoz HTTP bez omezení z obou segmentů místní sítě.
8. Druhé pravidlo povolí HTTP spolu s HTTPs a FTP pro naši skupinu Pracovníci a Knihovna. Tímto způsobem je zajištěna možnost automatického ověřování uživatelů na firewallu. Automatické ověření totiž probíhá až v okamžiku navazování spojení do Internetu. Pokud bychom tedy použili pouze druhé z pravidel, přístup na Internet by byl povolen jen již ověřeným uživatelům (tedy těm, kteří si prvně do prohlížeče ručně zadali www stránku pro ověření a až poté pokračují na Internet). Přidáním prvního

pravidla tedy umožníme automatické přihlašování přes Active Directory (viz uživatelské účty v předchozí části). Nesmíme však zapomenout v části Pravidla pro HTTP (záložka Pravidla pro URL) zakázat přístup uživatelům ke všem objektům a povolit jej pouze pro skupinu Pracovníci a Knihovna. Cílem tohoto vynuceného přihlášení je možnost analyzovat provoz a případně zavést další omezení pro konkrétní uživatele.

9. Zde zpřístupníme náš webový a poštovní server z Internetu, neboť povolujeme přístup na firewall pro HTTP, HTTPs, SMTPs a provádíme překlad cílové adresy na adresu našeho místního serveru Apl.
10. Některé programy používají službu AUTH (identd) ke zjištění, jakému uživateli patří příchozí spojení. Protože může poskytovat útočníkovi nežádoucí údaje, není dobré ji všem zpřístupnit. Ovšem pokud ji běžným způsobem zablokujeme (DROP), také to není dobře, neboť některé programy (např. SMTP servery) ji mohou využívat v rámci užitečného provozu. Pokud ji tedy budeme filtrovat, může docházet ke značnému zpomalení komunikace, když bude protistrana čekat na vypršení času vyhrazeného k vyřízení AUTH požadavku. Řešením je požadavek nikoliv „zahodit“, ale „odmítnout“.
11. A na konec zablokujeme veškerý síťový provoz, takže pakety, které nevyhoví žádnému předchozímu pravidlu firewall nepropustí.

4.4.2 Konfigurace filtrování protokolu HTTP

Další významnou možností zvyšující bezpečnost místní sítě je nastavení oprávnění uživatelům k přístupu k webovým serverům v Internetu. Častým zdrojem malware jsou právě servery nabízející buď erotický, nebo nejrůznější nelegální obsah jako jsou různé cracky umožňující obcházet zabezpečovací mechanizmus a zprovozňující software bez patřičné licence. Ve WinRoute můžeme přístup filtrovat jak podle pravidel, jejichž URL vyhovují určitým kritériím, tak i podle slov vyskytujících se na příslušné stránce. Mezi další možnosti patří i blokování určitých prvků WWW stránek (skripty), nebo vypnutí antivirové kontroly

pro určité stránky (firewall provádí antivirovou kontrolu- soubory si ukládá dočasně na disk a v případě nalezení viru soubor smaže). V našem případě nepoužijeme pro filtrování přístupů modul ISS Orange Filter používající mezinárodní databázi pro kategorizaci stránek, neboť tento vyžaduje zvláštní licenci.

4.4.2.1 Filtrování podle URL

Také při vyhodnocování těchto pravidel je postupováno odshora dolů, přičemž vyhodnocování se zastaví na prvním pravidle, které splňuje podmínky pro URL. Pokud budeme chtít zakázat přístup na všechny stránky, které neodpovídají nám nastaveným povolujícím pravidlům, musíme na poslední místo přidat pravidlo blokující vše. Po instalaci je však tento filtr nastaven tak, že vše je povoleno a blokovat budeme pouze přístup podle námi definovaných zakazujících pravidel. Tento způsob nastavení považuji za vhodnější, neboť povolit pouze určité stránky podle pravidel je příliš omezující.

V záložce Pravidla pro URL jsou vidět následující sloupce: Popis, akce, podmínka, vlastnosti. Popis obsahuje stručný popis pravidla včetně políčka umožňujícího zrušením zatržení vypnout pravidlo. Akce nastaví činnost, která má být provedena, na výběr máme následující možnosti: Povolit, zakázat, zahodit a přesměrovat na stránku pokud je splněna určitá podmínka. Poslední položka upřesňuje volby v pravidle, jako je antivirová ochrana, zakázaná slova.

Dále můžeme ještě upřesnit časovou platnost, skupinu IP adres, nebo uživatele pro které podmínka platí.

V našem případě budeme chtít zakázat přístup na webové freemailové servery pro zaměstnance obecního úřadu, neboť nadměrný poštovní provoz zbytečně zatěžuje síť a pro služební účely mají pracovníci vlastní poštovní přihrádky na poštovním serveru Apl. Ačkoliv by se toto mohlo na první pohled zdát zbytečné, provoz na freemailové servery tvoří významnou část celkového síťového provozu zejména u větších organizací, proto například Finanční ředitelství v Brně blokuje tento přístup v síti FINet pro pod něj spadající finanční

úřady. Zde využijeme již předem připravené skupiny Pracovníci a Knihovna. Na záložce Skupiny URL si dále vytvoříme skupinu nazvanou Freemail. Do této skupiny zařadíme podmínku, že URL obsahuje slovo mail, nebo posta (*mail*, *posta*). V nastavení pravidla poté již uvedeme:

Tab. 4.3: Filtrování podle URL

Popis	Akce	Podmínka	Seznam uživatelů
Freemailové servery	Přesměrovat	objekty ze skupiny Freemail	Pracovníci
Povolení přístupu	Povolit	všechny objekty	Pracovníci, Knihovna
Blokování přístupu	Zakázat	všechny objekty	

Jednotliví uživatelé z řad zaměstnanců obecního úřadu jsou zahrnuti do skupiny Pracovníci. Pokud se pokusí navštívit freemailový server (v URL uvedeno mail, nebo freemail) jsou přesměrováni na místní webovou stránku obsahující upozornění o zákazu přístupu. Další dvě pravidla vyplývají jak již bylo výše uvedeno z nastavení přístupu do Internetu pouze pro ověřené uživatele. Uživatel Knihovna je univerzální uživatel pro přístup z počítačů umístěných v knihovně pro anonymní uživatele. Tento uživatel nemá také blokován přístup přes web na freemailové poštovní servery, neboť pro ně neexistují na místním poštovním serveru poštovní přihrádky, jakož i odesílání přes SMTP server z tohoto nedůvěryhodného segmentu je zakázáno.

4.4.2.2 Filtrování podle zakázaných slov

Ve WinRoute je také možné hodnotit www stránky podle slov, které se na nich vyskytují. Po instalaci jsou vytvořeny dvě základní skupiny obsahující slova z kategorie Pornography a Warez/Cracks, přičemž každý si může samozřejmě vytvořit další vlastní skupiny. Zařazení slov do skupin nemá vliv na vyhodnocení, slouží spíše administrátorovi ke snazší orientaci.

Hodnocení probíhá tak, že při načítání webové stránky je na ní prováděno vyhledávání předdefinovaných slov. Pokud je takové slovo nalezeno, potom se zvýší hodnota o sumu, která je danému slovu přiřazena (i když se vyskytne na stránce vícekrát, vždy je započteno pouze jednou). Tuto sumu, zde nazývanou „váha“ můžeme sami přidělit jednotlivým výrazům. Po vyhledání všech zakázaných slov na stránce a zjištění celkového součtu jim přiřazených hodnot, dojde k porovnání této sumy s předdefinovanou tzv. prahovou hodnotou (typicky je nastavena na 70, ale opět je možné zvolit vlastní). Pokud je tato suma vyšší, dojde k zablokování přístupu na stránku. Nesmíme ovšem zapomenout toto nastavit v pravidlech pro URL.

V našem případě kromě již předdefinovaných a zablokovaných skupin budeme chtít blokovat i přístup na stránky zabývající se hazardními hrami. Proto si vytvoříme v Zakázaných slovech skupinu Hazardní hry a do ní přidáme následující slova: Vysoká výhra váha 25, riskuj 10, sazka 20, sportka 20, nabídka kurzů 30, casino 50, hazardní hry online 50, sázení po internetu 50. Další typická slovní spojení nám pomůže zjistit vyhodnocování Internetového provozu. Jelikož tuto metodu zakázaných slov můžeme považovat pouze za pomocnou, v praxi ji budeme muset zkombinovat s blokováním podle pravidel URL. Blokovat budeme jistě adresy jako je např. www.sazeni-po-internetu.cz, www.sazka.cz, www.ifortuna.cz.

4.5 Server apl.knezice.ji.cz

Server Apl je postaven na Linuxové distribuci Fedora Core 4. Jeho úkolem je poskytovat poštovní a webové služby. Poštovní služby zajišťuje pro pracovníky obecního úřadu program Sendmail, webové služby jsou dostupné nejen z místní sítě, ale i z Internetu o což se stará program Apache.

Server je fyzicky připojen do switche na němž je vytvořen segment jedna. Pro jeho zprovoznění je třeba ještě nakonfigurovat síťové rozhraní, tedy přidělit příslušné adresy a hodnoty síťovému zařízení. Nejčastěji se toto provádí příkazem ifconfig. V našem případě použijeme příkaz:

```
# ifconfig eth0 192.168.1.2 netmask 255.255.255.0 up
```

Dále musíme nastavit směrování tak, aby veškeré datagramy pro hostitele s adresou 192.168.1.* byly odeslány na rozhraní eth0:

```
# route add –net 192.168.1.0 netmask 255.255.255.0 eth0
```

Ještě zbývá nastavit tzv. defaultní bránu, tj. adresu zařízení, na které se mají odeslat pakety, které nelze doručit v rámci daného segment (vše ostatní pošli na adresu ……)

```
# route add default gw 192.168.1.1 eth0
```

Pokud uvedeme názvy sítí v souboru /etc/networks a hostitelů v /etc/hosts můžeme místo IP adresy použít tento název (v hosts nastavíme minimálně zpětnovazební rozhraní).

4.5.1 Filtrovací pravidla

K vyšší míře zabezpečení přispěje zprovoznění firewallu i na serveru Apl a nastavení následujících pravidel:

	Action	src	port	dst	port	flags	poznámka
1.	Allow	127.0.0.1	*	*	*	*	povolit vše pro zpětnovazeb. roz.
2.	Allow	192.168.1.3	*	apl	ssh	TCP	admin. přístup k serveru
3.	Allow	*	*	apl	http	TCP	přístup na web server
4.	allow	*	*	apl	https	TCP	zabezp. přístup na web server
5.	allow	192.168.1.0	*	apl	SMTPs	TCP	poštu přijímat z 1. segmentu
6.	allow	*	*	apl	SMTP	TCP	příjem pošty
7.	allow	192.168.1.0	*	apl	POP3s	TCP	výběr pošty z 1. segmentu
8.	allow	192.168.1.2	*	*	SMTPs	TCP	odesílání pošty do Internetu
9.	allow	192.168.1.0	*	apl		ICMP	omezeno na typ 8 (Echo request)

10.	allow	192.168.2.0	*	apl		ICMP	omezeno na typ 8 (Echo request)
11.	allow	apl	*	ms*		ICMP	omezeno na typ 0 (Echo reply)
12.	allow	192.168.1.2	*	*		ICMP	omezeno na typ 8 (Echo request)
13.	allow	*	*	apl		ICMP	omezeno na typ 0, 3, 11
14.	allow	192.168.1.2	*	gate	DNS	UDP	dotazy na jmenný server gate
15.	log	*	*	apl	*	*	logování všech příchoz. paketů
16.	block	*	*	*	*	*	vše zablokováno

ms* - místní segmenty (segment jedna + dva)

4.5.2 Nastavení filtrovacích pravidel

Konfigurace našeho serveru je zjednodušená tím, že má pouze jedno ethernetové rozhraní připojené do místní sítě a nezajišťuje žádné směrování mezi sítěmi. Při stanovení těchto pravidel postupujeme tak, že vše zakážeme a povolíme dostupnost pouze námi požadovaných služeb.

1. Prvním pravidlem povolujeme vše pro zpětnovazební rozhraní Io. Toto je vyžadováno pro správnou funkci celé řady programů.
2. Dále povolujeme přístup na server prostřednictvím ssh pouze z počítače administrátora (z IP adresy 192.168.1.3).
3. Zde povolujeme přístup na webový server nezabezpečeným protokolem http jak z místní sítě, tak i z Internetu.
4. Povolíme přístup na webový server i zabezpečeným protokolem https opět jak z místní sítě, tak i z Internetu (Předpokladem je konfigurace Apache, který toto umožní).
5. Další pravidlo se týká zabezpečení poštovního provozu, neboť povoluje přijímat poštu k odeslání zabezpečeným protokolem smtp pouze z prvního segmentu (kde jsou připojeny PC pracovníků obecního úřadu).

6. Příjem pošty bez omezení. Jelikož na serveru gate jsou nastavena pravidla blokující přístup SMTP z druhého segmentu, bude možný přístup ze segmentu 1 a z Internetu. Je důležité nastavit v serveru Sendmail omezení pro odesílanou poštu pouze z místní domény.
7. Pouze z prvního segmentu je povoleno stahovat zprávy prostřednictvím POP3s na místní pracovní stanice.
8. Pošta ze serveru apl je odesílána bez omezení cíle. Její další omezení je provedeno až na serveru Gate povolením pouze nadřízeného poštovního serveru poskytovatele připojení, který zabezpečí další rozeslání.
9. Pro kontrolní účely je povolen i protokol ICMP a to pouze typ 8 (Echo Request tzv. PING) a to ze segmentu jedna.
10. Stejně tak je povolen i protokol ICMP typ 8 ze segmentu dva.
11. Aby se počítače ze segmentu jedna a dva dozvěděli o úspěšnosti svého požadavku, je povoleno odeslání odpovědi (Echo reply) do těchto segmentů.
12. Abychom se mohli přesvědčit o dostupnosti okolních počítačů ze serveru Apl, je povolen ICMP typ 8 (Echo request) bez omezení určení (destination).
13. Povolení přijetí odpovědi na náš požadavek - typ 0 (Echo reply), 11 (Time exceeded) a 3 (Destination unreachable).
14. Dotazy na jmenný server jsou povoleny pouze na server Gate.
15. Předposledním pravidlem nastavujeme logování příchozích paketů i těch odmítnutých, z důvodu možnosti diagnostiky případných problémů.
16. Posledním pravidlem blokujeme veškerý příchozí i odchozí provoz.

Pro nastavení výše uvedených pravidel použijeme nástroj iptables (použijeme novější metodu iptables oproti starší ipchains). Program voláme s několika parametry:

Prvním je místo určení, kam chceme pravidlo zařadit (-A INPUT, -A OUTPUT), dále definujeme vlastní pravidlo:

-p	protokol
-i	rozhraní kterým byly pakety přijaty
-s	IP adresa odesílatele
--sport	zdrojový port
-d	cílová IP adresa
--dport	cílový port a jak má být s paketem naloženo
-j Drop	zahodit
-j ACCEPT	propustit
-j REJECT	paket zahozen, ale odesílatel informován chybovým hlášením ICMP
-j LOG	záhlaví paketu je zapsáno do systémového logu.

Zde jsme si ukázali pouze základní možnosti nastavení dostačující pro naše použití, program má ještě celou řadu dalších parametrů, o kterých je možné se dozvědět více v manuálu. Jednoduchý příklad pravidla:

```
iptables –A INPUT –i eth0 –p TCP –s 192.168.2.5 –sport 3000 –d 192.168.1.2
–dport 25 –j DROP
```

Pokud se v řetězci INPUT objeví TCP segment, který přišel na počítač přes rozhraní eth0, jeho odesílatelem bude 192.168.2.5 port 3000 a příjemcem port 25 adresy 192.168.1.2, tak jej nepouštěj.

Ještě se musím zmínit o parametru –P, kterým naše nastavování začínáme. Umožňuje změnit policy vestavěného chainu - v našem případě použité INPUT a OUTPUT (uživatelské chainy policy nemají). Pokud příchozí pakety nevyhoví žádnému pravidlu, použije se policy.

Konkrétní nastavení našich pravidel pak bude vypadat následovně:

```
1.   iptables –A INPUT –s 127.0.0.1 –j ACCEPT
     iptables –A OUTPUT -d 127.0.0.1 -j ACCEPT
2.   iptables –A INPUT –p TCP –s 192.168.1.3 –dport 22 –j ACCEPT
3.   iptables –A INPUT –p TCP –dport 80 –j ACCEPT
4.   iptables –A INPUT –p TCP –dport 443 –j ACCEPT
5.   iptables –A INPUT –p TCP –s 192.168.1.0 –dport 995 –j ACCEPT
6.   iptables –A INPUT –p TCP –dport 25 –j Accept
7.   iptables –A INPUT –p TCP –s 192.168.1.0 –dport 465 –j ACCEPT
8.   iptables –A OUTPUT –p TCP –dport 995 –j ACCEPT
9.   iptables –A INPUT –p ICMP –s 192.168.1.0 –icmp-type 8 –j ACCEPT
10.  iptables –A INPUT –p ICMP –s 192.168.2.0 –icmp-type 8 –j ACCEPT
11.  iptables –A OUTPUT –p ICMP –d 192.168.1.0 –icmp-type 0 –j ACCEPT
     iptables –A OUTPUT –p ICMP –d 192.168.2.0 –icmp-type 0 –j ACCEPT
12.  iptables –A OUTPUT –p ICMP –s 192.168.1.2 –icmp-type 8 –j ACCEPT
13.  iptables –A INPUT –p ICMP –d 192.168.1.2 –icmp-type 0 –j ACCEPT
     iptables –A INPUT –p ICMP –d 192.168.1.2 –icmp-type 11 –j ACCEPT
     iptables –A INPUT –p ICMP –d 192.168.1.2 –icmp-type 3 –j ACCEPT
14.  iptables –A OUTPUT –p UDP –d 192.168.1.1 –dport 53 –j ACCEPT
15.  iptables –A INPUT –j LOG
16.  iptables –P INPUT DROP
     iptables –P OUTPUT DROP
```

Pro kontrolu, že jsme zadali naše pravidla správně se můžeme přesvědčit výpisem chainů. Toto nám umožní parametr –L, popřípadě můžeme všechny pravidla v chainu zrušit parametrem –F.

4.6 Bezpečnost a uživatelé

Dosud jsme se otázkou bezpečnosti zabývali spíše z pohledu celé počítačové sítě (pohled správců informačního systému). Neméně zajímavé je však i hledisko jednotlivých uživatelů. Zde je třeba zdůraznit jejich zodpovědnost za bezproblémové a bezpečné provozování počítačů.

Centrem bezpečnosti v operačním systému Windows XP je Centrum zabezpečení. Zde můžeme nastavit možnosti internetu, automatické aktualizace, nastavení firewallu. Dále hlídá i použití antivirového programu a varuje nás před zastaralostí virových definic, popřípadě nepřítomností antiviru. Kromě všech těchto základních programů je vhodné použít i specializovaný program pro odhalování spyware. Kromě nastavení automatických aktualizací počítače je tedy nutné vždy používat minimálně následující trojici programů: firewall, antivirový program a program pro odhalování spyware. Toto však neznamená, že na počítači musí být nainstalován pouze jeden program, jako zástupce každé z těchto skupin (tj. pouze 3 programy). Některé programy integrují funkci firewallu a antiviru a zrovna tak lze použít současně i více programů odhalujících spyware. Toto řešení lze považovat za vhodnější, neboť žádný program není 100% spolehlivý, proto lze tímto zdvojením zvýšit bezpečnost počítače. Zatímco u detektorů spyware lze použít více programů současně, firewall bude pouze jeden. Pokud bychom totiž použili dvou, pouze bychom zvýšili složitost konfigurace (při opomenutí nastavení jednoho z nich by spojení nefungovalo) a naopak zvýšili riziko napadení tím, že i firewally mohou mít svoje bezpečnostní „díry“, nehledě na vyšší nároky na výkon počítače.

Nastavením firewallu jsme se již zabývali při zabezpečení celé počítačové sítě. Lze říci, že tyto pravidla byly nastaveny poměrně přísně, ale pro běžnou práci by neměly být omezením. Jelikož naše síť je určena pro provoz na Obecním úřadu (tedy pracovní provoz), je zbytečné povolovat některé další služby jako je např. Skype, P2P sítě, nebo ICQ. Jejich povolením bychom snížili bezpečnost LAN a to zejména u ICQ, kdy bývá celá řada virů šířena právě pomocí datových příloh (o sítích pro instant messaging bývá často hovořeno jako o „dírách do systému“). V případě nutnosti použití ICQ lze použít klienta ICQ umístěného na Internetu a

dostupného přes webové rozhraní, neboť protokol http (i https není blokován). Lze ovšem zvolit i jiné řešení, kdy přístup pomocí ICQ (popřípadě i jiného instant messageru) povolíme na firewallu pouze určenému klientu.

Asi nejdůležitější věcí, která uživatele zajímá, je bezpečnost vlastních dat a ochrana před jejich ztrátou. Většinou jim nedělá starosti ani tak zcizení dat, jako spíše možnost jejich zničení. A v praxi k tomu opravdu často dochází. Nejčastější příčinou ztráty, nebo poškození dat jsou kromě samotného uživatele, softwarové, nebo hardwarové problémy. I když i u těchto příčin můžeme často nalézt v pozadí zavinění uživatele.

4.6.1 Hardwarové příčiny ztráty dat

Pokud dojde k hardwarové poruše, závisí na součásti, která je poškozena. Z hlediska ztráty dat jsou nejnebezpečnější poruchy pevného disku, jelikož závady ostatních součástí počítače jako např. grafické karty, operační paměti, zdroje sice vedou k pádu počítače, nicméně data zůstanou většinou zachována v podobě, ve které byly naposled uloženy. Existují samozřejmě zákeřnější vady, které se neprojeví okamžitou ztrátou funkčnosti. Mezi takovéto patří nepřesné výstupní napětí elektrického zdroje, nebo vady motherboardu způsobené jeho stářím, kdy kondenzátory ztrácí svoji původní kapacitu. Počítač často po zapnutí funguje naprosto normálně, jakmile se ale zahřeje (což bývá právě v okamžiku kdy máte vaši práci těsně před dokončením) dojde k jeho zhroucení. Pokud ho opět po chvíli zapnete, zdá se vše opět v normálu. Často je příčinnou selhání také přehřátí počítače – ventilátory při své práci natahují do vnitř skříně kromě vzduchu i prach a ten se usazuje na součástkách a brání tak účinnému chlazení. K určité základní údržbě by proto mělo patřit i odstranění prachu pomocí vysavače a tak předcházet problémům (množství prachu někdy odpovídá spíše vysavači než PC). Při čištění si musíme dát pozor, abychom součástky nezničily statickou elektřinou, zvlášť nebezpečné je oblečení obsahující umělá vlákna – rozhodně nejjistější je se zbavit elektrického náboje uzemněním. Některým poruchám ovšem nezabráníme, neboť jsou způsobeny mechanickým opotřebením, ale obecně u starších komponent je třeba již problémy očekávat a počítat s nimi a proto např. věnovat dostatečnou pozornost zálohování dat jak si

řekneme ještě později. Poruchy hardware mohou být často také způsobeny přírodními živly, typicky úderem blesku. V případě zásahu do elektrické rozvodné sítě, pokud není počítač zabezpečen přepěťovou ochranou, způsobí zvýšené napětí zničení zdroje (někdy ovšem i motherboardu). Blesk se však nemusí projevit pouze přes napájení počítače – velkým nebezpečím je i pro připojení k Internetu prostřednictvím kabelového vedení. Není žádnou vzácností vidět spálený modem zničený právě bleskem. Toto nebezpečí však nehrozí jen venkovnímu vedení. Z vlastní zkušenosti mohu potvrdit, že i když blesk uhodí poměrně daleko od budovy, energie se může indukovat do datových vedení a na jedné straně spálit v počítačích síťové karty a na druhé straně porty ve switchi.

4.6.2 Softwarové příčiny ztráty dat

Mezi softwarové příčiny ztráty dat můžeme zařadit i útoky, o kterých jsme se zmínily již předchozích částech. Šlo přitom o úmyslné poškození či zničení dat. Ke ztrátě dat však může dojít i neúmyslně, sem můžeme zařadit různé chyby v software, které se mohou např. projevit pouze v určitých situacích, nebo kombinacích s konkrétním hardwarem. Softwarové příčiny jsou poměrně časté (při použití OS Windows), každý z vlastní zkušenosti jistě ví, že počítač po delší době od své instalace se stává čím dál pomalejší a stále častěji se vyskytují problémy se selháním programů i celého operačního systému. Příčinou je „zanášení registrů“, kdy po instalaci různých programů a pozdější odinstalaci nám zůstávají v systému různé knihovny a záznamy v registrech (vliv má samozřejmě i fragmentace disku). Pokud si tedy uživatel instaluje pouze nutné programy, které použije při své práci, vydrží mu systém stabilní. Uživatel by měl také vědět, co si na počítač instaluje, rozhodně při „surfování po internetu“ nepotvrzovat každý dotaz na instalaci software do PC. Při běžné práci není také nutné, aby měl uživatel přidělena administrátorská práva. Pod administrátorským účtem se přihlašovat pouze tehdy, pokud opravdu něco potřebuje nainstalovat. Pokud uživatel nemá přidělena administrátorská práva, lze to považovat za určitý základní stupeň ochrany, neboť se mu nepodaří některé programy nainstalovat (nemá povolen zápis do určitých částí registru, jakož i do systémových adresářů).

4.6.3 Ztráty dat způsobené uživateli

Selhání uživatelů bývají nejčastěji způsobena jejich neznalostí, méně často pak určitou neopodstatněnou důvěrou v to, že se nic nemůže stát. Chyby způsobené neznalostí je možné eliminovat vzdělávání pracovníků, pořádáním školení jak už jsme se zmínili v předchozích částech. Nahodilým chybám lze asi těžko zabránit, občas se to asi stane každému. Stačí omylem smazat soubor (mazání se Shift – tedy bez koše) a data jsou ztracena. Naštěstí i v tomto případě je možné data opět obnovit. Existuje celá řada programů pro obnovu smazaných dat - ačkoliv mají data příznak jako smazaná, až do jejich přepsání jsou stále dostupná na disku. Horší variantou je, pokud uživatel úplně zapomene data uložit a zjistí to až po delší době, což se také občas stává.

4.6.4 Zálohování uživatelských dat

Ze všeho co jsme si doposud řekli vyplývá důležitost zálohování dat, a to čím jsou data nepostradatelnější a tedy i cennější pro uživatele, tím více je třeba tomuto věnovat pozornost. Pokud se na otázku zálohování díváme z pohledu, zda se mají zálohy vytvářet automaticky, či raději toto ponechat pod kontrolou uživatele, dávám přednost automatickému vytváření záloh. Nelze ovšem toto aplikovat všeobecně, pro automatické provádění záloh je třeba vytvořit podmínky. Pokud by uživatel měl uloženy data (dokumenty atd. určené pro zálohování) na místním disku, potom považuji za lepší variantu ruční zálohování, kdy uživatel sám si provádí archivaci na záložní médium (síťový disk). I v tomto případě lze samozřejmě použít automatickou archivaci (existuje celá řada programů), ale uživatel by jej měl buď spouštět ručně, aby věděl v „jakém stavu dat“ ji provádí, nebo použít automatickou archivaci např. při odhlašování z počítačové sítě, při vypínání počítače. Za mnohem lepší řešení považuji ukládání dat na síťový disk (na server, kde má každý uživatel vytvořenou osobní složku, do které má přístup pouze on sám) a automatické provedení záloh v noci, kdy je jisté, že již žádné dokumenty nejsou otevřeny a upravovány. Uživatel ani nemusí vědět o tom, že jeho data se nenachází na jeho počítači, stačí složku Dokumenty přesměrovat na server do uživatelovy složky a tuto poté archivovat spolu s dalšími daty na serveru. Rozhodnutí, zda

data ukládat na místní disk, nebo raději na síťový je ovlivněno i spolehlivostí sítě. Pokud bude docházet k častým výpadkům sítě, nebo budou existovat jiné problémy se servery, nelze samozřejmě takové řešení doporučit, já se však, na základě mých zkušeností k němu přikláním. V závislosti na důležitosti dat se můžeme rozhodnout, jak dlouho budeme data archivovat před jejich přepsáním. Např. pokud budeme potřebovat dokument, který jsme smazali již před třemi dny, v případě, kdy zálohy nejsou přepisovány každý den, ale máme vytvořeno pět archivů do nichž vždy archivujeme příslušný den, jsme schopni tento dokument ze zálohy obnovit (5 dní v týdnu – pondělí vždy přepíše zálohu pondělí, úterý z úterka atd.). Jen připomínám, že zde se zabýváme uživateli, zálohování z hlediska správců informačních systémů jsme již stručně zmínili v kapitole 2.3.2. Pracovní stanice nebývají tak dobře zabezpečeny před poruchami, nebo výpadky napájení jako servery, které jsou vybaveny redundantními napájecími zdroji, UPS, diskovými poly. Pokud však stanice používají diskové pole, jde většinou o softwarové diskové pole (mirroring, nebo stripping). K zálohování dat, pokud nejsou k dispozici síťové disky, slouží nejčastěji mechaniky DVD-ROM, nebo DVD-RAM (disketové se již téměř nepoužívají, streamery se týkají spíše serverů). Při volbě, zda použijeme DVD-ROM, nebo DVD-RAM je důležité hledisko, zda vytvořené zálohy hodláme po čase přepisovat, nebo zda půjde o trvalé uložení dat. Pokud budeme zálohy přepisovat je vhodnější použít DVD-RAM, neboť tato technologie umožňuje mnohem vyšší počet přepisů DVD, než je možné u DVD RW. Častým záložním médiem jsou dnes rovněž USB Flash Disky a také externí disky připojené přes USB rozhraní. Dnes jsou všechny tyto zařízení již vybaveny rozhraním USB 2.0, na starší 1.1 narazíme pouze u starých zařízení.

4.6.5 Internet Explorer –častý zdroj bezpečnostních problémů

Většina uživatelů používá na svém počítači pro prohlížení webových stránek Internet Explorer (IE). Jeho nejnovější verze nese označení Internet Explorer 7.0. Jelikož IE bývá často zneužit k napadení počítače, řekneme si zde několik informací o možnostech jeho nastavení. Začneme možnostmi, které jsou obsaženy již v IE verze 6, což je jeho dnes asi nejrozšířenější verze.

4.6.5.1 Správce doplňků, blokování oken

Hned na začátku se musím zmínit o jedné důležité věci a tou je Správce doplňků. Celá řada uživatelů nemá o tomto nástroji ani ponětí a přitom právě on by jim často pomohl vyřešit jejich problémy. Správce doplňků slouží, jak již vyplývá z jeho názvu, ke správě objektů ActiveX a dalších doplňků IE, což jsou jednoduché programy rozšiřující možnosti prohlížeče. Pokud se uživatelům stále nastavuje stejná startovací stránka (ačkoliv oni mají nastavenou jinou), zobrazuje se určitý toolbar, nebo i dochází k pádům počítače, řešení umožňuje právě správce doplňků. Ve správci máme přehled o všech použitých doplňcích i základní informace o nich a to nejdůležitější – můžeme zde zakázat použití doplňku působícího potíže.

Dalším významným nastavením je možnost blokovat automaticky otevíraná okna. Je to velice užitečná vlastnost, nicméně může neznalým uživatelům způsobit i potíže. Někdy totiž je žádoucí, aby se automaticky otevíraná okna neblokovala – nejsou blokována okna ze zóny Intranet a Důvěryhodné servery. Aplikace umožňuje nastavit úroveň blokování a to Nízká: Povolit automaticky otevíraná okna na zabezpečených webech, Střední: Blokovat většinu automaticky otevíraných oken a Vysoká: Blokovat všechny automaticky otevíraná okna. Samozřejmě kromě těchto základních nastavení je možné si přidat do výjimek adresy serverů, u nichž nejsou okna blokována. Nedávno jsem se setkal s problémem blokování oken u jednoho uživatele, který se nemohl přihlásit do banky na svůj běžný účet. Server banky měl správně zařazen mezi důvěryhodné servery a blokování oken bylo vypnuto. Problém spočíval v tom, že si nainstaloval toolbar jednoho známého vyhledávače, který obsahoval i blokování automaticky otevíraných oken a nebral v potaz nastavení důvěryhodných serverů z IE.

4.6.5.2 Záložka Zabezpečení

V možnostech IE na záložce Zabezpečení nalezneme další možnosti nastavení týkající se bezpečnosti. Veškeré okolí počítače (Internet i LAN) je zde rozděleno do zón, přičemž každé zóně můžeme nastavit vlastní úroveň zabezpečení. Jsou zde předdefinovány zóny: Internet –

obsahuje servery neumístěné v žádné jiné zóně, z toho vyplývá nemožnost přidávat servery výběrově po jednom. Zóna Místní intranet - zahrnuje servery umístěné v LAN, přes tlačítko Servery se dostaneme do dalšího nastavení, kde nalezneme tři možnosti ovlivňující zařazení serveru do LAN a to: Zahrnout všechny místní servery neuvedené v jiných zónách, Zahrnout všechny servery, které obcházejí server proxy a Zahrnout všechny síťové cesty (adresy UNC). Z jejich názvu je patrná jejich funkce. Kromě těchto tří zaškrtávacích boxů zde nalezneme i tlačítko Upřesnit, umožňující přidat do této zóny konkrétní server (pokud zatrhneme box s https, půjdou nám přidat pouze zabezpečené servery). Zóna Důvěryhodné servery by měla obsahovat pouze servery, jimž důvěřujeme. Přidávat je sem můžeme opět přes tlačítko Servery a opět zde nalezneme zaškrtávací box Vyžadovat ověření všech serverů v této zóně serverem (https:). Poslední zónou je zóna Servery s omezeným přístupem, kam můžeme přidávat přes tlačítko Servery takové, které nejsou důvěryhodné. Úrovně zabezpečení předdefinované v IE jsou následující: Vysoká, Střední, Středně nízká a Nízká. Defaultně po instalaci jsou zónám přiděleny úrovně zabezpečení Internet – Střední, Místní intranet – Středně nízká, Důvěryhodné servery – Nízká a Servery s omezeným přístupem – Vysoká. Neznamená to však to, že bychom byli omezeni pouze těmito nastaveními, v každé zóně můžeme vytvořit vlastní úroveň zabezpečení, podle našich potřeb (přes tlačítko Vlastní úroveň). Z názvů jednotlivých položek, které můžeme ovlivnit je patrná jejich funkce, jsou seskupeny do následujících oblastí: komponent využívající technologii .NET Framework, ověřování uživatelů, ovládacích prvků ActiveX a modulů plug-in, skriptování, stažení a různé (seznam položek je poměrně dlouhý, rozhodně se vyplatí si jej pro lepší orientaci alespoň projít). Tento výčet však nelze považovat za úplný, bude se lišit podle nainstalovaných součástí – pokud si nainstalujeme prostředí Java, nalezneme zde možnosti jejího nastavení.

4.6.5.3 Záložka Osobní údaje, rodičovská kontrola

Další důležitou záložkou v Možnostech Internetu je záložka Osobní údaje, týkající se cookie souborů. Cookie jsou krátké soubory, do kterých si některé servery ukládají informace o uživatelích, jako např. nastavení uživ. prostředí na serveru, naše požadavky, historii

navštívených stránek apod. Celá řada serverů však může tyto informace zneužít nejčastěji k reklamním účelům. A právě na této záložce máme možnost si nastavit, které servery mohou soubory cookie používat a které mají přístup zablokován.

Alespoň stručně se zmíním o možnosti rodičovské kontroly, která je rovněž v IE obsažena. Je třeba si však říci, že ji nelze považovat za 100%, neboť ji lze poměrně jednoduše obejít. Tuto kontrolu nalezneme na záložce Obsah v části Poradce hodnocení obsahu pod tlačítkem Povolit. Hodnocení je prováděno pomocí služby RSACi (Internet Recreational Software Advisory Council), poskytované organizací ICRA (Internet Content Rating Association), součásti Family Online Safety Institute. Je možné samozřejmě využít i jiného systému hodnocení, hodnotícího úřadu. Na záložce jsou vytvořeny čtyři kategorie a to : Jazyk, Nahota, Násilí a Sex, přičemž u každé kategorie můžeme nastavit úroveň (k dispozici jsou 4 úrovně). Další záložka nám umožňuje nastavit konkrétní servery, které se mohou zobrazit vždy a naopak, které budou vždy zakázány. Důležité je zabezpečení všech těchto nastavení heslem, aby nemohly být změněny kýmkoliv.

4.6.5.4 Další nastavení ovlivňující bezpečnost

Bezpečnost informací o uživateli je také ovlivněna nastavením funkce Automatického dokončování, automaticky doplňujícího dříve použité hodnoty při zadávání údajů z klávesnice. Automatické dokončování lze použít při vyplňování webových adres, formulářů, uživatelských jmen a hesel na formulářích. U těchto jednotlivých položek můžeme tuto funkci vypnout, zrovna tak i nastavit, aby se nezobrazovala výzva k uložení hesel. I když nám usnadňuje práci, umožní dalším uživatelům pokud se dostanou na náš počítač zjistit celou řadu informací. Podobně i ukládání historie naposledy navštívených webových stránek - také zde můžeme nastavit kolik dní mají být zachovány. Vymazat můžeme jednorázově nejen historii, automaticky vyplňovaná data, hesla, ale i soubory cookie.

Při kontrole, co všechno náš IE používá bychom neměli zapomenout ani na možnost si prohlédnout použité objekty, které jsou ukryty v - V možnostech Internetu - záložka Obecné, část Dočasné soubory Internetu tlačítko Nastavení - tlačítko Zobrazit objekty. Zde se dozvíme

mnoho užitečných informací, např. zde bývá objekt mající na starost přehrávání flash animací - Shockwave Flash Object, někdy i objekt CAPICOM, např. nutný pro vyplňování daňových přiznání přes Daňový portál atd.

Přes Internet Explorer můžeme také pracovat s certifikáty. Přes tlačítko Certifikáty se dostaneme na jejich správu. Můžeme zde zjistit informace o jejich platnosti, vystaviteli a další. Můžeme zde importovat certifikáty, jakož i provádět jejich zálohování (vyexportovat na zálohovací médium).

Poslední věcí o které se musím alespoň okrajově zmínit je konfigurace IE na záložce Upřesnit, kde nastavujeme chování celého programu. Je zde opět celá řada nastavení, my se podíváme na část Zabezpečení. Právě zde nalezneme položky jako je Kontrolovat odvolání certifikátu vydavatele, kontrolovat podpisy stažených programů, používat protokoly SSL 2.0, 3.0 a TLS 1.0. Můžeme zde povolit spouštění aktivního obsahu z CD disků, ze souborů v místním počítači. Zapnout upozornění na neplatné certifikáty serverů, zjišťovat, zda nejsou odvolané. Významná je možnost nastavit automatické odstranění dočasných souborů po ukončení IE.

4.6.5.5 Internet Explorer 7.0

Doposud uváděné informace se týkali obou verzí Internet Exploreru. Verze 7.0 obsahuje oproti verzi 6.0 některá vylepšení, ve většině případů však jde pouze o kosmetické úpravy a odstranění již dlouho kritizovaných nedostatků (jako jsou záložky, u konkurence již dlouhou dobu naprosto běžné). U nastavení zabezpečení zóny došlo k přiklonění se k vytváření vlastních nastavení (což bylo možné i dříve) u rodičovské kontroly přibylo více kategorií. Významným zlepšením je přidání filtru Phishing útoků, uživatel má možnost sám oznámit webový server, pokud jej považuje za podezřelý.

Mezi další úpravy patří funkce ActiveX Opt-in, která po instalaci zakazuje použití většiny ActiveX objektů (prostřednictvím vyskakovacího panelu jej však můžeme povolit), skripty spouštěné na webových serverech jsou chráněny před interakcí s daty z jiných domén, u

každého nově otevřeného okna se zobrazí řádek s adresou, podporuje použití národních znaků v názvech domén a varuje před použitím vzhledově podobných znaků (snažící se působit dojmem určité známé domény). V případě nedostatečně nastaveného zabezpečení varuje IE uživatele v informačním řádku. [23].

V materiálech firmy Microsoft je uváděna celá řada zlepšení, která jsou mnohdy spíše marketingovým trikem. Je třeba se však zmínit, že IE byl nainstalován na operačním systému Windows XP, v případě použití Microsoft Vista prohlížeč běží v odděleném paměťovém prostoru a rovněž možnosti rodičovské kontroly by měly být rozsáhlejší.

4.7 Rizika hrozící v malé počítačové síti

Bezpečnostní rizika hrozící v malé počítačové síti jsou obdobné jako ve velké počítačové síti. Nicméně však zde existují určité odlišnosti. Zatímco velké organizace disponujícími velkými sítěmi mají větší finanční možnosti a o správu takovéto sítě se stará specializovaná osoba s potřebnými znalostmi, v malé organizaci může být tato správa přidělena osobě jako vedlejší činnost vedle její běžné pracovní náplně. Vše samozřejmě závisí na odborných znalostech, této osoby. Existuje zde vyšší riziko selhání administrátora sítě vedoucí k nefunkčnosti sítě, přičemž nemusí jít o úmyslné poškození ale pouze o podcenění problému, nebo nedostatek znalostí. Velké sítě vzhledem ke své velikosti a složitosti, jakož i šíři provozovaných aplikací obsahují více příležitostí k napadení. Obecně platí - čím složitější, tím větší riziko objevení mezery v zabezpečení (chyby různých programů apod.).

V malé počítačové síti běžné organizace naopak hrozí menší nebezpečí od profesionálních hackerů, neboť data v této síti nejsou pro ně potenciálně zajímavá, nicméně různí „amatérští“ hackeři často rádi zkouší svoje schopnosti pronikáním i do malých sítí, které bývají hůře zabezpečeny.

Další riziko souvisí opět s nižšími finančními možnostmi a tím i nižšími investicemi jak do hardware, tak i software. Rozhodně by měl být server zabezpečen proti výpadku napájení. Dnes již ceny UPS jsou na poměrně rozumné úrovni a není nutné mít zdroj s extrémně

dlouhou výdrží baterií. Postačí, pokud zdroj je schopný dodávat napětí během krátkodobého zakolísání napětí (které bývá nejčastější) a pokud výpadek trvá delší dobu zajistit jej po dobu vypínání serveru. Zrovna tak i otázka zálohovacích mechanizmů dat je poměrně snadno řešitelná bez výrazných finančních nákladů. Jako záložní zařízení můžou být použita běžná DVD-ROM, nebo ještě lépe DVD-RAM (jak již bylo zmíněno v části o zálohování dat), neboť takřka všichni výrobci DVD mechanik začali podporovat i tento formát vhodnější k častému přepisování. O nutnosti zabezpečení sítě firewallem se není třeba snad ani zmiňovat, neboť jde o naprostou samozřejmost. Zrovna tak by měly být všechny počítače a servery vybaveny antivirovými programy. Nevyplatí se ani podcenit bezpečnostní politiku uplatňovanou uvnitř organizace - čím přísnější, tím více se lze vyhnout v budoucnu problémům, rozhodně by ale neměla být na úkor efektivnosti práce. Vhodným zdrojem dalších informací nejen o rizikách, ale i možnostech zabezpečení dat je publikace od Jaroslava Horáka Bezpečnost malých počítačových sítí [24], nebo Bezpečnost sítí na maximum od Andrew Lockharta [25]. Problematikou útoků na počítačové sítě a obranou proti nim se zabývá také Hacking bez záhad [26]. K dané problematice však existuje celá řada nejrůznější literatury počínaje manuály k jednotlivým programům až po specializované publikace úzce se soustřeďující na konkrétní oblast.

4.8 Finanční hodnocení implementace sítě

Při stanovení nákladů na vybudování počítačové sítě musíme zohlednit nejen cenu hardware, ale i software, jakož i pozdější náklady související se správou. Jelikož ceny se neustále mění, budeme vycházet z cen platných v období září 2006, je třeba si však uvědomit, že ceny se mohou lišit i u různých prodejců. Proto lze tuto kalkulaci považovat pouze za orientační, nicméně rozdíly by neměly být příliš veliké.

4.8.1 Hardwarové náklady

Náklady na budování 100Mbps (100baseTX-FD) lokální sítě jsou přitom dnes již naprosto zanedbatelné: cena jednoho portu v přepínači ("switch") se dnes pohybuje okolo 120 Kč vč. DPH, příslušné rozhraní je dnes přitom již nejčastěji běžnou součástí PC, a pokud není, tak dovybavení jednoho PC síťovou kartou stojí max. 250 Kč vč. DPH. Cena kabelu vhodného pro budování lokálních sítí se pohybuje okolo 6 Kč/metr. Přitom 100Mbps síť je pro použití v rámci malé organizace plně dostačující, neboť síť je pouze čas od času lehce zatížena při výměně informací mezi pracovní stanicí a serverem, tisku na síťové tiskárně, nebo třeba přenosu souborů mezi PC. Maximální reálná rychlost 100 Mbps je až 12x vyšší než maximální teoretická rychlost internetu přes ADSL nebo přes kabelovou televizi, která typicky činí 8 Mbps. Počítačovou dvouzásuvku (2xRJ45 Cat.5e) je možné pořídit za cenu okolo 280,- Kč, rozdíl oproti jednoduché zásuvce (1xRJ45 Cat.5e) je zanedbatelný. V serverovně musíme kabely ukončit na patch panelu, který je buď připevněn přímo na stěnu (cena 12 portů RJ45 2400,- Kč), nebo je umístěn v datovém rozvaděči. V našem případě pořídíme datový rozvaděč (rack) 19"/ 400mm/6U za 3.900,- Kč a patch panel 16.port UTP Cat.5e, 1U 19´´ za 900,- Kč.

Obecně lze říci, že při výběru aktivních síťových prvků menší organizace vybírají především na základě poměru ceny a výkonu, větší pak zohledňují i značku a technickou podporu. Přestože v našem případě jde o opravdu malou síť ve které nehrozí, že by switch určený pro standardní provoz nezvládl nápor uživatelů, dáme přednost osvědčeným výrobcům. Použijeme dvakrát switch 3COM OFFICECONNECT DUAL SPEED SWITCH 8X10/100BASE-TX PLUS za 1500,- Kč. Při použití 8portového switche nám zůstává na segmentu jedna pouze jeden volný port, proto by bylo vhodné zvážit budoucí požadavky na rozšíření sítě a případně pořídit místo 8portového jeden 3COM OFFICECONNECT DUAL SPEED SWITCH 16X10/100BASE-TX PLUS za 2500,- Kč, který má 16 portů a vytváří tak dostatečnou rezervu do budoucna. Záložní zdroj použijeme Trust UPS 1000 Management PW-4105 za cenu kolem 3.000,- Kč (výkon 1000 VA, je schopen dodávat napětí po dobu 38 – 70 minut) a bezdrátový přístupový bod OvisLink WL-5460AP za cca 1.300,- Kč.

4.8.2 Softwarové náklady

Poslední položkou kterou musíme opatřit jsou servery se softwarem. Při nákupu software si nejdříve rozmyslíme, zda si pořídit OEM verzi, nebo krabicovou FPP. Hlavní rozdíl mezi softwarem OEM a krabicovým softwarem spočívá v licenci. Software OEM je licencován pouze pro používání s počítačovým systémem, do něhož byl původně nainstalován, zatímco krabicový software lze přenést do jiného počítačového systému. Dalším rozdílem je identita poskytovatele licence. Smlouva EULA softwaru OEM je licenční smlouva mezi výrobcem počítače a koncovým uživatelem, smlouva EULA softwaru FPP je licenční smlouva mezi společností Microsoft a koncovým uživatelem. Ačkoliv je tedy serverový software OEM cenově výhodnější, jeho použití je vázáno na kompletní počítač s nímž byl zakoupen. Microsoft poskytuje celou řadu licenčních programů včetně multilicencí, které však fungují formou upgrade ať už OEM tak i FPP produktů, zrovna tak není možné využít program SELECT vzhledem k nízkému počtu potřebných licencí[6].

K pořízení serverů můžeme přistoupit dvěma způsoby. Za prvé můžeme koupit servery s OEM softwarem, nebo obyčejné počítače a na ně nainstalovat serverový operační systém pořízený samostatně jako FPP produkt. Rozhodující je, jak často plánujeme servery obměňovat. Pokud to hodláme provádět poměrně často (každoročně), je vhodnější si nepořizovat přímo server, který je poměrně drahý, ale koupit si výkonné PC na které si nainstalujeme serverový operační systém. Vzhledem k rychlosti vývoje v oblasti výpočetní techniky je server za nějaký čas již zastaralý a pokud použijeme obyčejný PC, můžeme jej častěji nahrazovat výkonnějším a starý použít jako běžnou pracovní stanici (pokud koupíme přímo server, vzhledem k vyšším nákladům jej budeme chtít využívat delší dobu, během které však tento server může zaostat za obyčejnými PC). Toto samozřejmě neplatí pro výkonné servery za několik miliónů korun na nichž jsou provozovány náročné aplikace. Pro zajištění běžného provozu sítě však stačí obyčejné PC v ceně cca 15.000,- Kč (s integrovanou grafickou kartou, bez monitoru). Software tvoří významnou část nákladů na pořízení serveru

[6] Stručný přehled licenčních programů fy.Microsoft je uveden v příloze č.5

Gate, který používá operační systém Windows Server 2003 Standard Edition. Pokud koupíme krabicovou verzi Windows Server 2003 Std. R2 Win32 s licencí pro 15 klientů, vyjde nás to na 42.000,- Kč (10 klientů 36.500,-Kč + 5 klientů 5.500,-Kč).

Druhou možností je pořídit si přímo server s předinstalovaným OEM operačním systémem. K tomuto řešení sáhneme v případě, pokud počítáme s dlouhodobějším nasazením tohoto serveru. Takovéto servery se dnes nechají pořídit i v cenách kolem 20.000,- Kč. Jejich výhodou je stabilita, neboť používají základní desky a komponenty určené pro nepřetržitý provoz. Windows Server 2003 OEM s 15 klienty lze pořídit za cenu kolem 21.500,- Kč (10 klientů 18.500,- Kč + 5 klientů 3000,- Kč).

Jak již jsem dříve uvedl rozhodující je právě hledisko času, neboť obyčejné počítače nejsou určeny k nepřetržitému provozu (z vlastní zkušenosti však mohu říci, že pokud nepoužijeme naprosto neznačkové PC lze jej bez problémů rok i více provozovat jako server) a proto je budeme častěji nahrazovat novými. V tomto případě je vhodné si pořídit krabicové verze FPP software, které nám umožní jeho přenositelnost.

Software Kerio WinRoute Firewall pro 15 klientů přijde na 12.000,- Kč. Jelikož na serveru Apl je nainstalován operační systém Fedora Core, který je freeware, náklady se budou týkat pouze vlastního hardware. Abychom ochránili všechny počítače v síti před napadením různými viry, spywarem atd., nainstalujeme na ně program od fy. Symantec, Norton Internet Security 2007 CZ. Koupíme 15 licencí za 13.500,- Kč (licence pro 5 klientů vyjde na 4.500,- Kč). Tento produkt obsahuje i firewall.

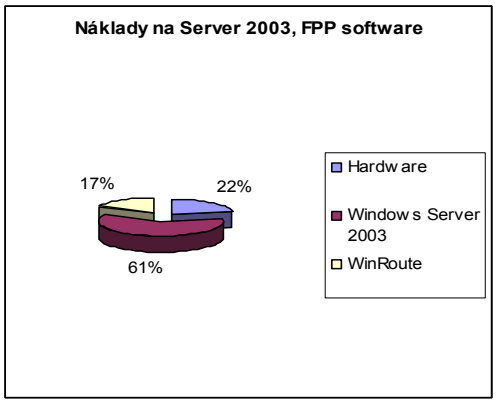
Pro srovnání se můžeme podívat na náklady týkající se pořízení serverů. Pouze pro připomenutí k rozdílu cen hardware – v prvním případě pořizujeme obyčejný počítač, v druhém přímo server (viz. výše).

Tab. 4.4: Stručný přehled nákladů na servery

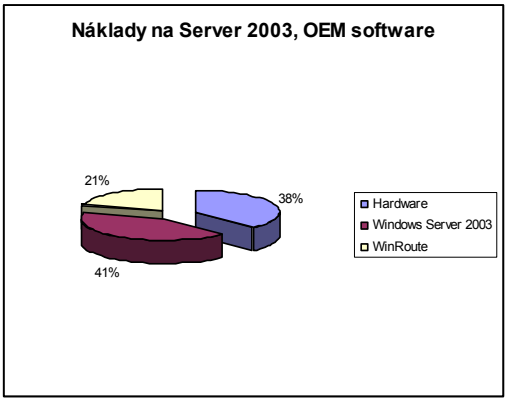
Položka	Orientační náklady FPP software	Orientační náklady OEM software
Server Windows 2003		
Hardware	15.000,- Kč	20.000,- Kč
Software	42.000,- Kč	21.500,- Kč
WinRoute	12.000,- Kč	11.000,- Kč
Celkem	69.000,- Kč	52.500,- Kč
Server Fedora		
Hardware	15.000,- Kč	20.000,- Kč
Software	0,- Kč	0,- Kč
Celkem	15.000,- Kč	20.000,- Kč

Z následujících grafů je vidět, že významnou část nákladů tvoří právě software. Jelikož v případě serveru postaveném na linuxové distribuci Fedora se náklady týkají pouze hardware, je v grafu zachycen pouze Windows Server 2003.

Obr. 4.6 Náklady na server 2003, FPP software



Obr. 4.7: Náklady na Server 2003, OEM software



V případě námi použitých komponent se cena pohybuje podle zvolené varianty v rozmezí 103.000,- Kč až 115.000,- Kč. Je však samozřejmě možné ušetřit a pořídit například levnější switche, UPS. Také jako server Apl může být použit již starší, méně výkonný PC. V oblasti software se však příliš prostoru pro úspory nenabízí. Součástí našeho výpočtu nejsou náklady

na jednotlivé uživatelské počítače, neboť obecní úřad jimi už musí být vybavený, zrovna tak jako náklady na zalištování kabeláže a náklady na práci (obecní úřad si může zajistit vlastními pracovníky). Zde jsme uvedli nejnutnější náklady spojené s propojením počítačů a vytvořením funkční počítačové sítě. Je třeba však počítat nejen s náklady na vybudování, ale i spojenými s údržbou, či budoucími upgrady software či hardware. Náklady na údržbu závisí s možnostmi, které má obecní úřad k dispozici. Domnívám se, že v dnešní době je schopen běžnou správu serverů zajistit i zaměstnanec, který se alespoň trochu orientuje v dané problematice. V následující tabulce 4.5 jsou uvedeny celkové náklady rozdělené podle jednotlivých položek.

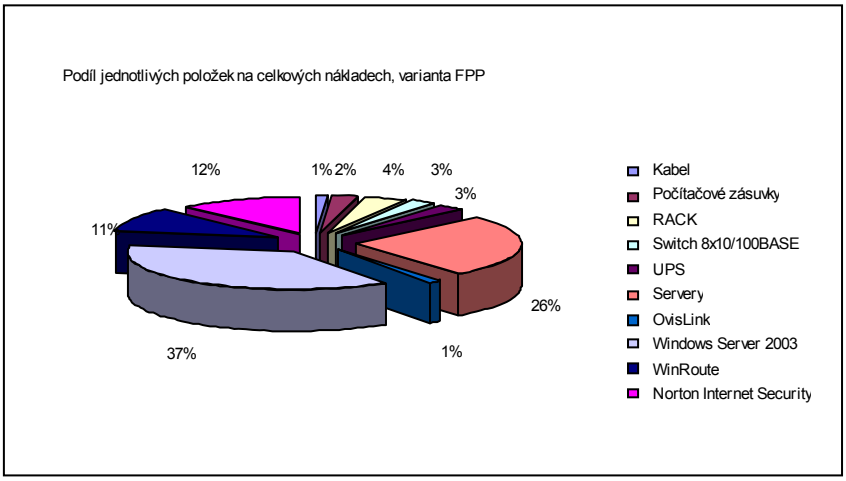
.

Tab. 4.5: Stručný přehled celkových nákladů

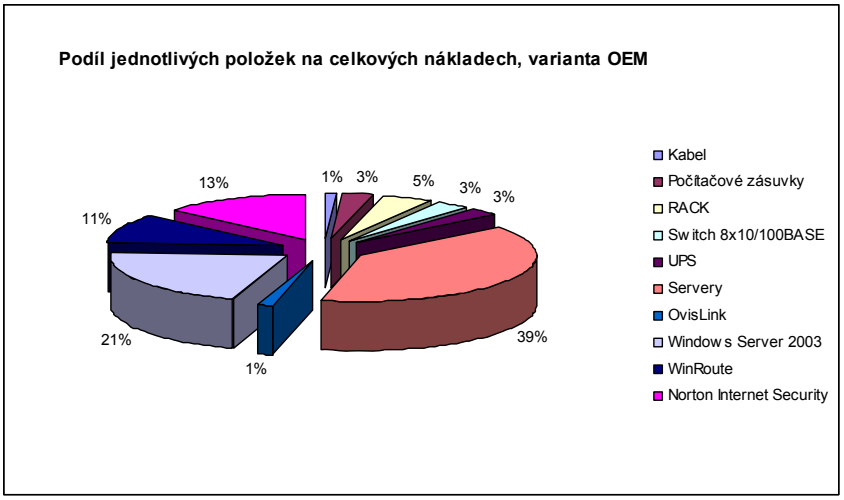
Položka	Počet	Orientační náklady FPP software	Orientační náklady OEM software
Hardware			
Kabel UTP Cat.5e	200 m	1.200,- Kč	1.200,- Kč
Počítačové zásuvky	10	2.800,- Kč	2.800,- Kč
RACK + patch panel 16xRJ45	1	4.800,- Kč	4.800,- Kč
Switch 8x10/100BASE	2	3.000,- Kč	3.000,- Kč
UPS	1	3.000,- Kč	3.000,- Kč
Servery	2	30.000,- Kč	40.000,- Kč
OvisLink WL-5460AP	1	1.300,- Kč	1.300,- Kč
Software			
Windows Server 2003	1	42.000,- Kč	21.500,- Kč
WinRoute	1	12.000,- Kč	11.000,- Kč
Norton Internet Security 2007 CZ	15	13.500,- Kč	13.500,- Kč
Součet celkem		113.600,- Kč	102.100,- Kč

Na jednotlivé náklady se můžeme také podívat z pohledu, jaký podíl zaujímají na celkových nákladech.

Obr. 4.8: Celkové náklady, varianta FPP software



Obr. 4.9: Celkové náklady, varianta OEM software



4.9 Shrnutí

V této části práce jsme využili teoretické základy z předchozích kapitol pro navržení konkrétní počítačové sítě. Při jejím návrhu jsme již od počátku brali ohled na otázku bezpečnosti a vlastní síť jsme rozdělili do dvou segmentů. Jednoho důvěryhodného, v němž jsou připojeny počítače pracovníků a druhého, sloužícího k připojení počítačů umístěných v knihovně pro volný přístup do Internetu. Síť je postavena na technologii 100 MBit/s Ethernetu. Stručně jsme se zmínili o některých službách, které jsou v naší síti provozovány

jako je DNS, což je nezbytný předpoklad pro správnou funkci poštovních a webových služeb i Active Directory.

Serverem, přes který je naše síť připojena do Internetu je gate.knezice.ji.cz, na kterém je nainstalován operační systém Windows Server 2003 Standard se Service Packem 1 a firewallem Kerio WinRoute 6.2. Tento server plní rovněž úlohu doménového kontrolleru (Active Directory), DNS serveru, souborového a tiskového serveru. Veškerá komunikace serveru gate s pracovními stanicemi je šifrována pomocí IPSec pracujícím v transportním módu. Uživatelská data, jakož i data určená ke sdílení nejsou ani na serveru ponechána nezajištěna, ale jsou opět chráněna, pomocí systému EFS.

Firewall ukrývá strukturu místní sítě před Internetem a filtruje pakety, které propustí z a do místní sítě, jakož i mezi oběma segmenty. Do Internetu povolí odchozí provoz protokoly FTP, HTTP, HTTPs, ale pouze ověřeným uživatelům. Naopak z Internetu je povolen přístup mapováním portů na server apl.knezice.ji.cz protokoly SMTP, HTTP a HTTPs, neboť na tomto serveru je nainstalován Sendmail a Apache. Mezi prvním segmentem a serverem gate je povolen provoz bez omezení, což však už neplatí pro druhý segment. Zde je povolen protokol LDAP a jeho zabezpečená varianta LDAPs pro komunikaci s Active Directory, protokol TCP, UDP (port 53) s dotazy na DNS server, dále protokol ICMP (populární PING). Protokol Kerberos V5 zajišťuje autentizaci uživatelů a je primárním protokolem pro ověřování v rámci domény serveru 2003, protokol IPSec umožňuje vytvořit šifrované spojení a my jej využijeme k šifrování komunikace serveru gate.knezice.ji.cz s klientskými počítači. S tím souvisí i použití protokolu IKE majícího na starost dynamickou výměnu kryptografických klíčů. A poslední služba Microsoft-DS - jde pouze o jiný název pro SMB/CIFS (port 445), používaný fy. Microsoft ke sdílení souborů a tiskáren. Na základě předchozích údajů je samozřejmé, že na klientských počítačích nemůže být použit starší operační systém než Windows 2000 (vyplývá z informací, které známe z teoretické části). Odesílání pošty ze serveru apl.knezice.ji.cz na server poskytovatele připojení probíhá zabezpečeným protokolem SMTPs, zrovna tak jako odesílání pošty z klientských stanic na náš poštovní server. Rovněž stahování pošty z našeho serveru probíhá zabezpečeným POP3s (pošta funguje pouze

z prvního segmentu). Uživatelé z druhého segmentu mají omezen přístup na první segment protokoly HTTP, HTTPs (na webový server Apache) a také PING.. Všichni uživatelé z místní sítě používají lokální jmenný server (DNS), který pracuje v režimu forwarding slave server a pouze tento má přístup do Internetu na DNS server poskytovatele připojení. Bezdrátové spojení je šifrováno pomocí IPSec v tunnel módu.

Kerio WinRoute však umožňuje kromě řízení přístupu podle komunikačních pravidel i filtraci na úrovni aplikačního protokolu HTTP a FTP. Filtrovat je možné podle URL i zakázaných slov. Pomocí adresy URL blokujeme přístup na freemailové servery, pomocí zakázaných slov kromě předdefinovaných skupin Pornography a Warez/Cracks ještě omezíme přístup na webové stránky s nabídkou hazardních her.

Jelikož server apl je postaven na linuxové distribuci Fedora a obsahuje tedy firewall iptables, použijeme jej k omezení přístupu na server na pouze námi požadované služby.

Na otázku zabezpečení jsme se podívali i z pohledu uživatelů, stručně jsme se zmínili o nejčastějších příčinách ztráty dat, které mohou mít původ v hardwarových, softwarových, nebo i uživatelských selháních. Proto je nutné nepodceňovat otázku včasného a propracovaného systému zálohování dat. Častým zdrojem problémů bývá internetový prohlížeč – v současné době je stále nejpoužívanější Internet Explorer, i když jeho podíl na celkovém počtu prohlížečů se pomalu snižuje. Z tohoto důvodu jsme se zabývali bezpečnostními možnostmi jeho nastavení.

Finanční hodnocení zachycuje nejvýznamnější položky spojené s vybudováním počítačové sítě. Z přehledu nákladů je patrné, že velkou část tvoří právě náklady spojené s pořízením software. Při pohledu do ceníků s produkty fy. Microsoft, by se mohlo zdát výhodnější pořídit místo samotného Microsoft Windows Server 2003 rovnou celý programový balík obsahující mimo Serveru 2003 ještě další aplikace, zejména Microsoft Exchange Server 2003 a Microsoft SQL Server 2000. Rozdíl v ceně se na první pohled nezdá být příliš veliký. Ve skutečnosti však pro připojení každého klienta k Exchange, nebo SQL Serveru budeme potřebovat licence i pro tyto připojení, což nám podstatně celý nákup prodraží. Proto jsme také sáhli k možnosti využít linuxovou distribuci, která nám umožní provozovat SQL server,

nebo poštovní server bez dalších nákladů. Na výběr máme celou řadu programů obsažených již přímo v distribuci Fedora.

Zapomenout nemůžeme samozřejmě ani na antivirovou ochranu všech pracovních stanic, kterou zajišťuje program od firmy Symantec Norton Internet Security 2007 CZ obsahující i vestavěný firewall.

V následující tabulce se pokusím o velice stručné zhodnocení odolnosti naší sítě proti útokům, o nichž jsme se zmínili již na počátku této práce.

Tab. 4.6: Přehled odolnosti naší sítě proti útokům

Odposlech sítě	Komunikace se serverem gate je šifrována pomocí IPSec, pošta je zajištěna pomocí SSL protokoly SMTPs a POP3s, bezdrátové spojení zabezpečuje IPSec tunel. Příchozí pošta z Internetu však není šifrována, zrovna tak jako web (přes HTTP)
Odposlech hesel	
Chybná autentizace	Je použit autentizační modul Kerberos V5 (heslo se sítí nepřenáší), zde spočívá riziko spíše na straně uživatele, aby nedošlo k prozrazení hesla.
Chyby v programech	Ochrana před těmito chybami spočívá v okamžité aktualizaci programů po uvolnění záplat výrobci.
Nedostupnost služby	Zde hrozí velké riziko právě u bezdrátového spoje, i když útočník nebude schopen data rozšifrovat, může přenos rušit neboť jde o volné pásmo a velká ztrátovost paketů znepřístupní Internet se všemi službami.
Ovlivnění trasy IP paketů	IPSec kombinuje vzájemné ověřování se sdílenými klíči založenými na kryptografii. I v tomto případě je možné použít techniku ARP Cache Poisoning – útočník pomocí protokolu ARP přesvědčí uživatele, že jeho MAC adresa je brána a bránu, že jeho MAC adresa je uživatel – data proudí přes útočníka, nicméně tento data pozměnit nemůže.
Sociální inženýrství, malware	Ochrana proti malware je v prvním stupni zajištěna firewallem na gate, každá pracovní stanice je vybavena antivirovým programem s firewallem, spammovými filtry i detekcí malware. Nejslabším článkem je zde člověk při využití sociálního inženýrství.

Závěr

Cílem této diplomové práce, jak již bylo zmíněno v úvodu, je nejen vytvořit vlastní návrh počítačové sítě, ale i poukázat na nutnost zabezpečení dat nejen ve velkých, ale i malých organizacích, jakou je i Obecní úřad v Kněžicích. Než jsme mohli v praktické části přistoupit k návrhu této počítačové sítě, museli jsme se nejprve seznámit s určitými základními pojmy, jež jsou nutné pro pochopení fungování počítačových sítí. Z tohoto důvodu jsme se v úvodu věnovali síťovým protokolům, které jsou nezbytné pro vzájemnou komunikaci mezi jednotlivými součástmi LAN. Standardizace protokolů je totiž velice významná pro zajištění bezproblémové komunikace mezi produkty různých výrobců. To, že existuje velké množství nejrůznějších protokolů je důsledkem jejich specializace. Každý slouží k určitým účelům, pro něž je co nejvhodněji uzpůsoben. Žádný z protokolů však nelze považovat za neměnný, jednou daný. Jako vše ostatní, tak i protokoly se vyvíjejí a stále vznikají novější verze a varianty – vždy je hledán co nejvhodnější kompromis mezi různými požadavky (př. jednoduchost a rychlost <=> bezpečnost). Stručně jsme se také zabývali nejčastějšími druhy útoků proti počítačům i počítačovým sítím a možnostmi ochrany nejen programovými prostředky, ale i fyzickými a personálními opatřeními v rámci bezpečnostní politiky. Jelikož námi navrhovaná počítačová síť je postavena na produktech firmy Microsoft, věnovali jsme se bezpečnosti dat právě v této síti. A to nejen prostředky operačního systému jako jsou uživatelské účty, přístupová práva k souborům a adresářům, ale i programovými možnostmi jako je šifrování dat pomocí systému EFS, ochrana před viry pomocí antivirových programů a samozřejmě je nutné zdůraznit i zodpovědnost jednotlivých osob.

V třetí části jsme vzali v úvahu připojení k Internetu, což má velký vliv na bezpečnost a zabezpečení dat. Prostředkem oddělujícím místní síť od Internetu je firewall. A právě firewallům je zde věnována hlavní pozornost – jejich principům, funkcím, možnostem. Je zde představen firewall Kerio WinRoute, který jsme v následující části nakonfigurovali pro provoz sítě obecního úřadu. Velice stručně jsme se zabývali několika nejznámějšími firewally, které však nejsou určeny pro ochranu celé sítě, ale pouze pro zajištění osobního počítače.

A nyní se již dostáváme k vlastnímu návrhu LAN. Otázce bezpečnosti je třeba věnovat pozornost od samého počátku, od návrhu topologie sítě. Již při nákupu zařízení je nutné se zajímat jaké má bezpečnostní možnosti a zda jsou odpovídající dnešní době. Rozhodně se nevyplatí v této oblasti šetřit za každou cenu a za nějaký čas zjistit, že dané zařízení je třeba vyměnit.

V praktické části jsme se zaměřili na ochranu dat před útoky z vnějšího prostředí - Internetu, tedy na správné nastavení firewallů. Mnoho běžných uživatelů považuje konfiguraci firewallu za příliš složitou činnost. A tak místo toho, aby se snažili vytvořit a nastavit jim vyhovující pravidla chránící jejich počítač, raději rezignují a beze snahy o pochopení principu firewallu automaticky potvrzují vše, na co se jich program zeptá. Výsledkem je poté firewall, který na jednu stranu stěžuje život uživateli, neboť nepropustí užitečnou komunikaci, na druhou stranu však obsahuje zbytečné bezpečnostní mezery. Přitom konfigurace firewallu chránícího ať již samotný počítač, nebo celou počítačovou síť není příliš složitá, nicméně vyžaduje určité znalosti a ochotu zjišťovat si nové informace. Proto jsem zde chtěl na příkladu malé počítačové sítě právě takové jednoduché nastavení ukázat. Existuje mnoho velkých organizací vytvářejících vlastní virtuální sítě, jakož i umožňující práci uživatelů v podnikové síti třeba z domova, u nichž bude konfigurace firewallů podstatně složitější. Samozřejmě že ani firewall není všelékem na bezpečnostní ohrožení, tvoří však jednu z důležitých součástí zabezpečení.

Dostatečnou pozornost je třeba věnovat také zajištění bezpečnosti LAN nejen před útoky z Internetu, ale i z místní sítě. Velká část úspěšných útoku přichází právě ze vnitř. A nemusí jít o žádné složité techniky – stačí „odkoukat“ heslo jiného uživatele. Právě ochrana v místní síti bývá často podceňována s tím, že uživatelé si vzájemně důvěřují. Taková důvěra je sice pěkná věc, ale bezpečnost dat na ni rozhodně nelze stavět. Administrátor, který chce zavést vyšší úroveň zabezpečení se často setká s odporem okolí, které takovéto opatření vnímá jako „šikanu uživatelů“. Nicméně navzdory takovýmto reakcím je třeba se nenechat odradit a bezpečnostní opatření nejen plánovat, ale i zavádět do praxe. Je třeba ovšem zdůraznit, že bezpečnostní prvky implementované do LAN nejsou výsledkem „svévole“ správce informačního systému, ale že jsou pouze jednou částí z celkové bezpečnostní politiky

organizace. Administrátor má místní síť plně pod kontrolou a může tak zavádět bezpečnostní opatření jako je nastavení doménové politiky, náhrada nezabezpečených protokolů jejich šifrovanými verzemi prostřednictvím SSL, popřípadě použít IPSec. To v případě Internetu jsou možnosti omezenější. Pokud potřebujeme navštívit a prohlédnout si určitou webovou stránku, která však neposkytuje možnost přístupu přes HTTPs, těžko s tím sami něco provedeme. Je třeba si uvědomit, že data v Internetu (ve většině případů) nejsou dostatečně zabezpečena a naše důvěrné informace, pokud je nějakým způsobem nezajistíme před zneužitím (nezašifrujeme), na Internet nepatří, takže rozhodně žádné posílání čísel bankovních účtů a hesel e-mailem :-). Tato situace by se měla nicméně o něco zlepšit, jakmile dojde k většímu rozšíření a častějšímu používání protokolu IP verze 6, který povinně používá IPSec (oproti dnes nejčastěji používané verzi 4).

V dnešní době, kdy se počet nejrůznějších útoků neustále zvyšuje, je třeba právě bezpečnosti věnovat dostatečnou pozornost. Zatímco dříve byly počítače často připojeny k Internetu pouze pomalými vytáčenými linkami, dnes jsou i domácí uživatelé připojeni vysokorychlostními spoji. Zrovna tak i náklady na vybudování malé sítě se staly přijatelnými i pro celou řadu běžných uživatelů, proto se stále častěji můžeme setkat s počítačovými sítěmi vytvořenými v rámci domácností. A tento trend se bude neustále zvyšovat s tím, jak bude docházet k vytváření domácích multimediálních sítí. Zatímco dříve počítače sloužily pouze jako pracovní nástroje, dnes stále více plní úlohu zábavní techniky. Jsou na nich uloženy multimediální soubory - písničky, filmy atd. Uživatelé však chtějí k těmto datům přistupovat nejen pouze z počítačů, ale i z dalších zařízení jako jsou televize, přehrávače hudby apod., a tak vytvářejí sítě propojující tyto elektrospotřebiče. Pokud však již jednou takováto síť existuje, logicky chtějí využít i možností Internetu, neboť zde naleznou nepřebernou zásobu nejrůznějších dat. S tím jak budou vznikat takovéto domácí sítě, otázka zabezpečení počítačových sítí se tak stále více bude dotýkat i běžných uživatelů.

Literatura

[1] **Craig, Hunt:** TCP/IP Network Administration 3rd Edition*, O'Reilly & Associates, Inc., 2002, ISBN 0-596-00297-1*

[2] **Staudek, Jan:** Vysokorychlostní sítě, intranety, extranety – trendy. *LANcom, ročník 9, číslo 2/1999, strany 18-24. ISSN 1210-2997*

[3] **Casad, Joe**: Sams Teach Yourself TCP/IP in 24 Hours, Third Edition, *Sams Publishing, 2003, ISBN: 0-672-32565-9*

[4] **Kolektiv autorů**: Linux Dokumentační projekt, *Computer press, 1998, ISBN: 80-7226-114-2,*

[5] **Wikipedia,** otevřená internetová encyklopedie na adrese: http://cs.wikipedia.org

[6] **Odvárka, Petr**: SSL protokol a jeho akcelerace

[7] **Labouret, Ghislaine**: A technical paper giving an overview of the IPsec standard

[8] **PeterS**: Komunikační protokoly, na serveru pcsvet.cz

[9] **Peterka, Jiří**: Aplikační protokoly TCP/IP

[10] **Sitera, Jiří:** Adresářové služby – úvod do problematiky*, Technická zpráva TEN-155 CZ, číslo 4/2000*

[11] **Sharpe, Richard:** Just what is SMB?, October 2002, na adrese http://samba.anu.edu.au/cifs/docs/what-is-smb.html

[12] **CodeFX**: CIFS Explained, Webpages CodeFX

[13] **Vidstrom, Arne**: The use of TCP port 445 in Windows 2000, Webpages Ntsecurity.nu

[14] **Hanáček, Petr - Staudek, Jan:** Bezpečnost informačních systémů a Internet*, LANcom, ročník 7, číslo 6/1997 strany 17-22, číslo 7-8/1997 strany 12-18, ISSBN: 1210-2997*

[15] **Svoboda, Ivan**: Aplikace šifrovacích systémů pro ochranu přenosu dat, *LANcom, ročník 7, číslo 4/1997, strany14-19, ISSN: 1210-2997*

[16] **Staudek, Jan:** Autentizace a kryptografie. *LANcom, ročník 8, číslo 12/1998, strany 15-20, ISSN 1210-2997*

[17] **Hanáček, Petr - Staudek, Jan:** Bezpečnost informačních systémů a Internet*, LANcom, ročník 7, číslo 6/1997 strany 17-22, ISSBN: 1210-2997*

[18] **Šetka, Petr:** Mistrovství v Microsoft Windows Server 2003**,** *Computer Press., 2003, ISBN 80-251-0036-7*

[19] **Pužmanová, Rita:** Bezdrátové lokální sítě podle IEEE I a II, na lupa.cz

[20] **Knapovský, Miroslav:** WiFi: Průniky do sítí a připojení k Internetu, na pctuning.cz

[21] **Němeček, Ivo**: Řešení firewall od firmy Cisco Systems, *LANcom, ročník 8, číslo 7-8/1998, strany 53-57, ISSN: 1210-2997*

[22] **Dostálek Libor, Kabelová Alena**: Velký průvodce protokoly TCP/IP a systémem DNS, *Computer Press., 2000, ISBN: 80-7226-323-4*

[23] **Webové stránky společnosti Microsoft: http://www.microsoft.com/cze/**, cit: březen 2007

[24] **Horák Jaroslav**: Bezpečnost malých počítačových sítí, *GRADA Publishing, 2003, ISBN: 80-247-0663-6*

[25] **Lockhart Andrew**: Bezpečnost sítí na maximum, *Computer Press., 2005, ISBN: 80-251-0805-8*

[26] **Kutz George; McClure Stuart; Scambray Joel**: Hacking bez záhad, *GRADA Publishing,, 2007, ISBN: 978-80-247-1502-5*

Použité RFC:

Internet Protocol	http://www.rfc-editor.org/rfc/rfc791.txt
IP Version 6 Addressing Architecture	http://www.rfc-editor.org/rfc/rfc4291.txt
Transmission Control Protocol	http://www.rfc-editor.org/rfc/rfc793.txt
User Datagram Protocol	http://www.rfc-editor.org/rfc/rfc768.txt
The TLS Protocol	http://www.rfc-editor.org/rfc/rfc2246.txt
Hypertext Transfer Protocol -- HTTP/1.1	http://www.rfc-editor.org/rfc/rfc2616.txt
Simple Mail Transfer Protocol	http://www.rfc-editor.org/rfc/rfc821.txt
Post Office Protocol - Version 3	http://www.rfc-editor.org/rfc/rfc1939.txt
Internet Message Access Protocol - Version 4rev1	http://www.rfc-editor.org/rfc/rfc3501.txt
The Kerberos Network Authentication Service (V5)	http://www.rfc-editor.org/rfc/rfc1510.txt
Protocol Standard For A NetBIOS Service on a TCP/UDP Transport: Concepts and Methods	http://www.rfc-editor.org/rfc/rfc1001.txt
Protocol Standard For A NetBIOS Service on a TCP/UDP Transport: Detailed Specifications	http://www.rfc-editor.org/rfc/rfc1002.txt

Odkazy na organizace zmiňované v textu:

IETF	http://www.ietf.org
IANA	http://www.iana.org
SNIA	http://www.snia.org
IEEE	http://www.ieee.org
ICRA	http://www.fosi.org/icra
FOSI	http://www.fosi.org

Seznam obrázků

Seznam tabulek

Seznam příloh

Příloha č.1 Bezpečnostní politika v organizaci:

Jak budovat, implementovat a spravovat celou infrastrukturu organizačních, procesních i technických opatření k zajištění bezpečnosti.

Rudolf Marek a Jiří Dastych

Každá organizace, bez ohledu na její zaměření, je při výkonu svých činností plně závislá na pracovnících a dostupných prostředcích - motných i nehmotných. Nezbytnou součástí základních manažerských plánů jsou proto i úvahy o tom, jak pracovníky a aktiva organizace chránit. Často se objevuje požadavek na vytvoření systému řízení bezpečnosti organizace. Organizace v něm pomocí stanovených cílů, strategií a politik hierarchicky rozvrhuje oblast řešení bezpečnosti od úrovně celé společnosti až po jednotlivé chráněné oblasti - ersonální, informační a fyzickou. Aktiva organizace mají svoji hodnotu, která je v absolutní většině případů pro organizaci z hlediska jejího fungování kritická. V případě ztráty nebo závažného poškození některých aktiv tak může dojít i k ukončení činnosti organizace, a tím ke značným finančním ztrátám majitele nebo akcionářů, nemluvě o obchodních partnerech, zákaznících i zaměstnancích.

Stanovení bezpečnostních požadavků

Systém řízení bezpečnosti je nedílnou součástí systému řízení organizace a představuje zejména plnění manažerských funkcí. Na začátku jeho tvorby se jedná o stanovení bezpečnostních požadavků. Nejobecnější formou těchto požadavků jsou správně stanovené bezpečnostní cíle, které vycházejí z obchodních cílů organizace, legislativy, smluv a interních požadavků. Jsou-li jasné cíle, je třeba vytyčit strategii ukazující principy a rámcové postupy pro jejich dosažení, následně se uplatní bezpečnostní politiky popisující, co je třeba udělat. Je výhodné vytvářet bezpečnostní politiky jako více provázaných hierarchických dokumentů, které na své úrovni řeší vždy příslušné oblasti bezpečnosti. Zpracovávány tak jsou:

- Bezpečnostní politika organizace zahrnující nejširší a nejvyšší politiky organizace směřující k ochraně jejich pracovníků a aktiv.
- Jako podřízená pro oblast informatiky je v organizaci požadována bezpečnostní politika informací.
- Jejím rozpracováním je bezpečnostní politika IT s případným vytvořením specializovaných bezpečnostních politik jednotlivých informačních systémů organizace.

Tak, jak se snižuje úroveň záběru jednotlivých politik ke konkrétním informačním systémům, rostou nároky na jejich "správné" sestavení. Zatímco nejvyšší politiky proklamativně prezentující vůli vedení k řešení bezpečnosti informací ukazují z vlastního řešení bezpečnosti pouze obecné základní principy a naznačují způsoby a platformy jejich vynucení v rámci organizace, tak bezpečnostní politika IT již prezentuje ve svých pravidlech široký souhrn pečlivě vybraných opatření, závazný pro celou oblast IT organizace. Pro sestavení obou zmíněných druhů politik tedy bude zapotřebí jiná výchozí znalostní báze jdoucí od obecného ke konkrétním opatřením prosazujícím bezpečnost.

Formulace bezpečnostní politiky

Jak tedy formulovat jednotlivé "správné" bezpečnostní politiky informací? K již uvedeným zdrojům politik (obchodní cíle, legislativa, smlouvy) je nutné připojit bezpečnostní rizika. Správné stanovení bezpečnostních rizik vůči aktivům dané organizace vytváří podklad pro identifikaci odpovídajících přiměřených bezpečnostních opatření. Tato opatření, jsou-li vhodně zobecněna, resp. rozpracována, tvoří základ bezpečnostní politiky požadované úrovně. Postupy vedoucí k ohodnocení rizik (přes stanovení hodnot aktiv) a k velikosti hrozeb a zranitelností jsou určující pro výsledné formulace bezpečnostních politik. Politiky tak odrážejí na příslušné úrovni požadovaná bezpečnostní opatření, která byla pro eliminaci zjištěných rizik formulována na základě výběru z katalogů (normy) nebo jako výstup z automatizovaného expertního systému (např. metoda analýzy a zvládání rizik CRAMM -CCTA Risk Analysis and Management Method). Pevná

a prokazatelná vazba mezi aktivy a přiměřenými formulacemi ochranných bezpečnostních politik je tak díky stanoveným rizikům vždy zajištěna. Zařazení pravidla o stanovování bezpečnostních rizik informací organizace, včetně jeho povinné aplikace do nadřazené politiky bezpečnosti informací, ukazuje, jak systémově správně řešit tvorbu bezpečnostních politik. Rámcové postupy, které vedou k formulaci a vytvoření specializovaných politik, jsou tak součástí politik nadřazených.

Od požadavků politiky k řešení bezpečnosti

Rozebrali jsme první obecnou část tvorby systému řízení bezpečnosti - stanovení bezpečnostních požadavků ve formě politik. Odpověď na otázku, jak přejít od požadavků k jejich řešení, tedy k implementaci politik, dává bezpečnostní projekt. Činnosti spojené s bezpečnostním projektem spočívají v nalezení a v popisu realizace stanovených bezpečnostních opatření v celé jejich šíři. Technická opatření je třeba promítnout do bezpečnostní architektury IT organizace, což znamená najít jednotlivé komponenty IT infrastruktury a na ně navázat jednotlivá požadovaná bezpečnostní opatření. Případně může být nutno pro jistou část bezpečnostních opatření stávající infrastrukturu vylepšit (nové prvky nebo prvky s novými, bezpečnost podporujícími vlastnostmi). Netechnická (fyzická, personální a procedurální) opatření je třeba dostat do života formou směrnic. Bezpečnostní projekt tvoří organizace ve spolupráci svých odborných IT útvarů s externím dodavatelem - bezpečnostním specialistou. Stranou projektu nesmějí zůstat případní dodavatelé aplikačního programového vybavení do organizace, neboť bezpečnostní projekt realizuje požadavky politik i v této oblasti. Výstupy z bezpečnostního projektu popisují, jak byly bezpečnostní architekturou realizovány a implementovány bezpečnostní požadavky z příslušných politik a jaké byly vytvořeny podpůrné procedury k jejich prosazení. Zpracované bezpečnostní příručky pro uživatele a správce pak dávají detailní návod pro obsluhu, nastavení a údržbu bezpečnostních mechanismů. Důležitou součástí bezpečnostního projektu je rozpracovávání vhodné řídící bezpečnostní struktury organizace, spolu s vydefinováním základních rolí, odpovědností a

povinností v systému řízení bezpečnosti, včetně vhodné klasifikace aktiv organizace. Vazba této organizační normy na základní manažerské činnosti organizace je zajištěna nadřazenou bezpečnostní politikou informací, která zavazuje vedení organizace bezpečnost řídit a spravovat. Dalším klíčovým dokumentem bezpečnostního projektu se základní platností pro celou organizaci je dokument "Obnova funkčnosti IT systémů organizace". Ten poskytuje rámcový návod na řešení havarijních situací v organizaci pomocí rozpracovaného systému detailních a průběžně aktualizovaných havarijních plánů jednotlivých informačních systémů. Základy nouzového plánování, vyjádřené v tomto dokumentu, mají přímou vazbu na bezpečnostní politiky, protože jsou spojeny s identifikovanými nejcennějšími aktivy a odvozeny od míry rizika jim hrozící. Pro řešení bezpečnostních incidentů v organizaci slouží "Manuál zvládání bezpečnostních incidentů", který definuje bezpečnostní incident a popisuje činnosti zúčastněných na jeho identifikaci, lokalizaci, zvládnutí a vyšetření. Bezpečnostní projekt dále obsahuje výčet a přiřazení netechnických bezpečnostních opatření zejména organizačního charakteru, která směřují do příslušných útvarů organizace (personální bezpečnost, fyzická bezpečnost, provozní a vývojová bezpečnost).

Implementace řešení bezpečnosti

Zpracovaný bezpečnostní projekt, který představuje realizaci bezpečnostních politik, je nyní třeba uvést v život - implementovat. Tato činnost představuje především manažerské úsilí, při kterém se organizace snaží implementací přeměnit bezpečnostní projekt ve fungující bezpečnostní systém. Stručně řečeno jde o to, jak vypracovaný bezpečnostní projekt, tedy jeho technickou i netechnickou část, zavést do každodenního fungování organizace. Při implementaci roste důležitost role organizace a jejích odborných útvarů. Celá činnost musí být v rámci organizace dobře koordinována a vedena, a to i ve směru k případným dodavatelům aplikačního vybavení. Dodavatel bezpečnostního projektu pomáhá při efektivní plošné implementaci technických opatření dle bezpečnostního projektu, upravuje a zpřesňuje bezpečnostní dokumentaci a spolupodílí se na

implementaci dalších, ve fázi projektu jen připravených, netechnických bezpečnostních opatření organizačního charakteru. Další jeho činností je školení implementátorů, správců i uživatelů tak, aby celkové bezpečnostní povědomí přispělo k pochopení, osvojení a vědomé podpoře implementovaných opatření u co nejširší komunity uživatelů. Implementace bezpečnostního projektu představuje velmi komplexní, rozsáhlou činnost, znatelně zasahující do běžného každodenního fungování organizace. Je třeba mít na zřeteli, že tvorba bezpečnosti a obzvláště její implementace je vždy proces, nikoli stav. Běžně se totiž stává, že původní časové odhady při implementaci byly vyčerpány, a to včetně připravených rezerv, a stále ještě zbývá uvést v život řadu např. netechnických organizačních opatření. Nechci na tomto místě navádět k "nedodělkům", ale ze zkušenosti připojuji, že je třeba vždy dobře zvážit, kam až je možné původní termíny posunout. Rozhodně díky zpřesňovanému harmonogramu je v každém okamžiku implementace zřejmé, jak práce postupují a co ještě zbývá. Je tedy možné "plánovaně" řídit přesun implementace některých organizačních opatření až na pozdější dobu. Vlastní implementace končí provedením akceptačních bezpečnostních testů majících za úkol přesvědčit a dokumentovat, že zvláště požadovaná technická opatření byla implementována správně, v požadovaném rozsahu a plně v souladu s bezpečnostní dokumentací.

Provozování, kontrola a vyhodnocení

Bezpečnostní systém je předán do provozu a podřízen periodické kontrole, zda realizovaná a implementovaná opatření bezpečnostních politik pracují efektivně a v souladu s tím, jak byla zamýšlena. Postupně jsou procházeny jednotlivé oblasti řešené v bezpečnostních politikách, případné odchylky jsou dokumentovány a odstraňovány nápravnými akcemi. Po jejich vyhodnocení v širším kontextu bezpečnostních politik pak dochází i k případným úpravám příslušných částí bezpečnostního projektu. Vykazuje-li bezpečnostní systém uspokojivý stav, je třeba věnovat se měnícím se podnikatelským požadavkům dané organizace, zachycovat a vyhodnocovat technologické změny a periodicky zkoumat stav hrozeb a zranitelností.

Závěr

Bezpečnostní systém představující správně vytvořené, realizované a do každodenního fungování organizace implementované bezpečnostní politiky se stává pevným základem funkčního systému řízení bezpečnosti organizace. Je základním prvkem jistoty managementu, že aktiva organizace jsou dostatečně zabezpečena proti poškození nebo zničení.

Vzhledem k narůstajícímu počtu útoků na data a jiná aktiva řady organizací může vést podceňování bezpečnostního systému k vážnému porušování povinností při správě majetku a zanedbávání chování dobrého hospodáře. Následky pak mohou být vážné pro organizaci i její vedení. Aktivní práce zaměřené na vybudování bezpečnostního systému organizace jsou tak pozitivním krokem managementu k zajištění aktiv organizace a čistého svědomí vzhledem k řešení potenciálních rizik. Informace o vytvoření bezpečnostního systému se v současnosti stává konkurenční výhodou na trhu, která deklaruje kvalitu firmy.

Příloha č.2 Druhy připojení k Internetu:

Převzato ze serveru http://tutorialy.lupa.cz/internetove-pripojeni

Komutované připojení

Dočasné připojení k Internetu je zpravidla realizováno pomocí telefonních linek, ať již analogových, digitálních či prostřednictvím mobilní telefonní sítě.

Dial-up

Za dial-up (tedy vytáčenou linku) je považováno připojení k Internetu přes analogovou, tedy klasickou telefonní linku. Pro připojení stačí pouze speciální zařízení, které zabezpečuje přenos dat pomocí telefonní linky, tzv. modem, a přístupové konto u některého z ISP. To lze získat i zdarma, takže uživatel platí pouze telekomunikační poplatky za dobu připojení. Tyto poplatky jsou řízeny speciálními internetovými tarify. Přenosová rychlost dosahuje až 56 kbit/s v závislosti na kvalitě telefonní linky.

ISDN

Připojení předpokládá vlastnictví speciální digitální telefonní linky ISDN, kterou lze získat buď novou instalací, nebo převedením z klasické analogové. Převedení na ISDN linku navíc není příliš nákladné. Pro připojení k Internetu se používá tzv. ISDN karta, která propojuje počítač se sítí ISDN. Poplatky jsou shodné jako u klasické telefonní linky, a to včetně nabídky připojení zdarma. Přenosová rychlost je 64 kbit/s (či 128 kbit/s, kde je však nutno počítat nejen s dvojnásobnou rychlostí, ale také dvojnásobnými telefonními poplatky).

Mobilní

Mobilní připojení je určeno pro uživatele, kteří potřebují mít přístup k Internetu z prakticky kteréhokoliv místa. Vše je vázáno pouze na signál příslušné mobilní sítě. Pro přístup je nutné

vlastnit telefon podporující potřebné datové služby či speciální modem, aktivovat tyto služby u mobilního operátora a v případě připojení pomocí telefonu zakoupit propojovací kabel (případně komunikovat prostřednictvím infračerveného portu), jehož součástí je i potřebný software. Připojení k Internetu pak zpravidla zajišťují přímo mobilní operátoři. Existuje několik technologií pro přístup, které umožňují nejen tarifikaci za dobu připojení, podle objemu přenesených dat, ale také měsíčním paušálem. Přenosové rychlosti se pohybují od 9,6 kbit/s po 115 kbit/s a v budoucnu se budou pohybovat až v řádu Mbit/s.

Pevné připojení

Druhů pevného připojení je mnoho, respektive trvalý datový okruh (tedy fyzickou trasu, po které jsou přenášena data a jež je základem pevného připojení) lze vybudovat řadou způsobů. Nejčastěji jsou to drátová vedení, stále více se však prosazují i optické kabely a především bezdrátové spoje včetně satelitních. V zásadě se liší pouze způsobem, jakým je uživatel propojen se svým poskytovatelem Internetu. Způsob zpoplatňování a další vlastnosti pak bývají stejné či velmi podobné u všech typů připojení.

Pronajatý datový okruh

Pod tímto pojmem se po fyzické stránce skrývá celá skupina různých způsobů připojení. Zákazník je zpravidla připojen drátovým či optickým vedením, případně variantou bezdrátového připojení. Základní vlastností je právě vysoká spolehlivost a bezpečnost služeb. Datový okruh je poskytován zpravidla některou telekomunikační společností; tento typ připojení lze bez problémů realizovat ve všech větších městech. Veškerá potřebná zařízení včetně jejich instalace většinou dodává telekomunikační společnost a poskytovatel Internetu. Uživatel platí jak za samotné připojení k Internetu, tak za pronájem datového okruhu. Přenosová rychlost se v závislosti na použité technologii pohybuje od několika desítek kb/s až po rychlosti v řádu Gbit/s.

Bezdrátové připojení

Je považováno za svým způsobem nouzové řešení, které se používá především tam, kde není buď možné či ekonomicky výhodné využít pronajatého datového okruhu. Základním předpokladem je přímá viditelnost mezi anténou poskytovatele Internetu a zákazníkem. Zákazník tedy může využít pouze služeb těch ISP, jejichž antény vidí z místa, kde bude umístěna jeho anténa. Kromě nákupu či pronájmu potřebných zařízení však uživatel nemusí platit pravidelný měsíční poplatek za pronájem přenosové linky - platí tedy pouze za služby přístupu k Internetu. Přenosové rychlosti se mohou pohybovat od několika desítek kbit/s po jednotky či desítky Mbit/s.

DSL technologie

Technologie digitálních účastnických linek (Digital Subscriber Line, tedy DSL) dokáže doslova vyždímat z klasických telefonních vedení vysoké přenosové rychlosti. Přenos dat je prováděn prostřednictvím modemů mezi uživatelem a telefonní ústřednou, odkud jsou data pomocí vlastní digitální sítě přenášena dále. Existuje několik technologií, v České republice je v současné době používáno tzv. ADSL. Plnému využití, které umožní až silná konkurence, však stále brání spory související s liberalizací trhu. Přenosové rychlosti se pohybují v závislosti na použité technologii a především délce linky (jak daleko je uživatel od ústředny) od stovek kb/s po desítky Mbit/s.

Kabelová televize

Pro připojení k Internetu lze s úspěchem využít také rozvody kabelové televize. Přípojka je osazena speciálními kabelovými modemy, které umožňují pomocí kabelové televize nejen sledovat televizní programy, ale také umožnit vysokorychlostní přístup k Internetu. Podmínkou je poskytování těchto služeb společností provozující tyto služby v dané lokalitě. Přenosová rychlost se pohybuje od desítek kb/s do přibližně 10 Mbit/s.

Satelit

Satelitního přístupu k Internetu je využíváno především všude tam, kde není možno zajistit jiný způsob připojení. Je totiž dostupné prakticky všude. V České republice je však také využíváno místo klasických způsobů připojení kvůli jejich problematické dostupnosti a cenám. Existují různé způsoby - buď jednosměrný přístup, kdy uživatel může data pouze přijímat a pro jejich odesílání musí vlastnit ještě jiné připojení k Internetu, nebo systémy schopné komunikovat oběma směry. Základní nevýhoda je dána vlastností satelitu. Signál musí překonat obrovské vzdálenosti, což představuje zpoždění při komunikaci přibližně čtvrt sekundy. Na rozdíl od jiných způsobů připojení, kdy odpověď na požadavek můžeme dostat za několik milisekund, to u satelitu může být více než půl sekundy! Náklady na připojení však bývají s výjimkou zřizovacích poplatků a s ohledem na přenosovou rychlost poměrně nízké. Přenosová rychlost se pohybuje od několika stovek kbit/s po desítky Mbit/s.

Silové rozvody

O využití silových rozvodů, tedy především elektrických vedení, pro přístup k Internetu se mluví již velmi dlouho. Tento typ připojení je však stále spíše testován než seriózně používán. V České republice zatím tyto služby představeny nebyly a je také dosti pravděpodobné, že se tak v dohledné době nestane. Přenosová rychlost se pohybuje nejčastěji kolem 10 Mbit/s.

Příloha č.3 Seznam služeb předdefinovaných ve WinRoute:

Jméno	Protokol	Zdrojový port	Cílový port	Popis
Any ICMP	ICMP	Libovolný	Libovolný	All ICMP Messages
BGP	TCP/UDP	Libovolný	179	Border Gateway Protocol
CITRIX	TCP	Libovolný	1494	Access To CITRIX Server From Internet
COFS	TCP	Libovolný	6000	ISS OrangeWeb Filter Service
CVS	TCP	Libovolný	2401	Concurrent Versions System (cvspserver)
DC++	TCP	Libovolný	411	Direct Connect Hub
DHCP/BOOTP	UDP	Libovolný	67-68	Dynamic Host Configuration Protocol/Bootstrap Protocol
DNS	TCP/UDP	Libovolný	53	Domain Name Service
eDonkey	TCP/UDP	Libovolný	4661-4665	eDonkey Peer-to-Peer Network
EGP	8	Libovolný	Libovolný	Exterior Gateway Protocol
Finger	TCP	Libovolný	79	Finger user information protocol
FTP	TCP	Libovolný	21	File Transfer Protocol
FTPS	TCP	Libovolný	989-990	FTP - Secured
Gnutella	TCP/UDP	Libovolný	6345-6349	Gnutella (Bearshare, Limewire) Peer-to-Peer Net.
Gopher	TCP	Libovolný	70	Internet Gopher
GRE	47	Libovolný	Libovolný	Generic Routing Encapsulation
H323	TCP	Libovolný	1720	H.323 Protocol
HTTP	TCP	Libovolný	80	HyperText Transfer Protocol - WWW
HTTP Proxy	TCP	Libovolný	3128	HTTP Proxy Server
HTTPS	TCP	Libovolný	443	HyperText Transfer Protocol - Secured
ICQ	TCP	Libovolný	5190	ICQ Instant Messaging
Ident	TCP	Libovolný	113	Ident
IKE	UDP	Libovolný	500	Internet Key Exchange
IMAP	TCP	Libovolný	143	Internet Mail Access Protocol
IMAPS	TCP	Libovolný	993	Internet Mail Access Protocol - Secured
InterBASE	TCP	Libovolný	3050	Borland InterBase
IPINIP	4	Libovolný	Libovolný	IP in IP
IPSec	50	Libovolný	Libovolný	IP Encapsulating Security Payload
IRC	TCP	Libovolný	6666-6668	Internet Relay Chat
Kazaa	TCP/UDP	Libovolný	1214	Kazaa Peer-to-Peer Network
KDS Admin	TCP/UDP	Libovolný	44335	Kerio Desktop Security Server Administration
Kerberos	TCP/UDP	Libovolný	88,749	Kerberos Network Authentication Service
Kerio VPN	TCP/UDP	Libovolný	4090	Kerio Virtual Private Network Service
KMS Admin	TCP/UDP	Libovolný	44337	Kerio Mail Server Administration
KNM Admin	TCP/UDP	Libovolný	44336	Kerio Network Monitor Administration
KPF Admin	TCP/UDP	Libovolný	44334	Kerio Personal Firewall Administration
KSF Admin	TCP	Libovolný	44340	Kerio ServerFirewall Administration
KSF CM	TCP/UDP	Libovolný	44339	Kerio ServerFirewall Central Management

KWF Admin	TCP/UDP	Libovolný	44333	Kerio WinRoute Firewall Administration
KWF Web Adm	TCP	Libovolný	4080	WinRoute web administration interface
KWF Web Admin-SSL	TCP	Libovolný	4081	WinRoute web administration interface - Secured
L2TP	UDP	Libovolný	1701	L2F/L2TP tunnel
LDAP	TCP	Libovolný	389	Lightweight Directory Access Protocol
LDAPS	TCP	Libovolný	636	Lightweight Directory Access Protocol - Secured
Lotus Notes	TCP	Libovolný	1352	IBM Lotus Notes software
Microsoft-DS	TCP	Libovolný	445	Microsoft Networking
MMS	TCP	Libovolný	1755	Microsoft Media Server Protocol
MS-SQL	TCP/UDP	Libovolný	1433-1434	Microsoft SQL Server and Monitor
MySQL	TCP	Libovolný	3306	MySQL DB Server
NetBIOS-DGM	UDP	Libovolný	138	NetBIOS Datagram Service
NetBIOS-NS	TCP/UDP	Libovolný	137	NetBIOS Name Service
NetBIOS-SSN	TCP	Libovolný	139	NetBIOS Session Service
NetMeeting	TCP	Libovolný	1503	Microsoft NetMeeting
NNTP	TCP	Libovolný	119	Network News Transfer Protocol
NNTPS	TCP	Libovolný	563	Network News Transfer Protocol - Secured
NTP	UDP	Libovolný	123	Network Time Protocol
PC Anywhere	TCP/UDP	Libovolný	5631-5632	Access to PC Anywhere From Internet
Ping	ICMP	Libovolný	Libovolný	ICMP Echo Request
POP3	TCP	Libovolný	110	Post Office Protocol
POP3S	TCP	Libovolný	995	Post Office Protocol - Secured
Postgres	TCP	Libovolný	5432	Postgres DB Server
PPTP	TCP	Libovolný	1723	Point-to-Point Tunneling Protocol
RADIUS	UDP	Libovolný	1812-1813	Remote Authentication Dial In User Service
RAP	TCP	Libovolný	7070	Real Audio Protocol
RDP	TCP	Libovolný	3389	Remote Desktop Protocol
RSVP	UDP	Libovolný	1698-1699	Resource Reservation Protocol
RTSP	TCP	Libovolný	554	Realtime Streaming Protocol
SCCP	TCP	Libovolný	2000	Skinny Client Control Protocol
SIP	UDP	Libovolný	5060	Session Initiation Protocol
SMTP	TCP	Libovolný	25	Simple Mail Transfer Protocol
SNMP	UDP	Libovolný	161	Simple Network Management Protocol
SNMP-Traps	UDP	Libovolný	162	Simple Network Management Protocol - Traps
Socks	TCP	Libovolný	1080	Firewall security protocol
SSH	TCP	Libovolný	22	Secure Shell
Syslog	UDP	Libovolný	514	Systém Logging Utility
Telnet	TCP	Libovolný	23	Telnet
Telnets	TCP	Libovolný	992	Telnet - Secured
UPnP	TCP/UDP	Libovolný	1900,2869	Universal Plug and Play Protocol
VNC	TCP	Libovolný	5900	Virtual Network Computing
Win. Messenger	TCP/UDP	Libovolný	1863,7001	Windows Messenger
WINS	TCP/UDP	Libovolný	1512	Microsoft Windows Internet Name Service

Příloha č.4 Seznam agend vedených obecním úřadem v Kněžicích

- Pronajímá bytové a nebytové prostory
- Pronajímá hrobová místa
- Provádí ověřování shody opisu nebo kopie s listinou a ověřování pravosti podpisu
- Přijímá nájemné z bytových a nebytových prostor ve vlastnictví obce
- Přijímá návrhy na vyhlášení místního referenda
- Přijímá oznámení o shromáždění
- Přijímá poplatky za pronájem hrobového místa
- Přijímá poplatky za znečištování ovzduší
- Přijímá přihlášení k trvalému pobytu a ohlášení změny místa trvalého pobytu
- Přijímá žádosti k instalování kamerového systému
- Přijímá žádosti o kácení dřevin rostoucích mimo les
- Přijímá žádosti o neinvestiční dotace v oblasti sportu
- Přijímá žádosti o povolení k provozování výherních hracích přístrojů
- Určuje popisná, orientační, evidenční čísla budov v obci
- Vybírá poplatky za provoz systému shromažďování, sběru, přepravy, třídění, využívání a odstraňování komunálních odpadů
- Vybírá poplatky za provozování výherních hracích přístrojů
- Vybírá poplatky za rekreační pobyt
- Vybírá poplatky za užívání veřejného prostranství
- Vybírá poplatky za zhodnocení stavebního pozemku možností jeho připojení na stavbu vodovodu nebo kanalizace
- Vybírá poplatky ze psů
- Vydává platební výměry na neuhrazené místní poplatky
- Vydává řády pro místní veřejné pohřebiště, jehož je provozovatelem
- Vydává vyhlášku o čistotě a pořádku v obci
- Vydává vyhlášku o chovu a držení zvířat na území obce
- Vydává vyhlášku o nakládání s odpady, zřizuje a provozuje skládky odpadů (obecní skládky)
- Vydává vyhlášku o územních zónách pro výpočet daně z nemovitostí
- Vydává vyhlášku o výši příspěvku na částečnou úhradu nákladů mateřské školy patřící pod správu obce
- Vyhlašuje varovný signál Všeobecná výstraha

Matrika

- Provádí zápisy do knihy manželství
- Provádí zápisy o určení otcovství souhlasným prohlášením rodičů
- Přijímá doklady k uzavření manželství
- Přijímá nalezené občanské průkazy a další potvrzení, občanské průkazy zemřelého
- Přijímá občanské průkazy do úschovy
- Přijímá oznámení o narození dítěte a provádí zápis do knihy narození
- Přijímá oznámení o úmrtí a provádí zápis do knihy úmrtí
- Přijímá oznámení o užívání české podoby cizojazyčného jména
- Přijímá oznámení o znovu přijetí předchozího příjmení po rozvodu

- Přijímá oznámení týkající se občanského průkazu, v daných případech přijímá občanský průkaz, vyzývá k vyzvednutí občanského průkazu
- Přijímá prohlášení o užívání dvou jmen
- Přijímá prohlášení o užívání pouze jednoho příjmení
- Přijímá prohlášení o volbě druhého jména
- Přijímá protokoly o uzavření církevního sňatku
- Přijímá souhlasné prohlášení osvojitelů o zvolení jména pro osvojence
- Přijímá žádosti o nahlédnutí do matriční knihy, vystavení matričního dokladu a vydává výpisy z matrik (rodné, oddací, umrtí listy)
- Přijímá žádosti o provedení zápisu příjmení ženy do matriční knihy
- Přijímá žádosti o uzavření manželství, zajišťuje svatební obřad
- Přijímá žádosti o vydání matričních dokladů (rodného, oddacího, úmrtního listu)
- Přijímá žádosti o vydání občanského průkazu
- Přijímá žádosti o vydání osvědčení a potvrzení o státním občanství České republiky
- Přijímá žádosti o vydání osvědčení o splnění požadavků zákona o rodině pro uzavření církevního sňatku
- Přijímá žádosti o vydání výpisu z evidence Rejstříku trestů
- Přijímá žádosti o vydání vysvědčení o právní způsobilosti k uzavření manželství v cizině
- Přijímá žádosti o vystavení osvědčení o státním občanství při vydání prvního občanského průkazu
- Přijímá žádosti o vysvědčení o právní způsobilosti k uzavření manželství
- Přijímá žádosti o zápis do zvláštní matriky
- Přijímá žádosti o zápis narození, uzavření manželství, úmrtí státních občanů ČR do zvláštní matriky v Brně
- Přijímá žádosti o zápis příjmení v matriční knize v mužském tvaru
- Přijímá žádosti o změnu jména nebo příjmení
- Přijímá žádosti o změnu příjmení za trvání manželství
- V daných případech zadržuje občanský průkaz
- Vede sbírku listin a matriční knihy narození, uzavření manželství a úmrtí
- Vydává občanský průkaz
- Vydává oddací listy
- Vydává osvědčení a potvrzení o státním občanství České republiky a zjišťuje státní občanství České republiky
- Vydává osvědčení pro uzavření církevního sňatku
- Vydává potvrzení o občanském průkazu
- Vydává potvrzení o skutečnostech zapsaných v matriční knize
- Vydává rodné listy
- Vydává úmrtní listy
- Vydává vysvědčení o právní způsobilosti k uzavření manželství v cizině

Příloha č.5 Stručný přehled licenčních programů společnosti Microsoft

	Krabice	OEM Nákup s hardware	MOL Microsoft Open License	OSL Open Subscription License	MYO Multi-Year Open	Select License	Enterprise Agreement	Enterprise Agreemnet Subscription
Velikost zákazníka	1 a více počítačů		5 a více počítačů	5 a více počítačů	5 a více počítačů	1500 a více bodů	250 a více počítačů	250 a více počítačů
Licence	trvalá	trvalá licence vázaná na harware	trvalá	dočasná pronájem licence	trvalá			dočasná pronájem licence
Produkty	Většina softwarových produktů společnosti Microsoft	Vybrané softwarové produkty společnosti Microsoft	**Open Business** Většina softwarových produktů společnosti Microsoft **Open Volume** 3 skupiny : aplikace operační systémy servery (* každá licence je bodově ohodnocená)	**Platformové produkty:** Windows Professional Upgrade Office Professional Core CAL **+ doplňkové produkty**	**Platformové produkty:** Desktop platform: Windows Professional Upgrade Office Professional Core CAL Další platformové produkty: Office Standard Windows CAL Exchange CAL **+ doplňkové produkty**	**3 skupiny :** aplikace operační systémy servery (* každá licence je bodově ohodnocená)	**Enterprise Platform:** Windows Professional Upgrade Office Professional Core CAL **+ doplňkové produkty**	**Enterprise Platform:** Windows Professional Upgrade Office Professional Core CAL **+ doplňkové produkty**
Instalační média	V ceně	N/A	Není zahrnuto v ceně (Nutno objednat zvlášť)	V ceně	V ceně	V ceně	V ceně	V ceně
Software Assurance	Možnost zakoupit ve vybraném multilicenčním programu		Možnost zakoupit při první objednávce	Součást programu		Možnost dokoupit	Součást programu	Součást programu
Garance ceny	Není		Není	3 roky		není	3 roky	3 roky
Způsob platby	při nákupu			3 roční platby	3 roční platby	Měsíční platby za nově instalovaný software	3 roční platby	3 roční platby
Cenové úrovně	není		**Open Business** 5 a více licencí **Open Volume** B (od 150 - 499 bodů / skupinu) C (od 500 bodů / skupinu)	**3 cenové úrovně** A (5 – 49 počítačů) B (50 – 249 počítačů) C (250 a více počítačů)	**Desktopové produkty:** A (5 – 49 počítačů) B (50 – 249 počítačů) C (250 a více počítačů) **Doplňkové produkty:** A (5 a více počítačů)	**podle počtu bod**ů A (1 500 - 11 999 bodů) B (12 000 - 29 999 bodů) C (30 000 - 74 999 bodů) D (75 000 a více bodů)	**4 cenové úrovně** A (250 – 2 399 počítačů) B (2 400 – 5 999 počítačů) C (6 000 – 14 999 počítačů) D (15 000 a více počítačů)	**4 cenové úrovně:** A (250 - 2399 počítačů) B (2 400 - 5 999 počítačů) C (6 000 - 14 999 počítačů) D (15 000 a více počítačů)
Objednávka	podle potřeby			roční		měsíční	roční	
Zvyšování počtu licencí				max. o 100% / rok		povinnost splnit předpokládanou výši odběru	podle potřeby	