Technická univerzita v Liberci

Hospodářská fakulta

Studijní program: Systémové inženýrství a informatika (6209R)

Studijní obor: Podnikatelská informatika

Bezpečnostní rizika připojení k Internetu a jejich řešení

Security risks of connecting to the Internet and their solutions

BP-MI-KIN-2005 14

Pavel STARÝ

Vedoucí práce: **Ing. Klára Antlová, Ph.D.** (KIN)

Konzultant: **Ing. Jaroslav Ploc** (OR-CZ spol. s r. o.)

Počet stran: 55 Počet příloh: 0

Datum odevzdání: 7. 1. 2005

Katedra informatiky **Školní rok 2004/2005**

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

pro:

Pavel Starý

Studijní program:

Systémové inženýrství a informatika (6209R)

Studijní obor č. 62 - 53 - 705

Podnikatelská informatika

Vedoucí katedry Vám ve smyslu zákona č. 111/1998 Sb. o vysokých školách a navazujících předpisů určuje tuto bakalářskou práci:

Název tématu:

Bezpečnostní rizika připojení k Internetu a jejich řešení

Zásady pro vypracování:

- Analýza problematiky informační bezpečnosti při práci v datových sítích
- Možnosti napadení a následky zanedbání informační bezpečnosti
- Návrh na zlepšení datového zabezpečení při připojení ke vzdálené síti
- Hodnocení navrženého řešení

Rozsah bakalářské práce : 25-30 stran
(do rozsahu nejsou započítány úvodní listy, přehled literatury a přílohy).

Doporučená literatura:

DOBDA, L: Ochrana dat v informačních systémech. Grada, Praha 1998
LÁTAL, I: Ochrana informací, dat a počítačových systémů. Eurounion, Praha 1996
RODRYČOVÁ, D; STAŠA, P: Bezpečnost informací jako podmínka prosperity firmy, Grada, Praha 2000
CURTIS, G.: Business Information Systems, 3-rd edd., Addison-Wesley, 1999

Vedoucí bakalářské práce: Ing. Klára Antlová, Ph.D.

Odborný konzultant: Ing. Jaroslav Ploc

Termín odevzdání bakalářské práce: 7.1.2005

Prof. Ing. Jan Ehleman, CSc.
vedoucí katedry

Prof. Ing. Jiří Kraft, CSc.
děkan Hospodářské fakulty

Prohlášení

Byl jsem seznámen s tím, že na mou bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, zejména § 60 - školní dílo.

Beru na vědomí, že Technická univerzita v Liberci (TUL) nezasahuje do mých autorských práv užitím mé bakalářské práce pro vnitřní potřebu TUL.

Užiji-li bakalářskou práci nebo poskytnu-li licenci k jejímu využití, jsem si vědom povinnosti informovat o této skutečnosti TUL; v tomto případě má TUL právo ode mne požadovat úhradu nákladů, které vynaložila na vytvoření díla, až do jejich skutečné výše.

Bakalářskou práci jsem vypracoval samostatně s použitím uvedené literatury a na základě konzultací s vedoucím bakalářské práce a konzultantem.

Datum: 7. 1. 2005

Podpis: .....

BAKALÁŘSKÁ PRÁCE

TÉMA: **Bezpečnostní rizika připojení k Internetu a jejich řešení**

RESUMÉ:

Bakalářská práce se zabývá problematikou informační bezpečnosti při práci v datových sítích. Rozebírá princip bezpečnostních rizik a poukazuje na možnosti napadení a následky zanedbání informační bezpečnosti. Dále shrnuje možnosti a způsoby zabezpečování počítačových sítí. Součástí práce je návrh datového zabezpečení středně velké počítačové sítě při připojení ke vzdálené síti. Za příklad pro řešení práce zvažuje návrh sítě, která má jedno připojení k Internetu a okolo dvaceti vnitřních uživatelů. Návrh řešení vychází z předpokladu, že bude sestavena celá síť. Hlavními body řešení je vytvoření striktní bezpečnostní politiky a návrh struktury sítě včetně jejího zapojení, vytvoření pravidel pro datový provoz a volby vhodného softwaru. Cílem návrhu je předložit strukturu sítě představující vyvážené řešení mezi bezpečností a riziky.

THEME: **Security risks of connecting to the Internet and their solutions**

SUMMARY:

Baccalaureate work is concerned with problems of an information security at work in data networks. It analyses a tenet of security risks and it refers to the possibilities of attacks and the aftermath of omission of the informaction security. Further it summarises the ways and means of securing the computer networks. The work contains a project of data securing of a medium sized computer network connected to a remote network. For instance for solution the work considers a project of a net, which has one interface to the Internet and about 20 inner users. The suggested solution comes out from presumption that the whole network will be built-up. The main points of the solution are creation of the strict security policy and the proposal of network desing including its connection, creation of data traffic rules, and selection of suitable software. The objective of the project is to propose the network design presenting well-balanced solution between safety factor and risks.

OBSAH

SEZNAM POUŽITÝCH SYMBOLŮ A ZNAČEK

Zkratka	Popis
ICT	informační a komunikační technologie
IP	Internet Protocol
TCP	Transmission Control Protocol (protokol kontroly přenosu)
FTP	File Transfer Protocol (protokol přenosu souborů)
DoS	Denial of Service (odmítnutí služby)
SW	software
HW	hardware
IDS	Intrusion Detection System (systém detekce útoků)
VPN	Virtual Private Network (virtuální privátní síť)
IDP	Intrusion Detection and Prevention (systém detekce a prevence útoků)
URL	Unique Resource Locator (adresa zdroje)
WWW	World Wide Web
ISO/OSI	International Standards Organization / Open System Interconnection (referenční komunikační model)
DMZ	Demilitarizovaná Zóna
HTTP	Hypertext Transfer Protocol
POP3	Post Office Protocol, verze 3 (protokol přenosu zpráv směrem k uživatelské složce)
CVP	Content Vectoring Protocol
SMTP	protokol přenosu zpráv
DNS	Domain Name Server (převaděč DNS adres na číselné IP adresy)
ISP	Internet Service Provider (poskytovatel internetových služeb)
IPS	Intrusion Prevention Systém (systém detekce a prevence útoků)
OS	operační sytém
NAT	Network Address Translation (překladač síťových adres)

ÚVOD

Námět na téma bakalářské práce pochází od společnosti OR-CZ, spol. s r. o. Tato firma je jedním z prvních systémových integrátorů - dodavatelů komplexních informačních technologií. Široký okruh jejích podnikatelských aktivit je zaměřen na komplexní problematiku informačních a komunikačních technologií (ICT) a oblastí, které s nimi bezprostředně souvisí. V prostředí konkurenčního boje význam informací stále vzrůstá. Ochrana počítačových systémů – informací a dat – je tak nutností.

Zabýváme-li se informacemi, které mají nějakou hodnotu danou tržními vztahy – nazveme je informační aktiva. Taková aktiva, nehledě na jejich využití, prostě existují a mohou se stát terčem útoku či zneužití – tzv. čelí hrozbám. Proto je zapotřebí věnovat se bezpečnostním opatřením. Nic není dokonalé a tyto opatření mohou mít své slabiny. Z toho důvodu je součástí zabezpečení také instalace protiopatření eliminujících známé slabiny.

Bakalářská práce se v souladu se zadáním člení do čtyř hlavních kapitol. V první kapitole je proveden rozbor současného stavu. V druhé kapitole je zpracováno analytické řešení problematiky s uvedením možných teoretických variant. Následující třetí kapitola předkládá vlastní návrh řešení včetně technického a ekonomického hodnocení. Závěrečná kapitola obsahuje jasně a logicky vyjádřené dosažené výsledky včetně závěru.

1. ROZBOR SOUČASNÉHO STAVU

Tato kapitola se zabývá analýzou problematiky informační bezpečnosti při práci v datových sítích.

1.1. ANALÝZA BEZPEČNOSTI NA INTERNETU

1.1.1. Původ problémů s bezpečností

Internet v dnešní podobě je prostředí, od kterého lidé čekají více než pro co byl původně stvořen. Využívá se pro obchodní transakce, on-line platby, komunikaci a pro mnohé další činnosti. Od Internetu se přitom očekává korektnost a důvěryhodnost – například, že se svěřená informace nedostane do nepovolaných rukou a je jistým způsobem zabezpečená.

V době, kdy vznikal (kdy vznikaly protokoly TCP/IP, na kterých dodnes funguje), se však nepředpokládalo, že se budou Internetu svěřovat důvěrné informace, ani že na něj budou kladeny rozsáhlé bezpečnostní požadavky. Úkolem autorů protokolů TCP/IP bylo vyvinout je tak, aby byly robustní (tj. odolné vůči poruchám) a efektivní, což se jim podařilo. S efektivitou souvisí také snaha autorů TCP/IP a Internetu o jednoduchost a minimum funkcí (jen ty, u kterých se očekává, že je všichni uživatelé budou potřebovat) s tím, že další funkce se budou implementovat volitelně na úrovni vyšších vrstev. Důsledkem je relativní jednoduchost a rychlost infrastruktury. Zabudování zabezpečujících mechanismů do vrstev by mělo za následek zdražení infrastruktury a její zpomalení. S tím by souvisel i pomalejší rozvoj.

Není proto na místě vytýkat Internetu, že není bezpečný. Navíc je zde možnost implementovat bezpečnost do Internetu tak, aby to nezatížilo existující aplikace a přineslo to bezpečnost těm aplikacím, které ji skutečně potřebují. Nicméně je fakt, že dodatečná implementace mechanismů na vyšších vrstvách je

méně efektivní než kdyby byly standardní součástí. Internet ale vděčí za svůj úspěch rozumné volbě kompromisů mezi faktory (efektivnost, míra zátěže, ...).

1.1.2. Důvody nebezpečí v Internetu

Je dobré si uvědomit, v jakém smyslu není Internet bezpečný. Mimo to, že problémům s bezpečností napomáhá jeho neurčitá vlastnická struktura a tedy fakt, že neexistují žádné závazné normy chování (až na některé standardy), lze důvody rozdělit na chování přenosových mechanismů a na chování aplikačních služeb.

Protokol IP

Protokol IP (Internet Protocol) je hlavním přenosovým protokolem síťové vrstvy. IP člení data na bloky označované jako pakety (IP datagramy), které přenáší nezávisle na sobě (nespojovaně = connectionless). Na každém uzlu se rozhoduje kudy půjde dál (každý datagram může jít jinou cestou). Ačkoli je to ideální pro robustnost a pro vyrovnání se s výpadky v síti, nelze tak předem zabezpečit přenosovou trasu. Další vlastností protokolu IP je nespolehlivost a to v tom smyslu, že data jsou kontrolována, zda nejsou po cestě poškozena – ale pokud zjistí, že jsou, nestará se o nápravu a pokračuje dál.

Data navíc nejsou kódována ani šifrována. Avšak to lze vyřešit kombinací řešení na transportní a aplikační vrstvě. Na transportní vrstvě je možné využít služeb protokolu TCP, jenž mění nespojované a nespolehlivé fungování protokolu IP na spolehlivé a spojované. Na aplikační vrstvě je pak potřeba zajistit vhodné zabezpečení (šifrování, kódování, ...).

Chování aplikací

To je druhým zdrojem nízké bezpečnosti dnešního Internetu. Některé aplikace totiž vychází z předpokladu, že se uživatelé chovají korektně. Jako příklad si uveďme situaci, kdy služby, které potřebují znát identitu uživatele (FTP, Telnet, ...), přenáší příslušné ID údaje a hesla v nezakódované podobě jako čistý

text – čímž je činní snadným terčem k odposlechu. Popřípadě u elektronické pošty není složité zfalšovat hlavičky e-mailu.

1.1.3. Požadavky na bezpečnost

V dnešní době se Internet používá k mnoha účelům a je samozřejmostí, že je zapotřebí dostatečná míra zabezpečení, spolehlivosti, věrohodnosti a další aspekty. Významným se stává elektronický obchod realizovaný v prostředí Internetu a mnohé další činnosti v oblasti informační společnosti. Je dobré si tedy specifikovat, co je zapotřebí, abychom mohli považovat Internet za dostatečně bezpečné a spolehlivé prostředí.

Identifikace a autentikace (identification, authentication): Identifikace slouží ke zjištění autora, původce, iniciátora atd. určité aktivity (např. u zpráv elektronické pošty je "identifikací" zjištění odesilatele z hlaviček přijaté zprávy). Autentikace ověří, že příslušné údaje "sedí" (neboli, u emailové zprávy, že odesilatelem je skutečně ten, kdo je uváděn jako autor).

Autorizace (authorization, access control): Oprávnění pro přístup k určitému zdroji či k provedení určité aktivity. Cílem je realizovat "přístupovou politiku", v rámci které mají různí uživatelé různá oprávnění.

Integrita dat (integrity): Obsah dat přenášených či alespoň zpřístupňovaných prostřednictvím Internetu může být různým způsobem pozměněn oproti stavu, kdy jej autor vytvořil - například v důsledku chyb při přenosu nebo v důsledku toho, že někdo jiný než původní autor tato data z nějakého důvodu pozměnil (data tím ztratí integritu). Snaha o zachování integrity se často redukuje na možnost spolehlivě určit, zda nedošlo ke změně dat. Dát tak uživateli jistotu, že data byla doručena nezměněná.

Důvěrnost dat (confidentiality): Zajištění důvěrnosti dat znamená zabezpečit je proti tomu, aby si je mohl přečíst někdo, kdo k tomu není oprávněný. V praxi je

toho typicky dosahováno zašifrováním dat takovým způsobem, aby zpětné dešifrování mohl provést pouze oprávněný příjemce dat a nikdo jiný.

Neodmítnutelnost (non-repudiation): Aby byla zajištěna věrohodnost úkonů realizovaných v Internetu, je nutné mít možnost prokázat, že jejich autor (původce) je skutečně vykonal a nemohl tak příslušný úkon popřít (odmítnout jeho "autorství").

Dostupnost (availability): Je důležité, aby služby či zdroje, které uživatel potřebuje, byly k dispozici. Pokud tomu tak není, znamená to nedostatek označovaný jako Denial of Service (DoS).

Žurnálování (auditing): Žurnálování zajišťuje zachování určité stopy po každé činnosti. To umožňuje později detekovat, kdo co udělal. Tento fakt hraje důležitou roli při bezpečnostních incidentech. Samotný fakt, že dochází k vytváření stop, může ovlivňovat chování uživatelů.

1.1.4. Možnosti

Možnosti k zajištění požadavků na identifikaci, autentikaci, integritu, důvěrnost a neodmítnutelnost jsou následující.

Symetrické šifrování: Využívá dva identické klíče (pro odesílatele a příjemce) – oba lze použít pro zašifrování i odšifrování. Používá se zejména pro zajištění:

- *důvěrnosti dat* – bez klíče je nikdo neodemkne,
- *identifikace, autentikace* – pouze druhá strana má klíč,
- *neodmítnutelnost* – data může zašifrovat pouze vlastník k líče.

Výhody: oproti asymetrickému šifrování má malou výpočetní náročnost

Nevýhody: manipulace s identickými klíči – pokud se klíč dostane do nepovolaných rukou, zabezpečení se zhroutí

Asymetrické šifrování: Využívá dva nestejné klíče (jeden zůstává utajen jako privátní klíč, druhý je volně k dispozici jako veřejný klíč).

Možnosti – k zašifrování lze použít:

Privátní klíč: Ten má k dispozici jen vlastník – čímž je splněna identifikace, autorizace, integrita a neodmítnutelnost. Odšifrování může provést veřejným klíčem kdokoli, což znamená, že není splněn požadavek na důvěrnost.

Veřejný klíč: Má k dispozici kdokoli – zašifrování může provést také kdokoli. Tím ale nelze splnit požadavek na – autentikaci, neodmítnutelnost, integritu (kdokoli sice nemůže data odšifrovat a pozměnit, ale může je úplně nahradit jinými daty, které korektně zašifruje). Odšifrovat data může však jen vlastník privátního klíče – tím je splněn požadavek na důvěrnost.

Jednorázová hesla: Je běžné, že se používají hesla – tradičně k autentikaci a autorizaci. Hrozí tu možnost zneužití (prozrazení, odposlech) vzhledem k tomu, že tato hesla jsou pak přenášena po nezabezpečené síti nebo jsou svěřována subjektům, které nemusí být vždy zcela důvěryhodné. Z těchto důvodů existuje možnost používat hesla s jednorázovou platností – pro jeden úkon.

Výhody: vyzrazení není nebezpečné – heslo nelze použít opakovaně

Nevýhody: generování hesel – je potřeba dopravit k uživateli vhodný generátor (SW,HW)

1.1.5. Důsledky bezpečnostních rizik v internetu

Každá privátní síť – domácí, firemní či školní – čelí hrozbám, jakmile se k Internetu připojí. Z toho důvodu je zapotřebí zajistit jejich ochranu, aby taková síť obstála před náhodnými či cílenými útoky a „přežila bombardování" virů, různého spywaru a dalších nežádoucích hrozeb, které se potulují Internetem. Podrobnějšími možnostmi komplexního zabezpečení se zabývá druhá kapitola.

1.2. MOŽNOSTI NAPADENÍ

Vnitřní přesvědčení, že zrovna mě napadení nepotká, může mít neblahé následky. Proto je dobré si uvědomit, jaká jsou rizika – v jaké podobě se mohou útoky vyskytnout.

1.2.1. Typy útoků

Následující seznam zmiňuje nejběžnější typy útoků.

DoS útok: Jedná se o útok na určitou službu. Má za následek zahlcení serveru či jeho zhroucení.

Buffer Overflow útok: Jedním z nejčastějších útoků je přetečení zásobníku (buffer overflow attack). Princip spočívá v tom, že funkce aplikace očekává při spojení *n* bytů a pak provede skok nebo návrat do paměťového segmentu, kde běží řídící program. Díky softwarové chybě ale není ošetřen limit počtu bytů. Útoční pak pošle do zásobníku několikanásobné množství dat, dojde k přetečení zásobníku a ke skoku na adresu např. rizikového kódu, jenž útočníkovi umožní spustit jeho příkazy a převzít kontrolu nad počítačem. Proti riziku se samozřejmě bojuje a existují nástroje i doporučení, které mají takové chyby odstranit.

Trojský kůň: Trojský kůň vykonává na počítači nežádoucí činnost, která má ve většině případů destruktivní ráz. Útočník ovládá napadený počítač do té míry, jak mu to program (trojský kůň) umožňuje - manipulovat s cílovým počítačem, získávat z něj soubory, snímat obrazovku, testovat rozsah IP adres, restartovat, pracovat se serverovou částí, zaznamenávat činnost klávesnice, dekódovat uložená hesla, spouštět soubory a provádět další nekalou činnost.

Scannování portů: Je to forma průzkumného útoku, jenž předchází samotnému útoku. Útočník si ověřuje dostupné služby nebo síťové adresy.

V současné době existují volně dostupné „nástroje pro hacking", díky nimž i nezkušení útočníci mohou způsobit značné škody.

1.2.2. Detekce útoků

Možnosti útoků jsou široké a je tak zapotřebí se proti nim řádně zabezpečit. Jedním z prvků jsou IDS sondy – pracující s mechanismem packetsignature, který vyhledává konkrétní řetězce v toku dat. Nevýhodou tohoto mechanismu je, že detekuje pouze známé útoky a navíc může generovat mnoho falešných alarmů, protože uplatňuje nebezpečné řetězce na veškerý provoz. To lze ošetřit mechanismem statefullsignature, jenž detekuje dané řetězce jen v situacích, kdy se může jednat o útok. Tím se redukuje počet falešných alarmů.

Další zajímavou možností pro odražení útoku může být tzv. *honey pot* (doslovně „medová past", což je trefným vyjádřením). Princip spočívá v tom, že útočník je přesměrován na server, který simuluje napadené služby, a ztrácí tak čas dobýváním neexistujících služeb.

Na obranu proti DoS útokům také existují určitá opatření. Principem je ověření, zda proběhly všechny kroky nutné pro sestavení spojení. Obrana pak spočívá v zablokování provozu na základě zdrojové adresy.

1.2.3. Sociální inženýrství

„Sociální inženýrství" je termín pro metodu, jež vede legitimní počítačové uživatele k poskytnutí užitečných informací, které pomáhají útočníkovi získat neautorizovaný přístup do jejich počítačového systému". Tento druh hrozby by neměl být podceňován. Nicméně je to natolik rozsáhlé téma, že se dostává nad rámec mé práce. Proto se odkazuji na literaturu [8] a [9].

2. ANALÝZA ŘEŠENÍ

Tato kapitola se zabývá možnostmi zabezpečení privátní počítačové sítě, které jsou momentálně k dispozici. Někteří lidé se totiž ještě stále domnívají, že pokusy o průnik do sítě se týkají „jen těch druhých". Takový omyl může být velice drahý. I ti více opatrní často počítají s tím, že jim firewall poskytne 100% ochranu. I tento omyl se může nepříjemně prodražit. Bezpečnost sítě je komplexní problematika a řešení se sestává z více komponent – firewall, antivir, VPN, IDS, IDP, URL filter, autentikace atd.

Faktem je, že realita dnešního světa diktuje firmám, aby propojovaly své privátní sítě s veřejným Internetem – ať už pro to, aby umožnily svým uživatelům přístup ke zdrojům Internetu nebo aby umožnily vzdálený přístup do firemní sítě. Nelze však mluvit pouze o firmách, jelikož totéž platí i pro privátní sítě dalších subjektů (školy, úřady). Nelze také opomenout, že se to týká i domácích počítačových sítí.

Opatrnost v této věci je velmi důležitá. Je zapotřebí zhodnotit možná rizika, ohrožení privátní sítě a jejích zdrojů a zajistit takové zabezpečení, které bude vyhovovat a dostačovat našim požadavkům na bezpečnost.

V otázce snahy o vzájemné propojování počítačových sítí figuruje obava jejich provozovatelů z neoprávněného přístupu z Internetu. Obavy z toho, aby se někdo cizí a nepovolaný nedostal ke zdrojům, které se nachází v privátní síti a nejsou určené pro vnější uživatele. Je také nežádoucí, aby někdo zvenku pronikl do připojené sítě a prováděl v ní nežádoucí akce – například smazání či pozměnění dat, provedení či ovlivnění určitých transakcí apod. Způsobů jak realizovat tyto činy je samozřejmě mnoho – ať neoprávněným získáním vzdáleného přístupu nebo nasazením trojských koňů či jiným způsobem.

Možností jak zabezpečit připojované sítě je mnoho. Liší se jak v ceně tak míře zabezpečení. Je dobré si uvědomit, že žádné zabezpečení není nikdy 100%. Asi vždy bude existovat nějaká možnost jak sebelepší zabezpečení prolomit a

pokud s tím budeme trochu počítat, můžeme na to být lépe připraveni. V praxi jde nakonec o určitý kompromis mezi požadovanou mírou zabezpečení a cenovými náklady, které jsme ochotni a schopni investovat. Avšak tento jednoduchý kompromis ještě ovlivňují určité faktory – například zda opatření zpomalují či jinak ztěžují prácí uživatelů zabezpečované sítě. Obecně bychom mohli souhlasit s tvrzením, že čím je větší míra zabezpečení, tím více budou ve svých aktivitách uživatelé omezování.

2.1. ROLE BEZPEČNOSTNÍ POLITIKY

Pokud uvažujeme o zabezpečení a jeho nejvhodnějším řešení, je zapotřebí celkově promyslet a zhodnotit situaci a následně si určit základní požadavky. Zvážit ochotu přijmout a realizovat určitá opatření. Zkrátka si musíme promyslet, co je v sázce, jaká jsou rizika ohrožení a čeho chceme zabezpečením dosáhnout a za jakou cenu.

Toto plánování se týká lidí z celé firemní hierarchie – od vedení až po technické pracovníky a uživatele. S problémy bezpečnosti by se tak měl seznámit každý pracovník. To, čeho bychom měli dosáhnout, je posouzení rizik ohrožení a jakou míru zabezpečení budeme požadovat. Je jasné, že bude zapotřebí brát v úvahu i finanční náklady na pořízení. V praxi si celé plánování můžeme představit jako volbu mezi třemi vytyčenými body – jež si pojmenujme jako riziko, míra zabezpečení a náklady. Ono to však není až tak jednoduše definovatelné, svou roli totiž bude hrát i to, jakou míru omezení, kterými zabezpečení zasáhne do práce uživatelů připojované sítě, budeme schopni přijmout.

Je možné (často spíše velmi pravděpodobné), že firma, která chce svou síť připojit, již provozuje určitý informační systém či jiné citlivé zdroje. V takovém případě se dá očekávat, že firma již má zpracovanou bezpečnostní politiku. Pak připojení sítě k veřejnému Internetu musí vycházet z této bezpečnostní politiky či lépe řečeno – mělo by ji doplňovat.

Každopádně, v této otázce platí osvědčené pravidlo „dvakrát měř, jednou řež". Což si lehce převedeme na „nejprve dobře promysli, a až pak realizuj".

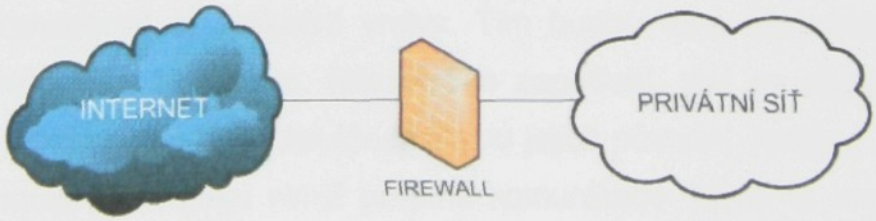
2.2. FIREWALL

Firewall je základním kamenem zabezpečení interní sítě. Obecně se jedná o zařízení provádějící inspekci a analýzu provozu procházejícího přístupovými body do interní (zabezpečované) sítě. Primárním úkolem firewallu je zabránit přístupu neautorizovaným uživatelům. Nejčastěji jsou to řešení kombinující využití programových a technických prostředků (softwaru i hardwaru).

Vedle této primární funkce však dnešní firewally mohou plnit také celou řadu dalších významných funkcí.

2.2.1. Funkce firewallů

Při plánování zabezpečení je dobré přihlédnout k tomu, co všechno by požadované řešení mělo zajišťovat, jaké další funkce by mělo plnit – vedle svého primárního účelu, jímž je ochrana připojované sítě. Vzhledem k tomu, že firewally dokáží plnit i řadu dalších funkci, je vhodné jejich koncepci volnit i s ohledem na to, jaké další funkce by měly být využívány a jaké míře. Pro ilustraci uvedu důležité funkce firewallů:



Obr. č. 1 – Použití firewallu
(vlastní tvorba)

Regulace přístupu - uživatelů privátní sítě do veřejného Internetu. Firma může chtít omezit přístup svých zaměstnanců k určitým serverům či nějakým

způsobem tento přístup regulovat či alespoň evidovat. Může také chtít regulovat určité služby či vázat omezení na konkrétní časové intervaly (na pracovní dobu).

Optimalizace připojení – v rámci firewallu může fungovat cache server, který v sobě uchovává objekty (WWW stránky), jež uživatelé chráněné sítě využívají. Tyto objekty tak stahuje jen při prvním požadavku a při dalších již poskytuje kopii, kterou si uchoval. Tímto způsobem nezatěžuje tolik přípojku a je možné, že tak uživatelům postačí levnější a pomalejší přípojka.

Antivirová ochrana – Zajištění ochrany sítě před virovou nákazou – kontrola elektronické pošty či např. přenos textových souborů s makroviry.

Řešení problému s IP adresami – Problémem Internetu je nedostatek IP adres. Tu musí mít přidělenu každý připojený uzel a musí být unikátní. Nicméně za firewallem se mohou používat i takové IP adresy, jež unikátní nejsou. Odpadá i závislost na providerovi, který připojení poskytuje.

Veřejné zpřístupnění zdrojů – Některé zdroje provozovatelé chráněných sítí mohou chtít zpřístupnit i pro uživatele z vnější sítě – prezentace firmy, obchodní nabídky. To je v rámci firewallu realizováno formou WWW či FTP serveru (přístupným z chráněné sítě i zvenčí).

Zabezpečená komunikace – Data v Internetu nejsou při přenosu nijak zabezpečena proti odposlechu. To je ale možné realizovat na vyšších úrovních – na úrovni transportní či aplikační vrstvy. Tím budou data šifrována ještě před přenosem veřejným Internetem. Nicméně je zapotřebí, aby na druhé straně byl někdo, kdo zakódovaná data dokáže vrátit do jejich původní podoby. Toto v praxi zajišťují koncové uzly, mezi nimiž probíhá komunikace. Může to realizovat také dvojice firewallů, která vytvoří zabezpečený tunel. Skrz Internet tak mohou být propojeny dvě privátní sítě, aniž by si koncové uzly musely uvědomovat existenci zabezpečujících mechanismů a přizpůsobovat se jim. Propojováním tunely mezi firewally lze realizovat celé privátní sítě vedoucí skrz Internet – VPN (Virtual Private Network).

Vzdálený přístup oprávněných uživatelů – Může být žádoucí, aby uživatelé firemních sítí měli přístup ke zdrojům a službám těchto sítí, i když zrovna nejsou ve firmě – jsou například u zákazníka. Firewall jim umožní vzdálený přístup.

2.2.2. Druhy firewallů

Firewally bereme v úvahu jako první linii zabezpečení, jako určitá opatření, která se dají realizovat na bázi:

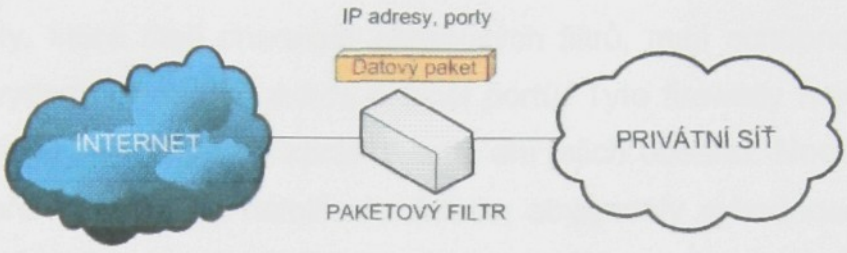
Organizačního opatření – opatření na této bázi mají za úkol určitým způsobem regulovat chování uživatelů chráněné sítě a způsob, jakým se bude nakládat se zdroji v této síti. Jde například o zákaz uživatelům přinášet nefiremní data na různých médiích a vkládat je do počítačů v chráněné síti. Dále třeba zákaz instalovat nové programy. Jedná se i o politiku hesel – uživatelům může být dáno za úkol pravidelně měnit svá hesla, zálohování dat a nenechávání citlivých dat na počítačích, které jsou připojené k síti. Je zřejmé, že čistě organizační opatření nemohou poskytnout velkou míru zabezpečení, ale v určitých případech může být takovéto zabezpečení (i z hlediska nákladů) dostačující.

Softwarového řešení – toto řešení nevyžaduje specifické technické prostředky, vzhledem k tomu, že je realizováno čistě softwarově – tedy programovými prostředky. V rámci složitosti a nákladů na zabezpečení může někdy postačit třeba jen vhodné nastavení existujících programových prostředků. Při vyšších nárocích je možností instalace dodatečných programů – například nadstavba nad operačním systémem routeru (dávající mu schopnosti k vykonávání funkce firewallu). Další možnost spočívá v instalaci samostatných programů, které realizují funkci firewallu – nikoli nadstavba.

Kombinované řešení – kombinace programových a technických prostředků je zřejmě nejvhodnější a je také nejpoužívanější. Díky své univerzálnosti dokáže poskytnou nejvyšší úroveň ochrany. Možnostmi tohoto řešení je například princip demilitarizované zóny (konkrétněji se těmto řešením budu věnovat dále).

2.2.3. Paketové filtry a aplikační brány

Důležitým faktorem pro firewally je otázka, na které úrovni pracují (v rámci sedmivrstvého modelu ISO/OSI). Typickými jsou firewally fungující na síťové a transportní vrstvě a pak na úrovni aplikační vrstvy.



Obr. č. 2 – Nasazení paketového filtru
(vlastní tvorba)

Paketové filtry

Paketovými filtry se nazývají firewally na úrovni síťové a transportní vrstvy. Data jsou totiž na úrovni síťové vrstvy přenášeny po blocích. Firewally, které pracují na této úrovni, zkoumají právě tyto pakety – kontrolují převážně obsah hlaviček paketů. V sítích, které fungují na bázi protokolů TCP/IP kontroluje IP adresy odesílatele a příjemce – a podle výsledku kontroly se rozhodne, jestli budou propuštěny dál nebo zda je zamítne a zahodí – odfiltruje. Paketový filtr tedy již na základě zkoumání IP adres dokáže povolit či zakázat veškerý tok dat od určitého vnějšího uzlu (podle adresy odesílatele) nebo k některému uzlu v připojené síti (na základě adresy příjemce).

Nicméně v praxi jsou na paketový filtr kladeny i důslednější požadavky kontroly než jen omezení přístupu od konkrétních uzlů, popř. ke konkrétním uzlům. Mohou se vyskytnout požadavky, aby se paketový filtr choval určitým způsobem k různým druhům služeb. Týká se to například elektronické pošty – může být požadováno, aby byla propouštěna elektronická pošta k uzlu, jenž plní roli poštovního serveru v chráněné síti a zároveň, aby k němu nebyl propouštěn žádný jiný provoz. V takovém případě musí filtr brát v úvahu i údaje o přenášených

datech, které odpovídají transportní vrstvě ISO/OSI. Jedná se o čísla portů – na jejich základě jsou identifikovány konkrétní entity v rámci odesílajících či přijímajících, navíc je s nimi identifikován i druh přenášených dat (např. port č. 25 – na tento port jsou zasílány datové pakety zajišťující přenos elektronické pošty, na cílovém uzlu je přijímá programová entita (démon) realizující funkci poštovního serveru.

Firewally, které mají charakter paketových filtrů, mají schopnosti omezeny tím, co lze vydedukovat z IP adres a čísel portů. Tyto firewally nejsou schopné rozumět formátu přenášených zpráv a tedy ani jejich obsahu. Nedokáží zkrátka analyzovat přenášená data natolik do detailu, aby mohly vyhodnocovat data na úrovni aplikační vrstvy. Například u elektronických zpráv nerozumí použitým poštovním adresám, i když podle čísla portu ví, že jde o elektronickou poštu (podobným způsobem se to týká přenášených souborů, WWW stránek a dalších možností přenosu). Toto omezení ve schopnostech paketových filtrů způsobuje fakt, že nejsou schopny rozpoznat některé možné útoky, které jsou rozpoznatelné až na úrovni aplikační vrstvy detailní analýzy, která vychází ze znalosti příslušné služby.

Aplikační firewally

Z výše zmíněného důvodu existují vedle paketových filtrů ještě firewally, které jsou označovány jako aplikační brány (či aplikační firewally). Tyto firewally pracují na úrovni aplikační vrstvy – to znamená, že svá rozhodnutí realizují na základě informací, které jsou dostupné na úrovni aplikační vrstvy.

Princip aplikačních firewallů je jednoduchý. Lze si jejich princip představit jako hlídače, který kontroluje veškerý provoz. Hlídačů je však více a každý z nich je specializován na určitou službu – například elektronická pošta procházející mezi vnějším Internetem a chráněnou sítí musí projít přes hlídače (aplikační bránu), který zná formát zpráv elektronické pošty a zná také její celkovou koncepci a architekturu. Aplikační brána je pak s těmito znalostmi schopná posoudit, zdá má

být zpráva předána dál či nikoli, navíc je třeba schopná odhalit případ útoku, který se maskuje jako přenos elektronické pošty.

Firewally pracující na principu aplikačních bran jsou tedy schopny splnit podstatně detailnější požadavky na ochranu privátní sítě – tím, že jsou schopny přesněji rozlišovat, co je nežádoucí přístup a co nikoli.

Na aplikační úrovni mohou firewally fungovat dvěma způsoby.

1) Obsahové filtry

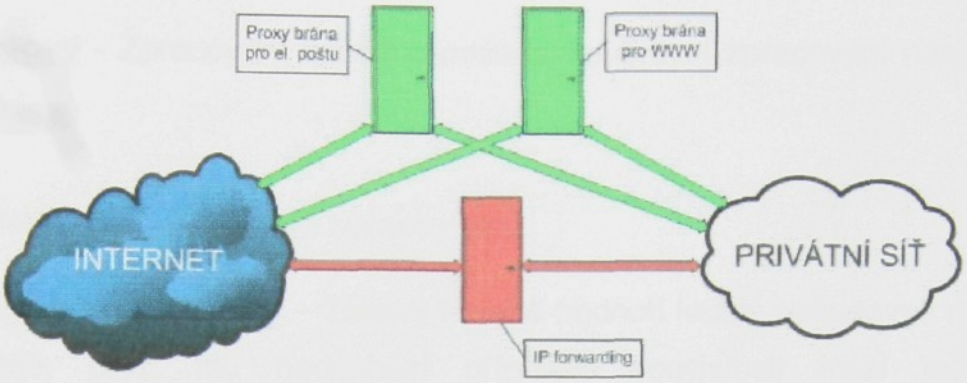
Tento způsob se podobá principu paketového filtru. Odlišuje se pouze tím, že při rozhodování využívá informací, které přísluší aplikační vrstvě. Takový uzel se tedy chová jako router (zajišťuje směrování na úrovni síťové vrstvy) a jen vnitřně během svého rozhodování pracuje i na aplikační vrstvě. Tyto druhy firewallů jsou označovány jako obsahové filtry (content filters).

2) Proxy brány

Toto řešení je v praxi obvyklejší – aplikační firewall na principu proxy brány. Doposud se u všech řešení předpokládalo, že síť je v podstatě pro jakýkoli datový paket přístupná. Tedy s ohledem na to, jak posoudí brána jeho oprávněnost ke vstupu – na síťové (kam pakety směřují) či aplikační vrstvě (co obsahují). U tohoto řešení však neexistuje, aby někdo zvenčí vstoupil do sítě či tušil, kdo je uvnitř sítě, a zároveň nesmí nic projít ven. Provoz pak funguje následujícím způsobem. Když někdo požaduje určitou WWW stránku z vnějšího okolí, předá požadavek proxy bráně, tak si stránku navenek vyžádá „svým jménem" a když je jí doručena, předá ji autorovi požadavku.

Lze si tedy představit situaci, kdy je nastaven apriorní zákaz veškerého přenosu síťových paketů z jedné sítě do druhé. Vzhledem k tomu, že se dnes na úrovni síťové vrstvy používá nejčastěji IP protokol, je zakázáno předávání IP paketů (IP forwarding). Proxy brána pak hraje důležitou roli zprostředkovatele se specializací na konkrétní službu (WWW, FTP, elektronická pošta). Uzel chráněné sítě pak musí své požadavky na vnější síť adresovat příslušné proxy bráně, která

je za něj vyřídí. Jinak by takový požadavek skrz aplikační firewall tohoto typu vůbec neprošel.



Obr. č. 3 - Představa fungování firewallu využívajícího proxy brány (vlastní tvorba)

Oproti řešením, které nepoužívají proxy brány, přináší toto řešení podstatnou odlišnost. Tato odlišnost spočívá ve faktu, že existence proxy bran již nemůže zůstat utajena koncovým uzlům chráněné sítě. Například pokud uživatel klikne na nějaký hypertextový odkaz, měl by WWW browser správně poslat příslušný požadavek přímo serveru, který obsahuje daný odkaz. Nicméně, při tomto řešení musí WWW browser zaslat tento požadavek proxy bráně, která zajistí vše potřebné. Aby se zajistil bezproblémový provoz, řeší se toto v praxi nastavením konfigurace WWW browseru – jednoduše se u něj nastaví, že musí spolupracovat s příslušnou proxy bránou. Velmi důležitým aspektem v této otázce je to, aby takovéto nastavení zůstalo skryto před uživatelem – správce sítě provede nastavení a uživatel pracuje s browserem stejně jako bez firewallu a proxy bran.

2.2.4. Stavové vs. bezestavové mechanismy

Existují dva základní způsoby, jakými mohou přenosové mechanismy a služby počítačových sítí fungovat – stavové (statefull inspection) a bezestavové (stateless inspection).

Bezestavový - Při tomto způsobu fungování je každý požadavek zpracováván nezávisle na historii (tedy nezávisle na předchozích požadavcích). Například WWW služba funguje bezestavově – požadavek WWW klienta na

načtení jedné WWW stránky je vyřizován bez závislosti na předchozích požadavcích klienta.

Stavový - Zpracování každého požadavku ovlivní zpracování následujících požadavků.

Firewally fungující těmito způsoby jsou:

Bezestavový firewall – Takový firewall hodnotí každý požadavek na přenos samostatně, čímž mu nedochází případné souvislosti mezi jednotlivými požadavky.

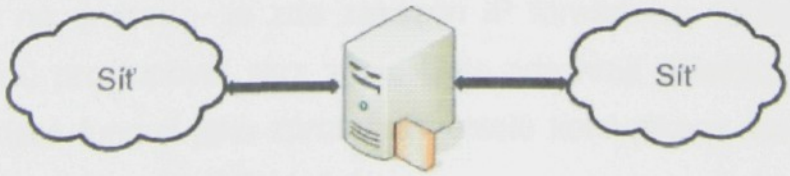
Stavový firewall – Firewally fungující stavovým způsobem si dokáží uvědomovat souvislosti mezi jednotlivými požadavky a mohou tak odhalit určité relace (sessions), které jsou tvořeny souvisejícími požadavky. Lze tedy říci, že mohou poskytnout vyšší stupeň ochrany.

2.2.5. Typy firewallů

Když se budeme zabývat typy firewallů a budeme je zvažovat v rámci celkové architektury, budeme před sebou mít dvě základní možnosti:

1) Dvounohý firewall
2) Demilitarizovaná zóna

Dvounohé firewally



Obr. č. 4 - Představa dvounohého firewallu
(vlastní tvorba)

Obrázek č. 4 představuje řešení pracující s jedním uzlem, který má dvě síťová rozhraní (či více). Tyto rozhraní jsou připojené do různých sítí, mezi kterými je pak zajištěno propojení.

Tento způsob řešení plní následující role:

1) Routeru - který mezi sebou propojuje dvě samostatné sítě a přenáší síťové pakety z jedné sítě do druhé.

2) Firewallu – oproti běžnému routeru je rozhodování o předání či nepředání konkrétního paketu náročnější, jelikož přenášené pakety a jejich obsah zkoumá detailněji.

Rozhodování přitom může probíhat v rámci:

1) Informací síťové a transportní vrstvy (síťové adresy a porty) – firewall na principu paketového filtru.

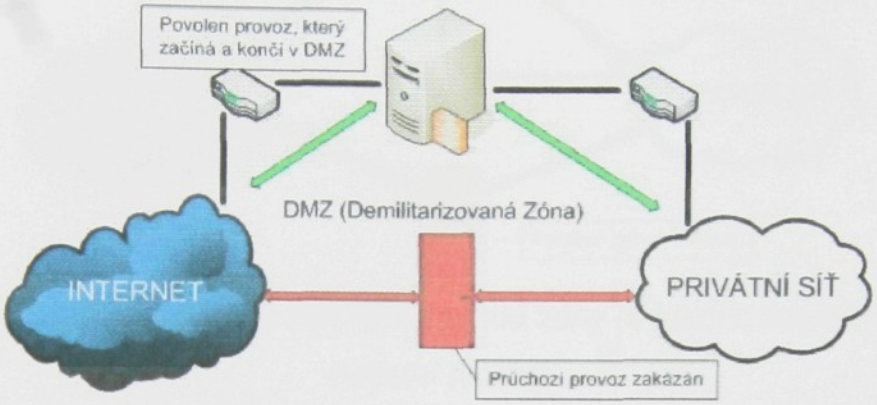
2) Úrovně aplikační vrstvy – princip aplikační brány (provedení obsahového filtru či využívající proxy brány).

Demilitarizovaná zóna

Pro toto řešení je možné využít analogie s nárazníkovým pásem mezi dvěma válčícími stranami, který tak zachovává přísnou neutralitu a je tak přístupný pro obě strany. Důležité je nicméně to, co tato demilitarizovaná zóna přináší v praxi. Přináší skutečnost, že skrze tuto demilitarizovanou zónu nemůže nic proniknout z jedné strany na druhou – je zde zakázán IP forwarding, takže žádné síťové pakety nemohou prostupovat skrz zónu. Dále zde hrají důležitou roli jednotlivé proxy brány, které fungují jako zprostředkovatelé komunikace mezi propojenými sítěmi, specializovaní na konkrétní služby.

Existují různé způsoby, jak uzpůsobit tyto řešení.

Zajímavou možností řešení (zřejmě principiálně nejjednodušší) je zapojení dvou routerů (viz obrázek č. 5). Mezi nimi pak vzniká příslušná demilitarizovaná zóna jako samostatná síť.



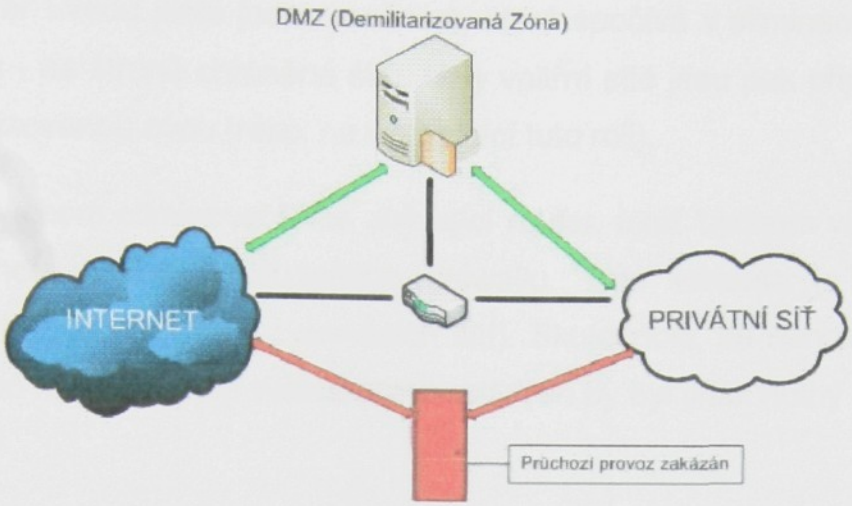
Obr č. 5 - Představa demilitarizované zóny (se dvěma routery) (vlastní tvorba)

Potom je ale důležité, aby byly routery nakonfigurovány takovým způsobem, aby umožňovaly přenos síťových paketů, který začíná či končí v demilitarizované zóně a zároveň zakazovaly přenos síťových paketů, který prochází skrz demilitarizovanou zónu. Těmto jednoduchým požadavkům jsou schopné dostát všechny routery.

Výhodou je větší bezpečnost (nutnost překonat dva omezující uzly).

Nevýhoda spočívá v nutnosti použít dva routery.

Existuje ale i možnost jak vystačit s jediným routerem. Musí však mít alespoň tří síťová rozhraní - pak jej stačí zapojit podle obrázku č. 6.

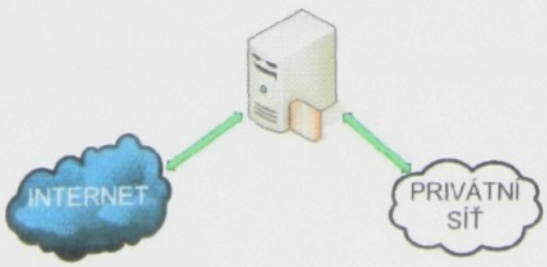


Obr č. 6 - Představa demilitarizované zóny (s jedním routerem)
(vlastní tvorba)

V praxi se možnosti neomezují pouze na uvedené dvě základní varianty firewallů (dvounohý a princip demilitarizované zóny). Existuje celá řada přechodových variant mezi těmito řešeními.

Demilitarizovaná zóna je v podstatě samostatnou sítí a může do ní být umístěno více různých uzlů, které plní roli proxy bran či například roli WWW serveru, který je dostupný z chráněné privátní sítě i z veřejného Internetu.

Obrázek č. 7 znázorňuje další možnost, kterou je zredukování demilitarizované zóny z celé sítě na jeden dvounohý počítač. Ten pak realizuje všechny potřebné činnosti, které jsou typické pro demilitarizovanou zónu.



Obr č. 7- Možnost redukce DMZ
(vlastní tvorba)

Na závěr uvedu ještě jednu možnost, která spočívá v eliminaci jednoho ze dvou routerů - na straně chráněné sítě. Uzly vnitřní sítě jsou pak připojeny přímo na demilitarizovanou zónu (resp. na uzel plnící tuto roli).

Mohli bychom eliminovat ještě zbývající router, čímž bychom vlastně získali již zvažovanou variantu dvounohého firewallu. Tato varianta je typická pro připojování malých sítí (např. i domácích sítí). Skutečnost, že nahrazuje potřebu samostatného routeru, je její velkou předností. Ten by byl jinak nutný pro připojení k Internetu.

2.2.6. Volba firewallu

Tato podkapitola o firewallech pojednávala o základních myšlenkách a principech, na kterých mohou fungovat. Je nutné si uvědomit, že před implementací nějakého konkrétního řešení musíme zvážit to, co chceme dosáhnout – tedy jaké jsou hrozby, rizika ztráty a co od zabezpečení očekáváme. Až po provedení takovéto rozvahy je na místě zvažovat konkrétní realizaci.

Pokud se jedná o zabezpečení sítě, kde by případné ztráty dat byly závažné (kde je v sázce hodně - většinou velké sítě), je při volbě vhodného řešení nutná spolupráce s odborníky (vzhledem k tomu, že v takových případech jde o nemalé částky – hlavní je ochrana zdrojů). Ti pak mohou doporučit firewally jak ze standardních a univerzálních komponent či nasazení nějakého specializovaného produktu.

Situace u malých či nejmenších sítí je trochu odlišná. Pro takové sítě bývají odborníci příliš drazí.

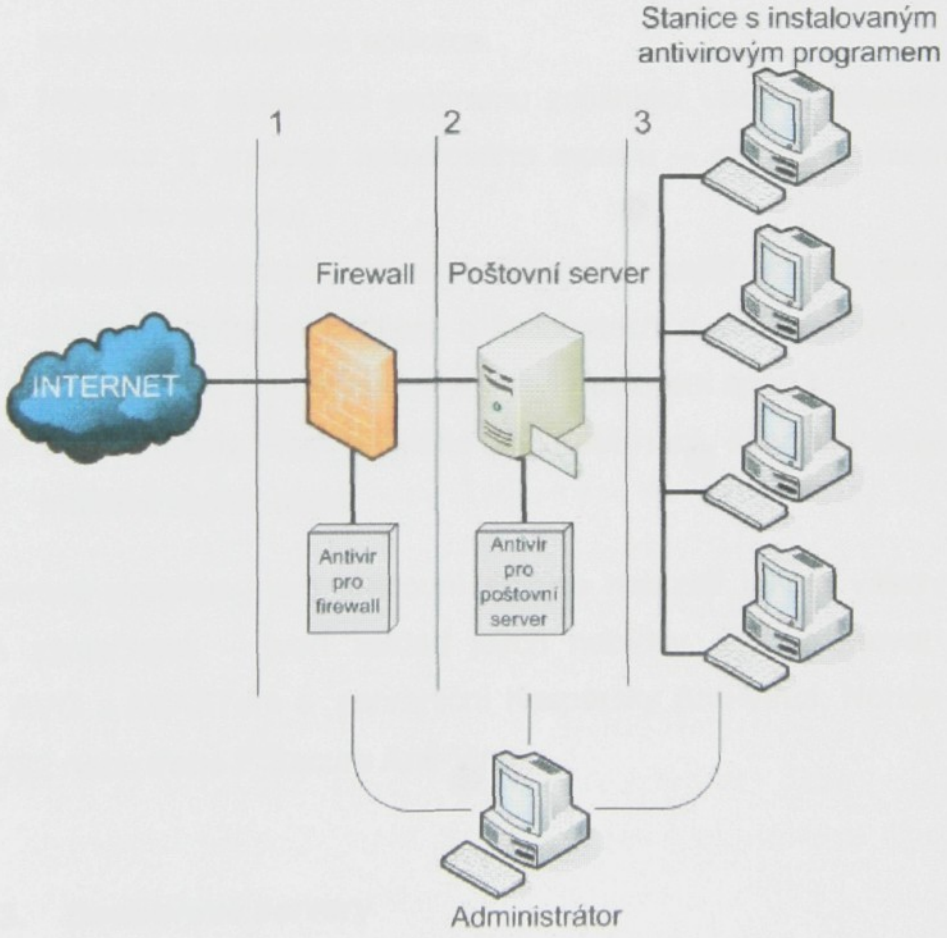
2.3. ANTIVIROVÁ OCHRANA

Není daleko od pravdy, že antivirové programy jsou nejčastěji aktualizovaný software. Důvodem k tomu je např. fakt, že dnešní e-mailoví červi jsou schopni se rozšířit po sítích celého světa během několika málo hodin. Vedle e-mailových

červů jsou hrozbou škodlivé kódy v podobě Trojského koně či Zadních dvířek (backdoor) či „klasických" virů.

2.3.1. Víceúrovňová ochrana

V oblasti antivirové ochrany se budu zabývat ochranou typické firemní lokální sítě střední velikosti a v ní umístěných pracovních stanic. Základní myšlenkou je nespoléhat se pouze na jednu úroveň antivirové ochrany, ale realizovat ji na více úrovních. Důležitým prvkem je také účinná centrální správa, která administrátorovi umožní pohodlně spravovat celý systém. Příklad struktury sítě znázorňuje obrázek č. 8.



Obr. č. 8 – Příklad struktury sítě

(vlastní tvorba)

2.3.2. Pracovní stanice

Zmínil jsem různé úrovně antivirové ochrany. Důležité je počítat s tím, že i kdyby byla na serverech a vstupních branách nasazena kvalitní antivirová ochrana, zůstává možnost nákazy prostřednictvím pracovních stanic. Základním prvkem tedy zůstává antivirový program na pracovní stanici a neměli bychom to opomenout.

Současný moderní antivirový program pro stanici se skládá z několika základních součástí:

1. On demand skener zajišťující prověření souborů na požádání.
2. On acces skener (rezidentní antivirový štít) kontrolující otevírané soubory a spouštěné aplikace.
3. Modul pro aktualizaci programu zajištující update databází virových signatur a upgrade antivirového motoru – engine (z Internetu nebo lokálního serveru).
4. Modul pro napojení na centrální správu zajišťující tok dat ze stanice k administrátorovi (hlášení o incidentech a stavu antiviru) a naopak (aktualizace, bezpečnostní politiky, nastavení apod.).
5. Další moduly, kam můžeme zahrnout např. speciální pluginy pro e-mailové klienty apod.

Antivirové programy pro pracovní stanice nabízejí takřka všechny známé antivirové společnosti – tvoří základ jejich nabídky. Lze jmenovat například "domácí" AVG s AVASTem a zahraniční Kaspersky Anti-Virus, Norton Antivirus, Eset NOD32 nebo třeba F-Secure Anti-Virus.

2.3.3. Souborové servery

Předtím, než se budu věnovat antivirové ochraně poštovních serverů a ostatních internetových vstupních bran, bych se pozastavil u problematiky antivirové ochrany serverů všeho druhu.

V případě antivirové ochrany souborových serverů se nejedná o ochranu serveru samotného, ale především o ochranu uložených dat.

Souborové viry se sice přímo na NetWare serverech množit nemohou, ale z infikované pracovní stanice, která má přístup ke sdílenému úložišti na souborovém serveru, může lehce dojít k infikování uložených dat. To stejné platí i pro makroviry, které mohou zneužívat jako nositele např. "wordovské" dokumenty. U Novellu si ale musíme dát pozor hlavně na "staré dobré" boot-viry, které mohou přímo ohrozit startovací "dosovskou" partition serveru.

U antivirové ochrany serverů se systémem Windows (NT/2000) je situace velmi podobná jako u pracovních stanic. Významně se neliší ani konstrukce a funkce antivirového programu, který je téměř totožný, jako jeho "kolega" na stanici. Pouze se zohledňuje možnost více procesorového prostředí a více se dbá na důraz ochrany síťového přístupu k datům.

U unixových/linuxových serverů není antivirová ochrana na takové úrovni, jako v případě Windows. Důvodem je náročnost vývoje řešení rezidentního štítu na unixový systém. Rozšířený je proto vývoj tzv. řádkových antivirových skenerů, které představují velmi jednoduchý ale zároveň výkonný nástroj, neumí však odhalit škodlivý kód v reálném čase. Pokud bychom ale chtěli vytvořit něco na způsob pseudorezidentní antivirové ochrany, musíme si pomoci programem, který spolupracuje s řádkových skenerem a předává mu příslušná data ke kontrole. Ty se zpravidla nasazují např. na poštovní agenty (Sendmail, Qmail, ...). Avšak i v této oblasti jsou již plnohodnotná antivirová řešení. Např. Kaspersky Antivirus for Linux Servers je vybavený plnohodnotným rezidentním štítem (jedná se o speciální „Anti-virus daemon“, který plní funkci štítu) pro detekci virů v reálném čase (pro el. poštu i souborový systém).

2.3.4. E-mailová komunikace

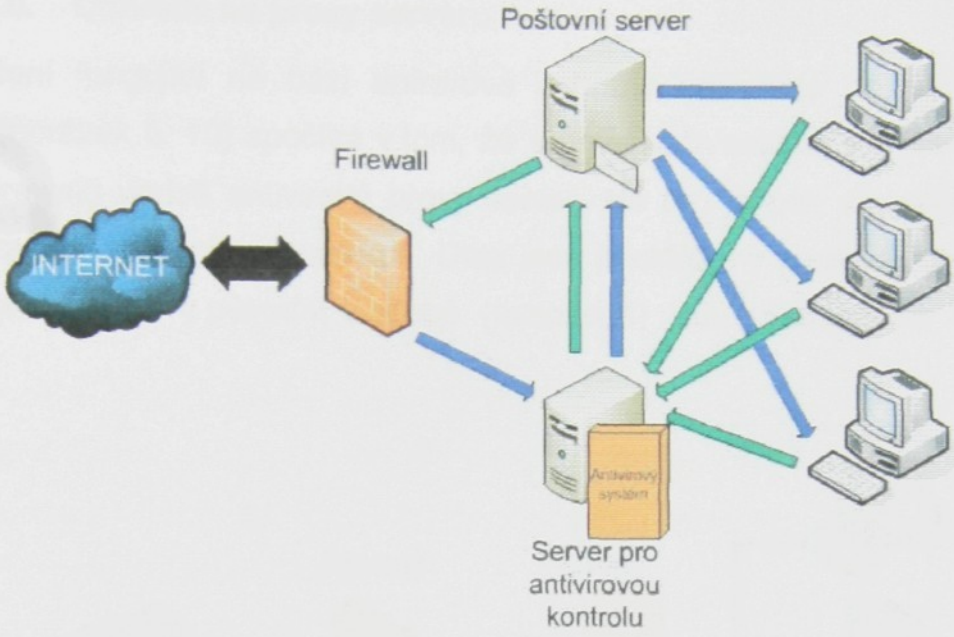
Ke komplexnímu zabezpečení je nutné zajistit antivirovou ochranu elektronické pošty. Řešení ochrany lze realizovat na úrovni vstupní brány nebo na úrovni poštovního serveru.

Následuje přehled poštovních serverů, které se vyskytují v praxi:

- Lotus Notes/Domino - nabídka antivirů je zde poměrně široká, jelikož MS Exchange patří k nejčastěji se vyskytujícím poštovním serverům.
- MS Exchange 5.x, 2000 - zde platí obdobná situace jako u Lotus Notes.
- Jiné poštovní servery (Windows) - obvykle neumožňují implementovat jakoukoli antivirovou ochranu, určenou např. pro Exchange (výjimkou je např. Kerio Mail server)
- Servery typu Winproxy nebo Winroute - obvyklá jsou řešení na systému Novell Netware (GroupWise nebo Merkury) nebo právě Winproxy, Winroute. Možnosti antivirové ochrany jsou obdobné jako u předchozího bodu.
- Linuxové poštovní servery - příkladem jsou Qmail, Sendmail či Postfix. Tyto jsou podporovány množstvím antivirových programů. Kvalitním řešením jsou produkty společnosti Kaspersky Lab. Z nekomerčních pak AmaViS (A Mail Virus Scanner).

Pro jiné existují antivirová řešení na základě tzv. SMTP-relay serveru. Toto řešení funguje tak, že pošta je doručena na vyhrazený server, kde je zkontrolována antivirem. Pokud projde kontrolou, je přeposlána na původní poštovní server a odtud doručena adresátovi.

Funkce takového řešení je znázorněna na obrázku č. 9.



Obr. č. 9 – Řešení na základě SMTP-relay serveru
(vlastní tvorba)

Rychlost tohoto řešení dovoluje použití relativně nevýkonného hardwaru – je využívána např. u poskytovatelů freemailových služeb.

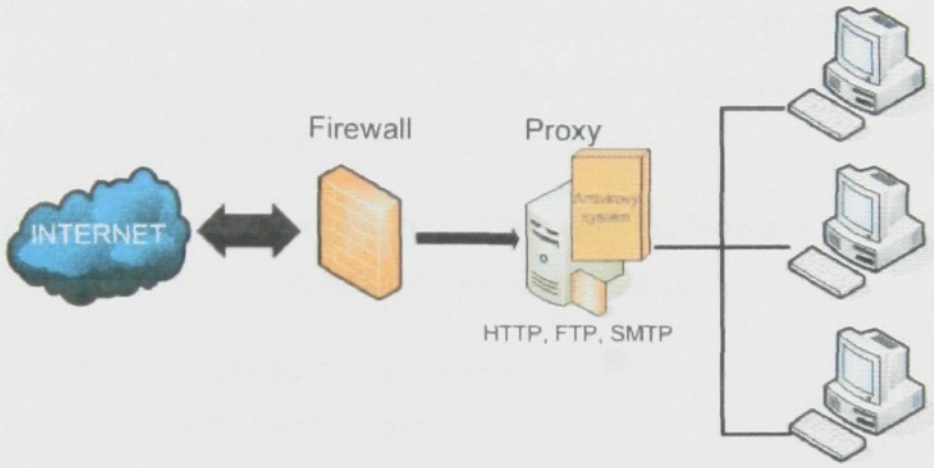
2.3.5. HTTP a další protokoly

Dalším protokolem, který je třeba brát v úvahu při zabezpečení je HTTP. V dnešní době jsou velmi rozšířené freemailové servery, na kterých uživatelé spravují své e-mailové schránky v prostředí na bázi webových stránek. To poskytuje přístup odkudkoli, nicméně je zde hrozba např. e-mailových červů. Na webových stránkách se navíc mohou nacházet škodlivé kódy v podobě skriptů či appletů, které mohou do systému uživatele instalovat např. „zadní vrátka".

Vedle HTTP je dobré zmínit také FTP protokol či POP3 (ten by administrátorem v lokální síti neměl být povolen). Snadným řešením je „postradatelné" protokoly zakázat přímo na firewallu.

2.3.6. Ochrana na proxy serveru

Řešení fungující na bázi antivirové ochrany nasazené na úrovni proxy serveru (obrázek č. 10) spočívá v tom, že se mezi uživatelské stanice a vstupní bránu (firewall) umístí antivirový proxy server. Na ten je pak ze vstupní brány přesměrována veškerá komunikace. Data jsou poskládány z paketů do souborů, jsou otestována a v původní podobě (rozložené) jsou předána na samotnou stanici.



Obr. č. 10 – Použití proxy serveru
(vlastní tvorba)

Princip je stejný i pro odchozí data. Nicméně je nutné u stanic a poštovních serverů v celé lokální síti přesměrovat provoz na proxy server.

Výhody:

- rychlost
- vhodné pro rychlé linky s velkým zatížením
- snadná instalace – stačí definovat, kam budou pakety směrovány
- nízké systémové nároky – zátěž procesoru a paměti

Nevýhody:

- vysoká cena - v řádech tisíců dolarů
- nesnadná aktualizace – oproti čistě softwarovým řešením
- náročná konfigurace sítě – pro správnou kontrolu ochozích dat

Existuje ještě řešení v podobě síťového prvku bridge(není přímo proxy serverem), u kterého odpadá potřeba překonfigurovat klientská nastavení a firewally. Do sítě pak lze zapojit tak, že jeho existence v podstatě není navenek patrná.

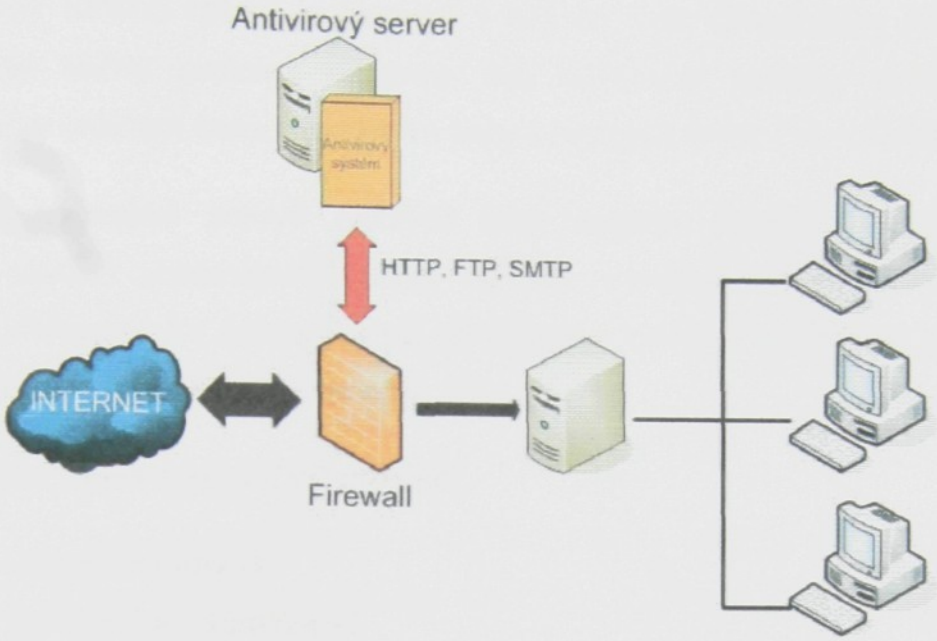
2.3.7. Ochrana firewallů

Samozřejmostí v řešení ochrany se staly firewally. Jako základní prvek antivirového řešení pro podnikové firewally je protokol CVP (Content Vectoring Protocol), který přesměrovává pakety na vyhrazený antivirový server umístěný ve vnitřní síti či v demilitarizované zóně.

Myšlenka instalovat antivirové programy přímo na firewall má několik negativ, protože instalace dalšího programu na firewall způsobuje:

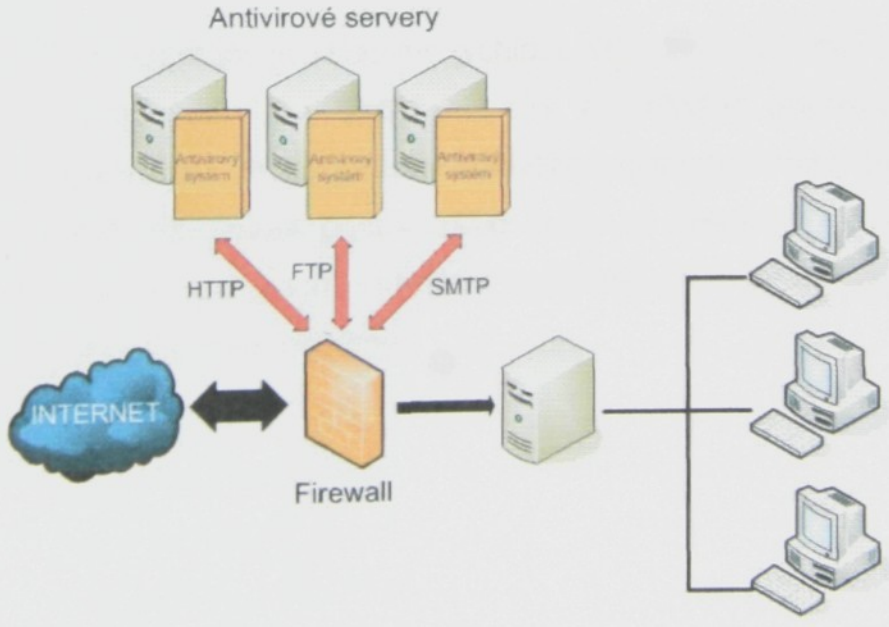
- narušení robustnosti a stability
- snížení jeho bezpečnosti

Požadavky na vyhrazený server jsou rychlost diskového zařízení, výkon procesoru, velikost operační paměti a připojení k firewallu co nejkratší cestou (např. křížový kabel s rychlou topologií bez meziprvků). Jejich důvodem je způsob, jakým se za pomoci protokolu CVP provádí antivirová kontrola protékajících dat. CVP přesměruje pakety na aplikační vrstvě (většinou na protokolech HTTP, FTP a SMTP) na antivirový server, kde se provede kontrola a pakety se vrátí firewallu, který podle výsledku kontroly rozhodne, zda je propustí či ne. Princip je vidět na obrázku č. 11.



Obr. č. 11 – Antivirová ochrana firewallu I.
(vlastní tvorba)

Antivirových serverů může být i skupina, ve které se rozdělí kontrola jednotlivých protokolů (viz obr. č. 12) mezi servery podle zátěže a rychlosti připojení.



Obr. č. 12 – Antivirová ochrana firewallu II.
(vlastní tvorba)

Příklad silného řešení je Firewall 1 NG od firmy Checkpoint, jenž dokáže nasadit na každý protokol dokonce dva antivirové servery, čímž zvládne obsluhovat v reálném čase internetové linky s rychlostí kolem 10 – 12 MB/s.

Pro uspokojivé pokrytí rychlých linek existuje řešení Clustering, které dovoluje nasadit „neomezený" počet serverů. Výhodou tohoto řešení je také snadné zálohování AV ochrany a tak při výpadku jednoho ze serverů je jeho role rozdělena mezi zbylé funkční servery.

Firewally podporující CVP protokol:

- Altavista Firewall
- Check Point FireWall-1
- Cyberguard Firewall for NT
- Gauntlet
- Milkyway/SLM SecurIT Firewall for Solaris
- Secure Computing Firewall for NT
- Secure Computing SecureZone
- Sun Solstice Firewall

Zásadním omezením je relativní rychlost. Obecně platí, že CVP skenery zvládají tok přibližně od 1,8 – 2MB/s. U sítě s rychlejším připojením je dobré uvažovat o clusteringu. Konfigurace takového systému může být složitá a náchylná k nestabilitě, avšak přináší nižší cenu za relativně spolehlivý prvek antivirové ochrany. Pokud jsme na hranici možností CVP, vyplatí se uvažovat o proxy architektuře antivirové ochrany.

3. NÁVRH ZABEZPEČENÍ STŘEDNĚ VELKÉ POČÍTAČOVÉ SÍTĚ

Tato kapitola se zabývá návrhem zabezpečení připojované středně velké firemní počítačové sítě. Bude zde navrženo řešení zabezpečení spolu s cenovým ohodnocením. Návrh řešení vychází z předpokladu, že bude sestavena celá síť.

3.1. DESIGN SÍTĚ

Za příklad pro řešení jsem zvolil návrh sítě, která má jen jedno připojení k Internetu a bude mít okolo dvaceti vnitřních uživatelů. Samozřejmě je možné rozsah rozšířit či zúžit podle potřeby, ovšem s tím, že bude vhodné užít rychlejší hardware, rozdělit síť do více menších podsítí či dokonce přidat více připojovacích bodů k vnější síti.

Stejně jako u většiny věcí, dobrá bezpečnost stojí peníze. Naštěstí ale mnoho dobrých bezpečnostních produktů je dostupných zdarma a lze takovou bezpečnost implementovat použitím hardwarových komponent a Open Source softwaru. Uvedený návrh sítě a jejího zabezpečení má poskytnout poměrně vysoký stupeň ochrany při ponechání některých dostupných služeb pro vnější síť.

3.2. BEZPEČNOSTNÍ POLITIKA

Nejprve je nutné vytvořit určitý základní dokument, který bude řešit bezpečnostní politiku podniku. Při vytváření dokumentu (a tedy celkové bezpečnostní politiky) je zapotřebí brát v úvahu hrozby vnější i vnitřní. Než začneme budovat síť, je potřeba si uvědomit několik "maličkostí". Většina útoků pochází překvapivě z řad lokálních uživatelů. V ochraně před lokálními uživateli nám pomáhá především *bezpečnostní politika* organizace, která určuje např. kdo má právo přístupu ke kterým zdrojům, jaká jsou omezení na připojení do sítě (např. v době od 8 do 20 hodin nemá nikdo právo připojovat žádný HW) a definuje postihy za nepovolenou činnost.

3.3. ZABEZPEČENÍ VŮČI VNITŘNÍM HROZBÁM

Tato zabezpečení vychází z definované bezpečnostní politiky. Abychom se totiž mohli spolehnout na zabezpečení připojované sítě a tedy na to, že naše data budou chráněna, musíme si vytvořit spolehlivé prostředí, ve kterém má být chráněná síť provozována. Sebelepší zabezpečení firewally a dalšími nástroji nebude nic platné, pokud případnému útočníkovi takřka „otevřeme dveře" tím, že mu například (ač neúmyslně) poskytneme přístupová hesla či nějakým jiným „faux pa" usnadníme průnik do sítě.

To znamená:

- vytvořit a dodržovat řádnou politiku hesel
  - Jedná se o notoricky známé poučení o volbě hesel, která nejsou odhadnutelná či snadno prolomitelná.
- striktně vymezit přístupová práva uživatelů sítě
  - Definovat práva uživatelům podle potřeby přístupu k datům či určitým službám.
- zákaz instalace programů
  - Nepovolit uživatelům volně instalovat programy, čímž by mohli ohrozit stabilitu a bezpečnost systému.
- definovat a dodržovat organizační opatření
  - Jde o dodržování chování uživatelů. Nepřinášet pochybná data na médiích zvenčí atd. Dále je možností uchovávat důležitá data na stanicích, které nejsou připojené k Internetu, tedy k vnější síti.
- provést technická opatření
  - Servery , aktivní prvky a všechny fyzické objekty musí být v uzamčených prostorách, kam má přístup pouze zodpovědný pracovník.
  - Zálohování důležitých dat – např. zavést automatické zálohování důležitých dat ze serveru

3.4. SESTAVENÍ SÍTĚ A ZABEZPEČENÍ DATOVÉHO PROVOZU

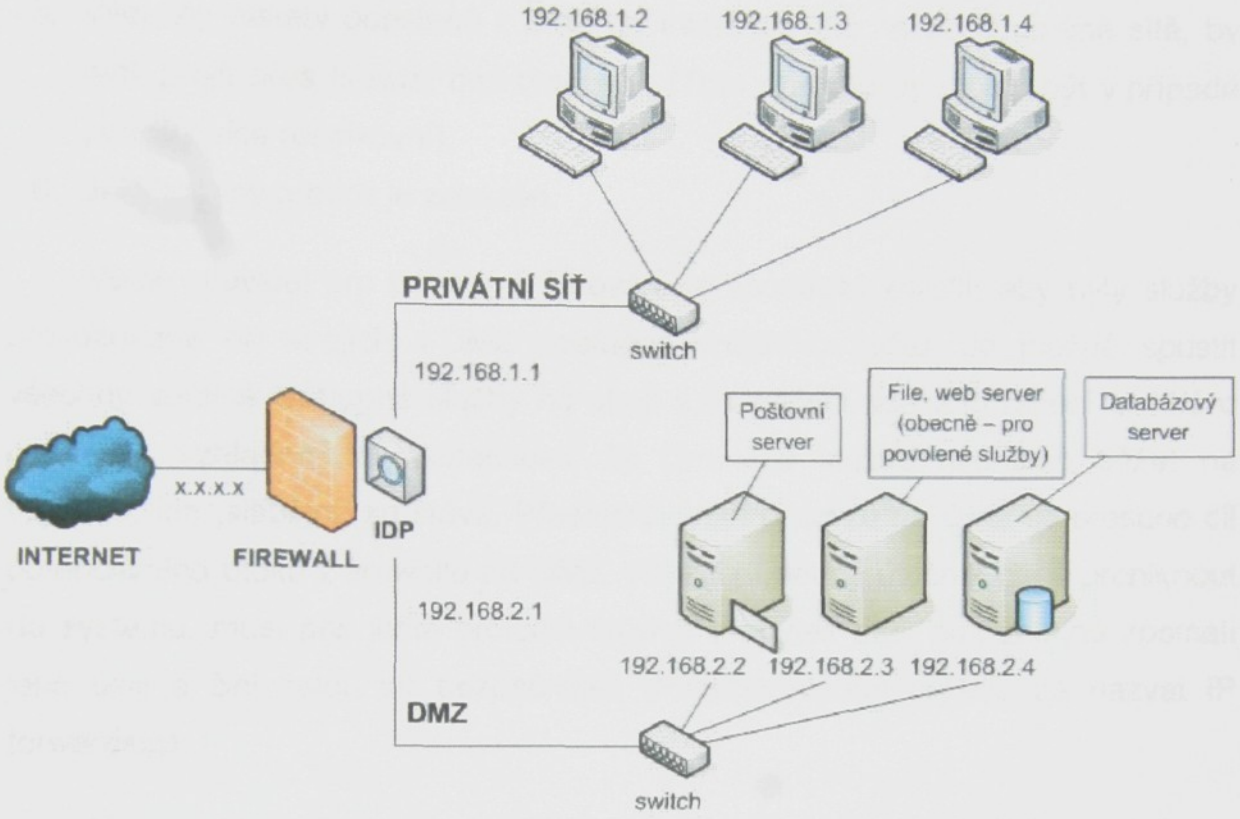
Design, jenž se jeví jako jednoduchý pro stavbu a udržování, využívá:

- **Firewall pro ochranu vnitřní privátní sítě**, do které se nelze připojit z vnější sítě
- **DMZ** („demilitarizovaná zóna") ve formě oddělené sítě s některými povolenými službami k vnějšímu světu (chráněnou tímtéž firewallem) - tyto služby mohou být: DNS, WWW, mail, FTP (tento seznam lze upravit podle potřeby). DMZ se může skládat z jednoho či více strojů – vše záleží na tom, jak složité řešení chceme mít
- **IDP** (Intrusion Detection and Prevention) – zajišťuje filtrování provozu a monitoring dat přicházejících a odcházejících z DMZ

Veškerý příchozí provoz do chráněné sítě bude kontrolován a filtrován firewallem běžícím na vyhrazeném počítači se třemi síťovými rozhraními:

- **Rozhraní A** připojuje firewall k Internetu. IP adresa rozhraní je přiřazena ISP (Internet Service Provider) (v tomto řešení budu používat x.x.x.x).
- **Rozhraní B** spojuje firewall s chráněnou sítí. IP adresa rozhraní bude v tomto řešení 192.168.1.1.
- **Rozhraní C** spojuje firewall s DMZ. IP adresa rozhraní pak zde bude 192.168.2.1.

Základní rozvržení sítě zobrazuje obrázek č. 13



Obr. č. 13. – Schéma struktury navrhované sítě
(vlastní tvorba)

Firewall bude používat následující pravidla pro provoz:

1. Všechny pakety odeslané z chráněné sítě na všechny povolené („legální") adresy budou procházet přes firewall bez omezení. (Toto pravidlo by mohlo být v případě potřeby více restriktivní).
2. Všechny pakety poslané z Internetu do chráněné sítě by měly být filtrovány a pouze ty, co jsou validními odezvami na požadavky, jenž byly původně odeslány z chráněné sítě, by do ní měli být propuštěny.
3. Všechny pakety poslané z Internetu do DMZ by měly být filtrovány a pouze ty, co směřují ke službám, které jsou povoleny, mohou projít přes firewall. Také všechny validní odezvy na požadavky, jenž byly původně odeslané z DMZ by do ní měly být puštěny. (Toto pravidlo by mohlo být v případě potřeby více restriktivní).
4. Všechny pakety odeslané z DMZ, co jsou validními odezvami na požadavky, které byly původně odeslány z chráněné sítě, by do ní měli být propuštěny.

5. Všechny pakety odeslané z DMZ do Internetu, ale ne do chráněné sítě, by měli projít přes firewall bez omezení. (Toto pravidlo by mohlo být v případě potřeby více restriktivní).
6. Jakýkoli jiný provoz je zakázán.

Vedle pravidel pro paketové filtrování je zapotřebí zajistit, aby byly služby provozované na strojích v DMZ dostupné vnějšímu světu. Je možné spustit všechny veřejně dostupné služby na stroji s firewallem, ale toto řešení si říká o problémy, vzhledem ke skutečnosti, že čím více služeb necháme běžet na firewallu, tím „slabším" se stává. Přesměrováním provozu na DMZ se přesune cíl potenciálního útoku z firewallu na DMZ. Pokud případný útočník chce proniknout do systému, musí pak ještě prolomit firewall a zbytek sítě, což značně zpomalí jeho úsilí a činí celou síť bezpečnější. (Přesměrováním paketů lze nazvat IP forwarding).

Menší sítě mají obvykle jednu IP adresu přiřazenou jejich ISP, a tak bude vhodné, aby měl firewall spuštěn nějaký druh „maskovacího" softwaru. Ten způsobí, že veškerý provoz z chráněné sítě a DMZ pochází jakoby z jediné stanice. Toto je nadstavbové bezpečnostní opatření, které činí chráněnou síť hůře ohrozitelnou, protože IP adresy stanic za firewallem nejsou pro vnější svět viditelné.

3.4.1. Hardware

Firewall

Počítač, na kterém bude běžet firewall, nemusí být „high-end". Je jen zapotřebí, aby vyhovoval pro tři síťová rozhraní (jedno pro připojení k Internetu, druhé pro připojení ke chráněné síti a třetí pro připojení k DMZ). Pro uvedené řešení jsem vybral PC stanici o následujících parametrech (lze použít jeden ze starších počítačů, který firma vlastní):

Tab. č. 1 – Server pro firewall

Parametry serveru pro firewall	
Procesor:	Intel Pentium III 600 MHz
HD:	4 GB
Paměť:	256 MB RAM
Síťové karty:	1 x 10/100 Mb/s – pro připojení k vnější síti 2 x 1 Gb/s – pro vnitřní síť a DMZ
Cena (s DPH)	7 000,- Kč

V tabulce jsou uvedeny pouze podstatné komponenty. Cena vychází z aktuálních ocenění komponent či sestav prezentovaných v prodejnách či bazarech, pokud se jedná o starší díly, které se již neprodávají. Celková cena zahrnuje celou sestavu i s monitorem (nejen uvedené komponenty).

Poštovní server

Vycházím z předpokladu, že firemní síť má 20 uživatelů. Rozhodl jsem se použít samostatný poštovní server obdobných parametrů jako pro firewall.

Tab. č. 2 – Poštovní server

Produkt	Cena (s DPH)
Poštovní server	6 000,- Kč

Cena vychází z aktuálních ocenění komponent či sestav prezentovaných v prodejnách či bazarech, pokud se jedná o starší díly, které se již neprodávají.

Servery

Při volbě serveru (pro účely file serveru, web serveru, a případné jiné služby) jsem se rozhodl pro produkt firmy Hewlett Packard - *HP ProLiant DL145*. Svým výkonem by měl vyhovovat požadavkům středně velkého podniku. Lze samozřejmě použít i jiný server, volba by závisela na konkrétních požadavcích pro budovanou síť. Nicméně pro daný případ toto řešení poskytne dostatečný výkon.

Tab. č. 3 – Servery

Produkt	Cena (s DPH)
Server - HP ProLiant DL145	56 229,- Kč
Databázový server - HP ProLiant DL145	56 229,- Kč

Obr. č. 14 - HP ProLiant DL145

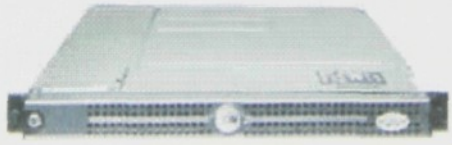
(zdroj: www.hpmarket.cz)

Specifikace serveru:

- Procesor: 2.2 GHz AMD Opteron 200 série, 1MB L2 cache
- Počet procesorů (max): 2
- Chipset: AMD Opteron 8000, s technologií HyperTransport
- Paměť: 1 GB (2 x 512MB) PC2700 DDR SDRAM
- Hard disk: 40 GB ATA, podpora ATA nebo SCSI
- Rackové provedení

IDP

IDP – neboli Intrusion Detection and Prevention – kombinuje IDS (Intrusion Detection) a IPS (Intrusion Prevention) sondy. Často používané zapojení IDS sondy je někdy mylně považováno za bezpečnostní opatření. IDS sonda pouze prověřuje probíhající provoz a upozorňuje firewall na případné útoky, nicméně samotnému útoku nezabrání. IDP řešení identifikuje a zastaví útoky na síťové a aplikační úrovni dříve než způsobí nějakou škodu. Sonda se zapojuje za firewall a doplňuje ho tak o další vrstvu zabezpečení.



Obr. č. 15 - NETSCREEN-IDP 10 IDP APPLIANCE

(zdroj: www.epinions.com)

Pro navrhované řešení zabezpečení sítě jsem zvolil produkt společnosti Netscreen - *NETSCREEN-IDP 10 IDP APPLIANCE*, jenž je znázorněn na obrázku č. 12. Zvolil jsem model *IDP 10*, který by měl dostatečně vyhovovat potřebám navrhované sítě.

Parametry:

- Přenosová rychlost – 100 Mb/sec
- Maximální propustnost – 20 Mb/sec
- Standardní paměť – 512 MB
- Operační módy – pasivní sniffer, inline bridge, inline Proxy-ARP, inline router
- Detekční mechanismy – Protocol Anomaly Detection, detekce „zadních vrátek" (backdoor), IP Spoofing, Denial of Service (DoS), dvouvrstvá detekce, Honeypot, detekce statefull signatur
- Update signatur – týdně a v případě pohotovosti

Kompletní informace o tomto produktu lze nalézt na www.juniper.net.

Tab. č. 4 – IDP

Produkt	Cena (s DPH)
NETSCREEN-IDP 10 IDP	* 161 868 Kč

** Ceny, které vychází z cizích měn, jsou přepočítávány na Kč kurzem ČNB ze dne 20. 11. 2004 (1 USD = 23,906 Kč) a jsou zaokrouhleny na celé Kč nahoru.*

Alternativní volba

Alternativním řešením pro IDS/IPS (IDP) by mohl být produkt firmy Cisco. Nicméně jsem od této firmy pro konkrétní potřebné IDP řešení nenašel adekvátní produkt. Pro funkci IDS by bylo možné použít například *Cisco Intrusion Detection System 4215 Sensor (IDS-4215-K9) Network Monitoring Device* (cca 120 000 Kč).

Přes možné alternativy jsem do svého návrh jsem zvolil produkt *Netscreen*, protože internetová prezentace, kterou jsem shlédl, mne přesvědčila o jeho

kvalitách. Možností by také bylo zvolit integrované řešení v podobě firewallu + IDS. To však neposkytne takovou míru zabezpečení a pokud bude prolomen firewall, bude zkompromitován i IDS.

Příslušenství

Pro zkompletování sítě volím následující příslušenství v rámci filosofie návrhu středně velké rychlé sítě. Tato síť má vyhovovat podniku, jenž vyžaduje spolehlivost a rychlost sítě.

Tab. č. 5 – Příslušenství

Produkt	Cena (s DPH)
3Com SuperStack 3 Switch 4250T 48-Port Plus 2 10/100/1000 (pro privátní síť)	31 678,- Kč
3Com SuperStack 3 Switch 4228G 24-Port Plus 2 10/100/1000 (pro DMZ)	18 326,- Kč
Záložní zdroj napájení APC Back-UPS CS 650I pro aktivní prvky (switche) a servery – 5 ks	15 785,- Kč
Příslušenství celkem	65 789,- Kč

Dále by bylo vhodné použít RACK na servery (pokud je daný server v rack provedení) a na switche.

Shrnutí

Hardware byl vybírán v duchu celého návrhu zabezpečení, tedy aby poskytl výkon a bezpečnost tam, kde je to zapotřebí, a nevázal zbytečně finanční prostředky.

Tab. č. 6 – Přehled vybraného hardwaru

Produkt	Cena (s DPH)
Server pro firewall	7 000,- Kč
Poštovní server	6 000,- Kč
Servery	112 458,- Kč
NETSCREEN-IDP 10 IDP Appliance	* 161 868,- Kč
Příslušenství	65 789,- Kč
HARDWARE CELKEM	**353 115,- Kč**

** Ceny, které vychází z cizích měn, jsou přepočítávány na Kč kurzem ČNB ze dne 20. 11. 2004 (1 USD = 23,906 Kč) a jsou zaokrouhleny na celé Kč nahoru.*

3.4.2. Software

Při rozhodování o tom, jaký systém a tedy další software nasadit, bychom měli zvážit několik hledisek. Zaprvé zde hraje roli cena, můžeme volit mezi komerčním a „free" softwarem. Nicméně je dobré si uvědomit, že volbou některého ze systémů Windows si ušetříme mnoho práce při konfiguraci firewallů atd. Systémy na bázi Unixu jsou zpravidla náročné na správu a konfiguraci, to je však vyváženo tím, že za ně nemusíme platit.

Návrh řešení, kterým se tato práce zabývá, se snaží předvést zabezpečení s ohledem na finanční náročnost při dosažení vysoké úrovně bezpečnosti. Vzhledem k širokému okruhu možností a finančním nárokům je tedy výhodnou volbou zaměřit se na Open Source software. Není to nijak špatná volba, protože mnoho hlavních volně dostupných operačních systémů poskytuje kvalitní software pro síťovou bezpečnost. Mnoho z těchto „free" řešení je také implementováno do komerčních produktů.

V otázce volby antivirového softwaru jsem se přiklonil k antivirům *NOD 32*. Kvalita těchto antivirů byla mnohokrát oceněna a prokázána v různých testech. Úspěšnost *NOD 32* se blíží ke 100%. Navíc je tento systém velice rychlý a díky použité programové technologii nezatěžuje tolik vlastní počítač.

Firewall

Na server plnící roli firewallu jsem zvolil operační systém *FreeBSD* (obecně tedy OS z rodiny BSD, založený na formě UNIXu).

Firewall jsem vybral opět z řad volně šiřitelných produktů. Zvolil jsem kombinaci paketového filtru a aplikační brány: *IPFilter* (je implementován v operačním systému FreeBSD) + *TIS Firewall Toolkit*.

Tab. č. 7 – Software pro firewall

Produkt	Cena (s DPH)
FreeBSD	zdrama
IPFilter + TIS Firewall Toolkit	zdarma

IPFilter umí filtrovat pakety, přesměrovat provoz a maskovat IP adresy (Network Address Translation - NAT). Konfigurace tohoto řešení však vyžaduje zkušeného administrátora.

Mail Server: licence pro 20 uživatelů

Tab. č. 8– Software pro poštovní server

Produkt	Cena (s DPH)
Kerio Mail Server 5	14 730,- Kč
Antivirus - NOD32 pro Kerio MailServer	7 200,- Kč

Servery

Na tyto servery volím operační systém Red Hat Enterprise Linux 2.1, který vyhovuje jejich požadavkům.

Tab. č. 9 – Software pro servery

Produkt	Cena (s DPH)
Red Hat Enterprise Linux 2.1	19 320,- Kč
Antivirus - NOD32 pro Linux File Server	20 000,- Kč

Stanice: licence pro 20 instalací

Tab. č. 10 – Software pro pracovní stanice

Produkt	Cena (s DPH)
Windows XP Professional + Service Pack 2	92 560,- Kč
Agnitum Outpost Firewall PRO 2.5	16 734,- Kč
Antivirus - NOD32 pro Windows 95/98/ME/NT/2000/XP	14 000,- Kč

Service Pack 2 pro Windows XP obsahuje *Windows XP Firewall*. Ten poskytuje základní ochranu, nefiltruje odchozí provoz, nedokáže blokovat trojské koně a emailové červy a nedetekuje DoS útoky.

Pro vyšší míru zabezpečení pracovních stanic jsem navíc použil *Outpost Firewall PRO 2.5*, produkt firmy Agnitum, který si svou kvalitou získal mnoho příznivců. Možností je tedy použít Outpost Firewall přes Windows XP Firewall.

Shrnutí

Vybraný software má mnoho alternativ. Mou snahou bylo zkombinovat „free" software s komerčním takovým způsobem, aby poskytl kvalitní bezpečnost v co nejoptimálnějším složení pro poměr „cena x kvalita". Z tohoto důvodu jsem například pro operační systém na firewallový server nasadil FreeBSD systém a naproti tomu jsem při výběru antivirového systému volil komerční NOD32 – a to díky jeho kvalitě. Pro pracovní stanice jsem vybral systém Windows XP Professional pro jeho obecnou uživatelskou přijatelnost.

Tab. č. 11 – Přehled nasazeného softwaru

Produkt	Cena (s DPH)
FreeBSD – operační systém	zdarma
Kerio Mail Server 5	14 730,- Kč
NOD32 pro Kerio MailServer	7 200,- Kč
Red Hat Enterprise Linux 2.1 and 3 SLES 8	19 320,- Kč
NOD32 pro Linux File Server (2 servery)	20 000,- Kč
Windows XP Professional + Service Pack 2 (20 uživ.)	92 560,- Kč
Agnitum Outpost Firewall PRO 2.5	* 16 734,- Kč
NOD32 pro Windows 95/98/ME/NT/2000/XP	14 000,- Kč
SOFTWARE CELKEM	**184 544,- Kč**

** Ceny softwaru, které vychází z cizích měn, jsou přepočítávány na Kč kurzem ČNB ze dne 20. 11. 2004 (1 USD = 23,906 Kč).*

3.5. ZÁVĚREČNÉ SHRNUTÍ

Pro shrnutí zmíním, že služby, které by měly být veřejně dostupné, lze určit podle potřeby. Běžnou volbou pro spuštění v DMZ je HTTP server. Další častou volbou je mít poštovní server a DNS (Domain Name Server) server pro virtual domain hosting.

Na trhu je mnoho dostupných řešení, doporučuji však vybrat takové, co známe, máme s ním (dobré) zkušenosti a má pozitivní odborné ohlasy (v různých testech, které se na Internetu hojně vyskytují). Při neznalosti toho, jak určitý software obsluhovat, je dobré hledat jiné řešení. Například pokud nevíme jak konfigurovat a ovládat DNS a potřebujeme jej pro virtual domain hosting, lze využít externí DNS servery. Existuje finančně nenáročná možnost pronajmout DNS server. Je také možné požádat svého providera, aby pro nás hostoval tyto domény na svém nameserveru (což je počítač se službou, která konvertuje názvy internetových domén na IP adresy a naopak).

4. HODNOCENÍ NAVRŽENÉHO ŘEŠENÍ

Cílem bakalářské práce je vytvořit návrh na zabezpečení počítačové sítě připojované k vnější síti. Hlavními body řešení je vytvoření striktní bezpečnostní politiky a návrh struktury sítě včetně jejího zapojení a volby vhodného softwaru.

V technickém zhodnocení je popsán výsledný návrh a jeho přínos.

Ekonomická část hodnocení podává přehled o finančních nákladech na realizaci navrhované sítě.

4.1. TECHNICKÉ HODNOCENÍ NÁVRHU

Prezentovaná struktura sítě představuje vyvážené řešení mezi bezpečností a riziky, ale rozhodně není bez skulin v bezpečnosti, ani to není nejbezpečnější řešení, jaké kdy bylo navrženo. Představuje však dobrý základ, na který by mohlo být navázáno jeho zlepšováním a adaptováním na základě konkrétních potřeb.

Řešené zabezpečení se opírá o definování bezpečnostní politiky, na jejímž základě jsou předložena organizační a technická opatření zajišťující obranu proti vnitřním hrozbám.

V dalších krocích je navržena samotná struktura sítě. Ta je tvořena vnitřní sítí a demilitarizovanou zónou, nad nimiž stojí firewall a IDP (Intrusion Detection and Prevention). Firewall, který tvoří první linii zabezpečení, je realizován na samostatném serveru, čímž má být dosaženo snahy o jeho maximální robustnost a stabilitu při zachování co nejvyšší bezpečnosti. Druhá linie zabezpečení je tvořena IDP zařízením, které je zapojeno za firewallem. Hlavním přínosem tohoto řešení je dosažení vyšší míry zabezpečení. Existující řešení, které kombinuje firewall a IDP může být snáze prolomeno právě díky vzájemné integraci obou prvků. Využití demilitarizované zóny, ve které jsou provozovány povolené služby jako poštovní server a file server, přináší další vrstvu zabezpečení.

4.2. EKONOMICKÉ HODNOCENÍ NÁVRHU

Výsledkem bakalářské práce je návrh zabezpečení sítě pro středně velký podnik, jenž klade důraz na její bezpečnost. Proto jsem volil některá zařízení, jejich náklady se znatelně projevily do celkové ceny návrhu. Jedná se konkrétně o zařízení Netscreen-IDP 10, jehož kvalita však může nabídnout velmi vysokou míru zabezpečení. Na druhou stranu jsem pro některá řešení (server pro firewall) zvolil zařízení s nízkými náklady.

Tab. č. 12 – Celkové náklady navrhovaného řešení

Produkt	Cena
Hardware	353 115,- Kč
Software	184 544,- Kč
CELKEM	**537 659,- Kč**

Celkové náklady na kompletní realizaci navrhované sítě s jejím zabezpečením.

ZÁVĚR

Bakalářská práce předkládá návrh na zabezpečení chráněné počítačové sítě ke vzdálené síti. Práce řeší strukturu sítě vzhledem k její bezpečnosti a dále implementaci bezpečnostních prvků a v softwarové, hardwarové, organizační a technické podobě.

V úvodní části byl proveden rozbor současného stavu formou analýzy problematiky informační bezpečnosti při práci v datových sítích. Tato část analyzuje bezpečnost Internetu, důvod rizik a možnosti napadení.

Dále byla vypracována analýza řešení pro bezpečnost datových sítí. Tato část pojednává o možnostech a formách použití firewallu. Dále řeší z komplexního hlediska antivirovou ochranu formou možností jejího nasazení na konkrétních úrovních.

Následující část zpracovává konkrétní návrh zabezpečení připojované sítě. Vzhledem ke snaze o komplexní řešení se zaměřením na vysokou míru bezpečnosti se návrh zabývá i samotným vytvořením chráněné sítě spolu s finančním ohodnocením použitých prvků, čímž se dostává mírně nad rámec zadání bakalářské práce.

V kapitole hodnocení řešení je návrh posouzen z technického i ekonomického hlediska spolu s vyčíslením celkových nákladů.

Předložený návrh struktury sítě spolu s jejím zabezpečením je určen pro středně velký podnik s přibližně 20 uživateli, který klade důraz na bezpečnost své datové sítě. Řešení poskytuje poměrně vysokou míru zabezpečení při přijatelných nákladech.

SEZNAM POUŽITÉ LITERATURY

[1] LÁTAL, I: Ochrana informací, dat a počítačových systémů. Eurounion, Praha 1996

[2] RODRYČOVÁ, D; STAŠA, P: Bezpečnost informací jako podmínka prosperity firmy, Grada, Praha 2000

[3] URL: http://www.linux.cz/seminare/prudka1999/bezpecnost_a_sprava.html (12. 11. 2004)

[4] URL: http://www.freebsd.org/ (10. 11. 2004)

[5] URL: http://coombs.anu.edu.au/ipfilter/ (11. 11. 2004)

[6] URL: http://www.actinet.cz/bezpecnost_informacnich_technologii/l19/cl25/st1/j1/Uvod_do_IDS/IPS.html (20. 11. 2004)

[7] URL: http://www.spacecentersystems.com/catalog/product_info.php/products_id/256993 (18. 11. 204)

[8] MITNICK, Kevin – SIMON, William: Umění klamu. Helion, Gliwice 2003.

[9] URL: http://www.fi.muni.cz/usr/jkucera/pv109/2003p/xsimek3sociotechnika.htm

[10] CURTIS, G.: Business Information Systems, 3-rd edd., Addison-Wesley, 1999