Technická univerzita v Liberci
Hospodářská fakulta

Studijní program: 6208T – Systémové inženýrství a informatika
Studijní obor: 62-53-705 – Manžerská informatika

Návrh bezpečnostního zajištění IS podniku

Enterprise's IS security design

DP-MI-KIN-2004 12

Ondřej Mlejnek

Vedoucí práce: Ing. Klára Antlová, PhD (katedra informatiky)
Konzultant : RNDr. Pavel Satrapa (katedra inženýrské informatiky, FM TUL)

Počet stran: 69
Počet příloh: 2
Datum odevzdání 5. ledna 2004

Katedra informatiky **Školní rok 2003/2004**

ZADÁNÍ DIPLOMOVÉ PRÁCE

pro :

Ondřej Mlejnek

Studijní program:

Systémové inženýrství a informatika (6209T)

Studijní obor č. M 6209

Manažerská informatika

Vedoucí katedry Vám ve smyslu zákona č. 1111/1998 Sb. o vysokých školách a navazujících předpisů určuje tuto diplomovou práci:

Název tématu:

Návrh bezpečnostního zajištění IS podniku

Zásady pro vypracování:

1. Koncepce bezpečnosti IS.
2. Hrozby a rizika, možnosti ochrany.
3. Návrh informačního zabezpečení ve firmě.

Rozsah diplomové práce: 50 - 60
(do rozsahu nejsou započítány úvodní listy, přehled literatury a přílohy)

Doporučená literatura:

1. Dobda, L: Ochrana dat v informačních systémech. Grada, Praha 1998.
2. Látal, I: Ochrana informací, dat a počítačových systémů. Eurounion, Praha 1996.
3. Rodryčová, D; Staša, P: Bezpečnost informací jako podmínka prosperity firmy. Grada, Praha 2000.
4. Dunsmore, B; Brown, J. W; Cross, M.:Mission

Vedoucí diplomové práce: Ing. Klára Antlová

Odborný konzultant: RNDr. Pavel Satrapa

Termín odevzdání diplomové práce: 5.1.2004

Prof. Ing. Jan Ehleman, CSc.
vedoucí katedry

Technická univerzita v Liberci
Hospodářská fakulta

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

V Liberci dne 31.3.2003

Prohlašuji, že jsem diplomovou práci vypracoval samostatně s použitím uvedené literatury pod vedením vedoucího a konzultanta. Byl jsem seznámen s tím, že na mou diplomovou práci se plně vztahuje zákon č. 121/2000 o právu autorském, zejména § 60 (školní dílo) a § 35 (o nevýdělečném užití díla k vnitřní potřebě školy).

Beru na vědomí, že TUL má právo na uzavření licenční smlouvy o užití mé práce a prohlašuji, že souhlasím s případným užitím mé práce (prodej, zapůjčení apod.)

Jsem si vědom toho, že užití své diplomní práce či poskytnutí licenci k jejímu užití mohu jen se souhlasem TUL, která má právo ode mne požadovat přiměřený příspěvek na úhradu nákladů, vynaložených univerzitou na vytvoření díla (až do její skutečné výše).

Po pěti letech si mohu tuto práci vyžádat v Univerzitní knihovně TU v Liberci, kde je uložena, a tím výše uvedená omezení vůči mé osobě končí.

V Liberci dne 5. ledna 2004 ..... Ondřej Mejzlík

Resumé

Tato diplomová práce má za cíl popsat jednotlivé aspekty bezpečnostního zabezpečení informačního systému v podniku, a to jak z teoretického, tak praktického pohledu. Práce postihuje obecnou koncepci bezpečnosti informačního systému a mapuje jednotlivé prvky v systému bezpečnostních opatření. V práci se věnuji také hrozbám a útokům, které ohrožují správnou funkci informačního systému podniku, především pak s ohledem na stále výraznější vliv celosvětové sítě Internet. V souvislosti s tím uvádím i možná řešení zabezpečení podnikové sítě, která může být cílem řady těchto útoků. V závěru pak navrhuji možné zabezpečení sítě v modelovém podniku ze segmentu malých a středních firem, podnikajících i prostřednictvím elektronického obchodování včetně vyčíslení finančních nákladů.

Abstract

This thesis' goal is to describe individual aspects of an enterprise information system security from theoretical as well as from practical point of view. This work deals with general concepts of information system security and maps individual components in security precaution system. I pay attention to possible threats and attacks that can endanger information system of an organization as well, especially regarding to ever growing influence of world-wide Internet network. In this context, I mention possible solutions for securing an enterprise's network, which could be the objective of such attacks. Finally, I introduce a network security design for a model company with e-commerce site from small/middle sized enterprise segment, including financial costs.

Obsah

Seznam obrázků

Seznam tabulek

Seznam použitých zkratek

AAA	Authentication, Autorization, Accontability – architektura systému autorizace
ACK	Acknowledgment – potvrzení
apod.	a podobně
ARP	Automatic Repeat Request – automatický požadavek na opakování, protokol pro kontrolu chyb
atd.	a tak dále
BOOTP	Bootstrap Protocol – samozaváděcí protokol
CRC	Cyclic Redundancy Check – cyklická kontrola nadbytečnosti
DDoS	Distributed Denial of Service – distribuovaný útok typu DoS
DHCP	Dynamic Host Configuration Protocol – protokol pro dynamické přidělování adres
DMZ	demilitarizovaná zóna
DoS	Denial of Service – útok typu odmítnutí služby
DSA	Digital Signature Algorithm – šifrovací algoritmus
FTP	File Transfer Protocol – protokol pro přenos souborů
HTTP	Hypertext Transfer Protocol – hypertextový přenosový protokol
CHAP	Challenge Handshake Authentication Protocol – protokol ověřující heslo
ICMP	Internet Control Message Protocol – protokol řídících zpráv Internetu
IDS	Intrusion Detection System – systém pro detekci vniknutí
IGMP	Internet Group Management Protocol – část IP protokolu pro skupinové adresování počítačů
IMAP	Internet Message Access Protocol – protokol umožňující klientovi přístup a manipulaci s elektronickou poštou na serveru
IP	Internet Protocol – protokol síťové vrstvy modelu TCP/IP, zajišťuje adresovací schéma celé sítě přenosem datagramů

IPSec	IP secured – zabezpečený Internetový protokol, norma pro šifrování paketu IP
IS	informační systém
ISAC	Information Sharing And Analysis Center – sdružení firem z USA, které má v úzké spolupráci s FBI napomoci zvyšovat elektronickou bezpečnost
IT	informační technologie
LAN	Local Area Network – lokální počítačová síť
MAC	Media Access Control – řízení přístupu na médium, spodní část linkové vrstvy
MB	mega byte
MD	Message Digest – transformační funkce pro tvorbu kontrolního součtu
MHz	megahertz
mj.	mimo jiné
MS	Microsoft
MTU	Maximum Transmission Unit – maximální jednotka přenosu
NAT	Network Address Translation – překlad síťových adres
např.	například
NFS	Network File System – síťový souborový systém nezávislý na prostředí
obr.	obrázek
OS	operační systém
OSI	Open Systems Interconnection – otevřené propojení systémů, standardizační program ISO
PAP	Printer Access Protocol – protokol přístupu k tiskárně
PC	Personal Computer – osobní počítač
PEM	PRIVACY ENHANCED MAIL – pošta s vyšší ochranou soukromí, využívá šifrování
PGP	Pretty Good Privacy – program pro zabezpečení a šifrování e-mailových zpráv
PIN	Personal Identification Number – osobní identifikační číslo
PKI	Public Key Infrastructure – infrastruktura veřejných klíčů
příp.	případně
RADIUS	Remote Authentization Dial-in User Service – vzdálená autentizace uživatele na komutované lince
RAM	Random Access Memory – operační paměť s přímým/náhodným přístupem
RARP	Reverze Address Resolution Protocol – reverzní protokol pro rozpoznání adresy
resp.	respektive
RFC	Request for Comments – definice standardů protokolů
RIPE	Réseaux IP Européens – skupina pro spolupráci s evropskými sítěmi
RSA	Rivest-Shamir-Adelman – asymetrický šifrovací algoritmus
SET	Secure Electronic Transaction – bezpečné elektronické transakce

S-HTTP	Secure Hypertext Transport Protocol – hypertextový protokol s bezpečnostní vrstvou
S-MIME	Secure Multipurpose Internet Mail Extension – bezpečné rozšíření Internetové pošty
SMS	Short Message Service – služba pro krátké textové zprávy
SMTP	Simple Mail Transfer Protocol – jednoduchý protokol pro přenos elektronické pošty v síti TCP/IP
SNMP	Simple Network Management Protocol – protokol pro snadné řízení sítě
SOHO	Small Office/Home Office – segment trhu počítačů a spotřebního zboží vhodná pro malé kanceláře nebo domácí použití
SQL	Structured Query Language – strukturovaný dotazovací jazyk
SSH	Secure Shell – šifrovaná obdoba protokolu Telnet nebo Rlogin
SSL	Secure Socket Layer – protokol pro zajištění bezpečeného přenosu dat
TACACS	Terminal Access Controller Access Controller System – protokol pro řízení přístupu terminálů
tab.	tabulka
TCP	Transmission Control Protocol – přenosový řídící protokol
TCP/IP	Transimission Control Protocol/Internet Protocol – soustava síťových protokolů
TFTP	Trivial File Transfer Protocol – zjednodušený protokol pro přenos souborů
tj.	to je
TLS	Transport Layer Security – bezpečnostní protokol
UDP	User Datagram Protocol – nespojovaný protokol transportní vrstvy pro přenos zpráv
UPS	Uninterruptible Power Supply – nepřerušitelný napájecí zdroj
vč.	včetně
VPN	Virtual Private Network – virtuální privátní sítě
WAN	Wide Area Network – rozlehlá síť
WWW	World Wide Web – distribuovaný hypertextový informační systém
XDR	External Data Representation – výměnný datový formát

Úvod

V první části (kapitoly 1–4) této práce se věnuji teoretickým poznatkům z oblasti bezpečnosti informačních systémů. Nejdříve vysvětlím důležité pojmy z oboru, dále uvádím obecné členění bezpečnosti a tento model později podrobněji popisuji. V další části pak rozebírám teoretické možnosti ochrany IS a v závěru první kapitoly se podrobněji věnuji bezpečnostní politice jako základnímu východisku při zavádění bezpečnosti IS. Jednotlivé části jsou pak doplněny reálnými daty z praxe – průzkumy provedenými v oblasti bezpečnosti IS podniků.

V druhé kapitole se zabývám problematikou bezpečnosti v síti Internet – nejprve popisuji vrstvový síťový model TCP/IP a v druhé části této kapitoly uvádím některé bezpečnostních mechanizmy jednotlivých vrstev modelu.

Kapitola 3 je věnována hrozbám a útokům, které ohrožují funkčnost informačního systému společnosti. Podrobně popisuji jednotlivé útoky na IS podniku vedené z nezabezpečené sítě Internet, která je zřejmě největší hrozbou bezpečnosti IS.

Nejobsáhlejší je část následující – kapitola 4 – ve které uvádím způsoby a prostředky zabezpečení a obrany informačního systému proti možným útokům. Podrobněji se pak zabývám firewally, které jsou nejdůležitějším prvkem v celkovém modelu zabezpečení sítě – uvádím základní principy jejich fungování a jednotlivá funkční řešení jejich uspořádání. Kromě toho se věnuji i dalším prostředkům zabezpečení jako jsou systémy IDS nebo antivirová ocrhana, v závěru kapitoly popisuji principy elektronického podepisování a struktutry PKI.

Pátá kapitola je věnována praktickému návrhu zabezpečení IS v modelovém podniku. Nejprve charakterizuji modelový podnik, jež je představitelem typické malé obchodní organizace. Firma obchoduje i prostřednictvím elektronického

obchodu a tak je zabezpečení IS tohoto podniku především zabezpečením vnitřní sítě proti útokům z Internetu. V navrhovaném modelu zabezpečení využívám teoretických poznatků z předchozích kapitol, především částí věnovaných firewallům. Při volbě vhodného firewallu zahrnuji i alternativní metodu zabezpečení formou softwarového řešení na bázi OS Linux. Bezpečnost IS však neznamená pouze technické prostředky ochrany, a tak uvádím i jiné způsoby, které zvyšují bezpečnost systému. V závěru této kapitoly pak přehledně vyčísluji i náklady spojené s navrhovaným zabezpečením informačního systému.

Kapitola 1
Koncepce bezpečnosti IS

1.1 Informační bezpečnost

Informační bezpečnost jako obor zabývající se zabezpečením informací v informačních systémech je relativně novým pojmem. Jeho počátky je možné vysledovat již v první polovině 80. let v období, kdy se v masovém měřítku začínají přesouvat agendy a data všeho druhu do privátních informačních systémů. Takovéto systémy se rázem stávají centrem soustředění nesmírných hodnot. Finanční instituce vedou ve svých informačních systémech evidence účtů svých klientů, podniky je používají pro řízení výroby, armády do nich umisťují i ty nejutajovanější informace o obraně států.

S rozvojem moderních informačních technologií a nasazováním informačních systémů do podniků však vzrůstá i možnost jejich zneužití. Rozsah problematiky počítačové kriminality dokumentuje i preambule Manuálu pro prevenci a kontrolu počítačové kriminality OSN: „Rozvoj světa informačních technologií s sebou nese i stinné stránky: otevřel dveře protispolečenskému a kriminálnímu chování způsobem, který by nikdy předtím nebyl možný. Počítačové systémy nabízejí nové a vysoce sofistikované možnosti porušování práva a především potenciálu pro páchání tradičních typů zločinů netradiční cestou. K ekonomickým škodám, které počítačová kriminalita přináší, je třeba připočíst závislost celého lidstva na počítačových systémech doslova ve všech oblastech denního života, od řízení letového provozu, železniční a autobusové dopravy po zdravotnictví a národní obranu. I jen malá chyba v počítačovém systému může znamenat ohrožení lid-

ských životů. Závislost společnosti na počítačových systémech má tedy hluboký lidský rozměr. Rychlé mezinárodní rozšiřování velkých počítačových sítí a možnost přistupovat k mnoha systémům skrze běžné telefonní linky zvyšuje zranitelnost těchto systémů a možnosti jejich zneužití nebo páchání kriminálních činů. Následky počítačové kriminality má tedy kromě vážných ekonomických nákladů také značné náklady z pohledu lidské bezpečnosti". [OSN94]

Systém zabezpečení informačního systému připomíná systém zabezpečení a ochrany významného objektu. Hlavním cílem je komplexnost a provázanost jednotlivých dílčích opatření. Pro dosažení maximálního účinku je nutná spolupráce informační bezpečnosti s osobní, majetkovou a dalšími typy zabezpečení příslušné organizace. Cílem provozovatele IS musí být zajistit co nejvyšší bezpečnost systému, což zaručuje minimální úniky a možnosti zneužití informací; v případě selhání některého bezpečnostního mechanizmu pak musí co nejrychleji dosáhnout původní stavu před daným incidentem.

Pod pojmem informační bezpečnost tedy chápeme ochranu informací během jejich vzniku, zpracování, ukládání, přenosů a likvidace prostřednictvím logických, technických, fyzických a organizačních opatření, která musí působit proti ztrátě důvěrnosti, integrity a dostupnosti (těmto třem stěžejním pojmům informační bezpečnosti se podrobněji věnuji v další části práce) těchto hodnot. [DOB98]

Říha [ŘÍH02] definuje informační bezpečnost jako „všechny aspekty související s definováním, dosažením a udržením důvěrnosti, dostupnosti, individuální zodpovědnosti, autenticity a spolehlivosti".

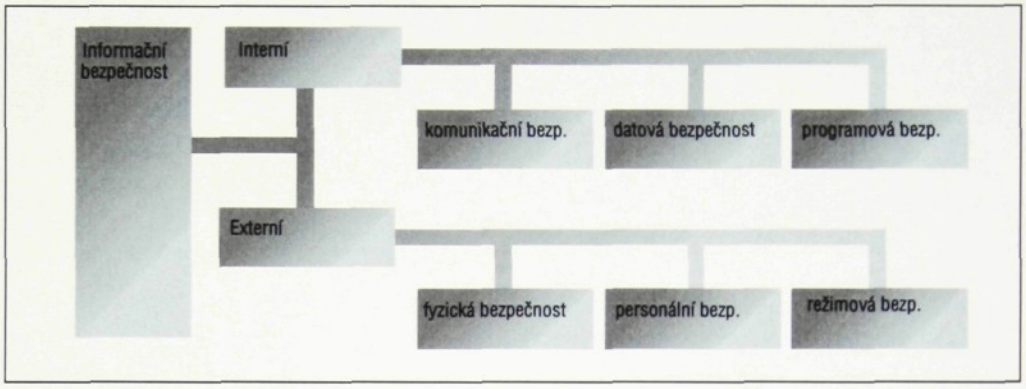
1.2 Bezpečnostní dekompozice IS

Každý informační systém se zpravidla skládá z několika základních částí – části datové, programové, technické a komunikační a osob, které systém využívají a provozují. Bezpečnost každé části informačního systému hraje nezastupitelnou roli při zajištění bezpečnosti celého informačního systému. Celková bezpečnost informačního systému je tedy dána bezpečností jeho jednotlivých částí, zejména pak části nejslabší. Je nutné si také uvědomit, že hlavním činitelem, který může ohrozit či napadnout informační systém je především člověk.

Nejobecnějším dělením informační bezpečnosti je rozdělení na interní a externí bezpečnost. Další dělení je patrné z obrázku 1.1.

1.2.1 Fyzická bezpečnost

Fyzickou bezpečností informačního systému se rozumí podle vyhlášky [NBU56] opatření použitá k zajištění fyzické ochrany aktiv informačního systému proti



Obr. 1.1 Dělení informační bezpečnosti. Zdroj: [lát96]

náhodným nebo úmyslným hrozbám. Je to tedy ochrana IS a jeho součástí proti neoprávněnému vniknutí osob, způsoby ničení již nepotřebných informací nebo již nepotřebných médií s informacemi, ukládání médií s informacemi, ochrana proti požáru, proti přírodním vlivům, nahodilým pohromám a haváriím. Zahrnuje všechna opatření, která slouží k zajištění fyzické ochrany aktiv proti náhodným a úmyslným hrozbám. Zajišťuje ochranu hmotných aktiv pomocí technických prostředků ochrany. Vyhláška Národního bezpečnostního úřadu [NBU339] stanovuje způsoby zabezpečení ochrany objektů, technické prostředky, použití technických prostředků, podmínky nasazení fyzické ostrahy a režimová opatření pro účely zajištění objektové bezpečnosti.

1.2.2 Režimová bezpečnost

Režmovou bezpečností rozumíme respektování mezinárodních, národních a interních právních a organizačních norem ve vztahu k existenci a provozu informačních systémů a vytvoření bezpečnostních pravidel provozu informačních systémů.

1.2.3 Bezpečnost personální

Personální bezpečnost je součást informačního systému, ale také ochrany informačního systému před jednáním nebo konkrétními událostmi způsobenými pracovníky. Zabývá se eliminací hrozeb způsobených lidským faktorem. Definuje postupy pro požadované stupně prověřování pracovníků a udělování práv zaměstnancům, kteří jsou seznamování s citlivými informacemi.

1.2.4 Bezpečnost programových prostředků

Touto bezpečností rozumíme nastavení programových (softwarových) prostředků tak, aby byly skutečným filtrem přístupu k informacím obsaženým v daném IS. Znamená to, že je třeba, aby byla zajištěna kontrola přístupu, autentičnosti

a identifikace uživatele, rozdělení pravomocí uživatelů, sledování a záznam činností systému a uživatelů apod.

1.2.5 Bezpečnost dat

Bezpečnost dat znamená ochranu v souborech a v databázích proti chybám, virům, ochranu citlivých dat, autorizaci a rozlišení přístupu k datům a další.

1.2.6 Bezpečnost komunikačních cest

Znamená ochranu komunikací mezi jednotlivými částmi informačního systému, a to nejen mezi prostředky výpočetní techniky, ale i jiné přenosové nebo komunikační techniky (faxové zprávy, přenos řeči telefonických rozhovorů, SMS apod.).

1.2.7 Bezpečnost technických prostředků

Bezpečnost technických prostředků znamená především jejich vhodný výběr a zajištění spolehlivosti a jejich okamžitého servisu, dále pak i kontrolu přístupu k těmto prostředkům a jejich ochranu před elektrostatickou elektřinou a elektromagnetickým zářením. Vyhláška [NBU56] zahrnuje bezpečnost programových prostředků a bezpečnost technických prostředků pod pojem „počítačová bezpečnost".

1.3 Bezpečný informační systém

Bezpečný informační systém můžeme definovat jako systém, který chrání informace během jejich vstupu, zpracování, uložení, přenosu a výstupu proti ztrátě dostupnosti, integrity a důvěrnosti a při jejich likvidaci proti ztrátě důvěrnosti. [LÁT96]

Z filozofického hlediska a z hlediska teorie systémů lze dojít k závěru, že v podstatě neexistuje žádný systém opatření, který by zaručil absolutní bezpečnost informačního systému. Takového stupně lze dosáhnout pouze jeho absolutní izolovaností, tj. vyloučením všech vstupů do a výstupů ze systému. Takový systém by ovšem nebylo možné k ničemu praktickému využít. Zvolený rozsah bezpečnosti efektivně pracujícího systému je proto vždy kompromisem mezi cenou, kterou jsme ochotni za bezpečný systém zaplatit a mírou rizika, kterou jsme ochotni připustit.

1.4 Požadavky na bezpečnost IS

Mezi základní požadavky na bezpečnost IS patří požadavky na dostupnost, integritu a důvěrnost.

1.4.1 Dostupnost

Dostupností rozumíme ochranu před neoprávněným odmítnutím služby nebo nemožností poskytnou informace – je to vlastnost objektů nebo celého informačního systému, která zabraňuje neautorizovanému zadržování zdrojů. Je to tedy vlastnost IS, která zajišťuje, aby data byla na správném místě ve správný čas – informace a služby musí být uživatelům poskytovány systémem včas, bez zbytečných prodlev a v libovolně zvoleném okamžiku. V praxi se dostupnost služeb systému zajišťuje především technickými metodami, které však vždy znamenají zvýšení finanční náročnosti řešení.

1.4.2 Integrita

Integrita vyjadřuje ochranu před neoprávněnou modifikací – celistvost, konzistenci systému a dat, které informační systém obsahuje a jejich shodu s realitou. Je to taková vlastnost objektu, umožňující změnit jej pouze autorizovaným způsobem, bez jakékoliv skryté nebo úmyslné manipulace s hodnotami objektu. Představuje tedy fakt, že objekt je stále platnou reprezentací určité informace. Integrita jako vlastnost objektu minimalizuje možnosti jeho neoprávněných změn.

1.4.3 Důvěrnost

Důvěrností rozumíme ochranu před prozrazením informace – utajení informací před neoprávněným přístupem. Je to charakteristika informace, která znemožňuje její odhalení neoprávněným subjektům. Jsou to funkce, které předcházejí hrozbám neautorizovaného přístupu k informacím a funkce, které řídí uživatelův přístup k objektům a zdrojům IS. Důvěrnost je definována jako vlastnost, kdy informace nemůže být odhalena nebo zneužita neautorizovanou osobou. [HÖN97]

1.5 Základní způsoby ochrany IS

Ochranou informačního systému rozumíme komplex organizačních (administrativních i režimových), technických, programových a sociálně-personálních opatření s cílem minimalizace možných ztrát informací v daném systému vznikajících a obíhajících [LÁT96]

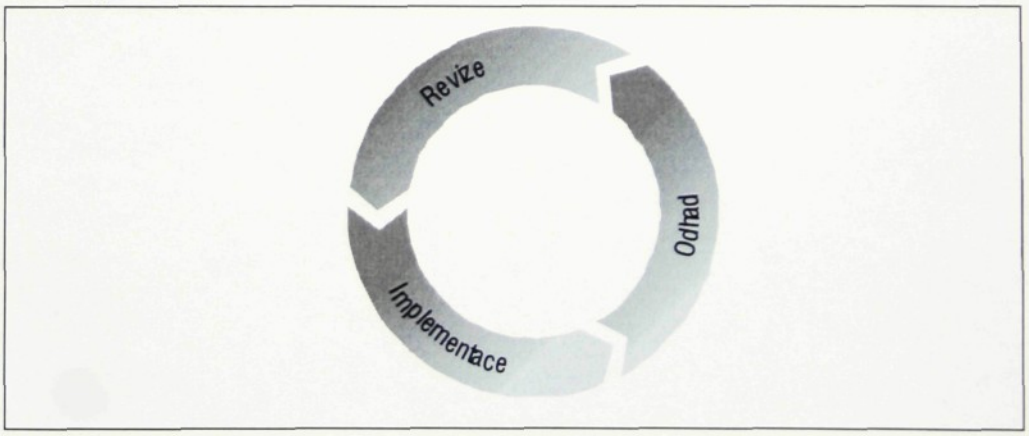
1.5.1 Bezpečnost jako proces

Bezpečnost informací a informačních systémů nelze chápat jinak než jako proces, který zahrnuje celou činnost organizace a její aktiva. Rovněž je nutné si uvědomit, že jednou vytvořená bezpečnost není řešením pro vždy – podmínky, v nichž se informace uchovávají a zpracovávají se totiž neustále mění. Protože bezpečnost se nezabývá jen ochranou, ale i dostupností, jde zvyšování bezpečnosti ruku v ruce s požadavkem na růst technických parametrů systémů. Cyklus zavádění a udržování informační bezpečnosti je pak neustálý proces, který periodicky kontroluje úroveň bezpečnostních opatření a podle potřeby je aktualizuje nebo vylepšuje.

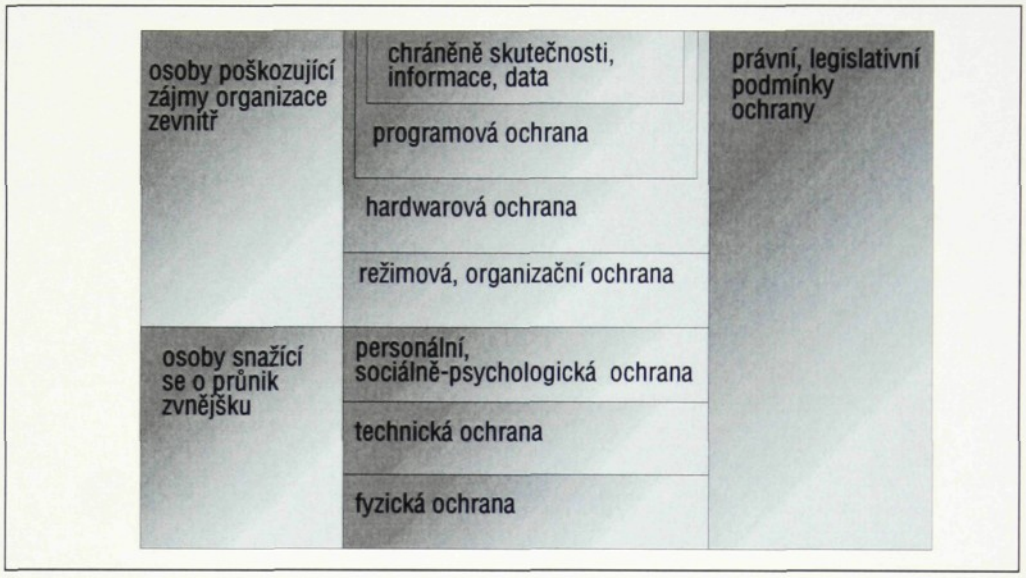
Zajištění bezpečnosti informačních systémů je dle [RUS01] procesem neustálého odhadu bezpečnostní situace (assesment), její zrevidování (revision) a implementace (implementation) změn. Tento proces permanentního vyhodnocování situace a zpětných vazeb vyjadřuje obr. 1.2. Komplexní systém ochrany lze pak vyjádřit schématem na obr. 1.3.

Konkrétní realizace informační bezpečnosti je závislá na mnoha vlivech jako jsou např. velikost systému, citlivost informací, dostupnost technologií či finanční možnosti organizace. Použité způsoby ochrany musí být efektivní, výkonné a přiměřené, aby působily nepřetržitě a uživatelům příliš nepřekážely při rutinní práci. Žádný bezpečnostní mechanismus zatím nedokáže pokrýt celý rozsah požadavků na ochranu a proto se požadované bezpečnostní úrovně dosahuje kombinací více nástrojů a metod.

Bezpečnost informačního systému se tedy vždy realizuje jako kombinace různých bezpečnostních mechanismů a opatření. Podle [EDI96] a dalších autorů v zásadě existují tři způsoby ochrany dat v informačních systémech a ty je možno vzájemně kombinovat. Těmito způsoby jsou organizační, fyzické a logické způsoby ochrany dat.



Obr. 1.2 Proces zajištění bezpečnosti IS. Zdroj [rus01]



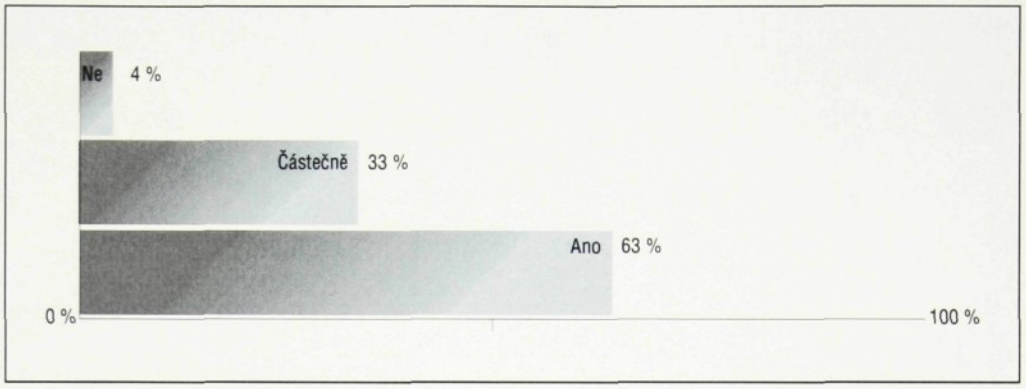
Obr. 1.3 Komplexní systém ochrany IS. Zdroj [lát96]

1.5.2 Organizační způsob ochrany dat

Opatření tohoto charakteru obvykle nejsou příliš nákladná, avšak jejich důsledným dodržováním lze dosáhnout podstatného zvýšení bezpečnosti. Jsou realizována formou vnitropodnikových nařízení a směrnic, které musejí pokrývat celou činnost informačního systému, řešení krizových stavů a zásady personální bezpečnosti. Směrnicemi musí být jasně vymezena a delegována zodpovědnost každého pracovníka za konkrétní věc. Všechna organizační opatření musí být vydávána písemně a každý pracovník s nimi musí být seznámen. Je vhodné provádět periodické ověřování, zda přijatá bezpečnostní opatření stále odpovídají reálné situaci. Tato opatření zahrnují především oblasti vymezení zásad a pravidel pro práci s výpočetní technikou v rámci organizace, určení stupně důvěrnosti a ochrany jednotlivých informací, dále pak personální práci – výběr, školení a prověřování pracovníků, stanovení stupně oprávnění pracovníků k přístupu k jednotlivým typům informací, postup identifikace pracovníka, potřebné ke vstupu do informačního systému, pravidla pro práci s hesly a šifrovými klíči, definice bezpečnostních zón a pravidla řízení vstupu do nich, postup při hlášení podezřelých událostí, které mohou narušit bezpečnost IS, postup při ničení nepotřebných nosičů informací a další činnosti.

1.5.3 Fyzický způsob ochrany dat

Jsou to opatření, použitá k zajištění fyzické ochrany informačního systému proti náhodným a úmyslným hrozbám. Zajišťují ochranu IS pomocí technických prostředků ochrany, jako jsou prostředky proti neoprávněnému vniknutí osob do objektů, ve kterých je informační systém umístěn, ochrana před přírodními vlivy a další. Dále řeší bezpečné uložení médií s informacemi, způsoby ničení již



Obr. 1.4 Graf využití fyzických způsobů zabezpečení. Zdroj [pib01]

nepotřebných informací a médií, nebo např. i zajištění nepřetržité dodávky stabilizované elektrické energie.

Podle průzkumu informační bezpečnosti [PIB01] využívá většina organizací prostředků fyzického zabezpečení k ochraně klíčových komponent IS. Třetina organizací má fyzicky zabezpečené pouze některé komponenty – viz obrázek 1.4.

1.5.4 Logický způsob ochrany dat

Zahrnuje soubor logických, tedy jak softwarových, tak hardwarových opatření, které se uplatňují v daném informačním systému. Do logického způsobu ochrany dat patří technická opatření, která se zabývají mj. kvalitním výběrem a nasazením technických prostředků (hardware) do IS a zajištěním jeho včasného servisu tak, aby nenarušil požadovanou dostupnost zdrojů informací v rámci informačního systému. Kromě technických opatření patří do skupiny logického způsobu ochrany dat i tzv. opatření programová. Programová opatření umožňují chránit informace přímo v počítačích pomocí programových bezpečnostních prostředků. Jde především o kontrolu přístupu, která zabraňuje neoprávněným uživatelům v práci s informacemi, k nimž nemají povolen přístup. Základním způsobem realizace je přístupové heslo. Další opatření můžou spočívat v monitorování činnosti, kdy je sledována a zaznamenávána podezřelá aktivita uživatele.

Identifikace a autentizace

Aby informační systém mohl rozlišovat pravomoci jednotlivých uživatelů, je nutné zajistit jejich identifikaci a autentizaci, stanovit způsob, místo a dobu, tj. jak, kde a kdy se přihlásí do informačního systému. Pouze v případě, že se entita (uživatel, proces) představí a prokáže svoji totožnost, je možné rozhodovat o tom, co smí, k čemu má oprávnění a co má zakázáno.

Identifikace

Identifikací rozumíme rozpoznání určité entity (zpravidla uživatele) informačním systémem, ovšem bez jakéhokoliv dalšího ověřování.

Autentizace

Autentizace je proces ověřování, zpravidla následující po identifikaci, že přihlášená entita je opravdu tím, za koho se vydává. Autentizace je založena na principu porovnávání přístupového identifikátoru uživatele s hodnotou, která je uložena v autentizačním zařízení. Účinná autentizace vyžaduje použití alespoň dvou faktorů identity. Těmito faktory jsou podle [DUN01]:

- **znalost (co daná osoba zná)** – zpravidla hesla a osobní identifikační čísla (PIN), jedná se o nejjednodušší, levné a nejčastěji používané řešení, nevýhodou jsou „slabá" hesla, která se dají snadno uhodnout
- **vlastnictví předmětu (co daná osoba vlastní)** – mechanické identifikátory, hardwarové nebo softwarové klíče (např. různé přístupové karty). Identifikační předmět je zpravidla spolehlivější než běžné přihlášení heslem. Je ovšem finančně náročnější.
- **biometrická identifikace (kdo daná osoba je)** – identifikace je založena na nějaké fyzické vlastnosti lidského těla (např. otisk prstu, obraz očního pozadí, rozpoznání hlasu, charakteristické rysy obličeje apod.). Autentizace je pak založena na fyziologických a biometrických vlastnostech, uživatel nemusí s sebou nic nosit nebo si pamatovat, avšak nevýhodou je značná finanční náročnost řešení.

Dle průzkumu informační bezpečnosti v ČR v roce 2001 [PIB01] naprostá většina (98 %) respondentů uvedla, že v jejich organizaci je vyžadována jednoznačná identifikace a autentizace uživatelů při přihlášení do hlavních systémů. V každé desáté organizaci jsou kromě hesel používány k identifikaci a autentizaci také jiné prvky.

Bezpečné heslo

Drtivá většina lidí používá snadno rozluštitelná hesla. Podle [ZEM03] více než polovina uživatelů používá obecné slovo, desetina má heslo složené pouze z číslic a jen deset až patnáct procent má heslo kombinované. Obecné zásady pro tvorbu odolného hesla jsou tedy:

Z pohledu uživatele:

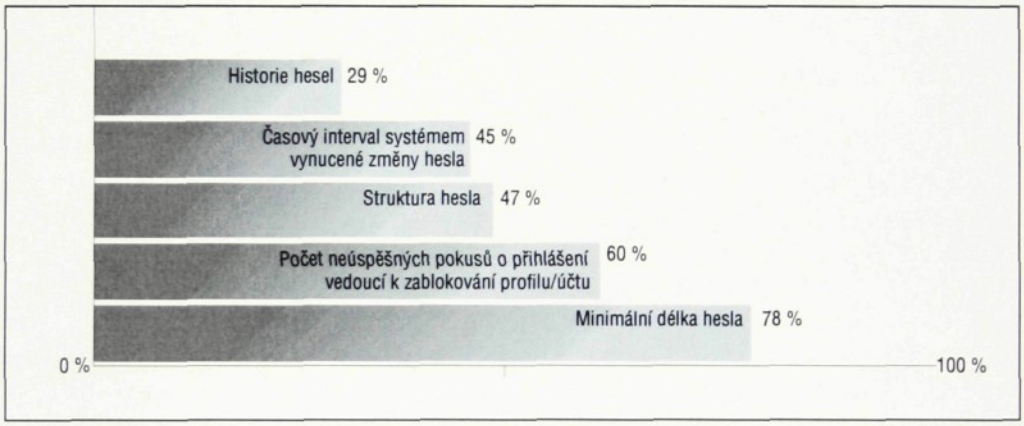
- délka hesla nejméně osm znaků
- nepoužívat obecná slova
- nepoužívat slova spojitelná s vlastní osobou, nikdy nepoužívat heslo totožné s uživatelským jménem

Z pohledu administrátora:

- stanovit počet možných neúspěšných pokusů o přihlášení
- vynutit změnu hesla po určitém časovém úseku

- kontrolovat strukturu hesla (vynutit určitou strukturu, např. použití kombinace čísel a písmen, nemožnost použít jako heslo „slovníková" slova apod.)

Průzkum [PIB01] zjistil, že většina organizací používá pro zdokonalení základní identifikace a autentizace pomocí hesla ještě minimální délku hesla a stanovuje i počet neúspěšných pokusů o přihlášení, po němž dojde k zablokování hesla. Méně než polovina organizací využívá rovněž kontrolu struktury hesla, interval vynucené změny hesla a historii hesel – viz obrázek 1.5. Přičemž je třeba poznamenat, že pouze nastavení všech zmíněných mechanizmů přispívá k rozumné míře ochrany pomocí hesel. Vyřazením jednoho nebo více mechanizmů značně snižuje účinnost zabezpečení. Pouze 9 % organizací využívá všechny zmíněné parametry hesel.

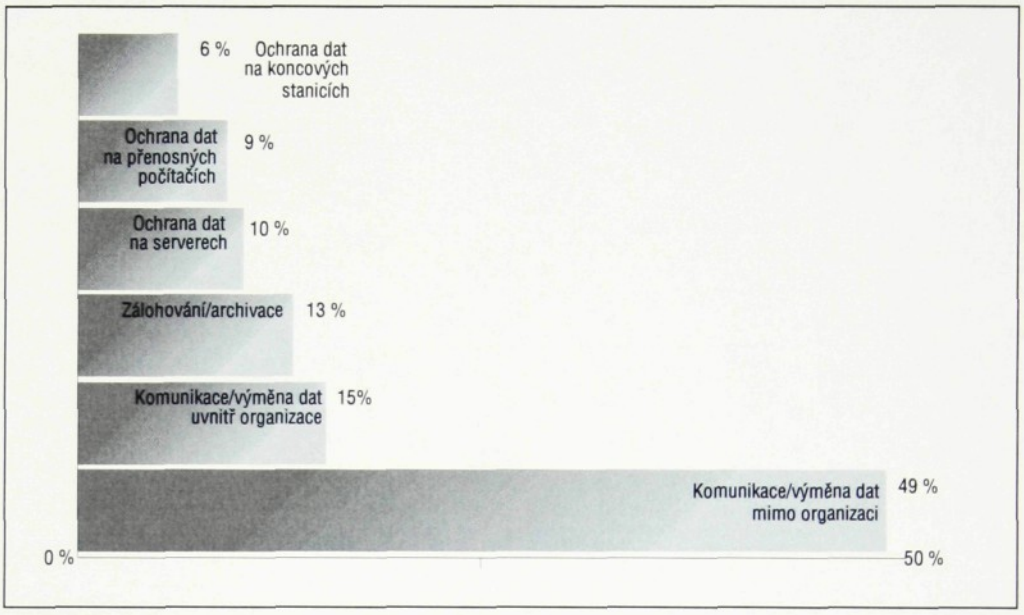


Obr. 1.5 Graf využití možností nastavení parametrů přístupového hesla. Zdroj [pib01]

Šifrování

Matyáš [MAT00] definuje kryptografii jako je vědu (a zčásti i umění) o tvorbě šifrovacích a dešifrovacích algoritmů. Kryptografie poskytuje řadu technik k utajení obsahu dat a zpráv, aby byly zabezpečeny při ukládání a přenosu – transformuje data takovým způsobem, aby nebyla běžnými prostředky čitelná. V případě odcizení šifrovaných dat nedojde, pokud zloděj nemá i šifrovací klíč, k úniku informací. Šifrování je považováno za nejdokonalejší způsob zabezpečení informací zejména při přenosech pomocí veřejných komunikačních sítí vč. Internetu.

Průzkum [PIB01] uvádí, že nejčastěji je šifrování používáno v souvislosti s komunikací mimo organizaci (49 %), v jiných oblastech je šifrování využíváno výrazně méně. V jakých souvislostech používají organizace šifrování zobrazuje obrázek č. 1.6.



Obr. 1.6 Graf využití šifrování jako prostředku zabezpečení IS. Zdroj [pib01]

Zálohování

Je to proces, ve kterém se v daném čase vytvoří jedna nebo více kopií požadovaných informací na záložních datových médiích, ze kterých může být v případě havárie nebo jiného selhání systému obnoven původní stav. Zálohování patří k jednomu z nejvýznamnějších nástrojů ochrany dat. Je to prevence, pojistka pro případ výpadku systému, selhání nebo katastrofy, která umožňuje uvést informační systém do původního nepoškozeného stavu. Vytváření záloh můžeme dělit na provozní a archivační.

Antivirová ochrana

Ochrana proti virům má své stálé místo v celkovém modelu bezpečnosti. Antivirová ochrana je jedním z bezpečnostních projektů týkajících se širokého okolí provozu IS a jeho uživatelů a nelze ji zjednodušit na jednorázovou instalaci antivirového produktu. Je třeba definovat uzavřenou antivirovou politiku, definovat práva a povinnosti všech, kteří jí mohou být dotčeni, určit časové návaznosti realizačních kroků apod.

Průzkum [PIB03A] uvádí, že nejčastějším bezpečnostním incidentem v podniku je virus rozšířený prostřednictvím elektronické pošty – v 89 % respondentů, vysoké je i procento rozšíření výskytu virů ze souborů stažených z Internetu.

Jednotlivé typy antivirového software se vzájemně liší buď umístěním (klient, server, brána) anebo tím, co prohledávají (elektronickou poštu, přenos souborů, komunikaci s webem). Více se budu možnostem antivirové ochrany věnovat v kapitole pojednávající o prostředcích obrany v sítích.

1.5.5 Ochrana dat v ČR a Euroregionu NISA

Podle průzkumu [TUL03] provedeného v rámci firem euroregionu NISA v roce 2003 na otázku zda má vyřešenou bezpečnost dat odpovědělo 63 % firem kladně, 20 % firem ji připravuje a 17 % nemá bezpečnost dat řešenou vůbec. Průzkum [PIB03A] ukázal, že pouze u 13 % organizací se někdo informační bezpečnosti věnuje na plný úvazek, což je vzhledem k vážnosti problému znepokojivé, většinou je informační bezpečnost v podniku v kompetenci útvaru IT/IS, pouze 3 % respondentů uvedlo existenci vlastního bezpečnostního oddělení. Stejný průzkum uvádí i zajímavou skutečnost, že poměr rozpočtu na zabezpečení k rozpočtu IT je 8 %.

1.6 Bezpečnostní politika

Systém řízení bezpečnosti je nedílnou součástí systému řízení organizace. 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.

Bezpečnostní politika musí být chápána jako souhrn principů a východisek pro strategická řešení. Představuje základ pro zajištění informační bezpečnosti. [RODO0] Bezpečnostní politika tedy představuje výchozí body pro návrh a realizaci všech úspěšných standardů, směrnic, procedur a opatření. Dokument politiky je všeobecným plánem, na jehož základě se informace získávají a využívají, určuje také oblasti, ve kterých je třeba tento proces třídit a kontrolovat.

Účelem bezpečnostní politiky je prosadit bezpečný informační systém. V bezpečnostní politice by měly být definovány struktury správy programového systému, zodpovědnosti jednotlivců i skupin, resp. týmů v organizaci a celkové bezpečnostní cíle. Důležitou roli hraje i zdůraznění úlohy jednotlivce a osobní zodpovědnosti každého zaměstnance organizace zavádějící bezpečný informační systém.

Bezpečnostní politika má obvykle charakter povinných zásad, měnitelných pouze několika správci. Musíme na ni pohlížet jako na normy, pravidla a praktiky, definující způsob zpracování, ochrany a distribuce citlivé informace v rámci činnosti informačního systému. [LÁT96]

1.6.1 Program informační bezpečnosti

Bezpečnostní politika by měla pokrýt všechny zdroje informačního systému v organizaci, tj. technické a programové vybavení, informace, personál apod. Výsledkem řešení by měl být program informační bezpečnosti, což dle [LÁT96] chá-

peme jako dokument koncepčního charakteru, který určuje metody a podmínky reálného řešení informační bezpečnosti a který je schválen vrcholovým vedením organizace.

Program by měl obecně zahrnovat:

- cíle organizace v oblasti informační bezpečnosti
- odpovědnost za jejich naplňování
- prostředky k jejich naplňování
- časové období nutné pro jejich naplňování
- hlavní zásady jejich naplňování
- zásady koordinace a informační, majetkové a osobní bezpečnosti organizace

1.6.2 Hierarchická struktura bezpečnostní politiky

Je výhodné vytvářet bezpečnostní politiky jako více provázaných hierarchických dokumentů, které na své úrovni řeší vždy příslušné oblasti bezpečnosti. Zpracovávány tak dle [MARO2] jsou:

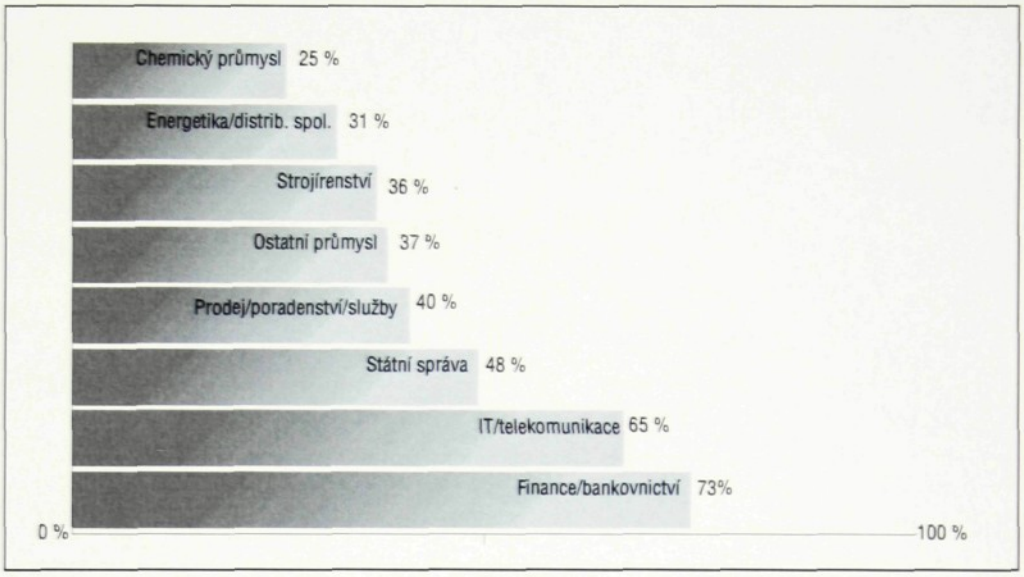
- bezpečnostní politika organizace zahrnující nejširší a nejvyšší politiky organizace, směřující k ochraně jejich pracovníků a aktiv
- bezpečnostní politika informací je v organizaci požadována jako podřízená pro oblast informatiky
- bezpečnostní politika IT je rozpracování bezpečnostní politiky informací a zahrnuje případné vytvoření specializovaných bezpečnostních politik jednotlivých informačních systémů organizace

Ačkoli prakticky všechny organizace přisuzují informační bezpečnosti význam nebo velký význam, neodpovídá toto mínění výskytu a kvalitě bezpečnostních politik. Neexistence tohoto dokumentu, nebo jeho nedostatečný rozsah má většinou za následek nedůslednou a nekonzistentní implementaci bezpečnosti v organizaci, a tím typicky vyšší výskyt a dopad bezpečnostních incidentů.

1.6.3 Bezpečnostní politika v ČR v praxi

Dle průzkumu stavu informační bezpečnosti [PIB03A] mělo bezpečnostní politiku definovanou v roce 1999 35 % organizací, v roce 2001 pak 43 % a v roce 2003 už 46 %, je zde tedy vidět rostoucí tendence k existenci bezpečnostní politiky.

Z hlediska oborů působnosti – viz obrázek 1.7 má pouze v oblastech finance/bankovnictví a IT/telekomunikace bezpečnostní politiku výrazně více než 50 % společností [PIB01]. Oproti roku 1999 došlo k výraznějšímu nárůstu organizací ve státním sektoru, které mají tento dokument připravený. Je nepochybné, že



Obr. 1.7 Graf rozšíření bezpečnostní politiky z hlediska oborů působnosti. Zdroj [pib01]

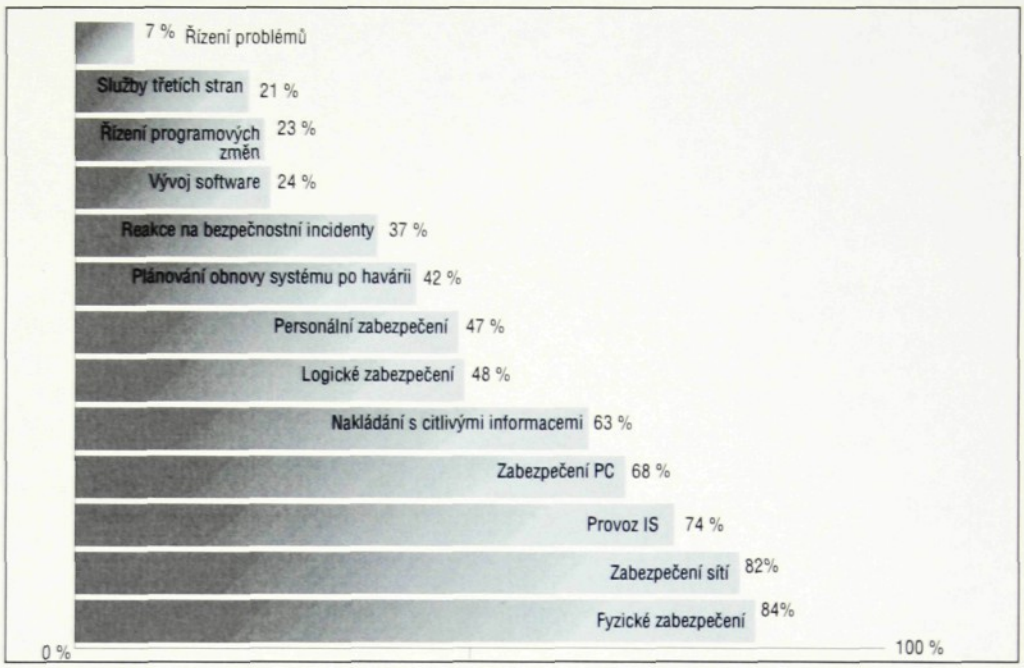
v tomto směru sehrál velmi pozitivní úlohu zákon o utajovaných skutečnostech [ZAK148], který existenci bezpečnostní politiky požaduje.

S velikostí organizace roste i pravděpodobnost existence bezpečnostní politiky. Zatímco pouze 40 % organizací s počtem zaměstnanců do 500 má politiku, u organizací nad 1000 zaměstnanců je to již 49 % [PIB01].

Většina bezpečnostních politik pokrývá fyzické zabezpečení, zabezpečení sítí a provoz informačních systémů. Překvapivý zůstává fakt, že vývoj a změny informačních systémů, tedy vedle provozu klíčové aktivity v oblasti IT, jsou součástí pouze zhruba každé čtvrté bezpečnostní politiky – viz obr. 1.8.

Bezpečnostní politika sama o sobě zvýšení bezpečnosti nepřinese. Bezpečnostní cíle musí být zpracovány do odpovídajících interních standardů a procedur, jejichž naplnění teprve přispívá k dosažení deklarované úrovně bezpečnosti. Z organizací, které mají přijatou bezpečnostní politiku přibližně třetina nemá, resp. většinou nemá, jednotlivé oblasti bezpečnostní politiky rozpracované do standardů [PIB01].

Necelých 70 % organizací seznamuje své zaměstnance s těmi částmi bezpečnostní politiky, které potřebují k výkonu svých funkcí [PIB01]. Polovina respondentů provádí kontrolu dodržování bezpečnostní politiky a standardů. Pouhých 37 % organizací svou politiku pravidelně aktualizuje [PIB01].



Obr. 1.8 Graf pokrytí oblastí IS bezpečnostní politikou. Zdroj [pib01]

Kapitola 2
Bezpečnost a Internet

1.1 Internet jako součást IS podniku

Internet, celosvětová počítačová síť spojující desítky milionů serverů a stovky milionů osobních počítačů (či jiných zařízení), přinesl do odvětví bezpečnosti informačních systémů jeden zcela nový, ale zásadní prvek. Otevřenost Internetové sítě umožňuje to, co v normálních počítačových sítích či systémech není možné. A právě otevřenost a neexistující hranice jsou dle [DOČ03] největším nebezpečím, které Internet přináší. Podle průzkumu [PIB03A] se od roku 1999 procento zaměstnanců s přístupem k Internetu zvýšilo ze 17 % na 47 %, což představuje značné rozšíření možných hrozeb pro celkovou bezpečnost IS podniku.

Bezpečnost sítí včetně sítě Internet jako součásti IS téměř každé současné organizace, lze obecně zajistit všemi prostředky, které bezpečnost IS zajišťují a jimž jsem se podrobněji věnoval v předchozí kapitole, v této části práce se zaměřím na specifické problémy zabezpečení v síti Internet.

V mnoha organizacích se původně lokální počítačové sítě (LAN) budovaly proto, aby počítače mohly sdílet periferní zařízení jako jsou tiskárny nebo záznamová media. Postupně se připojily další funkce LAN, jako sdílení dat a spouštění aplikací ze serveru. Dnešní distribuované aplikace však jdou mnohem dále. Automatická distribuce informací, multimedia, práce s grafickým zobrazením, přístup k síti Internet nebo konference začínají být v mnoha organizacích zcela běžné. Během jisté doby bude firma nebo organizace bez LAN a připojení k síti Internet

raritou. Díky rozvoji bezdrátových technologií pro připojení vzrůstá i mobilita uživatelů sítí.

Internet se stává „válečnou zónou", ve které může zaútočit kdokoliv na kohokoliv. Pojmy jako elektronická válka nebo informační válka tak nabývají nového významu. Ve válce bojují dvě strany, na Internetu není počet soupeřů omezen. S Internetem pracují začátečníci i pokročilí. Zdálo by se, že nejmenší rizika hrozí od začátečníků, ale opak je pravdou. Neznalého uživatele lze snadno zneužít anebo zmanipulovat, ten pak nevědomky slouží jako prostředník útoku a může se dostat do pozice spolupachatele (viz například DDoS útoky o kterých pojednávám dále).

1.2 Soustava protokolů TCP/IP

Řekne-li se dnes TCP/IP, je to obvykle chápáno jen jako označení dvou přenosových protokolů, používaných v počítačových sítích, konkrétně protokolů TCP (Transmission Control Protocol) resp. IP (Internet Protocol). Ve skutečnosti ale zkratka TCP/IP označuje celou soustavu protokolů, ne nutně vázanou na operační systém, přičemž TCP a IP jsou sice nejznámější protokoly této soustavy, ale zdaleka ne protokoly jediné. Správnější je ale podle [PET92] považovat TCP/IP za ucelenou soustavu názorů o tom, jak by se počítačové sítě měly budovat, a jak by měly fungovat. Zahrnuje totiž i vlastní představu o tom, jak by mělo být síťové programové vybavení členěno na jednotlivé vrstvy, jaké úkoly by tyto vrstvy měly plnit, a také jakým způsobem by je měly plnit – tedy jaké konkrétní protokoly by na jednotlivých úrovních měly být používány.

Pro svůj úzký vztah k síti Internet je soustava protokolů TCP/IP někdy označována také jako Internet Protocol Suite (doslova: soustava protokolů Internetu)

Zatímco referenční model ISO/OSI vymezuje sedm vrstev síťového programového vybavení, TCP/IP počítá jen se vrstvami čtyřmi.

1.2.1 Spojová vrstva

Nejnižší vrstva – vrstva síťového rozhraní (též spojová nebo linková vrstva) má na starosti vše, co je spojeno s ovládáním konkrétní přenosové cesty resp. sítě, a s přímým vysíláním a příjmem datových paketů. V rámci soustavy TCP/IP není tato vrstva blíže specifikována, neboť je závislá na použité přenosové technologii.

Vrstvu síťového rozhraní může tvořit relativně jednoduchý ovladač, je-li daný uzel přímo připojen například k lokální síti či ke dvoubodovému spoji, nebo může tato vrstva představovat naopak velmi složitý subsystém, s vlastním lin-

kovým přenosovým protokolem. Vzhledem k velmi častému připojování jednotlivých uzlů na lokální sítě typu Ethernet je vrstva síťového rozhraní v rámci TCP/IP často označována také jako Ethernetová vrstva (Ethernet Layer).

1.2.2 Síťová vrstva

Bezprostředně vyšší vrstva, která již není závislá na konkrétní přenosové technologii, je vrstva síťová, v terminologii TCP/IP označovaná jako Internet Layer, nebo též IP vrstva (IP Layer), a to podle toho, že je realizována pomocí protokolu IP. Úkol této vrstvy je v prvním přiblížení stejný, jako úkol síťové vrstvy v referenčním modelu ISO/OSI – stará se o to, aby se jednotlivé pakety dostaly od odesilatele až ke svému skutečnému příjemci, přes případné směrovače resp. brány.

Protokoly zahrnuté v této vrstvě jsou např. protokoly MTU, IP, ICMP či ARP.

1.2.3 Transportní vrstva

Třetí vrstva TCP/IP je označována jako transportní vrstva (Transport Layer), nebo též jako TCP vrstva (TCP Layer), neboť je nejčastěji realizována právě protokolem TCP. Hlavním úkolem této vrstvy je zajistit přenos mezi dvěma koncovými účastníky, kterými jsou v případě TCP/IP přímo aplikační programy. Podle jejich nároků a požadavků může transportní vrstva regulovat tok dat oběma směry a zajišťovat spolehlivost přenosu.

Přestože je transportní vrstva TCP/IP nejčastěji zajišťována právě protokolem TCP, není to zdaleka jediná možnost. Dalším používaným protokolem na úrovni transportní vrstvy je například protokol UDP, který na rozdíl od TCP nezajišťuje mj. spolehlivost přenosu. Protokolu UDP využívají např. služby SNMP, TFTP, BOOTP, NFS či DHCP, využívají ho také některé multimediální aplikace.

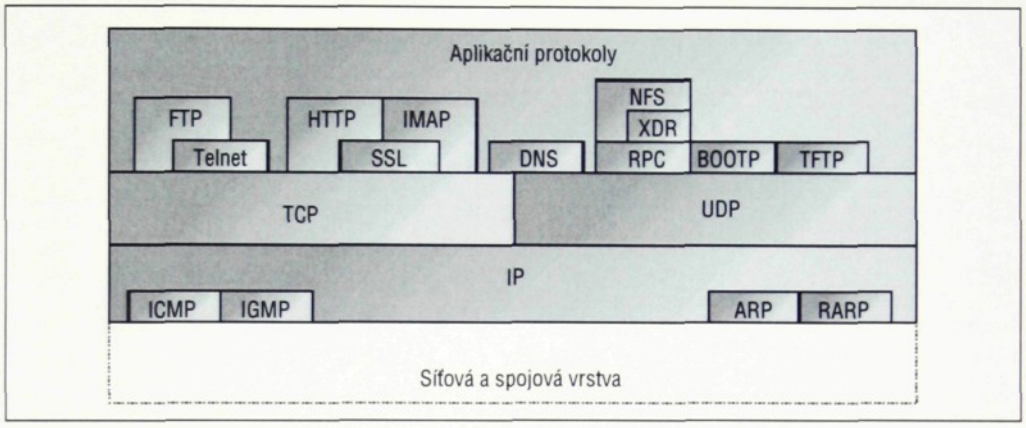
Rozdíl mezi protokoly TCP a UDP je v zásadě, jak jsem již uvedl, v tom, že TCP je tzv. spojovanou službou, tj. příjemce potvrzuje přijímaná data. V případě ztráty dat (TCP segmentu) si příjemce vyžádá zopakování přenosu. Protokol UDP přenáší data pomocí datagramů (obdoba telegramů), tj. odesílatel odešle datagram a nestará se o to, zdali byl doručen.

1.2.4 Aplikační vrstva

Nejvyšší vrstvou TCP/IP je pak vrstva aplikační (Application Layer). Jejími entitami jsou jednotlivé aplikační programy, které na rozdíl od referenčního modelu ISO/OSI komunikují přímo s transportní vrstvou. Případné prezentační a relační služby, které v modelu ISO/OSI zajišťují samostatné vrstvy, si zde musí jednotlivé aplikace v případě potřeby realizovat samy.

Aplikační vrstva zahrnuje protokoly jako HTTP, Telnet, FTP a SMTP.

Některé protokoly z rodiny protokolů TCP/IP, jejich strukturu a vzájemné vztahy znázorňuje obrázek 2.1.

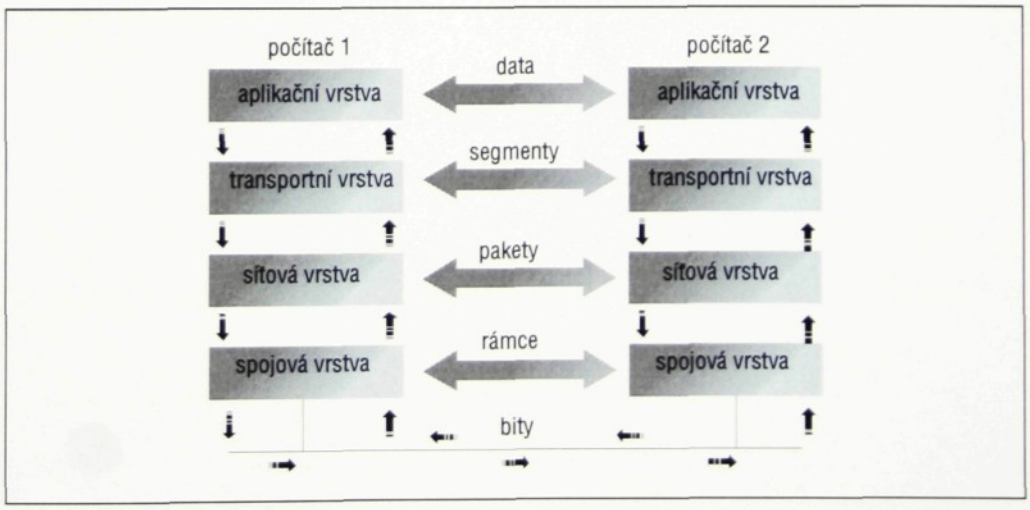


Obr. 2.1 Některé protokoly v modelu TCP/IP. Zdroj [dos00]

1.3 Komunikace v modelu TCP/IP

1.3.1 Princip komunikace vrstev

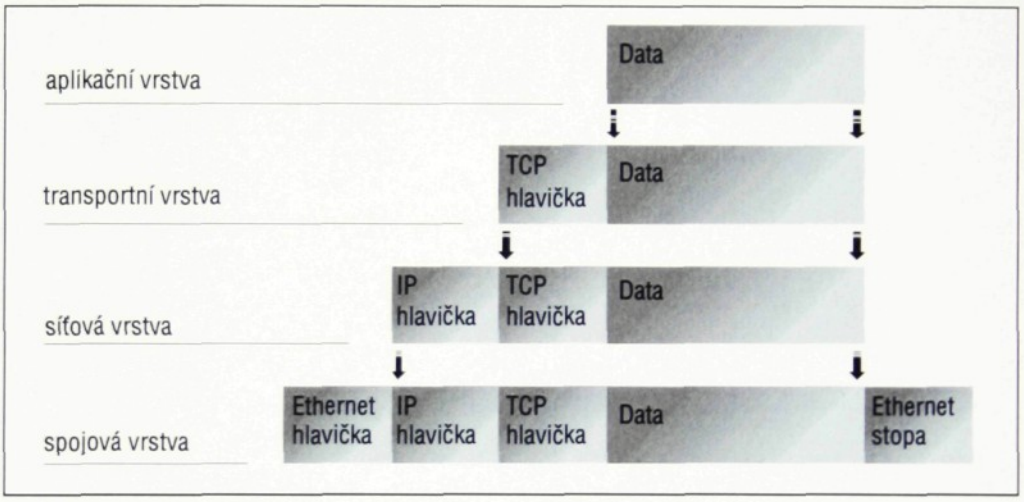
Vrstvové protokoly jsou navrženy tak, že každá vrstva příjemce přijme stejné objekty, které odešle odpovídající vrstva na zdrojové straně. Každá vrstva komunikuje se svým protějškem na druhé straně a nezajímá se o parametry či formáty používané vrstvami nad či pod danou vrstvou. Fyzicky vrstva předává data přes rozhraní vrstvy nad či pod touto vrstvou v rámci stejného systému. Komunikaci mezi vrstvami znázorňuje obrázek 2.2.



Obr. 2.2 Komunikace mezi vrstvami v modelu TCP/IP. Zdroj [dun01]

1.3.2 Zapouzdřování vrstev protokolu

Jak jsou data předávána z aplikační do transportní, síťové a spojové vrstvy, každý z protokolů data zpracuje a přidá k nim hlavičku, čímž danou vrstvu zapouzdří. V systému který tok dat přijímá, jsou hlavičky odstraněny tím, jak jednotlivé vrstvy postupně zpracovávají došlá data. Tento přístup zajišťuje určitou pružnost protože v zásadě vrchní vrstvy nemusí „zajímat" technologie kterou využívají vrstvy spodní. Např. pokud je vrstva síťová šifrována, TCP a aplikace zůstávají nezměněny. Princip zapouzdřování názorně vysvětluje obrázek 2.3.



Obr. 2.3. Zapouzdřování vrstev protokolu TCP/IP. Zdroj: [dun01]

1.4 Bezpečnost protokolů TCP/IP

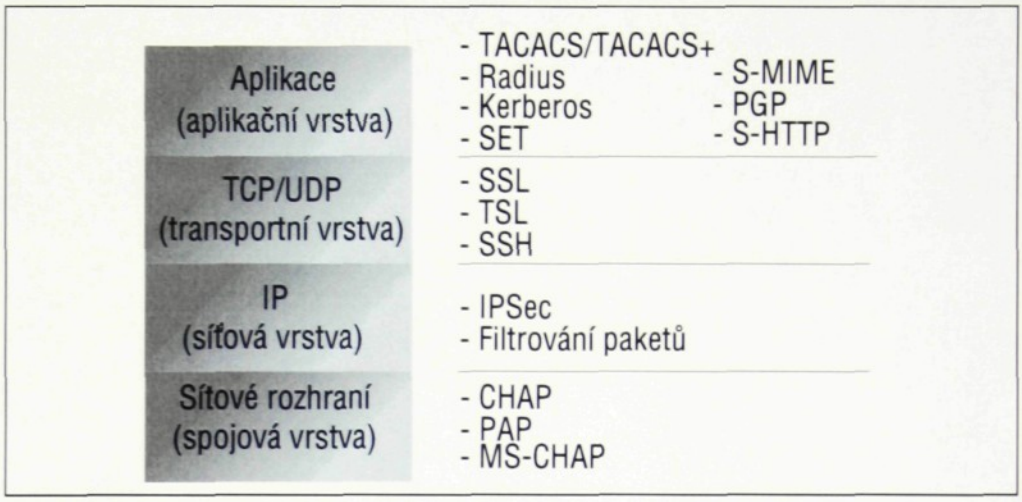
Protokol TCP/IP neřeší problematiku zabezpečení přenášených dat. Klasický model protokolu TCP/IP v sobě nezahrnuje žádnou vrstvu, která by se touto problematikou zabývala, proto se jednotlivé protokoly zajišťující bezpečnost nachází napříč všemi vrstvami modelu. Některé protokoly modelu TCP/IP zajišťující bezpečnost a jejich umístění ve vrstvové architektuře znázorňuje obrázek 2.4.

Mnoho z těchto protokolů využívá šifrování jako základní zdroj zabezpečení, šifrování, jakož i vysvětlení důležitých pojmů z této oblasti se podrobněji věnuji v kapitole 4.

1.4.1 Bezpečnost aplikační vrstvy

S-MIME

V Internetu byla publikována celá řada protokolů specifikujících bezpečnou poštu. Zejména se jednalo o protokoly PEM a MOSS, které se však v praxi neujaly.



Obr. 2.4 Bezpečnostní protokoly ve vrstvách modelu TCP/IP. Zdroj: [tcp98]

Prosadil se protokol PGP, avšak dle Dostálka [DOS01] se jeví právě S-MIME jasným favoritem protokolů pro bezpečnou poštu.

S-MIME lze podle [TCP98] považovat za specifický protokol typu SSL. Je to bezpečnostní opatření operující na aplikační úrovni, jeho použití je však omezeno na ochranu elektronické pošty prostřednictvím šifrování a elektronických podpisů Je založen na technologii veřejného klíče a používá certifikáty X.509 k zajištění identifikace komunikujících. S-MIME může být implementováno do koncových komunikačních systémů – např. různých e-mailových klientů.

PGP

PGP je kombinovaný šifrovací systém, který na rozdíl od architektury PKI nespoléhá na certifikační autority.

Navenek se jeví jako program s veřejným šifrovacím klíčem, plně využívající asymetrického šifrování, to se však ve skutečnosti používá pouze pro zakódování klíče symetrické šifry, kterou je pak zašifrována samotná zpráva. Digitálním podpisem je kontrolní součet zprávy (hash), který je zašifrován asymetrickou šifrou.

S-HTTP

Protokol S-HTTP (Secure HTTP) není podle [DUN01] příliš používán, ale byl přímo navržen tak, aby zajistil bezpečnost pro aplikace založené na web architektuře. S-HTTP je komunikační protokol založený na zprávách a dokáže bezpečně přenést jednotlivé zprávy. Zajišťuje důvěrnost, autenticitu a integritu posílané zprávy. Rozšiřuje HTTP o tagy pro šifrované a zabezpečené transakce, bývá implementováno do různých komerčních web serverů a většiny prohlížečů. S-HTTP server vyjednává s klientem o typu šifrování, které bude použito, transakce pak můžou být tedy šifrovány různými způsoby, záleží na daném serveru a klientu. S-HTTP

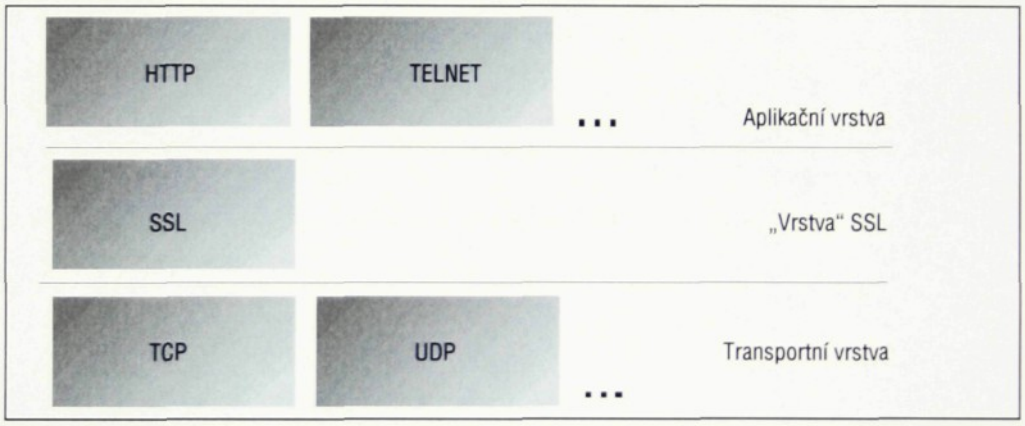
nevyžaduje od klientů, aby měly certifikáty veřejného klíče protože pro šifrování používá symetrické klíče.

1.4.2 Bezpečnost transportní vrstvy

SSL, TLS

Tento protokol vyvinula firma Netscape pro přenos základních dokumentů přes Internet. Konkurenční firma Microsoft vytvořila obdobný protokol PCT, oba protokoly jsou si vzájemně natolik podobné, že mnohému software nečiní žádných potíží podporovat oba dva protokoly současně. Tento protokol (SSL) byl obecně přijat pro zabezpečení a autentizaci komunikace mezi klienty a servery na Internetu.

Vrstva SSL (Secure Sockets Layer) řešící zabezpečení přenášených dat je vložena mezi aplikační protokol a protokol TCP – viz obrázek 2.5. Její přednost je tedy v tom, že je nezávislá na aplikačním protokolu, protokoly vyšší úrovně mohou být nad SSL protokolem vrstveny transparentně, tj. bez jejich úpravy.



Obr. 2.5 Protokol SSL jako „mezivrstva" aplikační a transportní vrstvou. Zdroj: [odv02]

Součástí úvodního dialogu (handshake) je výměna dat, ze které se odvodí tzv. sdílené tajemství. Sdílené tajemství je blok čísel, který znají pouze účastníci komunikace a všem ostatním je utajen. Od sdíleného tajemství se odvozují symetrické šifrovací klíče a tzv. tajemství pro výpočet kontrolního součtu.

SSL může šifrovat přenos dat mezi oběma účastníky komunikace. Pro šifrování se používá symetrická šifra jejíž šifrovací klíč je odvozen od sdíleného tajemství. Bohužel vzhledem k exportním omezením USA je délka šifrovacího klíče omezena, čímž je v našich podmínkách omezeno i využití SSL jako takového.

Jednotlivé přenášené fragmenty dat se doplňují o kontrolní součet zabezpečující integritu přenášených dat. Jelikož se kontrolní součet nepočítá pouze z fragmentu přenášených dat, ale fragment se pro výpočet kontrolního součtu zřetězí s ta-

jemstvím pro výpočet kontrolního součtu, je velice obtížné poopravit přenášená data během přenosu, je tedy poměrně solidně zabezpečena integrita přenášených dat.

SSL protokol poskytuje bezpečné spojení, které má tři základní vlastnosti:

- **Důvěrnost spojení**. Šifrování je použito po počátečním handshaku k definování tajných klíčů. Symetrické kódování je použito pro šifrování.
- **Autentizaci**. Identita komunikujících uzlů je autentizována s využitím asymetrického šifrování nebo veřejného klíče.
- **Integritu**. Spojení je spolehlivé, přenos zprávy obsahuje kontrolu integrity zprávy s využitím klíčů MAC.

Protokol TLS je pak vylepšením protokolu SSL, se kterým je zpětně kompatibilní. Tento protokol byl navržen a přijat jako standard pro zabezpečení komunikace na Internetu

SSH

SSH (Secure Shell) je program k přihlašování se na počítače prostřednictvím nezabezpečené sítě, ke spouštění příkazů na vzdálených počítačích a k přesouvání souborů z jednoho počítače na druhý. Poskytuje silnou autentizaci a bezpečnou komunikaci na nezabezpečeném kanále. Je určen jako náhrada programů telnet, rlogin, rsh, rcp, rsync, rdist a nově také ftp (SSH2).

Veškerá komunikace je automaticky šifrována. Klient ověřuje věrohodnost serveru na začátku každého spojení a stejně tak server ověřuje věrohodnost klienta. K ověřování jsou použity RSA nebo DSA klíče. Ověřovací agent běžící na uživatelském počítači může být použit k uschování RSA klíčů uživatele. V rámci SSH spojení lze použít i kompresi pro zmenšení přenášených dat.

Filtrování

Na transportní vrstvě lze provádět filtrování segmentů. Problematice filtrování se podrobně věnuji v kapitole 4.

1.4.3 Bezpečnost síťové vrstvy

IPSec

Pojem IPsec (IP Security Protocol) definuje přidání bezpečnostního mechanismu do standardní IP (síťové) vrstvy. IPSec protokol zajišťuje kontrolu přístupu, autentizaci, integritu dat i důvěrnost pro každý IP paket mezi dvěma komunikujícími body na síti.

Toto rozšíření je definováno na síťové vrstvě, je tedy nezávislé na protokolech vyšších vrstev (TCP,UDP). Aplikace tedy nemusí podporovat žádné speciální komunikační metody, aby mohla komunikovat přes IPsec. Pro aplikace je to naprosto transparentní rozšíření IP protokolu. IPsec se může používat buď na koncové stanici (terminal host) nebo na routeru (security gateway).

IPsec se dá používat ve dvou módech:

- **Transportní mód.** V tomto módu jsou chráněna data vyšších protokolů. IP hlavička zůstává nechráněná. Tento mód je použitelný jen na terminal hostu.
- **Tunnel mód.** Je přidána nová IP hlavička a takto pozměněný paket je přenesen na druhý konec „tunelu", kde je „vybalen". Tento přenosový mód musí podporovat Security Gateway, pro koncovou stanici je volitelný.

Protololu IPSec se využívá především při budování virtuálních privátních sítí (VPN). Problematice virtuálních privátních sítí se věnuji v kapitole 4.

Filtrování

Filtrování paketů síťové vrstvy je jedním z nejběžnějších způsobů zabezpečení sítí. Filtrování podrobněji rozebírám v kapitole 4, kde se věnuji problematice firewallů, kde je filtrování paketů jedním ze základních principů zabezpečení.

Bezpečnost spojové vrstvy

Bezpečnost spojové vrstvy je zajišťována jako spojení dvou bodů. Prostřednictvím speciálních hardwarových zařízení, která jsou fyzicky připojena na oba konce kabelu je prováděno šifrování a dešifrování. Tento způsob ochrany využívají především armádní či vládní instituce nebo banky. Takový způsob ochrany není vhodný pro rozlehlé sítě, protože pakety nelze v zašifrované podobě vystopovat.

Kapitola 3
Hrozby a útoky

1.1 Definice a kategorizace

1.1.1 Hrozba

Pojmem hrozba označujeme možnost využít zranitelné místo IS k útoku na něj – tedy ke způsobení škody na aktivech. Veškeré hrozby lze podle [HANOO] kategorizovat na:

objektivní

- **přírodní, fyzické** – požár, povodeň, výpadek napětí, poruchy..., u kterých je prevence obtížná a u kterých je třeba řešit spíše minimalizaci dopadů vhodným plánem obnovy, v tomto případě je třeba vypracovat havarijní plán
- **fyzikální** – např. elektromagnetické vyzařování
- **technické nebo logické** – porucha paměti, softwarová „zadní vrátka", špatné propojení jinak bezpečných komponent, krádež, resp. zničení paměťového média nebo nedokonalé zrušení informace na něm

subjektivní, tj. hrozby plynoucí z lidského faktoru

- **neúmyslné** – např. působení neškoleného uživatele/správce
- **úmyslné** – představované potenciální existencí vnějších útočníků (špioni, teroristi, kriminální živly, hackeři) i vnitřních útočníků (od-

haduje se, že 80 % útoků na IT je vedeno zevnitř útočníkem, kterým může být propuštěný, rozzlobený, vydíraný či chamtivý zaměstnanec), velmi efektivní z hlediska vedení útoku je součinnost obou typů útočníků.

1.1.2 Útok

Útokem, neboli bezpečnostním incidentem, rozumíme dle [HANOO] buďto úmyslné využití zranitelného místa ke způsobení škod/ztrát na aktivech IS nebo neúmyslné uskutečnění akce, jejímž výsledkem je škoda na aktivech. Útočit lze:

- **přerušením** – aktivní útok na dostupnost, např. ztráta, znepřístupnění, poškození aktiva, vymazání programu, vymazání dat apod…
- **odposlechem** – pasívní útok na důvěrnost, kdy neautorizovaný subjekt si neoprávněně zpřístupní aktiva jde např. o okopírování programu či dat
- **změnou** – aktivní útok na integritu, neautorizovaný subjekt zasáhne do aktiva, provede se např. změna uložených dat, přidání funkce do programu
- **přidáním hodnoty** – aktivní útok na integritu nebo autenticitu, tj. připad kdy neautorizovaná strana něco vytvoří – podvržení transakce, dodání falešných dat…

V této části mé diplomové práce se budu věnovat pouze útokům vedeným na IS firem především prostřednictvím sítě Internet. To proto, že se jedná o jednu z největších hrozeb pro firmy operující v oblasti elektronického obchodování – e-commerce. Cílem těchto útoků je vyřadit z provozu některou součást IS a znemožnit tak jeho správnou funkčnost, zamezit přístupu k určité službě či části IS nebo získat neoprávněný přístup k citlivým datům firmy (dle předchozí kategorizace tedy hrozbám subjektivním – úmyslným a následným útokům přerušením, změnou a přidáním hodnoty). Touto cestou může být negativním způsobem ovlivněn chod firmy a následně její úspěšnost na trhu, a to proto, že řada firem je dnes závislá na správném fungování svého informačního systému a na jeho vysoké dostupnosti, o firmách ve sféře e-commerce to platí téměř beze zbytku. Takový informační systém většinou zahrnuje servery provozující kritické aplikace databázového charakteru, prezentační Internetové a intranetové web servery a jeho součástí je i privátní síť LAN či WAN a připojení do Internetu.

1.2 Krádež informace

Krádež informace nemusí být podle [CHA98] aktivní nebo nějak zvlášť technicky založená. Lidé, kteří potřebují najít určité osobní informace mohou prostě dané osobě zavolat a zeptat se jí (a například předstírat že jsou někdo, kdo má právo to vědět) nebo mohou například odposlouchávat telefon. Podobné je to při zís-

kávání elektronických informací – útočníci se na ně mohou účinně zeptat (tím, že předstírají, že jsou počítač nebo uživatel s platným přístupem) nebo se mohou pasivně „napíchnout" do sítě a čekat až informace přijdou.

Únik informací představuje útok na důvěrnost a dle výše uvedené kategorizace dle [HAN00] o útok odposlechem. Únik informací nastane tehdy, když je útočník schopen získat informace, které by mu jejich vlastník jinak neposkytl. Únik informací neznamená automaticky dostatek informací, které by umožnily okamžitý přístup k systému, ale spíše informace, které by mohly dát inteligentnímu útočníkovi podnět k dalšímu postupu nebo informace, které by mohl použít v kombinaci s dalšími k případnému průniku do systému. V každém operačním systému existuje možnost úniku informací, to je nevyhnutelné. Operační systémy jsou natolik rozdílné, že útočníkovi stačí jen nepatrný podnět k tomu, aby určil jaký OS cíl útoku používá. Útočník pak sbírá co možná největší množství informací o svém cíli tak, aby mohl naplánovat útok. Pokud se nebude potenciálně napadený dostatečně bránit, můžou i zlomky informací sesbírané útočníkem dát v závěru dostatek podnětů ke zdárnému odhalení.

Klasickým příkladem úniku informací je podle [RUS01] služba finger. Dříve většina počítačů pod OS UNIX používala službu finger, která poskytovala různé informace o daném uživateli na daném počítači. Výstup této služby odkrývá mnoho důležitých informací jako např. uživatelské jméno, domovský adresář, použitý shell, aktivitu uživatele a další. Opět nutno podotknout, že tento druh informací nemusí zákonitě vést k útoku, skličující je ale zjištění jak často se uživatelské heslo shoduje s uživatelským jménem – a finger je rychlá cesta k nalezení řady uživatelských jmen.

1.3 Vniknutí

Tento typ útoku je podle [CHA98] nejčastějším případem útoků na počítačové systémy. Dojde-li ke vniknutí, mohou uživatelé dále používat své počítače, nejvíce útočníků chce využívat napadené počítače, jako kdyby to byli legitimní uživatelé. Rozsah možností získání přístupu je značné – od sociálně-technických (předstírání identity např. vysoce nadřízeného pracovníka a následné získání hesla od správce sítě), přes luštění hesla až po různé intriky, jak získat vstup bez znalosti hesla.

1.3.1 Útok na přístupové heslo

Útok na přístupové heslo je jedním ze způsobů, jak se útočník může dostat do jinak zabezpečené sítě a odtud pak provést další možné útoky. Na Internetu jsou běžně dostupné programy, které dokáží zjistit heslo pomocí různých metod. Základními metodami jsou podle [ZEM03]:

- **luštění hesla hrubou silou** (Brute Force Password Cracking) – principem je zkoušení všech možných variant do doby, než program objeví správné heslo.
- **slovníkově orientované útoky** (Directory Based Attacks) – spočívají v tom, že program zkouší všechny slova, která má uložena v předem připraveném souboru.
- **analýza prostého textu** (Plain Text Attack) – při použití této metody je nutné mít kromě zaheslovaného souboru ještě jeden bez hesla. Program porovnáním obou souborů zjišťuje rozdíly a algoritmus pro tvorbu hesla.

Správným nastavením parametrů hesel a dodržováním pravidel tvorby a správy hesel, tak jak jsem je uvedl v první kapitole, lze značně omezit úspěšnost této formy útoku.

Pokud se útočníkovi podaří zjistit superuživatelské heslo systému, mohou provádět na daném systému cokoliv co chtějí a prakticky jsou tak vypnuty veškeré další obranné mechanismy napadeného systému. Takovéto útoky Russel [RUSOO] nazývá „Elevation of Privileges Attack" – tedy útoky na zvýšení oprávnění. Jedná se o útoky proti integritě bezpečnostní struktury, které vedou většinou k dalším odhalením.

1.3.2 Útok na přístup k souborům

Útok na přístup k souborům je, jak již název napovídá, útokem, který dává útočníkovi přístup k souborům na systému. Je to útok proti důvěrnosti a integritě. Existuje množství podkategorií přístupu k souborům, jako např. přístup ke čtení, zápisu nebo povolení k vymazání. Přístup ke čtení přímo ovlivní pouze důvěrnost, ale ostatní modifikace práv se dotýkají integrity. Ovšem pokud je útočník schopen číst libovolné soubory na cílovém systému, další odhalení je téměř jistotou. Útočník může být schopen přístupu k souborům mnoha způsoby, především však v důsledků špatné konfigurace systému nebo bezpečnostních děr.

Specifickým útokem na přístup k souborům je útok na databáze. Jediný rozdíl je v tom, že je veden proti něčemu co není tradičním souborovým systémem.

1.4 Odmítnutí služby – Denial of Service

Útok typu „odmítnutí služby" (útok přerušením – útok na dostupnost služby) je útokem, který je namířený proti serveru (resp. celé síti) připojenému k Internetu. Jeho cílem je ochromení provozu tohoto serveru na základě zvýšení počtu přicházejících požadavků na obsloužení [MUKOO]. Dočkal [DOČOOB] definuje DoS útok jako útok, jehož cílem je zabránit oprávněným uživatelům v přístupu ke službám výpočetního systému, anebo alespoň tento přístup zpozdit. Příkladem

takového útoku je útok, při kterém hacker spustí program generující nějaká nesmyslná data, která jsou posílána na server. Server (nebo i celá síť providera) je pak zahlcen těmito přicházejícími daty a již není schopen reagovat na požadavky řádných uživatelů. V horším případě může dojít až k úplnému zhavarování a zhroucení. Někdy se stává, že primárním cílem není zhavarování serveru, ale že DoS útok je použit hackerem pouze jako doplňková akce sloužící například pro zametení stop, restartování vzdáleného počítače apod. Tyto útoky, které nevedou ke krádeži dat nebo hesel, ale které znemožňují funkčnost výpočetních systémů se v poslední době jeví jako nejefektivnější a pro firmy z oblasti e-commerce fatální. Podle způsobu provedení můžeme DoS útoky obecně rozdělit do tří skupin a sice na:

- útoky, které využívají chyb v implementaci protokolové sady TCP/IP (Ping of Death, Teardrops Attacks)
- útoky, které využívají nedokonalostí a nedostatků ve specifikaci TCP/IP (SYN attack, Land Attack)
- útoky založené na brutálním útoku, vedené hrubou silou (Smurf Attack)

1.4.1 Útoky, které využívají chyb v implementaci protokolové sady TCP/IP

Ping of Death (smrtící ping)

Ping je program, který přijímá od uživatele žádost o echo konkrétního uzlu sítě, na podkladě žádosti vysílá k cílovému uzlu paket žádosti o odezvu (echo_request), přijme paket odpovědi (echo_reply) a zobrazí ji ve vhodném tvaru. Hacker použije příkaz ping pro vytvoření IP paketu, který je větší než maximum povolené ve specifikaci IP protokolu. Tento abnormálně velký paket je pak poslán do cizí sítě. To může způsobit havárii, zamrznutí nebo restart celého systému.Tento útok je poměrně starý a všichni výrobci operačních systémů poskytují opravy – záplaty, které si s tímto typem útoku poradí.

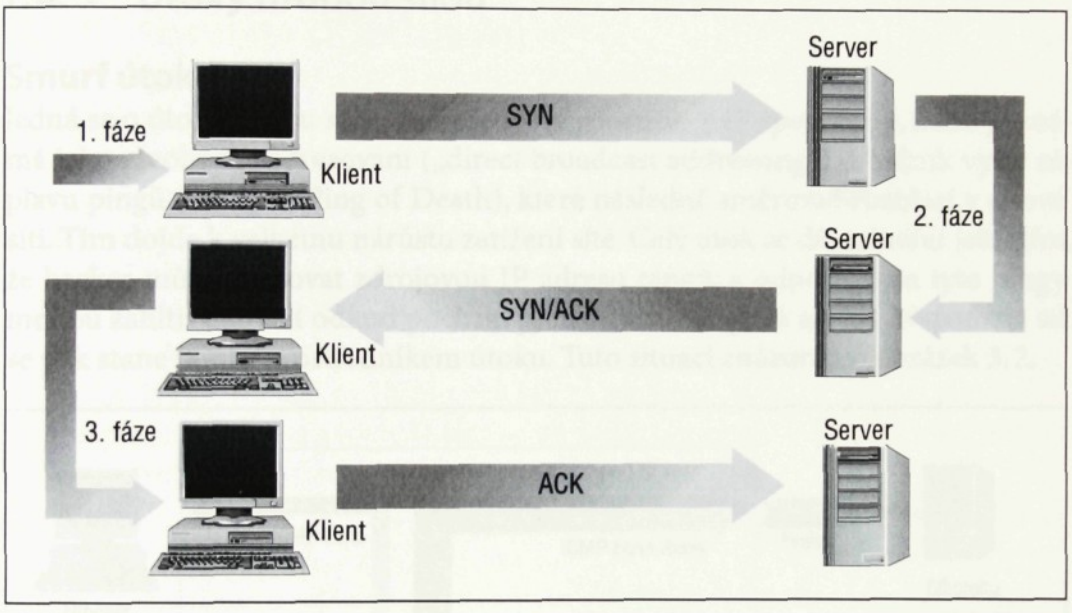
Teardrops útok

Novější typ útoku, který využívá slabosti při opětovném sestavování fragmentů IP paketu. Jedná se zde o to, že během své cesty se může paket dostat do sítě, ve které jeho délka přesahuje maximální povolenou délku – v tom případě je ve vstupním směrovači rozčleněn na menší fragmenty. Údaj o délce fragmentu se umisťuje do záhlaví. Pokud útočníkův počítač generoval fragmenty, jejichž délka neodpovídala údaji v záhlaví, operační systémy si se zpracováním takovýchto fragmentů nevěděly rady.

1.4.2 Útoky, které využívají nedokonalostí a nedostatků ve specifikaci TCP/IP

SYN útok

Tento útok využívá toho jakým způsobem se pomocí protokolu TCP/IP navazuje spojení. Proces navazování spojení se označuje jako tzv. „třífázový handshaking" (Three Way Handshake). Celé to funguje zhruba takto: Aplikace, která inicializuje session (tj. chce posílat data, komunikovat) posílá příjemci synchronizační paket SYN. Příjemce posílá zpátky potvrzovací paket TCP SYN-ACK, na který iniciátor odpovídá potvrzovacím paketem ACK. Po takovémto navázání komunikace jsou aplikace připraveny posílat a přijímat data, proces třífázového „handshakingu". zobrazuje obrázek 3.1.



Obr. 3.1 Třífázový „handshaking". Zdroj [rus01]

Při SYN útoku zaplavuje hacker cílový systém sériemi TCP SYN paketů. Každý paket způsobuje to, že cílový systém pošle odpověď SYN ACK. Zatímco cílový systém čeká na ACK které následují za SYN-ACK, zařadí všechny nevyřízené SYN-ACK odpovědi do fronty. Tato fronta má omezenou délku, obvykle docela malou. Jakmile je fronta plná, systém začne ignorovat všechny příchozí SYN požadavky. Pakety SYN-ACK jsou vyřazeny z fronty pouze když přijde zpět ACK nebo když interní časovač (který je nastaven na relativně dlouhé intervaly) ukončí celý proces navazování komunikace. Celý útok je „vylepšen tím", že v záhlaví příchozích SYN paketů je uvedena špatná nebo neplatná IP adresa. Všechny odpovědi SYN-ACK jsou posílány na tuto adresu, což zaručuje, že odpověď na SYN-ACK nikdy zpátky nepřijde. Tak se tedy vytvoří fronta objednávek, která je vždycky plná, což téměř znemožní se legitimním TCP SYN požadavkům dostat do systému.

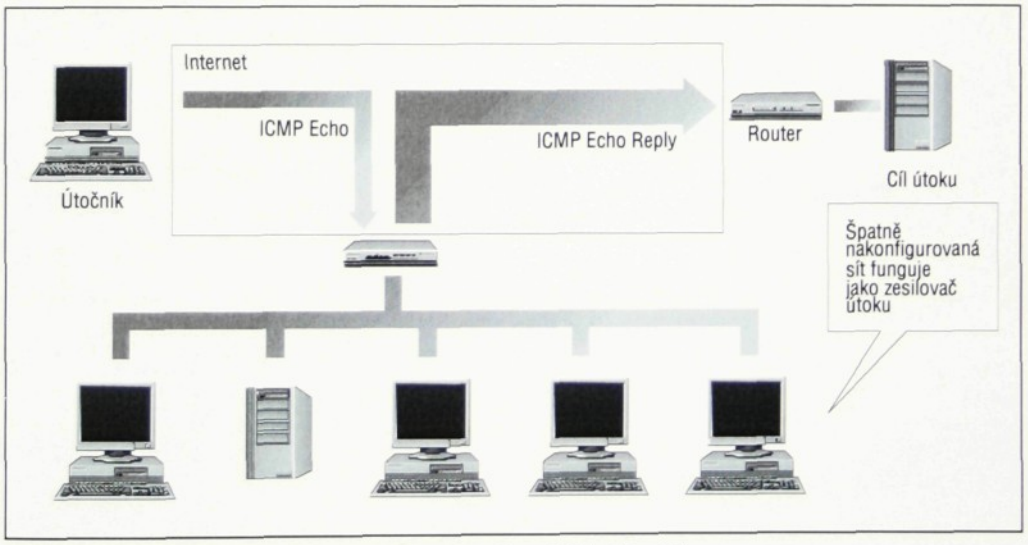
Land útok

Jednoduchý hybrid SYN útoku – hackeři zaplaví SYN pakety do sítě s předstíranou (zfalšovanou) zdrojovou IP adresou cílového systému, například běžně používané privátní IP adresy, a to z toho důvodu, že klasickému SYN útoku se začaly firewally bránit tím, že opakované SYN pakety od stejného uživatele likvidovaly. Ačkoliv tento typ útoku je nový, většina výrobců OS poskytuje opravy řešící tento problém. Jiným způsobem jak ochránit síť před Land útokem je mít firewall, který odfiltrovává všechny příchozí pakety s neplatnými IP adresami. Pakety, které přicházejí do systému se zdrojovými IP adresami které jsou identifikovány jako generované z interního systému, jsou zřejmě špatné. Filtrování paketů výrazně neutralizuje vystavení sítě tomuto typu útoku.

1.4.3 Útoky hrubou silou

Smurf útok

Jedná se o útok hrubou silou zaměřený na vlastnost v IP specifikaci, která je známá jako všeobecné adresování („direct broadcast addressing"). Útočník vyšle záplavu pingů (viz útok Ping of Death), které následně směrovač rozhlásí v cílové síti. Tím dojde k velkému nárůstu zatížení sítě. Celý útok se dá znásobit ještě tím, že hacker může zfalšovat zdrojovou IP adresu pingů, a odpovědi na tyto pingy mohou zahltit další síť odkud pochází předstíraná zdrojová adresa. Napadená síť se pak stane pouze prostředníkem útoku. Tuto situaci znázorňuje obrázek 3.2.



Obr. 3.2 Smurf attack. Zdroj [rus01]

Obrana proti tomuto druhu útoku spočívá v tom, že buď lze vypnout broadcast adresování, tedy za předpokladu, že to router dovoluje nebo lze filtrovat pingy pomocí firewallu a omezit tak echo provoz na malé procento z celkového provozu sítě.

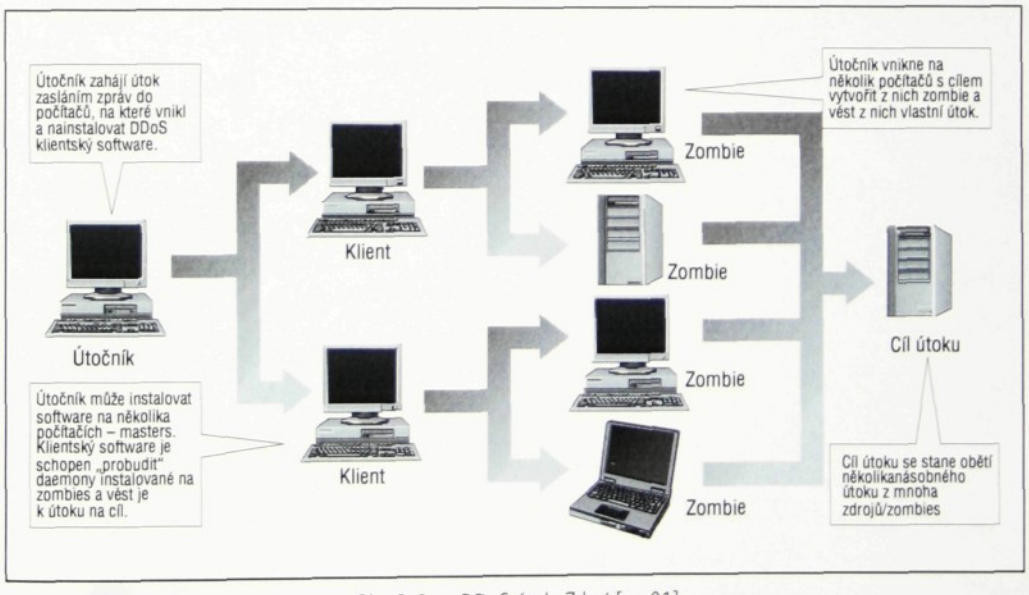
UDP Flood

Při tomto typu útoku hacker pomocí falšování zapne službu, která pro testovací účely generuje sérii znaků pro každý paket, který přijme, spolu s UDP echo službou jiného systému, která také odpovídá na jakýkoliv znak který přijme. Výsledkem je nonstop proud nesmyslných dat mezi dvěma systémy. Bránit se lze jednodušše – buď vypnout na každém počítači v síti UDP služby anebo požadavky na UDP služby filtrovat na firewallu. Nedoporučuje se úplný zákaz veškerého UDP provozu, může se tím totiž odmítnout některé legitimní aplikace jako např. RealAudio, které používá UDP jako svůj transportní mechanismus.

1.5 Distributed Denial of Service attack

1.5.1 Podstata DDoS útoku

Nová vlna útoků typu DoS se objevila v polovině roku 1999. Zneužívá skutečnosti, že v rámci TCP/IP zatím není použit žádný autentizační mechanizmus. Při dosavadních útocích nebylo velkým problémem detekovat útok a lokalizovat útočníka. Objev roku 1999 spočíval ve znásobení „palebné síly" útoku jeho spuštěním z mnoha, navíc cizích zdrojů. DDoS tedy označuje variantu DoS útoku vedeného ne z jednoho počítače, ale souběžně z velkého množství stanic. Slovo velké množství znamená v této souvislosti desítky, stovky a dokonce i tisíce stanic. Co se týká praktické realizace takového útoku, neznamená to, že v danou chvíli sedí u těchto stanic hackeři, nýbrž že na těchto stanicích (zombies) je nainstalován hackerem nějaký program (tzv. daemon), který se na pokyn hackera aktivuje a zasype oběť přívalem dat. Obrázek 3.3 znázorňuje typický DDoS útok.



Obr. 3.3 DDoS útok. Zdroj [rus01]

1.5.2 Průběh a hierarchie útoku

Průběh útoku lze podle [RUS01] znázornit ve dvou rovinách – podle funkce použitého počítače a podle použitého software, obě situace znázorňují obrázky 3.4, resp. 3.5.

Průběh DDoS útoku dle funkce použitého počítače (host):

útočník → master → zombie → cíl útoku

Obr. 3.4 Schéma průběhu DDoS útoku podle funkce použitého počítače. Zdroj [rus01]

master – tři až čtyři počítače, které jsou přímo řízeny útočníkem a které řídí a koordinují činnost zprostředkujících počítačů
zombie – stovky počítačů, které po obdržení příkazu z master počítače chrlí po stanovenou dobu pakety

Průběh DDoS útoku podle použitého software

útočník → klient→ daemon→ cíl útoku

Obr. 3.5 Schéma průběhu DDoS útoku podle použitého software. Zdroj [rus01]

klient – software, který předává zprávy od útočníka k zombies
daemon – software, které útočník spouští z počítačů zombie, program je spuštěn na pozadí a naslouchá příkazům k aktivaci útoku

1.5.3 Nástroje DDoS útoku

DDoS útoky jsou prováděny s použitím speciálních programů jako jsou např. Trinoo, TFN, TFN2K, Stacheldraht, Mstream, Trinity nebo Shaft.

Kapitola 4
Prostředky zabezpečení a obrany

Způsoby ochrany aktiv podniku v sítích, a to včetně Internetu, se v zásadě neliší od obecného modelu zabezpečení, kterému jsem se věnoval v první kapitole této diplomové práce, vykazují ovšem určité specifika. V této části se budu věnovat pouze problematice prostředků zabezpečení a obrany proti útokům v počítačových sítích včetně sítě Internet, a to především kvůli důležitosti takovéto ochrany nejen z pohledu firem podnikajících v oblasti e-commerce.

1.1 Přehled bezpečnostních mechanizmů

Dunsmore [DUN01] uvádí jako základní možnost ochranu využitím firewallů, proxy serverů a NAT. V širším pojetí, např. dle [DOČ00A] zajišťuje bezpečnost komunikace v Internetu celá škála nástrojů. Významnou roli mezi nimi plní ty kategorie bezpečnostního software, které jsou označovány jako „velká šestka síťové bezpečnosti":

- firewally
- virtuální privátní sítě (VPN)
- produkty pro analýzu zranitelnosti
- detektory průniku (IDS)
- antivirový software
- infrastruktura veřejného klíče (PKI)

Hrozba	Řešení bezpečnosti	Funkce	Technologie
Zachycení dat, nezákonné čtení nebo modifikace	Zašifrování	Zabrání falšování zakódováním dat	Symetrické zašifrování, nesymetrické zašifrování
Uživatelé uvedou nesprávně svoji identitu (spáchání podvodu)	Autentizace	Ověřuje a identifikuje odesílatele a příjemce	Digitální podpisy
Neautorizovaný uživatel na jedné síti získá přístup do jiné sítě	Firewall	Filtruje a zabraňuje určitému typu provozu, vstup na síť nebo server	Firewally, VPN

Tabulka 4. 1 Bezpečnostní hrozby a jejich možná řešení. Zdroj [kos98]

Kromě výše uvedených patří mezi další mechanizmy zajišťující bezpečnost počítačové sítě dle [TCP98] i následující protokoly a systémy:

- Network Address Translation (NAT)
- SOCKS
- Kerberos a další autentizační systémy (AAA)
- Secure Electronic Transaction (SET)
- Šifrování

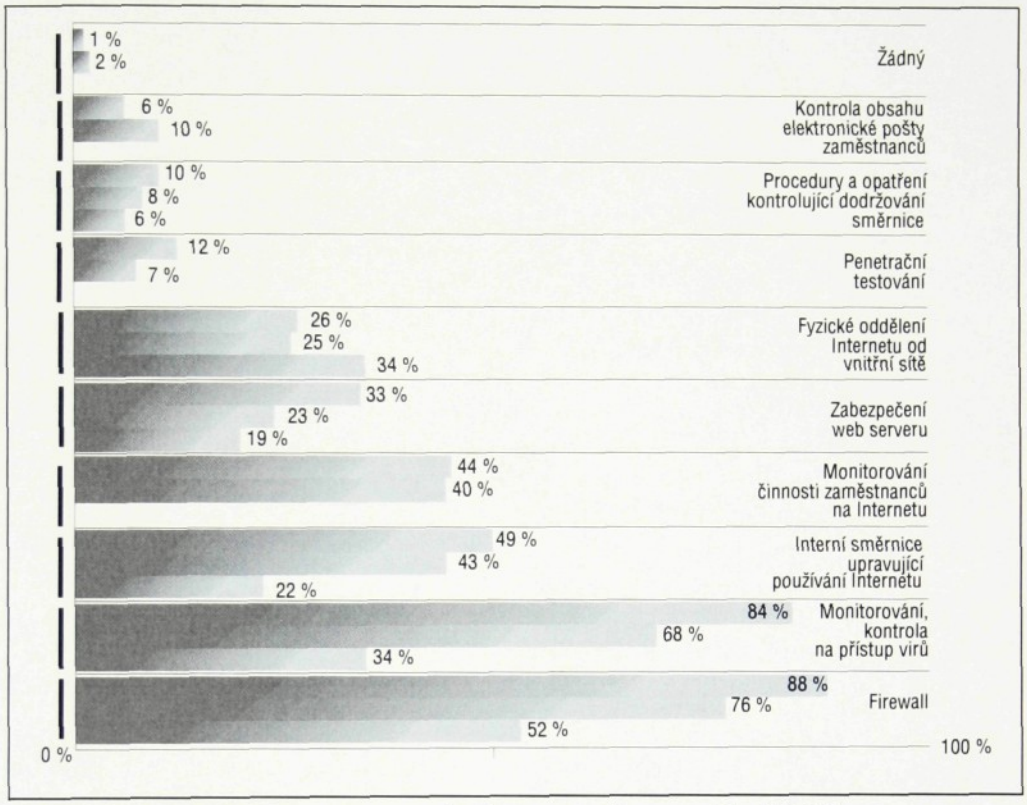
Některé z bezpečnostních hrozeb a jejich možná řešení zachycuje tabulka 4.1.

1.2 Situace v ČR

Prosazování jednotlivých bezpečnostních technologií v ČR z pohledu časového vývoje znázorňuje tabulka 4.2.

Prvek	Rok			
	1995	1998	2001	2003
Antivirus	Detekce na základě signatur	Navíc heuristika	Koexistence s desktop firewallem	Kombinovaný přístup (antivirus, desktop firewall, hybridní IDS)
Firewall	Minimální rozšíření	Paketové filtry	Aplikační proxy	kombinovaný přístup (firewall, VPN, hybridní IDS, antivirová gateway, filtrování obsahu)
IDS	Minimální rozšíření	Minimální rozšíření	tradiční IDS se signaturami	detekce anomálií

Tabulka 4. 2 Prosazování bezpečnostních technologií v ČR. Zdroj [rád02]



Obr. 4.1 Graf rozšíření způsobů zabezpečení Internetu. Zdroj [PIB03b]

Způsoby zabezpečení Internetu podle [PIB03B] znázorňuje obrázek 4.1. Působivý je pohled na údaje týkající se způsobů zabezpečení Internetu a elektronické pošty. Za poslední čtyři roky vzrostl o 36 % počet organizací chráněných firewallem, téměř třikrát počet organizací s antivirovým zabezpečením a více než dvakrát se zvýšil počet organizací, jež přijaly interní směrnici upravující používání Internetu. Poměrně velký počet organizací (12 %) již používá jako jednu z metod řešení bezpečnosti Internetu penetrační testování, tedy postupy simulující provedení skutečných útoků.

1.3 Systémy autentizace – architektura AAA

Architektura AAA – autentizace, autorizace a účtování (authentication, authorization, accounting) se používá pro ochranu IP sítí z hlediska přístupu. Autentizaci a autorizaci jsem se věnoval v první kapitole, účtování zodpovídá za záznam všech činností uživatele v systému.

1.3.1 Kerberos

Systém Kerberos je určen pro autentizaci uživatelů v případě přihlášení uživatele k systému či autentizace uživatele vůči serveru (službě) [DOS01]. Jedná se o starší systém, do popředí se v současnosti dostal zejména proto, že jej jako základní

autentizační mechanizmus pro uživatele používá systém Windows 2000. Systém Kerberos neřeší otázku šifrování dat, integrity přenášených dat – zabývá se pouze autentizací.

Kerberos používá jiný mechanizmus autentizace než standardní, u kterého je heslo sdíleno jako tajemství mezi uživatelem a systémem. Heslo nebývá uloženo přímo, bývá znehodnoceno nějakou jednocestnou funkcí (kontrolním součtem), uživatel se pak autentizuje tím, že heslo zašle systému – nebezpečí je v tom, že heslo bude odchyceno a následně zneužito útočníkem. V Kerberosu uživatel neposílá nezabezpečenou sítí heslo, ale použije jej jako šifrovací klíč, kterým zašifruje mj. jméno uživatele a aktuální čas. Serveru pak pošle místo klasického hesla tento zašifrovaný řetězec jako heslo a s tím i nezašifrovaně jméno uživatele.

Server nalezne podle jména jeho šifrovací klíč a řetězec dešifruje. Pokud se zaslané jméno shoduje se jménem v zašifrovaném řetězci a datum a ostatní údaje jsou akceptovatelné, je klient autentizován. Heslo musí být tedy známo jak klientovi, tak v nezměněné formě i serveru. V případě asymetrické kryptografie pak na straně serveru stačí, aby byl u jména uživatele udržován certifikát. V každém případě musí být databáze uživatelů a jejich klíčů dostatečně chráněna, protože je jádrem vnitropodnikové bezpečnosti, v případě použití asymetrické kryptografie pak není nebezpečná distribuce klíčů, ale citlivé je přiřazení uživatele – jeho certifikát.

1.3.2 Protokoly autentizace vzdáleného přístupu

TACACS/TACACS+

Systém řízení přístupu (Terminal Access Controller Access Control System) umožňuje prověřit každého uživatele na individuální bázi před přístupem ke směrovači nebo komunikačnímu serveru.

TACACS lze používat ve spolupráci se systémem Kerberos. Uživatel nejdříve od serveru systému Kerberos získá podklady pro autentizaci, aniž by se přenášelo heslo v síti, a na základě nich se pak autentizuje přístupovému serveru, kdykoli potřebuje vzdálený přístup.

Rozšířený systém TACACS+ již podporuje všechny tři složky architektury AAA prostřednictvím autentizace pro přihlášení se do systému (dialog mezi uživatelem a systémem pro ověření jména a hesla), autorizace (např. automatickým navázáním spojení se serverem a protokolem, který je uživateli dovoleno využívat) a shromáždění údajů o využívání systému uživatelem.

RADIUS

Služba pro autentizaci vzdálených uživatelů (Remote Authentication Dial-In User Service) v sobě zahrnuje všechny tři složky architektury AAA. V první řadě

RADIUS zodpovídá, podobně jako systém TCACS, za ověření uživatelů před přístupem do sítě. RADIUS má tři složky: protokol, servery pro autentizaci a klienty. Protokol pro komunikace mezi servery a klienty využívá transportního protokolu UDP. Transakce mezi serverem a klienty se autentizují prostřednictvím sdíleného hesla, které se nikdy nepřenáší v síti. Hesla uživatelů se posílají mezi klienty a serverem zašifrovaná.

Rozdíly mezi mechanizmy autentizace uživatelů pro vzdálený přístup vyjadřuje tabulka 4.3.

TACACS+	RADIUS
využívá transportního protokolu TCP	využívá transportního protokolu UDP
provádí šifrování celého paketu	šifruje pouze heslo
nezávislé na architektuře AAA	kombinace autentizace a autorizace
hesla v databázi mohou být zašifrována	hesla v databázi jsou nezašifrována

Tabulka 4.3 Rozdíly mezi TACACS+ a RADIUS. Zdroj [puž98]

1.4 Šifrování

Základy šifrování jsem popsal v první kapitole v rámci přehledu logické ochrany dat.

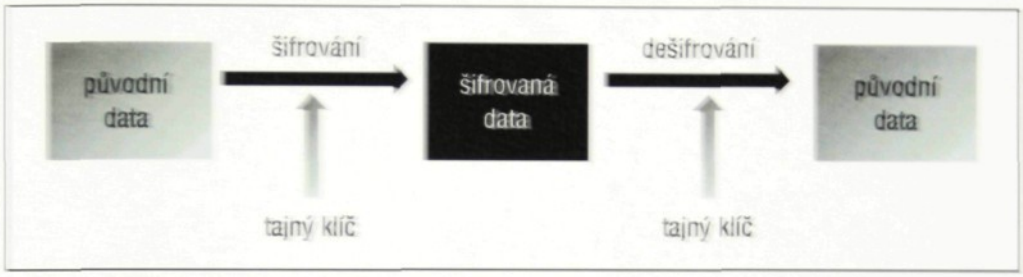
Šifrování je založeno na dvou částech: algoritmu a klíči. Kryptografický algoritmus je matematická funkce, která kombinuje prostý text nebo jiné srozumitelné informace s řetězcem čísel (klíčem), čímž se vytvoří nesrozumitelný šifrovaný text. Pro kvalitu šifrování jsou rozhodující použitý klíč a algoritmus.

Ačkoliv existují speciální šifrovací algoritmy, které nepoužívají klíče (např. hash funkce), zvláště významné jsou algoritmy používající klíče. Šifrování založené na klíčích má podle [KOS98] dvě přednosti: jednak je velmi těžké vymyslet nové šifrovací algoritmy – při použití klíče lze používat stejný algoritmus pro komunikaci s kýmkoliv, pro každého korespondenta je třeba použít pouze jiný klíč. Druhou výhodou je, že pokud se někomu podaří dešifrovat šifrované zprávy, stačí změnit pouze klíč, aby bylo možné zprávy znovu šifrovat – není nutné používat nový algoritmus.

Kryptografie je má dvě základní formy: symetrické (kryptografie s tajným klíčem) a asymetrické šifrování (kryptografie s veřejným klíčem). Význam rozdělení na dvě výše uvedené skupiny není podle Matyáše [MAT00] v rozdělení na dvě různé třídy bezpečnosti, ale v rozdělení s ohledem na problematiku správy klíčů a obecně i výkonu.

1.4.1 Symetrická kryptografie

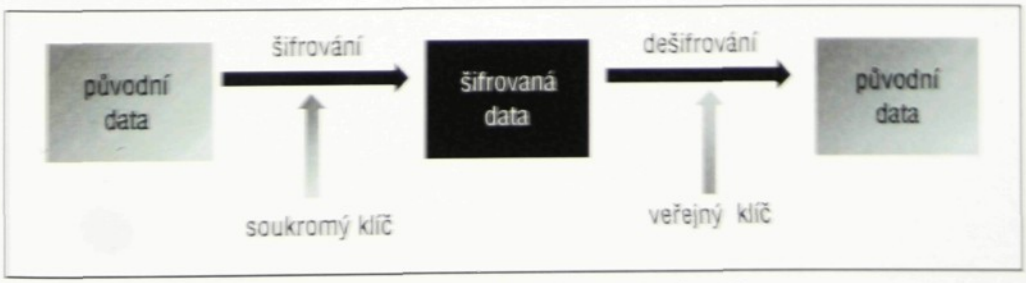
Symetrická kryptografie (kryptografie s tajným klíčem) je nejstarší forma kryptografie používající klíče. V tomto systému vlastní jak odesílatel tak příjemce stejný klíč, což znamená, že obě strany mohou zašifrovat a dešifrovat data tímto klíčem. Symetrické šifrování má však některá omezení: například se obě strany musí dohodnout na společném klíči. V případě více korespondentů se musí pro každého korespondenta udržovat zvláštní záznam tajného klíče. Pokud by se používal stejný klíč pro více korespondentů, pak tito si budou moci vzájemně číst (dešifrovat) zprávy. Systém symetrického šifrování má problémy při autentizaci, jelikož nelze prokázat identitu původce zprávy nebo jejího příjemce. Podstatu symetrického šifrování znázorňuje obrázek 4.2.



Obrázek 4.2 Symetrické šifrování. Zdroj [kun03]

1.4.2 Asymetrická kryptografie

Kryptografie s veřejným klíčem (asymetrická) je založená na odlišném principu než kryptografie s klíčem tajným. Místo jednoho klíče má každá komunikující strana klíče dva. Pomocí jednoho klíče může zprávu zašifrovat a druhá strana ji pak sama může dešifrovat pouze pomocí klíče druhého. Klíči pomocí kterého se šifruje (ten je dán veřejně k dispozici, aby mohly být přijímány šifrované zprávy) se říká veřejný klíč, a klíči, pomocí kterého je zpráva příjemce dešifrována (ten je pochopitelně chráněn) se říká tajný (soukromý, privátní…) klíč. Pomocí pokročilé matematiky lze k některým účelům použít oba klíče k opačným operacím, čehož se využívá např. u elektronických podpisů. Pro pochopení architektury systému je tedy nejdůležitější, že nikdy se nemůže šifrovat a dešifrovat tím samým klíčem, vždy musí být pro dešifrování použit ten druhý. Oba tyto klíče jsou spolu dle použitého algoritmu matematicky spjaty, pochopitelně ale ne natolik, aby se



Obrázek 4.3 Asymetrické šifrování. Zdroj [kun03]

dal jeden z druhého odvodit. Principy asymetrické kryptografie vystihuje obrázek 4.3.

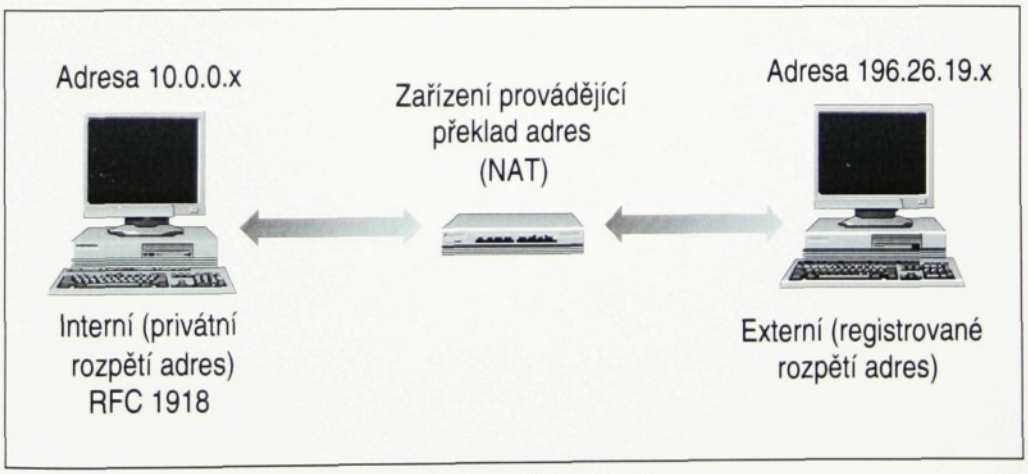
1.5 NAT

NAT (Network Address Translation) je mechanizmem používaným pro překlad IP adres používaných ve vnitřní síti na IP adresy, které je možno použít i ve vnější síti, případně i na jedinou takovou adresu.

Myšlenka NAT je založena na faktu, že pouze malá část počítačů z vnitřní privátní sítě komunikuje mimo tuto síť. IP adresa je pak tomuto počítači přiřazena až v případě, že opravdu potřebuje komunikovat s vnějším prostředím. Výhodou je to, že pro komunikaci s vnější sítí je potřeba mnohem menší počet IP adres než v případě, kdyby měl každý z počítačů vnitřní sítě danou vlastní IP adresu.

NAT se používá i jako bezpečnostní opatření, protože umožňuje skrýt strukturu vnitřní sítě a při překladu adres umožňuje aplikovat bezpečnostní politiku. Nicméně podle [TCP98] platí, že klienti, kteří komunikují s Internetem prostřednictví proxy nebo SOCKS serveru nevystavují svoji adresu na Internet a jejich adresa tedy nemusí být překládána. Pokud ovšem existuje důvod proč nevyužít proxy nebo SOCKS server, NAT může být použito k řízení provozu mezi vnitřní a vnější sítí bez zveřejňování adresy počítačů vnitřní sítě.

Prakticky je NAT je spouštěn na směrovači (routeru) nebo firewallu. Principy NAT vyjadřuje obrázek 4.4.



Obrázek 4.4 NAT. Zdroj [rus01]

1.6 Firewally

Firewall představuje dle [DOB98] systém či způsob realizace bezpečného spojení mezi lokální a veřejnou sítí při zachování funkcionality a bezpečnosti. Pod pojmem firewall se však nesmí chápat jen určité programové a technické vybavení, které chrání síť před neautorizovaným a nebezpečným přístupem z vnější sítě. Firewall je především implementace bezpečnostní politiky, která definuje povolené služby a možnosti přístupu pomocí technických prostředků, které jsou umístěny v bodě napojení informačního systému k vnější nechráněné a implicitně nebezpečné síti. Firewall pracuje v zásadě tak, že nutí veškerá síťová propojení procházet přes kontrolní systém, analyzuje komunikaci a na základě této analýzy povolí nebo zakáže propojení. Firewall může být dle [TCP98] realizován formou PC, midrange, mainframe, UNIX workstation, routeru nebo kombinací těchto prvků.

Firewall ukládá informace o provozu do souborů (logů), ze kterých lze nejenom vyčíst dílčí akce, ale i vytvářet sumární přehledy (reporty). Aktivní firewally nezapisují vniklé události pouze do logů, ale je na nich možné stanovit i jistá pravidla, kdy vzniklá událost může způsobit jistou akci – např. spuštění či ukončení programu, odeslání e-mailu, SMS zprávy s informací o události, ukončení proxy či filtru, na kterém k události došlo, zapsání IP adresy potenciálního útočníka na černou listinu, ukončení práce celého systému apod.

1.6.1 Funkční komponenty firewallu

Práce firewallu může být založena dle [DOS01] na několika mechanismech – filtrace, wrappery, proxy, brány či SOCKS. Nejdůležitějšími principy jsou pak dle [TCP98] filtrování (Packet-Filtering Router), proxy (Aplication Level Gateway) a Circut Level Gateway (SOCKS). Každá z těchto komponent má svoje specifické funkce, při stavbě efektivního firewallu se používají různé kombinace těchto funkcí.

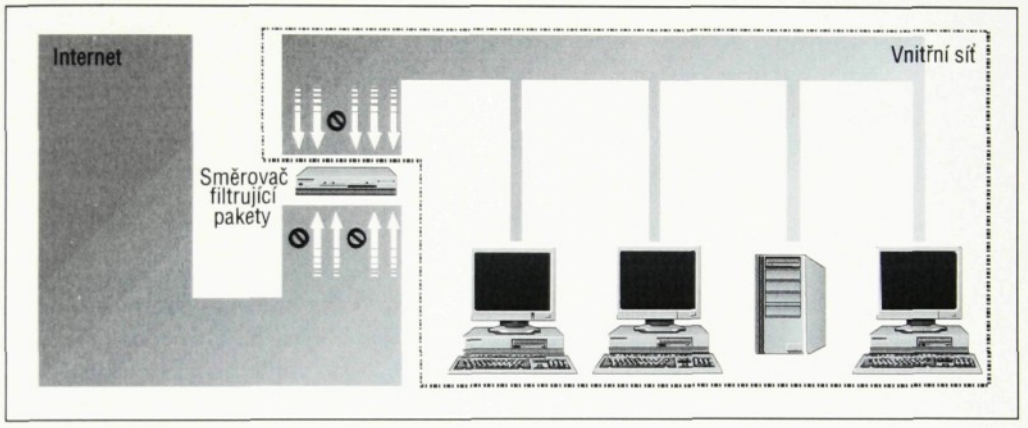
Filtrování paketů

Filtrace znamená kontrolu procházejících paketů aktivním prvkem sítě na základě jejich obsahu a následné rozhodnutí, může-li být paket poslán dále nebo ne. Filtr nemění obsah datových paketů. Filtraci lze přirovnat k cenzuře prováděné v některých případech s poštovními zásilkami.

Filtrování paketů je jednoduchá metoda, kterou lze zabránit průchodu nevhodných paketů sítí. Cílem filtrace je vytvořit polopropustný filtr, který umožňuje vlastním zaměstnancům přístup do Internetu, ale zamezuje přístup cizím uživatelům do vnitřní sítě.

Nastavení filtračních pravidel jsou založena na politice bezpečnosti sítí a jsou tedy vstupem do celého procesu filtrování.

Nevýhoda filtrování paketů je podle [TCP98] v tom, že pravidla pro filtrování paketů jsou často velmi složitá, v případě existence nějakých výjimek se situace ještě komplikuje a to s sebou nese možnost zanechání určité bezpečnostní díry. Další nedostatky jsou v tom, že schopnosti firewallů charakteru paketových filtrů jsou principiálně omezeny tím, co je možné vydedukovat ze síťových IP adres a čísel portu. Peterka [PETO1] zdůrazňuje především to, že takovéto firewally nemají schopnost analyzovat přenášená data tak detailně, aby mohly vyhodnocovat data odpovídající aplikační vrstvě – nerozumí například formátu přenášených zpráv, a tudíž ani jejich obsahu či použitým poštovním adresám, i když podle čísla portu poznají že jde o elektronickou poštu. Obrázek 4.5 znázorňuje funkci oddělovacího směrovače pro filtrování paketů.



Obr. 4.5 Oddělovací směrovač s filtrací paketů. Zdroj [cha98]

Proxy

Proxy (aplikační brána, Aplication Level Gateway) je program, který pracuje na aplikační úrovni. Skládá se ze dvou částí – pracuje jednak jako server, ale i jako klient. Serverová část proxy přijímá požadavky od klientů a předává je klientské části proxy, která jménem původního klienta předává požadavky na originální server.

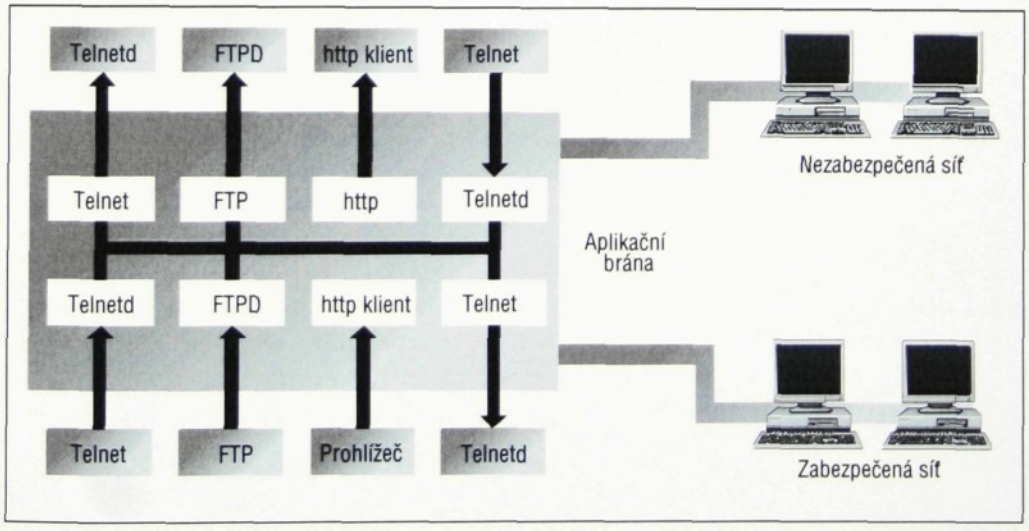
Proxy je tedy aplikace běžící na počítači se dvěma síťovými rozhraními, jedno je připojeno do vnitřní sítě, druhé do Internetu. Proxy jsou podstatně bezpečnější než pouhé filtrování paketů, na druhé straně jsou ovšem pomalejší a omezují činnost uživatele na úzce vymezený okruh služeb, které podporují. Pro každou službu totiž musí existovat aplikační brána – proxy, která je postavena mezi chráněnou a nedůvěryhodnou síť a kontroluje všechny pakety, které patří dané službě. Proxy, která je společná pro všechny aplikační protokoly může zajišťovat SOCKS server.

Princip činnosti aplikační brány je jednoduchý – všechny uživatelské programy komunikují s aplikační bránou, namísto aby komunikovali přímo se skutečným počítačem, který danou službu poskytuje. S tímto počítačem komunikuje až bezpečnostní brána, která veškerou komunikaci kontroluje, řídí a zabraňuje tomu, aby se vykonaly nepovolené operace.

Proxy může dále provádět filtraci a cache. Filtrace může podobně jako na při filtraci na směrovačích povolovat komunikace skrze proxy jen některým počítačům, zajímavější je však typ filtrace, který na směrovačích možný není (směrovač na rozdíl od proxy „nevidí" do aplikačního protokolu) – proxy může filtrovat např. povolování některých aplikačních příkazů a zakazování jiných nebo provádět filtraci obsahu jako jsou aplikace ActiveX nebo JavaScript, které představují určité potenciální riziko. Běžné je také udržování „černé listiny" serverů, kam si zaměstnavatel nepřeje, aby jeho zaměstnanci přistupovali. Funkce cache pak znamená, že proxy si může zpracované požadavky a jejich odpovědi ukládat na disk a v případě opakování stejného požadavku pak může odpovědět přímo z cache.

Aplikační brány představují mnohem komplexnější řešení nežli pouhá filtrace paketů. Jednak nabízejí možnosti zapisování událostí do logů, další výhodou je pak to, že používají silnou uživatelskou autentizaci [TCP98].

Nevýhodou aplikačních bran je to, že pokud chce uživatel využít připojení přes proxy server, musí změnit klientský software, který podporuje danou proxy službu. Toho lze docílit spíše změnou chování uživatelů nežli modifikací software. Například pokud se chce uživatel spojit na server Telnet přes proxy server, musí se neprve přihlásit a autentizovat na proxy serveru a poté pak na Telnet serveru samotném. To vyžaduje jeden krok navíc. Nicméně moderní Telnet klienti dokáží tento problém již řešit. Princip aplikační brány vyjadřuje obrázek 4.6.



Obr. 4.6 Proxy. Zdroj: [tcp98]

1.6.2 Architektura firewallů

Firewall je systém tvořený jedním nebo více počítači vyhrazený k bezpečnému oddělení vnitřní sítě od Internetu tak, aby mohli uživatelé vnitřní sítě přistupovat k informacím dostupným na Internetu [DOS01]. Dobře fungující firewall využívá kombinace výše uvedených funkčních komponent.

Některé služby, jako je filtrace, proxy či NAT, provádí firewall sám. Jiné služby, jako je zjišťování virů v datech procházejících firewallem či autentizace klientů, může vyžadovat od aplikací běžících i na jiných počítačích specializovaných pouze pro tyto účely. Takové počítače jsou zpravidla umístěny ve vnitřní síti. Firewall pak pracuje jako klient těchto serverů.

Podle [TCP98] existují čtyři důležité architektury firewallů, jsou to:

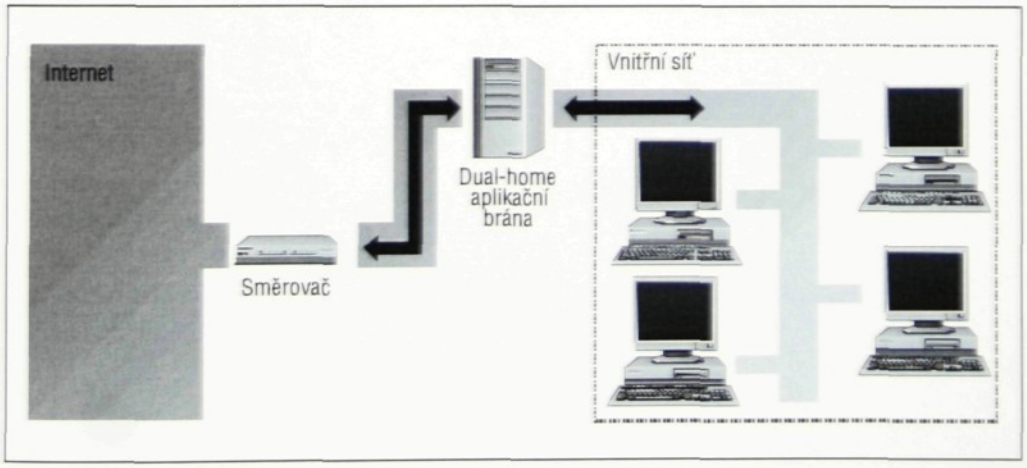
- Packet-Filtering Firewall
- Dual-Homed Gateway Firewall
- Screened Host Firewall
- Screened Subnet Firewall (DMZ)

Packet Filtering Firewall

Je to nejjednodušší implementace firewallu. Ochrana lokální sítě řeší pomocí filtrace paketů. Všechny počítače lokální sítě mají přímé spojení s veřejnou sítí, jediným oddělením je pouze filtrující logika. Základem bezpečnosti je definice pravidel filtrování. Filtraci paketů znázorňuje obrázek 4.5.

Dual-Homed Gateway Firewall

Tato implementace firewallu je vytvořena pomocí jednoduchého filtrujícího směrovače (Screening Router) a aplikační brány. Firewall je nakonfigurován tak, aby dovolil spojení z vnější sítě pouze na aplikační bránu, která provádí autentizaci a autorizaci veškeré přicházející komunikace – neexistuje tedy cesta, kterou



Obr. 4.7 Dual-Homed Gateway Firewall. Zdroj [dob98]

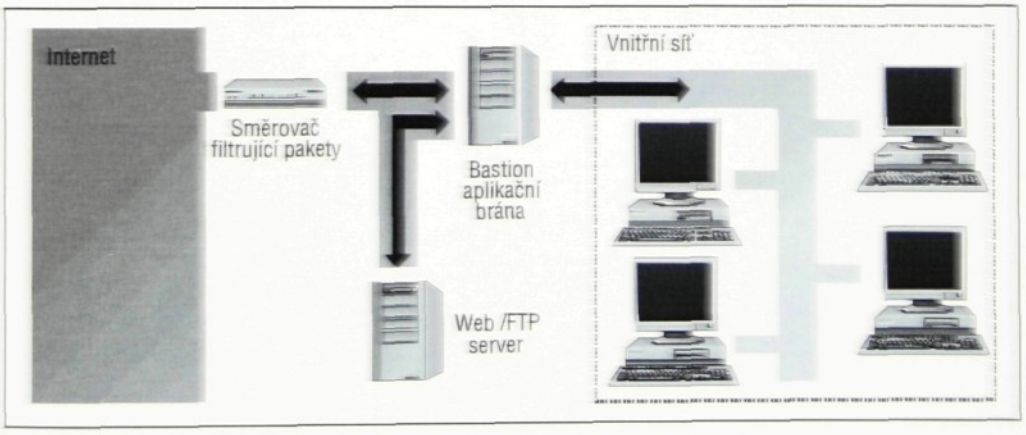
by mohl paket projít firewallem, pokud není tato služba na proxy definována. Všechna další spojení routeru na ostatní počítače vnitřní sítě jsou zakázána.

Ve srovnání s jednoduchým firewallem filtrujícím pakety, zaručují Dual-Homed Gateway Firewally, že jakýkoliv útok, který pochází skrze neznámou službu bude blokován. Tento typ firewallů používá metodu „co není výslovně povoleno je zakázáno".

Pokud je potřeba využít informačního serveru (WWW, FTP) tak, aby byl přístupný i od uživatelů z vnější sítě, může být buď instalován uvnitř chráněné sítě nebo může být umístěn mezi firewall a router, což nezaručuje vysokou úroveň bezpečnosti. Pokud je tedy instalován za firewall, musí být na firewallu aktivována proxy služba tak, aby umožnila přístup na server z vnitřní zabezpečené sítě. Pokud je informační server instalován mezi firewall a router, router by měl být schopen filtrace paketů a být vhodně nakonfigurován. Takový typ firewallu se nazývá Screened-Host Firewall.

Screened-host firewall

Tento typ firewallu se skládá z routeru filtrujícího pakety a aplikační brány. Router je konfigurován tak, aby směroval veškerý provoz na „bastion host" (aplikační bránu) a v některých případech na informační server. Protože vnitřní síť je na stejné podsíti jako bastion host, bezpečnostní politika umožňuje uživatelům z vnitřní sítě přístup ven buď přímo, nebo skrze proxy server. Toho může být dosaženo tím, že pravidla filtrujícího routeru jsou nastavena tak, že router propustí pouze provoz, který pochází z „bastion host". Obrázek 4.8 znázorňuje funkci firewallu typu Screened-Host Firewall.

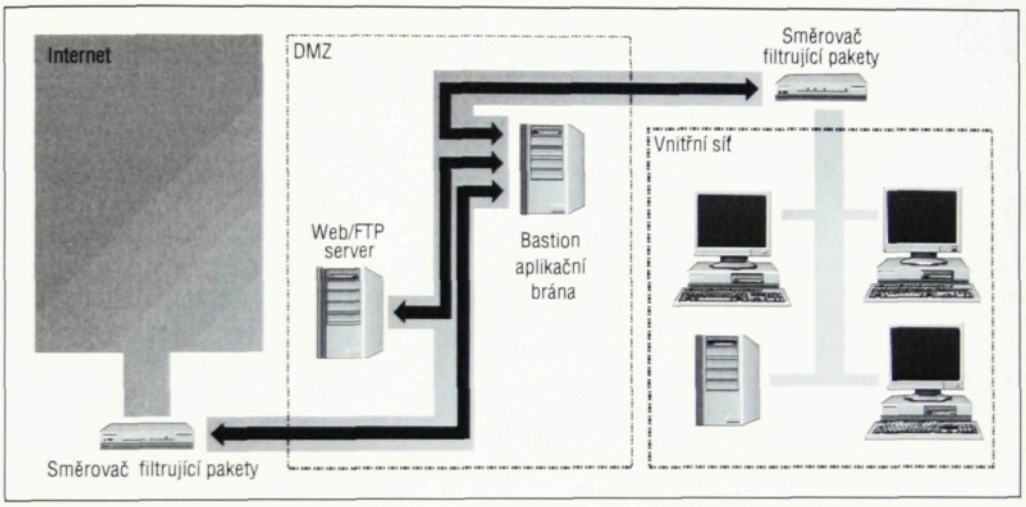


Obrázek 4.8 Screened-Host firewall. Zdroj: [tcp98]

Screened Subnet Firewall – demilitarizovaná zóna (DMZ)

Tento typ firewallu zahrnuje dva routery filtrující pakety a bastion host. Filozofií tohoto řešení je vytvořit „mezisítě" mezi vnější a vnitřní chráněnou sítí. Tato

mezisíť je připojena k vnější i lokální síti přes routery filtrující pakety. Bastion host (aplikační brána) je pak umístěna uvnitř „demilitarizované zóny". Aplikační brána kontroluje veškerá spojení, která procházejí přes tuto zónu. Screening router, který spojuje DMZ s vnější sítí, směřuje veškerou komunikaci pouze na aplikační bránu. Router spojující DMZ s interní sítí pak směruje pakety pouze mezi aplikační bránu a vnitřní síť. Tento router tedy chrání lokální síť jak proti vnější síti, tak i proti DMZ. Veškerá komunikace je tedy kontrolována aplikační bránou. Toto propojení představuje nejbezpečnější formu realizace síťového rozhraní, útoční by musel proniknout třemi oddělenými systémy aby se dostal do vnitřní sítě. Do DMZ je vhodné umístit i další servery, např. WWW server. Obrázek 4.9 vystihuje strukturu firewallu typu DMZ.



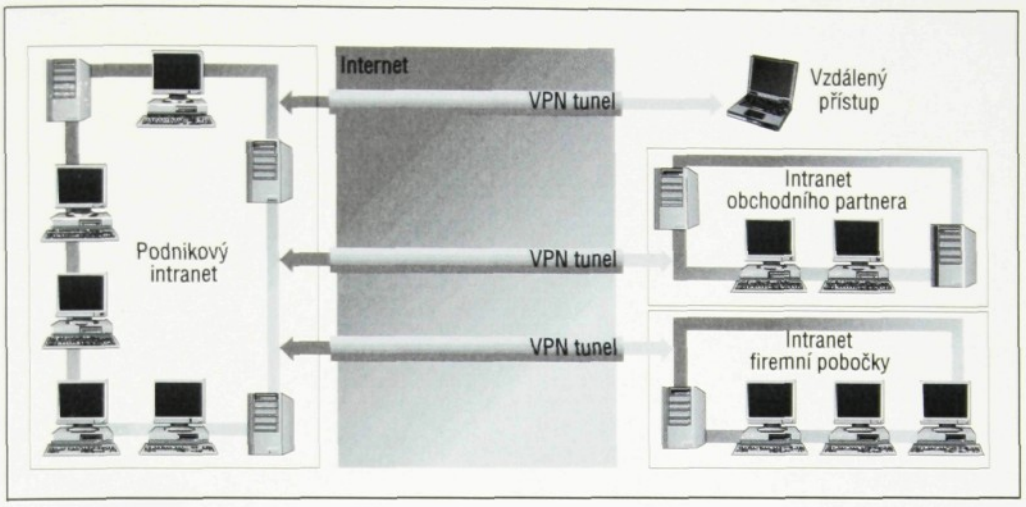
Obr. 4.9 Demilitarizovaná zóna. Zdroj [dob98]

1.7 Virtuální privátní sítě (VPN)

Virtuální privátní síť je rozšířením podnikového intranetu přes veřejnou nedůvěryhodnou síť jako je Internet při zachování bezpečeného spojení, které je zajišťováno tzv. tunely [TCP98]. VPN umožňuje bezpečné propojení poboček, vzdálených uživatelů a obchodních partnerů do rozšířené podnikové sítě. Názorně tuto situaci popisuje obrázek 4.10.

Technicky jsou virtuální privátní obvykle řešeny integrací do routerů nebo jako součást firewallů.

Existuje několik různých typů virtuálních privátních sítí. V závislosti na požadavcích na funkcí sítě pak můžeme přistoupit k vybudování sítě daného typu několika způsoby. Rozhodnutí, který způsob zvolit, závisí na druhu problému, který má daná VPN řešit, požadavcích na míru bezpečnosti sítě, požadavcích na škálovatelnost řešení a náročnosti na implementaci, správu a údržbu.



Obrázek 4. 10 Virutální privátní síť. Zdroj [tcp98]

1.8 Produkty pro analýzu zranitelnosti

Produkty pro analýzu zranitelnosti (bezpečnostní skenery) jsou nástroje bezpečnostního auditu, které slouží k periodické prověrce sítě a připojených počítačů. Produkty tohoto typu používají interní databázi známých bezpečnostních děr a chybných konfigurací. Zodpovědnost za aktualizaci této databáze spočívá u komerčních produktů na jejich výrobci. Někteří z nich se omezují na protokol IP, produkty dalších jsou schopny identifikovat chyby v rámci jiných síťových protokolů. Obdobně jako u skenerů virů úspěšnost produktu na analýzu zranitelnosti závisí na včasné aktualizaci příslušné databáze.

1.9 Detektory průniku (IDS)

Systémy pro detekci neoprávněného průniku umožňují zvýšit zabezpečení informačních systémů před útoky ze sítě Internet či z vnitřních sítí organizace, a jsou tak vhodným doplňkem k firewallové ochraně.

Systém pro detekci neoprávněného průniku (Intrusion Detection System – IDS) je tvořen kombinací softwarového a hardwarového vybavení vhodně zakomponovaného do počítačové sítě, která je schopna odhalit neoprávněné, nesprávné nebo anomální aktivity v síti. IDS detekuje útoky na aktivní prvky počítačové sítě nebo na servery. Kromě samotné detekce útoků poskytuje IDS také různé možnosti odezvy na útoky.

1.9.1 Základní členění

Detektory průniku umožňují operativně reagovat na zjištěné útoky na síť. Lze je dle [DOČOOA] v zásadě rozdělit na počítačově a síťově orientované.

Počítačově orientované

Počítačově orientované IDS jsou umístěny na jednotlivých počítačích v síti. Správu prvků systému IDS usnadňuje specializovaný dohledový software, který usnadňuje administrátorům provádění vzdálené konfigurace IDS senzorů. Jednotlivé IDS senzory komunikují s dohledovou stanicí a předávají jí informace o realizovaných útocích. Dohledový systém pak umožňuje konfigurovat reakci IDS systému na určité typu útoků. Dohledová stanice je schopna upozornit administrátora na probíhající útok např. elektronickou poštou nebo zprávou na pager. Prostřednictvím tohoto softwaru se rovněž realizuje aktualizace databáze signatur, která obsahuje charakteristiky známých útoků.

Síťově orientované

Síťově orientované IDS pasivně monitorují síťě, je vhodné umístit zejména do hraničních částí počítačové sítě. Typické je doplnění firewallové ochrany systémem IDS, kdy firewall realizuje filtraci provozu dle nastavených pravidel a systém IDS monitoruje datový provoz, upozorňuje na útoky a případně spolupracuje s firewallem nebo hraničním směrovačem při eliminaci neoprávněné aktivity. IDS lze umísťovat do segmentu mezi směrovač do Internetu a firewall, resp. mezi firewall a vnitřní část sítě, do demilitarizovaných zón (DMZ), ke směrovačům zabezpečujícím vzdálený přístup uživatelů do podnikové sítě. Segmenty, ve kterých se nacházejí kritické aplikační a databázové servery, jsou dalším místem, kde lze s výhodou využít vlastností IDS.

Společným problémem obou metod je, že spolehlivě detekují pouze známé metody průniku, a proto tento způsob obrany ztrácí účinnosti, pokud útočník přijde s něčím zcela novým. Detektory průniku je problém testovat a navíc se mohou samy stát terčem útoku.

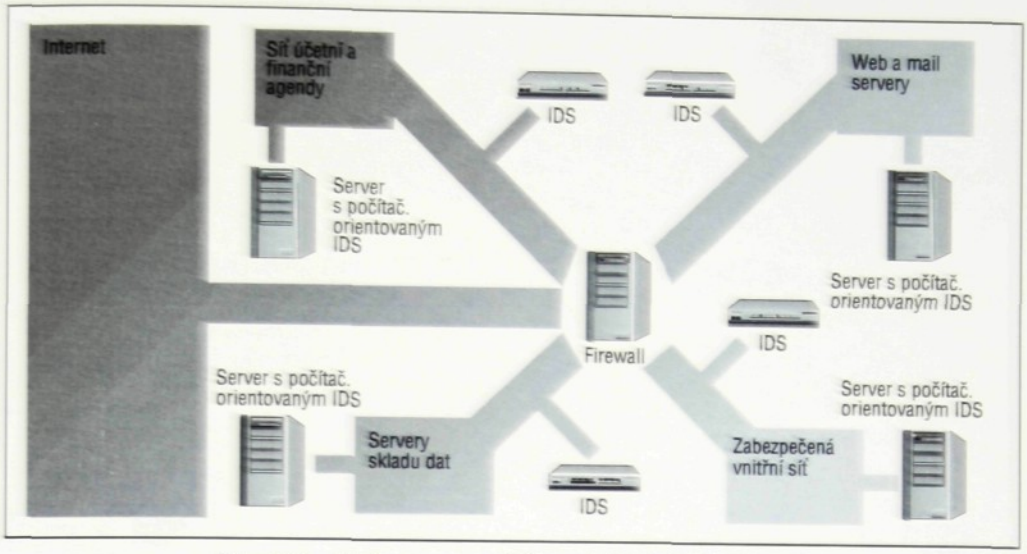
Obrázek 4.11 zobrazuje možnosti nasazení IDS v podnikové síti napojené na Internet.

1.9.2 Metody detekce

Hlavní metody detekce neoprávněného průniku jsou dle [PAN03] detekce vzoru, stavová detekce vzoru, dekódování protokolu, heuristická analýza a detekce anomálií.

Detekce vzoru

Systémy využívající tuto detekční metodu porovnávají datový provoz na síti s databází signatur známých útoků (signatura je množina podmínek, které když jsou splněny, indikují pokus o neoprávněný průnik). Tato metoda je jednoduchá, přesná, ale zároveň málo pružná. Detekce nových nebo modifikovaných útoků je problematická, protože závisí na existenci popisu daného útoku v databázi signa-



Obr. 4. 11 Možnosti nasazení IDS v podnikové síti. Zdroj [rus01]

tur. Obvykle se tato metoda omezuje pouze na inspekci jediného datového paketu, a je tedy snadno oklamatelná.

Stavová detekce vzoru

Rozšíření předchozí metody, které umožňuje analyzovat datový tok a detekovat signatury i v případě, že jsou rozděleny do více paketů.

Dekódování protokolu

Systém nejprve detekuje používaný protokol komunikace mezi entitami a následně na něj aplikuje předem definovaná pravidla a identifikuje případné porušení těchto pravidel.

Heuristická analýza

Tato metoda využívá statistické vyhodnocování parametrů monitorovaného provozu.

Detekce anomálií

Systémy s tímto mechanismem detekují odchylky od typického chování sítě. Největším problém u této metody je stanovit, co je tímto typickým chováním. Při implementaci těchto systémů se proto často používají algoritmy umělé inteligence, např. neuronové sítě. Při jakýchkoliv změnách v chování sítě IDS detekuje tyto změny a generuje alarm. Je tedy obtížné rozlišit skutečné útoky od falešných a také mohou nastat situace, kdy útok není detekován vůbec, protože se neodlišuje od normálního chování sítě. Naproti tomu výhodou tohoto mechanizmu je, že je schopen detekovat nové, doposud neznámé útoky.

Reálné IDS obvykle využívají kombinaci více detekčních metod. Odpovědí IDS na detekovaný útok může následně být reset podezřelého TCP spojení, zahájení

filtrace nebezpečného provozu na směrovači nebo firewallu a záznam podezřelé aktivity do logu. V prvních dvou případech IDS nejen monitoruje, ale i aktivně chrání prvky počítačové sítě a koncové stanice před důsledky případných útoků.

1.10 Antivirový software

Vysoký nárůst používání Internetu jako přenosového média jej logicky předurčil k použití jako přenosové cesty pro viry. S příchodem nových technologií, jako například Java, se dramaticky zvýšil nejen počet virů, ale i spektrum jejich činnosti. U antivirových produktů je také velmi důležitým aspektem reakční doba na nový virus, schopnost ho detekovat a také vyčistit. U posledních virů je právě tou nejhrozivější funkcí rychlost a čas jeho šíření. Úkol vymýtit viry z interní sítě se rozpadá do několika oblastí, dělených právě podle způsobu přenosu.

1.10.1 Možnosti umístění antivirové ochrany

Antivirové programy instalované na pracovní stanice jsou schopny poskytnout základní ochranu před viry na koncové stanici, ale ponechávají otevřené všechny přenosové cesty využívající sítě. Logickým vyústěním dalších úvah je ochrana souborových systémů na serverech poskytujících sdílené souborové systémy. Dalším krokem je ochrana prostředí, ve kterém se mohou viry přenášet například replikací databází. Zároveň je tak implementována ochrana elektronické pošty. Posledním krokem je zajistit znemožnění přístupu virů do interní sítě přes Internet, ať už stažením infikovaných dat uživatelem nebo jinými způsoby. Ve spolupráci s firewallem je možno provádět antivirovou ochranu přímo na firewallu, který spolupracuje s antivirovým serverem. Tím se uzavírá poslední možná přístupová cesta virů do zabezpečované sítě. Nad všemi výše uvedenými programy je nutno vytvořit centrální správu a pravidelný, pokud možno automatizovaný update definičních souborů.

1.10.2 Způsoby detekce

Skenování

Na počátku technologie skenování programů byl nápad, a to nápad geniální. Totiž vybrat z těla virů některé charakteristické skupiny instrukcí a takto získané sekvence použít pro hledání napadených programů. Koncepce sama sice vyžaduje pravidelnou aktualizaci, protože skener umí najít pouze viry, které zná, tato skutečnost je ale podle [HEI01] vyvážena jedinečnou schopností rozpoznat napadený program ještě před tím, než se nám ho podaří spustit.

Problém této koncepce ovšem nastal s příchodem polymorfních virů, které se automaticky proměňují v různých závislostech (kódují své identifikační charakteristiky), jejich tělo není stabilní a tím velmi ztěžují vlastní detekci. Pro některé z nich je sice možné stvořit sekvence (nebo několik sekvencí), která vir zachytí,

ale ta už obsahuje tolik variabilních částí, že se často najdou i zdravé programy, ve kterých nějaký fragment kódu nebo dat takové sekvenci vyhovuje. Moderní skenery obsahují emulátor strojového kódu, kterým se pokouší emulovat provedení dané zakódované charakteristiky, a pak mohou hledat sekvence až v dekryptovaném těle viru.

Kontrola integrity

Kontrola integrity (integrity checker, CRC checker) je založena na porovnávání aktuálního stavu důležitých programů a oblastí na disku s informacemi, které si o nich kontrolní program uložil při jejich příchodu do systému nebo při své instalaci. Pokud se do tímto způsobem chráněného počítače dostane vir, tak na sebe upozorní změnou některého z kontrolovaných objektů a je záhy detekován. Dají se tak spolehlivě zachytit i nové viry, o jejichž existenci nemají ponětí skenery, a které nemusí odhalit ani heuristická analýza. Nejprve je ovšem nutno kontrolu integrity správně nainstalovat. To především znamená zahrnout do seznamu kontrolovaných objektů pokud možno všechny důležité a často používané programy.

Heuristická analýza

Heuristická analýza (Heuristic Analyzer, Code Analyzer) podrobně analyzuje obsah souborů na pevném disku a vyhledává v něm různé podezřelé konstrukce (přímé zápisy na disk, převzetí kontroly nad operačním systémem apod.). Heuristická analýza je obecně fungující metoda, není tedy závislá na virové databázi a tímto způsobem lze odhalit i dosud neznámé viry. Heuristická analýza bývá většinou součástí skenerů, samostatně ji provozovat nelze.

Monitorování činnosti

Monitorovací programy (Behavior Blocker) obecně hlídají změny v nastavení systému a chrání systém především před replikací viru či spuštění nežádoucích činností trojských koní, a to na základě neustále kontroly a posléze aktivního zastavení takové ilegální akce. Monitorovací programy jsou tedy aktivními nástroji pro detekci virů na základě změn v chování systému, a to v reálném čase. Tyto programy zabraňují nelegálním akcím a signalizují, kdykoliv se cokoliv v systému pokouší o nějakou podezřelou akci, která má charakteristiky chování viru, popř. jinak škodlivého, ilegálního chování. Virus není ničím jiným než sekvencí příkazů, je zde tedy značná pravděpodobnost, že i legitimní programy mohou provádět stejné akce, a povedou tedy ve svém důsledku k signalizaci stejně jako virus.

1.11 Infrastruktura veřejného klíče (PKI)

PKI je soustavou technických a především organizačních opatření spojených s vydáváním, správou, používáním a odvoláváním platnosti kryptografických

klíčů a certifikátů [DOS01]. Poskytuje rovněž prostředky pro bezpečné využívání veřejných klíčů distribuovaných uživateli a systémy. Šifrování jsem se obecně věnoval již v první kapitole mé diplomové práce a i v předchozí části této kapitoly, v tomto oddílu budu podrobněji popisovat strukturu PKI a s tím spojenou problematiku oblasti elektronického podpisu.

1.11.1 Elektronické podpisy

Elektronické podpisy jsou jedním z hlavních přínosů asymetrické kryptografie. Elektronický podpis je v praxi jen sekvence čísel za určitým dokumentem. Oproti ručnímu podpisu je ovšem zvláštní rozdíl v tom, že ruční podpisy jednoho člověka na dvou různých dokumentech jsou ne-li stejné tak alespoň podobné, vedle toho elektronické podpisy jednoho člověka pod dvěma různými dokumenty jsou naprosto odlišné. Vedle matematického pozadí elektronických podpisů tomu tak je ze zřejmých důvodů – to, co můžeme udělat ve skutečnosti, např. okopírovat něčí podpis na jakýkoliv dokument, bychom mohli na počítači udělat ještě snáze, navíc by byl padělek od originálu naprosto k nerozeznání.

Hash

Klíčovým pojmem, nutným k porozumění filosofii elektronických podpisů je tzv. bezpečný výtah zprávy (Message Digest, Hash). Výtah zprávy (dále jen hash) je algoritmus, který z jakkoliv dlouhé posloupnosti znaků vytvoří číslo s konstantní délkou a to za stanovených podmínek.

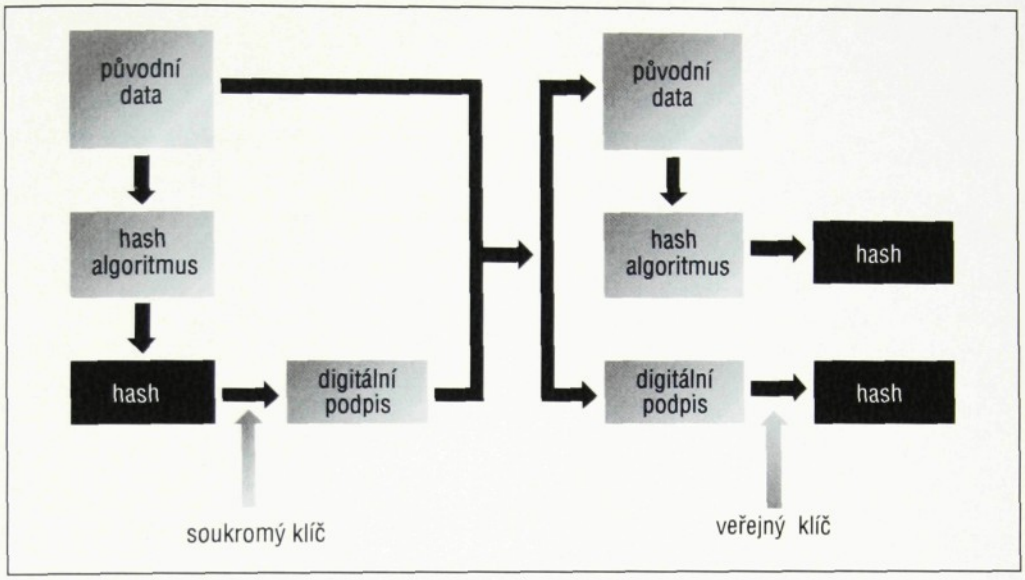
Spočítat hash jakékoliv zprávy musí být velmi jednoduché, ale vymyslet zprávu tak, aby měla nějaký konkrétní hash musí být velmi obtížné. Nejznámější v kryptografii používané algoritmy jsou MDx (Message Digest 2, 4, 5), SHA (Secure Hash Algorithm) a RIPE-MD. Bezpečnost hashovací funkce je přímo závislá na délce výstupního bloku, dále pak obvykle platí, že i malá změna ve vstupu způsobí velkou změnu ve výstupu.

Proces elektronického podepisování

Vlastní elektronický podpis (zde uvedený postup podle nejjednoduššího asymetrického algoritmu RSA) funguje v obecné rovině velmi jednoduše. Pokud chce A podepsat nějaký dokument, vygeneruje z něj výtah a zašifruje ho svým tajným klíčem. Toto přiloží k dokumentu, čímž ho podepíše. Na druhé straně B separuje podpis od dokumentu, spočítá výtah z textu a dešifruje podpis veřejným klíčem A. Tím dostane dvě hodnoty. Pokud se rovnají, je podpis platný.

Kdyby kdokoliv chtěl podpis zfalšovat, musel by mít jeho tajný klíč. Nebo by také mohl něčí podpis přiložit pod jiný dokument. Jenže to nejde, protože by se pak neshodovaly výtahy textu a dešifrovaného podpisu. A nemožnost vymyšlení dokumentu s daným hashem plyne přímo z výše uváděné definice výtahů ze zpráv. Jak je vidět, v kryptografii s veřejným klíčem vše stojí a padá s bezpečným

uschováním tajného klíče. Obrázek 4.12 názorně popisuje proces elektronického podepisování.



Obr. 4.12 Proces elektronického podepisování. Zdroj [kun03]

Vlastnosti elektronického podpisu

Po digitálním podpisu jsou podle [KOPO1] požadovány tyto základní vlastnosti:

- Identifikace
- Autentizace
- Integrita
- Nepopiratelnost

Identifikace zaručuje, že z přijaté zprávy jednoznačně vyplývá, od koho pochází, tedy kdo je jejím autorem. Autora určuje identifikace, ověření skutečné identity pak autentizace.

Autentizace (některé zdroje, např [TILL02] hovoří o nepopiratelnosti podpisu) – jen a právě vlastník má přístup k tajnému klíči. Elektronický podpis jednoznačně spojí dokument s daným klíčem. Každý klíč musí být nositelem nějaké jmenovky, aby se poznalo, čí ten klíč je. Kdokoliv si však může vytvořit klíče s libovolnou jmenovkou, s ním pak může šifrovat, dešifrovat či podepisovat. Bude to mít ale jeden háček: nebude to klíč dané osoby, ale někoho úplně jiného, někoho, kdo tento klíč podvrhl. Pro tento případ je do modelu elektronického podpisu zavedena tzv. důvěryhodná třetí strana – certifikační autorita – viz dále.

Integrita (též autentičnost zprávy) – příjemce musí mít možnost odhalit jakoukoliv změnu zprávy. Toho lze docílit použitím hashovací funkce: jakákoliv změna

vstupu způsobí radikální (tj. neúměrnou) změnu výstupu a při ověřování bude podpis neplatný.

Nepopiratelnost – autor nemůže později popřít autorství zprávy, resp. souhlas s obsahem zprávy, jedná se tedy o téměř dokonalou analogii s podpisem vlastnoručním.

1.11.2 Certifikační autorita

Zákon [ZEP00] definuje certifikační autoritu jako poskytovatele certifikačních služeb – subjekt, který vydává certifikáty a vede jejich evidenci, případně poskytuje další služby spojené s elektronickými podpisy.

Certifikační autorita je tedy instituce – důvěryhodná třetí strana, která svým podpisem na cizím veřejném klíči stvrzuje, že klíč patří skutečně tomu subjektu, který je napsán na jmenovce [TILL02]. Jde o víceméně identickou operaci jako elektronické podepisování dokumentů, rozdíl je pouze v interpretaci výsledku.

1.11.3 Certifikát

Dle Zákona o elektronickém podpisu [ZEP00] se certifikátem rozumí datová zpráva, která je vydána poskytovatelem certifikačních služeb, spojuje data pro ověřování podpisů s podepisující osobou a umožňuje ověřit její totožnost. Certifikát slouží k důvěryhodnému předání dat pro ověřování elektronického podpisu podepisující osoby [EP002]. Certifikát je tedy jakýsi podpis certifikační autority pod veřejným klíčem dané osoby, který zaručuje nepopiratelnost podpisu jím podepsaných zpráv.

Kapitola 5
Návrh zabezpečení IS podniku

V předchozích částech mé diplomové práce jsem se zabýval teoretickými možnostmi zabezpečení informačního systému podniku. V této části budu tyto teoretické možnosti aplikovat na zabezpečení IS modelové firmy. V úvodu budu charakterizovat modelový podnik a jeho specifické nároky na zabezpečení. V další části se zaměřím na zabezpečení podnikové sítě pomocí firewallu a doplním celkové zabezpečení dalšími prvky.

1.1 Modelový podnik

V této kapitole se budu snažit navrhnou optimální zabezpečení informačního systému podniku, přičemž budu pracovat s modelovou firmou ABC

1.1.1 Charakteristika podniku

Firma, ABC je menším obchodním podnikem zabývajícím se obchodováním s elektronikou. Součástí obchodního modelu je i elektronické obchodování (e-shop). Počet zaměstnanců je 17, z nichž 13 má přístup a využívá podnikovou síť, firma tedy spadá do skupiny malých a středních podniků. V současnosti pro naprosté zjednodušení neuvažuji o žádném bezpečnostním opatření v podniku kromě standardních fyzických opatřeních nutných pro provoz firmy (protipožární ochrana apod.).

1.1.2 Organizační struktura

Firma zaměstnává celkem 17 pracovníků. Organizační struktura společnosti je liniová. Na nejvyšší pozici je ředitel (majitel), kterému jsou podřízeni kromě asistentky ještě finanční oddělení, oddělení IT a obchodní ředitel. Obchodní ředitel pak dohlíží na oddělení marketingu, obchodní oddělení, oddělení dopravy a sklad. Konkrétní počty pracovníků a jejich zařazení do jednotlivých oddělení pak shrnuje tabulka 5.1.

Oddělení	Pozice pracovníka	Počet pracovníků
Ředitelství	Ředitel (majitel)	1
	Asistentka	1
	Obchodní ředitel	1
Finanční oddělení	Účetní	1
	Účetní personalistka	1
IT oddělení	Správce sítě	1
Marketingové oddělení	Vedoucí - e-obchod	1
	Propagace	1
Obchodní oddělení	Prodejce	2
	Nákupčí	1
	Reklamace	1
Oddělení dopravy	Dopravce	2
Sklad	Skladník	3
Celkem zaměstnanců		**17**

Tabulka 5.1 Zaměstnanci a jejich zařazení do jednotlivých oddělení. Zdroj vlastní.

1.1.3 Popis jednotlivých oddělení

Obchodní ředitel

Asi největší mrou se zabývá řízením podniku, má na starosti dobrý chod firmy, dále marketingové oddělení, oddělení dopravy, obchodní oddělení a sklad. Ve spolupráci s ředitelem naplňuje firemní strategii společnosti. Obchodní ředitel sdílí s ředitelem společnou asistentku.

Finanční oddělení

Zahrnuje dva zaměstnance, kteří mají na starosti jak zabezpečení personalistiky pro celou firmu, tak vedení celé účetní agendy, která je vzhledem k obchodní povaze firmy rozsáhlejší. Nutno poznamenat, že vzhledem k velikosti firmy nelze předpokládat, že účetní – personalistka, bude mít na starosti pouze personalistiku, podílí se i na jiných činnostech firmy v dané oblasti.

Oddělení IT

Hlavní náplní je správa sítě a technické podpora elektronického obchodu. Zabezpečuje hladký chod informačního systému, řeší běžné problémy v oblasti HW a SW, telekomunikačních a reprografických zařízení a má na starosti uživatelskou podporu všech uživatelů podnikového informačního systému.

Marketingové oddělení

Pod toto oddělení náleží veškeré činnosti spojené s propagací nabízeného zboží (a včetně výroby katalogů, reklamních letáků a dalších tiskovin) a také starost o dobré jméno firmy. Vedoucí oddělení má na starosti i záležitosti týkající se Internetového obchodu.

Sklad

Do náplně práce tří zaměstnaných skladníků patří přijímání, vyskladňování a manipulace se zbožím, samozřejmě včetně udržování přesné evidence ve firemní databázi.

Oddělení dopravy

Oddělení má dva pracovníky a příslušné dopravní automobily. Hlavní činností oddělení je rozvoz zboží zákazníkům a od dodavatelů.

Obchodní oddělení

Jedná se o největší oddělení ve firmě – sestává se ze čtyř lidí – dva prodejci, jeden nákupčí a další pracovník, který se zabývá agendou spojenou s vyřizováním reklamací.

- **Prodejci** – prodejci jsou dva – jeden zařizuje větší objednávky a druhý má na starosti požadavky menších klientů. Oba zároveň získávají nové zákazníky.
- **Nákupčí** – převážnou částí jeho práce je vyjednávání množstevních či jiných slev u jednotlivých dodavatelů, celková spolupráce s nimi a případné získávání dodavatelů nových.
- **Reklamace** – pracovník reklamací má na starosti jednak komunikaci se zákazníkem, který zboží reklamuje a také s dodavatelem, od kterého bylo reklamované zboží odebráno.

1.1.4 Podniková síť

Struktura a popis sítě

Podniková síť je založena na centrálním serveru v sídle firmy, ke kterému je lokálně připojeno 13 stanic, v lokální síti se nachází i několik síťových tiskáren. Počet uživatelů a jejich umístění přehledně uvádí tabulka 5.2.

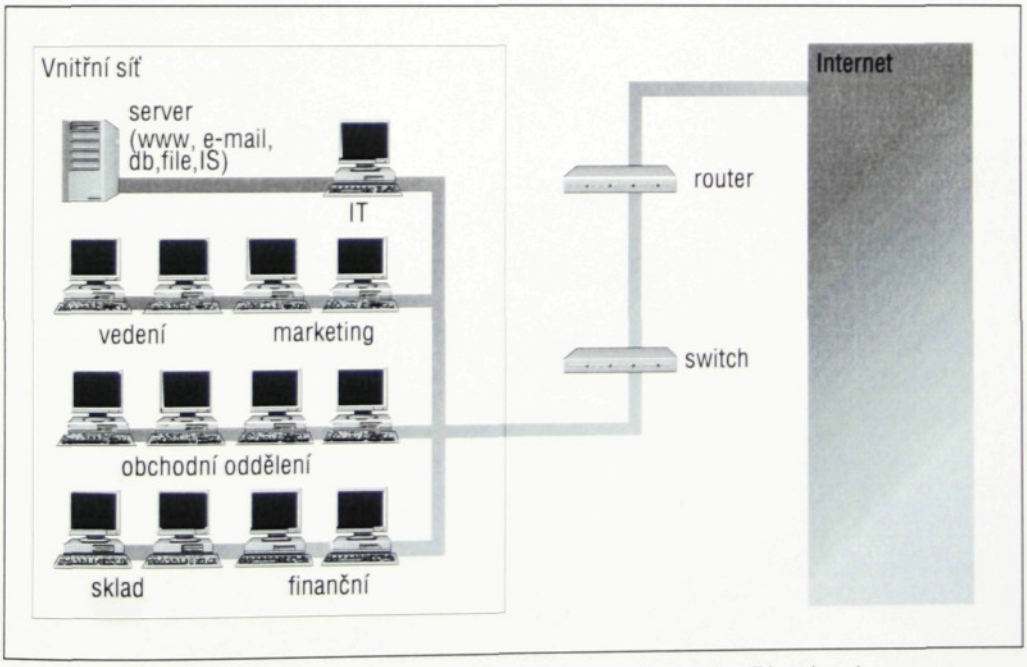
Oddělení	Pozice	Počítač
Vedení společnosti	Ředitel	1
	Asistentka	1
Finanční oddělení	Účetní	2
Marketingové oddělení	Vedoucí	1
	Propagace	1
Obchodní oddělení	Obchodníci + obch. ředitel	5
IT oddělení	Správce sítě	1
Sklad	Skladník	1
Celkem		**13**

Taulka 5. 2 Počet uživatelů a jejich umístění v rámci firmy. Zdroj vlastní.

Strukturu hardwarové části informačního systému v podniku znázorňuje obrázek 5.1.

Softwarové vybavení

V podniku je zaveden software integrovaného informačního systému ABRA, jehož základní část je spuštěna na centrálním serveru. Operačním systémem na serveru je Linux, na stanicích potom MS Windows XP Professional. Na serveru kromě toho běží i e-mailový server (Postfix), je zde umístěn www (Apache) a databázový (MySQL) server s elektronickým obchodem, server zároveň slouží i jako file server (Samba) pro úschovu sdílených dokumentů a programového



Obrázek 5. 1 Schéma hardwarové části informačního systému. Zdroj vlastní.

vybavení. Tato konfigurace bývá v řadě firmách běžně používaná, i když v mnoha případech bývá e-mailový server a server zajišťující elektronický obchod svěřen firmám specializujících se na poskytování hostingových služeb (především u menších firem jako je tato), a to kvůli nutné vysoké konektivitě (propustnosti připojení k síti Internet). Nicméně jsem zvolil tento model, protože na něm lze ilustrovat užití širších možností zabezpečení.

1.2 Netechnické způsoby zabezpečení

V první kapitole této mé diplomové práce jsem uvedl obecné principy ochrany dat, mezi nimi i způsoby organizační a fyzické – tedy ochranu netechnické povahy (z pohledu IT). Při návrhu zabezpečení informačního systému podniku musí být i tyto metody ochrany brány v úvahu. Jedná se o ekonomicky nenáročné, avšak značně účinné způsoby zabezpečení.

1.2.1 Organizační způsoby ochrany

Mezi organizační způsoby, které je vhodné uplatnit pro zvýšení bezpečnosti informačního systému podniku patří především vytvoření provozního řádu pracoviště, pracovních postupů (např. pro zálohování, antivirovou ochranu, incidentu, pro případ kdy PC putuje do opravy apod.) či oddělení pravomocí jednotlivých uživatelů (správce sítě bude mít jiné přístupové právo než např. účetní, ta bude mít zase jiné práva na přístup do systému než skladník apod.) Pro modelovou firmu navrhuji využití těchto organizačních způsobů ochrany:

- provozní řád pracoviště
- oddělit pravomoci uživatelů

1.2.2 Personální způsoby ochrany

Personální způsoby ochrany spočívají převážně v řádném zaškolení pracovníků, kteří přijdou do styku s informačním systémem, a to nejen pro práci se systémem jako takovým, ale i pro celkovou práci s osobním počítačem. Je alarmující, kolik problémů a bezpečnostních rizik (a s tím spojených dodatečných nákladů na jejich odstranění) způsobuje právě neznalost uživatelů.

Nutné je také obeznámit zaměstnance s pravidly pro tvorbu přihlašovacího hesla a vynutit se jejich dodržování, např. odmítnutím příliš jednoduchého hesla, vynucená obměna hesla po určité době apod.

Dobré je také nastavit určité mechanizmy, které by eliminovaly hrozby plynoucí z negativních osobních vlastností zaměstnanců jako je např. nepořádek či neopatrnost. Tyto mechanismy mohou mít formu určitých standardů a vyhlášek ve kterých jsou vymezeny pravidla práce a postihy plynoucí z jejich nedodržování. Ze způsobů personální ochrany navrhuji následující prostředky:

- zaškolení pracovníků na řádnou obsluhu PC a IS
- zaškolení pracovníků o bezpečnosti IS a tvorbě vhodného hesla
- vypracovat normy vymezující pravidla práce

1.2.3 Fyzické způsoby ochrany

Metody fyzické ochrany jsou např. způsoby zabezpečení objektu proti vniknutí – bezpečnostní dveře, nerozbitné sklo, mříže na okna serverovny apod. Jinou otázkou je ochrana proti požáru či povodni – protipožární dveře, hasící systémy, protipožární alarm, pravidla pro elektrické spotřebiče apod. (pořízení prostředků protipožární ochrany je dáno předpisy v rámci kolaudačního řízení a tedy předpokládám i jejich existenci v modelové firmě). Dále jsou to prostředky proti ztrátě napájení – tedy různé záložní zdroje (UPS), ochrany proti přepětí na silovém a datovém vodiči atd. Pro potřeby modelové firmy navrhuji následující způsoby fyzického zabezpečení:

- bezpečnostní dveře do serverovny
- mříže na okna serverovny
- elektronický zabezpečovací systém pro kanceláře
- záložní zdroj pro server

1.3 Technické způsoby zabezpečení

Technickým způsobem zabezpečení pro účely této části mé práce rozumím především zabezpečení podnikové sítě zařízením typu firewall, které je základním prvkem v bezpečnosti sítě, na níž je celý informační systém založen.

1.3.1 Typy firewallů na trhu

Výběr firewallu jako nejdůležitější součásti modelu zabezpečení sítí není jednoduchá záležitost. Kromě funkčního dělení, které jsem uvedl v patřičné kapitole zabývající se problematikou firewallů v praxi existuje i různé formy provedení firewallu. Každé z provedení má svoje výhody i nevýhody. V zásadě existují tři typy firewallů v závislosti na provedení:

- **vestavěné firewally** – tyto firewally jsou vestavěné buďto do směrovače nebo přepínače, v některých případech jsou standardní součástí těchto zařízení, někdy se dodávají jako dodatečný modul do aktivních síťových prvků, které jsou již používány. Protože tyto firewally pracují na IP vrstvě, nejsou schopny uchránit síť od útoků z aplikační vrstvy jako jsou viry, červy nebo trojské koně. V některých případech mohou být vestavěné firewally velmi výkonné, ale obvykle nabízejí méně možností jak ochránit síť.
- **softwarové firewally** – softwarové firewally jsou balíkem, který obsahuje programy, které nabízejí funkčnost firewallů. Tyto programy

Počet uživatelů	RAM	Výkon procesoru	Počet kanceláří	Prostupnost paketového filtru	Cenové rozmezí (Kč)
< 50	< 10 Mb	~ 66 MHz	1	< 10 Mbps	< 15 000,–
51–1000	65 MB	~ 200 MHz	2–299	< 100 Mbps	~150 000,–
1001–5000	128 MB	~ 500 MHz	300	< 200 Mbps	~300 000,–
> 5000	256 MB	~ 500 MHz +	>300	> 200 Mbps	~600 000,–

Tabulka 5.3 Nároky firewallů na hardware v závislosti na výkonu. Zdroj [tyl02]

se instalují nad existující operační systém a hardwarovou platformu. Tento typ firewallů je vhodným řešením především pro malé firmy, které chtějí kombinovat firewall s nějakým existujícím aplikačním serverem (např. www server). Právě díky možnosti kombinovat softwarové firewally na jednom počítači s dalším aplikačním software, jako např. antivirovou ochranou, IDS systémy se zdá být tento typ firewallů vhodný i pro nasazení pro modelový podnik ABC. Softwarové firewally tedy většinou nabízejí vyšší flexibilitu než firewally hardwarové. Někdy je ovšem toto rozhodnutí těžké a hardwarové firewally na druhou stranu nabízejí komplexní řešení, kde je nastavení a spuštění takového firewallu mnohdy mnohem rychlejší než u firewallu softwarového.

- **hardwarové firewally** – u hardwarových firewallů je celý firewall zakomponován do uceleného systému, který zahrnuje jak hardwarovou, tak softwarovou část. Také do některých moderních hardwarových firewallů jsou implementovány funkce jako VPN, IDS, antivirová kontrola atd.

1.3.2 Hardwarové nároky softwarových firewallů

Nároky softwarových firewallů na výkon hardwaru (počítače), na kterém jsou spuštěné závisí především na počtu uživatelů v síti, kterou daný firewall ochraňuje. Tabulka 5.3 nastiňuje problematiku hardwarových nároků v závislosti na výkonu firewallu. Nutno podotknout, že údaje o množství operační paměti RAM jsou údaji potřebnými pouze pro provoz firewallu, pokud jsou na daném počítači spuštěny jiné programy, musí být zohledněny i požadavky těchto aplikací.

1.3.3 Parametry důležité pro rozhodování

Počet uživatelů

Důležitým faktorem při výběru vhodného firewallu je počet uživatelů, které bude daný firewall zabezpečovat. Počet uživatelů, které potřebujeme ochránit určí to, zda budeme potřebovat firewall pro model SOHO nebo firewall typu Enterprise (podnikový), samozřejmě lze použít firewall typu Enterprise i pro zabezpečení

jediného uživatele, je to ovšem značně neekonomické a znamenalo by to i využití služeb, které daná firma nepotřebuje a nikdy nevyužije.

Většina firewallů určených pro segment SOHO dokáže zabezpečit až 50 uživatelů. Při požadavku zabezpečení více uživatelů je doporučeno využít produktů segmentu Enterprise.

Ceny

Ceny firewallů segmentu SOHO začínají zhruba na Kč 1 000,– za jednu licenci pro jednoho uživatele (softwarové firewally) až do zhruba Kč 15 000,– (u hardwarových firewallů).

Firewally pro model Enterprise se pohybují v cenové hladině zhruba od Kč 15 000,– až do Kč 600 000,– a jsou využívány v organizacích, které vyžadují více firewallů, které mohou být řízeny z jedno místa. To znamená, že Enterprise firewally musí mít možnost komunikovat s nějakou centrální správou, většina výrobců uvádí centrální řízení firewallů jako součást své nabídky.

1.3.4 Firewall jako integrace více forem ochrany

V řadě případů firewallů nabízených na trhu se jedná o zařízení kombinující několik způsobů ochrany, tedy základní funkčnost firewallu jako je filtrování paketů, příp. proxy, ale i další jako VPN, IDS nebo antivirovou ochranu. Tuto kombinaci bezpečnostních prvků nabízejí jak firewally softwarové, tak hardwarové.

1.4 Návrh na zabezpečení sítě podniku

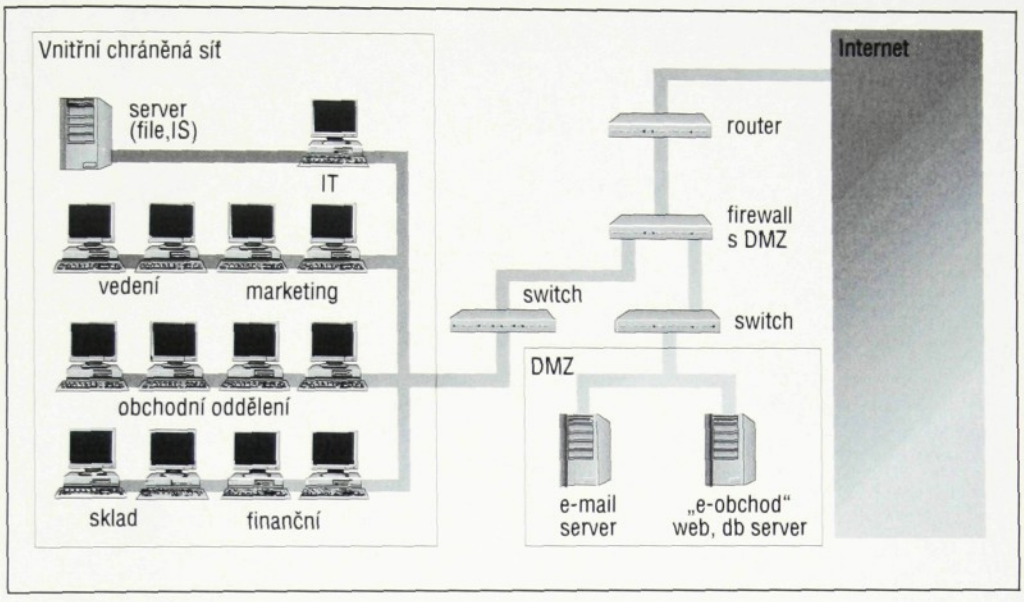
Na základě charakteristik modelové firmy ABC nyní specifikuji požadavky kladené na zabezpečení technické části informačního systému.

1.4.1 Firewall

Zabezpečení počítačové sítě včetně serveru bude provedeno zařízením – firewallem, které bude umístěno před vnitřní síť a server s webovým obchodem bude umístěn v demilitarizované zóně, aby k němu byl veřejný přístup (na rozdíl od vnitřní sítě). Tento firewall musí kromě běžných funkcí jako je filtrování paketů být také schopen vytvořit demilitarizovanou zónu. Další doplňkové služby mohou mít povahu detekce vniknutí nebo filtrování obsahu, výhodou by byla i možnost vytvoření virtuální privátní sítě (např. pro obchodníky na cestách apod.), ovšem není to podmínkou.

1.4.2 Antivirová ochrana

Antivirová ochrana bude zajišťována primárně na stanicích v kombinací s ochranou elektronické pošty na serveru. Na stávající poštovní server by bylo dobré umístit i určitou ochranu proti nevyžádané poště (spamu).



Obr. 5. 2 Návrh zabezpečení síťe modelového podniku. Zdroj vlastní.

1.4.3 Celkový návrh zabezpečení

V návrhu zabezpečení sítě figuruje jako hlavní prvek firewall s podporou demilitarizované zóny. Ten je umístěn mezi síť Internet a vnitřní podnikovou síť. Je také nutné oddělit některé funkce, které doteď spravoval jediný server. Do demilitarizované zóny je vhodné umístit server s podporou elektronického obchodu (www server a databázový server) a další samostatný pro elektronickou poštu. Samostatný poštovní server navrhuji pro zvýšení bezpečnosti – oddělené servery omezují např. nebezpečí průniku kvůli chybě ve skriptech webového obchodu. Server, který zajišťuje IS firmy a file server je vhodné umístit do zabezpečované sítě. Firewall je nastaven tak, že nepropustí žádné nežádoucí pakety do vnitřní sítě.

Je tedy nutné pořídit jak firewall samotný, tak i dva nové servery – jeden do vnitřní sítě a jeden pro e-mailový server. Pro oba účely nicméně bohatě postačí i méně výkonný, např. repasovaný, počítač (jednoduchý file server a software pro integrovaný IS nejsou tak hardwarově náročné jako web server s databázovou aplikací elektronického obchodu). Výkonově dostačující by byly počítače typu Pentium II na frekvenci kolem 400 MHz. Nutno poznamenat, že při stanovování výkonových požadavků u serveru pro elektronický obchod značně záleží na dostupné konektivitě (rychlosti připojení k Internetu), v případě pomalého přístupu stačí i pomalejší stroj. Opět bych zde podotkl, že v reálné situaci by byl elektronický obchod umístěn na server hostingové společnosti právě kvůli vyšší konektivitě. Obrázek 5.2 zachycuje stav podnikové sítě po zavedení všech uvažovaných bezpečnostních prvků.

1.5 Výběr konkrétních produktů

V této části budu konkretizovat obecný model zabezpečení sítě firmy. V první části vyberu vhodný nástroj antivirové ochrany, v druhé pak provedu volbu firewallu, v obou případech uvedu i finanční náročnost řešení, celkové finanční náklady pak vyčíslím v další části.

1.5.1 Volba antivirové ochrany

Jak jsem již uvedl, základní antivirová ochrana bude prováděna na jednotlivých stanicích. Samozřejmostí je správa celého systému antivirové ochrany z jednoho pracoviště – správu bude provádět správce sítě v IT oddělení.

Ochrana stanic a správa

Jako vhodný produkt se jeví program AVG Multilicence, který sdružuje produkty, které představují ucelenou antivirovou ochranu počítačových sítí a umožňuje její vzdálenou správu. Jedná se o ochranu pracovních stanic, ochranu souborových serverů a nástroj pro vzdálenou správu. Licenční model AVG Multilicence zahrnuje i nepřetržitou technickou podporu po dobu dvou let, po kterou je licence platná. Cena této multilicence pro modelovou firmu ABC, která počtem uživatelů spadá do skupiny 11–15 uživatelů je Kč 14 000,–.

Ochrana na poštovním serveru

Ochranu na poštovním serveru je vhodné zvolit od stejného dodavatele, vzhledem k tomu, že server je spuštěn pod operačním systémem Linux, zvolil jsem pro jeho zabezpečení produkt AVG Email Linux Edice. Tato edice je určena pro antivirovou ochranu poštovních serverů na platformě Linux. Součástí edice je i ochrana samotného souborového serveru/stanice, na které poštovní server běží. Cena toho produktu je složena ze dvou složek – složky za počet chráněných poštovních účtů a cena za instalaci na server. Modelová firma se 13 uživateli spadá do rozpětí do 25 uživatelů, kde je cena stanovena na Kč 4 500,–. Cena za instalaci na jeden server je pak Kč 13 500,–.

1.5.2 Výběr firewallu

Prvním vybraným řešením je použití hardwarového firewallu od renomované společnosti 3Com, jedná se o model 3Com OfficeConnect Internet Firewall 100 DMZ. Druhým, alternativním, řešením je pak použití „bastion host" počítače, na kterém bude pod operačním systémem Linux spuštěn software, zajišťující funkce firewallu a dalších požadovaných bezpečnostních služeb. Alternativní řešení udávám především z důvodu nepoměrně nižších nákladů.

3Com OfficeConnect Internet Firewall 100 DMZ

3Com OfficeConnect Internet Firewalls jsou účinné a dostupné produkty k zabezpečení malých sítí připojených k Internetu. Bezpečnostní brány jsou certifikovány agenturou ICSA a chrání zákazníkovu síť před neoprávněným přístupem

hackerů. Kromě toho může být použita i k řízení využití Internetu vnitřními uživateli sítě, včetně možnosti nastavení filtrů na nežádoucí stránky. 3Com OfficeConnect Internet Firewall 100 DMZ je určen pro 100 uživatelů a je osazen portem demilitarizované zóny. OfficeConnect Firewall 100 DMZ lze také upgradovat o podporu virtuálních privátních sítí VPN.

Firewall používá k zabránění průniku hackerů filtrování paketů, zabraňuje výše popsaným útokům DoS: Ping of Death, SYN Flood, Land attack či IP Spoofing, Teardrop nebo Bonk. Firewall dokáže blokovat ActiveX, Java nebo Cookies a tím zabrání hackerům použít je pro útok na systém. Zařízení zapisuje veškeré události do logů a také dokáže identifikovat probíhající útok. Firewall využívá technologie NAT pro překlad síťových adres. Velmi významnou charakteristikou je jednoduchost nastavení a spravování firewallu, vše je přednastaveno a pomocí průvodce lze jednoduše zadat požadované bezpečnostní politiky. Cena firewallu je stanovena na Kč 40 500,–.

Kontrola obsahu – Jako doplněk je možné použít sadu filtrů 3Com OfficeConnect Web Site. Tyto filtry umožňují blokovat přístup na servery se zvolenou tématikou, např. pornografie nebo rasová nesnášenlivost apod. Přístup k těmto serverům lze blokovat, nebo jenom zaznamenávat do logu. 3Com poskytuje na Web Site filter dvanáctiměsíční předplatné, při kterém jsou filtry automaticky každý týden aktualizovány. Produkt je optimalizován především pro co nejjednodušší instalaci a údržbu a podporuje konfiguračního průvodce. 3Com OfficeConnect Internet Firewall je součásti řešení pro malé kanceláře – řady OfficeConnect. Cena tohoto doplňku je Kč 5 300,–.

VPN – Jako další možné rozšíření lze použít OfficeConnect 168VPN Crypto Upgrade, což je software jimž lze OfficeConnect Internet Firewall upgradovat o podporu virtuálních privátních sít. VPN technologie umožňuje bezpečně přenášet soukromá data po veřejné síti – např. Internet. Data jsou mezi oběma body šifrována. OfficeConnect Firewall používá standardní technologii šifrování IPSec a je kompatibilní i s dalšími dodavateli bezpečnostních bran. Součást dodávku upgradu je jedná klientská licence šifrovacího software pro PC. Obecně není nastavení firewallu jednoduché, ale s pomocí průvodce je to možné zvládnout za několik desítek minut. Tento upgrade přijde na Kč 13 400,–.

Při použití dvou serverů v demilitarizované zóně je nutné zakoupit i přepínač nebo hub, cena takovéhoto zařízení se pohybuje kolem Kč 2 000,–

Linux Firewall

Požadované zabezpečení podnikové sítě a elektronického obchodu lze provést s výrazně nižšími náklady pomocí softwarového firewallu, který je spuštěn na linuxovém serveru. Náklady jsou při této variantě především poplatky za instalaci serveru a obecně za práci provedenou specialistou. Software samotný je většinou

typu OpenSource, tedy zdarma (profesionální firewally na bázi Linuxu jsou nabízeny i jako komerční produkty, např. SuSe Linux Firewall či Mandrake Multi Network Firewall, jejich cena je však výrazně vyšší – kolem Kč 60 000,–, ale většinou je v ní zahrnuta i technická podpora).

Cena za instalaci firewallu pro pokrytí potřeb modelové firmy a jeho nastavení by zřejmě nepřekročilo částku Kč 5 000,–, záleží samozřejmě na firmě, která tuto instalaci provede. Nutné by bylo při tomto řešení pořídit i počítač, na kterém by firewall byl spuštěn – opět ale stačí starší repasovaný počítač.

Výhodou je tedy značné ušetření nákladů a větší flexibilita daná softwarovou povahou firewallu. Nevýhodou je pak ve většině případů neexistence technické podpory a především vyšší náročnost na změny v nastavení a správu, vzhledem k velikosti modelového podniku nelze očekávat zaměstnání specialisty, který by se této problematice věnoval.

1.6 Finanční náročnost projektu

V této části práce se budu snažit vyčíslit celkové náklady za zabezpečení informačního systému v modelové firmě. Při stanovování cen jsem vycházel z ceníků daných komodit [CEN01], [CEN02], [CEN03] a [CEN04]. Celkové náklady vyjadřuje tabulka 5.4.

1.7 Zhodnocení

Model zabezpečení, tak jak ho navrhuji představuje pouze jedno z mnoha možných řešení. Při navrhování jsem volil hardwarovou platformu firewallu a to především z důvodu značně nižších nároků na znalosti při správě zařízení a podstatně kratší doby spuštění. V návrhu počítám i s dalšími opatřeními typu bezpečnostních dveří, mříží do oken či elektronickým zabezpečovacím zařízením pro kanceláře – tyto prostředky neslouží jen na zabezpečení informačního systému, ale celkově zabezpečují aktiva organizace. Nutností před spuštěním zabezpečovacího procesu by bylo definování bezpečnostní politiky a její rozpracování do určitých směrnic a bezpečnostních plánů, podle toho by pak následovaly další kroky, které jsem do návrhu zahrnul.

Položka	Částka (Kč)
Náklady personálního zabezpečení	
zaškolení pracovníků na řádnou obsluhu PC a IS (10 × 1000,–) zakázkové školení, cena cca Kč 1 000,– za hod.	10 000,–
Náklady fyzického zabezpečení	
bezpečnostní dveře do serverovny	15 000,–
mříže na okna serverovny	3 000,–
elektronický zabezpečovací systém pro kanceláře	15 000,–
záložní zdroj APC BackUPS 650MI (3 × Kč 3 700,–)	11 000,–
Náklady zabezpečení sítě	
Antivirová ochrana stanic	14 000,–
Antivirová ochrana pošty a serveru	18 000,–
3Com OfficeConnect Internet Firewall 100 DMZ	40 500,–
3Com OfficeConnect Web Site	5 300,–
3COM OfficeConnect Dual Speed Hub 5×10/100Base-TX	2 400,–
Repasované počítače 2 × Dell Optiplex GX 1 á Kč 3 950,– (PII 450Mhz, 128 MB RAM, 6GB HDD)	7 900,–
Celkem	**142 100,–**

Tabulka 5. 4 Celkové náklady na zabezpečení IS podniku. Zdroj vlastní.

Závěr

Obor bezpečnosti informačních systémů a bezpečnosti podnikových sítí proti útokům z vnějšího okolí je oblastí velmi rychle se měnící a rozvíjející. Vývoj a rozšiřování nových technologií, především pak rapidní nárust počtu uživatelů sítě Internet s sebou také nese zvyšující se riziko pro bezpečnost celé organizace. Především s rozvojem elektronického obchodování v jakékoliv formě se stává oblast bezpečnosti naprosto stěžejní a prvořadou záležitostí, které musí každá z firem působících v této oblasti věnovat zvýšenou pozornost. Je nutné se problematice bezpečnosti neustále věnovat a zdokonalovat systémy zabezpečení a jak jsem uvedl v první části mé práce, proces zajišťování bezpečnosti informačního systému je procesem téměř nekončícího cyklu zdokonalování, nasazování a revidování bezpečnostních opatření.

Cílem této práce bylo především postihnout širokou oblast bezpečnosti informačních systémů z pohledu hrozeb a možných útoků ze sítě Internet. Důležitou a dle mého názoru nosnou částí bylo pak vymezení metod ochrany a způsobů obrany, těm jsem také věnoval ve své práci největší prostor. Vlastní návrh zabezpečení, tak jak je uveden v páté kapitole není samozřejmě jediným možným řešením, ale spíše ilustrativním příkladem využití moderních metod ochrany informačních systému v praxi.

Seznam literatury

[DOB98] Dobda L.: Ochrana dat v informačních systémech. Grada Publishing, Praha 1998. ISBN 80-7169-479-7

[CEN01] Ceník bezpečnostních dveří a mříží firmy NEXT. URL: http://www.next.cz/

[CEN02] Ceník komponent PC, Compuco e-shop. URL: http://eshop.compuco.cz

[CEN03] Ceníky antivirových produktů AVG. URL: http://www.grisoft.cz

[CEN04] Ceník repasované výpočetní techniky. Firma Tenzor. URL: http://www.tenzor.cz/pcbazar/

[DOČ00A] Dočkal J.: Bezpečnost počítačové sítě. DSM – Data Security Management č.2/2000.

[DOČ00B] Dočkal J.: DDoS – Distribuovaný útok v Internetu. DSM – Data Security Management č.2/2000.

[DOČ03] Dočekal D.: Internet a bezpečí. Softwarové noviny č. 1/2003.

[DOS00] Dostálek L., Kabelová A.: Velký průvodce protokoly TCP/IP a systémem DNS, 2. aktualizované vydání. Computer Press, Praha 2000. ISBN 80-7226-323-4.

[DOS01] Dostálek L. a kolektiv: Velký průvodce protokoly TCP/IP – Bezpečnost. Computer Press, Praha 2001. ISBN 80-7226-513-X

[DUN01] Dunsmore B., Ballew L. A., Brown J. W., Cross M., Harper J.: Mission Critical Internet Security. Syngress Publishing, Rockland 2001. ISBN 1-928994-20-2

[EDI96] Kolektiv autorů: Elektronický obchod a EDI. UNIS Publishing, Brno 1996.

[EPO02] Kolektiv autorů: Elektronický podpis – přehled právní úpravy, komentář k prováděcí vyhlášce k zákonu o elektronickém podpisu a výklad základních pojmů. Anag, Olomouc 2002. ISBN 80-7263-125-X

[HAN00] Hanáček P., Staudek J.: Bezpečnost informačních systémů – metodická příručka zabezpečování produktů a systémů budovaných na bázi informačních technologií. Úřad pro státní informační systém, Praha 2000.

[HEI01] Heinige K.: Viry a počítače. PC World Edition 13. UNIS Publishing, Brno 2001. ISBN 80-86097-74-9

[HÖN96] Hönigová A., Matyáš V.: Anglicko-česká terminologie bezpečnosti informačních technologií. Computer Press, Praha 1996. ISBN 80-85896-44-3

[HÖN97] Hönigová A. Důvěrnost informací. Computer World. 1997, č. 23.

[CHA98] Chapman D. B., Zwicky E. D.: Firewally – principy budování a udržování. Computer Press, Praha 1998. ISBN 80-7226-051-0.

[KOP01] Kopecký J., Elektronický podpis a certifikační autorita. E-government č. 2/2001.

[KOS98] Kosiur, D.: Elektronická komerce, principy a praxe. Computer Press, Brno 1998.

[KUN03] Kunderová L.: Bezpečnost IS/IT [přednášky]. Brno 2003, Mendelova zemědělská a lesnická univerzita v Brně.

[LÁT96] Látal I. a kolektiv: Ochrana informací, dat a počítačových systémů. Eurounion, Praha 1996. ISBN 80-85858-32-0

[MAR02] Marek R., Dastych J.: Bezpečnostní politika v organizaci. Specializovaná příloha Informační bezpečnost, IT System. 2002, č. 4.

[MAT00] Matyáš V.: K čemu je kryptografie. Informační bezpečnost – katalog 2000-2001. DSM – Data Security Management, NBÚ Praha 2001.

[MUK00] Muknšnábl J.: Denial of Service Attack. Server Reboot.cz 2000. URL: http://www.reboot.cz/light.phtml?clanek=18

[NBU339] Vyhláška Národního bezpečnostního úřadu 339/1999 Sb o objektové bezpečnosti. URL http://www.nbu.cz/legislativa/vyhlaska_339.php.

[NBU56] Vyhláška Národního bezpečnostního úřadu č. 56/1999 Sb. o zajištění bezpečnosti informačních systémů nakládajících s utajovanými skutečnostmi, provádění jejich certifikace a náležitostech certifikátu. URL http://www.nbu.cz/legislativa/vyhlaska_56.php.

[ODV02] Odvárka P.: SSL protokol – principy a přínosy. Server Svět sítí. URL: http://www.svetsiti.cz/technologie.asp?id=127

[OSN94] Kolektiv autor: Manuál pro prevenci a kontrolu počítaové kriminality (United Nations Manual On

The Prevention Of The Computer Crime), OSN, 1994. URL: http://www.uncij.org/documents/eighthcongress.html

[PANO3] Panáček P.: Systémy pro detekci neoprávněného průniku. IT Systems č. 7–8/2003

[PETO1] Peterka J.: Principy firewallu. Softwarové noviny, leden 2001.

[PET92] Peterka J.: Co je čím ... v počítačových sítích. Computerworld č. 31/1992

[PIBO1] Průzkum stavu informační bezpečnosti v R 2001. PriceWaterhouseCoopers, DSM – Data security management, NBÚ, Praha 2001. ISBN 80-902858-3-X

[PIBO3A] Průzkum stavu informační bezpečnosti v ČR 2003. CD z ITsecurity conference 2003 – 5. ročník, Praha 25. září 2003.

[PIBO3B] Seige V, Mikeska L: PSIB '03 aneb v roce 2022 na tom budeme podstatně lépe. DSM – Data Security Management č. 4/2003.

[PUŽ98] Pužmanová R.: Moderní komunikační sítě od A do Z. Computer Press, Praha 1998. ISBN 80-7226-098-7

[RÁDO2] Rádl T.: Nové hrozby vyžadují moderní zabezpečení. IT System č. 4/2002.

[RODOO] Rodryčová D., Staša P.: Bezpečnost informací jako podmínka prosperity firmy. Grada Publishing, Praha 2000. ISBN 80-7169-144-5

[RUSO1] Russel R., Merkow M. S., Walshaw R., Bidwell T., Cross M., Streudler O., Ziese K.: Hack Proofing Your E-Commerce Site. Syngress Publishing, Rockland 2001. ISBN 1-928994-27-X

[ŘÍHO2] Říha P.: Slovník počítačové informatiky – výkladový slovník pro práci s informacemi, hardware a software včetně počítačových sítí, internetu a mobilních technologií. Montanex, Ostrava 2002. ISBN 80-7225-083-3

[TAYO2] Taylor L: How to Choose the Right Enterprise Firewall. Server Datamation, únor 2002. URL http://itmanagement.earthweb.com/secu/article.php/11076_974501_3

[TCP98] Murhammer M. W., Atakan O., Bretz S., Pugh L. R., Suzuki K., Wood D. H.: TCP/IP Tutorial and Technical Overview, sixth edition. IBM 1998.

[TILLO2] Till M:Asymetrická kryptografie v teorii a praxi. 4. 4. 2002. URL http://www.krypta.cz/articles.php?ID=171.

[TULO3] Výzkumný záměr HF TUL: Ekonomické problémy transformace hospodářství ČR s přihlédnutím ke specifikům Euroregionu Nisa. Průzkum KIN: Informační zabezpečení firem v euroregionu Nisa. Liberec 2003.

[ZAK148] Zákon č. 148/1998 Sb. o ochraně utajovaných skutečností a o změně některých zákonů. URL http://www.nbu.cz/legislativa/zakon.php

[ZEPO0] Zákon č. 227/2000 Sb o elektronickém podpisu.
URL http://business.center.cz/business/pravo/zakony/epodpis/
[ŽEM03] Žemlička M.: Hesla: nejlevnější, nejpoužívanější, ale určitě ne nejspolehlivější. Softwarové noviny č. 1/2003.

Přílohy

3Com OfficeConnect Internet Firewalls – přehled firewallů společnosti 3Com (4 strany)

3Com OfficeConnect Internet Firewall data sheet – dokumentace vybraného firewallu (4 strany)

3Com® OfficeConnect®
Internet Firewalls

The affordable way to protect your network from Internet hackers.

Internet Firewall with Alert LED, standard Ethernet connections and DMZ*.

Key Benefits

Protect your network.
Keep hackers out of your network while allowing Internet access to everyone in the office.

Control Internet use.
Block inappropriate material, determine which sites your staff can access, and log usage.

Share a single IP address.
All users on the network can be connected to the Internet through one IP address. This saves money by eliminating the need for multiple IP addresses from your service provider.

Affordable. Effective and secure firewall protection using technology similar to that used in systems employed by large organizations but at a fraction of the cost.

Easy to install and use.
OfficeConnect® Internet Firewalls use standard Ethernet connections and can be customized using a simple web-based interface, so little or no in-house expertise is required.

ICSA certified. Approved as effective firewall protection by the worldwide independent authority on Internet security.

Part of the award-winning OfficeConnect family.
As business requirements change, add other functions such as high-speed networking, Internet access, remote access, or print-sharing capabilities.

The OfficeConnect® Internet Firewalls are the affordable, effective way for small businesses to secure their networks. Hacker attack is a real risk and more common than many business people realize. If you have an Internet connection, hackers may get into your computers from anywhere in the world. Some want to steal data. Others spread havoc at random - using software easily available on the Internet to damage and destroy networks and information. It can pose a serious threat to your business.

In the past, robust high specification firewall protection was expensive, complex and required specialized in-house IT administration. Now you can have secure protection for a fraction of the cost and complexity. OfficeConnect® Internet Firewalls are easy to install and configure. They keep the hackers out and can also control Internet usage from your LAN. You can prevent access to inappropriate material, keep a log of which sites are being accessed most frequently and analyze how much bandwidth your Internet connection is using. Your entire office can share a single IP address from your Internet Service Provider (ISP) saving you money, and possibly removing the need for a specialized router.

3Com OfficeConnect® Internet Firewalls are a core part of the OfficeConnect family of products, providing small businesses with the power to share information, connect remote locations, and access the Internet. Delivering the advantages of networking to small businesses, the market-leading OfficeConnect system can help small businesses streamline operations, effectively manage costly resources, and increase communication within and between offices.

*DMZ port on Internet Firewall DMZ model only.

Internet Firewalls

Internet Security for small businesses

The OfficeConnect® Internet Firewall family

The two OfficeConnect® Internet Firewalls offer affordable Internet security for your Local Area Network (LAN) by denying unauthorized access and preventing Denial of Service (DoS) hacker attacks. Also, inappropriate Internet access from the LAN can be controlled by entering specific URLs or keywords. The Web Site Filter extends this capability by providing the Internet Firewalls with an automatically updated list of thousands of controlled sites according to pre-defined categories, such as pornography or racial intolerance.

OfficeConnect® Internet Firewall 25 provides Internet security for up to 25 users.

OfficeConnect® Internet Firewall DMZ provides Internet security for up to 100 users. It also features a De-Militarized Zone (DMZ) port. This is an additional port for connecting publicly accessible servers such as a web server. The DMZ port is protected from DoS hacker attacks, but can be accessed by external Internet users. A DMZ port enables customers to access your site without exposing your network to attack. It is essential if you trade using e-commerce or plan to in the future.

OfficeConnect Web Site Filter* provides Internet Firewalls with extended capabilities to control Internet access. You specify the categories of material and the Web Site Filter provides a list of thousands of controlled sites - and automatically updates it every week. Access to the sites can either be blocked or logged. The Web Site Filter is provided as a 12-month subscription. Both Internet Firewalls come with a free one-month trial.

Firewall security, logging and alerts
The firewalls use secure stateful packet inspection technology to deny unauthorized access to your LAN from the Internet and prevent DoS hacker attacks, including Ping of Death, SYN Flood, LAND Attack, IP Spoofing, Teardrop and Bonk. Hackers may try to use Java, ActiveX and Cookie technologies to attack networks, so the Internet Firewalls can either block these applications or allow them only from trusted sites. User Remote Access to the LAN is controlled by user name and password authentication. All events can be logged, and major security concerns can be flagged with an instant and automatic e-mail alert. The Internet Firewalls also feature an alert LED to show if a hacker attack is taking place or an attempt to access a blocked site is being made.

ICSA certified
The OfficeConnect Internet Firewalls are approved as effective firewall protection by the worldwide independent authority on Internet security.

Internet Filtering
Access to web sites can be controlled from, or restricted to particular web sites that you specify and type in. The Internet Firewalls can track the 25 most accessed sites and 25 top users of bandwidth. They can also log or block access to web sites containing specified keywords in the URL. The Web Site Filter extends these filtering capabilities to automatically control access to thousands of web sites matching chosen categories.

Share Internet access
The use of Network Address Translation (NAT) allows multiple LAN users to share a single IP address from an ISP. This means multiple users can access the Internet using an Ethernet modem (e.g. OfficeConnect Dual-Mode Cable Modem) and low-cost Internet account.

Easy to install and configure
Installation and configuration is simple. The equipment has been designed for use by small businesses with little or no in-house IT expertise. The Internet Firewalls fit between an Ethernet hub or switch and the modem or router using standard Ethernet connections. They come pre-configured and can be customized using a simple web-based interface and accessed with a web browser.

*The 3Com OfficeConnect Web Site Filter uses the CyberNOT™ list, which is licensed from The Learning Company. This list is developed and maintained by the The Learning Company's Cyber Patrol unit.

Office Connect Family

The 3Com OfficeConnect family is an integrated networking system, allowing small businesses to share computer resources, access the Internet, and connect remote locations or users.

OfficeConnect products include:

LAN Connectivity
Network interface cards
Hubs and switches
Networking kits
HP JetDirect print server

Remote Access and Internet Connectivity
Modems
LAN Modems
Routers
Internet firewalls

The OfficeConnect family offers a simple, reliable, and affordable solution for today's information-sharing needs.

Figure 1 shows a typical configuration for the OfficeConnect® Internet Firewall DMZ. The Firewall 25 product uses the same configuration but without the DMZ port.

Figure 1
OfficeConnect Internet Firewall DMZ
Typical Configuration

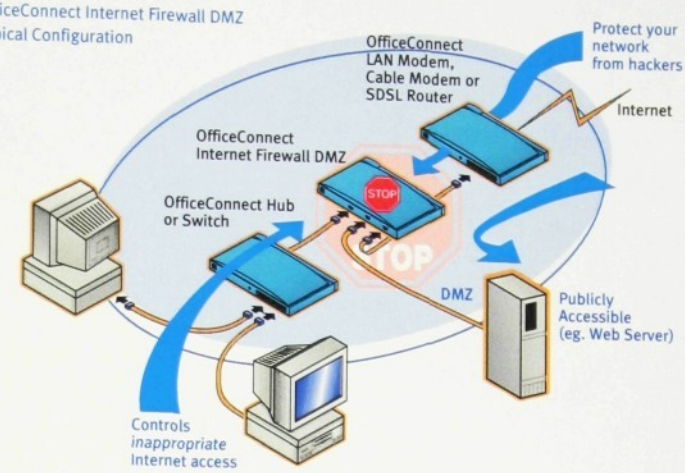


Figure 2. The optional OfficeConnect Web Site Filter controls access for 12 months to many thousands of web sites matching the chosen categories. Automatic weekly updates let you keep pace with the ever-changing Internet.

Figure 2
OfficeConnect Web Site Filter
Typical Configuration

OfficeConnect Internet Firewalls Features and Benefits

Firewall Security
Stateful packet inspection. Prevents unauthorized access and thwarts Denial of Service (DoS) attacks.
Remote Access Authentication. Allows users to access their private LAN via the Internet.
ICSA Certified. Approved by the worldwide authority in independent security services.
Security Alerts. Instant e-mail alerts and visual LED indication of major security concerns

Internet Filtering
Flexibility. Filtering can be customized on specified URLs and/or keywords.
Tracking. Logs 25 most accessed sites and 25 top users of bandwidth.
Web Site Filter (optional). Automatically controls access to thousands of web sites

Ease of use
Standard Ethernet connections and cabling. Allows simple connection to the network.
Web-based management interface. Simple unit configuration via a web browser.
NAT. Network Address Translation allows LAN users to share a single public IP address.
DHCP Server and Client. Dynamic Host Configuration Protocol supplies network addresses to computers automatically, simplifying configuration and management of the network.

Performance
10Mbps Ethernet LAN port. Higher transfer speeds than even the fastest Internet access technologies. Ensures the Internet Firewall will not be a bottleneck.

Compatibility
OS independent. Supports all TCP/IP network operating systems including Windows 95, Windows 98, Windows for Workgroups, Windows NT, UNIX and Mac OS (7.5.3 and above).

Reliability
Peace of mind. OfficeConnect® Internet Firewalls are backed by 3Com's telephone support and Lifetime Limited Warranty*.

* Not applicable to OfficeConnect Web Site Filter.

m®OfficeConnect®

OfficeConnect Internet Firewall 25
OfficeConnect Internet Firewall DMZ

3Com®

More connected.™

Specifications

OfficeConnect Internet Firewall 25

OfficeConnect Internet Firewall DMZ

Dimensions & Weight

Width: 220mm (8.7in); Height: 54.6mm (2.1in); Depth 185.4mm (7.3in); Weight: 870g (1.9lb)

Protocol Support

TCP/IP; DHCP;

Network address translator (RFC 1631) TCP/IP

Connectors

OfficeConnect Internet Firewall 25: Two 10BASE-T, RJ45 ports. LAN Port is Uplink/Normal selectable.

OfficeConnect Internet Firewall DMZ: Three 10BASE-T, RJ45 ports. LAN Port and DMZ port are Uplink/Normal selectable.

LED Indicators

Power; Alert; Link (per port); Transmit (per port); Receive (per port).

Power: 11VA

Standards Compliance

Functional: ISO 8802/3; IEEE 802.3

EMC: EN55022 Class B†; EN50082-1; FCC Part 15 Class B; ICES-003 Class B; VCCI Class B; AS/NZS 3548 Class B; CISPR 22 Class B

† Screened (shielded) cables must be used to ensure compliance with these standards.

Environmental: EN 60068 (IEC 68)

Safety: UL 1950; EN 60950; CSA 22.2 #950; IEC 950

Package Contents

OfficeConnect Internet Firewall 25 or Internet Firewall DMZ.

User Guide

Power adapter, one-piece clipping system, and rubber feet.

CD-ROM containing Companion Programs for the Internet Firewalls.

OfficeConnect Web Site Filter for Internet Firewalls

The OfficeConnect Web Site Filter will provide Internet filtering from inappropriate web sites* for 12 months, with weekly updates, after which time it will expire.The OfficeConnect Web Site Filter can only be used with an OfficeConnect Internet Firewall 25 or Internet Firewall DMZ.

Package Contents

User Manual with activation key to receive Web Site Filter and weekly updates.

System Requirements

An Internet access device - a modem or router - with 10BASE-T or 10/100BASE-TX Ethernet connection. Examples include 3Com's OfficeConnect ISDN LAN Modem, OfficeConnect 56K LAN Modem, OfficeConnect Remote 511 and 531 Access Routers, OfficeConnect Dual Mode Cable Modem, OfficeConnect Remote 840 SDSL Router.

An Internet connection provided by an Internet service provider.

A category 3 or 5 (data grade) twisted pair cable (up to 100m [328ft] long) to connect WAN port to Internet access device, LAN port to an Ethernet 10Mbps or 10/100Mbps hub or switch, and DMZ port to a server or Ethernet 10Mbps or 10/100Mbps hub or switch.

TCP/IP network operating system software. 3Com's OfficeConnect Internet Firewalls protect all networks running TCP/IP network operating systems software, including Windows 95, Windows 98, Windows NT, UNIX or Mac OS (7.5.3 and above).

At least one computer with Windows 95, Windows 98, or Windows NT and a CD-ROM drive is recommended, but not required

Warranty Summary

The OfficeConnect Internet Firewall 25 and Internet Firewall DMZ are covered by a lifetime warranty; the power adapter is also included in this warranty. To qualify for the warranty, you must submit a registration card. Advance hardware exchange is available during the first year; thereafter return the product to 3Com for repair.

The lifetime warranty is not offered where restricted or prohibited by law.

The OfficeConnect Internet Firewall 25 and Internet Firewall DMZ are covered by 90-day telephone support.

Ordering Information

OfficeConnect Internet Firewall 25	3C16770
OfficeConnect Internet Firewall DMZ	3C16771
OfficeConnect Web Site Filter	3C16772

OfficeConnect products

For more information please refer to the following publications:

OfficeConnect Fast Ethernet PCI NIC data sheet	400440-002
OfficeConnect 10/100 LAN PC Card data sheet	400509-001
OfficeConnect Hubs and Switches data sheet	400317-008
HP JetDirect 170X OfficeConnect External Print Server data sheet	400484-002
HP JetDirect 300X OfficeConnect Print Server data sheet	400427-002
OfficeConnect ISDN LAN Modem data sheet	400396-005
OfficeConnect 56K LAN Modem** data sheet	400397-003
OfficeConnect 56K Business Modem data sheet	400473-002
OfficeConnect Dual Mode Cable Modem data sheet	400510-001
OfficeConnect Fast Ethernet Networking Kit data sheet	400412-003
OfficeConnect Remote 511 and 531 Access Routers data sheet	400318-003
OfficeConnect Remote 840 SDSL Router data sheet	400508-001

**Available in North America only.
*The 3Com OfficeConnect Web Site Filter uses the CyberNOT™ list, which is licensed from The Learning Company. This list is developed and maintained by the The Learning Company's Cyber Patrol unit.
www.cyberpatrol.com

YEAR 2000 COMPLIANT

3Com warrants that this product will continue performing properly with regard to date sensitive data after January 1, 2000, provided that all other products used in connection or combination with this product, including hardware, software, and firmware, accurately exchange data sensitive data with this product. If it appears that this product does not perform properly with regard to date sensitive data after January 1, 2000, the customer may notify 3Com before April 1, 2000 or 90 days after shipment of this product by 3Com or its authorized reseller, whichever is later.

3Com shall, at its option and expense, provide a software update, product repair or product replacement, which would provide the proper performance. Any software update, replaced or repaired product will carry a Year 2000 Limited Warranty for 90 days or until April 1, 2000, whichever is later. This warranty excludes third party and Connections software CD-ROM. See http://www.3com.com/products/yr2000.html for more information.

3Com Corporation
5400 Bayfront Plaza
P.O. Box 58145
Santa Clara, CA 95052-8145
Phone: 1 800 NET 3Com
or 1 408 326 5000
Fax: 1 408 326 5001
World Wide Web:
www.3com.com

To learn more about 3Com products and services, visit our World Wide Web site at www.3com.com. 3Com is a publicly traded corporation (Nasdaq:COMS).

Printed in the U.K

400526-001 9/99

3com

DATA SHEET

3Com® OfficeConnect® Internet Firewall

Key Benefits

Easy to install and use
3Com OfficeConnect® Internet Firewalls use standard Ethernet connections and can be customized using a simple web-based interface, so little or no in-house expertise is required.

Control Internet use
Block inappropriate material, determine which sites that staff can access, and log usage.

ICSA Certified
Approved as effective firewall protection by the worldwide independent authority on Internet security.

Affordable
Effective and secure firewall protection using technology similar to that used in systems employed by large organizations, but at a fraction of the cost.

Protect your network
Keep hackers out of the network while allowing Internet access for everyone in the office.

Share a single connection and IP address
All users on the network can be connected to the Internet through one connection using one IP address. This saves money by eliminating the need to purchase multiple lines and IP addresses from your service provider.

Secure private connections across the Internet
By installing the optional Virtual Private Network (VPN) upgrade, save on costly leased lines or inter-office remote access communications by using standard IPsec to encrypt data sent over the public network.

The affordable way to protect the network from Internet hackers.

The OfficeConnect Internet Firewalls are the affordable, effective way for small businesses to secure their networks. Hacker attack is a real risk and more common than many people realize. Hackers from around the world can hack into computers with an Internet connection. Some want to steal data. Others spread havoc at random - using software easily available on the Internet to damage and destroy networks and information. Today, hacking is a serious threat to many organizations.

In the past, robust high specification firewall protection was expensive, complex, and required specialized in-house IT administration. Now secure protection is available for a fraction of the cost and complexity.

OfficeConnect Internet Firewalls are easy to install and configure. They keep hackers out and can also control Internet usage from the LAN. You can prevent access to inappropriate material, keep a log of which sites are being accessed most frequently and analyze how much bandwidth your Internet connection is using. An entire office can share a single IP address from an Internet Service Provider (ISP) saving money, and possibly removing the need for a specialized router.

3Com OfficeConnect Internet Firewalls are a core part of the OfficeConnect family of products, providing small businesses with the power to share information, connect remote locations, and access the Internet.

The 3Com OfficeConnect Internet Firewall family

Share Internet access
The use of Network Address Translation (NAT) allows multiple LAN users to share a single IP address from an ISP. This means multiple users can access the Internet using any modem or router with an Ethernet connection and low-cost Internet account.

3Com OfficeConnect Internet Firewall family
The OfficeConnect Internet Firewall 25 provides Internet security for up to 25 users; and the OfficeConnect Internet Firewall DMZ supports up to 100 users and features a De-Militarized Zone (DMZ) port. This is an additional port for connecting publicly accessible servers such as a web server. The DMZ port is protected from Denial of Service (DoS) hacker attacks, but can be accessed by external Internet users without exposing the network to attack. This functionality is essential for organizations considering e-commerce activity.

VPN upgrade
Through the purchase of this one-time upgrade, any OfficeConnect Internet Firewall can initiate and terminate up to five simultaneous secure IPsec VPN tunnels. This technology allows straight-forward office-to-office or remote access communication over the Internet, saving costs while enhancing productivity.

Internet Access Filtering
Allows you to deny access to certain web sites or allow access only to those sites you specify. The Internet Firewalls can track the most accessed sites and the top users of bandwidth. They can also log or block access to web sites containing specified keywords in the URL.

3Com OfficeConnect Web Site Filter*
This provides Internet Firewalls with extended capabilities to control Internet access. Specify the categories of material and the Web Site Filter provides a list of thousands of controlled sites - and automatically updates it every week. Access to the sites can either be blocked or logged. The Web Site Filter is provided as a 12-month subscription. Both Internet Firewalls come with a free one-month trial.

Firewall security, logging, and alerts
The firewalls use secure Stateful Packet Inspection technology to deny unauthorized access to the LAN and prevent Denial of Service (DoS) and hacker attacks, including Ping of Death, SYN Flood, LAND Attack, IP Spoofing, Teardrop, and Bonk. Hackers may try to use Java, ActiveX, and Cookie technologies to attack networks, so the Internet Firewalls can either block these applications or allow them only from trusted sites. All events can be logged, and major security concerns can be flagged with an instant and automatic e-mail alert.

3Com OfficeConnect Internet Firewall Typical Configuration

Figure 1 shows a typical configuration for the 3Com OfficeConnect Internet Firewall DMZ. The 3Com OfficeConnect Firewall 25 product uses the same configuration but without the DMZ port.

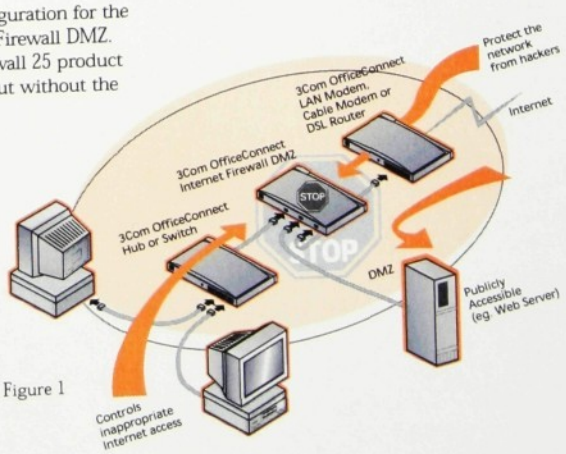


Figure 1

*The 3Com OfficeConnect Web Site Filter uses the CyberNOT™ list, which is licensed from The Learning Company. This list is developed and maintained by the The Learning Company's Cyber Patrol unit.

3Com OfficeConnect Internet Firewall Features and Benefits

ICSA Certified
3Com OfficeConnect Internet Firewalls are approved as effective firewall protection by the worldwide independent authority on Internet security.

Feature	Benefit
Firewall Security	
Stateful Packet Inspection	Prevents unauthorized access and thwarts Denial of Service (DoS) attacks.
ICSA Certified	Approved by the worldwide authority in independent security services.
Security Alerts	Instant e-mail alerts and visual LED indication of major security concerns.
Remote Access Authentication	Allows users to access their private LAN via the Internet.
Internet Filtering	
Flexibility	Filtering can be customized on specified URLs and / or keywords.
Tracking	Logs 25 most accessed sites and 25 top users of bandwidth.
Web Site Filter (optional)	Automatically controls access to thousands of web sites.
Ease of use	
Getting Started Wizard	Intuitive, user-friendly tool that makes installation quick and easy.
Web-based management interface	Simple unit configuration via a web browser.
Network Address Translation (NAT)	Allows LAN users to share a single public IP address.
DHCP Server and Client	Dynamic Host Configuration Protocol supplies network addresses to computers automatically, simplifying configuration and management of the network.
Standard Ethernet connections and cabling	Allows simple connection to the network.
Performance	
10Mbps Ethernet LAN port	Higher transfer speeds than even the fastest Internet access technologies. Ensures the Internet Firewall will not be a bottleneck.
Compatibility	
OS independent	Supports all TCP/IP network operating systems including Windows 95, Windows 98, Windows for Workgroups, Windows NT, Windows 2000, UNIX, and Mac OS (7.5.3 and above).
Reliability	
OfficeConnect Internet Firewalls are backed by 3Com's telephone support and Lifetime Limited Warranty*	Peace of mind.
VPN	
Standards-based IPSec VPN (optional)	Allows secure transmission of private data over the Internet using encryption without the cost of leased lines.
ARC4, DES and 3DES encryption	56-bit or 168-bit encryption ensures data security and compatibility with most IPSec VPN terminators.

* Not applicable to OfficeConnect Web Site Filter.

Specifications

Dimensions & Weight
Width: 228mm (9.12in);
Height: 54mm (2.1in);
Depth 185mm (7.3in);
Weight: 870g (1.9lb)

Protocol Support
TCP/IP; DHCP;
Network address translator
(RFC 1631) TCP/IP
IPSec

Connectors
OfficeConnect Internet
Firewall 25:
Two 10BASE-T, RJ45 ports. LAN Port is Uplink/Normal selectable.

OfficeConnect Internet
Firewall DMZ:
Three 10BASE-T, RJ45 ports. LAN Port and DMZ port are Uplink/Normal selectable.

LED Indicators
Power; Alert; Link (per port);
Transmit (per port);
Receive (per port).
Power: 11VA

Standards Compliance
Functional: ISO 8802/3;
IEEE 802.3

EMC: EN55022 Class B†;
EN50082-1; FCC Part 15 Class B;
ICES-003 Class B; VCCI Class B;
AS/NZS 3548 Class B; CISPR 22
Class B

† Screened (shielded) cables must be used to ensure compliance with these standards.

Environmental: EN 60068 (IEC 68)

Safety: UL 1950; EN 60950; CSA
22.2 #950; IEC 950

Package Contents
OfficeConnect Internet Firewall 25 or Internet Firewall DMZ.

User Guide

Power adapter, one-piece clipping system, and rubber feet.

CD-ROM containing Companion Programs for the Internet Firewalls.

Quick Start Guide

Ethernet Cables

OfficeConnect Web Site Filter for Internet Firewalls
The OfficeConnect Web Site Filter will provide Internet filtering from inappropriate web sites* for 12 months, with weekly updates, after which time it will expire. The OfficeConnect Web Site Filter can only be used with an OfficeConnect Internet Firewall 25 or Internet Firewall DMZ.

Package Contents
User Manual with activation key to receive Web Site Filter and weekly updates.

VPN Upgrade
Enables secure transmission of private traffic over the Internet through encrypted tunnels.

Package Contents
User Manual with activation key to enable VPN capabilities. CD containing a VPN client.

System Requirements
An Internet access device - a modem or router - with 10BASE-T or 10/100BASE-TX Ethernet connection. Examples include the 3Com OfficeConnect ISDN LAN Modem, OfficeConnect 56K LAN Modem, and OfficeConnect Remote 812 ADSL Router, and OfficeConnect Remote 612 ADSL Router.

An Internet connection provided by an Internet service provider.

A Category 3 or 5 (data grade) twisted pair cable (up to 100m [328ft] long) to connect WAN port to Internet access device, LAN port to an Ethernet 10Mbps or 10/100Mbps hub or switch, and DMZ port to a server or Ethernet 10Mbps or 10/100Mbps hub or switch.

TCP/IP network operating system software. The 3Com OfficeConnect Internet Firewalls protect all networks running TCP/IP network operating systems software, including Windows 95, Windows 98, Windows NT, Windows 2000, UNIX, or Mac OS (7.5.3 and above).

At least one computer with Windows 95, Windows 98, Windows NT, Windows 2000, and a CD-ROM drive is recommended, but not essential.

Warranty Summary
The OfficeConnect Internet Firewall 25 and Internet Firewall DMZ are covered by a lifetime limited warranty; the power adapter is also included in this warranty. To qualify for the warranty, you must submit a registration card or register on-line at the 3Com web site (http://support.3com.com).

The lifetime limited warranty is not offered where restricted or prohibited by law.

The OfficeConnect Internet Firewall 25 and Internet Firewall DMZ are covered by free 90-day telephone support.

**Limited geographical availability.
*The 3Com OfficeConnect Web Site Filter uses the CyberNOT™ list, which is licensed from The Learning Company. This list is developed and maintained by the The Learning Company's Cyber Patrol unit.

Ordering Information

3Com OfficeConnect Internet Firewall 25	3C16770
3Com OfficeConnect Internet Firewall DMZ	3C16771
3Com OfficeConnect Web Site Filter	3C16772
3Com OfficeConnect VPN Upgrade for Internet Firewall	3CR16773-93

3Com Corporation, Corporate Headquarters, 5400 Bayfront Plaza, P.O. Box 58145, Santa Clara, CA 95052-8145.

To learn more about 3Com solutions, visit www.3com.com. 3Com Corporation is publicly traded on Nasdaq under the symbol COMS.

400526-004 01/0

3com