Zabezpečení lokálních sítí a správa dat

Network security and data management

Jan Pich

Bakalářská práce
2010

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky

Univerzita Tomáše Bati ve Zlíně
Fakulta aplikované informatiky
akademický rok: 2009/2010

ZADÁNÍ BAKALÁŘSKÉ PRÁCE

(PROJEKTU, UMĚLECKÉHO DÍLA, UMĚLECKÉHO VÝKONU)

Jméno a příjmení:	**Jan PICH**
Studijní program:	**B 3902 Inženýrská informatika**
Studijní obor:	**Bezpečnostní technologie, systémy a management**
Téma práce:	**Zabezpečení lokálních sítí a správa dat**

Zásady pro vypracování:

1. **Vypracujte kritickou literární rešerši na dané téma.**
2. **Popište možnosti zabezpečení LAN proti útoku zvenčí, zabezpečení vzdálených přístupů a vzdáleného řízení PC.**
3. **Rozeberte možnosti správy a přístupových práv uživatelů do sítě, možnosti zálohování a ochrany datových souborů.**
4. **Navrhněte praktický příklad řešení zabezpečení sítě u firmy (výběr vhodných prostředků, cenová kalkulace).**

Pozn.: Zvažujte použití metod zabezpečení v prostředí Windows.

Rozsah práce:

Rozsah příloh:

Forma zpracování bakalářské práce: **tištěná/elektronická**

Seznam odborné literatury:

1. **Ludvík M., Štědroň B.:Teorie bezpečnosti počítačových sítí, Computer Media 2008**
2. **Merhaut F., Zelinka I.: Počítačové viry a bezpečnost,UTB Zlín, 2008**
3. **Endorf. C, Schultz E., Mellander J.: Hacking detekce a prevence počítačového útoku, Grada 2007**
4. **Horák J.: Bezpečnost malých počítačových sítí, Grada 2006**
5. **Grygar J.: Detekce a prevence počítačových útoků,diplomová práce,UTB Zlín, 2007**

Vedoucí bakalářské práce: **Ing. Milan Navrátil, Ph.D.**
Ústav elektroniky a měření

Datum zadání bakalářské práce: **19. února 2010**

Termín odevzdání bakalářské práce: **19. května 2010**

Ve Zlíně dne 19. února 2010

UNIVERZITA TOMÁŠE BATI VE ZLÍNĚ
Fakulta aplikované informatiky
L.S.

prof. Ing. Vladimír Vašek, CSc.
děkan

doc. Mgr. Milan Adámek, Ph.D.
ředitel ústavu

ABSTRAKT

Tato práce se zabývá možnostmi zabezpečení lokálních sítí s operačním systémem Windows. Nejprve se čtenář dozví možnosti vzdáleného řízení PC, vzdáleného připojení do sítě a zabezpečení těchto přístupů. Dále je rozebráno zabezpečení sítě a PC proti neoprávněným vzdáleným přístupům. Nechybí ani správa datových souborů, jejich ochrana před napadením těchto dat infiltrací, či přímo před samotným uživatelem. Okrajově je v práci zmíněna i správa uživatelů v síti – jejich účty a možnosti přístupu do nich. V praktické části je znázorněn praktický návrh sítě spolu s bezpečnostními prvky. Nechybí ani cenová kalkulace takového systému.

Klíčová slova: PC, zabezpečení, LAN, Windows, Firewall, data, uživatel.

ABSTRACT

This work deals with the possibilities of network security on Windows system. Firstly, the reader learns about the ability to remotely control a PC, remote connections to the network and the security of these approaches. Furthermore, the security of the network and PC against unauthorized remote approaches is described. There is also discussed management of data files, their protection against attacks and infiltrations or directly against the user. Marginally, user management of the network is mentioned as well as their accounts and access to them. The practical part shows the real network design with safety features including their price calculation.

Keywords: PC, security, LAN, Windows Firewall, data, user

Tímto bych chtěl poděkovat vedoucímu mé bakalářské práce Ing. Milanu Navrátilovi, Ph.D. za odborné znalosti, rady a věcné připomínky, které mi poskytoval během tvorby práce. Dále mé poděkování patří Ing. Ivo Machálkovi za odborné konzultace a informace z praxe daného tématu.

Prohlašuji, že

- beru na vědomí, že odevzdáním bakalářské práce souhlasím se zveřejněním své práce podle zákona č. 111/1998 Sb. o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách), ve znění pozdějších právních předpisů, bez ohledu na výsledek obhajoby;
- beru na vědomí, že bakalářská práce bude uložena v elektronické podobě v univerzitním informačním systému dostupná k prezenčnímu nahlédnutí, že jeden výtisk bakalářské práce bude uložen v příruční knihovně Fakulty aplikované informatiky Univerzity Tomáše Bati ve Zlíně a jeden výtisk bude uložen u vedoucího práce;
- byl/a jsem seznámen/a s tím, že na moji bakalářskou práci se plně vztahuje zákon č. 121/2000 Sb. o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších právních předpisů, zejm. § 35 odst. 3;
- beru na vědomí, že podle § 60 odst. 1 autorského zákona má UTB ve Zlíně právo na uzavření licenční smlouvy o užití školního díla v rozsahu § 12 odst. 4 autorského zákona;
- beru na vědomí, že podle § 60 odst. 2 a 3 autorského zákona mohu užít své dílo – bakalářskou práci nebo poskytnout licenci k jejímu využití jen s předchozím písemným souhlasem Univerzity Tomáše Bati ve Zlíně, která je oprávněna v takovém případě ode mne požadovat přiměřený příspěvek na úhradu nákladů, které byly Univerzitou Tomáše Bati ve Zlíně na vytvoření díla vynaloženy (až do jejich skutečné výše);
- beru na vědomí, že pokud bylo k vypracování bakalářské práce využito softwaru poskytnutého Univerzitou Tomáše Bati ve Zlíně nebo jinými subjekty pouze ke studijním a výzkumným účelům (tedy pouze k nekomerčnímu využití), nelze výsledky bakalářské práce využít ke komerčním účelům;
- beru na vědomí, že pokud je výstupem bakalářské práce jakýkoliv softwarový produkt, považují se za součást práce rovněž i zdrojové kódy, popř. soubory, ze kterých se projekt skládá. Neodevzdání této součásti může být důvodem k neobhájení práce.

Prohlašuji,

- že jsem na bakalářské práci pracoval samostatně a použitou literaturu jsem citoval. V případě publikace výsledků budu uveden jako spoluautor.
- že odevzdaná verze bakalářské práce a verze elektronická nahraná do IS/STAG jsou totožné.

Ve Zlíně …….……

podpis diplomanta

OBSAH

ÚVOD

Počítačová síť vzniká při propojení dvou a více počítačů. Jejím hlavním úkolem je přenos informací (paketů) z jednoho počítače do druhého. V dnešní době mají informace rozdílné hodnoty. Záleží na konkrétní situaci, kdy se hodnotí přínos informace, počet lidí, které danou informaci znají. Sítě se skládají z prvků aktivních a pasivních. Správná volba těchto prvků může napomoci k lepší bezpečnosti přenosu. Případný pachatel není omezen pouze naslouchání přenášené informace, ale má možnost tyto informace číst a měnit přímo na počítači, který nemusí být nutně součástí nějaké sítě.

Hlavní úkoly sítě:

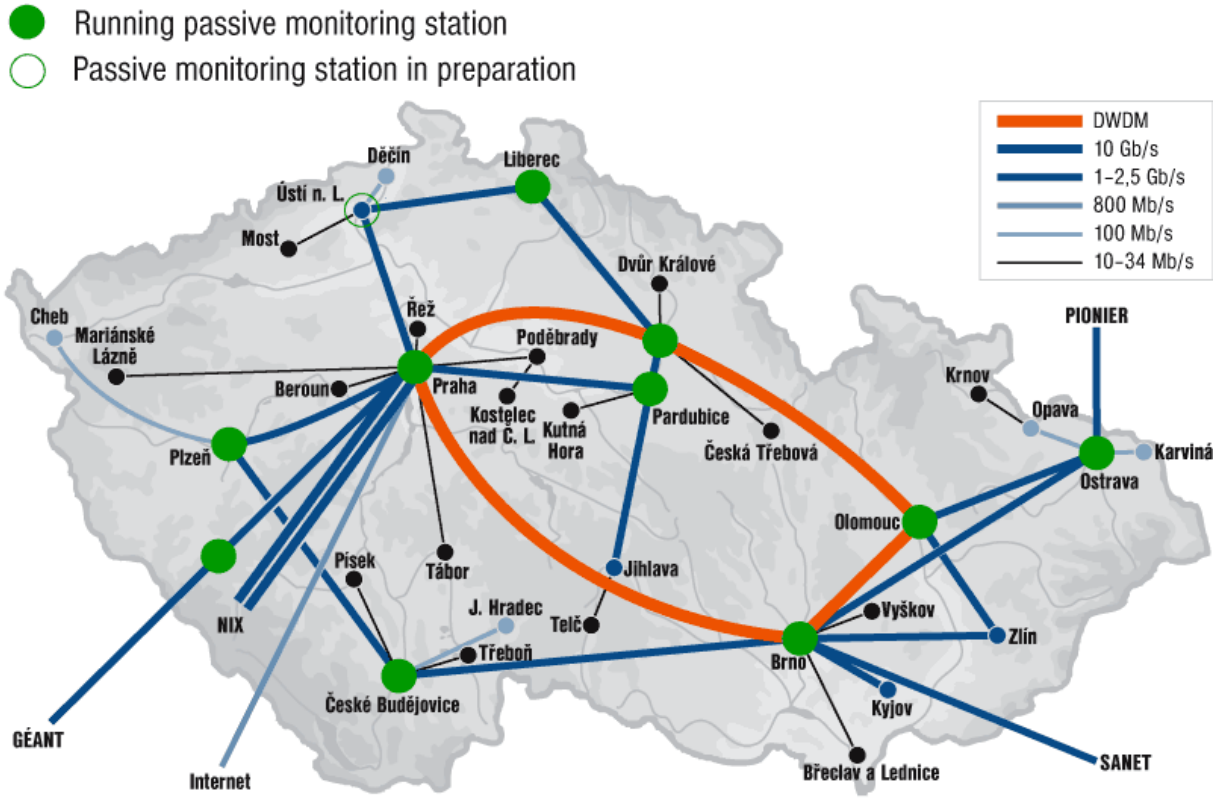
1. Komunikace - zasílání zpráv, přenos souborů, hlasová a obrazová komunikace v reálném čase

2. Sdílení prostředků - technické prostředky (disky, tiskárny, procesor, připojení na dálkové sítě), programy a data (např. databáze)

Historie sítí v ČR

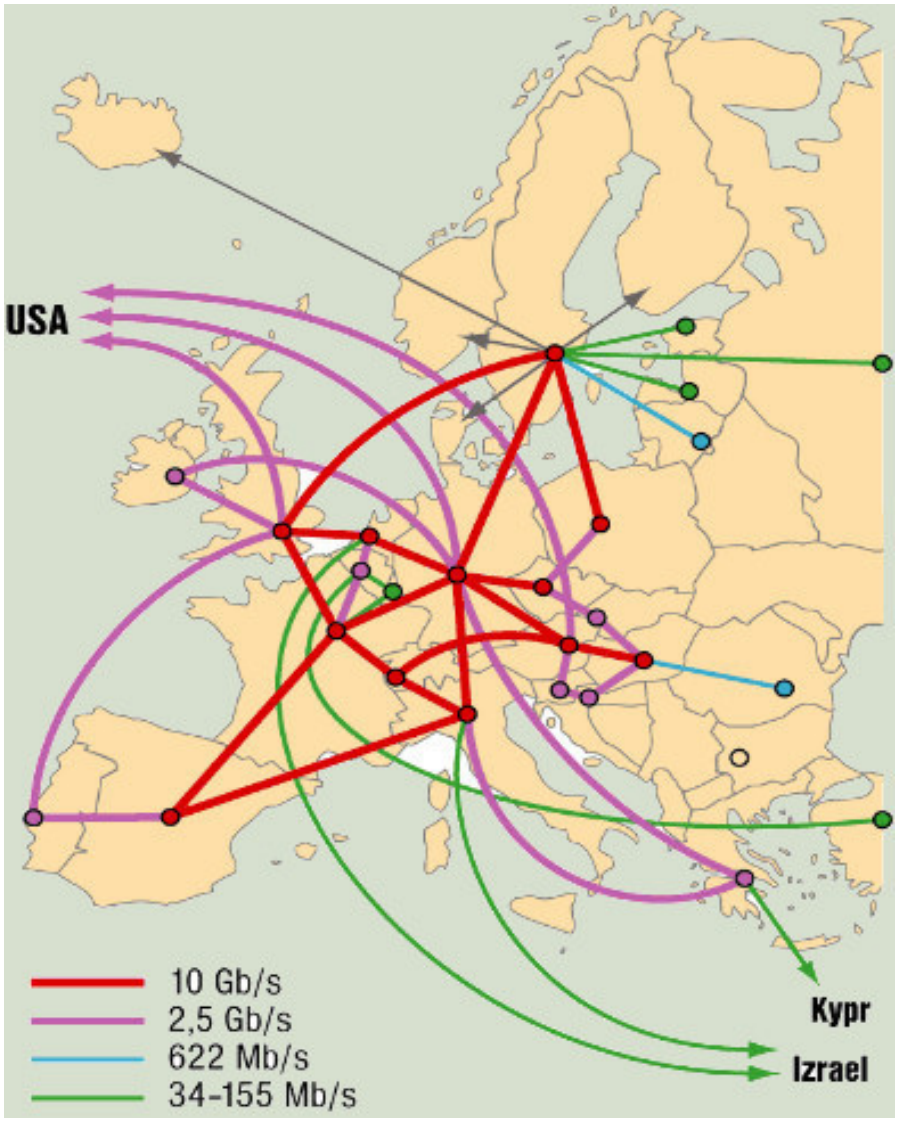
Po roce 1989 se odstranily politické zábrany pro připojení do mezistátních sítí, ale stávající infrastruktura nebyla vhodná pro vytvoření připojení. První sítě, které se zde začaly tvořit, byly spojené s veřejnými telefonními linkami a byly nekvalitní. Na začátku roku 1990 do ČR přichází síť FIDO, což je systém výměny souborů a zpráv mezi sdruženými BBS pomocí vzájemného volání modemů po klasických telefonních linkách. Pro nízké náklady byl tento systém velmi oblíbený. Vznikl v USA v San Francisku v roce 1984. Do roku 1992 fungují sítě BITNET a jejich evropská obdoba EARN. Síť BITNET začala být realizována v roce 1981 z iniciativy firmy IBM. Tvořena byla na principu propojení uzlových sálových počítačů v univerzitách a akademiích a sloužila akademikům a studentům pro sdílení databází a archivů. V tehdejší době připojení uzlu do počítačové sítě bylo finančně i časově náročné. Pokud se připojoval počítač do počítačové sítě, tak to trvalo i půl roku. Funkce byla taková, že každý počítač připojený do sítě věděl o všech ostatních. Pražský uzel EARN byl CSP12 a vedl do Brna, kde se jmenoval CSPUM12. Přenosová rychlost byla 9600 bitů/sekundu. V roce 1992 do ČR nastupuje internet. Internet jako takový vznikl jako projekt americké armády. Cílem bylo hledat řešení takové, abychom měli počítačovou síť, která bude funkční i po jaderném útoku na konkrétní část topologie sítě. Dosud totiž všechny sítě měly buď statický rámec jako je BITNET -

všechny uzly o sobě věděly všechno - nepoužitelný pro praxi, tak se to řešilo tak, že jste měli v síti určité centrum a to vědělo všechno o všem. Problém tedy byl, že v případě nefunkčnosti centra, přestala fungovat i síť jako taková. Hledaly se takové principy, které by nebyly závislé na funkčnosti centra a byly dynamické. Toto bylo základem pro další budování sítě - celosvětové. Síť CESNET je považována za oficiální připojení na Internet. Český projekt dostal jméno FESNET (Federal Educational and Scientific NET work). V roce 1992 se z původního projektu FESNET stal CESNET (Czech Educational and Scientific Network), zatímco na Slovensku se začal realizovat projekt sítě SANET.



Obrázek 1 *mapa sítě ČR*

Rozvoj služeb pro veřejnost začal v roce 1995, ale větší převrat v komerci internetu byl v roce 1999, kdy došlo k digitalizaci telefonní sítě. Začalo docházet ke snižování cen za připojení k internetu a cen osobních počítačů, ale především k rozšíření volných poskytovatelů připojení k internetu. Provozovatel CESNETU získal od Českého telekomunikačního úřadu povolení k poskytování neveřejných, datových telekomunikačních služeb na komerční bázi a tak se stal komerčním poskytovatelem Internetu.



Obrázek 2 *mapa sítě Evropy*

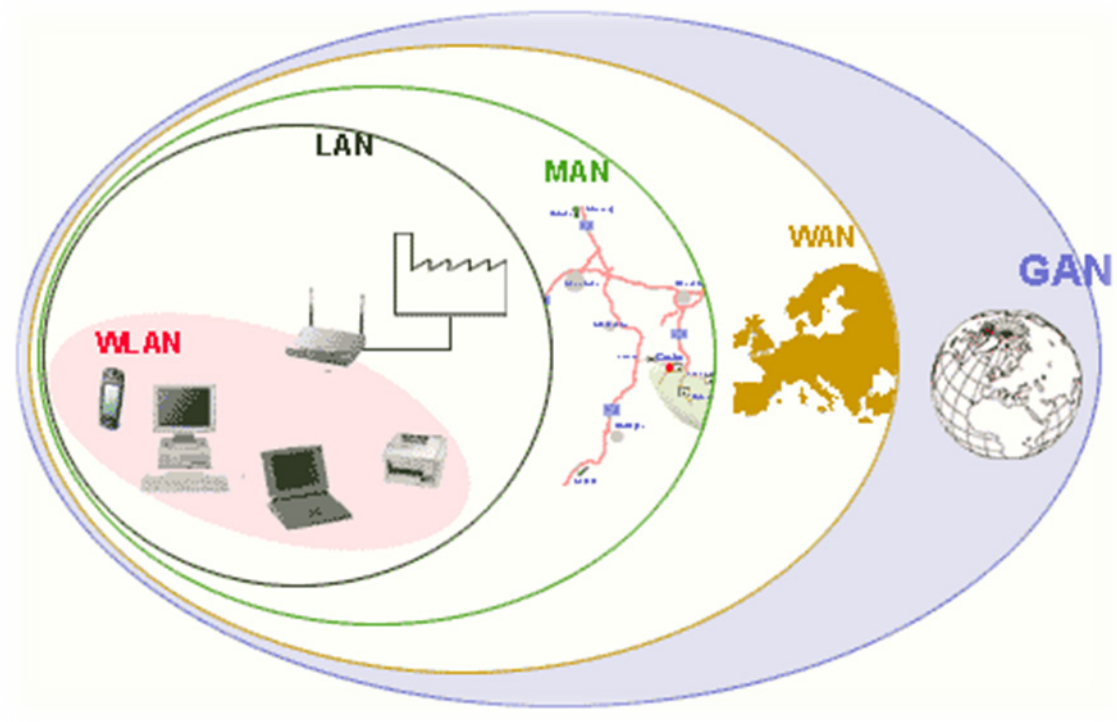
Rozdělení sítí

1.Lokální (LAN - local area network)

2.Městské (MAN - metropolitan area network)

3.Dálkové (WAN - wide area network)

4.Celosvětové (GAN - global area network)



Obrázek 3*rozdělení sítí*

LAN – Lokální sítě

Používají se na malé rozloze a jsou vždy v soukromém vlastnictví. Rozsah je několik stovek metrů. Propojují koncové zařízení, jako jsou PC, tiskárny, skenery nebo server. Pro přenos se používá metalické vedení nebo rádiové vlny. Zařízení připojená do sítě pracují bez navazování spojení, kdy sdílí jeden přenosový prostředek, ke kterému je umožněno připojit se. Přenosová rychlost je u lokálních sítí od desítek Mbit/s až do jednotek Gbit/s.

Do lokálních sítí můžeme zařadit:

- Ethernet
- Fast Ethernet
- Gigabit Ethernet
- Token Bus

- Token ring
- Wi-Fi

MAN - Městské sítě

Tyto sítě jsou obdobou sítí lokálních. Mají větší možnosti, co se týče počtu přístupových bodů. Realizovány jsou buďto drátově nebo bezdrátově. Jejich rozsah bývá několik desítek kilometrů. Bývají jak v soukromém vlastnictví, tak i ve veřejném. Přenosová rychlost je od desítek Kbit/s až do jednotek Gbit/s.

Normalizovanou sítí MAN je pouze protokol DQDB (Distributed Queue Dual Bus)

WAN - Dálkové sítě

Rozlehlá síť pokrývající velké území, které zasahuje například mimo město nebo stát. WAN jsou budovány jako soukromé nebo je budují poskytovatelé připojení k internetu za účelem připojení LAN do internetu. Pro síťové služby se používá nejčastěji protokol TPC/IP

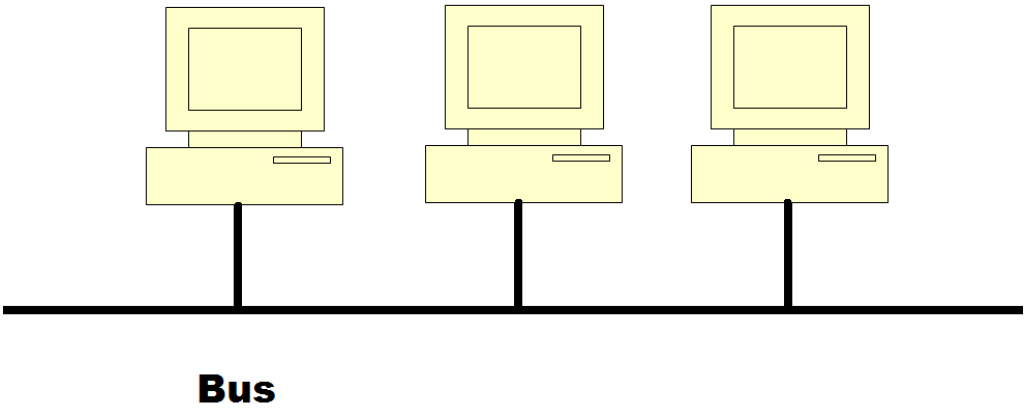
GAN - Celosvětové sítě

Globální síť spojuje několik kontinentů. Realizována je pomocí podmořských kabelů nebo pomocí družicového spojení. Rychlost se pohybuje v řádech Gbit/s.

Topologie LAN - Udává systém zapojení počítačů do LAN.

Sběrnicová topologie

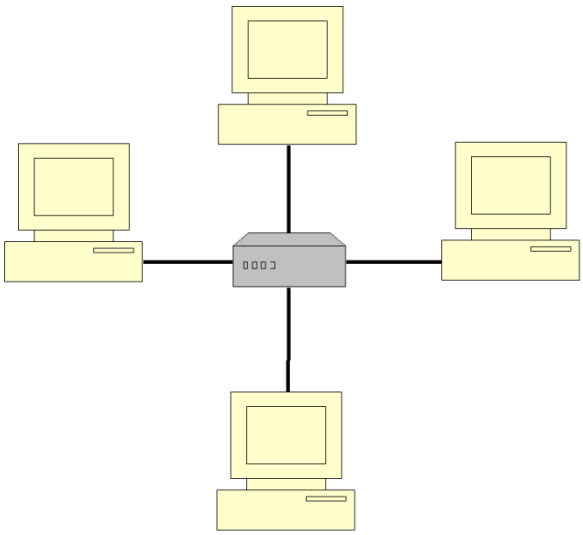
Topologie je realizována pomocí jednoho přenosového prostředku a to sběrnice. Přenos je prováděn po koaxiálním kabelu. Existují 2 druhy a to 10Base-2 a 10Base-5. Rozdíl je dán v použitém kabelu. Tuto technologii využívá Ethernet. Jedná se o starší technologii, dnes již méně používanou. Nevýhodou je nesnadné zjišťování závad, omezená délka kabelu ani za předpokladu použití aktivních prvků a omezený počet připojených stanic. Výhodou je nízká pořizovací cena.



Obrázek 4 *topologie sběrnicová*

Hvězdicová topologie

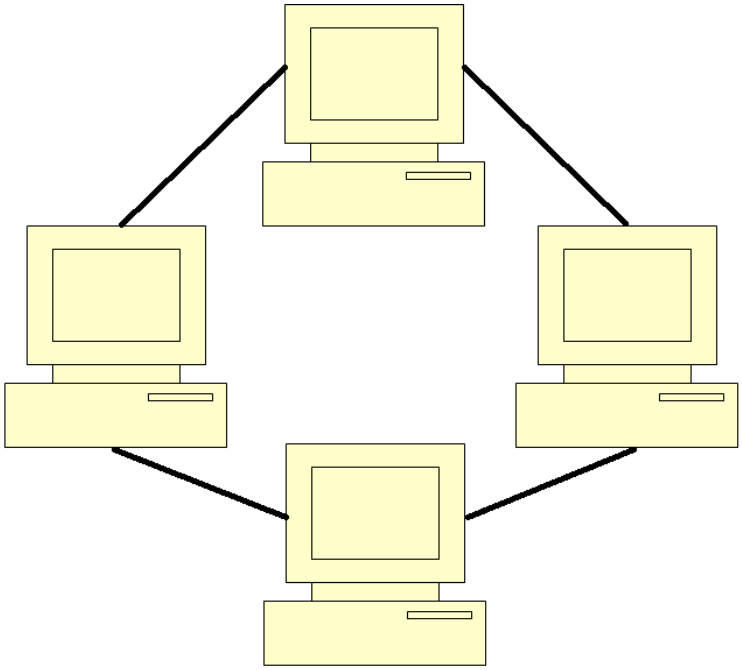
Nejpoužívanější topologie, kde se stanice připojují k hlavnímu hubu nebo switchi, kde mezi každou stanicí a switchem je vždy jen jedna cesta. Zapojení připomíná hvězdu, proto hvězdicová. Při poruše hubu zkolabuje celá síť, kdežto při poruše jedné z připojených stanic nebo porušení spojení mezi hubem a stanicí dojde pouze ke zkolabování dané stanice. Oproti sběrnicové topologii má mnohem větší výkonnost. Snadno ji můžeme rozšířit a nalézt případnou závadu. Nevýhodou je, že při větším rozsahu sítě je potřeba velké množství kabelu.



Obrázek 5 *topologie hvězda*

Kruhová topologie

Topologie, v níž každá stanice má vstup a výstup. Z výstupu stanice se připojí na vstup druhé stanice. Vytvoří tak pomyslný kruh. Pokud budeme mít počítačovou síť tvořenou 10 počítači, a budeme chtít poslat informaci z počítače číslo 5 na počítač číslo 10, informace musí projít přes počítače číslo 6,7, 8, 9, proto se kruhová topologie řadí mezi pomalejší metody. Nevýhodou je, že pokud nebude jedna ze stanic funkční, nebude funkční celá síť a to platí i v případě že přidáváme nový uzel. V tom případě je síť mimo provoz. Naopak výhodou jsou náklady na tvorbu sítě a jednoduchost tvorby sítě, protože přenášené pakety jdou jen jedním směrem.



Obrázek 6 *topologie kruhová*

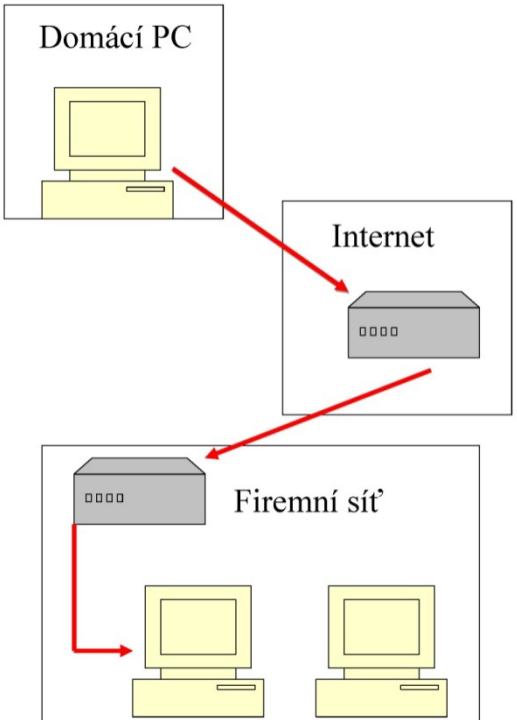
I. TEORETICKÁ ČÁST

1 VZDÁLENÉ PŘÍSTUPY

1.1 Úvod do tématu

Vzdálené přístupy a vzdálené řízení PC je dnes již standardním nástrojem zrychlení, zkvalitnění a zpohodlnění práce u většiny firem, ale i na domácí počítače lze vzdálené řízení využít. Pro firmy může vzdálené řízení mít několik uplatnění. V první řadě se používá pro zrychlení práce, kdy například obchodník je schopen se z obchodního jednání v New Yorku během několika málo okamžiků připojit do firemní sítě v Praze k datům na jeho osobním počítači nebo na hlavní server přímo do firemní sítě. Využívá se zde i pro vzdálenou správu, kdy technik je schopen se ze svého místa pracoviště připojit a nastavit vzdáleně PC kohokoliv jiného. Úspora času je nesmírná. Vzdálené řízení může však mít i charakter sledování výkonnosti pracovníků. Vedoucí oddělení je schopen na dálku a skrytě sledovat aktuální práci určitého pracovníka, či vyhledávat údaje o posledních navštívených stránkách webů a podobně. Pro domácnosti je charakter funkcí stejný. Majitel se může například připojit ke svému domácímu počítači a sledovat co právě dělají na počítači jeho děti. Využití může být i v komerční bezpečnosti, kdy se majitel rozhodne instalovat IP kamerový systém a serverem bude jeho hlavní domácí PC. Majitel pak může v době nepřítomnosti v objektu vzdáleně připojit na PC a sledovat dění z kamer.

Výhody, které vzdálené přístupy přináší je nespočet, ale nesmíme zapomenout na rizika, která sebou vzdálené připojení přináší. Pokud se budeme připojovat přes veřejnou síť (nejčastěji internet), je zde riziko napadení odposlechem, či sledováním datového toku. V takovém případě je schopen útočník sledovat každý náš pohyb. V případě sledování připojení do firemní sítě, je schopen zjistit hesla či citlivé údaje týkající se firmy. Při připojení do domácí sítě může útočník sledovat naše hesla nebo citlivé údaje uložené na disku. Datové toky jsou u většiny možností šifrované a pro zvýšení bezpečnosti se používají hesla. Více o zabezpečení jednotlivých možností bude napsáno v jednotlivých kapitolách.



Obrázek 7 *vzdálený přístup - znázornění*

1.2 Základní rozdělení vzdálených přístupů a řízení PC

1. VNC server
2. Vzdálená plocha ve Windows
3. VPN

1.3 VNC

1.3.1 VNC princip

Virtual Network Computing je program, který umožňuje vzdálené připojení pomocí grafického rozhraní na vzdálené PC přes síť (internet, LAN). VNC vytváří připojení pomocí klient – server. Server vytváří grafické rozhraní plochy a ukládá jej do operační paměti počítače a informace dále odesílá klientovi, kterému se sejmutá plocha zobrazuje. Uživatel sedící u serveru nemusí postřehnout, že se k němu klient připojil. Takto může klient sledovat aktuální práci na serveru, ale zároveň může klient PC ovládat s tím, že server uvidí jeho pohyby.

Pro komunikaci se využívá protokol RFB, jehož účel je co nejvíce komprimovat přenášené grafické objekty a tak program lze využít i v pomalejších sítích. Princip je v tom, že server a klient se nejdříve dohodnou na možné verzi protokolu kvůli kompatibilitě jako je druh komprese atd. a poté začne server sdílet data, ke kterým se klient připojuje. Nejdříve server sdílí celou plochu a poté se plocha rozdělí na obdélníky a odesílají se jen ty obdélníky, na kterých proběhla grafická změna. Tím je zajištěna maximální úspora velikosti dat.

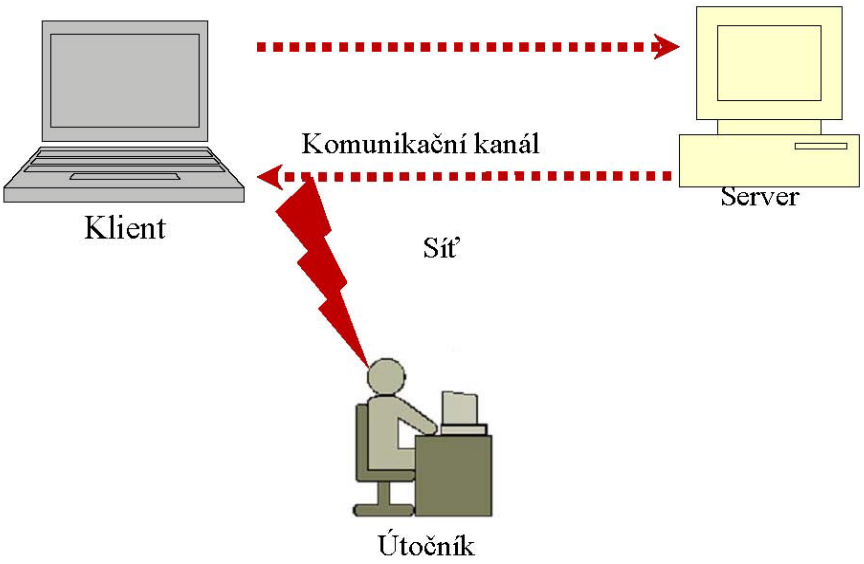
1.3.2 VNC připojení

VNC standardně používá TCP porty 5900 až 5906. Každý port koresponduje s jednotlivými obrazovkami (0 až: 06). V mnoha implementacích (např. RealVNC) je dostupný Java prohlížeč na portech 5800 až 5806, umožňující klientům ovládání mimo jiné i přes webový prohlížeč, podporující Javu. Ostatní porty mohou být použity, pokud jsou klient i server patřičně zkonfigurovány. Použití VNC přes internet funguje dobře, pokud je na obou koncích širokopásmové připojení. Nicméně někdy je třeba pokročilá konfigurace NAT, firewallu a routeru, aby spojení bezproblémově prošlo skrz.

1.3.3 VNC bezpečnost

Největší nevýhodou je bezpečnost. Autentizace pracuje formou challenge-response, což je systém otázky a odpovědi. Server vyzve klienta k zadání uživatelského jména a hesla. Tento krok je ještě stále šifrován a zabezpečen celkem dobře. Po povolení přístupu však samotný přenos dat šifrován není. Vzniká zde možnost odposlechu. Odposlech nemusí být jen sledování práce klienta na ploše, ale i záznam kliků myši nebo úderů klávesnice, kde se dají snadno odhalit hesla a podobně. Existují různé doplňovací moduly, které přenos šifrují, nebo máme možnost zvýšit bezpečnost použitím například VPN tunelu.

Protokol RFB lze využít i mimo operační systém Windows.

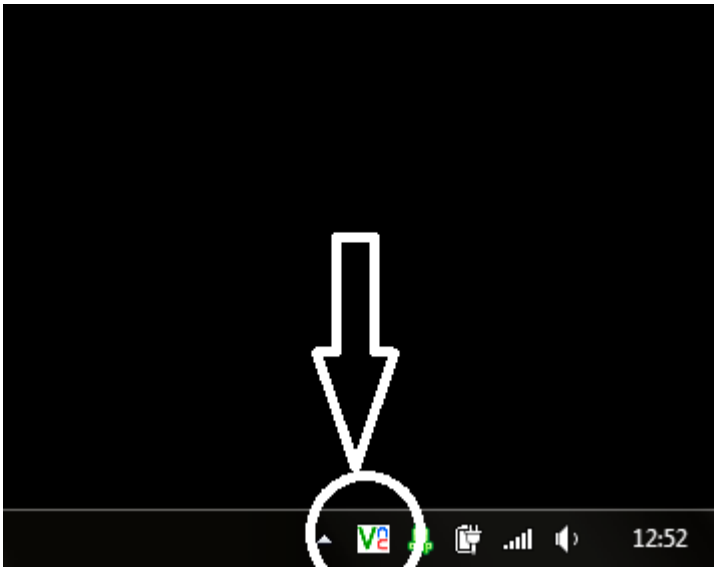


Obrázek 8 *odposlech při vzdáleném přístupu*

1.3.4 VNC nastavení programu

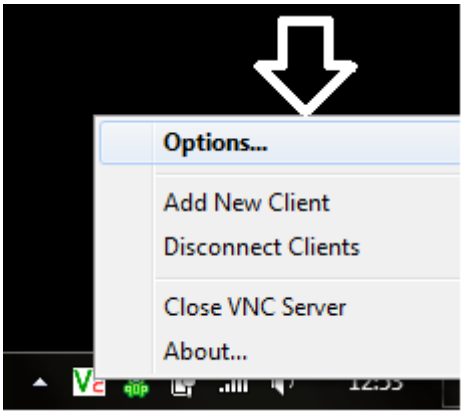
V této části bude zobrazeno základní nastavení programu po jeho instalaci. Budou zde zobrazeny pouze základní kroky k úspěšné funkci programu.

1. Ikona zobrazení spuštění programu VNC



Obrázek 9 *zobrazení ikony - VNC*

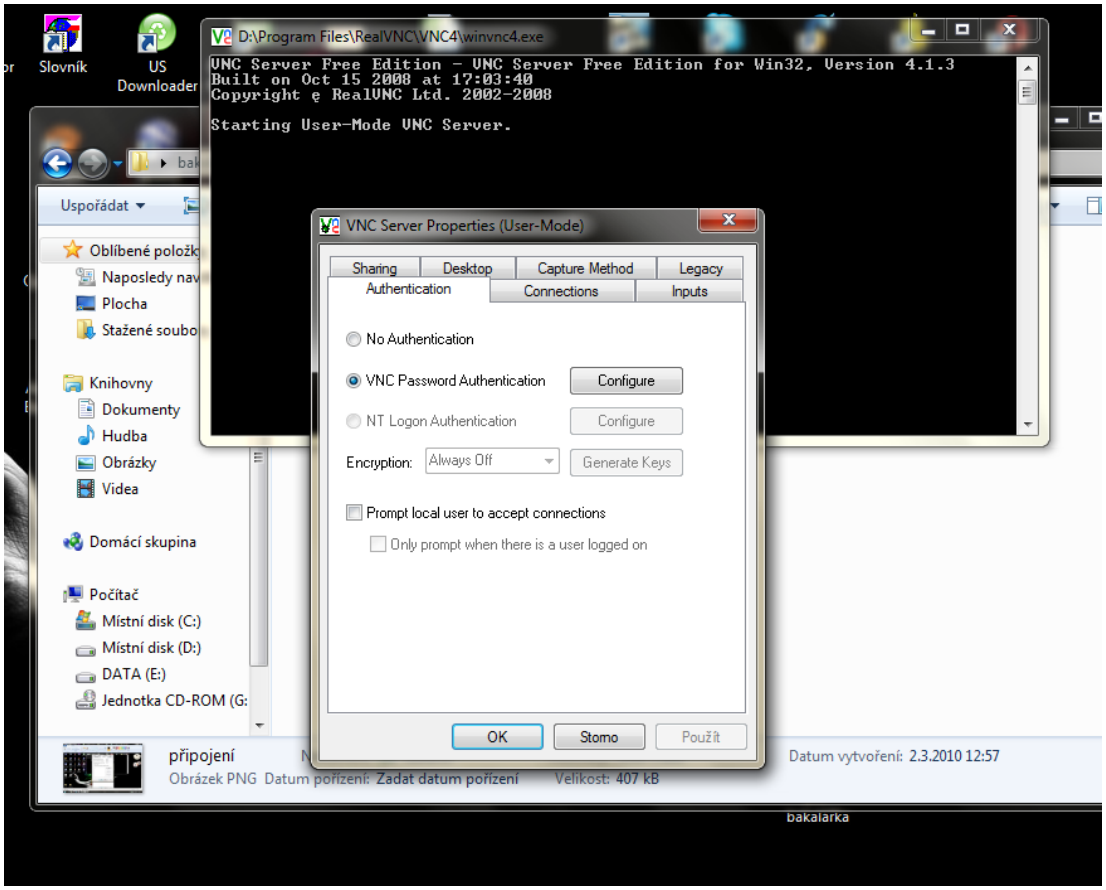
2. Nabídka nastavení



Obrázek 10 *nabídka nastavení - VNC*

Do této nabídky se dostaneme poklepáním pravého tlačítka na ikonu VNC

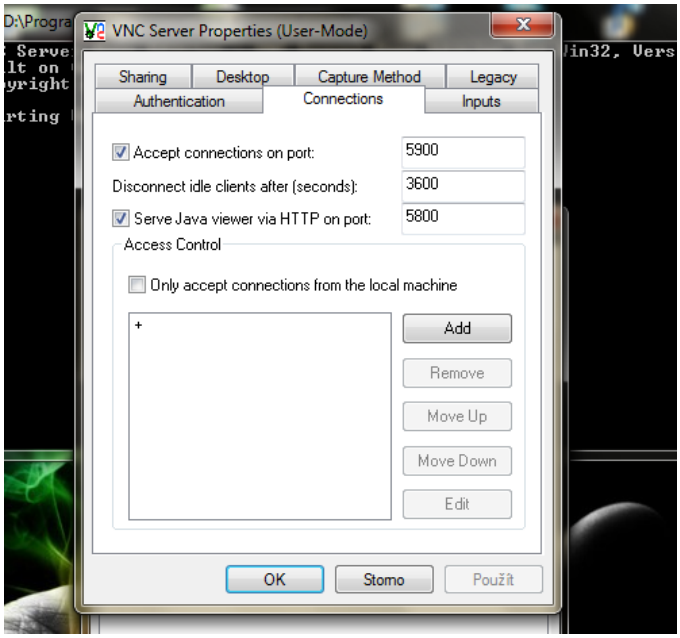
3. Nastavení hesla



Obrázek 11 *nastavení hesla - VNC*

V této nabídce nastavujeme, zda autentizace bude formou přihlašovacího jména a hesla či nikoliv.

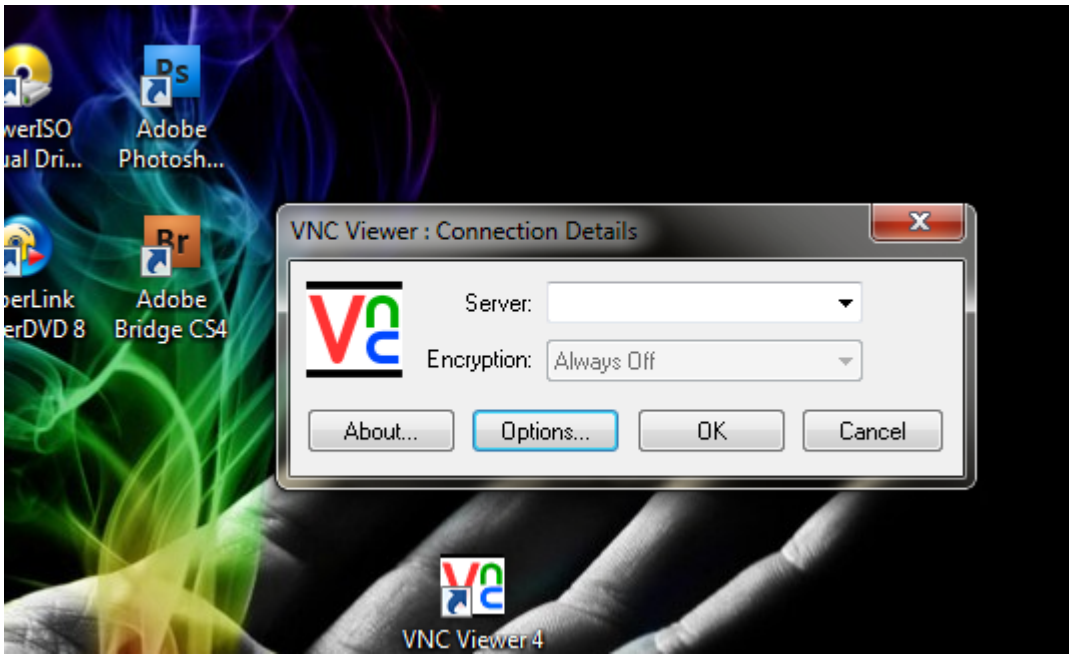
4. Nastavení připojení



Obrázek 12 *nastavení portů - VNC*

Nastavení portů a připojení

5. Samotné připojení klienta k serveru



Obrázek 13 *připojení ke klientovi - VNC*

Součástí programu je VNC viewer, přes který se klient připojuje k serveru. Do názvu server vepíšeme buďto IP adresu nebo název serveru. V položce options máme nabídku, v jaké kvalitě budou přenášené obrázky a podobně. Kvalitu volíme na rychlosti připojení do sítě, kde se nacházíme nebo kde se nachází vzdálený server.

1.4 Vzdálená plocha ve Windows

1.4.1 Vzdálená plocha Windows princip

Jedná se o program, který je součástí operačního systému Windows. Program se liší dle zakoupené verze systému. V některých verzích se dodávala verze, u které bylo možné se pouze připojit na daný systém, ovšem připojit se z daného systému do jiného nebylo možné. Takové systémy byli například Windows XP home, Vista home. U verzí, jako XP Professional, Vista Ultimate, Windows 7 Ultimate, byla dodávaná verze programu, kde fungovalo oboustranné připojení, kde se mohl uživatel připojit na daný systém i z jiného systému.

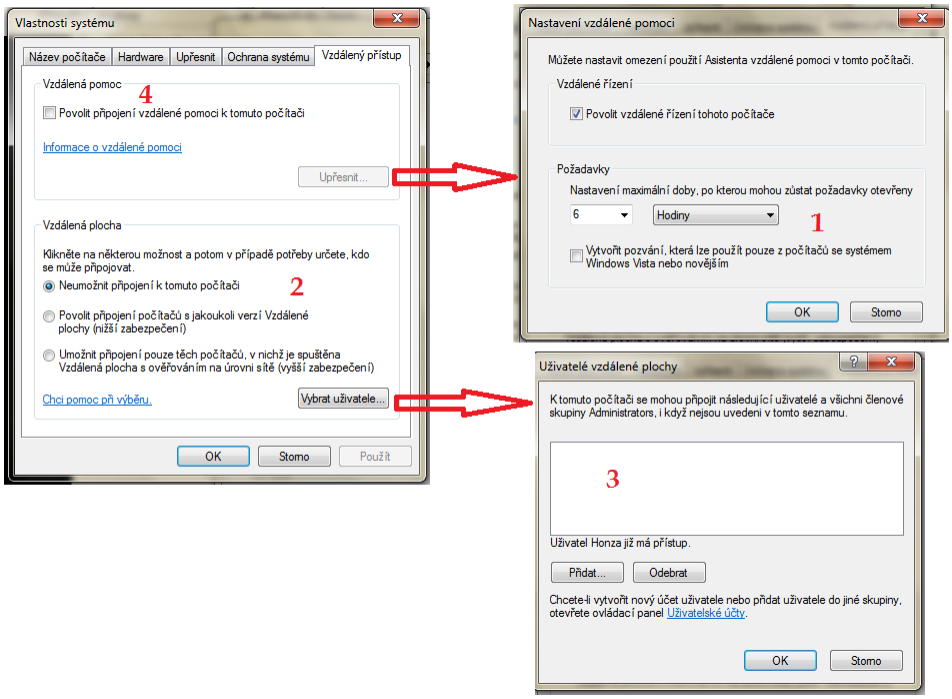
Po přihlášení ke vzdálenému serveru se veškerá práce na serveru ukončí a server pro uživatele přechází do stavu spánku, kdy uživatel vidí pouze černou obrazovku.

1.4.2 Vzdálená plocha bezpečnost

Pro nastavení vzdálené plochy ve Windows je potřeba přijmout některá opatření. Pro komunikaci je potřeba mít otevřený port číslo 3389 ve firewallu. Pro zvýšení bezpečnosti je dobré změnit číslo portu, protože některé škodlivé softwary mají tendenci zjišťovat, zda tento port má PC otevřený, a následně se pokoušet o nabourání do systému. Pro změnu portu uvedu návod v další kapitole o zvýšení bezpečnosti připojení. Dalším bodem zabezpečení je, že uživatel, který se vzdáleně připojuje na svůj účet, musí u svého účtu mít heslo. V nastavení programu je možno dále nastavit dobu, po kterou je možné program používat, jaké verze programu se mohou na daný systém připojit, nebo jaký uživatel má možnost vzdáleně řídit svůj účet. Komunikace mezi klientem a serverem je šifrována, ale je zde velké riziko odposlechu komunikace. Tato hrozba je způsobena tím, že nepoužívá certifikát pro autentizaci serveru, jako SSL / SSH. Tato hrozba se nazývá man in the middle attack. Tuto hrozbu lze vyloučit použitím VPN tunelu.

1.4.3 Vzdálená plocha základní nastavení

Zde bude ukázáno základní nastavení programu a změna portu pro používání programu.



Obrázek 14 *nastavení vzdálené plochy Windows*

1. Nastavení času pro používání programu
2. Nastavení možnosti připojení dle verze programu
3. Nastavení uživatelé, kteří mají právo se vzdáleně připojit
4. Základní povolení funkčnosti programu

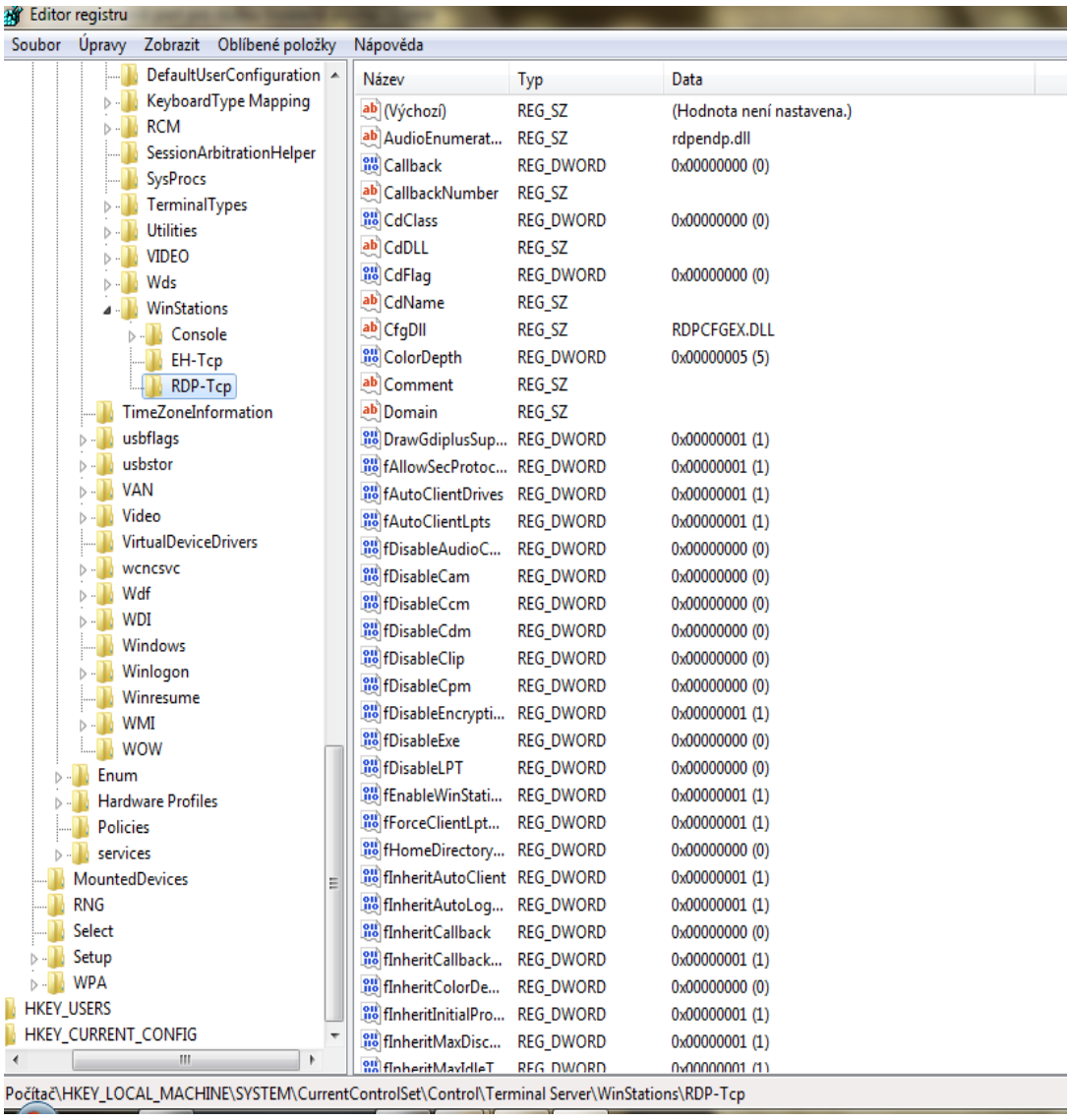
Změna portu zvýší bezpečnost při používání programu. Některé škodlivé aplikace zjišťují otevřenost tohoto portu a poté se pokoušejí o nabourání systému nebo informují majitele a tím vzniká hrozba, že někdo bude zkoušet procházet jeho systém. Změna portu by tedy neměla chybět při používání programu. Postup je následující:

1. Přihlásit se s oprávněním Administrátor.
2. V tlačítku Start zvolit Spustit a zde napsat - regedit.
3. Najít cestu:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\TerminalServer\WinStations\RDP-Tcp

4. V pravé části okna označte hodnotu PortNumber.
5. Z nabídky Úpravy zvolte Změnit.
6. Přepínač Číselná soustava nastavte na Desítková.
7. Do pole Údaj hodnoty zadejte číslo nového portu a potvrďte nastavení.
8. Ukončete Editor registrů a restartujte počítač.

Čísla portů jsou uvedená na internetu. Je potřeba vybrat číslo neobsazeného portu.



Obrázek 15 *změna portu vzdálené plochy v registru*

1.5 VPN

1.5.1 VPN princip

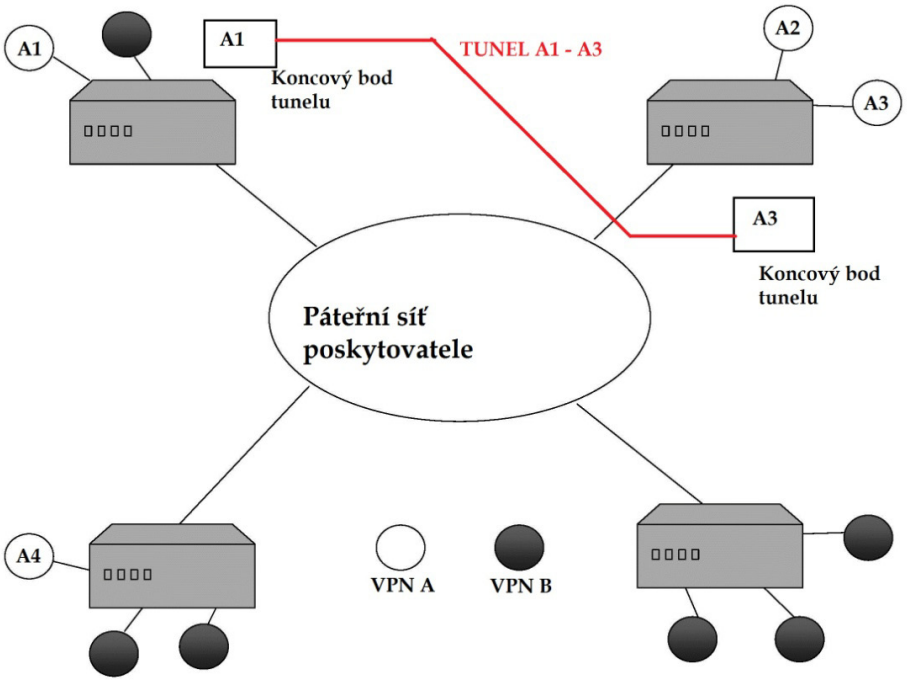
Virtual private network je způsob propojení dvou a více sítí, které jsou odděleny nedůvěryhodnou sítí, například přes internet. Je to prostředek, který virtuálně vytvoří „kabel“ a propojí tak sítě mezi sebou. Hlavní výhodou VPN je bezpečnost přenášených dat. Používá se nejčastěji pro zvýšení bezpečnosti vzdálených přístupů, kdy se vytvoří VPN připojení k síti a poté bude použit některý z programů pro vzdálenou správu. Je tak zajištěno, že nedojde k odposlechu přenášených dat. Vytváření VPN funguje na podobné principu jako například VNC, kdy se vytváří VPN server a na něj se pak připojují klienti. Připojením na VPN server tak získáme jistotu šifrovaného přenosu dat. Zjednodušeně lze říct, že VPN vytváří virtuální linku mezi dvěma sítěmi a po připojení se naskytují další možnosti síťového připojení.

1.5.2 VPN topologie

1.5.2.1 Topologie na síťové vrstvě

Základ pro vytvoření VPN na síťové vrstvě je práce se směrovacími informacemi. Informace, které provádějí směrování, obsahuje právě síťová vrstva. Je zde možnost modelů sítě, které určují způsob směrování, a to peer a overlay. Model sítě peer se liší od modelu overlay v tom, že směrovací informace jsou prováděny na každém uzlu cesty paketu informací k cíli, kdežto overlay směřuje paket na každém mezilehlém uzlu. U této metody mohou nastat problémy z důvodu větší výpočetní náročnosti. Mezi oběma modely zde existuje rozdíl ve škálovatelnosti obou modelů.

Prvním typem topologie na síťové vrstvě je filtrování směrovacích informací. Je založen na jednoduchém principu, kdy se snažíme o omezení propagace směrovacích informací o dosažitelnosti jiných sítí. Typově bychom tento model označili za peer. Je zde jeden směrovač, který zastupuje skupinu uzlů a navazuje spojení pouze se vstupním směrovačem poskytovatele spojení, ale ne se všemi ostatními sítěmi. Pro ukázku je uveden model:



Obrázek 16 *tunelování na síťové vrstvě*

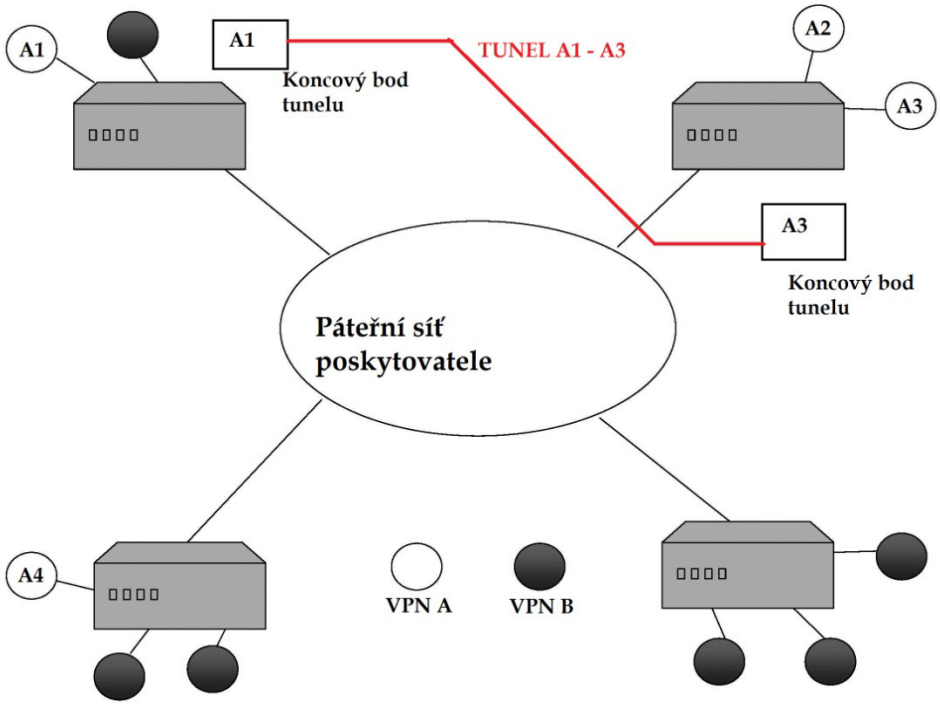
Na obrázku 16 je vidět, že směrovače ze sítě VPN A budou odesílat informace pouze pro směrovače patřící do sítě a tak nebudou mít jiné (v tomto případě VPN B) explicitní informace o dosažitelnosti, či existenci této sítě.

Tento způsob má ale své nevýhody. Jedním z nich je obtížné zabránění přístupu z jednotlivých částí VPN na nejbližší implicitní směrovač sloužící k externí komunikaci se sítěmi mimo danou vlastní VPN - implicitní směrovač dané sítě pro vnější komunikaci s ostatními částmi dané VPN musí být přístupný. Na tomto směrovači je nutná řádná implementace komunikačních filtrů k zablokování veškeré komunikace směřující mimo danou VPN.

Dalším typem topologie na síťové vrstvě je model klasického tunelování. Principem je vytvoření tunelu v síti, po kterém je přenášena komunikace. Tento typ můžeme zařadit jako overlay model VPN. Jak bylo výše uvedeno, overlay může mít problémy s výpočetní náročností. Tento případ nastává ve chvíli, kdy je spojení – bod s více body. Spojení typu bod - bod není problematické, kromě případu, kdy jeden uzel má vybudovat více spojů typu bod - bod s více koncovými uzly. Zde jde jen o lineární problém škálovatelnosti, zatímco u tunelů typu bod - více bodů, speciálně těch, co využívají

vytváření přímých spojení mezi koncovými body, je problém škálovatelnosti podstatně vážnější.

Tunely GRE (Generic Routing Encapsulation) – jsou budovány směrovači páteřní sítě, které mají funkci vstupního a výstupního bodu tunelu VPN. Paket informací vyslaný pro přenos tunelem je vybaven zvláštní hlavičkou a cílovou adresou, která je shodná se směrovačem na konci tunelu. Toto zabalení je na konci tunelu rozbaleno ve směrovači a následně pokračuje dle IP adresy k cíli.



Obrázek 17 *klasické tunelování*

Základním principem při tvorbě VPN pomocí tunelování je tedy vytvoření sady tunelů přes společnou sdílenou síť (ať už privátní síť, veřejnou síť poskytovatele spojení nebo Internet). Výhodou této metody je adresace. Přístupové body páteřní sítě, které jsou i koncovými body vytvořených tunelů, používají adresaci a směrování této společné sítě. Technika tunelování používá adresaci cílových bodů tunelů z tohoto adresového prostoru, zatímco pakety přenášené tímto tunelem používají adresy z adresového prostoru VPN. Výsledkem je tedy vzájemné "odstínění" obou adresových prostorů. Směrování v obou

sítích jsou od sebe izolovány, což je jeden ze základních principů použitého overlay modelu. Významnou předností tunelování je schopnost přenosu tunelem v principu libovolného síťového protokolu. Použitý protokol v rámci dané VPN je tak přenášen přes sdílenou páteř beze změn a je tak v podstatě pro VPN simulována privátní dedikovaná síť se zachováním funkčnosti použitého protokolu i s jeho směrováním. V tomto případě dojde ke vzájemnému odstínění obou sítí (společné přenosové sítě a VPN), i z hlediska směrování.

1.5.2.2 Topologie na spojové vrstvě

Pokud budeme při tvorbě VPN používat vlastní nebo pronajatý přenosový systém, získáme tak nejpoužívanější metodu vytváření VPN a to metodu virtuálních obvodů na spojové vrstvě. Můžeme si tak dovolit vytvoření nezávislé VPN na vyšší přenosové vrstvě a tím dosáhneme diskrétní VPN na síťové vrstvě. Můžeme je pak považovat za funkční analogii konvenčních privátních datových sítí. Konvenční privátní datové sítě používají kombinaci dedikovaných obvodů, které pronajímá poskytovatel spojení, a privátní komunikační infrastrukturu. Tímto je dosáhnuto kompletní, soběstačné, síťové infrastruktury. Základní charakteristikou pronajatých dedikovaných linek je způsob využití časového nebo frekvenčního multiplexingu a synchronizace odesílaných a přijímaných dat. Základní rozdíl mezi dedikovanými a virtuálními obvody je v neexistenci časové synchronizace přenosů a navíc zde ani nemusí existovat dedikovaná přenosová cesta. Proto může na rozdíl od dedikovaných obvodů docházet k přetížení sítě tvořené virtuálními obvody. Výhodou veřejných přepínaných sítí je velká flexibilita.

Tento způsob se používá, například v sítích Frame relay . V síti se mimo jiné udává pojem CIR (Committed Information Rate), který udává referenční hodnotu pro kontrolu velikosti přenosové rychlosti ve vstupním bodu sítě. Je-li překročena dohodnutá hodnota CIR, vstupní rámce dále síť akceptují, ale připadne jim označení DE (Discard Eligible), což má za následek, že takto označené rámce jsou jako první zahozeny, dojde-li na jejich cestě sítí k přetížení.

Tyto uvedené vlastnosti sítí s virtuálními obvody platí i pro sítě ATM (Asynchronous Transfer Mode). U sítě Frame relay není použita synchronizace datových přenosů mezi vysílačem a přijímačem. Obdobně je i využita funkce kontroly rychlosti

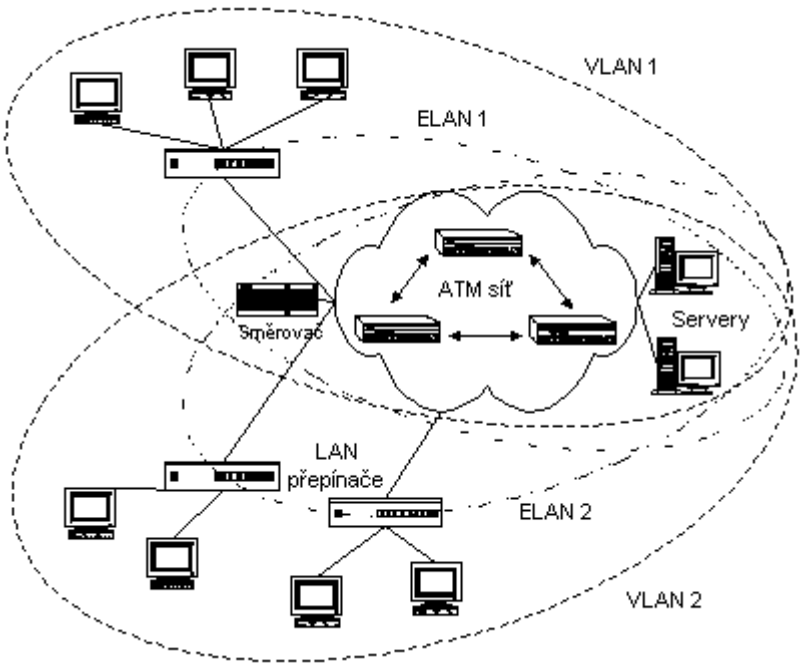
přenosu, a vstupní rámce mohou být označeny v případě překročení rychlosti jako CLP (Cell Loss Prority). Při označení jsou obdobně zahozeny, jako u sítě Frame relay.

Dalším typ mohou být virtuální sítě vytvořené LAN emulací. V heterogenních sítích tvořených jak segmenty sdíleného či přepínaného Ethernetu, tak technologií ATM, lze aplikovat VLAN (Virtual LAN) dvěma způsoby:

1. Pokud není při použití technologie ATM žádný koncový uzel, je toto prostředí páteře ATM pro virtuální sítě naprosto transparentní. Připojené LAN přepínače komunikují mezi sebou bez toho, že by si "uvědomovaly" existenci ATM sítě mezi sebou. Ovšem přes svou jednoduchost se tento systém nevidí při budování sítí často.

2. Druhým a častěji používaným způsobem je připojení serverů přímo do páteře ATM připojením. Členství těchto uzlů do sítě zajistíme použitím technologie emulace LAN (LANE - LAN Emulation).

Základní prvky LANE sítí jsou LES (LAN emulation server). Hlavní jejich úkol je mapování mezi MAC a ATM adresami LEC (LAN emulation client). LES dle požadavků jednotlivých LEC poskytuje překlad mezi MAC a ATM adresami, takže komunikace mezi LEC probíhá přímo po ATM síti. Protože LEC může být členem více ELAN, standard LANE umožňuje vytvoření více překrývajících se virtuálních sítí. Tak mohou uzly z různých ELAN přistupovat ke společným síťovým zdrojům bez nutnosti průchodu přes směrovač.



Obrázek 18 *emulované LAN*

2 ZABEZPEČENÍ NEOPRÁVNĚNÉHO VZDÁLENÉHO PŘÍSTUPU

2.1 Úvod do tématu

Neoprávněný vzdálený přístup je velmi nežádaný jev pro správnou funkci sítě nebo samotného počítače. Jelikož v PC a v síti uchováváme různé citlivé údaje a data, je potřeba zamezit případnému odposlechu datové komunikace v síti, který by hrozil formou vzdáleného přístupu. Pokud budeme realizovat síť, ve které budou citlivé informace, nejlepším prostředkem jak se bránit proti neoprávněnému vzdálenému přístupu je izolovat síť od veškerých externích sítí. Síť pak bude postavena pouze lokálně a případný útočník není schopen se vzdáleně do sítě připojit. V mnoha případech však tato možnost není a síť je připojena na další externí sítě, nejčastěji internet. V této variantě je velké riziko, že se do sítě vzdáleně někdo připojí. Možnost jak se proti takovému útoku bránit je použití firewallu. Útočník nemusí být definován jako fyzická osoba, může se jedna o škodlivý program, který je nadefinován, aby po připojení do naší sítě sdílel data, nebo zde působil nechtěnou reklamu a podobně. Útočník jako fyzická osoba se nazývá hacker. Zkušený hacker se do sítě dokáže připojit i přes veškeré softwarové a hardwarové ochrany. Obrana proti nim je pouze izolovat síť od veškerých externích sítí.

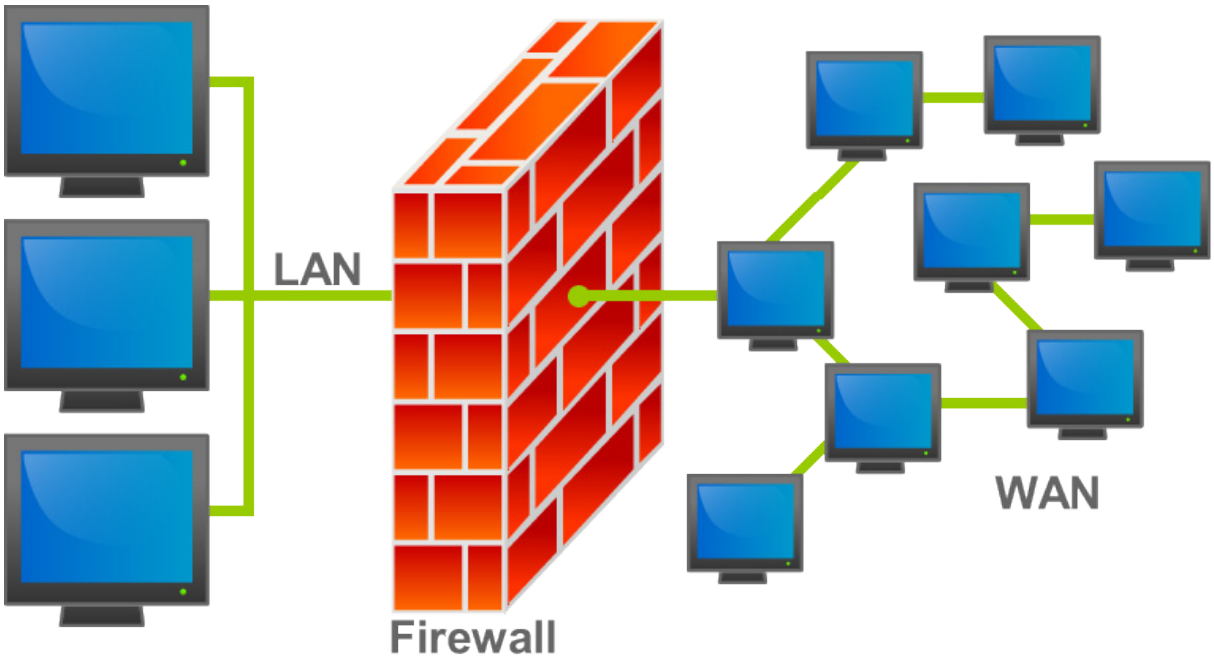
2.2 Firewall

Jedná se o softwarové a hardwarové zařízení, které kontroluje příchozí a odchozí spojení ze sítě. Odděluje od sebe dvě sítě a jeho konfigurací nastavíme pravidla, podle kterých tyto sítě budou komunikovat. V historii se jednalo o pravidla, kdy se identifikovali zdroje dat – zdrojová a cílová adresa. Moderní firewally zjišťují minimálně informace o stavu připojení a znalost kontrolovaných protokolů či prvky IDS.

Firewall je formou softwaru nebo hardwaru. V softwarové verzi máme buďto bezplatné, nebo placené verze. Rozdíl mezi nimi je v obsahu funkcí, kdy bezplatná verze obsahuje pouze základní nastavení a mnohdy je jeho funkce pod úrovní kvalitního zabezpečení. Placené verze mohou být například součástí antivirů nebo mohou obsahovat další funkce jako antispam, nebo antispyware. Součástí jsou také pravidelné aktualizace, kdy se program „učí“ nejnovější obranu. Ta je vytvářena z nejnovějších poznatků a zkušeností. Hardwarové firewally jsou nejčastěji součástí routerů, kdy se jedná o program uvnitř routeru a po následném nastavení a zapojení jako součástí sítě získáváme

hardwarový firewall. Zde nerozlišujeme placenou a neplacenou verzi. Z pravidla je firewall součástí každého routeru a jeho aktualizace se provádí přehráním novější verze firewaru v routeru a je zdarma.

V únoru 2009 proběhl test firewallů na webu: http://www.zive.cz/bleskovky/nove-testy-firewallu-outpost-vede-sunbelt-a-zone-alarm-se-propadaji/sc-4-a-145759/default.aspx kde výsledkem bylo, že některé firewally ke stažení zdarma mají lepší hodnocení bezpečnosti než některé placené firewally. Takže pravidlo, že placený firewall musí být zákonitě lepší, není vždy platné.



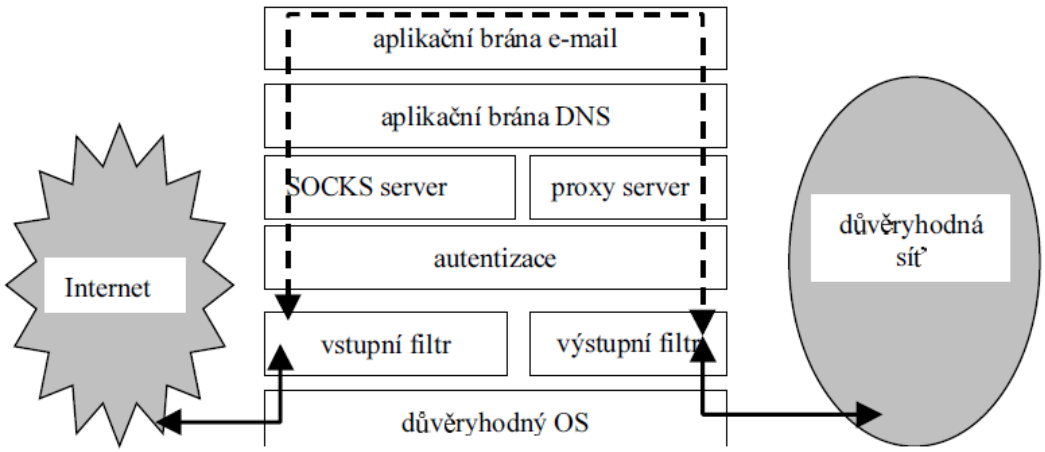
Obrázek 19 *znázornění firewallu*

Firewally pracují na bázi otevírání portů, přes kterou probíhá veškerá mimo síťová komunikace. Portů je v počítači okolo 65000. Právě tyto porty firewall kontroluje. Samotné nastavení programu vyžaduje určité zkušenosti. Dnes již ale existují firewally které jsou automatizované, kdy se využívá výše uvedených aktualizací vytvořených na základě zkušeností a analyzování. Firewall se po nainstalování nastaví dle standardů a pro další správnou funkci se v případě, že se objeví situace, kterou nemá předefinovanou, zeptá uživatele, zda má právě tuto komunikaci povolit či nikoliv.

Shrnutí funkce firewallu:

- Izolace vnitřní sítě - jeden bod přístupu.
- Znemožnění zmapování sítě zvenčí.
- Jemnější specifikace práv individuálních uživatelů.
- Sledování provozu na síti.
- Případné bezpečnostní díry v softwaru síťových služeb jsou odstíněny.

Struktura firewallu:



Obrázek 20 *struktura firewallu*

Základní dělení firewallů:

1. Paketové filtry
2. Aplikační brány:
3. Stavové paketové filtry
4. Stavové paketové filtry s kontrolou protokolů a IDS

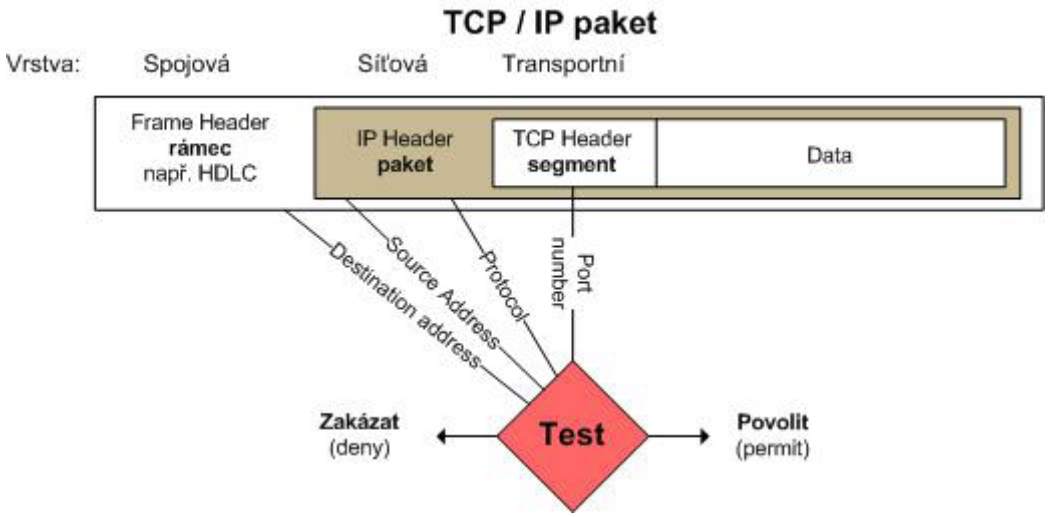
2.2.1 Paketové filtry

První a nejjednodušší technologie firewallů byla vydaná v roce 1998. Principem jsou pevně nadefinovaná pravidla, kdy se definuje přesně z kterého portu a adresy, na který

port a adresu lze paket informací poslat nebo přijmout. Ostatní datové toky jsou zakázány. Tento způsob je velmi rychlý, jelikož se firewall nemusí zabývat situacemi, které nejsou nadefinované. Nevýhodou je nedostatečné zabezpečení, například při využívání firewallu na audio, či video steaming. Firewall musí pro tyto náročné protokoly otevřít více portů, které tak nejsou pod dostatečnou kontrolou a vymaňují se mimo rámec, jež původně správce nastavil. Z toho vyplívá možné použití tohoto typu firewallu a to v sítích s předem určenými datovými přenosy. Ovšem při správném nadefinování je tento typ firewallu velice účinný.

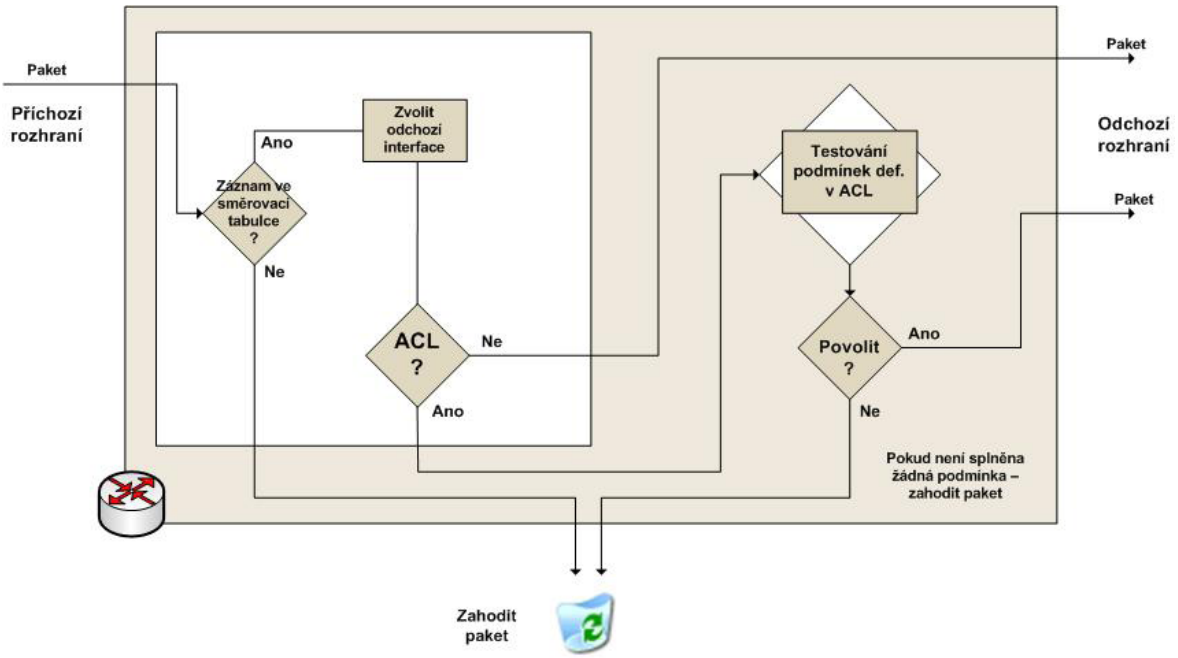
Typický zástupce je např.: ACL (Access Control Lists) ve starších verzích operačního systému IOS na routerech spol. Cisco Systems.

Funkce ACL:



Obrázek 21 *funkce ACL*

Tato funkce je integrována ve většině směrovačů.



Obrázek 22 *znázornění směrovače*

2.2.2 Aplikační brány

Novější metoda než paketové filtry. Oproti paketovým filtrům lze říct, že aplikační brány zcela oddělují dvě sítě. Metoda se někdy nazývaná „Proxy firewally“. Komunikace přes aplikační bránu funguje tak, že iniciátor spojení (klient) odešle požadavek spojení na aplikační bránu, která spojení zanalyzuje a odešle dál na server. Data přijímaná zpět pak aplikační brána odešle klientovi. Kontrola spojení je prováděna na 7 síťové vrstvě síťového modelu OSI. Při používání aplikační brány dochází k efektu, že server nevidí adresu iniciátora spojení, ale pouze adresu aplikační brány. Vysoké zabezpečení známých komunikačních protokolů je velkou výhodou u této možnosti. Nevýhodou je však vysoká náročnost na hardware.

Jako zástupce lze uvést The Firewall Toolkit (fwtk) a z něj vycházející Gauntlet spol. TIS později zakoupený společností NAI.

2.2.3 Stavové paketové filtry

Jedná se o vylepšenou metodu komunikace paketových filtrů, s tím rozdílem, že se ukládají již dříve povolené komunikace a při příštím odeslání požadavku není klient nijak omezován následným povolením komunikace. Příchozí spojení firewall analyzuje a

vyhodnotí ho jako dříve schválené a bezpečné nebo ho pošle k další analýze. Tímto získáváme dobrou míru bezpečnosti v poměru s dobrým výkonem. Bezesporu jedno z nejlepších řešení.

Metodu stavových paketových filtrů využívají např. firewall-1 spol. Check Point do verze 4.0, starší verze Cisco PIX, Cisco IOS Firewall

2.2.4 Stavové paketové filtry s kontrolou protokolů IDS

Tato metoda využívá kromě klasické kontroly o stavu spojení, či kontrole certifikátů, integrovanou funkci IDS (Intrusion Detection Systems – systémy pro detekci útoků). Tyto systémy pracují na podobném principu jako například antivirus, kdy pomocí databáze signatur a heuristické analýzy mohou odhalit vzorce útoků i ve zdánlivě nesouvisejících pokusech o spojení, např. skenování adresného rozsahu, rozsahu portů, známé signatury útoků uvnitř povolených spojení apod. Více o systému IDS v níže uvedené kapitole. Výhodou je snadná konfigurace systému při malé rychlosti oproti aplikačním branám, ale při srovnání s paketovými filtry je rychlost zhruba o 1/3 menší. Bezpečnost u této metody můžeme hodnotit kladně, protože kontrola známých protokolů je zde na dobré úrovni.

2.3 IDS

Systém IDS je velmi společný s firewallem, ale jeho princip je jiný. Firewall hlídá a otevírá porty, čímž efektivně ochrání zrovna nepoužívané služby. Ale porty jako je například přístup k webovým stránkám (TCP port 80), či přístup k portům poštovních služeb POP/SMTP/IMAP, jsou v zásadě otevřené pořád. Pokud by se útočník rozhodl využít slabin právě těchto portů, bude ve většině případů úspěšný i přes aktivní firewall. Zde je prostor pro zřízení systému IDS. Ten na rozdíl od firewallu kontroluje obsah datového toku a v něm se snaží hledat útoky na jednotlivé aplikace. V kombinaci s firewallem tak získáváme vyšší úroveň zabezpečení. Když by útočník přešel přes firewall, pořád by zde byl systém IDS, který by při správné konfiguraci měl útočníka zastavit.

2.3.1 Princip IDS

Pro analýzu paketu se používají v systému IDS 2 možnosti:

1. Rozeznávání signatur
2. Dekódování protokolů

2.3.1.1 Rozeznávání signatur

Signatury jsou speciální sekvence znaků, obsažené v paketu. Systém IDS pak vyhledává tyto sekvence v paketu dle databáze a rozhoduje, zda tyto pakety jsou či nejsou hrozbou. Pro zvýšení přesnosti a bezpečnosti kontroluje nejen sekvenci, ale i její umístění v paketu. Informace o signaturách, které byly označeny jako hrozba, získává systém z databáze která je pravidelně aktualizována a základě uživatelských zkušeností. Tuto databázi můžeme například srovnat s databází, kterou využívají antiviry.

2.3.1.2 Dekódování protokolů

V této metodě analýzy systém IDS dekóduje jednotlivé protokoly a v dekódovaném síťovém provozu, pak vyhledá zranitelnost a bezpečnostní hrozby (například přetečení zásobníku apod.). Je třeba také rozlišovat hardwarový IDS a softwarový IDS, což je podobné dělení, jaké můžeme nalézt i u firewallů. Hardwarový IDS je umístěn na samostatném, obvykle read-only, zařízení, které je externě připojeno k serveru. Výhodou je větší bezpečnost samotného IDS, nevýhodou pak vyšší cena. Tato řešení nabízí většina výrobců aktivních síťových prvků. Softwarové IDS pak mají výhody opačné – výhodu je možnost získání takového IDS zdarma (například celosvětově populární aplikace Snort) a nevýhodou pak možnost kompromitace IDS útočníkem.

3 OCHRANA DAT V PC

3.1 Úvod do tématu

V této kapitole se budeme věnovat ochraně dat v PC, který může nebo nemusí být připojen do lokální sítě. Jedná se o zabezpečení před ztrátou nebo znehodnocení dat uložených na discích v PC. Útok může být v tomto případě cílený, což je například napadení dat počítačovým virem nebo přihlášením neoprávněné osoby k datům. Útok může být ale i náhodného charakteru, jako například zničení disků bleskem nebo samovolné zničení. Jednotlivě se budeme zabývat ochranou před počítačovými viry, nevyžádanou poštou a správou uživatelů v síti. Kromě možnosti napadení dat virem se jedná o hrozby, které přicházejí lokálně. Nesmíme zapomenout na možnost, kdy hrozbou pro data může být sám uživatel, pro tento případ se budeme zabývat integrovanou funkcí operačního systému Windows, nástroje řízení uživatelských účtů. Také bude zmíněna metoda ochrany dat před nechtěným smazáním, či nepředvídatelnou situací zničení disku a to zálohováním dat.

3.2 Ochrana před viry

3.2.1 Úvod

Pojem virus vzniká díky podobnostem biologickému originálu a to v tom, že se dokáže sebe-replikovat (množit), ovšem jen pouze za předpokladu, že je připojen k hostiteli. V našem případě se jedná o soubory. Může být zapsán do jakékoli přípony. Nejčastěji se však používá přípona exe. Pro pochopení je potřeba si ujasnit rozdíl mezi strukturou a příponou: soubor například může mít příponu .dat, ale jeho struktura může být .exe a v tom spočívá záludnost viru. Samotný pojem virus je pouze zlidovělý název pro infiltraci systému. Infiltrace je neoprávněný zásah do systému. O tomto tématu - počítačové viry, lze napsat spoustu stránek. Ve své práci zmíním jen základní typy a jejich reakce a všeobecnou ochranu proti virům.

3.2.2 Typy virů

3.2.2.1 Trojské koně

Jedná se o druh infiltrace, která na rozdíl od jiných není schopná se množit. Nejčastěji se jedná o spustitelné soubory s příponou com a exe. Soubor ve většině případů neobsahuje nic jiného než tělo viru. Na první dojem se může zdát, že se jedná o užitečný program. Jeho funkcí je, že spustí nějakou akci, například mazání souborů. Jeho likvidace je snadná – stačí pouze infiltrovaný soubor smazat.

3.2.2.2 Backdoor

Jedná se o aplikace typu klient – server. Svým principem nápadně připomínají například aplikaci VNC. Rozdíl mezi nimi je však v tom, že do systému vstupují anonymně a pro běžného uživatele je téměř nemožné rozpoznat jejich přítomnost. Z toho důvodu je řadíme mezi infiltrace.

3.2.2.3 Červi

Pracují na nižší síťové vrstvě a nešíří se formou souborů, jako většina virů, ale formou paketů. Z infikovaného systému jsou rozesíláni červi na náhodně nebo podle určitého klíče vybrané IP adresy. Když dorazí paket od vybrané IP adresy se specifickou bezpečností dírou, může dojít k infiltraci a následnému dalšímu šíření červa. Tento druh infiltrace teda využívá nedokonalosti systému.

3.2.3 Antivirový program

Antivirový program je nejčastější ochranou počítače před možnou infiltrací. Jedná se software, který není součástí operačního systému Windows a je tedy nutné software doinstalovat. Máme dvě možnosti na výběr a to software stáhnout na internetu jako free verzi, nebo si program zakoupit.

Free verze programu bývá většinou zaměřena čistě na ochranu před viry a nenabízí již žádné další doplňkové verze. Mnohdy ani nestahuje aktualizace, potřebné pro ochranu před aktuálními viry. Od placené se též může lišit v počtu zachycených hrozeb. Porovnání placených a free verzí softwaru uvedu v níže uvedeném nezávislém testu.

Placené verze programu jsou většinou již v základu spojeny s nějakou doplňující funkcí, jako jsou firewally, antispam, antispyware a podobně. Licence se kupují buďto na dobu určitou nebo neurčitou a v případě že zabezpečujeme počítačovou síť, je potřeba nakoupit licence pro odpovídající počet PC v síti.

3.2.3.1 Test antivirových programů

V této kapitole uvedu nezávislý test placených antivirových programů.

Test provedl server http://www.antivirovecentrum.cz a je ze dne 23. 9. 2009

Antivirový program	Počet testů	Neúspěšný	Úspěšný	Procento úspěšnosti
ESET (NOD32)	63	3	60	95,3 %
Symantec Norton	59	7	52	88,2 %
Avira	25	5	20	80,0 %
Kaspersky	67	17	50	74,7 %
Norman	62	19	43	69,4 %
CA eTrust	56	16	40	71,5 %
F-Secure Anti-Virus	54	15	39	72,3 %
BitDefender	29	9	20	69,0 %
McAfee	64	21	43	67,2 %
TrustPort	13	4	9	69,3 %
Avast!	57	23	34	59,7 %
AVG	52	22	30	57,7 %
Sophos	66	16	50	75.8 %
Rising	7	4	3	42,9 %
Microsoft ForeFront	11	0	11	100,0%
Fortinet	25	9	16	64,0 %
RedStone	6	2	4	66,7 %

Obrázek 23 *test antivirových programů [6]*

3.2.3.2 Funkce antivirového programu

Antivirový program jako nástroj pro odstranění nebo eliminaci škodlivého softwaru v PC pro správnou funkci využívá dvě metody.

1. Zkoumání struktury souborů na disku. Porovnává zkoumanou strukturu souboru se svou databází a hledá možné shody.
2. Zkoumání chování programů. Opět porovnává se svou databází funkce a chování programu za účelem zjištění, zda funkce neodpovídá některému ze zjištěných škodlivých softwarů.

K dosažení dlouhodobé kvality programu je potřeba jej pravidelně aktualizovat. Vývoj nových škodlivých softwarů je neustále expandující a proto i vývoj obrany proti nim musí být na stále se zrychlující úrovni. Pro správnou funkci programu musí tedy uživatel pravidelně stahovat aktualizace, databáze virů, aby byl chráněn proti nejnověji zjištěným virům. U některých free programů jsou tyto aktualizace prováděny formou nové verze programu. Ta ale nevychází dostatečně často, aby byla zajištěna nejvyšší ochrana. U placených antivirových programů se aktualizace databáze vydávají z pravidla minimálně 1x denně.

Pokud se infikovaný soubor dostane na disk a databáze antivirového programu je dostatečně aktuální, má antivirový program několik možností co s infikovaným souborem udělat:

1. Pokusit se opravit/vyléčit soubor odstraněním viru ze souboru (pokud je to technicky možné)
2. Umístit soubor do karantény (virus se dále nemůže šířit, protože ho nelze dále používat)
3. Smazat infikovaný soubor (i s virem)

3.3 Ochrana před nechtěnými operacemi v PC

3.3.1 Úvod

Při zabezpečování počítačových sítí a PC nesmíme zapomenout na možnost, kdy potencionální útočník může být samotný uživatel PC. Při práci na PC může dojít k situaci, kdy uživatel nechtěně vykoná operaci, která může jeho data nějakým způsobem ohrozit. V této kapitole se budeme zabývat pouze typem operace, kdy může dojít vlivem nastavení systému k možnému ohrožení PC nebo celé sítě. Nebudeme tedy v této kapitole věnovat pozornost nechtěnému smazání dat. To bude řešeno v samostatné kapitole. K zabránění

nechtěnému nastavení nebo k operacím jejich důsledkem by mohlo být oslabení bezpečnosti systému. Existuje mnoho softwaru, který varuje uživatele před možným rizikem. Budeme se ale zabývat pouze integrovanými funkcemi v operačním systému Windows.

3.3.2 Řízení uživatelských účtů

Jedná se o integrovanou funkci v operačním systému Windows, která má za úkol varovat uživatele před operací, která by mohla ohrozit bezpečný chod systému. Tuto funkci je možné vypnou, ale doporučuje se tak jen zkušeným uživatelům. Při zadání vykonání operace je uživatel upozorněn ikonou, dle nebezpečnosti operace. Ikony jsou uvedeny níže. U operací jejichž důsledek by mohl být velmi nebezpečný pro chod systému, může program vyžadovat administrátorské heslo.

1. K pokračování této akce potřebuje systém Windows vaše povolení.

Jedná se o funkci, kde není známo, že program neovlivní stav systému. Upozorňuje uživatele, aby si zkontroloval, že program je 100% důvěryhodný.

2. Neznámý program požaduje přístup k tomuto počítači.

Nepodařilo se ověřit platný podpis programu, což může znamenat hrozbu pro PC, kde se program spouští. Nemusí to ale znamenat 100% hrozbu, protože celá řada starších programů platný podpis neměla. Toto upozornění slouží k tomu, aby si uživatel ověřil, co opravdu spouští za program.

3. Program potřebuje vaše povolení, aby mohl pokračovat.

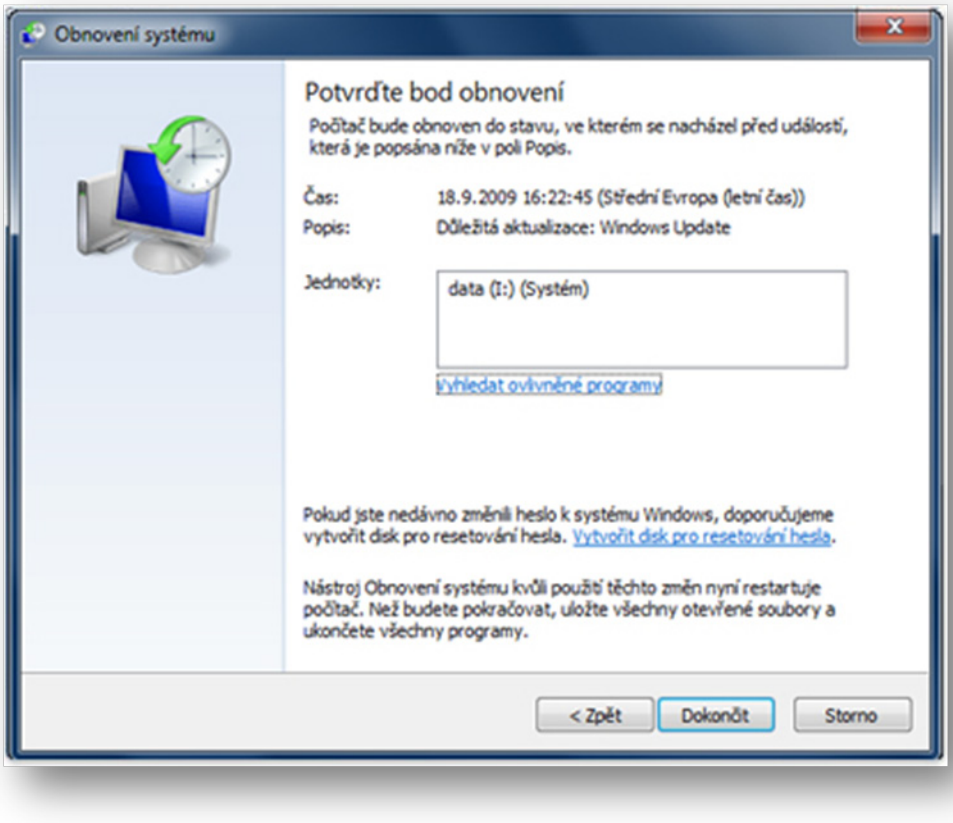
U programu se podařilo zjistit podpis a tím si uživatel může ověřit, že program je opravdu to, za co se vydává.

4. Tento program je blokován.

Tento program byl zablokován správcem systému. Pokud uživatel chce program spustit, musí kontaktovat správce, aby mu tento program odblokoval.

3.3.3 Obnovení systému

Jedná se funkci operačního systému Windows, která dokáže vrátit operační systém v čase. Program vytváří takzvané body obnovení, které se dle nastavení pravidelně vytváří. Obsahují informace o aktuálním nastavení systému. V případě že uživatel nechtěně nastaví, či jiným způsobem změní chod systému, může využít právě tuto funkci a vrátit nastavení do nejblíže vytvořeného bodu obnovení. Uživatelská data by měla zůstat nezměněná.



Obrázek 24 *okno programu obnovení systému*

3.4 Zálohování

3.4.1 Úvod

Při ochraně dat v PC nebo v síti je nedílnou součástí záloha dat. Možností jak nevratně přijít o data uložené na disku je mnoho. Pokud máme dobře nastavený systém zabezpečení, můžeme pominout možnost, kdy o data přijdeme vlivem neoprávněného vzdáleného přístupu nebo infiltrací dat. Ale stále zde zůstávají možnosti, kdy může dojít ke zničení disku a to díky blesku, nebo vadě při výrobě či stářím disku. Nesmíme zapomenout na možnost, že uživatel si data smaže sám. Zálohování můžeme provádět soukromně, kdy vlastníme diskové pole, na kterém se záloha provádí, nebo můžeme využít jednu z mnoha firem, které se zálohováním dat zabývají. Rozhodnutí je na nás, zda investujeme do koupě diskového pole nebo se uvážeme pravidelně platit za tuto službu.

Shrneme si tedy důvody proč zálohovat data, jaké hrozby mohou nastat a vlivem koho vznikly:

1. Vliv lidského faktoru: neúmyslné smazání či špatná manipulace, nedbalost.
2. Vliv chybného systému: výpadky napětí nebo operačního systému, selháním pevných disků, zničení vlivem programové chyby.
3. Vlivem úmyslného zničení: sabotáž, infiltrace, krádež.
4. Vliv fyzikálního jevu: požár, voda, blesk.

3.4.2 Zálohovací média

V této kapitole bude rozebráno, jaké typy médií můžeme při zálohování používat.

1. Optická média: CD a DVD nosiče mají již svou historii, ale stále patří ke kvalitním druhům nosičů, které se používají na zálohování dat. Při výběru média máme možnost zvolit z mnoha výrobců, avšak se doporučují spíše renomovaní výrobci. Záloha se provádí tak, že vybereme data, která chceme zálohovat a jednoduše zapíšeme pomocí mechaniky na nosič. Při archivaci nosičů je potřeba dodržovat několik podmínek od výrobce, jako je teplota, vlhkost nebo úrovně slunečního záření. Při dodržení těchto podmínek máme jistotu uložení dat až na 10 let. Při archivaci těchto nosičů je tedy nutné dodržovat tyto pravidla daná výrobcem. Při nedodržení podmínek mají tyto nosiče velmi krátkou odolnost, což je nevýhoda.

Výhodou je však jejich nízká pořizovací cena. Dnes již můžeme využívat i novější typy nosičů jako jsou BlueRay nebo HD DVD.

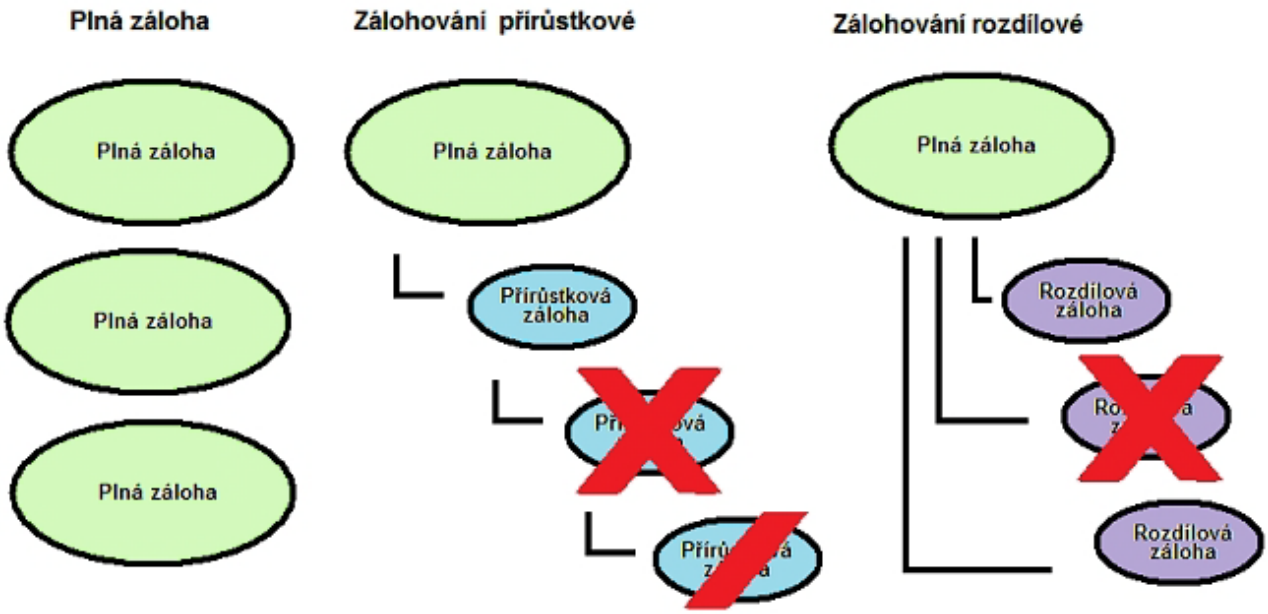
2. Pevné disky: jedná se o nezbytnou součást počítače. Je možno dokoupit další externí nebo interní disky pro zálohu dat. Toto řešení nabízí dobrý poměr mezi cenou a velikostí paměti. Nevýhodou je možné selhání disku.
3. NAS: zařízení NAS (Network Attached Storage) je typ zálohovacího média, které se zapojuje přímo do sítě, a po správné konfiguraci se již nemusíme starat o zálohování. Zařízení je plně automatické. Komunikace se zařízením probíhá na bázi protokolu TPC/IP. Konektivita může být jak USB, tak i LAN nebo WLAN.
4. Paměťové karty, flash disky: pokud se rozhodneme použít jako zálohovací médium flash disk nebo paměťovou kartu, zjistíme, že nákupní cena těchto médií je poměrně nízká vzhledem k jejich kapacitě. Ovšem jako zálohovací média nejsou vhodné z důvodu lehké zranitelnosti uložených dat. O data můžeme například přijít při malém výboji elektrostatické elektřiny. Ke krátkodobé záloze můžeme tyto média použít.
5. Záloha na FTP server: je realizována pomocí protokolu FTP (File Transfer Protocol), který vychází z klasického TPC/IP protokolu. Slouží pouze k výměně souborů mezi počítači. Existuje celá řada možností FTP serverů. Nejjednodušší typy nejsou příliš bezpečné, protože komunikace není zabezpečena. Přidávají se k tomuto protokolu různé firewally a komunikace se různě šifruje pro zvýšení bezpečnosti. Tento způsob zálohy je spíše vhodný pro skupinu. Pro jedno PC tento způsob zálohy není tolik vhodný.

3.4.3 Metody zálohování

V této kapitole bude uvedeno několik základních metod, jakými lze provádět zálohu dat.

1. Plná záloha: tento způsob zálohy pracuje na principu, že při každé záloze se zálohují všechna data. Tato metoda je nevýhodná z hlediska náročnosti využitého místa. Naopak je zde jistota uchování všech našich dat.

2. Přírůstková záloha: vytvoří se plná záloha a následující zálohy se provádí pouze u souborů, které byly vytvořeny od poslední plné zálohy. Získáváme tak plnou záloh + přírůstky. Vzniká nám tak odpad v podobě neaktualizovaných souborů.
3. Rozdílová záloha: tato metoda se řadí jako nejlepší. Nejdříve se opět udělá plná záloha a dále už jen změněné nebo nově vytvořené soubory. Oproti předchozí metodě máme výhodu v tom, že při zálohování touto metodou máme kompletní zálohu pospolu a ne rozdělenou na přírůstky a plnou zálohu.



Obrázek 25 *metody zálohování*

Na obrázku je znázorněno riziko, kdy dojde ke smazání jednoho z přírůstků. Při použití přírůstkové metody není možnost přečíst třetí přírůstek, pokud dojde ke smazání druhého přírůstku. Kdežto u rozdílové zálohy jsou přírůstky dělány nezávisle na předešlých.

Jako zvýšení bezpečnosti zálohy se využívá takzvaného zrcadlení.

Metoda zrcadlení disků je založena na zastupitelnosti disků - tzn. na udržování dvou identických kopií dat na dvou či více discích. V případě výpadku jednoho z nich pak bez problému počítač pracuje dál se zbývající kopií. Doba, po kterou jsou data nedostupná, je prakticky nulová. V případě výpadku jednoho z disků stačí vadný disk vyměnit za nový a po opětovném zapojení dojde k automatické synchronizaci a obnově dat ze zbylého disku

na nový prázdný disk. Nevýhodou zrcadlení jsou pořizovací náklady - při použití dvou disků dvojnásobné.

Při velkých objemech dat je lepší využít technologie RAID (Redundant Array of Inexpensive Disks) - skupina třech a více disků. Zjednodušeně lze říci, že data jsou v tomto případě rovnoměrně rozdělena mezi všechny disky. Jejich kapacita je tedy využita efektivněji než při pouhém zrcadlení. Tím klesají i náklady na reálnou diskovou kapacitu. Výpadek jednoho disku pak opět neznamená nedostupnost dat. Další vlastností RAID je větší rychlost zápisu dat oproti zrcadlení

4 ZABEZPEČENÍ NEOPRÁVNĚNÉHO LOKÁLNÍHO PŘÍSTUPU

4.1 Úvod do tématu

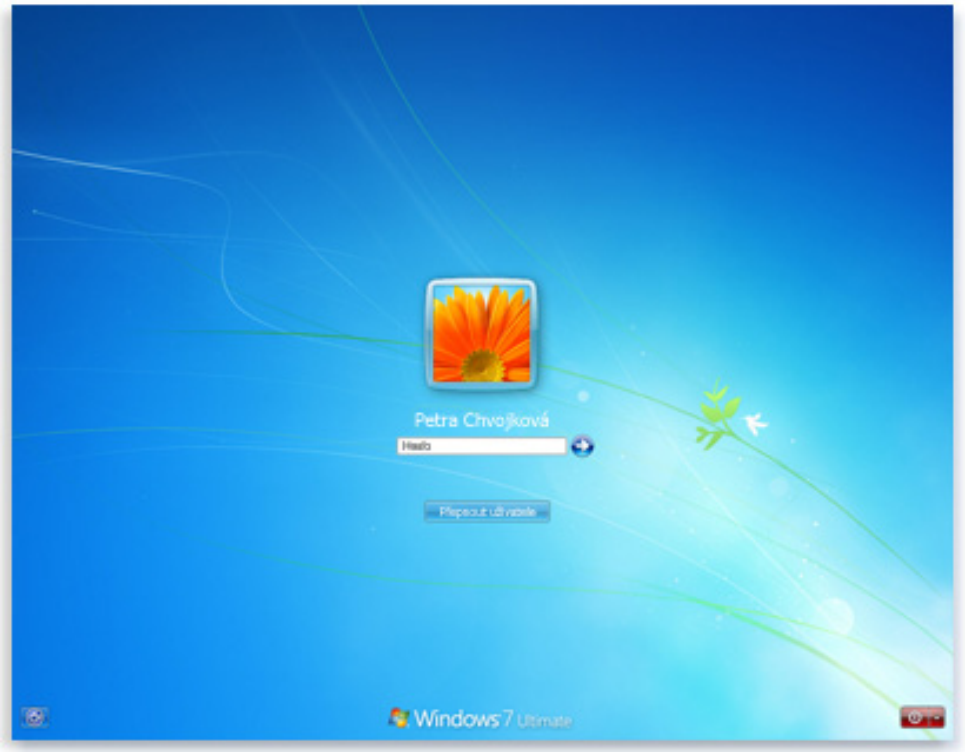
Doposud jsme se zabývali všemi možnými typy útoků na LAN, ale podstatnou součástí při tvorbě kvalitního zabezpečení lokální sítě je i ochrana proti lokálnímu útoku. Pokud nebudeme brát v potaz zabezpečení objektu, kde se daná LAN nachází, zůstává několik faktorů, které je potřeba zahrnout pro správné nastavení zabezpečení sítě. Řešení této problematiky spočívá ve správě uživatelů v síti. Tato problematika je řešena uživatelskými účty a přístupy do nich. Rozebrání hesel a jejich prolomení a další možnosti přístupu do účtu.

4.2 Uživatelské účty

Řízení přístupů uživatelů do sítě je realizováno vytvářením uživatelských účtů. V podstatě jde o to, že se určí jeden či více administrátorů sítě, kteří mají přístup do celého systému a sítě. Jejich úkolem je správné nastavení sítě, firewallu, správa dat a zálohování, obsluha softwaru pro zabezpečení. Jejich úkolem je též vytváření uživatelských účtů. Každý uživatel, který bude mít přístup do sítě, musí mít vytvořený svůj uživatelský účet.

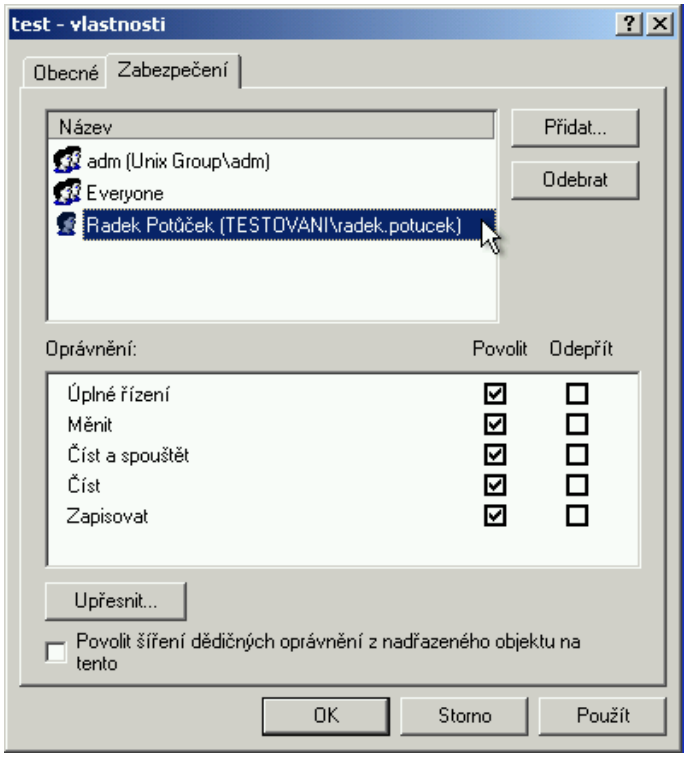
Možnosti nastavení práv v uživatelských účtech:

- Heslo a uživatelské jméno
- Jaké programy může daný uživatel obsluhovat
- Jaké nastavení systému je uživateli povoleno
- Které data uživatel může:
  - Úplně řídit
  - Měnit
  - Číst
- Popřípadě v jakém rozsahu může uživatel programy využívat
- Jaké disky uživatel může využívat
- Zda může instalovat programy



Obrázek 26 *přihlašovací obrazovka Windows*

Pro správu uživatelů v síti se uživatelské účty ve Windows příliš nepoužívají. Spíše se využívá specializovaného softwaru, jako je například Novell.



Obrázek 27 *nastavení práv uživatelů*

4.3 Hesla

Přístupy do uživatelských účtů nebo na PC jsou řízeny pomocí hesel. Hesla si uživatel vytváří sám nebo pomocí specializovaného softwaru. Heslo by měl znát pouze samotný uživatel, popřípadě správce sítě. Délka hesla by měla být minimálně 16 znaků, v kombinaci písmen, číslic a speciálních znaků. Nemělo by se jednat o obecně známé slovo, jako jsou přezdívky, jména manželů/manželek nebo obecná hesla jako je 1234 a podobně. Hesla by neměl mít uživatel stejná do více přihlašovacích účtů, jako je email, nebo komunikační programy. Je doporučeno pravidelně hesla měnit. Někdy se u správy uživatelů v síti dělá zvýšení bezpečnosti tak, že administrátor celé sítě nastaví, aby byl každý uživatel po X dnech vyzván k nastavení nového hesla. Hesla se mohou opakovat například až po třetím změnění.

4.3.1 BIOS heslo

Tento typ hesla se nastavuje v prvotním programu PC. Jeho prolomení je však vcelku snadná záležitost. Stačí resetovat BIOS, což se provádí odpojením od napájení a vyndání záložní baterie na základní desce.

4.3.2 Heslo ve Windows

Heslo se nastavuje k uživatelskému účtu. Uživatelský účet bude obsahovat uživatelské přihlašovací jméno a heslo + nastavení účtu (viz výše uvedené nastavení). Prolomení těchto hesel též není složité. Průměrně znalý uživatel je schopen prolomit toto heslo do několika minut. Záleží také na složitosti hesla. Prolomení se provádí pomocí specializovaného softwaru, který se spouští bootováním a poté se heslo zjišťuje z registru. Takovýto software i s návodem na obsluhu je volně ke stažení na internetu. Bezpečnost tohoto hesla tedy závisí na jeho složitosti. Ale i složitá hesla se dají po čase prolomit.

4.4 Tokeny

Token je speciální zařízení, které se využívá pro přístup do systému. Jedná se o speciální flash disk, který obsahuje identický klíč. Využívá se v kombinaci s heslem pro zvýšení bezpečnosti. Pro přístup do systému je potřeba mít vložený token v USB a zadat vygenerované nebo uživatelem zadané heslo. Nevýhoda je, že uživatel musí mít token vždy při sobě a je potřeba zajistit, aby nedošlo k jeho odcizení. Další nevýhoda nastává

v případě připojení tokenu při práci na PC. Může nastat situace, že v PC bude škodlivý software, který přečte identický klíč uložený na tokenu a takto přečtený klíč snadno zálohovat. Takto zálohovaný klíč je snadno zneužitelný a token ztrácí svou účinnost.

Obrázek 28 *token*

4.5 Biometrické snímače

Biometrické snímače jsou další možností, jak kontrolovat přístupy do systému. U některých notebooků se tyto snímače dodávají již v základní výbavě. Nejčastěji se jedná o snímače otisků prstů. Dají se využít i snímače rohovky a podobně. Tyto metody jsou však v praxi velice vzácné. Jejich nevýhodou je, že může dojít k poškození snímané části. Využívají se opět v kombinaci s heslem. Uložená předloha se zálohuje na pevném disku nebo na tokenu. Výhodou je identita.

Obrázek 29 *čtečka otisků prstů*

II. PRAKTICKÁ ČÁST

5 SOUHRNÉ INFORMACE

5.1 Informace o firmě

Pro vytvoření modelu zabezpečení sítě pro firmu je potřeba vytvořit fiktivní firmu. Firma nese název XXX. Jedná se o malou firmu podnikající v oblasti distribuce náplní do tiskáren. Orientují se na distribuci náplní hlavně pro firmy, ale na firmě je i obchod, který je určen pro obyčejné zákazníky. Firma má celkem 9 zaměstnanců a to ve složení: 3 jednatelé, 1 účetní, 3 obchodníci, 1 prodavač na prodejně a 1 řidič. Pro plnění svých pracovních povinností každý z nich potřebuje PC. Firma se nachází ve druhém patře budovy, ve které se nachází další firmy. Naše firma má v objektu 6 místností + toalety. Rozmístění místností je v příloze číslo 1 a užité místnosti firmy jsou ohraničeny červeně.

Čísla a využití místností:

2.08 - kancelář jednatelů

2.09 - kancelář obchodníků

2.10 - kancelář účetní a řidiče

2.13 - kuchyňka

2.14 - prodejna + sklad

2.15 - jednací místnost

5.2 Zadání zakázky

Pro zhotovení návrhu sítě bude potřeba několik informací. Uvažujme, že na vytvoření sítě je neomezený rozpočet, přičemž náklady na zhotovení by měly odpovídat velikosti firmy. Každý ze zaměstnanců bude využívat PC. Řidič, obchodníci, prodavač na prodejně a účetní budou mít stolní PC. Jednatelé budou využívat notebooky. Je tedy potřeba vyřešit připojení do sítě jak drátové, tak i bezdrátové. Celá síť bude připojena k internetu. Na serveru budou uložena data, přičemž jejich vyzrazení by mohlo mít likvidační dopad pro firmu. Ztráta dat by nemusela znamenat jistou likvidaci firmy, ale přesto si zákazník přeje jistou formu zálohy. Každý ze zaměstnanců připojených do sítě

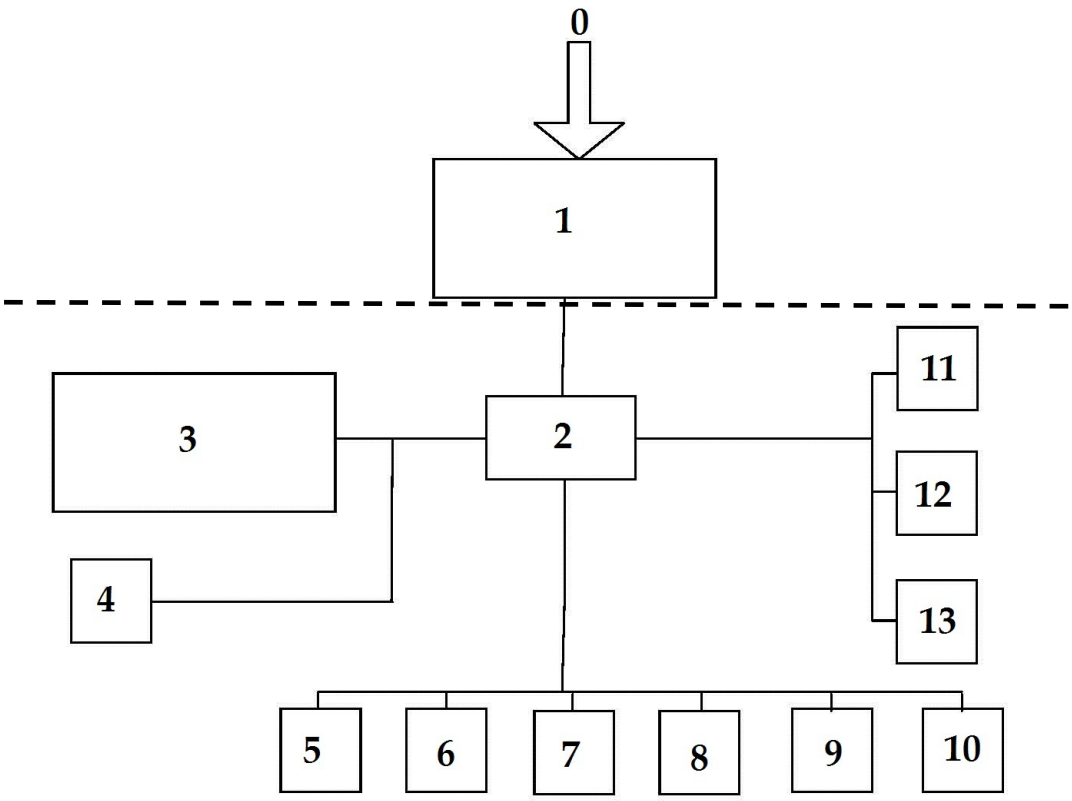
bude mít jiná práva, ať už v nahlížení do dokumentů uložených v síti, tak i v práci s nimi. Jednatelé se pohybují mezi novými zákazníky a potřebují se připojovat vzdáleně do sítě. Jednatelé se také potřebují pohybovat s notebookem po firmě. V síti by měly být dvě tiskárny.

5.3 Shrnutí požadavků a zhodnocení rizik

1) Síť je připojena k internetu, bude tedy potřeba vyřešit problém s neoprávněným vzdáleným přístupem, s infiltracemi, které hrozí při prohlížení webových stránek.
2) Jednatelé se připojují vzdáleně, je tedy potřeba vyřešit vzdálený přístup a jeho zabezpečení proti odposlechu.
3) Pohyb jednatelů s notebookem po firmě bude jednoduší s bezdrátovým připojením do sítě. Hrozí zde však riziko nepovoleného přístupu do sítě.
4) Zákazník požaduje zálohu dat. Jelikož se jedná o malou firmu, nebude potřeba volit drahé řešení od různých výrobců, postačí pouze zálohovací disk.
5) Je potřeba vyřešit ochranu serveru před přepětím.
6) Zaměstnanci budou mít odlišná práva v sítí. Problém se správou uživatelských účtů.
7) Připojení tiskáren do sítě neobnáší žádné riziko.

6 NÁVRH SÍTĚ

6.1 Blokové schéma



Obrázek 30 *blokové schéma návrhu sítě*

0 - WAN (vnější síť)

1- Router

2 - Switch

3 - Server

4 - Záložní disk

5 - PC1

6 - PC2

7 - PC3

8 - PC4

9 - PC5

10 - PC6

11 - Access point

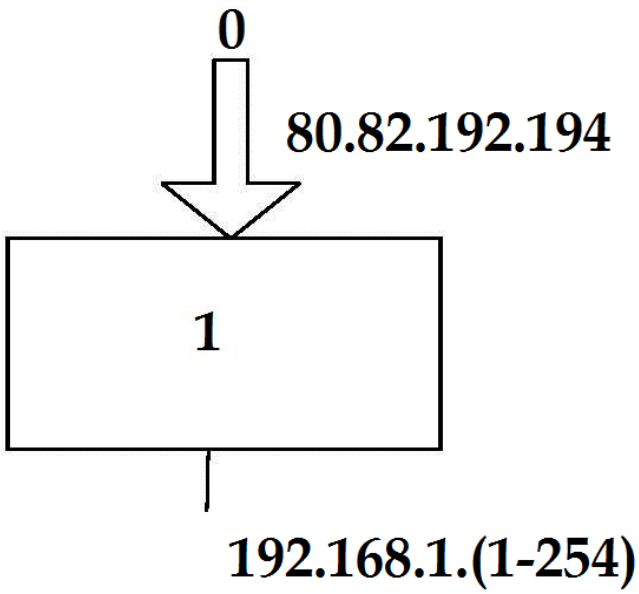
12 - Tiskárna

13 - Tiskárna

6.2 Použité prvky

6.2.1 Router

V blokovém schématu můžeme vidět, že router odděluje naši lokální síť od vnější (wan). Je tedy nepostradatelným prvkem při návrhu sítě. Router by měl obsahovat hardwarový firewall pro kontrolu datového spojení mezi vnitřní a vnější sítí. Na začátku routeru budeme mít veřejnou IP adresu, kterou nám poskytovatel přidělí. Po oddělení sítě již budeme mít IP adresy dle nastavení. Toto můžeme vidět na obrázku 31. Veřejná IP adresa je smyšlená, adresy vnitřní sítě volíme dle svého uvážení. Pro svůj návrh jsem zvolil rozsah IP adres 192.168.1.0 – 192:168.1.254

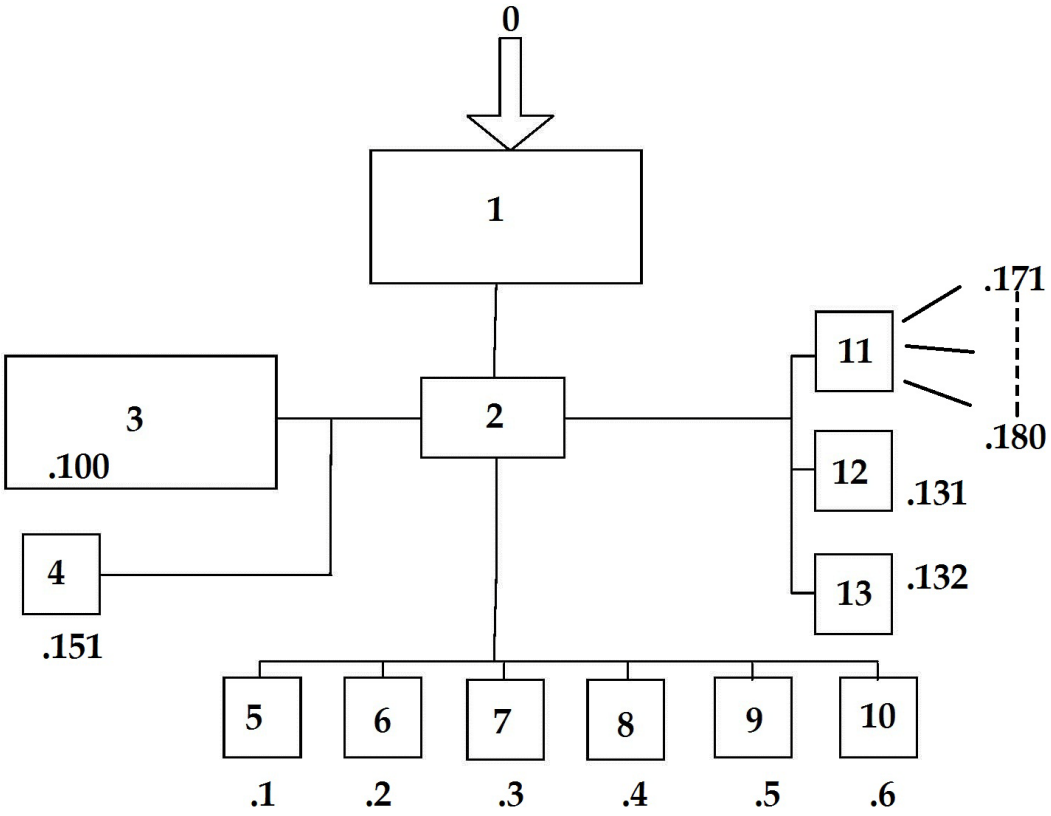


Obrázek 31 *router- oddělení sítí*

Další hodnoty, které se na routeru nastaví, jsou takzvané Dynamic Host Configuration Protocol (DHCP). Jedná se o aplikační protokol, který se používá pro automatické přidělování adres. Ve své podstatě je při použití DHCP síť přehlednější. Každý bod sítě bude mít svou přidělenou IP adresu. Hodnoty se musí samozřejmě nastavit i na zařízení. Ve finále může být vytvořen seznam IP adres, v našem případě v rozsahu 192.168.1.(0-254), a u každé použité adresy bude název zařízení, které má tuto adresu přidělenou. V případě že by se do sítě přidávaly další prvky, můžeme snadno v seznamu

přečíst volné IP adresy, které novému zařízení přidělíme. Takto vytvořený seznam je uveden v příloze číslo 2 – seznam přidělených IP adres.

Po přidělení IP adres by tedy naše síť mohla vypadat:



Obrázek 32 *schéma sítě po přidělení IP adres*

Na obrázku je vytvořený návrh sítě už po přidělení IP adres prvkům. Jsou uváděny, jen konečná čísla. Můžeme vidět, že pro přehlednost se například všem stolním PC přiřazují konečná čísla IP adres ihned ze začátku číselné stupnice. Prvky připojené bezdrátově k Access pointu dostanou konečné číslo IP adresy od 171 do 180. Tiskárny mají své místo na stupnici 130 – 140. Server 100.

Na routeru by se dále nastavovalo povolení pro vzdálené přístupy, ale k tomu se dostaneme přímo v kapitole, kde se budou řešit vzdálené přístupy.

Pro naši síť jsem vybral následující router.

Vigor 2950

Jedná se router od společnosti DrayTek.

Obrázek 33 *router vigor 2950*

Některé z parametrů:

Interface WAN: 10/100Mbit Cable/xDSL (RJ45)
Počet portů WAN: 2.00 ks
Počet portů LAN: 10/100 5.00 ks
Integrovaný přepínač [switch]: ano
Integrovaný modem ADSL: ne
Integrovaný acces point Wi-Fi: ne
Podpora VPN: ano

Ovládání

- Telnet
- Syslog
- WWW
- CLI

Cena routeru je k měsíci květen 2010 cca 10 000 Kč s DPH.

6.2.2 Switch

Toto zařízení má v síti za úkol propojit jednotlivé prvky. Může mít větší či menší počet portů. Také se rozlišuje, jakou nejvyšší možnou rychlostí může switch pracovat. Ještě můžeme switche rozdělit dle typu použité sítě. Ještě je potřeba si zjistit, kolik bude vlastně na swtich potřeba připojit zařízení.

Pro naši síť jsem zvolil switch typu:

D-LINK DGS- 1224T

Obrázek 34 *SWITCH DLIN DGS-1224T*

Některé z parametrů:

Rozšířená šířka pásma pro server a páteřní síť

Dva Combo porty pro Gigabit TP nebo Gigabit LX/SX přes Mini GBIC

Auto MDI/MDIX Uplink na každém portu

VLAN pro regulaci a bezpečnost toku dat a sdružování portů pro větší šířku pásma

Full-/Half-Duplex autonegotiation

Použití existujících měděných kabelů s kroucenými páry (Cat. 5e)

Bezproblémová integrace do existující infrastruktury sítě

Bezpečné Store-and-forward přepínání

Flow-Control proti ztrátám dat při přenosu

Podporovaná rychlost: 10/100/1000 Mbit/s

Jeho cena se k měsíci květen 2010 pohybuje cca 6 000 s DPH

6.2.3 Server

Zařízení, které v síti má za úkol sdílet tiskárny, sdílet data, ověřovat uživatele při vstupu do sítě. Dá se říct, že server je mozek celé sítě. Ve větších sítích jako je například internet může mít server za úkol uchovávat a sdílet data jako jsou například webové stránky. V naší síti má server za úkol uchovávat a sdílet příslušným uživatelům firemní data, ověřovat přístup uživatelů do sítě, sdílet tiskárny, popřípadě zajistit antivirovou ochranu. K této problematice se budeme věnovat v samostatné kapitole.

Nejprve rozebereme možnost správy uživatelů. Pro zajištění bezpečnosti dat v síti proti možnému lokálnímu útoku, budou mít uživatelé vytvořeny své uživatelské účty. V rámci bezpečnosti bude vytvořena doména. Uživatelům budou nadefinována jejich práva: kdo k jakým datům může nahlížet nebo je měnit, omezené možnosti instalace či prohlížení webových stránek. Uživatel se pak přihlašuje pod svým účtem do domény a správce tak získává plný přehled o uživatelích. Aby se uživatelé mohli připojit do domény, je potřeba používat operační systém, který připojení do domény podporuje. Byl to například operační systém Windows XP Professional nebo Windows 7 Professional.

Softwarové vybavení serveru je obdobné jako u klasického stolního PC. Server obsahuje operační systém, ve kterém už bývá obsažen firewall a základní software pro běh serveru. V našem případě tedy uvažujme, že na serveru bude potřeba operační systém a antivirový program.

Sdílení tiskáren a dalších komponentů již provede správce systému.

Zvolené komponenty:

TD200x

Jedná se o server od společnosti IBM.

Technické parametry:

Procesor: 1 x Intel® Xeon® E5520 processor (2.26 GHz, 8MB L3 Cache, 80W, DDR3-1066)

Paměť: 2 x 2 GB DDR3 1333MHz 1Rx4 RDIMM
Počet slotů**:** 16

RAID Options: 0,1,1E,5,6,10,50,60

Hard Disk
Typ: 2.5" Hot-Swap SATA/SAS
Počet volných slotů: 8

Optická mechanika: DVD RW
Ethernet: Dual Gigabit Ethernet (Integrated)
Diagnostika: LED
Zdroj: 2x920W Redundant

Cena k měsíci květen je cca 50 000 Kč s DPH

Obrázek 35 *server TD200x*

Lenovo 1 TB 7200 rpm SerialSATA HDD

Pevné disky pro server. Bude potřeba 6 disků. Jelikož zákazník požadoval zálohu dat, vybrali jsme server s možností zálohování. Typ zálohování bych zvolil RAID 1, což je klasické zrcadlení disků v poměru 1:1. To znamená, že data se zapisují na každý z disků. Pro systém budeme tedy potřebovat 2 disky a pro ostatní data 4. Získávám tím: 1 TB dat pro systém a 2 TB pro ostatní data.

Cena komponentu k měsíci květen 2010 cca 3 700 Kč s DPH.

V našem případě: 6 x 3 700 = 22 000 Kč s DPH.

Windows Server 2008 Standard

Operační systém pro server. Krabicová verze - CZ - (FPP). Licence není vázána na počítač, ke kterému byla zakoupena, na rozdíl od OEM, může se tudíž libovolně instalovat na jakýkoli počítač, ale vždy se musí využívat pouze tolik licencí současně (instalací), kolik jich je zakoupených.

Cena softwaru k měsíci květen 2010 cca 21 000 Kč s DPH.

6.2.4 PC1 – PC6

Stolní PC zaměstnanců. Do soupisky započítáme kompletní sestavu s monitorem a ovládacími prvky. K sestavám připočítáme i operační systém.

Nebudeme vybírat konkrétní sestavu, ale určíme si hranici 15 000 Kč s DPH na jedno PC. Při 6 PC se dostáváme na cenu 90 000 Kč S DPH.

Pokud bychom připočetli i 3 kusy notebooků pro jednatele, dostáváme se na cenu 135 000Kč s DPH.

6.2.5 Access point

Jedná se o aktivní síťový prvek, který má za úkol připojit do sítě bezdrátově další prvky. Pro naši síť je výhodou, pokud by jeden z jednatelů přecházel s notebookem do jiné místnosti, že je neustále připojen do sítě. Nevýhodou je však vzdálenost vysílaného signálu. Nedokážeme zabránit, aby Access point vysílal jen v našich místnostech a proto zde hrozí vážné riziko nabourání do sítě. Nastavením Access pointu získáme možnost šifrováním přenosu dat nebo zabezpečení přístupu dalším heslem. Je tedy potřeba vybrat odpovídající typ zabezpečení. Nejčastěji se používá typ zabezpečení WPA. Správným nastavením tedy získáme jistotu, že do sítě nebude připojen nežádoucí objekt.

Pro naši síť jsem vybral tento typ Access pointu:

DAP-1353 Wireless N Access Point

Přístupový bod D-Link **DAP-1353** z řady Wireless N je zařízení kompatibilní s návrhem normy 802.11n (draft), které umožňuje zvýšení přenosového výkonu až o 650 % - přenos je až 5× rychlejší než u bezdrátového spojení 802.11g a rychlejší než 100Mb/s

kabelový Ethernet1. Připojením přístupového bodu DAP-1353 k přepínači nebo směrovači budou uživatelé moci sdílet svoje vysokorychlostní připojení k Internetu s kýmkoli v síti a vytvořit bezpečnou bezdrátovou síť pro sdílení fotografií, souborů, hudby, videa, tiskáren a síťových úložišť dat v celém domě nebo kanceláři.

Technické parametry:

LAN: 1x 10/100
Norma IEEE: IEEE 802.11b/g/n
USB: ne
Zabezpečení: WEP/WPA/WPA2
Datová propustnost: 300 Mbps
Konektor ext. antény: RSMA female
VoIP: ne
Napájení: 5VDC 3A
Rozměry: 198 x 120 x 32 mm
Frekvence: 2,4 GHz
Operační mód: AP/client/WDS/repeater
Výstup na ext. anténu: RSMA male
WAN/WLAN: ano

Obrázek 36 *DAP-1353 Wireless N Access Point*

Cena produktu k měsíci květen 2010 je cca 3 300 Kč s DPH

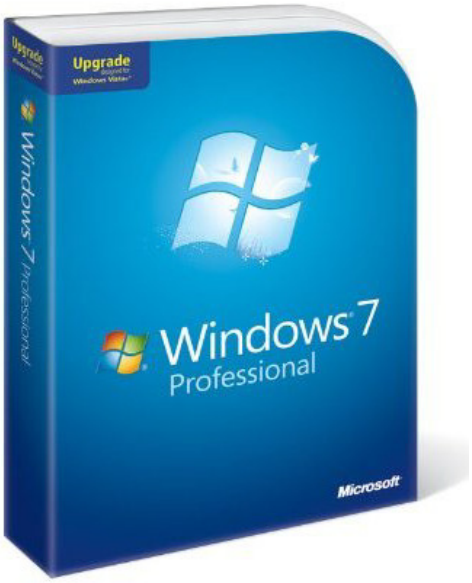
6.2.6 Tiskárny

Je potřeba vybrat takové zařízení, aby jej bylo možné připojit do sítě. Pro rychlost a kvalitu tisku bych volil spíše laserovou tiskárnu, než inkoustovou. Cena běžné laserové tiskárny se pohybuje okolo 4 000. Zvolme tedy pro naši firmu pouze orientační zařízení v ceně 4 000 Kč s DPH. Pro naši firmu budeme potřebovat 2 taková zařízení. Celkové náklady tedy budou 2 x 4 000 = 8 000 Kč s DPH

6.2.7 Doplňkový software

Windows 7 Professional

Operační systém pro PC a notebooky. Vyznačuje se svou stabilitou a nenáročností pro hardware počítače. Jeho součástí je již základní firewall, který chrání PC na kterém je systém nainstalován.



Cena produktu je k měsíci květen 2010 cca 3 500 Kč S DPH. Jedná se ale pouze o 1 licenci. Pro náš případ je potřeba zakoupit 6 ks licencí pro stolní PC a 3 ks licencí pro notebooky.

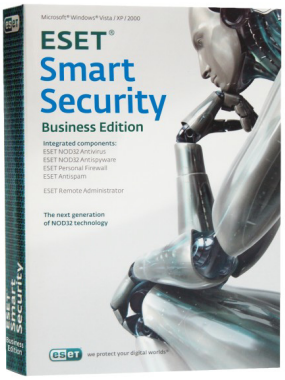
Celková kalkulace je tedy:

9 x 3 500 = 31 500 Kč

Obrázek 37*Windows Professional*

ESET Smart Security Business Edition

Antivirový systém určený pro firmy. Je určen pro PC.



Cena tohoto produktu k měsíci květen 2010 je:

5-10 PC:

1 235Kč na rok,

1 853Kč na 2 roky.

864Kč prodloužení rok

1 556Kč prodloužení na 2 roky

Obrázek 38 *eset smart security*

ESET NOD32 Antivirus pro Windows File Server

Antivirový systém pro servery. Ideální v kombinaci s antivirovým systémem eset na PC.

Ceník:

Licence na rok: 4 147Kč

Licence na 2 roky: 6 346Kč

Prodloužení licence na rok: 2 832Kč

Prodloužení licence na 2 roky: 5 290Kč

Obrázek 39 *eset Nod32 Windows file server*

6.2.8 Doplňkové zařízení

V doplňkových zařízeních lze uvést další prvky sítě, které nemusíme zákonitě použít, ale jejich použití může být ke zlepšení celkové bezpečnosti sítě. Jedná se hlavně o: přepěťové ochrany, zálohovací zdroje, zálohovací disky.

Tyto zařízení již do kalkulace sítě přidávat nebudu.

6.3 Řešení vzdálených přístupů

Jeden ze zákazníkových požadavků byl vzdálený přístup do sítě. Tato problematika je poměrně složitá na řešení, hlavně co se týče správné konfigurace hardwaru a softwaru. Pokud zabezpečujeme síť proti neoprávněnému přístupu, použijeme nejčastěji firewall. Jak již bylo řečeno, firewall může být jak hardwarového, tak i softwarového typu. Softwarové typy jsou již obsaženy v operačních systémech. Hardwarové typy jsou obsaženy například v routerech. Zde nastává již zmíněný problém s konfigurací. Hardwarové firewally bývají obtížné pro nastavení. Nastavit absolutní zákaz nevyžádaného přístupu není až tak složité nastavení, ale nastává problém v případě, že udělujeme výjimku určitému softwaru či uživateli.

Vzdálené přístupy budeme tedy řešit dvěma způsoby:

1. Vzdálenou plochou
2. VNC, či obdobný program

6.3.1 Vzdálený přístup pomocí vzdálené plochy

Tuto metodu můžeme využívat při vzdáleném přístupu. Jedná se celkem o bezpečnou metodu z důvodu šifrovaného přenosu. Pro správnou funkci musí být nakonfigurovaný router. Nastavení bude následující: připojení přes port 3389 směrovat na adresu 192.168.1.100. Při zadání veřejné IP adresy mě router přesměruje přímo na server, kde se ověří příslušný uživatel sítě. Pokud by se uživatel chtěl připojit přímo na své PC, je možná konfigurace routeru a zadání IP adresy by vypadalo následovně: veřejná IP:X3389 kde X je konečné číslo IP zařízení, na nějž se chceme připojit a 3389 je číslo portu vzdálené plochy.

6.3.2 Vzdálený přístup pomocí VNC

Metoda pracuje na podobném principu jako předchozí. Mění se zde čísla portů a bezpečnost přenosu. Jak bylo uvedeno v kapitole o vzdálených přístupech, metoda vzdáleného připojení pomocí programu VNC není příliš bezpečná, jelikož přenos dat není nijak šifrován. Pro zvýšení bezpečnosti se používají VPN tunely. Volba metody a správné nastavení VPN tunelu je na správci sítě, který ji bude konfigurovat. Pro tunelování můžeme použít dvě metody a to připojení na 2 hardwarové zařízení nebo 2 softwarová zařízení. V našem případě můžeme využít obou těchto metod, jelikož jsme použili router s podporou VPN. Abychom tedy správně tunelovali, museli bychom přistupovat vzdáleně ze zařízení, které podporuje VPN. Softwarové tunelování je též použitelné, z důvodu že jsme použili operační systémy, které tunelování podporují.

7 KONEČNÉ SHRNUTÍ

7.1 Dodržení požadavků

Pro přehlednost ještě jednou uvádím seznam požadavků zákazníka. Dále bude komentář, jakým způsobem se jednotlivé požadavky řešili.

- Síť bude připojena k internetu
- Potřeba vzdáleného přístupu
- Správa uživatelů v síti
- Bezdrátové připojení pro notebooky
- Ochrana dat zálohováním
- Ochrana proti přepětí
- Ochrana dat před neoprávněným lokálním a vzdáleným přístupem
- Celkové ochránění dat proti zničení

Síť bude připojena k internetu. Oddělení sítí bude zprostředkovávat router špičkové kvality, který postaví nepropustnou zeď mezi vnější a vnitřní sítí. Je tak zaručena ochrana proti neoprávněnému vzdálenému přístupu. Dále k zajištění ochrany před neoprávněným vzdáleným přístupem slouží operační systémy, které již v sobě mají integrovány další firewally. Operační systémy byly voleny tak, aby měly co největší kompatibilitu s dnešními programy a pro uživatele co nejjednodušší ovládání. Přes svou jednoduchost jsou velice stabilní. Nastavení domény a vytvoření uživatelských účtů s různými právy zajišťuje správu uživatelů v sítí a dokonalý přehled o uživatelských právech. Rozdělením práv uživatelů a vytvořením uživatelských účtů, získáváme ochranu proti neoprávněnému lokálnímu útoku nebo ztrátě dat vinou zaměstnance. Volbou vhodného a velmi výkonného serveru je zajištěna celková stabilita sítě. Na serveru je také nastavena záloha dat podle RAID 1 a tím je zajištěna ochrana dat v případě nečekaného selhání jednoho z disků. Ke zvýšení rychlosti celé sítě nepřispívá jen server, ale i gigabitový switch. K přístupu do sítě bezdrátově nám poslouží Access point, který je na velmi dobré úrovni, co se týče své rychlosti. Zabezpečením přenosu a přístupu do něj získáme pohodlný přístup do sítě z notebooku. Pro bezpečnost proti přepěťové ochraně má zákazník možnost dokoupit jednu z mnoha přepěťových ochran. Celkovou bezpečnost dat proti napadení nějaké infiltrace

nám zajišťuje vysoce spolehlivý antivirový systém. Kombinací pro server a pro PC tak máme zaručenu vysokou odolnost proti těmto hrozbám.

7.2 Cenová kalkulace

Hardware:

Typ hardwaru	Počet	Cena 1 kusu [Kč]	Celková cena [Kč]
DrayTek Vigor 2950	1	10 000	10 000
D-LINK DGS- 1224T	1	6 000	6 000
TD200x	1	50 000	50 000
Lenovo 1 TB 7200 rpm SerialSATA HDD	6	3 700	22 000
D-Link DAP-1353	1	3 300	3 300
Tiskárny	2	4 000	8 000
PC	9	15 000	130 000
Celkem:			229 300

Tabulka 1 *cenová kalkulace hardwaru*

Kalkulace softwaru

Název softwaru	Počet	Cena 1 KS [Kč]	Celková cena [Kč]
Windows Server 2008 Standard		21 000	21 000
Windows 7 Professional	9	3 500	31 500
ESET Smart Security Business Edition	1	1 235	1 235
ESET NOD32 Antivirus pro Windows File Server	1	4 147	4147
Celkem			57 882

Tabulka 2 *cenová kalkulace softwaru*

ZÁVĚR

Zabezpečení lokálních sítí je v dnešní době nezbytnou součástí pro miliony lidí, jelikož vytváření lokálních sítí není výsadou jen firem a institucí, ale i domácností. Každé propojení 2 a více PC vytváří síť. Čtenář by po přečtení této práce měl být seznámen se základními hrozbami, které mohou nastat při vlastnictví lokální sítě. V případě uskutečnění těchto hrozeb by mohly nastat nedozírné následky pro majitele sítě. Práce kromě seznámení se hrozbami poučuje čtenáře základními formami obrany proti těmto útokům. Jedná se o celosvětově používaná základní pravidla. Existuje spousta jiných metod, většinou se jedná o konkrétní řešení od konkrétních výrobců. Též rozlišujeme obranu dle používaného operačního systému. V práci jsou uvedeny metody základního běžně používaného typu, pro celosvětově známý operační systém Windows od firmy Microsoft. Tato práce je tedy předně určena pro běžně znalého uživatele, který má zájem, aby jeho data nebyla volně přístupná všem lépe orientovaným útočníkům v kyberprostoru. Pokud budeme uvažovat situaci, kdy je lokální síť připojena na nějakou vnější síť, hrozí vždy riziko prolomení zabezpečení sítě. Výše uvedené metody tedy slouží ke zmenšení rizika prolomení. Obsahem práce byl i praktický návrh sítě a jejího zabezpečení. Síť byla realizována pro menší smyšlenou firmu. I přes malý počet výpočetní techniky (9 PC) se cena takto realizovaného projektu vyšplhala ke 300 000 Kč. V projektu jsou aplikovány metody z teoretické části. Tento návrh se může zdát pro takto malou firmu zbytečně finančně náročný, avšak když se zamyslíme nad hodnotou dat, které budou na firemní síti, zjistíme, že investice do kvalitního projektu se vrací v podobě jistoty. Výběr komponentů byl čistě náhodný, nejedná se v žádném případě o reklamu či propagaci nějakého výrobku. Ceny byly určovány buďto z webových stránek výrobců, nebo byly zprůměrovány od několika prodejců. Možností pro výběr je mnohem víc.

ZÁVĚR V ANGLIČTINĚ

Today the local area networks (LAN) security is a necessary part for millions of people, because LAN creation is not a privilege only for companies and institutions, but also for households. Every connection of 2 and more PCs creates a network. After reading this work reader should be familiarized with the basic threats which may happen while having the LAN. If these threats come true, far-reaching consequences can happen to the network owner. Except the familiarization with threats the thesis indoctrinates readers with the basic form of defense against these attacks. Those are the worldwide used basic rules. There are many other methods, mostly the concrete solutions from the concrete makers. Also we discriminate defense according to used operating system. In this work, there are presented the methods of the basic commonly used type for the worldwide known Windows operating system made by Microsoft Company. So this work is in the first place addressed to a currently competent user, who is interested in not having free information for better oriented attackers in the cyberspace. If we think of a situation the LAN is connected to an external network, there is always a risk of breaking network security. So the above methods are instrumental to reduce the risk of breaking. The aim of this work was also to practically project a network and its security. The network has been implemented for a smaller fictive company. Despite few computer technology (9 PCs) the price of in this way implemented project climbed up to 300 000 CZK. In the project, there are applied the methods from the theoretical part. This design may seem for in this way small company unnecessarily expensive but if we think about an information value that will be on the corporate network, we make out the investment in the quality project returns like the safety. Selection of components was purely random, it is in no case some advertisement or promotion of a product. The prices were determined either from maker´s websites or by averaging from several dealers. There are much more options for the selection.

SEZNAM POUŽITÉ LITERATURY

Monografické publikace:

[1] ENDORF, Carl; SCHULTZ, Eugene; MELLANDER, Jim. Hacking - *detekce a prevence počítačového útoku*. 09/2005 . GRADA, 2005. 356 s. ISBN 80-247-1035-8.

[2] LUDVÍK, Miroslav; ŠTĚDROŇ, Bohumír. *Teorie bezpečnosti počítačových sítí*. ČR: computer Media, 2008. 98 s. ISBN 80-86686-35-3.

[3] GRYGAR, Josef . *Detekce a prevence počítačových útoků*. Zlín, 2007. 98 s. Diplomová práce. UTB Zlín.

WWW stránky:

[4] KOBEŠOVÁ, Lucie. Historie sítí v ČR. *Seminární práce* [online]. 2007, 1, [cit. 2010-05-06]. Dostupný z WWW: <http://home.zcu.cz/~kobesova/index.html>.

[5] Svět sítí & Infinity, a.s. *Svět sítí* [online]. 2000-2010 [cit. 2010-05-06]. Svět sítí. Dostupné z WWW: <http://www.svetsiti.cz/default.asp>.

[6] Amenit s.r.o. *Antivirové centrum* [online]. 1998 - 2010 [cit. 2010-05-06]. Antivirové centrum. Dostupné z WWW: <http://www.antivirovecentrum.cz/>.

SEZNAM POUŽITÝCH SYMBOLŮ A ZKRATEK

Bbs (*Bulletin Board System*) - systémem elektronických nástěnek, které jsou rozděleny podle témat, do kterých mohou uživatelé přispívat

Lan (L*ocal area network*) – lokální síť

Man (M*etropolitan area network*) – městská síť

Wan (W*ide area network*) – rozlehlá síť

Gan (*Global area network*) – globální síť

Pc (P*ersonal computer)* - osobní počítač

Tpc/Ip (*Transmission Control Protocol/Internet Protocol)* - primární transportní protokol /protokol síťové vrstvy

Vnc (*Virtual Network Computing)* – virtuální síťové řízení

Vpn (*Virtual private network)* – virtuální privátní síť

Rfb (R*emote framebuffer*) – vzdálená matice

Ssl (*Secure Sockets Layer*) - vrstva bezpečných socketů

Ssh (*Secure Shell)* – zabezpečený protokol

DQDB (*Distributed Queue Dual Bus)* – protokol používající sběrnicovou topologii

GRE *(Generic Routing Encapsulation)* – protokol určený k zabalení paketů

CIR *(Committed Information Rate)* – minimální průchodnost sítě

DE *(Discard Eligible*) – varování, že bylo překročeno CIR

ATM *(Asynchronous Transfer Mode)* – standart pro vysokorychlostní síťovou architekturu

CLP *(Cell Loss Prority)*- iznačení rámců při překročení rychlosti

VLAN *(Virtual LAN)* – bezdrátová síť

LANE *(LA N Emulation)* – emulovaná lokální síť

LES *(LAN emulation server)* -

IDS (Intrusion Detection Systems) – server v emulované síti

ACL (Access Control Lists) – seznam pro řízení přístupů

IOS *(Internetwork Operating System)* – operační systém používaný na směrovačích cisco

NAS *(Network Attached Storage)* – datové úložiště na síti

FTP *(File Transfer Protocol)* – protokol určený k přenosu dat

RAID *(Redundant Array of Inexpensive Disks)* – metoda zrcadlení (zálohování)

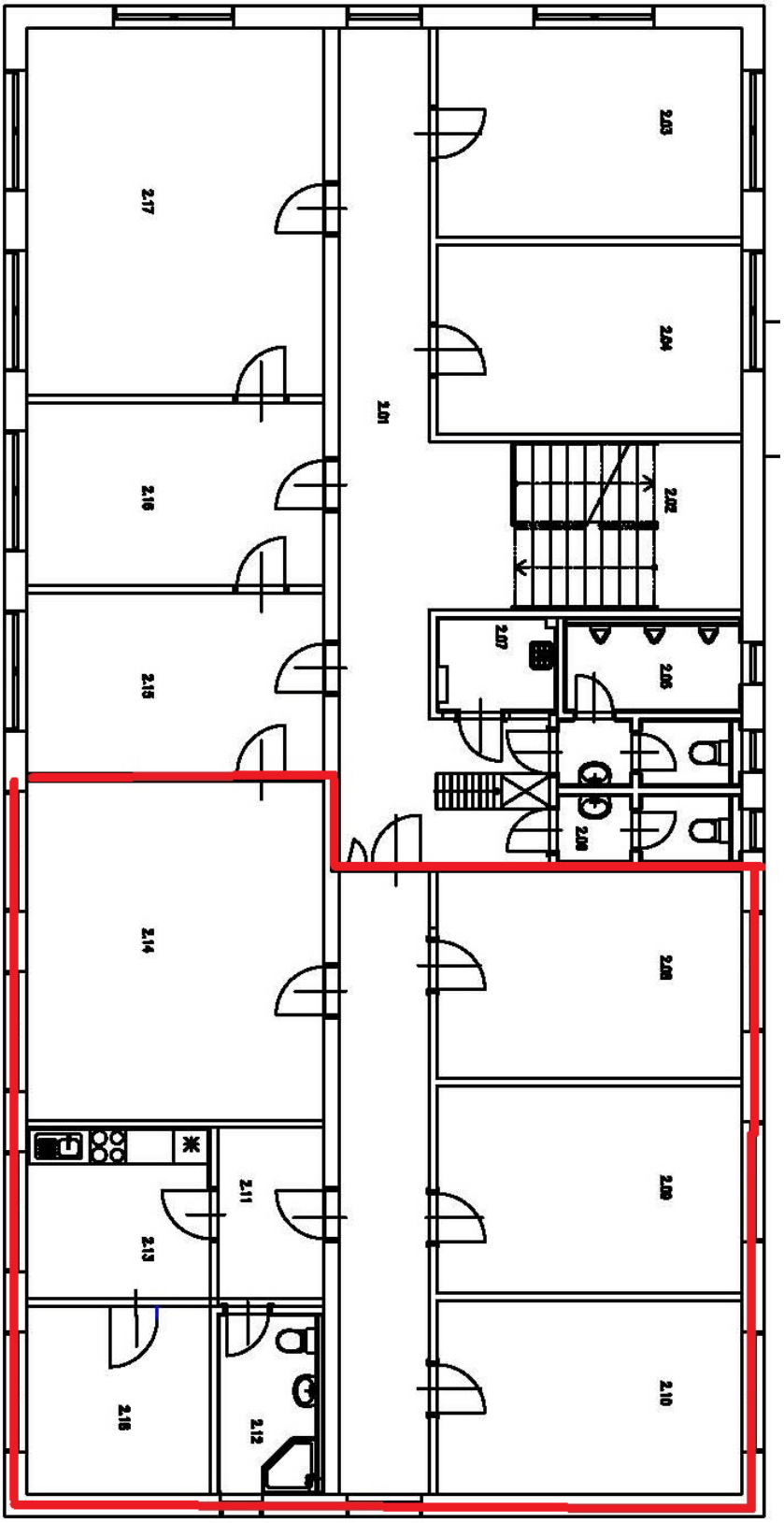
DHCP *(Dynamic Host Configuration Protocol)* – aplikační protokol

SEZNAM OBRÁZKŮ

SEZNAM TABULEK

SEZNAM PŘÍLOH

PŘÍLOHA 1: ROZLOŽENÍ MÍSTNOSTÍ V OBJEKTU



Příloha 1 *rozmístění místností v objektu*

PŘÍLOHA 2: SEZNAM PŘIDĚLENÝCH IP ADRES

koncové číslo IP	prvek	koncové číslo IP2	prvek3	koncové číslo IP4	prvek5
0	PC 1	43		86	
1	PC 2	44		87	
2	PC 3	45		88	
3	PC 4	46		89	
4	PC 5	47		90	
5	PC 6	48		91	
6	PC 7	49		92	
7		50		93	
8		51		94	
9		52		95	
10		53		96	
11		54		97	
12		55		98	
13		56		99	
14		57		100	Server
15		58		101	
16		59		102	
17		60		103	
18		61		104	
19		62		105	
20		63		106	
21		64		107	
22		65		108	
23		66		109	
24		67		110	
25		68		111	
26		69		112	
27		70		113	
28		71		114	
29		72		115	
30		73		116	
31		74		117	
32		75		118	
33		76		119	
34		77		120	
35		78		121	
36		79		122	
37		80		123	
38		81		124	
39		82		125	
40		83		126	
41		84		127	
42		85		128	

Příloha 2 *tabulka přidělených IP adres*

koncové číslo IP	prvek	koncové číslo IP2	prvek3	koncové číslo IP4	prvek5
129		172	WAN 1	215	
130		173	WAN 2	216	
131	Tiskárna 1	174	WAN 3	217	
132	Tiskárna 2	175	WAN 4	218	
133		176	WAN 5	219	
134		177	WAN 6	220	
135		178	WAN 7	221	
136		179	WAN 8	222	
137		180	WAN 9	223	
138		181		224	
139		182		225	
140		183		226	
141		184		227	
142		185		228	
143		186		229	
144		187		230	
145		188		231	
146		189		232	
147		190		233	
148		191		234	
149		192		235	
150		193		236	
151		194		237	
152		195		238	
153		196		239	
154		197		240	
155		198		241	
156		199		242	
157		200		243	
158		201		244	
159		202		245	
160		203		246	
161		204		247	
162		205		248	
163		206		249	
164		207		250	
165		208		251	
166		209		252	
167		210		253	
168		211		254	
169		212			
170		213			
171		214			