JIHOČESKÁ UNIVERZITA

v Českých Budějovicích

PEDAGOGICKÁ FAKULTA

Katedra fyziky

Zabezpečení dat při bezdrátovém spojení do privátní počítačové sítě

Bakalářská práce

Vypracoval: **Václav HANKETA**

Vedoucí práce: **PaedDr. Petr Adámek, Ph.D., katedra fyziky**

Datum odevzdání:

Prohlášení

Prohlašuji, že jsem svou diplomovou práci vypracoval samostatně a použil jsem pramenů, které cituji a uvádím v přiloženém seznamu literatury.

V Českých Budějovicích dne 17. října 2005 .....

podpis

Obsah

1 Bezpečnost informací, řešení bezpečnostních rizik, projekt

1.1 Informace v podobě aktiva organizace

Význam informací a práce s nimi v prostředí konkurenčního boje stále vzrůstá. Informace s obsahem analytických závěrů se stávají velmi cenným zbožím. Vysoký stupeň zabezpečení informací je předpokladem pro prosperující a rozvíjející se organizaci. Pro ukládání a využívání informací ve formě dat nejen v počítačové síti, ale i na médiích jako jsou diskety, výměnné disky a další média pro trvalé uchování dat, se musí stát objektem bezpečnosti. Nelze však opomenout ani uživatele informačních systémů, kde lidský faktor představuje nejrizikovější složku [1].

Vlastní realizace zabezpečení informací je proces zahrnující celou činnost organizace. Řešení zabezpečení informací je náročná, složitá a finančně nákladná záležitost. Ne vždy, z hlediska investic organizace, jsou tato opatření prioritou. Současně se nelze domnívat, že jednou vytvořená bezpečnostní opatření jsou řešením trvalým. Stále se mění podmínky při práci s informacemi. Současně je potřeba reagovat na rafinovanost, znalost a technické vybavení „zájemce" o informace organizace.

Předpokladem pro zajištění bezpečnosti je žádoucí vznik bezpečnostního managementu organizace. Posláním managementu je proklamace, realizace a údržba informační bezpečnosti, osvěta a zvyšování bezpečnostního vědomí, a především analýza bezpečnostních rizik [2].

1.2 Komplexní řešení bezpečnosti

Proces řešení bezpečnosti představuje zpracování studie bezpečnosti, bezpečnostní politiky a bezpečnostního projektu. Studie bezpečnosti je popis stavu informační bezpečnosti. Bezpečnostní politika vyjadřuje globální a systémovou bezpečnostní politiku. Bezpečnostní projekt je soubor opatření k zajištění bezpečnosti. Ve všech fázích tvorby systému bezpečnosti probíhá proces nepřetržitého hodnocení všech aktivit, z nich odvozených regulačních opatření a vyvození důsledků.

1.3 Bezpečnost informací a zákony

Povinnost zabezpečit informace uložené a využívané pomocí informačních systémů ukládají i některé právní normy. Zákon č. 256/1992 Sb., [3] o ochraně osobních údajů v informačních systémech, upravuje ochranu osobních údajů a povinnosti související s ochranou informací při provozování informačních systémů. Zákon č. 148/1998 Sb., [3] o ochraně utajovaných skutečností a o změně některých zákonů, vymezuje utajované skutečnosti, které je nutno v zájmu České republiky utajovat a skutečnosti, s nimiž by neoprávněné nakládání mohlo způsobit újmu České republice.

1.4 Bezpečnostní rizika

Pro řešení bezpečnostní politiky je třeba zdůraznit některé případy, které mohou výrazným způsobem ovlivnit bezpečnost informací v organizaci. Nelze pominout elektronickou poštu stejně jako Intranet a Internet, nelze zapomenout na elektronický podpis a kryptografickou ochranu.

1.4.1 Internet a Intranet

Internet je komunikační systém vázaný na výpočetní techniku spojenou pomocí počítačové sítě. Nemá svého vlastníka ani předepsané použití. Každý, kdo ho používá, má minimálně nutné technické vybavení, může přistupovat ke všem vystaveným stránkám a využívat je. Internet tak funguje jako komunikační prostředí. Bezpečnost internetu není v podstatě žádná. Nelze předem stanovit, jakými cestami se informace v síti pohybují, a kdo může být jejich příjemcem. Již samo přenosové prostředí je nedůvěryhodné. Bezpečnost je potom třeba vynutit na straně odesílatele i příjemce nebo vytvořit v tomto komunikačním prostředí chráněný kanál. Zveřejněné údaje nejsou chráněny žádnou právní normou. Právní otázky jsou stálým předmětem zájmu právníků i laické technické veřejnosti.

Intranet je využití technických vlastností internetu v rámci jedné organizace. Poskytovatel i příjemce jsou ze stejné organizace a informace v ideálním případě mohou procházet důvěryhodným prostředím. V tomto prostředí se mohou definovat přístupová práva k různým informacím a selektivní výběr jejich zobrazení. Bezpečnostním rizikem je proniknutí neoprávněných osob do intranetové sítě z vnějšího komunikačního prostředí.

1.4.2 Elektronická pošta

Elektronická pošta je přenos zpráv ve formě počítačových souborů nechráněným prostředím internetu. Není možné jednoznačně určit, kde všude jsou e-mailové zprávy zaznamenávány a kdo je během přenosu četl nebo dokonce upravil. Zprávy s obsahem citlivých informací je třeba zabezpečit vhodným způsobem, např. pomocí kryptografie. Bezpečnost elektronické pošty je zajištěna právně zákonem č. 29/2000 Sb., [3] o poštovních službách, tento zákon zaručuje poštovní tajemství a trestním zákonem č. 412/2002 Sb., [3] úplné znění trestního zákona, který za porušení tohoto tajemství ukládá trestní odpovědnost.

1.4.3 Obchodní komunikace

EDI je způsob obchodní komunikace, při níž se zprávy posílají jako předem dohodnuté formuláře. Informace jsou v těchto formulářích na stanovených místech a v předepsaných tvarech. Převod do podoby EDI formuláře a zpět probíhá v dané počítačové aplikaci. Přenosový protokol umožňuje poměrně snadné a spolehlivé zabezpečení. Zprávy mohou být před odesláním zašifrovány.

1.5 Způsoby ochrany informací

Citlivé informace je třeba chránit před neoprávněným přístupem pomocí kryptografických ochran, což jsou zvláštní úpravy informací při předávání nedůvěryhodnými kanály. Proces šifrování a způsob tvorby oprávnění jsou provázeny administrativně technickými prostředky. Šifrování a dešifrování jsou speciální operace, postavené obvykle na matematických aparátech realizovaných prostřednictvím speciálních zařízení (šifrátory, dešifrátory, šifrující faxy, šifrující telefony, šifrující modemy, kryptofaxy, kryptotelefony, kryptomodemy). Mimo tato speciální zařízení lze ke kryptografickým účelům použít počítače vybavené speciálními programovými prostředky. Provoz šifrovacích zařízení a manipulace s klíči vyžadují zřízení a provozy režimových pracovišť. Účinné ochrany informací je nutné dále zajistit použitím vhodných technických prostředků pro znemožnění přístupu do informačních systémů organizace z nedůvěryhodných datových spojů.

1.5.1 Šifrování symetrickou šifrou

Šifrování i dešifrování jsou založeny na existenci jediného klíče, kde odesílatel i příjemce zprávy jsou vlastníkem jednoho stejného klíče.

DES – Data Encryption Standard [3]

Délka klíče této šifry je pouze 56 bitů. Předpoklad bezpečnosti tohoto algoritmu byl zpochybněn a to již v roce 1998, kdy došlo k veřejnému rozlomení šifry.

IDEA – International Data Encryption Algorithm [3]

Délka klíče této šifry dosahuje 128 bitů. Díky velkému oboru klíčů je použití útoku na šifru nepraktické.

Šifrování pomocí tajného klíče (sdílené tajemství), spoléhá na tajnou hodnotu, kterou znají obě strany. Prostá znalost hodnoty dokládá tomu, kdo klíč poskytuje, že žadatel o klíč je důvěryhodný. Pomocí komunikace typu výzva a odezva lze zajistit, že se po síti přenáší pouze hodnota „hash" tajemství, nikoliv samotné tajemství. Variacemi jednorázových hesel lze zase zjistit, že tajemství se po každém použití mění. Problém se šifrováním pomocí tajného klíče spočívá ve výměně klíčů. Neexistuje žádný skutečně bezpečný způsob, jak by se mohly obě strany najednou tajný klíč dozvědět, aniž by proběhla předtím nějaká forma nezašifrované komunikace. Obvykle k výměně dochází v mysli jedince, který nastaví na dvou různých koncových systémech stejný tajný klíč. Algoritmy šifrování na principu tajného klíče jsou mnohonásobně rychlejší než algoritmy šifrování na principu veřejného klíče. Ve většině implementovaných systémů se bezpečná autentizace provádí na principu veřejných klíčů a ustavením komunikačního kanálu, kterým se pak bezpečně vymění sada tajných klíčů, takže lze použít vysokorychlostní algoritmus šifrování tajným klíčem.

1.5.2 Šifrování nesymetrickou šifrou

Při šifrování nesymetrickou šifrou s veřejným klíčem existuje na straně odesílatele i příjemce sada párových klíčů. Jednomu se říká „veřejný klíč" a druhému „soukromý klíč". Zprávu zašifrovanou jedním klíčem lze dešifrovat pouze druhým klíčem ze stejného páru. Z veřejného klíče nelze odvodit soukromý klíč a naopak. Soukromý klíč je citlivá informace, s níž je třeba bezpečně manipulovat.

Pokud by „zájemce" zachytil veřejný nebo šifrovací klíč, může data pouze šifrovat a přenášet je příjemci. Není však schopen obsah dat, který zachytí, dešifrovat.

1.5.3 Šifrování datové části

Šifrování datové části se používá k zamlžení obsahu vložených dat, aniž by bylo nutné celý paket zapouzdřovat do jiného paketu. V tom je šifrování datové části stejné jako standardní propojování sítí IP kromě toho, že datová část se šifruje. Šifrování datové části data zamlží, ale neutajuje informace z hlavičky, takže z nich lze zjistit podrobnosti o interní síti. Šifrování

datové části lze doplnit jednou z řady bezpečných šifrovacích technik, které se liší po zvoleného řešení VPN.

1.5.4 Antivirová ochrana

Újmy způsobené aktivitami škodlivého softwaru jsou jen obtížně vyčíslitelné. Jedná se o poškození dat, nedostupnost informačních systémů a nepoužitelnost datových nosičů. „Počítačové viry" mají schopnost vlastního množení a infiltrace do jiných systémů. Pro svou funkci potřebují hostitelský program. „Trojské koně" se tváří jako užitečné programy, ale způsobují škodlivé funkce. „Červy" se chovají podobně jako viry, ale nepotřebují hostitelský program. „Makroviry" jsou specifické tím, že jejich nositeli jsou datové soubory využívající maker počítačových programů (Word, Excel apod.). Problém antivirové ochrany je stejně jako celá problematika bezpečnosti informací problémem vyžadujícím komplexní řešení. V první řadě jde o činnost preventivní – zabránit infekci, infiltraci škodlivého softwaru do informačních systémů. Jestliže je preventivní část antivirové ochrany prolomena, nastupuje část léčebná, tzn. odstranění následků infekce a uvedení informačních systémů do původního stavu.

Antivirová ochrana je jednou ze součástí bezpečnostních projektů týkajících se širokého okolí provozu informačních systémů a jeho uživatelů. Nelze ji zjednodušit na jednorázovou instalaci antivirového produktu. Je třeba definovat uzavřenou antivirovou politiku, definovat práva a povinnosti všech, kteří jí mohou být dotčeni. Nedílnou součástí antivirové ochrany je včasná a důsledná aktualizace virové databáze.

1.5.5 Způsoby útoků „zájemců" do komunikačního prostředí

Ochrana a obrana před útočníky spočívají především ve znalosti způsobů a možností pronikání do informačních systémů. Do počítačové sítě lze vniknout přímo použitím počítače v síti, připojením přes Internet nebo připojením k síti přímo, obvykle prostřednictvím bezdrátového připojení. Malé množství možných směrů relativně dobře vymezuje hranice zabezpečení a je tedy možné je ještě více izolovat.

1.5.5.1 Odposlech a špehování

Informace o síti lze jednoduše získat odposlechem síťového provozu a pak se počítačů v síti dotazovat na informace o nich samotných. Zájemce o data neboli útočník může komunikovat s počítači, které poskytují služby např. DNS [4], na něž se ostatní počítače spoléhají. Počítače v síti o sobě a o tom, jak jsou nakonfigurované, dobrovolně vyzrazují množství informací,

zejména pokud jsou ponechány ve své původní konfiguraci od dodavatele operačních systémů. Mnoho síťových protokolů hesla nešifrují, takže jakýkoliv počítač na cestě mezi klientem a serverem může uživatelská jména a hesla vysledovat. Proti sledování nejsou ale bezpečné ani všechny zašifrované přihlašovací postupy, protože v případě, že je přihlašovací postup naivní, může útočník uživatelská jména a zašifrovaná hesla zaznamenat a použít je později na server, stejně jako to původně udělal oprávněný uživatel. Analýzou síťového provozu lze zjistit IP [4] adresy zdrojových a cílových počítačů, umístění bran a směrovačů, a v neposlední řadě zprávy o dostupnosti síťových služeb. U standardních serverů jsou služby nastavené tak, aby poslouchaly na následujících portech.

Jednoduché služby TCP/IP obvykle poslouchají na těchto portech: [4]

Port	**Služba TCP/IP**
7	Echo
8	Discard
13	Daytime
17	Quote of the Day
19	Charakter generator

Internetové servery většinou poslouchají na těchto portech:

Port	**Server**
21	File Transfer Protocol
22	Telnet
70	Gopher
80	World Wide Web
119	Net News
23	Secure Shell
443	Secure http

Souborové servery obvykle poslouchají na těchto portech:

Port	**Služba**
53	Domain Name Service
135	RPC Locator Service
136	NetBIOS Name Service WINS
139	NetBIOS Session Service
515	LPR používá službu tisku TCP/IP
530	Remote Procedure Call
3389	Terminal Services

Poštovní servery jsou obvykle nastaveny, aby poslouchaly na portech:

Port	Poštovní server
24	Simple Mail Transfer Protocol
110	Post Office Protocol
143	Internet Mail Access Protocol

1.5.5.2 Odepření služby

Existuje řada metod, jimiž může útočník napadnout počítač nebo službu, kterou poskytuje [4]. Většina útoků je prováděna pomocí TCP/IP, protože TCP/IP je nejrozšířenější protokol pro tvorbu sítí. Ping of Death (ozvěna smrti) je speciálně vytvořený paket ICMP, který porušuje pravidla pro stavbu paketů, může počítači, jenž ho přijme, způsobit úplné zhroucení, pokud síťový software tohoto počítače nekontroluje korektnost formátu paketů ICMP před tím, než je zpracuje. Obdobou je deaktivování síťových funkcí počítačů s přetížením, což jsou pokusy o připojení nebo požadavky o získání informací. Úvodní paket protokolu TCP je jednoduchý a lze ho vygenerovat. Zpracování tohoto paketu a odpověď na něj spotřebuje mnohem více procesorového času a operační paměti. Útočník může na cílový počítač posílat pakety jeden za druhým, a ten nebude pak schopen zpracovávat běžný legitimní provoz. Cílem útoků dále jsou především služby, jež jsou základními prvky sítí založených na TCP/IP nebo Windows. Patří sem služba RPC, NetBIOS, DNS a WINS. Útočník, který získá kontrolu nad směrovači sítě a pozmění směrovací tabulky, může části sítě izolovat a nasměrovat síťový provoz ze sítě ven. Mnoho síťových zařízení včetně počítačů se serverem založeným na Windows, lze spravovat na dálku pomocí SNMP. Kromě špehování dat může útočník pomocí SNMP změnit konfiguraci sítě tak, aby odepírala službu počítačům v síti nebo dokonce, aby směrovala data ze sítě ven.

1.5.5.3 Zneužívání protokolů

Zneužívání protokolů je v současnosti nejoblíbenější forma útoků na Internetu. Jsou to útoky založené na napadení chyb ve veřejné službě, za účelem získání většího přístupu než by bylo normálně možné. Cílem útočníka je proniknout přes zabezpečení sítě a získat informace nebo prostředky na počítačích v síti. Sada protokolů TCP/IP obsahuje nepříliš využívanou možnost, v níž se uvádí přesná cesta, kterou by měl paket projít při průchodu sítě založené na TCP/IP. Tato možnost se nazývá „přímé směrování" a útočník může jejím prostřednictvím posílat data

z počítače, přičemž data vypadají jako by pocházela z jiného důvěryhodnějšího zdroje. Útočník může pomocí přímého směrování převzít totožnost připojeného uživatele a vložit do jinak neškodné komunikace mezi serverem a autorizovaným klientským počítačem další informace. Další taktikou sloužící k průniku sítě je převzetí totožnosti služby, od které získávají klientské počítače při startování systému informace o konfiguraci. Převzetím totožnosti serveru DHCP lze přesměrovat klientské počítače v síti tak, aby komunikovaly téměř s kterýmkoliv hostitelským počítačem, převzetím WINS může útočník vracet neplatné nebo nepřátelské IP adresy jmen počítačů v NetBIOS a převzetím DNS může vracet také neplatné nebo nepřátelské IP adresy pro internetová jména.

1.5.6 Oddělení informačních systémů od nedůvěryhodného prostředí

Součástí bezpečnostního projektu je třídit informace podle stupně důležitosti a najít řešení při zajištění bezpečnosti informací, jak na úrovni zpracování v organizaci, tak i znemožnit průnik „zájemcům" z nedůvěryhodného prostředí. Pro oddělení informačních systémů provozovaných v organizaci od nedůvěryhodného prostředí je vhodné použít bezpečnostní prvek datové komunikace – „Firewall".

1.5.7 Bezpečnostní softwarové nástroje

Pomocí Firewallů nelze zajistit některé funkce zabezpečení jako například analýzu zranitelnosti a šifrování disků. Je možné použít softwarové nástroje, které jsou při procesu zabezpečení dat mimořádně užitečné. Při zajištění zabezpečení pomocí mnoha jednoúčelových nástrojů je potřeba dbát opatrnosti, neboť nejsou integrovány, nejsou robustní a stále závisejí na bezpečnosti implementace protokolů TCP/IP v operačním systému, který nemusí být odolný proti útokům typu odepření služby. Nedostatečná integrace různých bezpečnostních nástrojů vytváří efekt „ementálu", kdy kombinace samostatných nástrojů ponechává v zabezpečení chráněného hostitele díry. Více nástrojů nemohou předejít problémům, kterým lze zabránit pomocí integrovaného řešení. Použitím samostatného překládání adres NAT a proxy se budou data zpracovávat proxy serverem nebo předávat do nedůvěryhodného prostředí sítě pomocí překladu adres. Kvalitní Firewally mohou plnit funkci proxy i překládání adres pro průchozí připojení.

Systém Windows je standardně dodáván s mnoha jednoduchými nástroji, které lze použít při správě zabezpečení. Nástroj „Prohlížeč událostí" zobrazuje protokoly systému a umožňuje filtrovat zobrazení pouze na určité typy událostí. Obsahuje informace o narušení zabezpečení,

jako například uzamčení účtu. Protokolování zabezpečení je nutné ve „Správci uživatelů" povolit, protože veškeré auditování je standardně zakázáno.

```
13.12.2004  9:23:38  Security  Success Audit  Account Management  644  NT  AUTHORITY\SYSTEM
    GAMA  User Account Locked Out:
    Target Account Name:  abraxas
    Target Account ID:  S-1-5-21-1524461650-500578088-56781596-1005
    Caller Machine Name:  \\SPRAVCE
    Caller User Name:  SYSTEM
    Caller Domain:  NT AUTHORITY
    Caller Logon ID:  (0x0,0x3E7)
```

Program „Sledování sítě" systému Windows umožňuje zachytávat síťové pakety a zobrazit o nich velmi podrobné informace s uvedením protokolů. Tento nástroj je velmi užitečný při sledování využití sítě a také při hledání určitých paketů při analýze problémů zabezpečení. Verze „Sledování sítě" obsažená v systému Windows dokáže zachytit pouze příchozí a odchozí pakety příslušné pracovní stanice, což omezuje použití jako nástroje pro monitorování celé sítě.

Program „Sledování výkonu" je jedním z nejužitečnějších nástrojů systému Windows pro optimalizaci a sledování výkonu. Poskytuje také několik funkcí souvisejících se zabezpečením dat. Tento nástroj pracuje s jednotlivými parametry označovanými jako „čítače", které souvisejí se systémem, a umožňují nastavení minimální a maximální hodnoty jednoho nebo více parametrů čítačů, tvorbu protokolu vybraných čítačů, zobrazují počty pokusů uživatelů o přístup k souborům bez příslušných práv a počet neplatných pokusů o přihlášení. Čítač TCP umožňuje sledovat používání sítě a chyby protokolu TCP/IP.

Příkaz „Ping" odešle zprávy typu „Echo" protokolu ICMP vzdálenému hostiteli. Tyto zprávy umožňují zjistit, zda je hostitel k dispozici pro další přenosy protokolu TCP/IP. Tento příkaz je užitečný hlavně při sledování stavu vzdáleného spojení.

Příkaz „Tracert" umožňuje zobrazit směrovače mezi dvěma komunikujícími hostiteli.

Příkaz „Telnet" umožňuje vytvořit konzolové uživatelské relace s víceuživatelskými počítači a je užitečný, zejména při zjišťování přítomnosti a funkčnosti různých služeb sítě.

Nástroj „Internet Scanner" společnosti Internet Security Systém je nejkomplexnějším nástrojem kontroly zabezpečení pro systémy Windows, Linux a Solaris. Kontroluje velké množství běžných problémů zabezpečení a řadí je podle úrovní rizik, které představují. Skener zabezpečení je založen na modelu klient/server, a proto lze skenovat systémy vzdáleně.

Analyzátory protokolu slouží jako testovací nástroje sítí. Přijímají a dekódují nízkoúrovňové informace z paketů pro všechny rámce procházející přes trasu, ke které jsou připojeny.

Nástroje pro kontrolu síly hesel načítají šifrovaná hesla uložená na serveru a snaží se je dešifrovat hrubou silou. Čím déle dešifrování hesel trvá, tím jsou silnější. Síťové nástroje pro

kontrolu síly hesel se s vysokou frekvencí pokoušejí vzdáleně přihlásit, ale jsou mnohem pomalejší než místně spouštěné nástroje tohoto typu.

1.6 Bezpečnostní ochranné systémy typu Firewall

Pomocí Firewallu se na hranici privátní sítě vytvářejí kontrolní body zabezpečení. V těchto bodech probíhá kontrola všech paketů, které mezi privátní sítí a nedůvěryhodným prostředím procházejí a podle toho, jak pakety splňují pravidla nastavená ve Firewallu, Firewall určí, zda je jednotlivě propustit nebo zablokovat. Je-li Firewall správně nastavený, má datová síť k dispozici nejvyšší možnou míru ochrany. Bez tohoto konceptu by každý hostitelský počítač v rámci sítě musel provádět funkce zabezpečení sám, zbytečně by zatěžoval své prostředky a zdroje, a tak by v lokálních a rychlých sítích zvyšoval dobu potřebnou k připojení, autentizaci a zašifrování dat. Použitím Firewallu lze soustředit veškeré externí služby zabezpečení do optimálního zařízení vyhrazeného přímo k tomuto účelu.

1.6.1 Prvky Firewallu

Firewall kontroluje a schvaluje nebo zamítá jednotlivé pokusy o připojení mezi interní a externí sítí. Robustní Firewally chrání síť na všech vrstvách, a to od linkové až po aplikační.

Filtrování paketů – odmítá pakety TCP/IP od neautorizovaných uživatelů a pokusy o připojení k neautorizovaným službám.

Překládání síťových adres NAT, maskování adres IP – překládá IP adresy interních hostitelských počítačů a skrývá je před monitorováním zvenčí.

Šifrovaná autentizace - umožňuje uživatelům externích sítí prokazovat Firewallu svou totožnost a získat tak přístup k privátní síti z externích lokalit.

Propojování virtuálních privátních sítí – ustavuje bezpečné propojení mezi dvěma privátními sítěmi přes nedůvěryhodné komunikační prostředí.

2 Protokoly bezdrátového spojení, normy, parametry

2.1 Technologie sítě IEEE 802.11 [7]

Místo metalického vedení je u bezdrátového spojení IEEE 802.11 využita schopnost šíření elektromagnetického vlnění vzduchem. Liší se však frekvencemi, na kterých jsou data

přenášena. Standard ***b*** a standard ***g*** pracují na frekvenci 2,4 GHz, standard ***a*** na frekvenci 5 GHz [5].

U různých standardů existují různé typy modulace

IEE 802.11b	CCK/DSSS	
IEE 802.11b+	PBCC	
IEE 802.11g	CCK/OFDM	CCK/DSSS
IEE 802.11a	OFDM	
IEEE 802.11h	OFDM s DFS	

Všechny typy modulace mají společné to, že posílají datový paket sestavený ze dvou částí. Ten se skládá z hlavičky a datové části. Přenos dat se uskutečňuje ve formě paketů. Informace od odesílatele jsou rozděleny do paketů, aby mohly být lépe transportovány k příjemci, který je opět složí dohromady. Tento postup odpovídá postupu, který používá protokol TCP/IP pro přenos dat. Každý soubor, který má být po síti přenesen, je rozdělen do paketů a odeslán. Pokud se paket na své cestě ztratí nebo pokud dorazí k cíli poškozen, je o něj znovu zažádáno a je poslán znovu. Příjemce data opět roztřídí a složí dohromady. Datový paket v bezdrátových sítích se skládá ze dvou částí, a to informační a datové. První část slouží jako upozornění celé síti, že bude následovat přenos dat pro účastníka sítě (preambule). Poté je zaslána hlavička, která příjemci sděluje, jak velká jsou přenášená data, a nakonec se přenesou data jako druhá část paketu. Aby se více zařízení v síti WLAN neovlivnilo, děje se vše v přesně stanoveném pořadí. Když jedno zařízení pošle preambuli, ví ostatní zařízení, že se budou posílat nějaká data. Počkají na sdělení, jak dlouho bude přenos trvat, a teprve po uplynutí této doby začnou opět komunikovat. Zde platí pravidlo RTS/CTS. Pouze pokud na vysílacím/přijímacím kanálu žádná komunikace neprobíhá, je nový paket odeslán.

U standardu Wireless LAN IEEE 802.11b jsou obě části pomocí CCK modulovány pouze na jeden nosič. Proto představuje CCK nejjednodušší mechanizmus. Rychlejší Wireless LAN IEEE 802.11a používá modulaci na více nosičů OFDM pro data a pro preambuli/hlavičku. Data jsou rozdělena do více blízko sebe ležících „podnosičů" rozdělených do 5 GHz frekvenčního pásma. Tyto spolu s menším informačním paketem jsou důvodem vyšší přenosové rychlosti těchto sítí. Standard IEEE 802.11g je v praxi něco mezi tím. Nabízí to nejlepší z obou světů – mechanizmus CCK pro preambuli a hlavičku a OFDM pro datovou část bezdrátového paketu. Výhodou tohoto mechanizmu je zpětná kompatibilita se standardem IEEE 802.11b, neboť používá podobnou modulaci CCK. Díky tomu je kompatibilní, a proto mohou být nová zařízení kombinována se starými. Současné použití zařízení standardů ***b*** a ***g*** má však jednu zásadní nevýhodu; a to, že pomalejší zařízení brzdí ta rychlejší. U standardu IEEE 802.11b se používá

systém DSSS pro zlepšení příjmu v oblasti rušivých vlivů. Signál je uměle rozptýlen do širšího rozsahu a informace jsou tak uchovány v normálním podkresovém rušení frekvenčního spektra. Technologie rozprostřeného spektra se používá pro dosažení rychlých datových přenosů v pásmu ISM. Tradiční rádiové technologie se soustředí na vměstnání co největšího počtu signálů do relativně úzkého pásma. Rozprostřené spektrum oproti tomu používá matematické funkce pro rozptýlení signálu do širokého frekvenčního bloku. Používání rozprostřeného spektra ovšem nepřináší žádnou odolnost proti zarušení – mohou být rušeny podobnými systémy, interferencemi a provozem klasických vysílačů pracujících s úzkým rádiovým pásmem. Pro použití standardu IEEE 802.11 ***a/h*** jsou vyhrazeny dva frekvenční rozsahy. Rozsah od 5150 do 5350 MHz je určen pro přenosy v budovách. Pro přenosy vnějším prostředím lze využít až 1 W výkonu antény. Frekvenční rozsah určený pro tento typ použití je 5470 až 5725 MHz. Velkou výhodou standardů IEEE 802.11 ***a/h*** je, že umožňují současný provoz na 19 kanálech a jsou určeny především pro profesionální nasazení.

2.2 Licence pro kmitočtová pásma WLAN

Vysílací techniky pro širokopásmové přístupové sítě WLAN jsou stanovené udělenými licencemi v pásmu řádu GHz a jsou vhodné pro přenos datové komunikace do rychlosti 155 Mb/s. Tato kmitočtová pásma jsou k dispozici bez licencí a bez poplatků, platí však určitá technická omezení týkající se například vysílacího výkonu. Sítě WLAN používají zpravidla pásmo ISM 2,4 GHz určené doporučením standardu IEEE 802.11. Rádiový provoz v přístupových sítích povoluje Český telekomunikační úřad obecně generální licencí, ve které jsou určeny přidělené kmitočty. Generální licence GL 38/R/2001 k provozování vysílacích rádiových zařízení, která jsou součástí účastnických terminálů v pevných bezdrátových přístupových sítích a slouží k připojení koncových telekomunikačních zařízení k veřejně telekomunikační síti, povoluje provoz na kmitočtech v rozpětí 24,5 – 29,1 MHz s duplexním odstupem 1008 MHz. Vstupem České republiky do EU musí být správa kmitočtového spektra řízená Telekomunikačním úřadem v souladu s nařízením Evropského institutu pro telekomunikační normy ETSI, a to především schválenou normou ETS 300 328. Před zahájením telekomunikační činnosti podle generální licence je nutné tuto činnost písemně přihlásit k registraci u Telekomunikačního úřadu.

2.3 Autentizace a bezpečnost WLAN

Všechna řídící data a také skutečný síťový provoz se přenáší pomocí šíření elektromagnetického vlnění vzduchem. Toto prostředí je nutné definovat prostředím nedůvěryhodným. Ke zvýšení bezpečnosti sítí slouží mechanizmy jako autentizace a šifrování.

Autentizace Open System představuje jednoduchý mechanizmus, s jehož pomocí se lze přihlásit do sítě. Klient pošle požadavek přístupovému bodu na autentizaci, ten na požadavek odpoví a pošle data nazpět. Pouze pokud je přístup klientovi zakázán, je požadavek na autentizaci odepřen. Tento mechanizmus umožňuje přístup k základové stanici každému účastníkovi sítě, pokud mu to není explicitně zakázáno.

Zdánlivě bezpečnější autentizační mechanizmus se nazývá Shared Key Authentification. Přístup je povolen pouze těm stanicím, které se identifikují správným klíčem (WEP nebo WPA TKIP). Pro přihlášení do sítě přístupový bod požaduje autentizaci a pošle klientovi automaticky vygenerovaný řetězec s tím, aby klient tento řetězec pomocí síťového šifrovacího klíče zašifroval a výsledek poslal zpět. Přístupový bod následně zkontroluje, zda byl řetězec správně zašifrován. Zde je bezpečnostní riziko, neboť se testovací řetězec přenáší jednou zašifrovaný a podruhé nezašifrovaný. Pro přenos dat se používá šifrovací kód algoritmu WEP, data jsou kódována pomocí kombinace šifrování RC4 a operací s matricemi.

Tato technologie ochrany zpočátku dávala naději, že umožní zabezpečené propojení sítí, aniž by došlo ke snížení bezpečnosti. WEP šifrování je z podstaty nedostatečné.

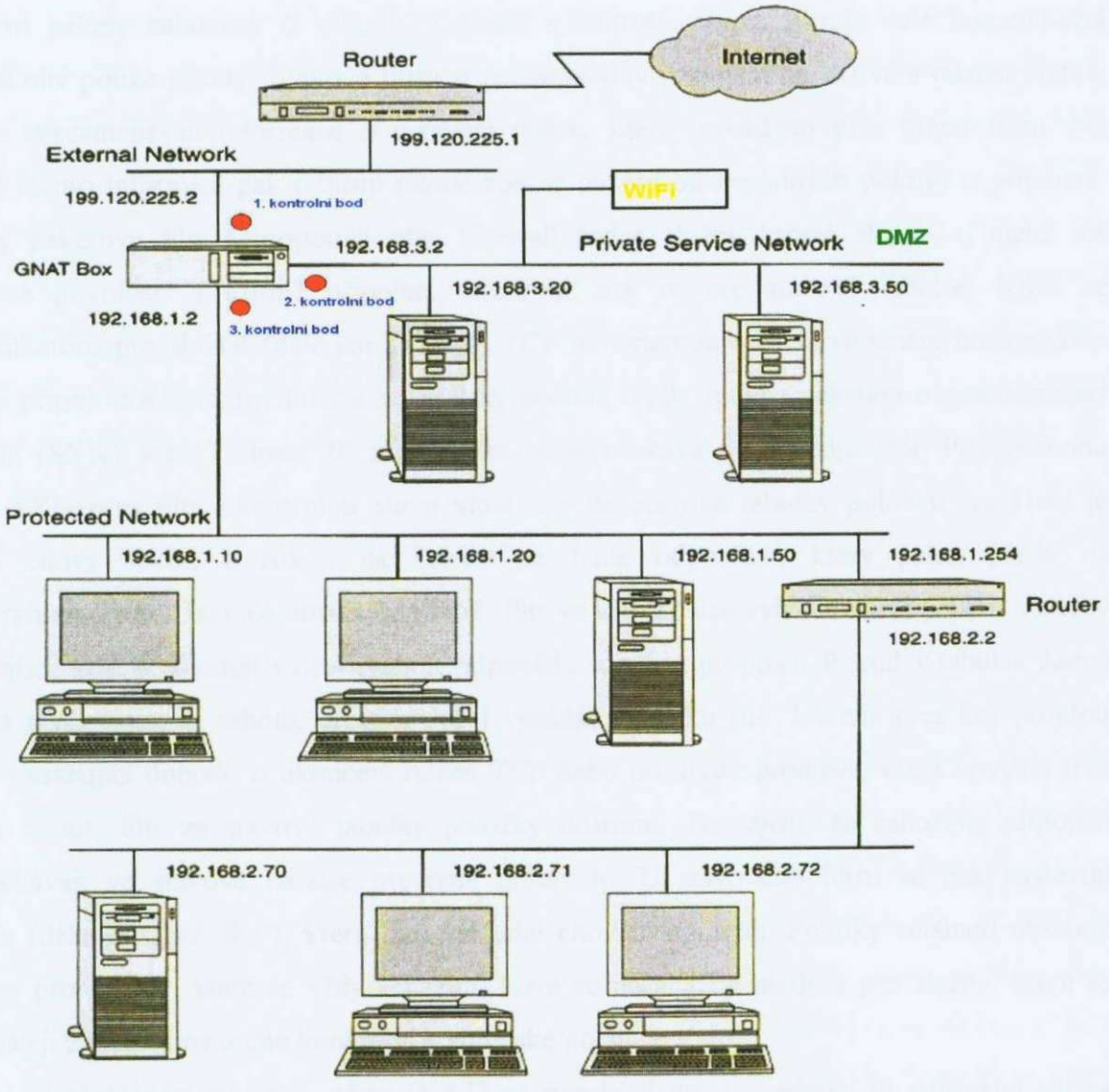
Zabezpečení WPA je vybaveno rozšířeným inicializačním vektorem, technikou automatické změny klíče po připojení nového zařízení do sítě a kontrolou integrity, která má zabránit změně dat na cestě od odesílatele k příjemci. Byla doplněna technologie Per Packet Mixing – měnící se pozice inicializačního vektoru v paketu a protokol TKIP – Temporal Key Integrity Protocol zabezpečení šifrovacího klíče. Protokol TKIP generuje vlastní šifrovací klíče. Šifrovací algoritmus DES – Data Encription Standard byl nahrazen algoritmem AES – Advanced Encryption Standard. AES patří mezi blokové šifrovací algoritmy. Délka bloku a délka šifrovacího klíče může být větší než DES.

3 Návrh a realizace sítě

Návrh komplexního řešení bezpečnosti a bezpečnostního projektu vede k rozhodnutí, jaké úsilí by se mělo do zabezpečení sítě investovat. Je nutné znát hodnotu dat v síti, publicitu nebo viditelnost organizace a škody, které by mohly ztráty služeb způsobit. Také je třeba zamyslet se nad tím, s jakou mírou narušení nebo omezení sítě se ve jménu bezpečnosti chceme smířit.

3.1 Firewall typu GNATBOX s vlastním operačním systémem

GNATBOX je filtr paketů a překladač adres s certifikátem ICSA, který funguje na vlastním operačním systému spouštěném z jedné diskety. Obsahuje server proxy protokolu SMTP a server rozděleného DNS. Chrání proti falšování adres IP a běžným útokům typu odmítnutí služby. Neposkytuje sice prostředí operačního systému Unix, ale jeho jádro a zásobník protokolu TCP/IP jsou odvozeny od systému BSD, což je operační systém Unix typu open-source.



Obr. 1 *Architektura počítačové sítě* [11]

3.1.1 Hlavní funkce Firewallu

- filtr paketů s kontrolou stavu
- překladač adres NAT
- podpora DMZ
- přesměrování portů
- sítě VPN
- protokolování a upozorňování na e-mail

Paketový filtr s kontrolou stavu uchovává stav celé komunikace TCP/IP, která prochází přes Firewall, a v paměti na základě tohoto zapamatovaného stavu pak určí, zda by měly být jednotlivé pakety zahozeny či nikoliv. Zařízení s kontrolou stavu filtruje celé komunikační toky, nikoliv pouze pakety. Stavové filtry si pamatují stav připojení na síťové a relační vrstvě, protože zaznamenávají informace o ustavení relace, které procházejí přes bránu filtru. Na základě těchto informací pak odlišují platné zpětné pakety od neplatných pokusů o připojení. Stavový paketový filtr nepropouští přes Firewall žádné služby kromě služeb, u nichž má nastavené povolení, a kromě připojení, která už má ve své stavové tabulce. Když se k identifikátoru pro službu (dále jen „soket“) TCP na externím nedůvěryhodném hostitelském počítači připojí důvěryhodný interní hostitelský počítač, vyšle spolu s paketem o synchronizaci připojení (SYN) soket (adresu IP a port), na němž očekává přijetí odpovědi. Při průchodu paketu SYN přes filtr s kontrolou stavu vloží filtr do stavové tabulky položku, ve které je uveden cílový soket, a soket, na kterém se bude odpovídat, který paket předá na nedůvěryhodnou síť. Jakmile dorazí odpověď, filtr ve své tabulce vyhledá zdroj paketu a cílový soket zjistí, zda se shodují s očekávanou odpovědí, a paket propustí. Pokud v tabulce žádná položka není, paket se zahodí, protože nebyl vyžádán zvnitřku sítě. Jakmile přes filtr projdou pakety obsahující dohodu o ukončení relace TCP nebo po určité prodlevě, která obvykle trvá několik minut, filtr ze stavové tabulky položky odstraní. To zajistí, že zahozená připojení nezanechávají ve stavové tabulce otevřené průchody. U stavového filtru se pak nastavují pravidla (dále jen „politiky“), která tato základní chování upravují. Politiky většinou obsahují předpisy pro pakety, které se vždy zahazují, které se nezahazují nikdy a pro služby, které se propouštějí zvnějšku na určité konkrétní hostitelské počítače v síti.

Pomocí překládání síťových adres (NAT) se převádějí privátní adresy IP v privátní síti na jedinečné veřejné adresy IP, které lze použít na Internetu. Překládání síťových adres účinně skrývá všechny informace o interních hostitelských počítačích na úrovni TCP/IP. Veškerý provoz vypadá, jako kdyby pocházel z jedné adresy IP. Při zavedení funkce NAT lze potom na interní síti použít libovolný interval adres IP bez ohledu na to, zda adresy IP jsou již někde

použity. Když pakety procházejí přes Firewall, převádí se všechny adresy interních hostitelských počítačů na adresu Firewallu, a ten tak postupně skryje všechny interní adresy IP. Pomocí překladové tabulky pošle datovou část interního hostitelského počítače znovu ze své vlastní adresy a eviduje všechny sokety na externím rozhraní, které přísluší soketům na interním rozhraní. Počítačům v nedůvěryhodném prostředí se všechen provoz na síti jeví, jako kdyby procházel z jednoho velmi zaneprázdněného počítače.

Firewall GNATBOX umožňuje použít DMZ, které mají pravidla zabezpečení pro jednotlivá připojená rozhraní, takže poskytuje funkce dvou Firewallů. Se třemi rozhraními, kterými jsou externí síť, interní síť a síť veřejných serverů lze nastavit pravidla zabezpečení tak, aby blokovala pokusy o připojení k interní síti, ale propouštěla určité protokoly na veřejné servery. V rámci jednoho produktu jsou tak k dispozici funkce dvou Firewallů. Při realizaci bezdrátového připojení je využita demilitarizovaná zóna k vytvoření přípojného bodu.

Při propojování sítí LAN přes nedůvěryhodné prostředí je nutné najít způsob, jak chránit datový provoz, který mezi těmito sítěmi prochází. V ideálním případě by neměly počítače v jednotlivých sítích vědět, že na komunikaci s počítači v jiné síti je něco zvláštního. Počítače vně virtuální sítě by neměly mít možnost zachytávat provoz, který probíhá mezi jednotlivými sítěmi LAN, či vkládat do komunikačního toku svá vlastní data. V podstatě je zapotřebí privátní a chráněný tunel přes pojící prostředí. Virtuální privátní síť VPN je způsob, jak rozšířit síť LAN přes nedůvěryhodné prostředí sítě (WiFi připojení) na vzdálenou síť a ke vzdáleným klientským počítačům [Obr. 1]. Provoz LAN je zapouzdřen do zašifrovaných paketů IP. Zašifrované pakety nemohou nezvané počítače v nedůvěryhodném prostředí sítě číst a do paketů lze uložit jakoukoliv formu komunikace přes LAN včetně přístupu k souborům a tiskárnám, elektronické poště na LAN, RPC a přístupu klientů a serverů do databáze. VPN lze ustavit pomocí Firewallu GNATBOX a klientský přístup na VPN lze zprovoznit pomocí softwaru. Virtuální privátní síť řeší problém přímého přístupu přes nedůvěryhodné prostředí na servery kombinací zapouzdření IP, šifrované autentizace a šifrování datové části. Paket IP může obsahovat jakékoli druhy informací, programové soubory, údaje z tabulkového procesoru, zvukové toky anebo i jiné pakety IP. Jakmile paket IP obsahuje jiný paket IP, říká se tomuto typu vkládání zapouzdření IP, IP přes IP nebo IP/IP. Koncový bod tunelu, na němž je protokol pro tvorbu tunelů, bude přijímat pakety IP, odstraní z nich interní paket a dešifruje ho. Šifrovaná autentizace se používá na bezpečné ověření totožnosti vzdáleného uživatele, aby systém mohl určit, jaká úroveň zabezpečení je pro uvedeného uživatele přiměřená. VPN pomocí šifrované autentizace určuje, zda se může uživatel účastnit šifrovaného tunelu či nikoliv a mohou také autentizaci použít k výměně tajných nebo veřejných klíčů pro šifrování datové části. I když VPN lze vytvořit pomocí jakéhokoliv silného šifrovacího algoritmu a nějaké formy zapouzdření IP, použijeme implementaci standardu IPSec organizace IETF pro bezpečnou komunikaci přes IP, která autenticitu a soukromí komunikace IP zajišťuje pomocí

šifrování. IPSec má mechanizmy, kterými lze provádět autentizaci jednotlivých paketů IP a zajištění, že nedojde k jejich úpravě, šifrování datové části jednotlivých paketů IP mezi dvěma koncovými systémy a zapouzdřování soketů TCP nebo UDP mezi dvěma koncovými systémy v rámci zašifrovaného propojení IP tunelu.

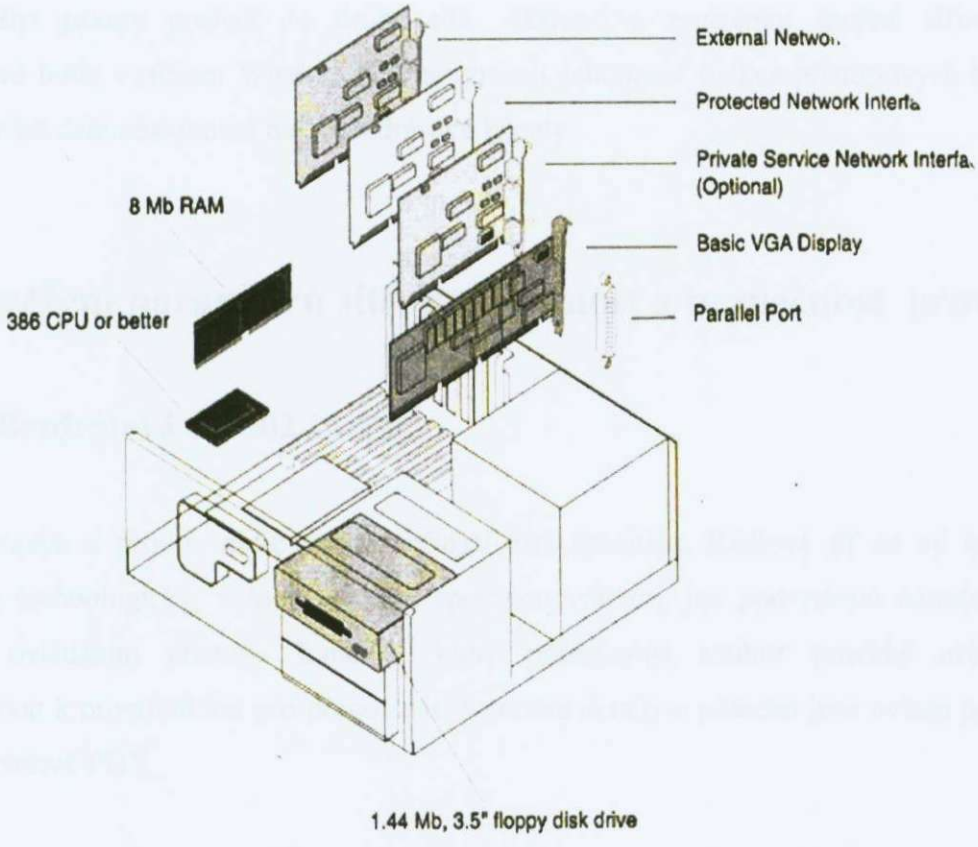
Firewall GNATBOX se vyznačuje složitým mechanizmem protokolování, který zahrnuje automatickou interpretaci mnoha typů útoků. Podobně jako u jiných systémů automatické analýzy protokol Firewallu, bohužel, často uvádí nesprávné typy útoků, ke kterým mohlo dojít. Je potřeba tuto analýzu považovat pouze za orientační.

16 5 Dec 9 19:27:28 NAT: Close UDP [200.1.1.41/1235]->[10.144.36.164/61547]->[10.144.34.13/53] Pkts 1 1, Bytes 57 110.
16 5 Dec 9 19:27:28 NAT: Close TCP [200.1.1.41/1236]->[100.30.10.1/31170]->[100.30.10.17/80] Pkts 5 4, Bytes 441 2183.
17 5 Dec 9 19:27:29 FILTER: Remote access filter blocks: UDP bcast tl0 [100.30.10.11/1033]->[255.255.255.255/8351] l=45.
16 5 Dec 9 19:27:35 NAT: Close UDP [200.1.1.84/1026]->[10.144.36.164/61552]->[10.144.34.13/53] Pkts 1 1, Bytes 65 118.
16 5 Dec 9 19:27:36 NAT: Close UDP [200.1.1.36/1106]->[10.144.36.164/61553]->[10.144.34.13/53] Pkts 1 1, Bytes 66 119.
16 5 Dec 9 19:27:37 NAT: Close UDP [200.1.1.36/1107]->[10.144.36.164/61554]->[10.144.34.13/53] Pkts 1 1, Bytes 73 126.
16 5 Dec 9 19:27:45 NAT: Close TCP [200.1.1.66/1398]->[100.30.10.1/31171]->[100.30.10.12/9000] Pkts 3 3, Bytes 144 120.
17 5 Dec 9 19:27:59 FILTER: Remote access filter blocks: UDP bcast tl0 [100.30.10.11/1033]->[255.255.255.255/8351] l=45.
16 5 Dec 9 19:28:22 NAT: Close UDP [200.1.1.84/1026]->[10.144.36.164/61559]->[10.144.34.13/53] Pkts 4 4, Bytes 228 228.
17 5 Dec 9 19:28:29 FILTER: Remote access filter blocks: UDP bcast tl0 [100.30.10.11/1033]->[255.255.255.255/8351] l=45.
16 5 Dec 9 19:28:45 NAT: Close TCP [200.1.1.66/1399]->[100.30.10.1/31172]->[100.30.10.12/9000] Pkts 3 3, Bytes 144 120.
17 5 Dec 9 19:28:59 FILTER: Remote access filter blocks: UDP bcast tl0 [100.30.10.11/1033]->[255.255.255.255/8351] l=45.
16 5 Dec 9 19:29:22 NAT: Close UDP [200.1.1.84/1026]->[10.144.36.164/61560]->[10.144.34.13/53] Pkts 5 5, Bytes 280 280.
17 5 Dec 9 19:29:29 FILTER: Remote access filter blocks: UDP bcast tl0 [100.30.10.11/1033]->[255.255.255.255/8351] l=45.
16 5 Dec 9 19:29:45 NAT: Close TCP [200.1.1.66/1400]->[100.30.10.1/31173]->[100.30.10.12/9000] Pkts 3 3, Bytes 144 120.
17 5 Dec 9 19:29:59 FILTER: Remote access filter blocks: UDP bcast tl0 [100.30.10.11/1033]->[255.255.255.255/8351] l=45.
18 5 Dec 9 19:30:20 WWW: [200.1.1.36/1109]->[100.30.10.17/80] GET http://tp4cb//nod_32_aktualizace/update.ver.
17 5 Dec 9 19:30:29 FILTER: Remote access filter blocks: UDP bcast tl0 [100.30.10.11/1033]->[255.255.255.255/8351] l=45.

3.1.2 Požadavky na systém Firewallu

- procesor kompatibilní s procesory Intel Pentium řady 386, 486 nebo novější
- 16 MB operační paměti
- disketová jednotka
- tři síťové adaptéry
- grafický adaptér VGA nebo kompatibilní
- port tiskárny pro připojení obvodu ochrany před kopírováním

Velkým nedostatkem produktu GNATBOX je omezená podpora síťových adaptérů. Protože operační systém vychází ze systému BSD, jsou k dispozici pouze ovladače síťových adaptérů pro tento operační systém. Podporována je většina adaptérů výrobců 3Com, Compaq, Dec, SMC, Intel [Obr. 2].



Obr. 2 *Konfigurace adaptéru VGA a síťových karet* [11]

3.2 Bezdrátové přemostění dvou sítí

Spojení dvou budov sítí LAN pomocí kabelového Ethernetu lze uskutečnit na vzdálenost až 100 metrů. Protože pokládka metalického vedení není možná, byla přijata v rámci bezpečnostního projektu možnost realizace propojení sítí pomocí rádiového přemostění sítí s ohledem na co nejúčinnější zajištění bezpečnosti provozu informačních technologií. Předpokladem je využití služeb Firewallu GNATBOX při začlenění přípojného bodu rádiového provozu v demilitarizované zóně a vytvoření funkčního tunelu VPN technologie.

3.2.1 Přístupové body

Přístupové body pracují pouze jako mezistanice mezi kabelovou a bezdrátovou sítí. Pouze pokud oba Access Pointy disponují funkcí Point to Point Bridge, existuje možnost přemostění. Pro přemostění dvou sítí LAN jsou potřebné dvě zařízení Wireless Access Point 802.11g 54 Mbps. Princip Wireless Bridge k propojení lokálních sítí se nazývá Point to Point. Přístupový bod v režimu síťového přemostění neplní úlohu Access Pointu, oba přístupové body v režimu

Point to Point plní funkci síťového mostu. Vytvářejí tak fyzické propojení mezi sítěmi a příslušné pakety posílají do druhé sítě. Aktivací a spuštěním spojení síťového mostu přístupové body v režimu Wireless Bridge ztrácejí schopnost funkce přístupových bodů a nelze pomocí nich dále obsluhovat další bezdrátové klienty.

4 Ověření parametrů sítě, propustnost a bezpečnost provozu

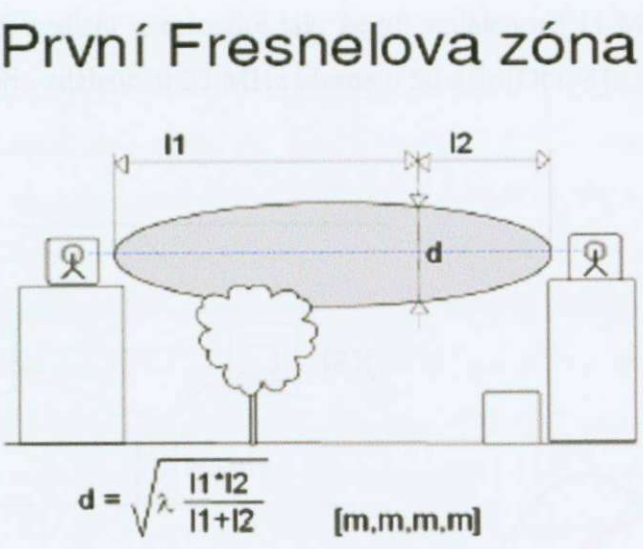
4.1 Bezdrátová síť 802.11 [7]

Výstavba a provoz rádiové sítě přináší jistá specifika. Rádiová síť se od kabelové sítě odlišuje technologicky, a to především spojovou vrstvou, její podvrstvou označovanou jako MAC, ovládáním přístupu k médiu, který představuje soubor pravidel určujících, jak přistupovat k prostředkům pro přenos dat. Samotné detaily o přenosu jsou ovšem ponechány na fyzické vrstvě PHY.

4.1.1 Komponenty bezdrátové sítě [7]

Připojení je realizováno pomocí konektoru RJ-45 (ethernet), a tak jediným rozdílem zůstává rychlost spojení 10 nebo 100 Mb/s. Skutečná přenosová rychlost standardu 802.11g se při příznivé situaci pohybuje okolo 20 Mb/s, zbytek do teoretické rychlosti 54 Mb/s tvoří data používaná transportní vrstvou, tedy režie provozu bezdrátové sítě.

Napájení zařízení standardu 802.11 je uskutečněno pomocí síťového adaptéru. Přístupové body ve funkci síťového mostu jsou vybaveny externími směrovými anténami. Vyzařovací úhel popisuje anténu a definuje do jakého směru a pod jakým úhlem anténa vyzařuje. Na plánu antény je zakresleno, jak anténa vyzařuje, a podle úchytných bodů lze zjistit, kde je střední rovina vyzařování. Zisk (gain) je nejdůležitější parametr antény [6]. Čím větší ziskovost, tím vzdálenější signál je anténa schopna zachytit. Jde o poměr mezi intenzitou vyzařování v daném směru k intenzitě vyzařování, kterou bychom obdrželi, kdyby energie přijatá anténou byla vyzařována rovnoměrně do všech směrů, tedy izotropní anténou (dipól). První Fresnelova zóna nejlépe vyjadřuje šíření elektromagnetické vlny v prostředí. Vlna se šíří po přímce, ale protože se jedná o vlnění, proto podléhá dalším fyzikálním zákonům (Huygensův princip). Převážná část energie vlny je nesena v prostoru okolo přímky spojující vysílací a přijímací antény. Celkové rozložení energie elektromagnetické vlny má tvar elipsoidu s největším průměrem uprostřed trasy [Obr. 3].



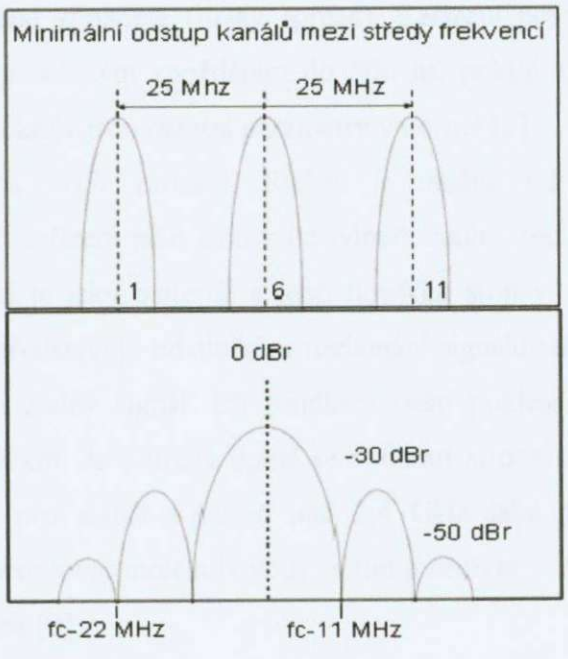
Obr. 3 *Rozložení energie elektromagnetické vlny* [11]

4.1.2 Šíření rádiového signálu, vlivy a rušení

Do šíření rádiových signálů v pásmu nad 2 GHz vstupuje značné množství faktorů. Největší hrozbu představují systémy postavené na modulaci FHSS [7].

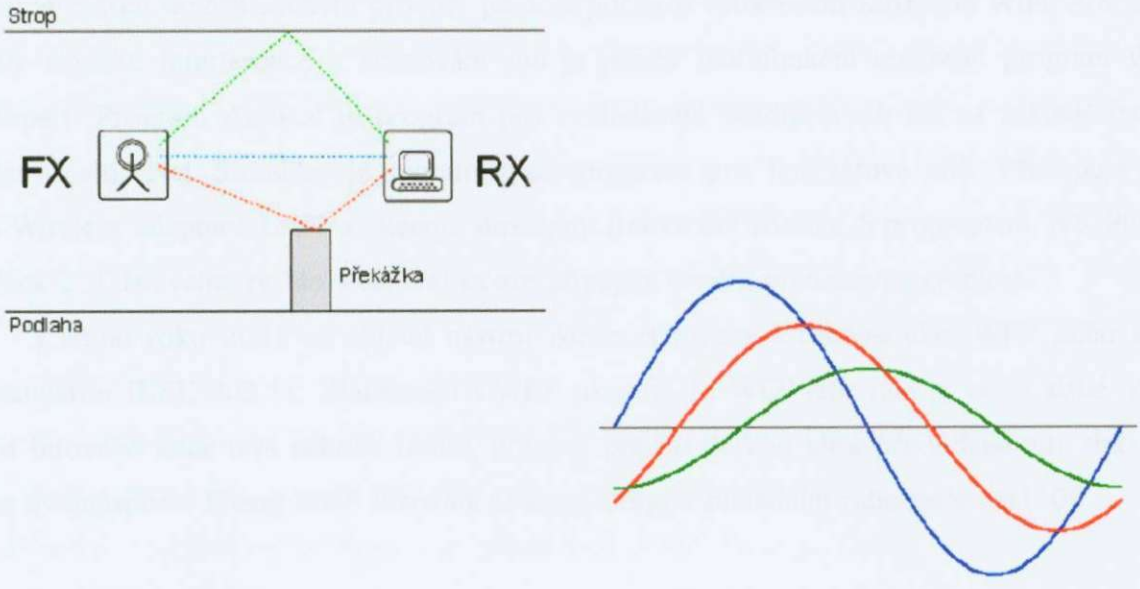
K dispozici je 13 povolených kanálů. Bohužel to neznamená, že máme 13 plnohodnotných frekvencí, ale technologie rozprostřeného spektra znamená vysílání do frekvenčního rozsahu 22 MHz. Odstup mezi kanály je pouze 5 MHz. Vysílání na jednom kanálu se překrývá s vysíláním na sousedních čtyřech kanálech.

KANÁL	FREKVENCE
1	2,412
2	2,417
3	2,422
4	2,427
5	2,432
6	2,437
7	2,442
8	2,447
9	2,452
10	2,457
11	2,462
12	2,467
13	2,472
14	2,484



Obr. 4 *Rozprostření energie při vysílání* [11]

Spodní detail obrázku ukazuje, jak ve skutečnosti vypadá vysílání na jednom kanálu. Energie se při vysílání rozprostírá tak, že při vzdálenosti 11 MHz od centrální frekvence klesne o 30 dBr a při vzdálenosti 22 MHz klesne o 50 dBr [Obr. 4].



Obr. 5 *Vícecestné interference*

Vysílač TX a přijímač RX zařízení používají všesměrové antény. Vzhledem k tomu, že se signál od překážek odráží, vytvoří se velké množství různých signálových cest od vysílače k přijímači. Na obrázku [Obr. 5] jsou znázorněny tři cesty. Zatímco původní signál putující po přímé cestě dorazil nejsilněji, odražené signály dorazily později posunuté v čase. Rádiový signál je vlnění a vlnění se v každém bodě skládá. Časový rozdíl mezi přijetím prvního a posledního signálu se nazývá rozprostřené zpoždění (delay spread). Zařízení pracující se standardem 802.11 se umí vyrovnat s rozprostřeným zpožděním do 500 ns, pokud zpoždění překročí tuto hranici nebude trasa funkční, ačkoliv jsou ostatní parametry v normě [8].

Další rušení mohou představovat jiná WiFi zařízení. Rušení je možné od dalších komerčních nebo spotřebních mikrovlnných zařízení jako jsou mikrovlnné trouby, technologie „bluetooth“ a bezdrátové telefony. Důležité je jaký materiál a jeho tloušťka stojí v cestě při průchodu signálu. Železobeton a silné zdi představuje odstínění a rozlámání signálu tak, že po 15 metrech nezachytí běžná anténa 2 dBi žádný signál. Při prudkém dešti poklesne signál o 0,05 dB/km, při běžném dešti o 0,02 dB/km. Je potřeba úplně se vyhnout stromům a listí. Mokré listí signál zcela odstíní. Voda je pro signál v pásmu nad 2,4 GHz také problém. Mikrovlny o této frekvenci mají schopnost excitovat molekuly vody, a tím jí ohřívat. Voda tedy vlny této frekvence pohlcuje a je jimi ohřívána [9].

4.1.3 Bezpečnost sítě 802.11

Zásadním problémem je skutečnost, že nelze vymezit s dostatečnou přesností prostor, kde je ještě elektromagnetické vlnění sítě standardu IEEE 802.11 možné registrovat a přijímat. V této síti je potom snadné zachytit provoz pomocí počítače vybaveném zařízením WiFi. Pro analýzu síly signálu, interference a skenování sítě je použit multifunkční testovací program WLAN Expert. Program Aerosol je program pro vyhledávání bezdrátových sítí na základě interních názvů sítí. Net Stumbler je monitorovací program pro bezdrátové sítě. Přistupuje přímo k Wireless adaptéru LAN a skenuje dostupný frekvenční rozsah. S programem WS Ping Pro Pack 2.30 lze velmi rychle otestovat síťové připojení a měřit přenosovou rychlost.

V srpnu roku 2001 se objevil nástroj AirSnort určený k rekonstrukci WEP klíčů v sítích standardu IEEE 802.11. Zkušenosti s WEP ukazují, že WEP šifrování je velmi slabé. Zjištění 64 bitového klíče trvá několik hodin, přičemž použití delšího klíče prodlužuje tuto dobu vždy na dvojnásobek. Přesto WEP šifrování se stává alespoň základním zabezpečením [10].

4.2 Propustnost a bezpečnost Firewallu GNATBOX

Již při návrhu bezpečnostního projektu a realizaci sítě byla vyjádřena míra paronie, která je pro tuto konkrétní síť vhodná a byla nastavena pravidla pro Firewall, která chrání síť před možným proniknutím.

Při rozhodování, zda určitý paket přes Firewall povolit či nikoliv, začne nastavený software s prvním pravidlem ve své sadě postupovat k poslednímu pravidlu, dokud není paket buď výslovně povolen, výslovně zakázán anebo dokud nedojde Firewall na konec pravidel. Pravidla je vždy nutné hodnotit ve stanoveném pořadí, aby nedocházelo k nesrovnalostem.

Program musí pakety odlišovat na základě rozhraní, na které dorazí, a rozhraní, z něhož budou posílány. Toto je podstatné, protože Firewall nemůže ve skutečnosti opravdu důvěřovat zdrojovým a cílovým adresám v samotných paketech, neboť tyto hodnoty lze snadno zfalšovat. Paket, který dorazí na externí rozhraní a udává, že je z vnitřní sítě, je jasným příznakem toho, že se děje něco velmi podezřelého.

Firewall umí filtrovat podle typů paketů TCP, UDP, ICMP, protože některé typy paketů jsou pro provoz sítě nezbytné. Jsou povoleny pakety ICMP s odezvou typu Echo reply směrem do sítě tak, aby mohly klientské počítače ověřit konektivitu na hostitelské počítače umístěné mimo síť, ale jsou zakázány pakety ICMP se žádostmi typu Echo request směrem do sítě na tyto klientské počítače.

Firewall třídí provoz podle toho, odkud přichází a kam je určen. Externím počítačům je povoleno, aby ustavovaly připojení k dostupnému internímu webovému serveru, serveru FTP

a k serveru v demilitarizované zóně, ale rozhodně je zakázáno ustavovat připojení k interním klientům. Interním klientům je povoleno ustavovat připojení opačným směrem. Firewall je schopen permanentně blokovat problematické hostitelské počítače a sítě, nepovoluje jim žádný přístup a je schopen blokovat veškerý přístup k citlivým počítačům v síti.

Obdobně je nutné požadovat řízení paketů TCP a UDP podle toho, na jaké porty přicházejí a směřují. Externím uživatelům je povoleno připojovat se z jakéhokoliv portu na své vlastní počítače pouze na těch interních portech, které používají externě viditelné služby typu HTTP a FTP. Není povoleno externím uživatelům připojovat se na jakékoliv porty na interních počítačích, protože Trojské koně fungují tak, že otevírají porty nad 1023. Uvnitř sítě ale uživatelé potřebují iniciovat připojení přes zdrojové porty vyšší než 1023 s cílovým portem všech možných běžných portů protokolu TCP. Z těchto důvodů je zavedena restrikce pro uživatele pouze na několik cílových portů.

U hostitelských počítačů a směrovačů lze nastavit v hlavičce paketů IP mnoho vlastností. Některé vlastnosti jsou známé tím, že jsou zneužity k obcházení zabezpečení, přičemž nejčastěji zneužívanou možností je přímé směrování. Firewall pakety s nastaveným přímým směrováním zahazuje.

Firewall GNATBOX umí odlišovat mezi pakety, jenž požadují připojení a pakety, které se pouze posílají nebo odpovídají přes již ustavené připojení. Rozdíl mezi těmito dvěma typy paketů tvoří pouze jeden bit (ACK). Pakety, které požadují připojení, mají tento bit vymazaný a všechny ostatní typy ho mají nastavený. Toto pravidlo je užito u zdrojových a cílových vlastností k povolení připojení pouze k těm portům, které jsou v pravidlech uvedeny a pouze v tom směru, jenž je povolen.

Uvedená pravidla pro pakety se zabývají pouze hlavičkou paketů IP nebo ICMP, datová část se nekontroluje. Pravidla pro pakety neumí odstranit z e-mailů viry ani neumí utajit existenci interních počítačů [11].

4.3 Bezpečnost prvků v reálném provozu

S vysokou úrovní zabezpečení provozu sítě je nutné:

- Permanentně provozovat činnosti, které zajišťují zřejmé mezery v zabezpečení a nemají žádný negativní efekt na dostupnost v nedůvěryhodném prostředí. Bezpečnostní produkty, a to ať už takové, které se starají o zajištění systémů před možnými hrozbami jako jsou antivirové či antispywarové aplikace, firewally, systémy pro detekci průniků a podobné, nebo takové, které mají za úkol aktivní zajištění počítačů a dat (autentizační systémy, šifrovací prostředky, generátory VPN, ochranné nástroje, limitery

uživatelského přístupu a další) jsou aplikace a systémy jako každé jiné. I tyto aplikace jsou programovým dílem a i ony se musí před svým nasazením velmi důkladně testovat. Obvykle se testuje schopnost aplikace ubránit se proti pokusu o nechtěné vyřazení z provozu nebo proti napadení nějakým běžně známým způsobem. Chyby v bezpečnostních produktech jsou často stejné povahy jako nedostatky v běžných systémech. Prevencí před možným nebezpečím plynoucím z chyb, nedostatků či nechtěných vlastností firewallu, antivirových programů nebo jiných ochranných prostředků, je použití jejich zdvojení. Na jednom počítači nelze aplikovat dva antivirové programy(docházelo by k jejich kolizím), ale je možné použít zdvojenou ochranu v rámci práce s e-mailovým účtem. Zatímco jeden antivir se nachází na serveru, jiný chrání poštu doručovanou do lokální e-mailové aplikace.

- Instalovat nejaktuálnější záplaty operačních systémů, jak na klientských počítačích, tak i na serverech v síti. Počet objevených chyb a bezpečnostních nedostatků operačních systémů stoupá. Jak se zvyšuje počet objevených chyb, stoupá i rychlost jejich opravy a aktualizace příslušných produktů. Nikdy ale nelze říci, že by tento proces dostatečně kopíroval nacházení nových nedostatků, a tak jsou systémy vždy v určitý okamžik svého životního cyklu zranitelné.

- Neumísťovat síťové účty uživatelů na počítače se službami nedůvěryhodné sítě (webový server, server FTP, Firewall) a pro tyto počítače mít zvláštní administrátorské účty s různými hesly. Aplikovat Centrální správu identit. Správa identit je v informačních systémech proces správy uživatelů a systémových entit v celé organizaci. Necentrální správa účtů je velice nákladná manuální činnost a je náchylná na lidské chyby. Správa identit tyto distribuované a manuální úkony centralizuje a automatizuje, čímž při zvýšené bezpečnosti současně snižuje náklady a náchylnost k chybám. Aplikace a systémy mohou využít jednotnou bezpečnostní platformu a úložiště, a to buď přímo, nebo pomocí automatizovaných replikací se svým vlastním úložištěm. Není tedy nutné nadále spravovat uživatelské účty individuálně v jednotlivých aplikacích, ale lze vše implementovat centrálně z jednoho místa. Jakékoliv změny uživatelských účtů se tak automaticky promítnou do všech integrovaných a synchronizovaných aplikací a systémů.

- Vyhodnocovat systémové záznamy a vyhledávat neúspěšné pokusy o přihlášení k síťovým službám a neúspěšné pokusy o přihlášení k serverům.

- Kontrolovat systémové uživatelské účty a zajišťovat nepovolené přidávání nebo úpravu uživatelských účtů pro síťové služby.

- Deaktivovat veškeré nepotřebné služby na síti a na vlastních serverech nedůvěryhodného prostředí sítě.

- Sledovat dostupné informace od specializovaných společností zabývajících se bezpečností dat a operačních systémů. Tyto společnosti vydávají pravidelné informace o nejnovějších nalezených rizicích a jejich možném řešení.

Seznam použitých zkratek

AES	Advaced Encryption Standard
BSD	Operační systém Unix typu open-source
CCK	Complementary Code Keying
DES	Data Encryption Standard
DFS	Dynamic Frequency Selection
DHCP	Dynamic Host Configuration Protocol: Počítač se spuštěnou službou DHCP umožňuje automatickou dynamickou konfiguraci adres IP a souvisejících informací klientům s podporou protokolu DHCP
DMZ	Demilitarized Zone
DNS	Domaine Name Server: Hierarchická distribuovaná databáze obsahující mapování názvů domén DNS k různým typům dat, například adresám IP. Služba DNS umožňuje vyhledání počítačů a služeb podle srozumitelných názvů a také vyhledání jiných informací uložených v databázi
DSSS	Direct Sequence Spread Spectrum
EDI	Electronic Data Interchange
ETSI	European Telecommunications Standards Institute
FHSS	Frequency Hopping Spread Spectrum
FTP	File Transfer Protocol: Člen sady protokolů TCP/IP používaný ke kopírování souborů mezi dvěma počítači v síti Internet. Oba počítače musí podporovat příslušné role protokolu FTP: jeden musí být klientem a druhý serverem FTP

HTTP	Hyper Text Transfer Protocol
HTTPS	Hyper Text Transfer Protocol Secure
ICMP	Internet Control Message Protocol: Protokol ICMP umožňuje hostitelům a směrovačům využívající komunikaci IP ohlašovat chyby a vyměňovat si omezené řídící a stavové informace
IDEA	International Data Encryption Algorithm
IEEE	Institute of Electrical and Electronics Engeneers
IMAP	Internet Mail Access Protocol
IPSec	Internet Protocol Security
IP	Internet Protocol
LPR	Line Printer Remote: Nástroj umožňující připojení, který je spuštěn na klientských systémech a slouží k tisku souborů do počítače se serverem LPD
MAC	Media Access Control
NAT	Network Address Translation
NNTP	Net News Transfer Protocol
OFDM	Orthogonal Frequency Division Multiplex
PBCC	Packet Binary Convolutional Coding
POP	Post Office Protocol
RPC	Remote Procedure Call: Služba RPC je určena k předávání funkcí volaných aplikacemi do vzdáleného systému prostřednictvím

	počítačové sítě. Služba RPC se obvykle používá pro vzdálenou správu výpočetní techniky
RTS/CTS	Request to Send/Clear to Send
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SSID	Service Set Identifier
TCP	Transport Control Protocol: Sada síťových protokolů používaných v síti Internet, která poskytuje komunikaci v rámci vzájemně propojených sítí tvořených počítači s různou hardwarovou architekturou a různými operačními systémy. Protokol TCP/IP zahrnuje standardy pro komunikaci počítačů a konvence propojování sítí a směrování provozu [12]
TKIP	Temporal Key Integrity Protocol
UDP	User Datagram Protocol: Doplněk protokolu TCP nabízející službu datagramů bez připojení, která nezaručuje doručení ani správné uspořádání doručených paketů
VPN	Virtual Private Network
WLAN	Wireless Local Area Network: Technologie WLAN umožňuje uživatelům vytvářet bezdrátová připojení v rámci místní oblasti. Sítě WLAN lze používat v dočasném místě firmy nebo na jiných místech, kde by instalace příliš mnoha vodičů byla na překážku, nebo jako doplnění stávající sítě LAN
WEP	Wired Equivalent Privacy
Wi-Fi	Wireless Fidelity
WPA	Wi-Fi Protected Access

IETF (Internet Engineering Task Force): Skupina IETF je standardizační organizace pro síť Internet

ISM (Intersite Messaging Service): Služba podporující přenosy pro asynchronní zasílání zpráv mezi sítěmi. Každý přenos má dvě hlavní role: odesílání/příjem a topologické dotazy

NetBIOS (Network basic input/output systém): Rozhraní API (Application Programming Interface), které mohou využívat programy v místní síti (LAN). Systém NetBIOS poskytuje programy s jednotnou sadou příkazů pro požadování služeb nižší úrovně, mezi něž patří správa názvů, řízení relací či posílání datagramů mezi uzly v síti

IEEE: Organizace Institute of Electrical and Electronics Engineers založená v roce 1963. IEEE je organizace sdružující inženýry, vědce a studenty známá především vývojem standardů v počítačovém průmyslu a v elektronice

PAKET: Přenosová jednotka síťových vrstev OSI (Open Systems Interconnection) skládající se z binárních informací reprezentujících data a záhlaví obsahující identifikační číslo, zdrojovou a cílovou adresu a data pro řízení chyb

SOKET: Identifikátor pro konkrétní službu v konkrétním uzlu sítě. Soket je tvořen adresou uzlu a číslem portu, které identifikuje služby. Existují dva druhy soketů – datové obousměrné proudy a datagramy

TELNET: Protokol terminálové emulace používaný v síti Internet k přihlášení k síťovým počítačům. Protokol TELNET také odkazuje na aplikace, které používají tento protokol pro uživatele, kteří se přihlašují ze vzdáleného umístění

TRACERT: Příkaz určující trasu tím, že do cíle odešle zprávy protokolu ICMP s požadavkem na odezvu se zvyšujícími se hodnotami polí TTL (Time to Live). Zobrazenou cestu představuje seznam bližších rozhraní směrovačů na trase mezi zdrojovým hostitelem a cílem. Bližší

rozhraní je rozhraní směrovače , které je k odesílajícímu hostiteli z hlediska cesty nejblíže

WINS: Služba, která dynamicky mapuje adresy IP na názvy počítačů (názvy pro rozhraní NetBIOS). Umožňuje tak uživatelům přístup k prostředkům na základě názvu, není tedy nutné používat adresy IP, jejichž zapamatování je složité

Závěr

Tato diplomová práce se zabývá řešením bezpečnostních rizik při provozu výpočetní techniky v počítačových sítích. Byly zde vyjádřeny a použity prvky zajišťující bezpečnost a spolehlivost zpracovávaných dat. Již při realizaci a následném provozu počítačových sítí se ovšem ukazuje, že i s použitím současných prostředků je potřeba neustále sledovat vývoj informačních technologií. Jsou vyvíjeny nové prostředky a aplikace, které je nutné implementovat do stávající konfigurace.

Seznam použité literatury

[1] Rodryčová, D.: Jak prezentovat firmu, produkt, sebe, názor. Grada, Praha 1998.

[2] PricewaterhouseCoopers, Národní bezpečnostní úřad a časopis DSM – data security management: Průzkum stavu informační bezpečnosti, 1999.

[3] Rodryčová, D., Staša, P.: Bezpečnost informací, Grada Publishing, Praha 2000.

[4] Strebe, M., Perkins, Ch.: Firewally a proxy servery, Computer Press, Brno 2003.

[5] Jansen, H., Rötter, H. a kol.: Informační a telekomunikační technika, Europa Sobotáles, Praha 2004.

[6] Černohorský, D., Nováček, Z.: Antény a šíření rádiových vln, VUT, Brno 2001.

[7] Köhre, T.: Stavíme si bezdrátovou síť Wi-Fi, Computer Press, Brno 2004.

[8] Hrdina, Z., Vejražka, F.: Digitální rádiová komunikace, ČVUT, Praha 1994.

[9, 10] Odborné publikace uveřejněné na internetu, www.zcomax.cz.

[11] Technická dokumentace dodavatelů a prodejců výpočetní techniky

[12] Häberle, H. a kol.: Průmyslová elektronika a informační technologie, Europa Sobotáles, Praha 2003.